ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ВИННИЧЕНКА

Кваліфікаційна наукова праця
на правах рукопису

КРУШЕНІЦЬКИЙ ВЛАДИСЛАВ СЕРГІЙОВИЧ

УДК 342.9:351.88:004.738.5(477)

ДИСЕРТАЦІЯ
АДМІНІСТРАТИВНО-ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ У ПУБЛІЧНО-ІНФОРМАЦІЙНІЙ СФЕРІ

081 «Право»
Подається на здобуття наукового ступеня доктора філософії

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

_____ **В. С. Крушеніцький**

Науковий керівник –
доктор юридичних наук, професор
Соболь Євген Юрійович

Кропивницький – 2025

АНОТАЦІЯ

Крушеніцький В. С. Адміністративно-правові засади забезпечення національної безпеки у публічно-інформаційній сфері. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 081 «Право». – Центральноукраїнський державний університет імені Володимира Винниченка, Кропивницький, 2025.

У дисертації здійснено комплексне наукове дослідження адміністративно-правових засад забезпечення національної безпеки в публічно-інформаційній сфері, що набуває першорядного значення в умовах цифровізації, гібридних форм протидії, зростання інформаційних загроз та активізації дезінформаційних впливів на суспільно-політичні процеси. Національну безпеку в інформаційному просторі важливо розглядати одним із значущих елементів державної політики й водночас системоутворювальним механізмом захисту конституційного ладу, прав і свобод людини, демократичних інститутів та суверенітету держави.

У роботі розкрито теоретико-правові засади формування поняття і змісту інформаційної безпеки, визначено її місце в системі національної безпеки України, окреслено основні принципи та елементи адміністративно-правового регулювання відносин у публічно-інформаційній сфері. Особливу увагу зосереджено на аналізі нормативно-правових актів, що визначають механізми запобігання, виявлення, нейтралізації та реагування на інформаційні загрози, а також забезпечують баланс між захистом державних інтересів і гарантуванням конституційних прав громадян.

Підґрунтям цього дослідження є міждисциплінарна методологія, що поєднує доктринальні підходи адміністративного права, теорії національної безпеки, публічного управління, інформаційного права та міжнародно-правових стандартів діяльності держави у сфері кібербезпеки та інформаційної безпеки. Застосування комплексного наукового підходу дало змогу проаналізувати

діяльність органів публічної влади й правоохоронних інституцій щодо забезпечення національної безпеки в інформаційному просторі, виявити недоліки чинної системи реагування на інформаційні загрози, визначити актуальні механізми та інструменти їх запобігання.

Розкрито зміст, сутність і ключові структурні характеристики національної безпеки в публічно-інформаційній сфері; простежено її становлення як особливої сфери державної політики для забезпечення цілісності інформаційного простору, стійкості комунікаційного середовища та захищеності критично важливих інформаційних ресурсів. Доведено, що інформаційна безпека є компонентом безпекової системи держави й показником рівня демократичності публічного управління, здатності держави реагувати на гібридні загрози та підтримувати стандарти прозорості, відкритості й об'єктивності суспільного дискурсу.

Окреслено коло суб'єктів та об'єктів забезпечення національної безпеки в публічно-інформаційній сфері. Зокрема, окреслено три групи суб'єктів: стратегічні (Президент України, Верховна Рада України, РНБО, Кабінет Міністрів України), що формують політику у сфері інформаційної безпеки; операційно-виконавчі (центральні органи виконавчої влади, Служба безпеки України, правоохоронні органи), що реалізують заходи протидії загрозам; суспільно-громадські (інститути громадянського суспільства, ЗМІ, аналітичні центри, освітні установи), які забезпечують інформування, експертний супровід, громадський моніторинг та формування інформаційної культури.

Об'єктами державного впливу визначено інформаційні ресурси, критичну інфраструктуру, комунікаційні платформи, цифрові сервіси, а також інформаційні потоки, що можуть стати каналами деструктивного впливу. Основні напрями забезпечення інформаційної безпеки охоплюють моніторинг інформаційного середовища, превентивні заходи, протидію дезінформації, забезпечення кібербезпеки, правозастосовну діяльність, комунікаційну політику та просвітницькі ініціативи.

Проаналізовано сучасний стан державної політики в галузі національної безпеки в публічно-інформаційному вимірі. З'ясовано, що національну політику структуровано неповністю, її елементи часто продубльовано, розвинено фрагментарно або не пов'язано управлінською логікою, попри значний масив нормативно-правових актів. Виявлено відсутність єдиної узгодженої концепції розвитку системи інформаційної безпеки, нестачу механізмів координації та системного управління ризиками. Доведено, що відсутність комплексного підходу ускладнює реагування на гібридні інформаційні впливи, знижує ефективність правоохоронної діяльності та перешкоджає формуванню стійкого комунікаційного середовища.

Представлено багаторівневу модель адміністративно-правового регулювання інформаційної безпеки, що поєднує конституційні норми, базові закони, спеціальне інформаційне й законодавство в галузі кібербезпеки, підзаконні акти й урядові стратегії. Наголошено на важливості імплементації міжнародних стандартів, передусім європейських (NIS2, GDPR, Кодекс практик ЄС щодо дезінформації), спрямованих на прозорість управління даними, зміцнення кіберстійкості й посилення відповідальності суб'єктів цифрових послуг. Підкреслено, що забезпечення інформаційної безпеки охоплює обов'язки держави й створення умов для активної участі громадян, медіа та інститутів громадянського суспільства в розбудові безпечного інформаційного середовища.

Систематизовано адміністративно-правові форми забезпечення інформаційної безпеки: від нормативних та контрольних до правозастосовних, превентивних, моніторингових та комунікаційних. До таких форм належать розроблення регулятивних документів; здійснення державного нагляду та аудиту інформаційної безпеки; реагування на кіберінциденти; державний та громадський моніторинг інформаційних потоків; проведення інформаційних кампаній; організація прескомунікацій; застосування санкцій та інших юридичних інструментів впливу. Виокремлено перспективні цифрові форми:

використання алгоритмічних систем раннього виявлення загроз, функціонування електронних платформ для звітності суб'єктів інформаційного простору, інтерактивні інструменти оцінки інформаційної доброчесності та кіберстійкості.

У дослідженні засвідчено, що ефективність інформаційної безпеки залежить не лише від формальних процедур, а й від їх реальної здатності забезпечувати своєчасне виявлення ризиків, оперативне реагування та належну міжвідомчу координацію. З огляду на це адміністративно-правові механізми упорядковано за рівнем регламентації (нормативно закріплені, частково регламентовані, гнучкі ініціативні); за суб'єктами реалізації (державні, муніципальні, громадські, приватні); за функціональним призначенням (превентивні, контрольні, реагувальні, аналітичні); за формами здійснення (публічні, цифрові, змішані), тобто адміністративно-правові механізми розглянуто як динамічну систему, що забезпечує адаптивність державної політики до еволюції інформаційних загроз.

Проаналізовано міжнародні стандарти у сфері інформаційної безпеки, що формують європейську систему протидії інформаційним загрозам. У документах Ради Європи, ЄС, НАТО та ООН засвідчено, що захист інформаційного простору вимагає збалансованого поєднання безпекових інструментів і демократичних гарантій, передусім захисту прав людини, свободи слова та доступу до інформації. У міжнародних правових актах зазначено, що інформаційну політику держави потрібно вибудовувати на зміцненні суспільної довіри, підвищенні прозорості алгоритмічних систем, гарантуванні відповідальності суб'єктів цифрових платформ. Водночас у міжнародних стандартах окреслено межі допустимого втручання держави: інформаційна безпека не може легітимувати надмірну цензуру, політичний тису або обмеження свободи вираження поглядів.

Доведено, що в умовах євроінтеграції забезпечення публічно-інформаційної безпеки має перейти від розрізнених ініціатив до комплексної інституційної моделі, заснованої на ризик-орієнтованому управлінні, технологічній інтеграції, належному адмініструванні даних і розвитку механізмів співрегулювання.

Аргументовано важливість прийняття спеціального закону «Про інформаційну безпеку», модернізації законодавства про кібербезпеку, дані та цифрові платформи, створення єдиного координаційного центру управління інформаційною безпекою, а також запровадження інституту уповноважених з управління даними. Системне впровадження таких інструментів сприятиме підвищенню стійкості держави до інформаційних загроз, формуванню прозорого, передбачуваного та людиноцентричного інформаційного порядку й зміцненню партнерства між державою, суспільством і приватним сектором.

Ключові слова: адміністративне регулювання, адміністративно-правове забезпечення, адміністративно-правові засади, адміністративно-правовий механізм, адміністративно-правові засоби, адміністративно-правове регулювання, адміністративно-правовий механізм взаємодії, адміністративна відповідальність, інформація, публічна інформація, доступ до публічної інформації, публічна влада, публічно-інформаційна сфера, інформаційна сфера, інформаційна безпека, інформаційний простір, інформаційні загрози, дезінформація, цифрове середовище, цифровізація, цифрова безпека, цифрова економіка, цифрові виклики, цифрові загрози, кіберпростір, кіберзахист, економічна безпека, національна економіка, безпекове середовище, національна безпека, публічне управління, державна політика, цифрове урядування, спільна діяльність, взаємодія, правоохоронні органи, інформаційний простір, цифрові інновації та технології, безпека, сектор безпеки, публічне управління у сфері безпеки, адміністративне право.

ANNOTATION

Krushenitskyi V. S. Administrative and legal principles for ensuring national security in the public information sphere. – Qualification scientific work in the form of a manuscript.

Dissertation for the degree of Doctor of Philosophy in specialty 081 «Law». – Volodymyr Vynnychenko Central Ukrainian State University, Kropyvnytskyi, 2025.

The dissertation presents a comprehensive scientific study of the administrative and legal principles of ensuring national security in the public information sphere, which is gaining key importance in the context of digitalization, hybrid forms of counteraction, the growth of information threats and the intensification of disinformation influences on socio-political processes. National security in the information space appears not only as an element of state policy, but as a system-forming mechanism for protecting the constitutional order, human rights and freedoms, democratic institutions and state sovereignty.

The work examines the theoretical and legal foundations of the concept and content of information security, defines its place within Ukraine's national security system, and identifies the key principles and elements of administrative and legal regulation in the public information sphere. Particular emphasis is placed on analysing regulatory acts that establish mechanisms for preventing, detecting, neutralizing and responding to information threats, as well as ensuring a balance between protecting state interests and safeguarding citizens' constitutional rights.

The dissertation research is based on an interdisciplinary methodology that combines doctrinal approaches of administrative law, national security theory, public administration, information law and international legal standards of state activity in the field of cyber and information security. The use of a comprehensive scientific approach made it possible to investigate the activities of public authorities and law enforcement institutions in ensuring national security in the information space, identify shortcomings of the current system of responding to information threats, and determine relevant mechanisms and tools for their prevention.

The content, essence and key structural characteristics of national security in the public information sphere are revealed. Its formation as a special sphere of state policy, designed to ensure the integrity of the information space, the stability of the

communication environment and the protection of critically important information resources, is traced. It is proven that information security is not only a component of the state's security system, but also an indicator of the level of democracy of public administration, the state's ability to respond to modern hybrid threats and maintain high standards of transparency, openness and objectivity of public discourse.

The range of subjects and objects of ensuring national security in the public information sphere is outlined. Three groups of subjects are distinguished: strategic (President of Ukraine, Verkhovna Rada, National Security and Defense Council, Cabinet of Ministers), which determine policy in the field of information security; operational and executive (central executive bodies, Security Service of Ukraine, law enforcement agencies), which implement measures to counter threats; public (civil society institutions, media, analytical centers, educational institutions), which provide information, expertise, public monitoring and the formation of information culture.

The objects of state influence are identified as information resources, critical infrastructure, communication platforms, digital services, as well as information flows that can become channels of destructive influence. The main areas of information security include monitoring of the information environment, preventive measures, countering disinformation, ensuring cyber protection, law enforcement, communication policy, and educational activities.

The current state of state policy in the field of national security in the public information sphere is analyzed. It is established that despite a significant array of regulatory legal acts, national policy remains incompletely structured, its elements are often duplicated or develop fragmentarily. The absence of a single, coordinated concept for the development of the information security system, the lack of integrated coordination mechanisms and systemic risk management are revealed. It is proven that the lack of a comprehensive approach complicates the response to hybrid information influences, reduces the effectiveness of law enforcement activities and hinders the formation of a sustainable communication environment.

A multi-level model of administrative and legal regulation of information security is presented, which combines constitutional norms, basic laws, special information and cybersecurity legislation, by-laws and government strategies. The importance of implementing international standards, primarily European ones (NIS2, GDPR, EU Code of Practice on Disinformation), aimed at increasing the transparency of data management, strengthening cyber resilience and increasing the responsibility of digital service providers, is emphasized. It is emphasized that ensuring information security includes not only the duties of the state, but also the need to create conditions for the active participation of citizens, media and civil society institutions in the formation of a safe information environment.

Administrative and legal forms of ensuring information security are systematized: from regulatory and control to law enforcement, preventive, monitoring and communication. Such forms include the development of regulatory documents; implementation of state supervision and audit of information security; response to cyber incidents; state and public monitoring of information flows; conducting information campaigns; organization of press communications; application of sanctions and other legal instruments of influence. Promising digital forms are highlighted: use of algorithmic systems for early detection of threats, functioning of electronic platforms for reporting by subjects of the information space, interactive tools for assessing information integrity and cyber resilience.

The study shows that the effectiveness of information security depends not only on formal procedures, but also on their real ability to ensure timely risk identification, prompt response and proper interdepartmental coordination. In view of this, administrative and legal mechanisms are arranged by level of regulation (normative, partially regulated, flexible initiative), by implementing entities (state, municipal, public, private), by functional purpose (preventive, control, response, analytical) and by forms of implementation (public, digital, mixed).

The international standards in the field of information security, which form the European system for countering information threats, are considered. The documents of the Council of Europe, the EU, NATO and the UN emphasize that the protection of the information space requires a balanced combination of security measures and democratic guarantees, in particular the protection of human rights, freedom of speech and access to information. International documents determine that the information policy of the state should be aimed at strengthening public trust, increasing the transparency of algorithmic systems, and ensuring the responsibility of digital platform entities. At the same time, the limits of permissible state intervention are also highlighted: information security cannot serve as an excuse for excessive censorship, political pressure or suppression of freedom of speech.

It is proven that in the context of European integration, ensuring public information security should move from disparate initiatives to a comprehensive institutional model based on risk-based management, technological integration, proper data administration, and the development of co-regulation mechanisms. The need to adopt a special law «On Information Security», modernize legislation on cyber defense, data, and digital platforms, create a single coordination center for information security management, and introduce the institute of data governance officers is argued. The systematic implementation of such tools will contribute to increasing the state’s resilience to information threats, the formation of a transparent, predictable, and human-centric information order, and the strengthening of partnerships between the state, society, and the private sector.

Keywords: administrative regulation, administrative and legal support, administrative and legal principles, administrative and legal mechanism, administrative and legal means, administrative and legal regulation, administrative and legal mechanism of interaction, administrative responsibility, information, public information, access to public information, public authority, public and information sphere, information sphere, information security, information space, information

threats, disinformation, digital environment, digitalization, digital security, digital economy, digital challenges, digital threats, cyberspace, cyber defense, economic security, national economy, security environment, national security, public administration, state policy, digital governance, joint activities, interaction, law enforcement agencies, information space. digital innovations and technologies, security, security sector, public administration in the field of security, administrative law.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ,

у яких опубліковано основні наукові результати дисертації:

1. Крушеніцький В. С. Публічно-інформаційна сфера як складова системи національної безпеки України. *Право і суспільство.* 2023. № 3. С. 585–590. URL: https://doi.org/10.32842/2078-3736/2023.3.88.

2. Крушеніцький В. С. Органи публічної влади як суб'єкти формування та реалізації політики національної безпеки в інформаційному просторі. *Наукові записки. Серія: Право.* 2024. № 17. С. 252–256. URL: https://doi.org/10.36550/2522-9230-2024-17-252-256.

3. Крушеніцький В. С. Адміністративно-правові механізми реагування на інформаційні загрози: теоретико-правовий аспект. *Право та державне управління.* 2024. № 4. С. 468–472. URL : https://doi.org/10.32782/pdu.2024.4.64.

4. Крушеніцький В.С. Зарубіжний досвід забезпечення національної безпеки у публічно-інформаційній сфері. *Науковий вісник Сіверщини. Серія: Право.* 2025. №3(26). С. 19–28. URL: https://doi.org/10.32755/sjlaw.2025.03.019.

5. Крушеніцький В. С. Роль Ради національної безпеки і оборони України у формуванні державної політики інформаційної безпеки. *Наукові записки. Серія: Право.* 2025. № 18. С. 164–167. URL: https://doi.org/10.36550/2522-9230-2025-18-164-167.

які засвідчують апробацію матеріалів дисертації:

1. Крушеніцький В. С. Роль правоохоронних органів у забезпеченні національної безпеки в інформаційному просторі. *Сектор безпеки України: актуальні питання науки та практики:* збірник наукових статей, тез доповідей та повідомлень за матеріалами XIII Міжнародної науково-практичної конференції (27 березня 2025 р., Національний юридичний університет імені Ярослава Мудрого, м. Харків). У 2-х частинах. Частина 1. Серія «Сектор безпеки України». Вип. 54. Харків: Друкарня Мадрид, 2025. С. 54–58.

2. Крушеніцький В. С. Принципи адміністративно-правового регулювання інформаційної безпеки в Україні: сучасний стан і перспективи розвитку. *Актуальні проблеми національного законодавства:* збірник матеріалів Міжнародної науково-практичної конференції, м. Кропивницький. 17 квітня 2025 р. Частина 1. Кропивницький, 2025. С. 104–106.

3. Крушеніцький В. С. Сутність та особливості національної безпеки у сфері публічної інформації. *Актуальні питання адміністративного права та адміністративного судочинства*: збірник наукових статей, тез доповідей та повідомлень за матеріалами II Міжнародної науково-практичної конференції (15 травня 2025 р., Національний юридичний університет імені Ярослава Мудрого, м. Харків). Серія «Сектор безпеки України». Вип. 55. Харків: Друкарня Мадрид, 2025. С. 64–69.

4. Крушеніцький В. С. Адміністративно-правові засоби забезпечення національної безпеки у публічно-інформаційній сфері. *Сталий розвиток економіки, права та державного управління в умовах глобальних викликів.* Міжнародна науково-практична конференція. 28 травня 2025 р. м. Анже, Франція. Видавництво Scholarly Publisher ICSSH. 2025. С. 66–68.

ЗМІСТ

ВСТУП

Обґрунтування вибору теми дослідження. Вибір теми дослідження зумовлено нагальною потребою держави модернізувати правові та організаційні механізми забезпечення національної безпеки в умовах розвитку інформаційного суспільства та цифрової трансформації. Нині інформаційний простір постає як один із визначальних компонентів національної безпеки, оскільки через нього відбувається комунікація, управління суспільними процесами, формування громадської думки та вплив на економічну й політичну стабільність. Водночас спостерігається наростання гібридних загроз, кібератак, дезінформаційних кампаній, маніпулятивних практик у соціальних мережах і спроб втручання в роботу об'єктів критичної інфраструктури. За таких умов актуалізується потреба вибудови цілісної адміністративно-правової системи, здатної забезпечувати превентивний, контрольний і примусовий вплив на інформаційні процеси, формувати дієві механізми міжвідомчої координації та підтримувати належний баланс між інтересами національної безпеки й дотриманням прав і свобод громадян у цифровому середовищі.

Тема дослідження вирізняється значною науковою й практичною вагомістю в контексті євроінтеграційних процесів, оскільки поступ України до європейського політичного, економічного та правового простору потребує гармонізації національного законодавства у сфері інформаційної безпеки з європейськими стандартами, зокрема NIS/NIS2, GDPR та іншими міжнародними нормами. Її актуальність посилюється тим, що сучасні технологічні зміни у сфері публічного управління, активне впровадження штучного інтелекту, платформізація комунікацій, цифровізація соціально-гуманітарних процесів та освітнього середовища вимагають від держави оновлення та підвищення ефективності адміністративно-правових механізмів регулювання й контролю інформаційного простору.

Зв'язок теми дисертації із сучасними дослідженнями. Проблематика забезпечення національної безпеки в публічно-інформаційній сфері нині посідає одне з чільних місць з-поміж першорядних напрямів досліджень у галузі адміністративного права, інформаційного права та публічному управлінні. Її актуальність зумовлено зростанням масштабів і складності інформаційних впливів, ускладненням форм гібридних загроз та потребою у формуванні дієвої системи протидії деструктивним інформаційним процесам. У сучасному науковому дискурсі питання адміністративно-правового регулювання інформаційної безпеки віддзеркалено в працях українських і зарубіжних дослідників, які вивчають проблеми нормативного забезпечення, організації діяльності уповноважених суб'єктів, міжнародної співпраці та імплементації загальновизнаних стандартів безпеки.

У вітчизняній правовій науці питання адміністративно-правового забезпечення національної безпеки в публічно-інформаційній сфері досліджує багато науковців, що засвідчує його багатовимірність та міждисциплінарність. Вагомий внесок у розроблення теоретичних і методологічних засад цієї проблематики зробили В. Авер'янов, В. Бевзенко, А. Берлач, Ю. Битяк, Н. Бортник, П. Діхтієвський, І. Гриценко, О. Карасс, Л. Кисіль, А. Козловський, В. Колпаков, О. Кузьменко, В. Курило, Є. Курінний, Н. Лесько, Р. Мельник, В. Настюк, О. Остапенко, А. Селіванов, О. Харитонова, В. Цвєтков, Я. Шевченко, Ю. Шемчушенко та інші дослідники.

У галузі інформаційного права окремі питання правового забезпечення інформаційної безпеки й еволюції інформаційного суспільства стали предметом ґрунтовних досліджень В. Антонюка, І. Арістової, О. Баранова, І. Діордіці, О. Дзьобаня, О. Довганя, О. Золотар, С. Єсімова, В. Калетніка, Р. Калюжного, М. Коваліва, В. Кондратенко, Б. Кормича, Т. Костецької, О. Кохановської, В. Ліпкана, Ю. Лісовської, А. Манжули, А. Марущака, Г. Новицького, Т. Перуна,

В. Пилипчука, Є. Соболя, О. Сокуренко, О. Солодкої, Т. Ткачука, О. Тихомирова, В. Цимбалюка, М. Швеця, І. Шопіної, О. Яреми та інших учених.

Монографічні дослідження, у яких комплексно представлено адміністративно-правові засади забезпечення національної безпеки в публічно-інформаційній сфері, у сучасній юридичній науці все ще є винятком. Наявні напрацювання здебільшого зосереджено на окремих сегментах проблематики – кібербезпеці, діяльності окремих суб'єктів сектору безпеки, цифровій трансформації публічного управління або захисті інформаційних прав людини.

У дисертаційних дослідженнях останнього десятиліття, зокрема в працях М. Баран «Адміністративно-правове забезпечення інформаційної безпеки в Україні» (2022) та О. Пугачова «Удосконалення державних механізмів забезпечення інформаційної безпеки України» (2025), виокремлено важливі концептуальні підходи до проблеми, проте розглянуто її фрагментарно – переважно в межах кіберзахисту, державного управління чи окремих напрямів інформаційної політики. У цих розвідках повною мірою не охоплено питання, пов'язані з правовим статусом суб'єктів публічної адміністрації, міжвідомчою взаємодією, превентивними та юрисдикційними механізмами реагування, впливом цифрової трансформації, імплементацією міжнародних стандартів (NIS2, GDPR, ISO/IEC 27001) та гарантуванням інформаційних прав людини.

З огляду на це обрана тема передусім відповідає сучасному науковому дискурсу й послідовно його розвиває, пропонуючи цілісний авторський підхід до аналізу адміністративно-правових засад функціонування державної системи інформаційної безпеки. У дослідженні структуровано принципи, елементи, механізми та суб'єктний склад інформаційної безпеки, інтегровано національні та європейські стандарти, сформовано концептуальні передумови для модернізації публічного управління в інформаційних відносинах.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертацію виконано відповідно до пріоритетних тематичних напрямів розвитку

науки і техніки, затверджених постановою Кабінету Міністрів України від 30 квітня 2024 р. № 476. Зокрема, особливу увагу зосереджено на напрямах, що охоплюють розвиток інформаційних і комунікаційних технологій, систем штучного інтелекту, кіберфізичних систем, Інтернету речей, робототехніки, методів комп'ютерної обробки сигналів, технологій глибокого навчання та аналізу великих даних, а також інфраструктури суперкомп'ютерних обчислень, хмарних сервісів, інтегрованих баз даних і національних інформаційних ресурсів. У роботі враховано актуальні тенденції цифровізації публічного управління, інтеграції алгоритмічних систем і штучного інтелекту в діяльність органів влади, а також спричинені ними виклики, пов'язані з гібридними інформаційними загрозами в умовах євроінтеграційних процесів. Тематику дослідження узгоджено з пріоритетами цифрової трансформації соціально-гуманітарної сфери та освіти в цифрову епоху. Дослідження виконано в межах плану науково-дослідної роботи Центральноукраїнського державного університету імені Володимира Винниченка «Концептуально-методологічні засади правового регулювання процесу європейської інтеграції України» (державний реєстраційний номер 200116U006126).

Мета й завдання дослідження. Метою дослідження є комплексний аналіз адміністративно-правового забезпечення національної безпеки в публічно-інформаційній сфері України з урахуванням міжнародних стандартів і кращих практик, виявлення прогалин у законодавстві та правозастосуванні, а також розроблення рекомендацій щодо вдосконалення нормативно-правових, організаційних і технологічних механізмів протидії інформаційним загрозам і підвищення ефективності національної системи інформаційної безпеки.

Для реалізації поставленої мети сформульовано такі завдання дослідження:

– розкрити поняття, зміст і сутність національної безпеки в публічно-інформаційній сфері;

- визначити систему й принципи адміністративно-правового регулювання забезпечення інформаційної безпеки;
- проаналізувати нормативно-правові акти у сфері національної безпеки в інформаційній сфері та оцінити їх результативність;
- схарактеризувати діяльність органів публічної влади щодо забезпечення національної безпеки в публічно-інформаційній сфері;
- з'ясувати роль правоохоронних органів у забезпеченні безпеки національного інформаційного простору;
- дослідити механізми адміністративно-правового реагування на інформаційні загрози та їх запобігання;
- узагальнити зарубіжний досвід забезпечення національної безпеки в публічно-інформаційній сфері та окреслити можливості його імплементації в Україні;
- обґрунтувати напрями вдосконалення адміністративно-правового регулювання національної безпеки в публічно-інформаційній сфері в умовах євроінтеграційних процесів.

Об'єктом дослідження є суспільні відносини та адміністративно-правові механізми, що забезпечують реалізацію державної політики у сфері інформаційної безпеки, формування нормативної бази та координацію діяльності органів публічної влади в публічно-інформаційній сфері.

Предмет дослідження – адміністративно-правові засади забезпечення національної безпеки в публічно-інформаційній сфері.

Методи дослідження. Для досягнення мети та виконання завдань дисертаційної роботи застосовано комплекс взаємопов'язаних загальнонаукових і спеціально-правових методів, що забезпечили всебічне, системне й об'єктивне опрацювання проблематики адміністративно-правового забезпечення національної безпеки в публічно-інформаційній сфері.

Методи аналізу та синтезу використано для деталізації об’єкта та предмета дослідження, зокрема для розкриття поняття і сутності національної безпеки у публічно-інформаційній сфері (підрозділ 1.1). За допомогою методу узагальнення сформовано теоретико-методологічні засади забезпечення інформаційної безпеки України та систематизовано наукові підходи до розуміння механізмів адміністративно-правового регулювання (підрозділ 1.2).

Діалектичний і логічний методи використано для встановлення причинно-наслідкових зв’язків у розвитку системи інформаційної безпеки, а також для уточнення понятійно-категоріального апарату дисертаційного дослідження.

Абстрактно-логічний метод забезпечив формування висновків і пропозицій у підсумкових положеннях роботи.

Порівняльно-правовий метод застосовано під час аналізу нормативно-правового забезпечення інформаційної безпеки України та в процесі вивчення зарубіжного досвіду (підрозділи 1.3, 3.1, 2.3).

Метод систематизації дозволив упорядкувати нормативно-правові акти, що регулюють національну безпеку в інформаційній сфері, виокремити їхні структурні зв’язки та визначити ключові елементи системи державного управління в цій сфері (підрозділ 1.3).

Системний метод застосовано для визначення концептуальних основ забезпечення національної безпеки в публічно-інформаційній сфері, для аналізу діяльності органів публічної влади (підрозділ 2.1) та правоохоронних органів (підрозділ 2.2).

Метод моделювання впроваджено для розроблення шляхів удосконалення державних механізмів забезпечення інформаційної безпеки України (підрозділ 3.2). Моделювання дало змогу сформувати оптимальні адміністративно-правові рішення та організаційні моделі реагування на інформаційні загрози.

Нормативною базою дослідження є Конституція України та законодавство у сфері національної й інформаційної безпеки, зокрема закони України: «Про національну безпеку України»; «Про основні засади забезпечення кібербезпеки України»; «Про інформацію»; «Про медіа»; «Про електронні комунікації»; «Про Державну службу спеціального зв'язку та захисту інформації України»; «Про захист інформації в інформаційно-телекомунікаційних системах»; підзаконні акти, стратегічні документи, відомчі регламенти органів публічної влади.

Емпіричну основу становлять практичні матеріали діяльності органів публічної влади у сфері інформаційної та національної безпеки, результати комплексних моніторингів стану інформаційного середовища України, аналітичні огляди, експертні матеріали, фахові дискусії та професійні консультації. Важливе значення мають також наукові публікації, довідково-енциклопедичні видання. Окрім того, емпіричною основою є авторські узагальнення, сформовані на підставі аналізу отриманих даних, актуальної правозастосовної практики та власних спостережень у процесі дослідження.

Наукова новизна отриманих результатів. Дисертація є однією з перших у вітчизняній адміністративно-правовій науці комплексних праць, у якій системно розкрито концепцію адміністративно-правових засад забезпечення національної безпеки в публічно-інформаційній сфері з огляду на європейські стандарти й виклики цифровізації. У дослідженні сформульовано й обґрунтовано низку нових наукових положень, висновків і практичних рекомендацій.

Уперше:

– комплексно обґрунтовано й систематизовано принципи адміністративно-правового регулювання інформаційної безпеки України, що дало змогу сформувати їх узагальнену багаторівневу класифікацію за сферою дії, функціональним призначенням, змістовно-ціннісною орієнтацією та джерелом нормативного закріплення;

– запропоновано концепцію ухвалення базового закону «Про інформаційну безпеку», який має забезпечити уніфікацію термінології, усунення нормативних колізій, чіткий розподіл повноважень між суб'єктами забезпечення інформаційної безпеки, стандартизацію адміністративних процедур та імплементацію європейських стандартів кібербезпеки та інформаційної безпеки;
– розроблено авторську трирівневу модель розмежування суб'єктів інформаційної безпеки в публічно-інформаційній сфері, яка поєднує інституційний, функціональний та управлінський підходи, визначає сфери відповідальності, повноваження й канали взаємодії; її впровадження може стати основою Концепції єдиної системи управління інформаційною безпекою України, забезпечивши узгодженість дій державних, муніципальних і громадських структур та підвищення ефективності публічного адміністрування;
– запропоновано системну класифікацію адміністративно-правових механізмів реагування та запобігання інформаційним загрозам, структуровану на три взаємопов'язані групи: превентивні для своєчасного попередження ризиків й підвищення кіберстійкості; оперативно-реагувальні забезпечують швидку локалізацію та усунення наслідків інформаційних інцидентів і відновлення функціонування критичних систем; юрисдикційні гарантують невідворотність юридичної відповідальності, підтримання правопорядку й дотримання законності в інформаційному просторі.

Удосконалено:

– інституційно-правову модель діяльності СБУ та інших суб'єктів сектору безпеки, що передбачає нормативне розмежування повноважень, розвиток ефективної міжвідомчої взаємодії та перехід до проактивного формату реагування на загрози;

- трактування механізмів адміністративно-правового реагування на інформаційні загрози; обґрунтовано, що вони є комплексом юридичних, організаційних і процедурних інструментів для превентивного, контрольного й примусового впливу держави на інформаційні процеси;
- організаційні й процедурні механізми забезпечення інформаційної безпеки через упровадження мультирівневого управління із залученням регіональних центрів кіберстійкості, посилення інституційних гарантій інформаційних прав людини та створення аналітико-прогностичної підсистеми для превентивного реагування на загрози; реалізація цих заходів підвищує її ефективність, стійкість і динамічність національної системи інформаційної безпеки та забезпечує її відповідність європейським стандартам демократичного публічного адміністрування.

Набуло подальшого розвитку:

- розуміння національної безпеки в публічно-інформаційній сфері, яке розглянуто як комплексний світоглядно-правовий феномен, що охоплює техніко-інфраструктурні, правові й ціннісно-гуманітарні компоненти та забезпечує формування стійкого, достовірного й захищеного інформаційного середовища держави;
- узагальнення зарубіжного досвіду забезпечення національної безпеки в публічно-інформаційній сфері, що дало змогу виокремити ключові складники ефективної системи інформаційної безпеки. Аналіз практик США, ЄС, Франції, Німеччини, Естонії, Польщі, Ізраїлю та Китаю продемонстрував, що провідні держави поєднують правові, інституційні, технологічні, освітні та міжнародно-координаційні механізми;
- формування інституційної структури управління інформаційною безпекою, у межах якої ключову роль відіграють національні агентства, урядові CERT-структури, координаційні ради, аналітичні центри та

центри передового досвіду, що забезпечують стратегічне планування, міжвідомчу координацію, реагування на кіберінциденти та міжнародне співробітництво.

Практичне значення отриманих результатів полягає в можливості використання матеріалів дисертації, її висновків, пропозицій і рекомендацій у низці сфер.

У *науково-дослідній діяльності* результати дисертації можуть стати підґрунтям для подальших теоретичних розвідок стосовно вдосконалення адміністративно-правових механізмів забезпечення інформаційної безпеки, розвитку системи реагування на інформаційні загрози, формуванню концепцій стійкості держави до гібридних впливів; матеріали можна використати в наукових проєктах, що стосуються модернізації державної політики в публічно-інформаційній сфері, цифрового врядування та захисту національних інтересів в умовах інформаційних війн (акт впровадження, довідка Науково-дослідного інституту публічного права).

В *освітньому процесі* висновки й рекомендації можна використати для розроблення навчальних дисциплін, спецкурсів, програм підвищення кваліфікації з адміністративного й інформаційного права, національної та інформаційної безпеки; для підготовки лекційних і семінарських занять у професійній підготовці юристів, державних службовців, фахівців з кібербезпеки, публічного управління й цифрової політики (довідка про впровадження Центральноукраїнського державного університету ім. Володимира Винниченка).

У *законотворчій діяльності* сформульовані в роботі ідеї, висновки та пропозиції можна враховувати під час розроблення проєктів законів і підзаконних актів, спрямованих на модернізацію державної інформаційної політики, зміцнення системи кіберзахисту, регламентацію діяльності органів публічної влади у сфері протидії інформаційним загрозам, у процесі гармонізації українського законодавства зі стандартами ЄС і НАТО.

У *правозастосовній діяльності* основні висновки та практичні рекомендації можуть слугувати інструментом для органів публічної влади, правоохоронних структур, СБУ, органів місцевого самоврядування та інших суб'єктів під час формування внутрішніх політик і процедур інформаційної безпеки, розроблення алгоритмів реагування на інформаційні інциденти, удосконалення систем моніторингу й нейтралізації деструктивного впливу, здійснення превентивних заходів, розгляду звернень громадян і ухвалення управлінських рішень у сфері захисту інформаційного простору держави.

Особистий внесок здобувача. Сформульовані в дисертації положення, узагальнення, висновки, пропозиції та рекомендації обґрунтовано на підставі особистих досліджень здобувача, здійснених у процесі самостійного опрацювання, аналізу й інтерпретації наукових, нормативних, статистичних та емпіричних джерел. Усі результати одержано автором особисто й вони не дублюють раніше опубліковані наукові розробки інших дослідників.

Апробація результатів дослідження. Основні результати проведеного дослідження, його концептуальні наукові положення та висновки оприлюднено на міжнародних і всеукраїнській науково-практичній конференції, зокрема: «Сектор безпеки України: актуальні питання науки та практики» (м. Харків, 27 березня 2025 р.), «Актуальні проблеми національного законодавства» (м. Кропивницький, 17 квітня 2025 р.), «Актуальні питання адміністративного права та адміністративного судочинства» (м. Харків, 15 травня 2025 р.), «Сталий розвиток економіки, права та державного управління в умовах глобальних викликів» (м. Анже, Франція, 28 травня 2025 р.).

Структура та обсяг дисертації. Робота складається з анотації, вступу, трьох розділів, які містять вісім підрозділів, висновків, списку використаних джерел (178 найменувань на 20 сторінках) і додатків (4 додатки). Загальний обсяг дисертації становить 230 сторінок.

РОЗДІЛ 1
ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ У ПУБЛІЧНО-ІНФОРМАЦІЙНІЙ СФЕРІ

1.1. Поняття та сутність національної безпеки у публічно-інформаційній сфері

Сучасний етап розвитку українського суспільства позначений масштабними трансформаціями у сфері державного управління, цифрових технологій і комунікацій. В умовах глобалізації, інтенсивного поширення цифрових медіа та зростання впливу інформації на прийняття політичних рішень питання національної безпеки виходить за межі традиційного воєнного виміру й охоплює комплекс політичних, соціальних, правових, комунікаційних та кібернетичних чинників. У такому контексті наукове осмислення сутності й особливостей забезпечення національної безпеки у публічно-інформаційній сфері набуває стратегічного значення для держави.

Проблематика національної безпеки у публічно-інформаційній сфері безпосередньо корелює з предметом дисертаційного дослідження, оскільки інформаційна політика та комунікаційна діяльність органів публічної влади становлять ключові елементи системи державного управління. Інформаційна безпека як складова національної безпеки визначає рівень стабільності демократичного ладу, ступінь довіри громадян до інституцій влади та ефективність реалізації конституційних прав людини на інформацію.

Дослідження зазначеної проблематики забезпечує інтеграцію теоретичних положень національної безпеки з практикою функціонування публічно-інформаційної сфери, що дозволяє простежити взаємозв’язок між станом інформаційної безпеки держави та якістю інформаційної взаємодії в суспільстві. Поєднання теорії й практики дозволяє формувати науково обґрунтовані рішення для вдосконалення державної політики у сфері інформаційної безпеки.

Інформація, яка є основою суспільного розвитку, водночас стає й засобом впливу. Її використання у публічному управлінні має амбівалентний характер: з одного боку – це інструмент відкритості, демократизації, прозорості державних процесів; з іншого – потенційний канал дестабілізації, маніпуляцій і загроз. Саме ця подвійність інформаційних процесів визначає актуальність міждисциплінарного підходу, який інтегрує знання з правознавства, соціології, політології, кібернетики й комунікативістики.

Становлення України як демократичної та правової держави значною мірою залежить від стабільності суспільних відносин, захищеності прав, свобод і законних інтересів людини та громадянина. У цьому контексті забезпечення національної безпеки виступає однією з ключових функцій держави, адже саме вона є гарантією збереження конституційного ладу, правопорядку та стабільного розвитку суспільства [1, с. 214].

Питання національної безпеки у публічно-інформаційному просторі України набуло особливого значення після 2014 року, коли розпочалася гібридна агресія проти нашої держави. Інформаційна війна, дезінформаційні кампанії, кібератаки, поширення фейкових наративів і психологічні операції стали невід'ємним елементом сучасних конфліктів. Після 24 лютого 2022 року масштаби цих загроз зросли у багато разів, що актуалізувало питання створення ефективної системи захисту інформаційного простору, стійкості національної свідомості та формування критичного мислення громадян.

Окрім воєнних аспектів, суттєвими викликами постають внутрішні ризики, пов'язані з функціонуванням публічно-інформаційного простору: недостатній рівень цифрової і медіаграмотності населення; низька культура інформаційної безпеки в органах публічної влади; витоки службової й персональної інформації; поширеність маніпулятивних технологій у політичних комунікаціях; циркуляція недостовірних даних у соціальних мережах, що створює підґрунтя для дестабілізації суспільних настроїв і підриву довіри до державних інституцій.

Актуальність дослідження підсилюється і потребою оновлення нормативно-правової бази, узгодження національної інформаційної політики з європейськими стандартами безпеки та прав людини, визначеними у документах ЄС і Ради Європи.

Проблема з'ясування сутності національної безпеки у публічно-інформаційній сфері є багатовимірною: вона охоплює філософське осмислення інформації як соціального феномена, правове регулювання процесів комунікації, технічні аспекти кіберзахисту та етичні стандарти публічної комунікації. Її наукове вирішення створює теоретичну основу для формування ефективної політики держави у сфері захисту інформаційного простору та консолідації українського суспільства.

Переходячи до розгляду теоретико-правових основ поняття національної безпеки, слід підкреслити, що саме ця категорія є концептуальним ядром державної політики в умовах глобальної взаємозалежності та цифрової взаємодії. Від її чіткого визначення залежать не лише юридичні межі повноважень державних інституцій, а й стратегічна логіка реагування на сучасні загрози – від збройних конфліктів до маніпуляцій у кіберпросторі. Таким чином, теоретико-правове осмислення безпеки створює базис для розроблення конкретних механізмів її забезпечення у публічно-інформаційній сфері.

Поняття «безпека» історично формувалося як універсальна суспільна цінність. Ще давньоримський державний діяч і філософ Цицерон наголошував, що природою «кожній живій істоті дано прагнення до самозахисту, збереження власного життя, уникнення всього шкідливого та здобуття всього необхідного для існування» [2; 3], тобто політичний діяч один з перших зауважував, що прагнення всього живого до безпеки є абсолютно природнім та піддається загальним суспільним законам. З урахуванням викладеного можемо дійти висновку, що генезис поняття «безпека» бере початок в античній філософській традиції. У період постійних війн, територіальних конфліктів та боротьби за

ресурси домінувала ідея про те, що фундаментальною метою будь-якої держави є збереження її цілісності, гарантування порядку та забезпечення захищеності громадян. За умов тогочасної реальності відсутність небезпеки фактично ототожнювалася з наявністю безпеки, а необхідною умовою її підтримання визнавалося об'єднання людей у політичні спільноти. Саме колективність забезпечувала відчуття захисту та знижувала ризики зовнішнього нападу, завоювань чи інших форм недоброзичливості, тоді як індивідуальне існування розглядалося як більш уразливе.

У трактаті «Держава» Платон визначає безпеку як стан захищеності поліса і спосіб «запобігання шкоди державі» [3; 4]. На його думку, відповідальність за гарантування безпеки покладена на охоронців (воїнів), які мають «охороняти державу від зовнішніх ворогів, а всередині – оберігати громадян, щоб … не було бажання та … сил творити зло» [3; 4]. Фактично Платон одним із перших запропонував концепцію соціально стійкої державної системи безпеки, яка функціонує в межах чітко встановлених законів і правил, а будь-яке їх порушення становить загрозу як для окремої особи, так і для держави загалом. У його позиції вбачаємо й ранні спроби окреслення безпекового середовища, адже філософ наголошує на єдності інтересів громадянина, спільноти та держави у процесі забезпечення умов безпечного існування [3].

У середньовічній інтелектуальній традиції (Т. Аквінський, Августин Блаженний) безпека осмислювалася як елемент морального та божественного порядку, а її гарантами виступали церковні та державні інституції. У добу Нового часу відбувається зміщення акцентів у бік природно-правової доктрини: Т. Гоббс у «Левіафані» розглядає державу як інструмент подолання «війни всіх проти всіх» і забезпечення безпеки громадян, тоді як Дж. Локк стверджує, що право на життя та безпеку належить до фундаментальних природних прав людини, які держава зобов'язана гарантувати [5].

У XIX–XX ст. категорія безпеки зазнає суттєвого змістового розширення, набуваючи соціально-політичного та інституційного виміру. В епоху двох світових воєн формується концепт «державної безпеки», орієнтований на захист суверенітету, територіальної цілісності та стабільності політичної системи. У цей період безпека починає трактуватися не лише як результат військової могутності, а як комплексна характеристика життєздатності держави та її здатності протистояти внутрішнім і зовнішнім ризикам.

У доктринальних підходах простежується спільна тенденція: державна безпека визначається як структурний компонент національної безпеки, що співвідноситься з нею у співвідношенні «частина — ціле». Зокрема, О. Вовк розглядає державну безпеку як складову національної безпеки, що відображає стан захищеності державної влади, суверенітету, територіальної цілісності та громадської злагоди, забезпечених діяльністю державних органів у нормативному та практичному вимірах [6, с. 47; 9]; В. Настюк визначає її як систему загальних і спеціальних заходів для гарантування стабільного існування держави як політичної організації суспільства, а також на її захист від реальних і потенційних загроз зовнішнього та внутрішнього походження, здатних порушити нормальне функціонування державних інститутів [7, с. 56; 9].

У працях А. Янчука подано розширене тлумачення, оскільки державна безпека функціонує як форма реалізації національної безпеки, забезпечувана державними інституціями шляхом застосування розвідувальних, контррозвідувальних та оперативно-розшукових заходів. Її метою є охорона суверенітету, незалежності, конституційного ладу, територіальної цілісності, економічного, науково-технічного та оборонного потенціалу, а також протидія загрозам з боку іноземних спецслужб, організованих злочинних груп і окремих осіб, включно з попередженням корупційних правопорушень, що становлять небезпеку для національної безпеки України [8, с. 351; 9].

Після 1945 р. у зв'язку зі створенням Організації Об'єднаних Націй, сформувався новий глобальний підхід до безпеки. Він базується на принципах міжнародного права, колективної відповідальності держав та необхідності підтримання міжнародної стабільності через багатосторонньої дипломатії й механізмів мирного врегулювання конфліктів. У цей період формується концепція безпеки як стану міжнародної рівноваги, у якому загрози одній державі розглядаються як загрози для всієї міжнародної спільноти.

Наприкінці XX – на початку XXI століття концепція безпеки зазнає суттєвої трансформації, переходячи від державоцентричної парадигми до комплексного, багатовимірного підходу. У цей період формується концепція «людської безпеки», закріплена у ключових документах ООН і Програми розвитку ООН (UNDP, 1994) [10]. Вона ґрунтується на ідеях «свободи від страху» (*freedom from fear*) та «свободи від нужди» (*freedom from want*), які утворюють дві провідні дослідницькі школи.

Перша школа інтерпретує людську безпеку як захищеність від насильства, спрямовуючи увагу на збройні конфлікти, миротворчі операції, механізми їх запобігання та врегулювання. Друга школа розширює спектр загроз, включаючи до них природні катастрофи, голод, епідемії, економічну нестабільність та інші чинники, що безпосередньо впливають на життя й добробут людини [11]. У підході підкреслено, що джерела небезпеки можуть бути не лише воєнними, а й соціально-економічними, екологічними, інформаційними та культурними.

Людина постає центральним суб'єктом безпеки, а її права, свободи та базові потреби – ключовим критерієм оцінки стану безпекового середовища. Відтак сучасне розуміння безпеки передбачає переорієнтацію з виключно оборонного виміру на гуманітарний, де пріоритетом стає забезпечення гідних, захищених і передбачуваних умов життя для кожного індивіда. Це зумовлює необхідність інтеграції гуманітарних, соціальних, інформаційних та правових механізмів у національні системи безпеки.

У науковій літературі безпека трактується як багатовимірна категорія, що охоплює природні, техногенні, соціально-політичні й комбіновані загрози. Як слушно зазначає І. Корж, усі небезпеки можна систематизувати за чотирма основними групами: природні (явища природи, стихійні лиха, інфекції), техногенні (аварії, вибухи, випромінювання), соціально-політичні (конфлікти, тероризм, злочинність) та комбіновані, які поєднують ознаки кількох типів загроз [16]. Такий підхід формує цілісне розуміння безпеки як взаємозалежної системи природних, технічних і соціальних чинників.

В українській науковій традиції питання безпеки набуло особливого розвитку після здобуття незалежності у 1991 році. У перші роки становлення державності поняття «національна безпека» ототожнювали переважно з воєнною чи оборонною сферою проте вже в 2000-х рр. завдяки працям В. Ліпкана, О. Бандурки, В. Антипова, В. Гребенюка, О. Власюка, О. Зелінського та інших учених сформовано системне бачення безпеки як міждисциплінарного феномена.

Термін «національний» походить від латинського *natio* – «народ». В українській науковій та правничій традиції слово «нація» нерідко використовується у значеннях, близьких до понять «країна» або «держава», що корелює з усталеним міжнародно-правовим дискурсом. Етимологічний аналіз засвідчує багатовимірність цього поняття: прикметник «національний» може характеризувати як суспільно-політичні процеси, що відбуваються в межах нації, так і сукупність її унікальних рис – культурних, історичних, ментальних чи організаційних. У такому контексті він часто набуває значення, тотожного або наближеного до поняття «державний».

Водночас наукова традиція демонструє тенденцію до переосмислення цієї категорії з огляду на сучасні соціально-економічні перетворення, насамперед зменшення монопольної ролі держави у регулюванні суспільних процесів. Це обумовлює підвищену актуальність ширшого застосування терміна «національна безпека». Як слушно зазначає професор О. Прохожев, концептуальний акцент

переноситься з держави як виняткового суб'єкта безпеки на особистість та суспільство, що підкреслює пріоритет гуманітарного виміру безпекової політики [19; 20; 178]. Така інтерпретація узгоджується з глобальними тенденціями розвитку людиноцентричної парадигми безпеки, що фіксують роль громадянина як центрального елемента сучасної безпекової архітектури.

Авторський колектив монографії «Національна безпека: світоглядні та теоретико-методологічні засади» під загальною редакцією професора О. Дзьобаня пропонує розглядати поняття «національна безпека» у кількох аспектах: як безпеку народу – громадянської спільноти, що може мати одноетнічну й мультикультурну структуру; як безпеку суспільства – історично сформованої соціальної спільноти зі спільними умовами життєдіяльності; як безпеку держави – політико-правової форми самоорганізації нації, що забезпечує виконання загальних функцій і здійснення управління [19; 20; 178].

Запропонована багаторівнева концептуалізація дає змогу інтегрувати гуманітарні, соціальні та інституційні виміри у цілісну модель національної безпеки. Вона відображає перехід від класичної державоцентричної моделі до комплексного бачення, у якому інтереси особи, суспільства та держави перебувають у взаємозалежності. Аналізована термінологія демонструє еволюцію поняття «національний» від етнокультурного до політико-правового й безпекового змісту та підкреслює необхідність сучасного системного підходу до формування політики національної безпеки.

У поглядах Х. Марковича поняття національної безпеки розкривається як стан захищеності держави від впливів внутрішнього та зовнішнього характеру, які потенційно можуть загрожувати її територіальній цілісності, суверенітету, політичній стабільності, економічному розвитку, рівню соціальної безпеки чи добробуту населення [1; 13, с. 12]. Ця позиція деталізує зміст безпеки через перелік ключових сфер, що піддаються ризикам, та підкреслює взаємозалежність між збереженням основ державності й умовами життя громадян.

Особливої уваги заслуговує концептуальний підхід А. Собакаря та М. Коваліва, які розуміють державну безпеку як захищеність державного суверенітету, конституційного ладу, економічного, науково-технічного й оборонного потенціалу, а також інформаційної сфери та державної таємниці від усіх форм внутрішніх і зовнішніх загроз з розвідувальною та терористичною діяльністю [1; 14, с. 158].

Науковці підкреслюють, що забезпечення такої безпеки вимагає застосування комплексної системи заходів політичного, правового, економічного, організаційного, військового та ідеологічного характеру, що мають відповідати рівню загроз і сприяти захисту національних інтересів України. Останні вони трактують як сукупність внутрішніх та зовнішніх потреб держави у забезпеченні сталого розвитку особистості, суспільства та держави.

Узагальнення наведених дослідницьких підходів дає підстави стверджувати, що сучасне розуміння національної та державної безпеки характеризується суттєвим розширенням змісту відповідних категорій. Якщо класичні концепції акцентували увагу переважно на захисті державності, то сучасні дослідження включають до структури безпеки широкий комплекс соціальних, економічних і гуманітарних чинників, інтегруючи до неї інтереси особистості й суспільства. Еволюція наукових уявлень рухається до комплексної, багатовимірної моделі, у межах якої стійкість держави розглядається у зв’язку зі станом соціальної стабільності, рівнем розвитку суспільства та реалізацією прав і свобод громадян. Це відповідає глобальним тенденціям формування людиноцентричної безпеки та створює методологічне підґрунтя для розбудови збалансованої національної безпекової системи України.

У межах зазначених підходів національна безпека визначається як стан захищеності життєво важливих інтересів особи, суспільства та держави від будь-яких загроз, який забезпечується діяльністю спеціально створених органів, нормативно-правовими інструментами, стратегічними документами та

механізмами управління ризиками. Українські дослідники підкреслюють інтегративну природу цього поняття: воно охоплює політичні, економічні, соціальні, екологічні, культурні та інформаційні компоненти, що функціонують як цілісна система.

Сучасна українська правова доктрина трактує безпеку не лише як результат (стан захищеності), але й як безперервний процес моніторингу, прогнозування, запобігання, реагування та відновлення. Це відображає перехід від реактивної до превентивної моделі забезпечення безпеки, яка узгоджується зі стандартами ЄС і НАТО та відповідає вимогам сучасного безпекового середовищ

У теорії державного управління та права виділяють кілька методологічних підходів до визначення сутності національної безпеки:

1. Системний підхід – розглядає безпеку як багаторівневу систему, у якій взаємодіють підсистеми: політична, воєнна, економічна, інформаційна, екологічна, соціальна тощо. Вона має свої інституційні елементи, функції, суб'єкти та механізми [17].

2. Функціональний підхід – тлумачить безпеку як діяльність держави й суспільства, спрямовану на захист національних інтересів. Згідно з ним, основною ознакою безпеки є наявність ефективної системи управління ризиками та кризами [18].

3. Ціннісно-гуманітарний підхід – акцентує увагу на людині як центральній фігурі системи безпеки. Безпека у цьому контексті трактується як гарантія реалізації прав і свобод громадян, соціальної стабільності та справедливості [19].

4. Правовий підхід – фокусує увагу на нормативному забезпеченні безпеки, правовому статусі суб'єктів та механізмах юридичної відповідальності за порушення її принципів [19].

Слід констатувати, що сучасне осмислення національної безпеки має ґрунтуватися на комплексному поєднанні системного, функціонального, ціннісно-гуманітарного та правового підходів, кожен із яких репрезентує

окремий вимір цього багаторівневого й поліструктурного феномена. Системний підхід дає змогу розглядати безпеку як інтегровану сукупність взаємопов'язаних підсистем, від узгодженості яких залежить стабільність функціонування держави. Функціональний підхід акцентує увагу на діяльнісній природі безпекової сфери, зосереджуючись на результативності механізмів прогнозування, попередження та нейтралізації загроз. Ціннісно-гуманітарний підхід орієнтує дослідження на людину як ключового суб'єкта та бенефіціара безпеки, підкреслюючи вагомість гуманітарних, морально-етичних і комунікативних чинників у забезпеченні стійкості суспільства. Правовий підхід, у свою чергу, забезпечує нормативну впорядкованість, правову визначеність та легітимність діяльності суб'єктів безпеки, гарантує реалізацію принципів верховенства права, прозорості й підзвітності.

Водночас сучасна безпекова парадигма, на нашу думку, потребує подальшого методологічного розширення шляхом упровадження інтегративно-інноваційного підходу, який об'єднує аналітичний потенціал державного управління, правознавства, соціології, психології та інформаційних технологій. Такий підхід створює підґрунтя для формування адаптивної, прогностично орієнтованої системи національної безпеки, спроможної адекватно реагувати на динаміку глобальних викликів і забезпечувати збалансований розвиток оборонного, соціального, економічного та гуманітарного складників.

На нашу думку, слід визначити доцільним:

- розробити науково обґрунтовану концепцію адаптивного управління національною безпекою, що ґрунтуватиметься на принципах прогнозування, ризик-менеджменту й аналітичного моделювання загроз;
- запровадити інституційний механізм інтеграції гуманітарної безпеки у державну політику, зокрема через освітні програми з формування культури безпеки, критичного мислення та медіаграмотності;

- удосконалити правові механізми забезпечення інформаційної та кібербезпеки, гармонізувавши їх із нормами європейського права та стандартами Ради Європи;
- створити міждисциплінарну систему моніторингу безпекового середовища, що використовуватиме інструменти штучного інтелекту та аналітичних платформ для прогнозування ризиків;
- посилити роль громадянського суспільства у формуванні політики безпеки, зокрема шляхом розбудови механізмів публічного контролю, соціальної відповідальності та взаємодії між державою й суспільством.

Уважаємо, що національна безпека має розглядатися не лише як стан захищеності держави, а як динамічна система взаємодії держави, суспільства та громадянина, заснована на принципах законності, людиноцентризму, міждисциплінарності та інноваційності. Такий підхід забезпечує перехід від традиційної оборонної моделі до сучасної концепції безпеки сталого розвитку, у центрі якої перебуває людина – її права, свободи й гідність як головна цінність державної політики України.

Підсумовуючи викладене, можна стверджувати, що поняття національної безпеки охоплює як стан захищеності, так і систему взаємопов’язаних заходів, спрямованих на його досягнення та підтримання. Це багатовимірна, інтегральна категорія, що поєднує ціннісні орієнтири, інституційні механізми, державну політику та правове регулювання.

У розширеному трактуванні національна безпека України визначається як інтегрований стан захищеності життєво важливих інтересів особи, суспільства та держави від зовнішніх і внутрішніх загроз. Досягнення цього стану забезпечується комплексом політичних, правових, економічних, інформаційних, соціокультурних та воєнних заходів, спрямованих на збереження державного суверенітету, демократичного ладу, територіальної цілісності та стійкого розвитку держави в умовах глобалізованого середовища.

Перейшовши від загальнотеоретичного аналізу категорії національної безпеки, доцільно конкретизувати її зміст у контексті публічно-інформаційної сфери, яка за сучасних умов набуває визначального значення для стійкості держави та суспільства. Саме в цьому сегменті формується інформаційна картина реальності, що впливає на рівень довіри громадян до влади, результативність державної політики та спроможність суспільства протидіяти маніпуляціям, дезінформації та іншим деструктивним впливам.

Окремо варто наголосити, що суспільні інформаційні відносини та інформаційні правовідносини у сфері публічної інформації мають аналогічну природу й закономірності функціонування, як і відносини в ширшій інформаційній сфері. Такий підхід дає підстави розглядати публічну інформацію як невід'ємний елемент інформаційної сфери держави, що підтверджується позиціями сучасних наукових досліджень [21].

Публічно-інформаційна сфера є структурним елементом системи публічного управління, адже забезпечує циркуляцію суспільно значущої інформації між органами влади та громадянами. Вона формує канали зворотного зв'язку між державою та суспільством, через які здійснюється комунікація, громадський контроль, участь громадян у прийнятті рішень. Водночас цей простір не обмежується лише діяльністю органів державної влади, оскільки охоплює також взаємодію засобів масової інформації, цифрових платформ, громадських організацій і соціальних мереж, що стають активними учасниками процесів формування громадської думки. У результаті інформаційний компонент набуває стратегічного значення, перетворюючись на ресурс державної потуги, чинник соціальної стабільності та об'єкт правового захисту.

Публічно-інформаційна сфера – це сукупність інформаційних потоків, інститутів і засобів комунікації, через які здійснюється інформування, взаємодія та вплив на суспільство. Вона включає як традиційні засоби масової інформації – телебачення, радіо, пресу, – так і цифрові канали: соціальні мережі, онлайн-медіа,

месенджери, форуми, відеоплатформи. Державна влада, громадянське суспільство, освітні й наукові інститути, приватні медіа – ці суб'єкти формують інформаційне середовище, в якому циркулюють ідеї, думки, факти, оцінки. Однією з головних особливостей сучасного етапу розвитку інформаційного простору є його відкритість, динамічність, технічна складність і високий рівень взаємопов'язаності між глобальним і національним контекстом [22].

Публічно-інформаційна сфера виконує низку функцій, які мають безпосередній вплив на стан національної безпеки. По-перше, вона забезпечує інформування населення про дії органів влади, події в країні та світі. По-друге, формує громадську думку, що прямо впливає на легітимність державної влади. По-третє, бере участь у мобілізації суспільства в умовах криз, надзвичайних ситуацій або воєнної агресії. По-четверте, виконує освітню функцію, формуючи критичне мислення, рівень медіаграмотності та інформаційну культуру громадян. Нарешті, вона слугує майданчиком для діалогу, конкуренції ідей та контролю за владою, що є необхідним елементом демократії [22].

У межах національної безпеки публічно-інформаційна сфера виконує подвійну роль. З одного боку, вона забезпечує відкритість, прозорість і підзвітність влади, що є необхідною умовою функціонування демократичної держави та запорукою реалізації права громадян на доступ до інформації. З іншого боку, саме ця відкритість створює потенційні ризики для державної стабільності у разі поширення деструктивних інформаційних впливів, пропаганди, маніпуляцій чи кібератак. Така амбівалентність обумовлює потребу в чітко визначеній державній політиці, що забезпечує баланс між свободою інформації та необхідністю її захисту.

Законодавче визначення національної безпеки, закріплене у Законі України «Про національну безпеку України» 2018 р., підкреслює, що вона охоплює захист державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших життєво важливих інтересів від реальних і

потенційних загроз [23]. Якщо ж розглядати це поняття у площині публічно-інформаційної сфери, воно набуває додаткового змістового наповнення. Тут йдеться не лише про оборону фізичних чи політичних інтересів держави, а й про захист інформаційного середовища, що забезпечує належне функціонування публічних інститутів, стабільність громадської свідомості та довіру до держави. Таким чином, національна безпека у публічно-інформаційній сфері постає як стан захищеності державних і суспільних інформаційних ресурсів, каналів комунікації, публічної інформації та інформаційної інфраструктури від будь-яких загроз, які можуть порушити їхню цілісність, достовірність або доступність.

Важливим складником поняття є усвідомлення того, що інформаційна безпека – це не лише технічна, а передусім соціально-комунікаційна категорія. Йдеться про забезпечення умов, за яких інформація виконує функцію розвитку, освіти, консолідації, а не інструменту дестабілізації.

У науковому виданні «Інформаційна та кібербезпека: концептуальні засади та практичні аспекти» вчений О. Горбенко під поняттям «інформаційна безпека» розуміє стан інформаційного середовища, за якого забезпечується стійкість до зовнішніх та внутрішніх загроз, гарантовано права та свободи громадян в інформаційній сфері, а також захищені національні інтереси держави [24; 25].

Цікавою є позиція вченого С. Морозова, викладена в монографії «Стратегії забезпечення інформаційної та кібербезпеки держави [6]», де під інформаційною безпекою вбачається певна система заходів та механізмів, спрямованих на захист інформаційних ресурсів та забезпечення інформаційної суверенності держави в умовах глобалізації та інформаційних вій [25; 26].

Дослідник І. Ткаченко пов’язав дефініцію «інформаційна безпека» з дотриманням правових норм і визначає її як стан захищеності інформаційних ресурсів, при якому забезпечується їх цілісність, конфіденційність та доступність, а також дотримання правових норм в інформацій-ній сфері [25; 27].

Загалом інформаційна сфера є простором реалізації національних цінностей, світоглядних орієнтирів, мовної ідентичності, а тому будь-які загрози, спрямовані на її руйнування, становлять безпосередню небезпеку для національного буття. У цьому контексті варто наголосити, що інформаційна безпека є не тільки предметом правового регулювання, а й сферою суспільної свідомості, де формуються норми поведінки, ціннісні орієнтири та моральна відповідальність за поширення інформації.

Особливого значення набуває розуміння, що забезпечення національної безпеки у публічно-інформаційній сфері передбачає не лише реактивні, а й превентивні дії. Ефективна політика має ґрунтуватися на принципах раннього виявлення загроз, моніторингу інформаційного простору, аналізу тенденцій та формуванні суспільної стійкості до маніпуляцій. Стійкість, у свою чергу, визначається рівнем довіри громадян до державних інституцій, розвитком критичного мислення, поширенням медіаграмотності та підвищенням культури інформаційного споживання. Виокремлені чинники формують «інформаційний імунітет» суспільства, який є не менш важливим за технічні засоби кіберзахисту.

Інформаційний імунітет – це здатність ідентифікувати маніпуляцію, фейк, оцінити рівень їх небезпеки і вміння їм запобігти. Виробити імунітет можна лише за допомогою підвищення медіаграмотності та дотримання правил інформаційної гігієни. Центр протидії дезінформації при РНБО України пояснює, як отримати інформаційний імунітет: отримувати інформацію лише з офіційних джерел; не варто реагувати на занадто емоційні повідомлення; не поширювати неперевірену інформацію [28; 30].

«Інформаційний вірус не береться з повітря, а лягає на живильне середовище, яке є в суспільстві: якщо була нагнана паніка в ЗМІ та додалося, що люди не довіряють владі, а лише собі, а також те, що люди бояться за свою безпосередню безпеку, – це зручний ґрунт для Росії зробити інформаційний вірус з розхитування ситуації…» [29; 30].

Національна безпека у публічно-інформаційній сфері реалізується через складну систему інституційних, правових, організаційних і комунікаційних механізмів. Держава виконує в цій системі координуючу функцію, визначаючи стратегії, пріоритети, стандарти і правила взаємодії. Проте ефективність забезпечення безпеки неможлива без участі громадянського суспільства, журналістської спільноти, наукових і освітніх закладів, які здійснюють інформаційно-просвітницьку діяльність, формують етичні норми комунікації та забезпечують контроль за дотриманням принципів відкритості й достовірності інформації. Взаємодія держави та суспільства в цій площині має ґрунтуватися на взаємній довірі та спільній відповідальності за інформаційне середовище.

Змістовне наповнення поняття національної безпеки у публічно-інформаційній сфері охоплює взаємодію інформаційних технологій, правових норм і соціальної поведінки. Воно включає захист інфраструктури й охорону нематеріальних складових: моральних, культурних і ментальних основ нації. Інформаційна безпека перебуває в тісному зв’язку з гуманітарною та духовною безпекою, оскільки деструктивний вплив на мову, історичну пам’ять чи систему цінностей може послабити державу не менше, ніж пряма збройна агресія.

Отже, сутність національної безпеки у публічно-інформаційній сфері полягає у створенні гармонійного та стійкого інформаційного середовища, яке забезпечує стабільність функціонування держави, формує суспільну довіру, підтримує конституційні принципи демократії та права людини. Її головна мета – гарантувати захищеність публічної комунікації, зберегти достовірність і правдивість інформації, запобігти інформаційним маніпуляціям та забезпечити розвиток громадянського суспільства в умовах свободи слова. У цьому сенсі національна безпека у публічно-інформаційній сфері є не стільки технічним або адміністративним механізмом, скільки світоглядним і правовим феноменом, що визначає ціннісні орієнтири держави й суспільства у цифрову епоху.

1.2. Система та принципи адміністративно-правового регулювання інформаційної безпеки

Забезпечення належного рівня інформаційної безпеки є одним із ключових завдань сучасної держави, оскільки воно визначає стабільність функціонування публічної влади, рівень довіри громадян та стійкість конституційного ладу. У структурі національної безпеки ця сфера займає особливе місце, адже саме через ефективні механізми адміністративно-правового регулювання забезпечується реалізація державної політики щодо захисту інформаційного простору, нейтралізації деструктивних інформаційних впливів і протидії кіберзагрозам.

Дослідження адміністративно-правових засад забезпечення інформаційної безпеки передбачає з'ясування її змісту, структурних компонентів та принципів функціонування, визначення інституційних елементів системи, а також аналіз правових механізмів взаємодії суб'єктів публічної адміністрації. Особливого значення набуває вивчення нормативно-правових основ діяльності органів влади, процедурного інструментарію їхнього управлінського впливу та методологічних засад, що визначають спрямованість державної політики у сфері інформаційної безпеки й забезпечують її узгодженість із загальнонаціональними безпековими пріоритетами.

Актуальність цієї проблематики зумовлена низкою об'єктивних чинників зовнішнього та внутрішнього характеру. На зовнішньому рівні вона пов'язана з глобалізацією інформаційних комунікацій, інтенсивним розвитком цифрових технологій, транснаціональним характером кіберзагроз, а також необхідністю гармонізації українського законодавства зі стандартами Європейського Союзу, НАТО та провідних міжнародних безпекових інституцій. На внутрішньому рівні актуальність визначається потребою підвищення ефективності системи публічного управління, зміцнення кіберстійкості критичної інформаційної інфраструктури, удосконалення міжвідомчої координації, оптимізації процедур

адміністративного реагування на інформаційні інциденти та підвищення рівня інформаційної культури й медіаграмотності громадян.

В умовах трансформації публічного управління та цифровізації суспільних відносин особливої ваги набуває оновлення правового регулювання на засадах демократичного врядування, верховенства права, пропорційності, публічності й відкритості, що забезпечують оптимальне співвідношення між свободою вираження поглядів і гарантіями безпеки держави. Сучасна модель інформаційної безпеки має спиратися на принцип партнерства між державою, бізнесом і громадянським суспільством для спільного формування стійкого, збалансованого й безпечного інформаційного середовища. Окреслення змісту, системних характеристик і принципів такої моделі становить основний науковий фокус дослідження адміністративно-правового регулювання інформаційної безпеки як ключового елемента національної безпекової політики України.

Розвиток правового регулювання у сфері інформаційної безпеки вимагає звернення до фундаментального поняття адміністративно-правового регулювання, що становить один із ключових інструментів реалізації публічної влади у демократичній правовій державі.

Адміністративно-правове регулювання у сучасній науковій традиції визначається як один із різновидів правового регулювання, що має власний механізм, структуру та функціональне навантаження [31, с. 153; 35]. Уже це базове положення демонструє прагнення відмежувати адміністративно-правовий вплив від інших галузей права, підкресливши його специфічну спрямованість на сферу публічного управління.

У наукових розвідках О. Надьон справедливо зауважує, що своєрідність адміністративно-правового регулювання виявляється не тільки у специфічних адміністративних нормах, а й у тому, що саме через адміністративне право можна простежити форми та методи діяльності органів державної влади [32, с. 18–19; 35]. Ця думка є суттєвою, оскільки зміщує фокус із «нормативної оболонки» на

практичний вимір: адміністративне право не лише закріплює правила, а й дозволяє зрозуміти архітектоніку управлінських процесів – від організаційних процедур до примусових механізмів забезпечення виконання владних рішень.

Водночас О. Матвійчук звертає увагу на проблему відсутності єdinого методологічного підходу до визначення цього поняття, що зумовлює численність дефініцій і розмитість ознак, які пропонуються на означення категорії адміністративно-правового регулювання [33, с. 110; 35]. Наявність такої проблеми є закономірною для галузі, де регулятивний вплив поширюється на надзвичайно різнорідні суспільні відносини – від публічних послуг до безпеки, від кадрової політики до інформаційної діяльності. Саме тому питання методологічної уніфікації тут принципове: без нього неможливо створити узгоджену систему адміністративно-правових понять.

У цьому контексті цінним є підхід О. Гуміна та Є. Пряхіна, які пропонують двовимірне трактування адміністративно-правового регулювання – у широкому та вузькому сенсах [34, с. 46; 35]. У широкому розумінні адміністративно-правове регулювання передбачає впорядкування суспільних відносин державними органами, їх юридичне закріплення, охорону, практичну реалізацію та розвиток. Це визначення охоплює усю сферу взаємодії держави з громадянами та організаціями, підкреслюючи системний і процесуальний характер регулятивної діяльності.

У вузькому ж значенні зміст категорії змінюється залежно від того, які саме суспільні відносини розглядаються. Така диференціація є методологічно виправданою, оскільки адміністративно-правовий вплив у сфері інформаційної політики, наприклад, має зовсім інші завдання та інструменти, ніж у митній, земельній чи безпековій сферах. Отже, у вузькому сенсі дефініція конкретизується через специфіку регульованих відносин, структуру суб’єктів та особливості юридичних процедур.

На думку В. Теремецького, адміністративно-правове регулювання – це «цілеспрямований вплив правових норм, прийнятих державою, який забезпечується відповідними адміністративно-правовими засобами, за допомогою якого врегульовуються суспільні відносини» [36, с. 51; 39].

Аналогічної позиції дотримується також П. Литовченко, який визначає адміністративно-правове регулювання, як планомірний вплив адміністративно-правових норм на визначені суспільні відносини, що здійснюється за допомогою адміністративно-правових засобів, із ціллю забезпечення прав, свобод і інтересів фізичних чи юридичних осіб, зокрема, у публічно-правовій сфері для звичного функціонування суспільства та держави [37, с. 130; 39]; С. Стеценко вважає, що адміністративно–правове регулювання – це сукупність правових засобів, за допомогою яких здійснюється правове регулювання суспільних відносин у сфері адміністративного права [38, с. 63; 39].

Як бачимо, у загальнотеоретичному розумінні під адміністративно-правовим регулюванням розуміють діяльність уповноважених суб'єктів публічної адміністрації, спрямовану на встановлення, конкретизацію та реалізацію правових норм, процедур і засобів управлінського впливу в окремих сферах суспільного життя. Його сутність полягає у забезпеченні належного порядку публічного управління, упровадженні законодавчих приписів у практику діяльності органів виконавчої влади та забезпеченні прав і свобод громадян через адміністративні засоби.

У структурі правової системи України адміністративно-правове регулювання відіграє системоутворювальну роль, оскільки саме через нього реалізується принцип верховенства права у сфері публічних відносин. Воно поєднує в собі дві взаємопов'язані сторони – нормотворчу, що встановлює правила поведінки, і правозастосовну, спрямовану на їх практичне втілення. Ця діяльність охоплює як упорядкування внутрішньої організації публічної адміністрації, так і встановлення зовнішніх меж взаємодії між органами влади,

юридичними особами та громадянами. Адміністративно-правове регулювання є правовим механізмом управління і гарантією реалізації конституційного принципу підзвітності й прозорості держави перед суспільством.

У сфері інформаційної безпеки адміністративно-правове регулювання набуває специфічних ознак, зумовлених особливостями самого предмета впливу. Йдеться про відносини, що виникають у процесі створення, оброблення, зберігання, поширення та захисту інформації, а також забезпечення стабільності функціонування інформаційних систем і мереж. На відміну від багатьох інших сфер публічного адміністрування, інформаційна безпека має динамічний, технологічно мінливий характер, що потребує оперативного реагування державних органів і високого рівня адаптивності правових норм. Тому адміністративно-правове регулювання тут характеризується превентивною спрямованістю, оскільки головна його мета полягає не лише у подоланні наслідків інформаційних інцидентів, а насамперед у створенні умов, які унеможливлюють їх виникнення.

Предметній сфері адміністративно-правового регулювання інформаційної безпеки характерні такі ознаки: невід’ємність інформаційних відносин або обумовленість ними; взаємопов’язаність і взаємозалежність інформаційних відносин з об’єктами національних інтересів в інформаційній сфері; взаємозв’язок адміністративно-правового регулювання інформаційної безпеки з урахуванням виникнення, виявлення та запобігання загрозам національним інтересам в інформаційній сфері з метою розроблення та застосування механізмів ефективної протидії загрозам [40].

Діяльність із забезпечення інформаційної безпеки виражається в адміністративно-правовому регулюванні, предметна спрямованість якого визначається сукупністю суспільних відносин в інформаційній сфері, спрямованої на зміцнення рівноправного стратегічного партнерства у галузі інформаційної безпеки з Організацією північноатлантичного договору (НАТО) і

Європейським Союзом, захисті суверенітету України в інформаційному просторі, протидії застосуванню інформаційних технологій для порушення стабільності економічного розвитку й зміни стратегічного курсу європейської інтеграції, забезпеченні територіальної цілісності й суверенітету України [40].

Водночас важливою особливістю цього регулювання є підпорядкованість публічним інтересам, що випливає з конституційного принципу служіння держави людині. Інформаційна безпека не може тлумачитися як самодостатня технічна або військова категорія – вона є складником гарантії прав і свобод особи, зокрема права на інформацію, на приватність, на захист персональних даних. Адміністративно-правовий вплив має поєднувати державні пріоритети із суспільними цінностями, забезпечуючи баланс між захистом національних інтересів і дотриманням демократичних стандартів інформаційної відкритості.

Характерною рисою адміністративно-правового регулювання інформаційної безпеки є також поєднання норм матеріального і процесуального права. Матеріальні норми визначають права, обов'язки та відповідальність суб'єктів інформаційної діяльності, тоді як процесуальні норми регламентують порядок реалізації цих приписів – процедури контролю, моніторингу, реагування на порушення, застосування санкцій тощо. Таке поєднання забезпечує цілісність регулятивного впливу, узгодженість між принципами законності, ефективності й оперативності управлінських рішень.

Адміністративно-правовий механізм виступає ключовим інструментом реалізації державної інформаційної політики, оскільки саме через нього забезпечується практична координація діяльності суб'єктів публічної адміністрації, встановлюються стандарти інформаційної безпеки, а також здійснюється контроль і нагляд за дотриманням вимог законодавства у цій сфері.

Зміст адміністративно-правового механізму охоплює як нормотворчу діяльність – розроблення та прийняття нормативно-правових актів і управлінських рішень, – так і впровадження адміністративних процедур у сфері

ліцензування, аудиту, сертифікації, моніторингу та реагування на інформаційні інциденти. Важливим його елементом є також реалізація механізмів юридичної відповідальності за порушення вимог інформаційної безпеки, що виконує превентивну, охоронну та дисциплінуючу функції адміністративного права.

Слушною є позиція Б. Мельник, який також акцентує увагу, що адміністративно-правовий механізм забезпечення інформаційної безпеки держави є невід'ємним складником системи національної безпеки. Він включає сукупність правових норм, інституційних структур і організаційно-управлінських заходів, спрямованих на захист держави, суспільства й громадян від загроз в інформаційному просторі. У сучасних умовах цей механізм набуває особливої актуальності, адже інформаційна безпека стає системоутворювальним елементом державного управління, особливо в умовах військової агресії та гібридних загроз, що поєднують традиційні військові дії з інформаційно-психологічним впливом [41, с. 11].

Адміністративно-правове регулювання інформаційної безпеки слід розглядати як багаторівневу систему управлінських і правових впливів, спрямовану на формування безпечного інформаційного середовища, у межах якого реалізується державна політика у сфері національної безпеки. Його теоретико-правова основа поєднує нормативну визначеність, процедурну чіткість і соціально-ціннісний зміст, що забезпечує відповідність сучасним принципам публічного управління та демократичного врядування. Саме через цей механізм держава не лише встановлює правові рамки інформаційної діяльності, а й гарантує реальний захист інформаційного суверенітету, прав громадян і стабільність національного простору.

Система адміністративно-правового регулювання інформаційної безпеки України є складним, багатоелементним утворенням, у якому поєднано правові норми, інституційні механізми, організаційні процедури та засоби публічного управління, спрямовані на забезпечення захисту національного інформаційного

простору. Її структура визначається функціональним призначенням адміністративного права – забезпеченням ефективної реалізації державної політики, координації діяльності органів виконавчої влади, підтриманням рівня публічної безпеки та законності у сфері інформаційних відносин.

Структура кожної системи передусім залежить від її складових елементів. У свою чергу, і властивості елементів значною мірою обумовлюються структурою системи, яку вони утворюють. Структура (лат. structura – будова, розміщення, порядок) розглядається як спосіб закономірного зв'язку між складовими частинами предметів і явищ [42, с. 127; 45].

Кожна система характеризується певною структурою, остання є її обов'язковим атрибутом, властивістю. Тому структура не може існувати поза системою, адже вона є її характерною ознакою. З іншого боку, з огляду на загальнофілософське розуміння структури, вона не збігається з елементами системи, а відображає зв'язки між ними (елементами). На думку В. Тарасенко, структура ж відображає зв'язки (вертикальні, горизонтальні тощо) між цими й іншими елементами: джерелами, принципами, адміністративно-правовими відносинами, статусом суб'єктів адміністративного права тощо.

Загалом застосування системно-структурного підходу має низку переваг. У загальнонауковому розумінні системно-структурний підхід визначається як «напрям методології наукового пізнання й соціальної практики, у підґрунті якого лежить розгляд об'єктів як систем: він орієнтує дослідження на розкриття цілісності об'єкта, на виявлення багатоманітних типів зв'язків у ньому і зведення їх у єдину теоретичну картину» [43, с. 276; 45]. З огляду на це І. Прангішвілі правильно зауважує, що системно-структурний підхід являє собою сукупність методів і засобів, що надають можливість досліджувати властивості, структуру й функції об'єктів, явищ або процесів, якщо уявити їх як системи з усіма складними взаємозв'язками, впливом складників на систему й на навколишнє середовище, а також впливом самої системи на її структурні компоненти [44, с. 16; 45].

На доктринальному рівні систему адміністративно-правового регулювання у сфері інформаційної безпеки можна схарактеризувати як сукупність взаємопов'язаних елементів: нормативно-правового, інституційного й організаційно-функціонального. Кожен виконує специфічну роль, але лише у взаємодії забезпечує цілісність і результативність функціонування системи.

Нормативно-правовий елемент охоплює сукупність актів різної юридичної сили, що визначають зміст державної інформаційної політики, правовий статус суб'єктів, порядок їх діяльності, компетенцію, відповідальність та способи правового реагування на порушення у сфері інформаційної безпеки. Його ядром є Конституція України [46], яка у ст. 17 та 34 закріплює взаємозалежність між інформаційною свободою та обов'язком держави забезпечувати захист суверенітету, територіальної цілісності й інформаційної безпеки.

На розвиток конституційних положень спрямовано Закон України «Про національну безпеку України» [23], який визначає інформаційну безпеку одним із ключових напрямів державної політики. Важливе значення має також Закон України «Про основні засади забезпечення кібербезпеки України» [47], що визначає правові та організаційні основи захисту кіберпростору.

Сукупність наведених нормативно-правових актів не є вичерпним, проте саме вони формують базове інституційно-правове підґрунтя, у межах якого відбувається становлення та розвиток адміністративно-правових інститутів, процедур і управлінських практик у сфері забезпечення інформаційної безпеки держави. Зміст, структура та функціональні особливості цього правового комплексу будуть докладніше розкриті у наступному підрозділі дослідження.

Наступним є інституційний елемент системи який відображає сукупність суб'єктів, уповноважених здійснювати публічне управління у сфері інформаційної безпеки. Центральне місце у ній посідає Рада національної безпеки і оборони України, координує і контролює діяльність органів виконавчої влади у сфері національної безпеки і оборони [48], а також у сфері захисту

інформаційного простору та забезпечення кіберстійкості. Важливими виконавчими ланками є Служба безпеки України (через підрозділи з контррозвідувального захисту інтересів держави у сфері інформаційної безпеки), Державна служба спеціального зв'язку та захисту інформації України, Міністерство цифрової трансформації, Міністерство культури та інформаційної політики, Національна рада з питань телебачення і радіомовлення, а також структурні підрозділи органів місцевого самоврядування, що відповідають за реалізацію державної інформаційної політики на регіональному рівні.

Значну роль у системі відіграють і інституції громадянського суспільства – професійні медіаоб'єднання, освітні установи, експертні ради, які здійснюють громадський контроль, аналітичну підтримку та просвітницьку діяльність у сфері інформаційної безпеки. Таким чином, сучасна модель управління базується на принципі поліцентризму. Принцип поліцентризму, на якому базується сучасна модель управління, передбачає поєднання та взаємодію державних і громадських суб'єктів у сфері інформаційної безпеки. Його реалізація сприяє підвищенню адаптивності системи до нових викликів, гібридних загроз і технологічних трансформацій. У цьому сенсі поліцентризм виступає проявом еволюції публічного управління – від монополії держави на інформаційний контроль до інтеграційної моделі, у якій кожен з учасників інформаційного простору виконує специфічну, але взаємопов'язану функцію.

Водночас поліцентризм не позбавлений ризиків: розширення спектра суб'єктів впливу на інформаційний простір створює передумови для появи «інформаційних вірусів», маніпуляцій громадською думкою, дифузії ціннісних орієнтацій. Тому завдання держави полягає не у централізації, а у встановленні ефективних адміністративно-правових механізмів координації, контролю та відповідальності, які забезпечать гармонійний баланс між свободою інформації та безпекою суспільства [49].

Організаційно-функціональний елемент системи охоплює управлінські процедури, форми й методи адміністративного впливу, за допомогою яких реалізуються норми права. Серед них – моніторинг інформаційного простору, здійснення кіберзахисту, реагування на інциденти, контроль за дотриманням законодавства у сфері інформації, ліцензування діяльності операторів телекомунікацій і провайдерів, проведення експертиз інформаційних ресурсів, інформаційно-аналітична діяльність та формування державних стандартів безпеки. Ці функції мають переважно превентивний характер і спрямовані на своєчасне виявлення, локалізацію та нейтралізацію потенційних загроз.

У межах системи адміністративно-правового регулювання важливе місце посідає координаційна взаємодія між органами публічної влади, оскільки вона забезпечує узгодженість управлінських рішень, послідовність дій та раціональне використання ресурсів у сфері забезпечення інформаційної безпеки держави.

Координація посідає одне з ключових місць серед управлінських функцій, оскільки її сутність полягає в упорядкуванні взаємозв'язків між суб'єктами управління з метою досягнення узгодженості дій та консолідації зусиль для реалізації спільних завдань. У науковій літературі поняття координація (від лат. coordinatio – упорядкування, узгодження) трактується як невід'ємний елемент управлінського процесу, що забезпечує узгодженість і системність діяльності різних компонентів керованої структури. У словникових джерелах координація визначається як управлінська функція, спрямована на встановлення впорядкованих зв'язків і ефективної взаємодії між організаціями, підрозділами та учасниками управлінського процесу з метою гармонізації їхніх дій і досягнення спільних результатів [50].

З позицій управлінської діяльності, координація може бути розглянута як заснований на законі управлінський вплив суб'єктів вищого рівня на нижчі рівні системи, спрямований на узгодження діяльності взаємодіючих підсистем при збереженні їх автономності [50; 51]. В. Т. Білоус, зокрема, вважає координацію

самостійним засобом організації управління, який забезпечує узгоджене функціонування автономних цілеспрямованих систем [50; 52, с. 65].

З огляду на те, що інформаційна безпека є міжвідомчою, ефективність адміністративно-правового регулювання у цій сфері значною мірою залежить від рівня координації дій суб'єктів, належного обміну інформацією, узгодженого планування та чіткого розмежування компетенцій. Координаційна взаємодія реалізується через урядові дорадчо-консультативні органи, спеціалізовані міжвідомчі комісії, оперативно-аналітичні центри реагування (зокрема, Національний координаційний центр кібербезпеки при РНБО України), а також через форми публічно-приватного партнерства. Останні забезпечують залучення технологічного потенціалу приватного сектору, експертної спільноти та громадських організацій, що дозволяє сформувати багаторівневу й адаптивну систему підтримання інформаційної стійкості держави.

Характеризуючи систему адміністративно-правового регулювання, слід наголосити, що її результативність визначається не лише наявністю комплексної нормативної бази, а й інституційною спроможністю публічної адміністрації забезпечити практичне виконання правових приписів. На цьому рівні формується ефективність правозастосування: здатність адміністративних процедур відповідати темпам розвитку інформаційно-комунікаційних технологій, оперативно реагувати на нові типи загроз, забезпечувати належний рівень прозорості, відповідальності й підзвітності органів влади, тому система адміністративно-правового регулювання має бути відкритою до постійного оновлення, технологічної модернізації та концептуального перегляду, що є передумовою її життєздатності у швидкозмінному цифровому середовищі.

Адміністративно-правове регулювання інформаційної безпеки постає як структуровано організований комплекс нормативних, інституційних і процедурних компонентів, об'єднаних спільною метою – забезпеченням захищеності інформаційного простору України, реалізації державної політики у

сфері національної безпеки та утвердження принципів правової держави в умовах цифрової трансформації. Його концептуальна сутність полягає в інтеграції правових норм і управлінських рішень у цілісну систему правового впливу, що ґрунтується на засадах законності, публічності, пропорційності, ефективності та технологічної адаптивності.

Ефективність будь-якої системи правового регулювання визначається не лише її нормативною насиченістю, а передусім тими принципами, на яких вона ґрунтується. Сам термін *principium* (лат. — «початок», «основа») відображає вихідний характер фундаментальних положень, що визначають спрямованість і логіку правового впливу. У сучасній юридичній науці принципи права розглядаються широко й варіативно, однак домінує підхід, згідно з яким вони становлять основні, узагальнені ідеї та засадничі положення, що виражають сутність права через категорії свободи, справедливості та гуманістичних цінностей. Саме принципи фіксують у праві об'єктивні закономірності суспільних відносин, відображають базові цінності, правові традиції та соціально-культурні орієнтири розвитку суспільства.

Принципи публічного управління у цьому контексті розглядаються як вихідні управлінські положення, що визначають природу, спрямованість і зміст діяльності публічної адміністрації та можуть бути формалізовані у вигляді правових норм і правил [53, с. 21; 54]. У науковій літературі наголошується, що принципи – це сукупність універсальних ідей, які визначають сутність відповідного явища, його функції та соціальне призначення. Вони виступають найбільш загальними нормами, що поширюються на всіх суб'єктів правовідносин, забезпечуючи єдність правового регулювання та внутрішню узгодженість правової системи [55, с. 122; 57].

Окремі автори визначають принципи права як особливий різновид правових норм (норми-принципи), як керівні ідеї, що задають загальну спрямованість і зміст правового регулювання, або як інформаційне відображення

в праві ключових зв’язків, що реально існують у правовій системі [56, с. 128; 57]. Принципи становлять внутрішній концептуальний стрижень правового механізму, забезпечуючи його цілісність, стабільність та передбачуваність.

У сфері інформаційної безпеки значення принципів набуває особливої ваги. Вони виконують роль регулятивних орієнтирів, що визначають оптимальне співвідношення між двома базовими цінностями демократичного суспільства – свободою інформації та необхідністю захисту державних, суспільних і приватних інтересів. Саме принципи забезпечують збалансованість управлінських рішень, легітимність втручання у публічно-інформаційну сферу та відповідність діяльності органів публічної влади стандартам верховенства права.

Адміністративно-правове регулювання інформаційної безпеки, як складна система управлінських і правових відносин, спирається на комплекс принципів, що відображають загальноправові засади, адміністративно-правові закономірності та специфічні вимоги інформаційно-безпекової сфери. Вони виступають методологічним підґрунтям діяльності органів публічної адміністрації, визначають межі допустимого втручання у сферу комунікацій, формують стандарти поведінки суб’єктів владних повноважень і забезпечують прозорість реалізації державної політики.

У широкому розумінні принципи адміністративно-правового регулювання інформаційної безпеки – це закріплені в нормах права або виведені з його змісту базові засади, які відображають сутність, зміст і спрямованість діяльності публічної адміністрації у сфері захисту інформаційного простору, визначають взаємозв’язок між правовими нормами, процедурними механізмами та суспільними потребами. Їх природа є дуальною: вони мають нормативно-доктринальний характер, тобто одночасно виражають як законодавчу волю держави, так і науково-теоретичне осмислення сутності публічного управління.

До правових принципів забезпечення інформаційної безпеки, за тлумаченням О. Олійника, належать такі основоположні положення:

– принцип законності − полягає у застосуванні механізмів забезпечення інформаційної безпеки та механізмів і технологій управління системою забезпечення інформаційної безпеки тільки на основі чинного законодавства та нормативно-правової бази регулювання як суспільних інформаційних відносин, так і міжнародного інформаційного співробітництва;
– принцип пріоритету норм міжнародного права над національним законодавством, за винятком Конституції України, в системі забезпечення інформаційної безпеки полягає в прямій дії норм та принципів міжнародного права на всій території країни на рівні Конституції України;
– принцип права власності в процесі забезпечення інформаційної безпеки передбачає гарантування прав суб'єктів України на інформацію за винятком обмежень, встановлених чинним законодавством;
– принцип економічної доцільності системи забезпечення інформаційної безпеки полягає в оцінюванні секретності й конфіденційності як споживацьких властивостей і включення їх вартості до загальної ціни виробленої продукції [58, с. 170−171; 59].

Організаційними принципами забезпечення інформаційної безпеки, на думку вченого, є такі:

– принцип об'єктивності, тобто об'єктивної оцінки реальних і потенційних загроз інформації і сфері її обігу, стану правового й організаційного забезпечення, а також реальних можливостей застосування матеріально-технічних, кадрових і фінансових ресурсів;
– принцип наукового підходу до організації забезпечення інформаційної безпеки передбачає передусім всебічне пізнання об'єктивних законів і закономірностей розвитку інформаційної сфери та механізмів їх

практичної реалізації; а також наукове осмислення і юридичне закріплення на рівні законодавчих, нормативно-правових актів та інших державних рішень усього комплексу проблем, пов'язаних із формуванням, удосконаленням системи забезпечення інформаційної безпеки та управління цією системою;

– принцип комплексного підходу до організації забезпечення інформаційної безпеки – створення взаємопов'яханих зв'язків, відповідних засобів і методів, що спрямовані на забезпечення безпеки інформації, що підлягає захисту; принцип безперервності забезпечення інформаційної безпеки − повсякденне (безперервне) застосування як загальних, так і спеціальних засобів і методів забезпечення інформаційної безпеки на всіх її етапах [58, с. 170−171; 59].

За нашим переконанням, принципи верховенства права, законності, справедливості, гуманізму, правової визначеності та пропорційності становлять загальноправові засади адміністративно-правового регулювання інформаційної безпеки, формуючи ієрархію правових цінностей у відносинах держави й особи.

Принцип верховенства права, закріплений у статті 8 Конституції України [46], визначає, що будь-яке адміністративне рішення має відповідати не лише букві, а й духові закону, узгоджуючись із загальними засадами справедливості, розумності та добросовісності. У сфері інформаційної безпеки цей принцип виконує функцію противаги надмірній бюрократизації та дозволяє уникати свавільних рішень під виглядом захисту національних інтересів.

Принцип верховенства права є ключовою конституційною засадою, яка визначає всі аспекти функціонування держави, включно із сферою інформаційної безпеки. Цей принцип передбачає, що всі суб'єкти правовідносин – і держава, і громадяни – діють у межах закону. У сфері інформаційної безпеки це означає, що заходи, спрямовані на протидію загрозам, мають ґрунтуватися на правових нормах, бути обґрунтованими та пропорційними [60; 63].

Згідно із цим принципом, держава зобов'язана забезпечувати прозорі правові механізми для захисту інформаційного простору. Це включає як розробку законів, що регулюють діяльність в інформаційній сфері, так і забезпечення їх ефективного виконання. Принцип верховенства права також вимагає, щоб будь-які обмеження прав і свобод громадян в інформаційній сфері мали законодавче підґрунтя та не порушували основоположних прав людини [61; 63].

Застосування принципу верховенства права у сфері інформаційної безпеки також передбачає наявність ефективних механізмів судового контролю за діяльністю органів, що забезпечують інформаційну безпеку. Громадяни повинні мати можливість оскаржувати рішення та дії державних органів у випадку, якщо вони вважають, що їхні права було порушено внаслідок заходів, спрямованих на забезпечення інформаційної безпеки [62; 63].

Принцип верховенства права передбачає, що всі суб'єкти правовідносин, включаючи органи державної влади, повинні діяти в межах закону. У сфері інформаційної безпеки це означає, що держава повинна здійснювати свою діяльність на основі правових норм, забезпечуючи прозорість і підзвітність своїх дій. У сфері інформаційної безпеки принцип верховенства права означає, що держава повинна здійснювати свою діяльність в інформаційній сфері виключно на законних підставах, дотримуючись прав і свобод громадян та забезпечуючи прозорість і підзвітність своїх дій. Це включає в себе створення чіткої правової бази для регулювання інформаційної безпеки, яка повинна відповідати як міжнародним стандартам, так і національним інтересам [63].

Дійсно, в контексті інформаційної безпеки цей принцип виконує роль запобіжника проти свавільних або непропорційних рішень, що можуть прийматися під приводом захисту національних інтересів.

Верховенство права у сфері інформаційної безпеки доцільно розглядати як філософсько-правову категорію, що поєднує юридичний та етичний виміри

державного управління, спрямовані на досягнення балансу між інтересами безпеки держави та гарантіями прав людини в інформаційному суспільстві.

Принцип законності у сфері інформаційної безпеки є базовою правовою категорією, що визначає межі, порядок і зміст діяльності держави та інших суб'єктів у цій сфері. Він забезпечує правову передбачуваність, стабільність і послідовність функціонування системи інформаційної безпеки, виступаючи гарантією дотримання прав людини та недопущення свавілля при реалізації владних повноважень.

Він полягає у застосуванні механізмів забезпечення інформаційної безпеки та механізмів і технологій управління системою забезпечення інформаційної безпеки тільки на основі чинного законодавства та нормативно-правової бази регулювання як суспільних інформаційних відносин, так і міжнародного інформаційного співробітництва [58].

У цьому контексті принцип законності передбачає, що будь-яке втручання державних органів в інформаційну сферу можливе лише у межах, визначених законом, із дотриманням процедурних гарантій, а всі дії мають переслідувати легітимну мету, бути необхідними та пропорційними. Таким чином, законність у сфері інформаційної безпеки забезпечує баланс між потребами державного захисту та правами особи, слугуючи підґрунтям ефективного правового регулювання інформаційних відносин.

Принцип пропорційності є системоутворювальною засадою правового режиму інформаційної безпеки, що визначає межі допустимого втручання держави у сферу реалізації права на інформацію та свободу вираження поглядів. Його зміст полягає у забезпеченні балансу між публічними інтересами національної безпеки та приватними правами особи, насамперед правом на доступ до інформації, її поширення та використання.

Відповідно до усталеної практики Європейського суду з прав людини (справи Handyside v. the United Kingdom, Sunday Times v. the United Kingdom),

обмеження інформаційних прав є допустимим лише тоді, коли воно ґрунтується на законі, переслідує легітимну мету та є «необхідним у демократичному суспільстві». Зазначене положення становить нормативне підґрунтя принципу пропорційності, який виконує роль критерію правомірності адміністративних рішень і дій у сфері інформаційного контролю.

Як слушно зазначає І. Завидняк, пропорційність у системі забезпечення національної безпеки не може тлумачитися одновимірно, адже вона передбачає обрання «необхідного засобу», який забезпечує досягнення легітимної мети з мінімальним втручанням у сферу прав і свобод людини[66; 68]. Цей підхід відображений, зокрема, у Порядку отримання дозволу суду на здійснення заходів, які тимчасово обмежують права людини, що діяв у 2007–2016 роках (Resolution of the Cabinet of Ministers, 2007). У зазначеному акті було закріплено низку норм, спрямованих на забезпечення співмірності заходів оперативно-розшукової діяльності з цілями органів, уповноважених на їх проведення [64; 68].

Водночас концепція пропорційності в інформаційно-правових відносинах розвивається у контексті доктрини «балансування» (balancing), що передбачає пошук оптимального співвідношення між обмеженням права на інформацію та досягненням суспільно необхідної мети. Як зазначає Б. Тоцький, непропорційним вважається втручання, яке не забезпечує досягнення легітимної мети або досягає її частково, оскільки в такому випадку порушується співвідношення між засобами та результатом [65; 68].

На думку Р. Майданика, органи публічної влади не мають права покладати на громадян обов’язки, що виходять за межі тієї міри необхідності, яка об’єктивно зумовлена публічним інтересом. У межах реалізації владних повноважень держава зобов’язана дотримуватися вимоги пропорційності: застосовуваний захід повинен бути співмірним із метою, заради якої він запроваджується, а обсяг втручання — не перевищувати меж, визначених реальними потребами суспільства [67; 68].

Ця концепція відображає фундаментальний європейський підхід до обмеження прав людини лише в тій мірі, у якій це є необхідним у демократичному суспільстві. Принцип пропорційності виконує функцію інструменту контролю за надмірністю державного втручання, забезпечуючи баланс між публічним інтересом та індивідуальними правами. Він також визначає стандарти належного врядування, у межах яких рішення публічної адміністрації мають бути обґрунтованими, оптимальними та мінімально обтяжливими для особи.

Принцип пропорційності у сфері інформаційної безпеки виконує роль інструменту правового контролю за діяльністю держави, спрямованого на забезпечення оптимального співвідношення між захистом інформаційного простору та гарантіями свободи слова, думки й інформації.

Принцип пропорційності у сфері інформаційної безпеки – це загальноправова конституційна засада, яка вимагає, щоб будь-яке втручання державних органів у реалізацію інформаційних прав і свобод людини здійснювалося на основі закону, переслідувало легітимну мету, було необхідним у демократичному суспільстві, адекватним поставленій меті та мінімально обмежувало права особи, забезпечуючи баланс між національними інтересами та свободою інформаційної діяльності.

Безумовно, загальноправові принципи забезпечують ціннісну єдність правової системи та формують рамкові межі діяльності органів публічної адміністрації, створюючи правовий фундамент для реалізації спеціальних засад інформаційної безпеки.

Розглянувши загальноправові принципи, доцільно звернутися й до адміністративно-правових, оскільки саме вони становлять безпосередній предмет даного дослідження. Адміністративно-правові принципи є концептуальною основою функціонування публічної адміністрації, відображаючи об’єктивні закономірності її організації та діяльності. Вони визначають спрямованість і

зміст управлінського впливу держави на суспільні відносини, зокрема у сфері забезпечення інформаційної безпеки.

Для побудови зазначеної системи принципів доцільно звернутися до наукових підходів, запропонованих у юридичній доктрині. Зокрема, А. Манжула виокремлює такі принципи правового регулювання діяльності науково-дослідних установ, як системність, динамізм, компетентність і функціональність, підпорядкованість (централізм) [69, с. 7; 72]. Аналізуючи адміністративно-правове регулювання у сфері автомобілебудування, Ю. Пірожкова пропонує багаторівневу систему принципів, що включає: загальні принципи – системності, об'єктивності, саморегулювання, зворотного зв'язку, гласності, змагальності, стимулювання; часткові принципи, що застосовуються у різних суспільних підсистемах; організаційно-технологічні принципи – єдиноначальності, поєднання державного, регіонального і місцевого регулювання, конкретності, ієрархії, делегування повноважень [70, с. 70; 72].

Досить розгалужену систему принципів подає С. Ківалов, який поділяє їх на: загальносистемні (об'єктивність, демократизм, розподіл влади, правова впорядкованість, законність, публічність); структурно-цільові (узгодженість і взаємодоповнення цілей, підпорядкування локальних цілей загальнодержавним); структурно-функціональні (диференціація функцій, концентрація зусиль, відповідність регуляторного впливу потребам об'єктів управління); структурно-організаційні (єдність системи державної влади, територіально-галузева організація, різноманітність організаційних зв'язків); структурно-процесуальні (відповідність функцій компетенції, персональна відповідальність, стимулювання ефективності діяльності) [71, с. 165; 72].

Беручи до уваги наведені наукові підходи, ми можемо сформулювати власне бачення системи адміністративно-правових принципів регулювання у сфері інформаційної безпеки, що поєднує загальні закономірності публічного адміністрування з особливостями функціонування інформаційної сфери.

До системи адміністративно-правових принципів належать, зокрема, принципи публічності, підзвітності, превентивності, оперативності, координації та субординації. Кожен із них виконує самостійну функцію у механізмі реалізації публічного управління, забезпечуючи узгодженість дій органів виконавчої влади, ефективність адміністративних рішень і дотримання законності в процесі управлінської діяльності.

Принцип публічності означає відкритість і прозорість діяльності органів публічної влади. Його зміст полягає у тому, що громадськість має бути поінформована про рішення, заходи й результати державної політики у сфері інформаційної безпеки. Цей принцип забезпечує довіру до влади та підсилює її легітимність. Його реалізація ґрунтується на положеннях Закону України «Про доступ до публічної інформації» [73], який визначає правові засади відкритості діяльності суб'єктів владних повноважень.

Принцип підзвітності та відповідальності є одним із ключових у системі адміністративно-правового регулювання сфери інформаційної безпеки. Його сутність полягає в тому, що органи виконавчої влади, їх посадові особи та інші суб'єкти публічного адміністрування несуть персональну юридичну відповідальність за неналежне виконання покладених на них повноважень, ухвалення неправомірних рішень або бездіяльність, що призвела до порушення прав громадян у сфері інформаційної безпеки.

Зміст цього принципу передбачає існування дієвого механізму контролю – парламентського, судового та громадського, – який забезпечує прозорість дій публічної адміністрації, запобігає зловживанням владними повноваженнями та гарантує притягнення до відповідальності винних осіб. Такий підхід сприяє утвердженню правової держави, зміцненню довіри суспільства до органів влади й формуванню відкритого управління.

Як зазначає М. Александрова у своїй дисертаційній роботі, основним контролюючим принципом електронного урядування є підвищення підзвітності

діяльності органів державної влади [59]. Дослідниця справедливо підкреслює, що підзвітність і прозорість є взаємопов'язаними категоріями: з одного боку, електронізація управлінських процесів скорочує час ухвалення рішень, а з іншого – створює ризик формальної безвідповідальності посадовців.

На нашу думку, реалізація принципу прозорості та підзвітності у сфері інформаційної безпеки має ґрунтуватися на таких положеннях:

– кожне управлінське рішення працівника органу влади повинно підтверджуватися електронним цифровим підписом, що забезпечує персоніфікацію відповідальності;
- держава повинна гарантувати відкритий доступ до єдиних реєстрів управлінських рішень, ухвалених на всіх рівнях публічного управління (крім тих, що становлять державну таємницю);
- механізми підзвітності мають передбачати зовнішній аудит, регулярне оприлюднення звітів про діяльність органів влади у сфері інформаційної безпеки та можливість громадського реагування на виявлені порушення.

Безсумнівно, принцип підзвітності та відповідальності в умовах цифрової трансформації набуває нового змісту: він поєднує правові, етичні та технологічні аспекти для забезпечення законності, довіри й ефективності діяльності органів публічної влади у сфері захисту інформаційного простору держави.

Принцип превентивності визначає профілактичність адміністративно-правового впливу. Сутність полягає у спрямуванні зусиль держави на випередження загроз, зниження рівня ризику й створення умов для безпечного функціонування інформаційного середовища. Превентивна діяльність реалізується через моніторинг кіберінцидентів, системи раннього попередження, регулярне оновлення нормативної бази, освітні програми з медіаграмотності та цифрової культури.

Принцип оперативності у сфері інформаційної безпеки є одним із базових орієнтирів адміністративно-правової діяльності, спрямованої на своєчасне

виявлення, попередження й нейтралізацію інформаційних загроз. Його сутність полягає у здатності органів публічної адміністрації швидко, ефективно й у межах законодавчо визначених процедур реагувати на виклики, що виникають у цифровому середовищі.

Оперативність передбачає не лише швидкість дій, а й їх ефективність, доцільність і правову виваженість. У сфері інформаційної безпеки це означає:

- постійний моніторинг інформаційного простору, виявлення кіберзагроз у режимі реального часу;
- наявність чітко визначених адміністративних процедур реагування, які не допускають бюрократичного зволікання;
- забезпечення технічної готовності державних структур (сертифіковані системи захисту, кіберцентри реагування, спеціалізовані підрозділи);
- координацію міжвідомчої взаємодії та швидкий обмін інформацією між державними, військовими й громадськими структурами;
- -підготовку кадрового потенціалу, спроможного ухвалювати рішення в умовах інформаційної турбулентності.

Як слушно зазначають фахівці з адміністративного права, принцип оперативності засуджує практику штучного або невмотивованого зволікання з прийняттям управлінських рішень. Його реалізація вимагає, щоб розгляд справ, запитів і звернень здійснювався не формально в межах установлених строків, а в оптимальний для досягнення мети час, тобто тоді, коли рішення ще має практичну користь і значення для суб’єкта звернення [74].

У сфері інформаційної безпеки принцип оперативності має подвійне значення: по-перше, як організаційно-функціональна вимога до діяльності органів виконавчої влади – діяти швидко, узгоджено й технічно готово; по-друге, як правова гарантія ефективності реагування на інформаційні інциденти, що мінімізує шкоду від кіберзагроз і дезінформаційних атак.

Оперативність виступає не лише ознакою якісного адміністрування, а й умовою забезпечення національної стійкості інформаційного простору, оскільки своєчасне реагування є ключем до запобігання кризовим явищам, порушенням прав громадян і втраті довіри до державних інституцій.

Принцип координації та субординації відображає ієрархічну й водночас мережеву природу системи публічного управління. У сфері інформаційної безпеки він означає узгодженість дій центральних і місцевих органів виконавчої влади, правоохоронних структур, органів місцевого самоврядування, а також партнерську взаємодію з приватними суб'єктами та міжнародними організаціями.

Принцип координації та субординації є невід'ємною складовою ефективного адміністративно-правового регулювання у сфері інформаційної безпеки тому, що:

- він забезпечує цілісність і узгодженість системи управління, коли дії органів не розірвані, не фрагментовані, а інтегровані;
- дозволяє поєднати вертикаль (єдине керівництво, централізоване регулювання) із мережею горизонтальних зв'язків (швидка кооперація, партнерство, адаптація до нових ризиків);
- підвищує здатність держави реагувати на складні інформаційні виклики – бо розсинхронізація чи «споріднені мінісистеми», що не комунікують, створюють слабкі місця;
- сприяє ефективному використанню ресурсів – уникання дублювання, забезпечення чіткого розподілу повноважень, злагодженої комунікації.

Упровадження принципу координації та субординації в політику й практику інформаційної безпеки створює цілісну управлінську модель, у якій поєднуються вертикальні та горизонтальні механізми взаємодії. Така модель забезпечує узгодженість дій державних і приватних суб'єктів, підвищує ефективність реагування на інформаційні загрози, мінімізує ризики

фрагментарності управлінських рішень і сприяє збереженню єдності інформаційного простору держави.

У контексті подальшого теоретичного осмислення варто звернутися до спеціальних принципів інформаційної безпеки, що конкретизують зміст і спрямованість адміністративно-правового регулювання цієї сфери. Саме вони формують науково обґрунтовану основу галузевої політики, відображаючи баланс між загальноправовими засадами й особливостями цифрової епохи.

До спеціальних принципів, що визначають специфіку державного управління у сфері інформаційної безпеки, ми вважаємо слід віднести баланс між свободою інформації та її захистом, інтегрованість, технологічна адаптивність, наукова обґрунтованість, системність і комплексність.

В основі цього принципу лежить діалектична єдність двох цінностей – свободи доступу до інформації та обов’язку держави гарантувати інформаційну безпеку. Відповідно до статті 34 Конституції України, кожен має право вільно збирати, зберігати, використовувати й поширювати інформацію, проте здійснення цих прав може бути обмежене законом «в інтересах національної безпеки, територіальної цілісності або громадського порядку» [46]. Аналогічна позиція закріплена у статті 10 Конвенції про захист прав людини і основоположних свобод, яка визначає, що свобода вираження поглядів включає не лише право на поширення інформації, а й обов’язок уникати шкоди для репутації та прав інших осіб [75].

У національному законодавстві баланс між відкритістю та захистом регламентується, зокрема, Законом України «Про інформацію» (ред. 2024 р.), який у статті 5 визначає принципи достовірності, повноти, відкритості та законності інформації [76], а також Законом України «Про захист персональних даних» (ред. 2023 р.), що встановлює межі обробки конфіденційної інформації [77]. Правова система України спирається на європейську доктрину «proportional balance» – пропорційного балансу між свободою слова та безпекою суспільства.

Особливої актуальності цей принцип набуває у цифрову добу, коли інформаційні технології перетворюють кожного користувача на потенційного творця контенту, а соціальні мережі – на головний інструмент впливу на громадську думку. Відсутність правової культури та цифрової етики призводить до поширення фейків, кібербулінгу, мови ворожнечі. Правова політика держави має поєднувати захист свободи слова з інформаційною відповідальністю, формуючи «превентивно-правову культуру поведінки в мережі».

У практичному вимірі цей принцип реалізується через: прозоре регулювання контенту без запровадження цензури; впровадження саморегуляції медіа та платформ відповідно до Кодексу ЄС про протидію дезінформації; забезпечення права на забуття та видалення недостовірної інформації; посилення цифрової грамотності користувачів, що формує внутрішні механізми етичного самоконтролю.

Принцип балансу між свободою інформації та її захистом є комплексним, міждисциплінарним і поєднує елементи конституційних прав людини, адміністративно-правових гарантій та інформаційної безпеки. Його реалізація забезпечує стійкість демократичного суспільства, запобігаючи як надмірному державному втручанню (цензурі), так і інформаційному хаосу.

Українська правова система поступово формує європейську модель інформаційної рівноваги, де пріоритетом є не обмеження, а відповідальне користування свободою слова.

В умовах постійних інформаційних загроз ключовою умовою ефективності цього принципу є підвищення правової та цифрової культури громадян, розвиток саморегуляційних механізмів у медіапросторі та належна судова практика щодо захисту честі, гідності й персональних даних.

Принцип інтегрованості означає узгодження національних заходів у сфері інформаційної безпеки з міжнародними стандартами, зокрема із Керівними принципами ООН щодо інформаційної безпеки та Директивою (ЄС) 2022/2555

про заходи високого спільного рівня кібербезпеки в Союзі (NIS 2) [78]. Він забезпечує сумісність національної системи з європейською безпековою архітектурою, сприяючи обміну досвідом і спільним протоколам реагування.

Принцип технологічної адаптивності відображає необхідність постійного оновлення правового регулювання відповідно до темпів розвитку цифрових технологій. Інформаційна сфера надзвичайно динамічна, тому нормативна система має бути гнучкою, здатною реагувати на появу нових викликів, таких як штучний інтелект, блокчейн-технології, біометричні дані тощо.

Принцип наукової обґрунтованості передбачає, що формування державної політики у сфері інформаційної безпеки має базуватися на доказовій аналітиці, експертних оцінках, результатах наукових досліджень і прогнозах розвитку загроз. Це забезпечує раціональний характер управлінських рішень і підвищує їхню ефективність.

Принцип системності та комплексності вимагає розглядати інформаційну безпеку не ізольовано, а як складову загальної системи національної безпеки. Він передбачає взаємозв’язок між кібербезпекою, політичною, економічною, воєнною, соціальною й гуманітарною безпекою, що дозволяє здійснювати цілісну державну політику.

Таким чином, принципи адміністративно-правового регулювання інформаційної безпеки утворюють ієрархічно впорядковану систему, яка поєднує універсальні правові цінності та спеціальні вимоги інформаційного суспільства. Вони визначають концептуальні засади формування державної політики, спрямованої на забезпечення стійкості інформаційного середовища, розвиток демократичної комунікаційної культури та зміцнення правової державності. Застосування цих принципів у практичній діяльності публічної адміністрації забезпечує узгодженість, передбачуваність і легітимність дій держави, сприяє формуванню довіри громадян до інститутів влади та підвищує ефективність національної системи безпеки.

Запропонована нами класифікація дозволяє розглядати принципи адміністративно-правового регулювання інформаційної безпеки як багаторівневу систему норм і цінностей, що забезпечує єдність теоретичного, нормативного та практичного вимірів державної політики у сфері захисту інформаційного простору. Її перевага полягає у тому, що вона: відображає як вертикальну (від загального до спеціального), так і горизонтальну (функціонально-ціннісну) структуру принципів; дозволяє інтегрувати міжнародні стандарти безпеки у національну правову систему; формує цілісний підхід до розуміння інформаційної безпеки як правового, управлінського і гуманітарного феномену.

У межах цієї класифікації принципи не лише виконують функцію методологічних орієнтирів, а й виступають критерієм оцінки ефективності адміністративно-правової практики – від нормотворення до правозастосування. Саме їх дотримання забезпечує узгодженість державної політики з потребами суспільства та стандартами демократичного врядування.

Отже, можна стверджувати, що дослідження загальноправових, адміністративно-правових і спеціальних принципів дало змогу сформувати узагальнену класифікацію принципів адміністративно-правового регулювання інформаційної безпеки України, яку вибудувано на ієрархії правового регулювання, узгоджено з тенденціями інформаційної політики та зорієнтовано на вимоги європейського правового простору. Уважаємо, така класифікація повинна спиратися на ключові критерії – сферу дії, функціональне призначення, змістовно-ціннісну орієнтацію і джерело нормативного закріплення.

За сферою дії принципи розподіляються на три рівні:

– загальноправові, що становлять фундамент правової системи та відображають універсальні цінності – верховенство права, законність, справедливість, пропорційність, пріоритет прав і свобод людини;
– галузеві (адміністративно-правові), які конкретизують загальні засади у сфері публічного управління, визначаючи порядок діяльності органів

виконавчої влади – публічність, відкритість, підзвітність, ефективність, превентивність, координацію та субординацію;

– спеціальні, що відображають особливості інформаційного простору – баланс між свободою інформації та її захистом, достовірність і цілісність даних, технологічну адаптивність, системність, наукову обґрунтованість і міжнародну інтегрованість.

За функціональним призначенням принципи поділяються на:

– регулятивні, які визначають організаційні основи діяльності суб'єктів адміністративно-правових відносин;
– гарантійні, спрямовані на забезпечення реалізації прав і свобод людини, запобігання зловживанням владою та забезпечення правового захисту;
– превентивно-захисні, орієнтовані на попередження інформаційних загроз, формування стійкості інформаційного простору та підвищення готовності суб'єктів до реагування;
– інтеграційно-координаційні узгоджують дії між органами державної влади, приватним сектором і громадянським суспільством.

За змістовно-ціннісною орієнтацією доцільно виокремити:

– демократично-правові принципи гарантують свободу вираження думки, прозорість і підзвітність влади, а також довіру до державних інститутів;
– безпеково-захисні принципи, що відображають обов'язок держави забезпечити безпечне функціонування комунікаційного середовища та захист прав суб'єктів інформаційних відносин;
– етико-гуманітарні принципи, спрямовані на формування моральної відповідальності держави, ЗМІ та користувачів за достовірність, правдивість і суспільну корисність інформації.

1.3. Нормативно-правові акти у сфері забезпечення національної безпеки в інформаційній сфері

Ефективне функціонування системи інформаційної безпеки держави є неможливим без чітко структурованої та внутрішньо узгодженої нормативно-правової бази, яка визначає компетенцію суб'єктів публічної адміністрації, регламентує порядок їх взаємодії та встановлює межі допустимого втручання у сферу комунікацій. За умов інтенсивної цифровізації, ускладнення інформаційного середовища, зростання кількості кіберінцидентів і посилення гібридних загроз формування такої бази набуває стратегічного значення, оскільки від її системності, правової визначеності та відповідності принципам демократичного врядування залежить стійкість національного інформаційного простору й результативність державної політики у сфері національної безпеки.

Система нормативно-правового забезпечення інформаційної безпеки України має багаторівневу, ієрархічно впорядковану структуру. Її логіка побудована за класичною схемою: Конституція України, закони, підзаконні нормативні акти, міжнародно-правові договори, доктринальні та стратегічні документи, стандарти і технічні регламенти. Кожен з рівнів має функціональне призначення у формуванні правового режиму інформаційної безпеки.

Верхній рівень правової ієрархії становить Конституція України, яка закріплює базові засади національної безпеки, свободи слова, права на інформацію та недоторканності приватного життя. Вона окреслює концептуальні межі взаємодії держави, суспільства й особи в інформаційній сфері та виступає першоджерелом ключових принципів формування державної політики у сфері інформаційної й кібербезпеки.

На нашу думку, саме конституційний рівень правового регулювання створює методологічне підґрунтя для побудови всієї системи інформаційної безпеки, оскільки він задає не лише правові, а й ціннісні орієнтири державної

політики – рівновагу між інформаційною відкритістю суспільства та гарантіями його безпечного розвитку.

Відповідно до ст. 8 Конституції України, у державі визнається і діє принцип верховенства права [46]. У контексті інформаційної безпеки, як зазначалося у підрозділі 1.2, цей принцип означає, що будь-які обмеження свободи вираження поглядів, доступу до інформації чи цифрової комунікації можуть здійснюватися виключно на підставі закону, бути необхідними у демократичному суспільстві та пропорційними легітимній меті. Верховенство права у сфері інформаційної безпеки виконує стримувально-врівноважувальну функцію – не дозволяє державі діяти свавільно, водночас легітимізуючи правомірні заходи захисту національного інформаційного простору. У цьому контексті воно слугує методологічним стрижнем для всієї системи правового регулювання, забезпечуючи баланс між владними повноваженнями та індивідуальними свободами.

Відповідно до ст. 17 Конституції України, захист суверенітету та територіальної цілісності держави, забезпечення її економічної й інформаційної безпеки належать до найважливіших функцій держави [46]. Це положення надає інформаційній безпеці конституційного статусу, закріплюючи обов’язок держави формувати ефективну систему органів, процедур і механізмів, спрямованих на охорону національного інформаційного простору. У науковій літературі слушно підкреслюється, що зазначена конституційна норма становить інституційну основу державної політики у сфері кіберзахисту, протидії дезінформації, інформаційно-психологічним впливам, а також захисту критичної інформаційної інфраструктури. Реалізація приписів ст. 17 Конституції визначає стратегічні напрями розвитку законодавства у сфері інформаційної безпеки [79, с. 457], формуючи системно узгоджену нормативну базу, орієнтовану на забезпечення стійкості держави до внутрішніх і зовнішніх інформаційних загроз.

Уважаємо, що, конституційне закріплення інформаційної безпеки засвідчує про еволюцію національної правової доктрини – від технократичного до ціннісно-правового підходу до безпеки, у межах якого інформаційну безпеку розглядають як елемент державного суверенітету й індикатор демократичної зрілості суспільства, гарант стабільності публічного управління і засіб забезпечення реалізації прав і свобод людини в інформаційному середовищі.

У ст. 34 Конституції України кожному гарантовано право на вільний збір, зберігання, використання і поширення інформації в будь-який спосіб, що створює підґрунтя для функціонування демократичного інформаційного простору. Водночас друга частина цієї статті передбачає можливість обмеження відповідного права законом – в інтересах національної безпеки, територіальної цілісності чи громадського порядку, з метою запобігання заворушенням або злочинам, охорони здоров'я населення, захисту репутації чи прав інших осіб [46].

Як бачимо, Конституція України формує механізм пропорційного балансу між свободою слова та безпекою, що повністю корелює з усталеною практикою Європейського суду з прав людини, зокрема у справах Handyside v. the United Kingdom (1976) та Sunday Times v. the United Kingdom (1979) [80; 81]. У зазначених рішеннях Суд підкреслив, що свобода вираження поглядів є однією з фундаментальних засад демократичного суспільства, однак її можна обмежити за наявності трьох умов: законності, необхідності та пропорційності втручання.

За нашим розумінням, українська модель реалізації принципу свободи інформації у поєднанні з безпековими обмеженнями засвідчує про еволюцію конституційного регулювання у напрямі європейських стандартів. Її особливість полягає у прагненні не звужувати свободу слова, а запроваджувати правові інструменти її відповідального використання – насамперед через закони «Про інформацію» [76], «Про захист персональних даних» [77], «Про медіа» [82] та судову практику Верховного Суду, що враховує позиції ЄСПЛ.

У попередньому підрозділі зазначено, проблематика балансу між свободою інформації та її захистом є одним з базових спеціальних принципів інформаційної безпеки, адже в цифрову добу саме інформація стає водночас ресурсом розвитку та потенційною загрозою. З огляду на це, забезпечення такого балансу є не лише конституційним обов'язком держави, а й ключовою умовою ефективності системи адміністративно-правового регулювання інформаційної безпеки.

З огляду на це можна стверджувати, що ст. 34 Конституції України виконує подвійну функцію: з одного боку, вона гарантує інформаційну відкритість і свободу комунікації як невід'ємний елемент демократії; з іншого – закладає правовий механізм їх узгодження з інтересами державної та громадської безпеки. У результаті формується європейський тип правового мислення, заснований на принципі відповідального користування свободою інформації, що є наріжним каменем сучасної моделі інформаційної безпеки України.

У ст. 32 Конституції України закріплює право кожного на невтручання в особисте і сімейне життя та на захист від незаконного збирання, зберігання, використання і поширення конфіденційної інформації [46]. Вона створює конституційну основу інформаційної безпеки особи, зобов'язуючи державу гарантувати захист персональних даних і недоторканність приватного життя. У цифровому середовищі ця норма набуває особливого значення, адже порушення приватності часто має не лише етичні, а й безпекові наслідки. На наш погляд, держава повинна забезпечити ефективний адміністративно-правовий механізм захисту приватності із запобіжними й компенсаційними засобами. У цьому аспекті важливо формувати культуру обережного поводження з персональними даними – від освітніх програм до державних стандартів кібергігієни.

Додатково значення для сфери інформаційної безпеки мають ст. 15, яка забороняє цензуру та гарантує свободу діяльності засобів масової інформації; ст. 19, що зобов'язує органи державної влади діяти лише в межах, визначених Конституцією та законом; а також ст. 92, яка встановлює, що основи

національної безпеки та громадського порядку визначаються виключно законами України [46]. Ці положення формують правовий каркас конституційного режиму інформаційної безпеки, у межах якого будь-яке втручання держави у сферу комунікацій повинно бути юридично обґрунтованим, прозорим і підзвітним. На наш погляд, саме дотримання цього принципу підзвітності є передумовою формування довіри громадян до політики держави в інформаційній сфері.

Конституційні засади забезпечення інформаційної безпеки України утворюють цілісну триєдину систему: ціннісну – орієнтовану на пріоритет прав людини, свободу інформації та приватність; інституційну, що визначає обов'язок держави захищати суверенітет і національний інформаційний простір; і функціональну – побудовану на принципах законності, пропорційності та підзвітності. Конституція України, на нашу думку, є не лише формальним джерелом права, а й методологічним стрижнем адміністративно-правового регулювання інформаційної безпеки. Вона задає нормативну єдність державної політики, визначає рамки легітимного втручання у сферу інформаційних прав і водночас гарантує, що безпека не стане засобом обмеження людської свободи, а залишатиметься її необхідною умовою.

Наступним рівнем у структурі правового регулювання інформаційної безпеки є законодавче ядро, яке конкретизує положення Конституції України та формує нормативну основу державної інформаційної політики. Норми цього рівня визначають стратегічні цілі, принципи, суб'єктів і механізми реалізації державної політики у сфері захисту інформаційного простору, забезпечуючи баланс між відкритістю комунікаційного середовища та національними інтересами безпеки.

До ключових нормативно-правових актів належать:

– Закон України «Про національну безпеку України» [23] визначає інформаційну безпеку одним із пріоритетних напрямів державної політики та встановлює систему суб'єктів її реалізації;

- Закон України «Про інформацію» [76] окреслює правові засади інформаційних відносин, класифікацію інформації, права й обов'язки суб'єктів;
- Закон України «Про основні засади забезпечення кібербезпеки України» [47] – регламентує організаційні та правові основи функціонування системи кіберзахисту, компетенцію відповідальних органів і механізми реагування на кіберінциденти;
- Закон України «Про доступ до публічної інформації» [73] забезпечує відкритість діяльності органів влади та реалізацію принципу прозорості управління;
- Закон України «Про захист персональних даних» [77] визначає порядок обробки інформації, що стосується приватного життя людини, і закріплює правові гарантії її захисту;
- спеціальні нормативні акти – «Про електронні комунікації» [83], «Про електронну ідентифікацію та електронні довірчі послуги» [84], «Про критичну інфраструктуру» [85] – деталізують технічні та організаційні вимоги до цифрової безпеки, сертифікації, електронної ідентифікації та функціонування об'єктів критичної інформаційної інфраструктури.

Сукупність зазначених актів формує нормативне підґрунтя державної системи інформаційної безпеки, у межах якого визначено компетенцію органів публічної влади, правовий статус операторів телекомунікацій, провайдерів і користувачів, а також закріплено механізми реалізації прав громадян на інформаційну захищеність.

З огляду на системну роль законодавчого рівня у формуванні механізму інформаційної безпеки, доцільним є більш детальний аналіз ключових актів, які визначають архітектоніку правового регулювання у цій сфері.

Закон України «Про національну безпеку України» є провідним актом стратегічного характеру, що встановлює засади державної політики у сфері національної безпеки, зокрема інформаційної та кібербезпеки. Відповідно до статті 3, інформаційна безпека визнається одним із основних напрямів державної безпеки поряд із військовою, економічною, екологічною та соціальною. Стаття 4 закріплює принципи державної політики безпеки – верховенство права, пріоритет прав і свобод людини, демократичний цивільний контроль над органами сектору безпеки, комплексність і збалансованість заходів [23].

Особливістю цього закону є визначення інституційної системи суб'єктів інформаційної безпеки, до якої належать Рада національної безпеки і оборони України, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації України, Міністерство цифрової трансформації, Міністерство оборони, Національний банк України тощо. У такий спосіб створюється координаційна основа міжвідомчої взаємодії, визначаються компетенція органів влади, розподіл повноважень і відповідальності між ними.

Наукове значення цього закону полягає в тому, що він забезпечує інтеграцію безпекової, інформаційної та кіберполітики держави, закладаючи підвалини для побудови цілісної системи стратегічного управління інформаційною безпекою. На нашу думку, зазначений акт виконує роль нормативного «мосту» між конституційними принципами та галузевим законодавством, оскільки саме він визначає рамкові параметри політики інформаційної безпеки, які конкретизуються у спеціальних нормативних актах.

Наступним елементом законодавчої системи, що конкретизує положення Конституції України та принципи, визначені Законом «Про національну безпеку України», є Закон України «Про інформацію» [76]. Саме він виступає основним нормативним актом, який закладає загальні засади правового регулювання інформаційних відносин і формує підґрунтя для розвитку спеціального законодавства у сфері інформаційної та кібербезпеки.

Цей закон визначає правові основи інформаційної діяльності, статус інформації як об’єкта правовідносин і встановлює принципи її обігу в демократичному суспільстві. У ст. 1 сформульовано ключові поняття, що становлять понятійно-категоріальний апарат галузі: інформація, документ, захист інформації, суб’єкт владних повноважень [76]. Такий підхід забезпечує цілісність і системність подальшого розвитку інформаційного права, сприяючи уніфікації термінів у суміжних актах – зокрема у законах про електронні комунікації, персональні дані та засоби масової інформації .

Відповідно до ст. 2, інформаційні відносини ґрунтуються на принципах достовірності, повноти, своєчасності, свободи поширення інформації, законності її обмеження, а також дотримання балансу між відкритістю і захистом персональних даних [76]. Ці принципи є основоположними для формування державної політики у сфері інформаційної безпеки, оскільки вони забезпечують узгодження інтересів особи, суспільства та держави в інформаційному просторі.

Особливо важливими є ст. 25–31, які гарантують реалізацію права на інформацію. Зокрема, ст. 31 закріплює право особи вимагати усунення недостовірної чи упередженої інформації, поширеної щодо неї, ст. 27 передбачає юридичну відповідальність за порушення законодавства у сфері інформації [76]. Ці норми є ефективним механізмом правового захисту інформаційних прав і свобод, який охоплює превентивний і відновлювальний аспекти.

Закон має важливе науково-прикладне значення, адже виконує одночасно дві функції: регулятивну – визначаючи правові межі інформаційної діяльності, та гарантійну – забезпечуючи реалізацію і захист прав суб’єктів інформаційних відносин. Він поєднує публічно-правовий і приватно-правовий підходи, що дозволяє застосовувати його норми у найширшому спектрі соціальних, економічних і управлінських відносин.

Наступним ключовим нормативним елементом у системі правового забезпечення інформаційної безпеки України є Закон України «Про основні

засади забезпечення кібербезпеки України» [47]. На відміну від попередніх законодавчих актів, цей Закон не обмежується лише декларуванням загальних принципів діяльності у сфері інформаційної безпеки, а формує цілісну операційно-правову рамку функціонування національного кіберпростору, визначаючи механізми координації, реагування та взаємодії суб'єктів під час виникнення кіберінцидентів і кіберзагроз.

Зазначений Закон конкретизує положення Закону України «Про національну безпеку України» у частині регулювання діяльності у сфері кібербезпеки, виступаючи його спеціальним нормативним розвитком. У статті 1 Закону закріплено базові дефініції – «кібербезпека», «кіберзахист», «кіберінцидент», «кібератака» тощо, що забезпечує термінологічну єдність і точність правового регулювання у відповідній сфері**.**

Важливим аспектом Закону є визначення системи суб'єктів забезпечення кібербезпеки, серед яких провідну координаційну роль відіграють Рада національної безпеки і оборони України, Державна служба спеціального зв'язку та захисту інформації, Служба безпеки України, Міністерство оборони України, Національна поліція, а також оператори критичної інформаційної інфраструктури. У Законі окреслено основні механізми реагування на кіберінциденти, що передбачають оперативну координацію дій, інформаційний обмін, проведення технічного розслідування, а також застосування заходів юридичної відповідальності до винних осіб [47].

Закон України «Про основні засади забезпечення кібербезпеки України» формує операційний нормативний фундамент національної системи кіберзахисту, спрямований на забезпечення реалізації принципів превентивності, координації, технологічної адаптивності та інституційної узгодженості дій державних і недержавних суб'єктів у сфері інформаційної безпеки.

Безперечно, Закон України «Про захист персональних даних» [77] посідає особливе місце в системі нормативно-правового забезпечення інформаційної

безпеки, оскільки визначає гуманітарно-правовий вимір цифрової безпеки – захист приватного життя та інформаційної автономії особи. Його норми спрямовані на реалізацію положень ст. 32 Конституції України [46], а також на імплементацію положень Конвенції Ради Європи № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» [86] та Регламенту (ЄС) 2016/679 (GDPR) у національне законодавство.

У ст. 2 закріплено базові терміни: «персональні дані», «обробка персональних даних», «згода суб'єкта персональних даних» [77], що забезпечує концептуальну визначеність й уніфікованість правового регулювання, дозволяє адаптувати українське законодавство до європейської термінологічної практики. Визначення терміну «згода суб'єкта даних» підкреслює добровільний і свідомий характер участі особи в інформаційному обігу, що є однією з ключових гарантій цифрової демократії.

Особливе значення має ст. 6, що закріплює принцип мети й пропорційності обробки даних. Згідно з нею, персональні дані слід збирати із чітко визначеною метою, оброблятися у межах, потрібних для її досягнення, і не підлягати подальшій обробці, несумісній із цією метою. У такий спосіб закон забезпечує баланс між інтересами суспільства в обігу інформації і правом людини на інформаційну приватність. З науково-правової позиції, норма конкретизує принцип пропорційності втручання у приватну сферу, який є складовою верховенства права і відповідає усталеній практиці Європейського суду з прав людини (справи Rotaru v. Romania, S. and Marper v. the United Kingdom).

Не менш важливим є положення ст. 24, яке визначає повноваження Уповноваженого Верховної Ради України з прав людини як незалежного національного органу контролю за дотриманням законодавства про захист персональних даних. Інституційна роль Уповноваженого полягає у здійсненні моніторингу, розгляді скарг суб'єктів персональних даних, проведенні перевірок і застосуванні заходів реагування. Таким чином, реалізується принцип

інституційної автономії контролю, що відповідає європейським стандартам незалежного нагляду у сфері захисту приватності.

Окремо варто зазначити, що чинна редакція закону (2023 р.) передбачає розвиток механізмів інформованої згоди, права на забуття та права на переносимість даних, що відображає поступову адаптацію українського законодавства до положень GDPR і практик ЄС. Це посилює персоніфікований характер правового захисту в умовах цифровізації публічних послуг і розширення електронного урядування.

На нашу думку, Закон України «Про захист персональних даних» формує гуманітарну площину інформаційної безпеки, у центрі якої – особистість як носій інформаційних прав і суб'єкт контролю над власними даними. Його значення полягає не лише в техніко-юридичному регулюванні, а й у зміщенні акценту з державоцентричної на людиноцентричну модель безпеки. Саме тому цей закон можна розглядати як основу для розвитку етико-правової концепції цифрової безпеки, що поєднує принципи приватності, гідності, автономії та відповідальності у сучасному інформаційному суспільстві.

Закон України «Про електронні комунікації» [83] є ключовим етапом у модернізації правового регулювання телекомунікаційної сфери, спрямованим на гармонізацію українського законодавства з правом Європейського Союзу. Його ухвалення ознаменувало перехід від застарілої концепції «зв'язку» до сучасної категорії «електронних комунікацій», що відображає конвергенцію цифрових технологій, телекомунікацій і мережевого середовища.

У системі інформаційної безпеки цей закон виконує інституційно-захисну функцію, визначаючи правові засади створення, функціонування та захисту електронних комунікаційних мереж і послуг. Згідно зі статтями 3–5, до основних принципів державної політики у сфері електронних комунікацій належать технологічна нейтральність, безпека мереж, конфіденційність зв'язку, а також захист прав користувачів [83]. Така структурна побудова відповідає європейській

моделі Digital Single Market [88], у межах якої безпека розглядається не лише як технічний, а й правовий обов'язок операторів.

Закон закріплює зобов'язання операторів і провайдерів забезпечувати стійкість мереж, попередження кіберінцидентів і взаємодію з Національним центром оперативно-технічного управління мережами телекомунікацій. Це сприяє формуванню механізму співрегулювання, де приватний сектор виступає активним учасником забезпечення інформаційної безпеки, а держава – координатором і наглядовим суб'єктом.

Особливу увагу приділено запровадженню поняття «оператор суттєвих послуг». Це поняття створює підґрунтя для віднесення суб'єктів електронних комунікацій до критичної інфраструктури залежно від рівня їхнього впливу на національну безпеку. У такий спосіб закон посилює сумісність української системи кіберзахисту з європейською архітектурою безпеки та забезпечує правову інтеграцію у простір ЄС.

Уважаємо, що цей нормативний акт має подвійне значення: по-перше, він є інструментом цифрової трансформації, що регламентує нову модель електронних комунікацій з урахуванням інноваційного розвитку; по-друге, елементом безпекової політики, який закладає правові основи для забезпечення кіберстійкості телекомунікаційних систем. Його впровадження сприяє реалізації принципів координації, технологічної адаптивності та субсидіарності у сфері адміністративно-правового регулювання інформаційної безпеки.

Закон України «Про критичну інфраструктуру» [85] є логічним продовженням розвитку національної системи безпеки для інституціоналізації підходів до захисту життєво важливих об'єктів. Це структурно-функціональна основа управління критичними системами, до яких належать об'єкти енергетики, транспорту, фінансів, охорони здоров'я, цифрових комунікацій тощо.

У Законі закріплено, що інформаційна безпека є ключовим критерієм віднесення об'єктів до критичної інфраструктури, що підкреслює її

інтегративний характер у забезпеченні національної стійкості. Закон вводить поняття «національна система захисту критичної інфраструктури» [85], у межах якої реалізуються принципи координації, субординації та превентивності, спрямовані на попередження кризових ситуацій, кіберінцидентів і дестабілізаційних впливів.

Також важлива процедура категоризації об'єктів, що дозволяє визначати рівні критичності й вимоги до сертифікації та аудиту безпеки. У цьому аспекті закон впроваджує ризик-орієнтований підхід, наближений до європейських стандартів, зокрема до вимог Директиви (ЄС) 2022/2557 (CER Directive) [89].

Закон також запроваджує механізми державного моніторингу і взаємодії між органами влади та операторами критичної інфраструктури, що забезпечує узгодженість дій у межах єдиної системи національної безпеки. Наукове значення цього закону полягає у тому, що він формує інституційний міст між інформаційною, кібер- та технічною безпекою, створюючи правову основу для побудови мультидисциплінарної моделі безпекового управління.

Закони «Про електронні комунікації» та «Про критичну інфраструктуру» у сукупності забезпечують перехід від фрагментарного до системного підходу у правовому регулюванні цифрової безпеки. Вони формують нормативну платформу, яка поєднує вимоги європейських директив, національні особливості управління та сучасні принципи адміністративного права – координацію, превентивність, пропорційність і технологічну адаптивність.

Здійснений аналіз положень чинного законодавства дозволяє констатувати, що нормативно-правова база України у сфері інформаційної безпеки є достатньо розвиненою та структурно впорядкованою, хоча потребує подальшого концептуального оновлення й узгодження з європейським правом.

По-перше, системність і взаємодоповнюваність законодавства передбачає формування цілісного комплексу нормативних актів, які регулюють різні рівні забезпечення інформаційної безпеки – від конституційних гарантій (Конституція

України, Закон «Про національну безпеку України») до спеціалізованих актів (зокрема, Закон «Про основні засади забезпечення кібербезпеки України», Закон «Про критичну інфраструктуру», Закон «Про захист персональних даних»). Така ієрархічна побудова відповідає європейській доктрині multi-layer security governance, що поєднує правові, організаційні й технологічні засоби захисту.

По-друге, інтегрованість у міжнародний правовий простір засвідчує орієнтацію України на адаптацію положень acquis communautaire – правових надбань Європейського Союзу. Значну частину законів України розроблено на основі чи з урахуванням європейських актів, з-поміж яких Регламент (ЄС) 2016/679 (GDPR), Директива (ЄС) 2016/1148 (NIS 1), Директива (ЄС) 2022/2557 (CER Directive), Директива (ЄС) 2022/2555 (NIS 2). Це забезпечує нормативну сумісність і сприяє інтеграції України у цифрову безпекову архітектуру ЄС.

По-третє, превентивна спрямованість є однією з ознак правового регулювання. Законодавчі норми дедалі частіше орієнтовані на реагування на загрози та на їх попередження через розвиток кіберкультури, системи моніторингу інцидентів, стандартизацію процедур реагування і формування державної політики кіберстійкості. Положення узгоджують з принципом превентивності, закріпленим у Концепції національної безпеки України.

По-четверте, водночас спостерігаються окремі колізії та термінологічні розбіжності. Зокрема, неврегульованими залишаються питання розмежування компетенцій між Службою безпеки України, Державною службою спеціального зв’язку та захисту інформації, Міністерством цифрової трансформації; у різних нормативних актах паралельно використовуються поняття «кіберзахист», «інформаційна безпека» та «захист інформації». Це свідчить про відсутність єдиного концептуального підходу до визначення категоріального апарату інформаційного права.

По-п’яте, наявна потреба гармонізації з європейським правом, зокрема з положеннями Директиви (ЄС) 2022/2555 (NIS 2), що встановлює спільні

стандарти кібербезпеки для критичних секторів, та Регламенту (ЄС) 2016/679 (GDPR), у якому визначено загальні принципи захисту персональних даних. Така гармонізація сприятиме підвищенню правової визначеності й ефективності взаємодії українських інституцій з європейськими структурами у цифровій сфері.

Узагальнюючи, можна стверджувати, що законодавче забезпечення інформаційної безпеки України формує нормативне підґрунтя для функціонування національної системи кібер- та інформаційного захисту, забезпечує баланс між інтересами держави та правами людини, а також закладає основи для технологічної модернізації безпекового сектору. Його подальший розвиток має ґрунтуватися на принципах системності, наукової обґрунтованості, технологічної адаптивності та міжнародної інтегрованості, що дозволить сформувати стійку й ефективну модель адміністративно-правового регулювання у сфері інформаційної безпеки України.

Розгляд законодавчого рівня регулювання дозволяє перейти до аналізу підзаконних нормативно-правових актів, що є операційним виміром системи правового забезпечення інформаційної безпеки. На ньому конкретизуються законодавчі приписи, формуються механізми практичної реалізації державної політики у сфері кібер- та інформаційного захисту, здійснюється адміністративне регулювання взаємодії суб’єктів безпекового сектора.

Підзаконні нормативні акти відіграють роль інструментів адміністративного управління, які встановлюють організаційно-процедурні засади функціонування систем інформаційної безпеки, координаційні механізми, стандарти технічного захисту та порядок реагування на кіберінциденти.

Система підзаконних актів у сфері інформаційної безпеки має багаторівневу структуру, що включає укази Президента України, постанови Кабінету Міністрів України та накази центральних органів виконавчої влади (ЦОВВ). Кожен із цих рівнів має власне функціональне призначення, яке відображає ступінь деталізації та галузевої спеціалізації нормативного впливу.

Укази Президента України виступають стратегічно-програмними актами, які визначають пріоритети державної політики. Зокрема, Указ № 47/2017 «Про Доктрину інформаційної безпеки України» [90] заклав концептуальні засади національної політики у сфері інформаційного суверенітету, протидії дезінформації, розвитку інформаційної культури та стратегічних комунікацій. Доктрина підкреслила гуманітарно-правову природу інформаційної безпеки, розглядаючи її як складову сталого розвитку та демократичного врядування.

Подальший розвиток доктринальних положень відбувся в Указі Президента № 392/2020 «Про Стратегію національної безпеки України «Безпека людини – безпечна країна» [91], який уперше закріпив концепцію human security, тобто безпеки людини як центрального елемента національної безпеки. Інформаційна безпека в цьому контексті набула гуманітарного змісту, що пов’язує її не лише з технічним захистом даних, а й із правами людини, приватністю, гідністю та інформаційною стійкістю суспільства.

Указ Президента № 447/2021 «Про Стратегію кібербезпеки України» [92] деталізував механізми реалізації державної політики у сфері кіберзахисту, визначивши ключові принципи – координацію, публічно-приватне партнерство, технологічну адаптивність та гармонізацію з європейськими стандартами, зокрема Директивою (ЄС) 2022/2555 (NIS 2) [78]. Важливим здобутком цього документа стало створення інституційного підґрунтя для діяльності Національного координаційного центру кібербезпеки при РНБО, який забезпечує міжвідомчу взаємодію та стратегічне управління ризиками.

Постанови Кабінету Міністрів України виконують нормативно-організаційну функцію, конкретизуючи механізми реалізації положень законів і указів Президента. Наприклад, Постанова КМУ № 518 від 19 червня 2019 р. [93] затвердила Положення про єдину державну систему кіберзахисту, визначивши структуру, принципи та порядок взаємодії суб’єктів, а також створивши основу для функціонування CERT-UA як урядового центру реагування на інциденти.

У постанові № 943 від 09 жовтня 2020 р. [94] закріплено процедуру категоризації об’єктів критичної інформаційної інфраструктури, запровадивши ризик-орієнтований підхід і державний нагляд за безпекою таких об’єктів.

Накази центральних органів виконавчої влади мають переважно техніко-регламентний характер і забезпечують практичну реалізацію державної політики.

Згадані вище акти забезпечують функціональну дієвість системи правового регулювання, перетворюють норми права на конкретні адміністративні алгоритми. Підзаконні нормативно-правові акти у сфері інформаційної безпеки виконують роль практичного механізму реалізації державної політики, який поєднує законодавчу визначеність із адміністративною гнучкістю. Їх значення полягає у забезпеченні цілісності правової системи, координації між органами влади, підвищенні рівня правової визначеності й технологічної адаптивності.

Безперечно, підзаконний рівень нормативного забезпечення є функціональною ланкою між нормотворенням і правозастосуванням, що забезпечує ефективність адміністративно-правового механізму у сфері інформаційної безпеки України; формує основу для реалізації принципів превентивності, координації, публічності та наукової обґрунтованості, сприяючи підвищенню кіберстійкості держави в умовах сучасних інформаційних викликів.

Україна є також стороною низки міжнародних угод, що становлять фундамент її інформаційної політики:

– Європейська конвенція про захист прав людини і основоположних свобод (1950) – визначає стандарти свободи слова та приватності [95];
– Будапештська конвенція про кіберзлочинність (2001) – встановлює міжнародні механізми протидії кіберзлочинам [96];
– Директива (ЄС) 2022/2555 (NIS 2) – задає високий спільний рівень кібербезпеки в державах-членах ЄС, на яку орієнтується Україна[78];
– Керівні принципи ООН з інформаційної безпеки – формують універсальні стандарти поведінки держав у кіберпросторі.

Імплементація цих актів гармонізує законодавство України з європейськими підходами й забезпечує міжнародну сумісність системи кіберзахисту.

Окрему групу становлять доктрини, стратегії та концепції, що визначають політичні орієнтири держави: Стратегія національної безпеки України «Безпека людини – безпечна країна» (Указ Президента № 392/2020) [91]; Стратегія кібербезпеки України (Указ Президента № 447/2021) [92]; Стратегія розвитку інформаційного суспільства (КМУ, 2013, оновлення 2021 р.)[97]. Ці акти програмно-нормативні й виконують інтеграційну функцію – поєднують правові норми з управлінськими цілями та міжнародними зобов'язаннями України.

До найнижчого, але надзвичайно важливого рівня належать державні стандарти (ДСТУ), технічні регламенти, внутрішні політики безпеки органів влади та суб'єктів критичної інфраструктури.

Ієрархічна система нормативно-правових актів у сфері інформаційної безпеки України – багаторівнева, поліструктурна і взаємопов'язана; поєднує нормативність (через закони і підзаконні акти), міжнародну інтегрованість (через участь у глобальних і європейських ініціативах) і технологічну адаптивність (через стандартизацію й цифрові механізми реалізації).

Попри сформований і активний розвиток нормативної бази, правове поле інформаційної безпеки України характеризується відсутністю внутрішньої узгодженості, що проявляється на рівні термінології, компетенцій, процедур і співвідношення між актами різної юридичної сили. Це створює перешкоди для стабільного правозастосування та ефективної реалізації державної політики.

У процесі аналізу чинної нормативно-правової бази у сфері забезпечення інформаційної безпеки України виявлено термінологічні неузгодження, які істотно впливають на цілісність правового регулювання, ускладнюють правозастосування та створюють передумови для дублювання компетенцій між органами публічної влади. Відсутність єдиної системи термінів у нормативно-

правових актах різного рівня негативно позначається на якості реалізації державної політики у сфері кібер- та інформаційної безпеки, оскільки породжує множинність тлумачень ключових понять.

Передусім відсутність єдиного визначення поняття «інформаційна безпека». У різних джерелах термін трактується неоднозначно. Так, відповідно до Закону України «Про національну безпеку України» [23] інформаційна безпека визначається як стан захищеності життєво важливих інтересів людини, суспільства і держави від реальних та потенційних загроз в інформаційній сфері. Натомість Закон України «Про інформацію» [76] фактично ототожнює її із захистом права на інформацію, що звужує її зміст до гарантій реалізації конституційних прав громадян.

У результаті сформувалося різнорівневе тлумачення цього поняття:

– у конституційно-правовому аспекті – як складника національної безпеки;
– у галузевому (інформаційному) праві – як техніко-правової категорії, спрямованої на захист даних і інформаційних ресурсів.

Такий дуалізм змісту ускладнює формування єдиної концепції інформаційної безпеки та вимагає розроблення узагальненого доктринального визначення, що інтегрувало б обидва підходи.

Також спостерігається невизначеність співвідношення між поняттями «кібербезпека» та «інформаційна безпека».

Закон України «Про основні засади забезпечення кібербезпеки України» [47] виділяє кібербезпеку як окремий напрям національної безпеки, визначаючи її метою забезпечення стійкості кіберпростору. Проте більшість підзаконних актів (зокрема, Постанова КМУ № 518 від 19.06.2019 р. «Про затвердження Положення про єдину державну систему кіберзахисту» використовують термін «захист інформації» без чіткої кореляції з кіберкомпонентом.
У результаті формується термінологічний дуалізм, за якого «інформаційна безпека» має ширше соціально-правове значення, тоді як «кібербезпека»

обмежується технічною сферою захисту електронних систем і мереж. Такий підхід призводить до дублювання норм, складності імплементації міжнародних стандартів та фрагментації політики у сфері цифрової безпеки**.**

Окрім того, трапляється непослідовне вживання понять «технічний захист інформації» і «кіберзахист».

У нормативних актах Державної служби спеціального зв'язку та захисту інформації «технічний захист інформації» визначено як комплекс організаційно-технічних заходів, спрямованих на запобігання несанкціонованому доступу, витоку чи спотворенню інформації. Натомість у Законі України «Про основні засади забезпечення кібербезпеки України» цей термін узагалі не застосовується, що зумовлює розрив між техніко-організаційним змістом відповідної діяльності та її нормативно-правовим відображенням.

У практиці державних установ це спричиняє неоднакові критерії аудиту: об'єкти, що підпадають під дію системи технічного захисту інформації, не завжди включаються до переліку критичної інформаційної інфраструктури, хоча рівень ризику їх функціонування є ідентичним. Така непослідовність ускладнює формування єдиної методики оцінки ризиків і сертифікації систем безпеки.

Можна зазначити, що термінологічні неузгодження у сфері інформаційної та кібербезпеки є системними й потребують нормативного та науково-доктринального узгодження.

Для подолання виявлених колізій доцільно:

- розробити єдиний глосарій термінів у сфері інформаційної безпеки на рівні підзаконного акту (наприклад, постанови КМУ або відомчого стандарту);
- уніфікувати визначення понять «інформаційна безпека», «кібербезпека», «технічний захист інформації» в межах Національної стратегії кібербезпеки;

– забезпечити гармонізацію української термінології з європейськими підходами.

Усунення термінологічних неузгоджень сприятиме формуванню цілісної системи адміністративно-правового регулювання інформаційної безпеки, підвищить ефективність управлінських рішень і забезпечить сумісність національного законодавства з європейськими стандартами цифрової стійкості.

Після виявлення термінологічних неузгоджень у нормативно-правовому полі інформаційної безпеки доцільно перейти до аналізу інституційних диспропорцій у системі державного управління, які становлять не менш суттєву проблему ефективності реалізації державної політики у цій сфері. Інституційна фрагментованість, дублювання функцій і нечітке розмежування повноважень між основними суб'єктами безпекового сектору знижують рівень керованості, створюють правову невизначеність і послаблюють здатність держави оперативно реагувати на інформаційні та кіберзагрози.

Перетин повноважень між Службою безпеки України та Державною службою спеціального зв'язку та захисту інформації. Відповідно до Закону України «Про Службу безпеки України» [98], на СБУ покладено функції контррозвідувального захисту інтересів держави в інформаційній сфері, що охоплює виявлення, запобігання та припинення деструктивних інформаційних впливів, а також забезпечення захисту державних інформаційних ресурсів.

Водночас Закон України «Про основні засади забезпечення кібербезпеки України» [47] визначає ДССЗЗІ координатором у сфері кіберзахисту державних інформаційних ресурсів, покладаючи на неї функції технічного регулювання, сертифікації засобів захисту, організації криптографічного контролю та адміністрування державних реєстрів у цій сфері.

На практиці це спричиняє перетин компетенцій: обидва органи здійснюють аудит об'єктів критичної інформаційної інфраструктури, розробляють власні нормативно-методичні документи, іноді з різними вимогами до процедур

безпеки. Відсутність єдиної підзвітності та координаційного центру створює ситуацію паралельного управління, що суперечить принципу субординації, закріпленому в адміністративному праві.

На нашу думку, доцільним є чітке розмежування компетенцій: СБУ має зосередитися на контррозвідувальних і кримінально-процесуальних функціях, тоді як ДССЗЗІ – на нормативно-технічному регулюванні, стандартизації та сертифікації засобів захисту. Запровадження спільного міжвідомчого регламенту могло б усунути дублювання і забезпечити єдність управлінської вертикалі.

Також спостерігається неврегульований розподіл функцій між Міністерством цифрової трансформації України та Радою національної безпеки і оборони України (РНБО).

Згідно з Положенням про Міністерство цифрової трансформації України (затвердженим постановою КМУ № 856 від 18.09.2019 р.) [99], Мінцифра є центральним органом виконавчої влади, що формує державну політику у сфері цифрової трансформації та кібербезпеки. РНБО виступає як координуючий орган у сфері національної безпеки, включно з інформаційною та кібербезпекою.

Унаслідок цього спостерігається функціональне перетинання компетенцій: РНБО визначає стратегічні напрями та ухвалює рішення на рівні політики, тоді як Мінцифра реалізує їх у практичній площині, однак без чіткої підпорядкованості. Відсутність єдиної вертикалі між стратегічним плануванням і виконавчою реалізацією призводить до фрагментації управління та дублювання програмних документів.

З огляду на це доцільно розробити модель інтегрованого управління, у межах якої РНБО здійснює загальну координацію, а Мінцифра – операційну імплементацію рішень із чітким процедурним зворотним зв’язком.

Також потрібно зазначити недостатнє нормативне визначення ролі органів місцевого самоврядування у сфері інформаційної безпеки. Ні Закон України «Про інформацію» [76], ні Закон «Про основні засади забезпечення кібербезпеки

України» [47], не встановлюють конкретних повноважень місцевих органів влади у сфері інформаційної безпеки. Водночас саме на місцевому рівні зосереджені об’єкти критичної інфраструктури (енергетика, транспорт, водопостачання, комунальні мережі), що підвищує ризик локальних кіберінцидентів.

Відсутність нормативно визначених процедур взаємодії з державними структурами фактично формує *вакуум управління ризиками* на муніципальному рівні. У таких умовах органи місцевого самоврядування позбавлені чітких алгоритмів реагування, не мають доступу до оперативної інформації щодо кіберінцидентів, а їхні дії у кризових ситуаціях нерідко носять фрагментарний або ситуативний характер. Особливо це проявляється під час масштабних інформаційних атак, техногенних інцидентів чи деструктивних інформаційних кампаній, коли відсутність швидкого каналу комунікації з національними суб’єктами безпеки фактично унеможливлює своєчасну локалізацію загроз та мінімізує ефективність превентивних заходів.

Такий стан справ засвідчує нагальну потребу в інституційному посиленні горизонтальної й вертикальної взаємодії. Одним із перспективних напрямів є створення регіональних центрів кіберзахисту, інтегрованих у національну систему реагування та взаємодіючих з НКЦК при РНБО, ДССЗЗІ, СБУ та Мінцифрою. Такі центри можуть виконувати функції локального моніторингу, первинної аналітики, інцидент-респондентства, а також навчально-методичної підтримки для органів місцевого самоврядування.

Узагальнюючи, можна стверджувати, що інституційна складова державного управління у сфері інформаційної безпеки потребує суттєвої оптимізації та централізації координаційних механізмів. Необхідним є впровадження чіткої системи розмежування повноважень між СБУ, ДССЗЗІ, Мінцифрою та РНБО України, побудованої на принципах субординації, відповідальності та функціональної узгодженості. Це забезпечить підвищення ефективності реалізації державної політики, своєчасність реагування на

інформаційні та кіберзагрози, а також посилить інституційну стійкість національної системи інформаційної безпеки.

Після окреслення інституційних розбіжностей у системі державного управління логічним є перехід до аналізу процедурно-нормативного рівня забезпечення інформаційної безпеки. Саме він демонструє не лише фрагментарність чинного законодавства, а й відсутність уніфікованих алгоритмів практичної реалізації інформаційно-безпекової політики. Процедурна неврегульованість створює додаткові управлінські колізії, оскільки закони містять переважно декларативні норми, тоді як конкретні механізми їх застосування розпорошені між численними підзаконними актами, що ускладнює реалізацію принципу правової визначеності та знижує ефективність державного управління в інформаційній сфері.

По-перше, існують колізії у сфері захисту персональних даних. Закон України «Про захист персональних даних» [77] закріплює дозвільний принцип – обробка персональних даних можлива лише за згодою суб'єкта або на підставах, визначених законом. Водночас стаття 29 Закону «Про інформацію» [76] дозволяє поширення відомостей про службових осіб без їхньої згоди, якщо така інформація пов'язана з виконанням публічних функцій. Це породжує правову колізію між правом на приватність і правом на доступ до інформації. Відсутність у національному праві чіткої процедури оцінки пропорційності втручання, яка закріплена у General Data Protection Regulation (ЄС) 2016/679 (GDPR) [100] , створює ризик вибіркового тлумачення та зловживань.

По-друге, ієрархічна невпорядкованість між актами різної юридичної сили. Укази Президента України № 47/2017 «Про Доктрину інформаційної безпеки України» [90], № 392/2020 «Про Стратегію національної безпеки України» [91], та № 447/2021 «Про Стратегію кібербезпеки України» [92] фактично містять норми прямої дії, що виходять за межі делегованих законом повноважень виконавчої влади. Зокрема, передбачено створення нових інституцій і визначення

термінів, не закріплених у законодавстві. Подібна практика суперечить статті 19 Конституції України, згідно з якою державні органи мають діяти лише на підставі та в межах закону, що призводить до зміщення нормативної ієрархії.

Окрім того, бракує механізму узгодження між секторальними актами. Закони, що регулюють інформаційно-комунікаційний простір («Про електронні комунікації», «Про медіа», «Про основні засади забезпечення кібербезпеки»), функціонують автономно, без системного «зшивання» норм, що спричиняє секторальну фрагментацію, коли суб'єкти господарювання підпадають під різні правові режими контролю без єдиних стандартів безпеки та відповідальності.

Сукупність окреслених неузгодженостей має комплексний функціональний ефект, що проявляється у ускладненні правозастосування, подвійному підпорядкуванні суб'єктів, низькій ефективності міжвідомчого моніторингу та недостатній гармонізації з правом ЄС.

Виявлені процедурно-нормативні колізії підтверджують системний характер проблеми, що охоплює термінологічний, інституційний, процедурний і ієрархічний рівні правового регулювання. Для забезпечення узгодженості нормативного поля та підвищення ефективності державної політики у сфері інформаційної безпеки необхідним є впровадження комплексу заходів:

– кодифікації (створення базового закону «Про інформаційну безпеку»);
– гармонізації з європейським правом (NIS 2, GDPR, Cybersecurity Act);
– інституційної консолідації (створення єдиного координуючого органу при РНБО);
– стандартизації процедур;
– формування єдиного державного реєстру кіберінцидентів.

Важливість прийняття Закону України «Про інформаційну безпеку» випливає з виявленої у дослідженні структурної фрагментарності й внутрішньої неузгодженості чинного нормативно-правового поля. Сьогодні регулювання інформаційної та кібербезпеки «розкидане» між низкою конституційних норм,

базових і спеціальних законів, підзаконних актів, доктрин і стратегій, які часто використовують різні, а іноді й взаємно суперечливі дефініції («інформаційна безпека», «кібербезпека», «технічний захист інформації», «кіберзахист»), допускають перетин компетенцій між СБУ, ДССЗЗІ, Мінцифрою, РНБО та фактично залишають поза належним регулюванням роль органів місцевого самоврядування. Відсутність єдиного системоутворювального акта унеможливлює формування узгодженого понятійно-категоріального апарату, ускладнює правозастосування, створює ризики дублювання або прогалин повноважень і послаблює спроможність держави своєчасно реагувати на інформаційні та кіберзагрози в умовах гібридної війни й цифрової трансформації.

Закон «Про інформаційну безпеку» має виконувати функцію базового нормативного каркаса для всієї системи адміністративно-правового регулювання у цій сфері. Його ключові завдання полягають у закріпленні єдиного, людиноцентричного й комплексного визначення інформаційної безпеки, узгодженого з категоріями національної, кібер- та гуманітарної безпеки; уніфікації термінології та співвідношення основних понять, усуненні наявних термінологічних розбіжностей; визначенні чіткої структури повноважень і відповідальності суб'єктів публічної влади й запровадженні ефективної координаційної моделі; кодифікації принципів, стандартів і процедур забезпечення інформаційної безпеки, зокрема щодо захисту персональних даних, реагування на кіберінциденти, категоризації критичної інфраструктури та ведення реєстру кіберінцидентів; забезпеченні системної гармонізації з правом ЄС (GDPR, NIS 2, CER тощо) та формуванні внутрішньо узгодженої імплементаційної моделі.

Отже, ухвалення Закону України «Про інформаційну безпеку» є не лише техніко-юридичною потребою «наведення ладу» в окремій галузі, а й ключовою умовою формування стійкої, передбачуваної та людиноцентричної моделі

національної безпеки в публічно-інформаційній сфері, здатної забезпечити баланс між правами людини, інтересами держави та викликами цифрової епохи.

Реалізація цих напрямів сприятиме формуванню уніфікованої, передбачуваної та ефективної системи правового регулювання інформаційної безпеки, здатної забезпечити інтеграцію України до європейського цифрового простору та належний рівень технологічної стійкості.

ВИСНОВКИ ДО РОЗДІЛУ 1

У першому розділі дисертації зосереджено увагу на теоретико-правових засадах забезпечення національної безпеки у публічно-інформаційній сфері: окреслено понятійно-категоріальний апарат, визначено структуру та принципи адміністративно-правового регулювання, комплексний аналіз багаторівневої нормативної бази з урахуванням європейських стандартів, актуальної судової практики та виявлених колізій у чинному законодавстві.

1. У результаті проведеного аналізу встановлено, що національна безпека в комунікаційному вимірі є динамічною системою взаємодії держави, суспільства й громадянина, спрямованою на забезпечення стабільності, довіри та захищеності публічно-інформаційного простору. Її сутність полягає у поєднанні політичних, правових, соціальних, економічних та інформаційно-комунікаційних складників, що визначає міждисциплінарність досліджуваного феномена.

2. Обґрунтовано гуманітарно-правову природу інформаційної безпеки, яка розглядається не лише як технічна або організаційна категорія, а насамперед як правова умова реалізації прав людини, збереження суспільної довіри до держави та забезпечення стійкості демократичного комунікаційного середовища.

3. Доведено, що еволюція поняття національної безпеки – від античної ідеї *bonum commune* до сучасної концепції «людської безпеки» – засвідчує зміщення акцентів із пріоритетності державних інтересів на визнання людини центральним суб’єктом безпекових відносин.

4. Установлено, що публічно-інформаційна сфера є ключовим сегментом системи національної безпеки, у межах якого формуються довіра до влади, легітимність політичних рішень та стабільність демократичного ладу. Водночас її відкритий характер, незважаючи на важливість для демократичного розвитку, породжує загрози дезінформації, маніпуляцій, кібератак і гібридних впливів, що потребує комплексного нормативно-правового реагування.

5. Сформульовано авторське визначення публічно-інформаційної безпеки як стану захищеності інформаційного простору держави, суб'єктів публічного управління та громадян від інформаційних і комунікаційних загроз, який забезпечує стабільність функціонування публічних інститутів, реалізацію права людини на достовірну інформацію та підтримання довіри до держави.

6. Підкреслено, що публічно-інформаційна безпека виконує роль індикатора ефективності державного управління, оскільки її забезпечення потребує збалансування між принципами відкритості та вимогами захисту стратегічних національних інтересів. Також вона є складником і критерієм демократичної зрілості суспільства.

7. Визначено, що адміністративно-правове регулювання інформаційної безпеки становить комплексну діяльність публічної адміністрації, спрямовану на забезпечення стабільності функціонування інформаційного простору держави, захист прав громадян та реалізацію державної політики у сфері національної безпеки. З'ясовано, що воно інтегрує нормотворчу, організаційно-управлінську та контрольну складові, забезпечуючи взаємодію суб'єктів публічного управління, громадянського суспільства й приватного сектора.

8. Засвідчено, що адміністративно-правове регулювання інформаційної безпеки має трирівневу будову – нормативно-правову, інституційну та організаційно-функціональну. Саме їх узгоджена взаємодія гарантує цілісність і результативність державної політики у сфері інформаційної безпеки. Підкреслено, що ефективність системи визначається не кількістю нормативних

актів, а наявністю чітких процедур, механізмів координації та принципів належного публічного адміністрування.

9. Розкрито положення про класифікацію принципів адміністративно-правового регулювання інформаційної безпеки за чотирма критеріями: сферою дії, функціональним призначенням, змістовно-ціннісною орієнтацією та джерелом нормативного закріплення. Розвинено зміст спеціальних принципів – балансу свободи інформації та її захисту, технологічної адаптивності, наукової обґрунтованості, системності та міжнародної інтегрованості, що забезпечують узгодженість національного законодавства зі світовими стандартами.

10. Аргументовано, що ефективне адміністративно-правове регулювання інформаційної безпеки можливе за умови поєднання правових, організаційних і технологічних механізмів, побудованих на засадах верховенства права, законності, пропорційності та публічності. Застосування системного підходу дозволяє розглядати інформаційну безпеку як інтегральну частину національної безпеки, що забезпечує баланс між державними інтересами, правами людини й міжнародними зобов’язаннями України.

11. Визначено складність багаторівневої структури нормативно-правової системи забезпечення інформаційної безпеки України, що охоплює конституційний, законодавчий, підзаконний і міжнародно-доктринальний рівні. Така ієрархічна модель створює основу для формування збалансованої державної політики у сфері інформаційного та кіберзахисту, забезпечуючи поєднання стратегічних принципів, закріплених у Конституції, з конкретними механізмами їх реалізації в галузевих і технічних актах. Уперше системно узагальнено взаємозв’язок між цими рівнями, що дозволило виокремити ключові закономірності розвитку інформаційного законодавства в Україні.

12. Доведено, що конституційні норми формують методологічну й ціннісну основу національної інформаційної політики, закріплюючи принципи верховенства права, пропорційності, свободи інформації та недоторканності

приватного життя. Саме Конституція задає баланс між свободою вираження поглядів і безпековими обмеженнями, що відповідає практиці Європейського суду з прав людини та загальновизнаним європейським стандартам.

13. Удосконалено підхід до систематизації законодавчого рівня: виокремлено його ядро, яке становлять закони «Про національну безпеку України», «Про інформацію», «Про основні засади забезпечення кібербезпеки України», «Про захист персональних даних», «Про електронні комунікації» та «Про критичну інфраструктуру». Сукупно вони формують концептуальний і правовий каркас національної інформаційної безпеки, у межах якого гармонізовано інтереси держави, суспільства та особи. Показано, що зазначені акти забезпечують реалізацію комплексного підходу – від гарантій свободи інформації до превентивного захисту інформаційного простору від кіберзагроз.

14. Обґрунтовано, що сучасна нормативна база зберігає ознаки термінологічної та інституційної фрагментарності. У різних актах паралельно вживаються поняття «інформаційна безпека», «кібербезпека», «технічний захист інформації», що призводить до неоднозначного тлумачення компетенцій державних органів і дублювання функцій. Для усунення цих неузгодженостей доцільно запровадити єдиний державний глосарій термінів і кодифікувати галузеве законодавство у формі базового закону «Про інформаційну безпеку».

РОЗДІЛ 2
АДМІНІСТРАТИВНО-ПРАВОВІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ У ПУБЛІЧНО-ІНФОРМАЦІЙНІЙ СФЕРІ

2.1. Діяльність органів публічної влади щодо забезпечення національної безпеки у публічно-інформаційній сфері

Основним елементом у системі реалізації державної політики у сфері національної безпеки України є суб'єкти публічної влади, до складу яких входять як державні, так і недержавні інституції, уповноважені забезпечувати виконання завдань у безпековій сфері, оскільки вони формують цілісну організаційно-правову систему, спрямовану на гарантування захисту національних інтересів, стабільності конституційного ладу, суверенітету та територіальної цілісності держави, на забезпечення ефективного функціонування публічно-інформаційного простору в умовах зростання кібер- та інформаційних загроз.

Передусім доцільно звернути увагу на термінологічну складову досліджуваної проблематики, зокрема на категорію «суб'єкти публічної влади». У сучасній юридичній науці цей термін використовується для позначення сукупності органів та інституцій, уповноважених від імені держави або територіальної громади здійснювати владні повноваження у публічних інтересах.

Аналіз сучасних наукових підходів до визначення сутності публічної влади засвідчує важливість позиції І. Глобенка, який справедливо наголошує, що система публічної влади України складається з державної влади та органів місцевої публічної влади. Науковець трактує місцеву владу як «вид публічної влади, яка реалізується від імені суб'єктів, що функціонують у межах певних адміністративно-територіальних одиниць, а також здатність її носіїв упорядковувати поведінку мешканців цих одиниць і впливати на розвиток місцевого життя» [101, с. 83]. Такий підхід підкреслює подвійну природу

публічної влади, що поєднує централізовані державні та децентралізовані місцеві механізми управління.

Водночас І. Глобенко слушно зауважує, що публічна влада, втілена у формах державної та місцевої, здійснюється через єдину систему органів публічної влади, яка включає державні інституції всіх гілок влади – законодавчу, виконавчу та судову – а також органи місцевого самоврядування [101, с. 83], що дає підстави розглядати публічну владу як інтегровану інституційно-правову систему, зорієнтовану на реалізацію публічного інтересу й забезпечення суспільного блага.

Для доповнення цієї позиції Д. Волох пропонує розгорнуте визначення суб'єкта публічного права, під яким розуміє органи, установи, організації або інші юридично оформлені утворення, створені з метою реалізації публічного інтересу, виконання завдань публічного управління та забезпечення загального блага. Вони наділені публічною правосуб'єктністю і функціонують у межах повноважень, визначених чинним законодавством [102, с. 194]. Такий підхід акцентує на нормативній легітимності діяльності суб'єктів публічної влади та підкреслює, що їхня компетенція обмежується виключно публічно-правовими завданнями, спрямованими на захист прав і свобод громадян.

Узагальнення наведених наукових поглядів дає підстави стверджувати, що суб'єкти публічної влади становлять юридично організовану систему державних і самоврядних інституцій, наділених владними повноваженнями для реалізації публічних інтересів, підтримання правопорядку та забезпечення ефективного управління у межах правового поля держави. Суб'єкти публічної влади становлять основу механізму реалізації державної політики в усіх сферах суспільного життя, зокрема й у сфері національної безпеки.

Законодавче визначення суб'єктів, що забезпечують національну безпеку України, пройшло тривалий шлях еволюції. У Законі України «Про основи національної безпеки України» від 19 червня 2003 р. № 964-IV (втратив чинність)

було закладено широкий суб'єктний склад, який охоплював практично всі гілки влади та інститути громадянського суспільства. До нього належали: Верховна Рада України, Президент, Кабінет Міністрів, Рада національної безпеки і оборони, міністерства та інші центральні органи виконавчої влади, Національний банк, суди, прокуратура, антикорупційні органи, місцеві державні адміністрації, органи місцевого самоврядування, Збройні Сили України, Служба безпеки України, прикордонна та розвідувальні служби, інші військові формування, органи цивільного захисту, громадяни та об'єднання громадян [102]. Така модель мала інклюзивний характер і відображала уявлення про багаторівневу, публічно-суспільну природу безпеки, у межах якої державні, військові й громадські структури спільно виконують захисну функцію.

Ухвалення Закону України «Про національну безпеку України» від 21 червня 2018 р. № 2469-VIII суттєво змінило архітектоніку правового регулювання. У ньому запроваджено системне поняття «сектор безпеки і оборони», який, відповідно до ст. 12, об'єднує органи державної влади, Збройні Сили, розвідувальні та правоохоронні структури, оборонно-промисловий комплекс, сили цивільного захисту, а також громадські об'єднання й громадян, що добровільно беруть участь у забезпеченні безпеки [23]. У цій нормі виокремлено чотири взаємопов'язані складникиі:

- сили безпеки – розвідувальні, правоохоронні, спеціальні органи та сили цивільного захисту;
- сили оборони – Збройні Сили України й інші військові формування;
- оборонно-промисловий комплекс;
- громадські об'єднання та громадяни, які добровільно беруть участь у забезпеченні національної безпеки.

При цьому ч. 2 ст. 12 Закону конкретизує коло основних суб'єктів сектору безпеки і оборони, до яких віднесено Міністерство оборони, Міністерство внутрішніх справ, Національну гвардію, Національну поліцію, Службу безпеки

України, Державну прикордонну службу, Державну службу спеціального зв'язку та захисту інформації, апарат РНБО, розвідувальні органи, а також інші спеціалізовані структури [23].

Наукове осмислення цих змін дає О. Нестеренко, який зазначає, що порівняно з попередньою редакцією Закону суб'єктний склад став більш системним, однак він залишається неповним. Зокрема, у чинному законі поза межами сектору безпеки фактично залишено керівні суб'єкти – Президента України, Верховну Раду, Кабінет Міністрів, судові органи, народ України та інститути громадянського суспільства, хоча їхня роль у системі гарантування безпеки є фундаментальною. Учений вважає некоректним те, що керівництво у сферах національної безпеки і оборони (ст. 13 Закону) розглядається окремо від самого сектору безпеки. У зв'язку з цим він пропонує внести зміни до ч. 1 ст. 12 Закону, доповнивши чотири існуючі складові п'ятою – «керівництво у сферах національної безпеки й оборони», а наприкінці ч. 2 цієї статті додати фразу «та інші уповноважені органи» [104, с. 34].

На нашу думку, пропозиція О. Нестеренка є цілком обґрунтованою та відповідає логіці системного підходу до публічного управління. Вона дозволила б усунути інституційну асиметрію між політичними суб'єктами керівництва та виконавчими структурами сектора безпеки, підвищити прозорість і підзвітність механізмів ухвалення стратегічних рішень [104, с. 34].

Водночас, пропонуємо розширити концепцію в напрямі функціонального розмежування суб'єктів на три взаємопов'язані рівні:

– стратегічно-керівний (Президент України, Верховна Рада України, РНБО, Кабінет Міністрів України) – формує політику та визначає пріоритети національної безпеки;
– операційно-виконавчий (сили безпеки, оборони, правоохоронні органи, розвідувальні служби) – реалізує рішення та здійснює реагування на загрози;

– суспільно-громадський (інститути громадянського суспільства, ЗМІ, експертні спільноти, волонтерські організації) – забезпечує демократичний контроль, аналітичну підтримку та комунікацію між державою і громадянами.

Удосконалення законодавства у цьому напрямі сприятиме побудові інтегрованої системи національної безпеки, у якій чітко визначено повноваження, підзвітність і взаємодію всіх учасників безпекового процесу, що, у свою чергу, відповідає європейським принципам democratic security governance та вимогам ефективного публічного адміністрування.

Визначення загальної структури суб'єктів, що забезпечують національну безпеку, дає підстави перейти до аналізу специфіки діяльності органів публічної влади в публічно-інформаційній сфері, яка сьогодні є одним із ключових напрямів державної політики безпеки та складником національної стійкості.

У наукових дослідженнях О. Олійника слушно запропоновано багаторівневу модель організаційно-функціональної системи забезпечення інформаційної безпеки держави, що дозволяє комплексно осмислити як вертикаль управління, так і горизонталь взаємодії між суб'єктами різного правового статусу [105, с. 219–220; 106]. Учений виокремлює чотири взаємопов'язані рівні, кожен із яких виконує специфічні завдання у структурі національної безпеки.

Перший рівень – стратегічний (загальнодержавний) – охоплює ключові центри прийняття рішень: Верховну Раду України, Президента України, Кабінет Міністрів України. Його зміст полягає у формуванні політико-правових орієнтирів, ухваленні законодавчих актів, визначенні засад міжнародного співробітництва у сфері інформаційної безпеки. Саме цей рівень забезпечує цілісність державної політики, нормативну узгодженість і міжнародну легітимність безпекових рішень.

Другий рівень – організаційно-виконавчий (відомчо-територіальний) – реалізується через центральні органи виконавчої влади, правоохоронні органи, суди та органи місцевого самоврядування. Він має прикладний характер, адже спрямований на практичне впровадження політики, визначеної на стратегічному рівні. На цьому рівні відбувається координація, методичне забезпечення, контроль та нагляд у межах галузевої компетенції суб'єктів публічної влади.

Третій рівень становлять об'єкти критичної інформаційної інфраструктури – підприємства, установи, організації, телекомунікаційні мережі та інформаційні ресурси, управління якими здійснюється з використанням електронно-комунікаційних технологій. До цієї групи належать секторні системи енергетики, транспорту, фінансів, охорони здоров'я, цифрових державних послуг та зв'язку. Від стабільності й захищеності їхнього функціонування залежить безперервність роботи державних інститутів, стійкість економіки, безпека суспільних комунікацій і загальна кіберстійкість держави, що зумовлює підвищених вимог до адміністрування, моніторингу та реагування на інциденти у цих системах.

Четвертий рівень – суспільно-громадський – представлений громадянами, громадськими об'єднаннями, засобами масової інформації та аналітичними центрами. Саме цей рівень втілює принцип демократичного цивільного контролю, сприяє підвищенню інформаційної культури, протидії дезінформації та поширенню правової свідомості у сфері безпеки.

Варто погодитися з автором, що центральна роль у системі адміністративно-правового забезпечення інформаційної безпеки належить державним органам, проте, згідно з положеннями Закону України «Про національну безпеку України» від 21.06.2018 р. № 2469-VIII [23] та Стратегії інформаційної безпеки України (Указ Президента № 685/2021) [107], ключовим чинником результативності стає інтеграція державних і недержавних акторів у єдину систему реагування. З огляду на це модель інформаційної безпеки стає багаторівневою, міжсекторальною і мультидисциплінарною.

Як слушно зазначає В. Стебловський, система забезпечення інформаційної безпеки не обмежується державними органами: вона включає також органи місцевого самоврядування, інститути громадянського суспільства та окремих громадян, які реалізують інформаційно-безпекові функції у межах власних повноважень [106], тому модель має не лише вертикальний, а й горизонтальний вимір, тобто функціонує як система взаємодії держави, суспільства і бізнесу.

У своїй розвідці дослідник пропонує класифікацію суб'єктів побудови безпекового середовища в інформаційній сфері, що враховує характер публічної влади та сферу охоплення інформаційного простору. Зокрема, науковець пропонує розглядати такі групи суб'єктів:

1. За критерієм належності до публічної влади: державні органи та органи місцевого самоврядування; суб'єкти громадянського суспільства.

2. За масштабом охоплення інформаційної сфери: державні органи – Президент України, Верховна Рада України, Кабінет Міністрів України, інші центральні органи виконавчої влади, органи сектору безпеки та оборони; органи місцевого самоврядування, що здійснюють управління інформаційними ресурсами на регіональному рівні; громадські об'єднання, наукові установи, освітні заклади, засоби масової інформації; підприємства, установи та організації різних форм власності, діяльність яких пов'язана з інформаційною сферою [106].

На нашу думку, ця класифікація є методологічно виправданою, адже вона поєднує інституційний (владний) і функціональний (суспільний) аспекти безпеки. Водночас вважаємо доцільним доповнити її третім критерієм – рівнем управлінської компетенції, що дозволить розмежувати:

- суб'єктів стратегічного управління (Президент України, РНБО, Верховна Рада, Кабінет Міністрів);
- суб'єктів виконавчо-операційного рівня (центральні та місцеві органи влади, правоохоронні структури, ДССЗЗІ, Мінцифра, СБУ);

– суб’єктів суспільно-громадського впливу (громадські організації, медіа, освітні й аналітичні інституції).

Запропонована трирівнева типологія дозволяє чіткіше визначити сфери відповідальності, повноваження та канали взаємодії суб’єктів інформаційної безпеки в межах адміністративно-правової системи.

Її практичне впровадження може стати основою для розроблення Концепції єдиної системи управління інформаційною безпекою, що забезпечить узгодженість дій між державними, муніципальними та громадськими структурами у сфері захисту інформаційного простору України.

У системі забезпечення національної безпеки в публічно-інформаційній сфері провідну роль відіграють органи публічної влади, компетенція яких визначається Конституцією України, Законом України «Про національну безпеку України» (2018) та низкою спеціальних нормативно-правових актів. Їх діяльність формує багаторівневу архітектуру управління – від стратегічного визначення пріоритетів до практичного реагування на інформаційні загрози.

Президент України виступає гарантом державного суверенітету, територіальної цілісності та, відповідно, інформаційного суверенітету держави. До його конституційних повноважень належать визначення стратегічних пріоритетів у сфері інформаційної та кібербезпеки, затвердження відповідних стратегій і рішень Ради національної безпеки і оборони (зокрема, Стратегії інформаційної безпеки України 2021 року). У разі виникнення інформаційних або кібернетичних загроз Президент забезпечує координацію діяльності силових структур і може запроваджувати правові режими надзвичайного чи воєнного стану, враховуючи інформаційний аспект безпеки.

Рада національної безпеки і оборони України (РНБО) виконує функції центрального координаційного органу з питань національної безпеки, у тому числі – в інформаційній сфері. РНБО узгоджує дії суб’єктів сектору безпеки, здійснює моніторинг стану національного інформаційного простору, ініціює

заходи реагування на кібератаки, інформаційні операції та пропагандистські кампанії. Важливим аспектом її діяльності є розроблення пропозицій Президентові щодо вдосконалення політики інформаційної безпеки та визначення напрямів міжвідомчої взаємодії.

Верховна Рада України реалізує законодавчу та контрольну функції у сфері інформаційної безпеки. Вона приймає нормативно-правові акти, що визначають засади інформаційного суверенітету, ратифікує міжнародні договори (зокрема, Будапештську конвенцію про кіберзлочинність), проводить парламентські слухання з питань інформаційної політики та контролює виконання урядових програм у цій сфері. Така діяльність парламенту сприяє гармонізації українського законодавства з європейськими нормами й посиленню демократичного цивільного контролю над сектором безпеки.

Кабінет Міністрів України виступає центральною ланкою у реалізації державної політики інформаційної та кібербезпеки. Він координує діяльність центральних органів виконавчої влади – зокрема, Міністерства цифрової трансформації, Міністерства культури та інформаційної політики, Державної служби спеціального зв'язку та захисту інформації України (ДССЗЗІ) – а також забезпечує виконання міжнародних зобов'язань держави у сфері захисту інформації. Саме урядова вертикаль забезпечує операційну стійкість інформаційного простору, перетворюючи стратегічні рішення Президента й РНБО на конкретні управлінські механізми.

З огляду на викладене, чинна компетенційна модель органів публічної влади у сфері інформаційної безпеки потребує оптимізації у двох напрямах:

1. Посилення міжвідомчої координації між Президентом, РНБО, Кабінетом Міністрів та профільними міністерствами шляхом нормативного закріплення чіткої вертикалі взаємодії й уникнення дублювання повноважень.

2. Інституційне оформлення спільної відповідальності органів публічної влади, приватного сектору та громадянського суспільства у забезпеченні безпеки

публічно-інформаційного простору – відповідно до принципів good governance та концепції whole-of-society security approach, що передбачає участь усіх соціальних суб'єктів у захисті національного інформаційного середовища.

У системі публічної влади України виконавча гілка влади посідає провідне місце у практичній реалізації політики національної безпеки в інформаційній сфері. На відміну від законодавчої та судової гілок, які формують нормативно-правову основу, встановлюють правила регулювання та гарантують верховенство права, виконавчі органи забезпечують щоденне функціонування механізмів державної інформаційної політики, здійснюють управлінський моніторинг, координацію суб'єктів безпеки та оперативне реагування на інформаційні й кібернетичні загрози.

Саме на виконавчу владу покладено завдання підтримувати операційну стійкість публічно-інформаційного простору, реалізовувати національні стратегії, забезпечувати роботу систем раннього виявлення інцидентів, організовувати міжвідомчу взаємодію та впроваджувати превентивні заходи. Її діяльність визначає здатність держави підтримувати безперервність функціонування критичної інформаційної інфраструктури та забезпечувати захист суспільних комунікацій в умовах зростання гібридних ризиків.

Ключовими суб'єктами у цій сфері виступають Міністерство цифрової трансформації України (Мінцифра), Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ), а також Міністерство культури та інформаційної політики України (МКІП). Вони утворюють трикомпонентну систему, у межах якої поєднуються технічний, комунікаційний та гуманітарний виміри інформаційної безпеки.

Міністерство цифрової трансформації України (Мінцифри) є центральним органом виконавчої влади, діяльність якого спрямовується і координується Кабінетом Міністрів України[108]. Мінцифри є основним 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 [108].

На відміну від класичних «силових» суб'єктів, діяльність міністерства спрямовано не лише на реагування на загрози, а й на попередження їх через створення безпечних цифрових екосистем. Основними завданнями Мінцифри є:

1) забезпечення формування та реалізації державної політики: у сферах цифровізації, цифрового розвитку, цифрової економіки, цифрових інновацій та технологій, робототехніки та роботизації, електронного урядування та електронної демократії, розвитку інформаційного суспільства; 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 електронних довірчих послуг та електронної ідентифікації й інвестицій в

ІТ-індустрію; у сфері розвитку ІТ-індустрії; у сфері розвитку та функціонування правового режиму ДіяСіті;

2) забезпечення формування та реалізації державної політики у сфері хмарних послуг [109, с. 186].

Одним із ключових досягнень державної політики цифрової трансформації є інституціоналізація принципу «security by design», що означає інтеграцію безпекових механізмів у процес проєктування, розроблення та функціонування державних електронних сервісів. Прикладом реалізації підходу є платформа «Дія», яка стала ядром цифрової екосистеми публічних послуг в Україні. Вона відповідає положенням Директиви (ЄС) 2022/2555 (NIS2), що визначає стандарти управління ризиками кібербезпеки на рівні державного управління.

Аналіз звіту про діяльність Міністерства цифрової трансформації України за 2023 р. засвідчує, що роботу органу спрямовано на системну цифровізацію всіх сфер суспільного життя, зокрема адміністративного управління, освіти, охорони здоров'я, економіки, оборони та комунікаційного простору держави. Порталом «Дія» користуються понад 20 мільйонів громадян, що підтверджує масштабність і соціальну значущість реалізованої цифрової політики.

Через портал забезпечено доступ до 115 електронних публічних послуг, і ця кількість постійно зростає. Водночас у 2023 році Мінцифрою здійснено значний нормативно-правовий супровід цифрової трансформації – підготовлено до 30 проєктів нормативно-правових актів для унормування процесів електронної ідентифікації, захисту персональних даних, кібербезпеки та надання електронних послуг у межах принципів відкритості й прозорості [109, с. 186; 110].

Діяльність Міністерства цифрової трансформації України у 2023 році засвідчила перехід від фрагментарного впровадження окремих електронних сервісів до формування цілісної моделі цифрової держави, у межах якої безпека, довіра та захист персональної інформації розглядаються як невід'ємні елементи управлінської архітектури. Такий підхід передбачає інтеграцію безпекових

механізмів у всі етапи розроблення й функціонування цифрових продуктів, удосконалення процедур управління даними, розвиток інфраструктури електронної взаємодії та забезпечення стійкості державних інформаційних систем до кіберзагроз.

Водночас нормативна база поки що не передбачає обов'язкової незалежної сертифікації державних цифрових систем на відповідність вимогам кіберстійкості, що створює вразливість для критичних даних.

На наш погляд, слід внести зміни до Закону України «Про основні засади забезпечення кібербезпеки України», передбачивши створення Національного центру аудиту кіберстійкості державних цифрових сервісів, який би функціонував при Мінцифрі з обов'язковим щорічним аудитом ключових державних інформаційних ресурсів.

Одним із провідних суб'єктів у системі публічної влади, що забезпечує реалізацію державної політики у сфері національної безпеки, є Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ). Її діяльність має виключно техніко-правовий та координаційний характер, охоплюючи формування і реалізацію державної політики у сферах криптографічного й технічного захисту інформації, кіберзахисту, функціонування урядового зв'язку, а також управління інформаційно-комунікаційними системами держави.

Згідно зі ст. 3 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» [111; 112] його основними завданнями є:

- формування державної політики у сфері криптографічного та технічного захисту інформації;
- організація захисту державних інформаційних ресурсів та інформації з обмеженим доступом;
- нормативно-правове регулювання та технічне забезпечення безпеки інформаційно-комунікаційних систем;

– участь у реалізації політики у сфері електронного документообігу та електронних довірчих послуг [112].

Відповідно до статті 14 цього ж Закону, ДССЗЗІ уповноважена здійснювати державний контроль за станом криптографічного та технічного захисту інформації, встановлювати порядок створення і використання засобів захисту, проводити сертифікацію систем, визначати криптографічні алгоритми, а також організовувати експертизу і аудит інформаційної безпеки на об’єктах критичної інфраструктури [111; 112].

Водночас аналіз практики діяльності відомства показує, що його робота залишається переважно реактивною – спрямованою на усунення наслідків інцидентів, а не на запобігання їм. Превентивні інструменти – такі як прогнозування кіберзагроз, оцінка вразливостей, формування культури кібергігієни та підготовка кадрів – не набули системного характеру. Це обмежує потенціал держави у формуванні проактивної моделі кіберзахисту, побудованої на принципах випереджувального аналізу ризиків.

Оновлене Положення про Адміністрацію ДССЗЗІ (затверджене постановою КМУ № 411 від 03.09.2014 р.) [112; 114] деталізує повноваження служби щодо участі у міжнародному співробітництві, розроблення проєктів законодавчих актів, здійснення державної експертизи засобів криптографічного захисту та погодження міждержавних передач таких засобів. Важливою новелою останніх років стало узгодження діяльності ДССЗЗІ з вимогами безпеки НАТО: служба отримала повноваження з акредитації з питань захисту інформаційно-комунікаційних систем, які обробляють інформацію з грифом обмеженого доступу, відповідно до стандартів Комітету безпеки НАТО [112; 113].

Також у науковій літературі обґрунтовується позиція, що повноваження ДССЗЗІ потребують модернізації відповідно до євроінтеграційного напряму держави. Учені наголошують на доцільності позбавлення служби невластивих функцій щодо регулювання захисту конфіденційної інформації у приватному

секторі та переходу до системи управління інформаційною безпекою (ISMS) на основі міжнародних стандартів ISO/IEC 27001 і 27032 [112; 115, с. 130–131].

Відомо, що чинна нормативна база ДССЗЗІ (зокрема, НД ТЗІ – нормативні документи системи технічного захисту інформації) формувалася ще у 1990-х рр. Часткові оновлення не повністю відповідають вимогам сучасних європейських протоколів безпеки, що обмежує інтеграцію України до єдиного цифрового ринку ЄС. На думку керівництва відомства важливо створити Національну систему стандартизації у сфері захисту інформації, яка б поєднувала національні напрацювання з вимогами NIST (США) та ENISA (ЄС) [112; 116].

З огляду на зазначене, вважаємо за доцільне внести низку змін до законодавства, а саме:

1. Створити інститут незалежної сертифікації засобів криптографічного захисту за стандартами ISO/IEC 15408 (Common Criteria) із залученням приватних лабораторій під контролем ДССЗЗІ.

2. Удосконалити систему нормативних документів НД ТЗІ, визнавши їх джерелом техніко-правових стандартів, що підлягають обов’язковому перегляду кожні п’ять років із публікацією відкритих результатів аудиту.

Безперечно, Державна служба спеціального зв’язку та захисту інформації України є фундаментальним елементом інституційної архітектури публічно-інформаційної безпеки, який забезпечує технологічну основу для реалізації державної політики у сфері національної безпеки. Її подальший розвиток має відбуватися шляхом поєднання технічної компетенції, аналітичної спроможності та міжнародної інтегрованості, що дозволить перетворити ДССЗЗІ на сучасний центр кібербезпеки європейського типу.

У системі публічної влади, відповідальній за формування політики у сфері інформаційної безпеки, Міністерство культури та інформаційної політики України (МКІП) виконує гуманітарно-комунікаційну функцію. Його діяльність охоплює формування державної інформаційної політики, протидію

дезінформації, розвиток стратегічних комунікацій, а також підвищення рівня медіаграмотності населення.

Відповідно до Положення про Міністерство культури та інформаційної політики України, затвердженого постановою Кабінету Міністрів України від 16 жовтня 2019 р. № 885 (зі змінами) [117], МКІП забезпечує реалізацію державної політики у сферах інформаційного суверенітету, національного контенту, захисту інформаційного простору від деструктивних впливів, а також координацію діяльності органів влади з питань стратегічних комунікацій.

У структурі Міністерства діє Центр стратегічних комунікацій та інформаційної безпеки, що виконує такі завдання:

- інформаційно-аналітична підтримка державних інституцій у протидії дезінформації;
- виявлення та моніторинг інформаційних операцій;
- координація державної комунікаційної політики у кризових ситуаціях;
- розроблення освітніх та просвітницьких програм із медіаграмотності.

Попри значний потенціал цього центру, аналіз практики показує, що компетенції МКІП залишаються розпорошеними між інформаційною політикою та культурною сферою. Це створює адміністративне перевантаження й не завжди забезпечує належний рівень міжвідомчої взаємодії з Міністерством цифрової трансформації, Держспецзв'язку та СБУ.

З урахуванням зазначеного, пропонується посилити інституційну роль існуючого Центру стратегічних комунікацій та інформаційної безпеки, зокрема:

1. Надати центру статус урядового міжвідомчого органу з аналітично-координаційними функціями, підпорядкованого безпосередньо Кабінету Міністрів України.

2. Розширити його повноваження в частині координації державних і регіональних стратегічних комунікацій, а також інтегрувати освітні програми з

медіаграмотності у систему підготовки державних службовців, журналістів і педагогів.

3. Створити в межах Центру окрему платформу стратегічних наративів, яка б забезпечувала узгодженість державних меседжів у внутрішній та зовнішній інформаційній політиці (у взаємодії з МЗС та Міноборони).

Як бачимо, МКІП виступає інституційним носієм гуманітарного виміру інформаційної безпеки, який формує комунікаційну стійкість суспільства до дезінформаційних впливів. Його діяльність має бути спрямована на зміцнення інформаційного імунітету громадян, що є не менш важливою складовою національної безпеки, ніж технічний або військовий захист.

Узагальнюючи, можна констатувати, що діяльність органів виконавчої влади у сфері забезпечення національної безпеки в публічно-інформаційній сфері в Україні характеризується поступовим переходом від інституційної роз'єднаності до інтегрованої моделі управління ризиками, однак відсутність єдиного центру стратегічної координації зумовлює дублювання повноважень і ускладнює реалізацію єдиної державної політики.

Система забезпечення національної безпеки у публічно-інформаційній сфері ґрунтується на спільній діяльності Президента України, РНБО, Верховної Ради, Кабінету Міністрів, а також таких органів, як Міністерство цифрової трансформації (Мінцифра), Державна служба спеціального зв'язку та захисту інформації (ДССЗЗІ) і Міністерство культури та інформаційної політики (МКІП). Вони формують багаторівневу систему управління, у якій поєднано політичні, технічні та комунікаційні механізми забезпечення інформаційної безпеки.

До сильних аспектів цієї системи належать наявність стратегічних документів і чітко визначених повноважень; існування технічних органів (як-от ДССЗЗІ) та інституцій гуманітарного профілю (МКІП); розвиток цифрових державних сервісів, у яких безпека враховується вже на етапі розробки (*security by design*).

Водночас спостерігаються певні проблеми: недостатня узгодженість дій між стратегічними та виконавчими органами; перевага реагування на загрози над їх попередженням; часткова невідповідність національних стандартів міжнародним вимогам. Для підвищення ефективності пропонується впровадити все ж таки трирівневу модель управління з чітким розподілом функцій:

Стратегічний рівень – Президент, РНБО, Верховна Рада, Кабінет Міністрів. Вони визначають політику, пріоритети, ухвалюють стратегії й закони. Доцільно закріпити у законодавстві керівництво у сфері безпеки як окрему складову сектора та запровадити щорічний «Єдиний план публічно-інформаційної безпеки», який стане основою для роботи всіх органів.

Виконавчий рівень – Мінцифра, ДССЗЗІ, СБУ, Національна поліція та інші. Вони безпосередньо реалізують державну політику. Доцільно створити при Мінцифрі Національний центр аудиту кіберстійкості, який перевірятиме надійність державних цифрових систем. ДССЗЗІ має перейти від реагування на інциденти до проактивного захисту, створивши єдиний центр аналізу кіберзагроз.

Громадський рівень – Центр стратегічних комунікацій при МКІП, ЗМІ, громадські організації, навчальні заклади. Їх завдання – підвищувати медіаграмотність, виявляти дезінформацію та сприяти формуванню культури інформаційної безпеки. Центр доцільно посилити, надавши йому міжвідомчий статус і право координувати інформаційну політику держави.

Практична реалізація цієї моделі передбачає:

- на стратегічному рівні – закріплення керівництва сектором інформаційної безпеки на законодавчому рівні та запровадження щорічного «Єдиного плану публічно-інформаційної безпеки»;
- на виконавчому рівні – створення при Мінцифрі Національного центру аудиту кіберстійкості та перехід ДССЗЗІ до проактивних моделей захисту через формування єдиного центру аналізу кіберзагроз;

– на громадському рівні – посилення ролі Центру стратегічних комунікацій при МКІП шляхом надання йому міжвідомчого статусу та функцій координації інформаційної політики держави.

Отже, інтеграція трирівневої моделі управління, закріплена в базовому законі «Про інформаційну безпеку», сприятиме формуванню цілісної, узгодженої та ефективної системи публічно-інформаційної безпеки України, що відповідає європейським стандартам democratic security governance та принципам результативного публічного адміністрування.

Для вдосконалення правового регулювання варто: внести зміни до Закону «Про національну безпеку України», чітко визначивши відповідальність держави, бізнесу й громадян у сфері інформаційної безпеки; оновити Закон «Про основні засади забезпечення кібербезпеки України», запровадивши регулярну сертифікацію державних ІТ-систем; переглянути положення про ДССЗЗІ та МКІП, розмежувавши їх технічні та комунікаційні функції.

2.2. Роль правоохоронних органів у забезпеченні національної безпеки в інформаційному просторі

Правоохоронні органи України відіграють ключову роль у забезпеченні інформаційної безпеки держави, адже саме вони здійснюють виявлення, розслідування та запобігання загрозам у цифровому середовищі. До таких загроз належать кібератаки, дезінформаційні кампанії, незаконний збір і поширення персональних даних, а також злочини, що вчиняються з використанням інформаційно-комунікаційних технологій [118].

В умовах гібридної війни, яку веде проти України держава-агресор, інформаційна сфера перетворилася на один із головних фронтів протистояння. Це зумовлює необхідність переосмислення ролі правоохоронних структур – від реагування на вже скоєні правопорушення до створення ефективної системи раннього попередження й профілактики кіберзагроз. Для цього потрібні

модернізація технічних ресурсів, розвиток аналітичних спроможностей, підвищення кваліфікації кадрів, а також оновлення правових механізмів, що регламентують діяльність у сфері інформаційної безпеки.

Очевидно, що правоохоронні органи стають не лише суб'єктами примусового впливу, а й активними учасниками формування національної політики безпеки в інформаційному просторі, забезпечуючи стабільність, правопорядок і довіру до цифрової держави.

Цілком погоджуючись із позицією С. Усик, варто наголосити, що правоохоронні органи як складова силового блоку держави відіграють ключову роль у протидії посяганням на інформаційну безпеку. Їх діяльність спрямована не лише на виявлення та припинення порушень у цій сфері, а й на формування системи запобіжних заходів, здатних мінімізувати ризики інформаційних атак, кібершахрайства, витоку даних і дезінформації [119, с. 103].

В Україні функціонує розгалужена система правоохоронних органів, які виконують завдання із забезпечення національної безпеки в інформаційному просторі. Її складають органи з різним функціональним призначенням і рівнем підпорядкування — Служба безпеки України, Кіберполіція, Національна поліція, окремі підрозділи Державної служби спеціального зв'язку та захисту інформації та інші структури, залучені до реагування на інформаційні та кібернетичні загрози. Кожен із них реалізує свої повноваження у межах визначеної компетенції — від розвідувально-аналітичної роботи та превентивної діяльності до досудового розслідування правопорушень у сфері інформаційної безпеки.

Безсумнівно, правоохоронні органи є інтегрованою та функціонально взаємозалежною системою державного захисту інформаційного простору, у межах якої поєднуються правові, організаційні й технічні механізми протидії загрозам, спрямованим на підрив інформаційного суверенітету, стабільності держави та безпеки суспільних комунікацій.

Кіберполіція України, що є структурним підрозділом Національної поліції, спеціалізується на виявленні, розслідуванні та запобіганні кіберзлочинам. Її діяльність охоплює боротьбу з шахрайством у цифровому середовищі, несанкціонованим доступом до інформаційних систем, кібератаками на фінансові установи та інтернет-шахрайством. Окрему увагу Кіберполіція приділяє профілактиці злочинів – проведенню інформаційних кампаній і навчальних заходів, спрямованих на підвищення рівня цифрової грамотності населення, оскільки більшість кіберінцидентів відбувається через необізнаність користувачів у сфері кібербезпеки [118].

Зауважимо, що формування нормативно-правової бази для діяльності цього територіального органу відбувалося у стислі терміни та в доволі динамічному режимі. Так, після ухвалення постанови Кабінету Міністрів України від 13 жовтня 2015 року № 831 «Про утворення територіального органу Національної поліції» [120], якою було започатковано створення нового підрозділу, уже через два дні Міністерство внутрішніх справ України видало низку ключових наказів. Зокрема, наказ № 1250 від 15 жовтня 2015 року «Про проведення позачергового атестування осіб начальницького складу підрозділів боротьби з кіберзлочинністю» [121] та наказ № 1251 від тієї ж дати «Про проведення конкурсу на заміщення вакантних посад старших інспекторів, інспекторів і спеціальних агентів інформаційних технологій міжрегіонального територіального органу Департаменту кіберполіції Національної поліції» [122]. Цими документами були визначені правові засади формування кадрового складу новоствореного органу, умови проведення конкурсу та критерії добору висококваліфікованих фахівців у сфері інформаційних технологій [123].

Розроблення концепції реформування підрозділів боротьби з кіберзлочинністю здійснювалося з урахуванням найкращих європейських і світових практик, а також рекомендацій авторитетних міжнародних організацій. Такий підхід забезпечив гармонізацію національної системи протидії

кіберзлочинності з міжнародними стандартами. Адже у більшості розвинених країн світу ефективна боротьба з кіберзагрозами ґрунтується на створенні спеціалізованих відомств або служб, що мають відповідну експертизу та повноваження. Зокрема, у США цю функцію виконує Федеральне бюро розслідувань (FBI), у Великій Британії – Національне агентство з протидії злочинності (National Crime Agency), у Китаї – Народна поліція (People's Police), у Японії – Національне поліцейське агентство (National Police Agency), у Франції – Центральне управління з боротьби зі злочинністю у сфері інформаційних технологій (Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication) [123].

Переконані, що створення територіальних органів Кіберполіції України стало логічним кроком у процесі адаптації національної правоохоронної системи до глобальних тенденцій кіберзахисту та зміцнення потенціалу держави у сфері інформаційної безпеки.

Твердження І. Казанчук і В. Яценко про те, що система кібербезпеки в Україні залишається слабкою, загалом є обґрунтованим, хоча потребує певного уточнення з урахуванням сучасних тенденцій [124].

Справді, на момент проведення їхнього дослідження (2020 р.) в Україні існували суттєві проблеми: фрагментарність нормативно-правової бази, недостатня координація між суб'єктами кібербезпеки, низький рівень цифрової грамотності населення та обмежені ресурси правоохоронних органів. Частина цих викликів актуальна й сьогодні – особливо у сфері правозастосування, імплементації міжнародних стандартів і розподілу відповідальності між державними структурами [124].

Водночас, із 2021 р. спостерігається суттєве посилення інституційної спроможності України у сфері кіберзахисту: ухвалено Стратегію кібербезпеки України до 2025 р., розширено повноваження Кіберполіції, налагоджено співпрацю з NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) та

ENISA. Також розвивається система публічно-приватного партнерства й розпочато впровадження освітніх ініціатив із кіберграмотності.

Отже, із твердженням дослідниць можна частково погодитися: Україна дійсно тривалий час мала фрагментовану систему кіберзахисту, однак нині відбувається її структурне зміцнення. Проблеми не зникли, але спостерігається поступовий перехід від реактивної до проактивної моделі управління кібербезпекою, що свідчить про позитивну динаміку розвитку галузі.

Служба безпеки України (СБУ) є ключовим стратегічним суб'єктом у системі забезпечення інформаційної безпеки держави. Її діяльність спрямована на протидію зовнішнім і внутрішнім загрозам у кіберпросторі, захист критичної інформаційної інфраструктури та запобігання деструктивним інформаційним впливам. Основні завдання СБУ полягають у здійсненні контррозвідувальних заходів щодо запобігання кібератакам з боку іноземних спецслужб, нейтралізації інформаційно-психологічних операцій, виявленні та розслідуванні злочинів, пов'язаних із кібершпигунством, витоком державної таємниці, незаконним збором і використанням конфіденційних даних. Важливою складовою її діяльності є також співпраця з міжнародними партнерами у сфері кібербезпеки, що забезпечує обмін оперативною інформацією, спільне реагування на кіберінциденти та формування спільної аналітичної бази для протидії глобальним кіберзагрозам [118].

Окрім того, СБУ свою діяльність щодо забезпечення інформаційної безпеки України спрямовує на обмеження та усунення низки негативних чинників впливу на стан національної безпеки в інформаційній сфері, зокрема: посилення негативного впливу на інформаційний простір України, що загрожує розмиванням суспільних цінностей і національної ідентичності; недостатні обсяги вироблення конкурентоспроможного національного інформаційного продукту; наближений до критичного стан безпеки інформаційно-комп'ютерних

систем в галузі державного управління, фінансової і банківської сфери, енергетики, транспорту, внутрішніх та міжнародних комунікацій тощо [137].

Відповідно до Закону України «Про основи національної безпеки України» від 19 червня 2003 р. № 964-IV [103], функції Служби безпеки України у сфері забезпечення національної безпеки, зокрема інформаційної, були визначені доволі детально та комплексно. Згідно зі ст.10 цього закону, СБУ здійснювала постійний моніторинг процесів, що впливають на стан національної безпеки, прогнозувала зміни та загрози, здійснювала інформаційно-аналітичне забезпечення діяльності інших суб'єктів національної безпеки, розробляла пропозиції щодо нейтралізації дестабілізуючих чинників, а також брала участь у міжнародному співробітництві у сфері інформаційної безпеки.

Такий підхід відображав прагнення законодавця забезпечити системність і прозорість діяльності СБУ у межах інформаційного простору, окреслити широкий спектр її превентивних, аналітичних і координаційних повноважень.

Натомість у чинному Законі України «Про національну безпеку України» від 21 червня 2018 р. № 2469-VIII [23] підхід до регулювання ролі СБУ суттєво змінено. Закон містить узагальнене визначення завдань цього органу, визначаючи його як державний орган спеціального призначення з правоохоронними функціями, що забезпечує державну безпеку, у тому числі кібер- та інформаційну безпеку. Конкретизація напрямів діяльності СБУ передбачена вже не на рівні закону, а у підзаконних нормативно-правових актах.

З одного боку, така зміна свідчить про позитивну тенденцію до кодифікаційної спрощеності та гнучкості правового регулювання, що дозволяє оперативніше адаптувати діяльність СБУ до сучасних викликів, зокрема у сфері кіберзагроз і гібридної війни. Крім того, це відповідає європейській практиці, де детальні процедурні аспекти роботи спецслужб, як правило, не фіксуються безпосередньо в законі.

Водночас відмова від деталізації функцій СБУ, властивої закону 2003 р., має і негативні наслідки. Відсутність чітко визначеного переліку завдань у законі може призвести до зменшення прозорості діяльності Служби, створює ризик надмірного розширення її повноважень через підзаконні акти та ускладнює здійснення громадського й парламентського контролю за її роботою.

Порівняльний аналіз двох законів засвідчує, що реформу 2018 р. спрямовано на концептуальне оновлення системи національної безпеки, проте вона потребує балансу між гнучкістю у правовому регулюванні та збереженням належного рівня визначеності повноважень Служби безпеки України, особливо у сфері інформаційної та кібербезпеки.

Як зазначає В. Макарчук, аналіз стратегічних документів та нормативно-правових актів, які визначають компетенцію правоохоронних органів у сфері інформаційної безпеки, дозволяє виокремити кілька груп їхніх повноважень.

1. Інформаційно-аналітичні – пов’язані зі збором, опрацюванням і використанням інформації для прийняття управлінських рішень у сфері безпеки. Так, відповідно до ст. 24 Закону України «Про Службу безпеки України», СБУ має повноваження здійснювати аналітичну роботу для забезпечення національної безпеки, оборони, науки, економіки та екології.
2. Профілактично-запобіжні – спрямовані на попередження злочинів у сфері кібербезпеки. СБУ проводить перевірки готовності об’єктів критичної інфраструктури до кібератак і розробляє превентивні заходи у сфері кіберзахисту.
3. Протидійно-реагувальні – включають розслідування кіберінцидентів, кібератак на державні ресурси та забезпечення реагування на інформаційні операції, що загрожують державній безпеці.

4. Оперативно-технічні – охоплюють діяльність із технічного регулювання, розроблення та використання спеціальних технічних засобів для отримання інформації, необхідної для запобігання загрозам.
5. Моніторингові – передбачають постійний нагляд за інформаційним простором, зокрема моніторинг ЗМІ та Інтернету з метою виявлення проявів дезінформації, закликів до насильства чи посягань на територіальну цілісність держави.
6. Правообмежувальні – стосуються обмеження участі компаній, пов'язаних із державами-агресорами, у проектах кіберзахисту та заборони використання їхніх технологій чи послуг у сфері захисту державних інформаційних ресурсів [125, с. 325–326].

Очевидно, що СБУ не лише реалізує функції з протидії кіберзагрозам, а й координує діяльність інших правоохоронних структур у межах державної політики інформаційної безпеки. Її компетенція охоплює як стратегічний, так і практичний рівні забезпечення безпеки в інформаційному просторі, що робить цей орган одним із ключових елементів системи національної стійкості України.

Попри значну роль Служби безпеки України у забезпеченні інформаційної безпеки, аналіз її діяльності дає змогу окреслити низку проблемних аспектів, що знижують ефективність реалізації державної політики у цій сфері:

– надмірна концентрація повноважень – СБУ одночасно здійснює аналітичні, контррозвідувальні, слідчі й технічні функції, що створює ризики дублювання завдань інших органів (Кіберполіції та ДССЗЗІ) і ускладнює координацію;
– реактивність роботи – основна увага зосереджена на розслідуванні скоєних кіберінцидентів, тоді як превентивна діяльність (аудит вразливостей, прогнозування атак, підготовка кадрів) є епізодичною;
– недостатня публічна комунікація та відкритість – відсутній регулярний звітний формат щодо стану інформаційної безпеки, що ускладнює

громадський контроль і формування культури кіберзахисту серед населення;

- застаріла технічна база та нормативна база – низка внутрішніх інструкцій і технічних регламентів не повністю відповідає міжнародним стандартам (ISO/IEC 27001, NIST, ENISA);
- обмежений міжвідомчий обмін даними – інформаційні ресурси СБУ не інтегровано належним чином з базами Кіберполіції, ДССЗЗІ та Мінцифри, що знижує швидкість реагування на складні кіберінциденти.

На нашу думку, безперечно, важливо вдосконалити діяльність Служби безпеки України у сфері інформаційної безпеки з огляду на такі пропозиції:

1. Нормативне уточнення повноважень. Доцільно внести зміни до Закону України «Про Службу безпеки України» та суміжних нормативно-правових актів, чітко визначивши розмежування компетенцій між СБУ, Кіберполіцією, Держспецзв'язку та Мінцифрою. Це забезпечить узгодженість дій і запобігатиме дублюванню функцій.
2. Інтеграція інформаційних систем. Варто запровадити єдину захищену платформу обміну даними між СБУ, Кіберполіцією, ДССЗЗІ та іншими органами сектору безпеки. Це підвищить оперативність реагування на кіберінциденти та ефективність міжвідомчої взаємодії.
3. Оновлення нормативно-технічної бази. Необхідно гармонізувати чинні нормативи СБУ із міжнародними стандартами кіберзахисту – ISO/IEC 27001, NIST, ENISA – та впровадити незалежний аудит технічних засобів захисту інформації.
4. Підвищення прозорості діяльності. Доцільно запровадити щорічний публічний звіт СБУ про стан кібербезпеки держави, який міститиме статистику кіберінцидентів, результати міжнародної співпраці та аналіз тенденцій. Це сприятиме формуванню довіри суспільства й забезпеченню демократичного контролю.

5. Кадрове та освітнє забезпечення. Рекомендується створити галузеву систему підготовки фахівців із кібербезпеки на базі вищих навчальних закладів спільно з СБУ, МОН і Мінцифрою, що дозволить формувати сучасні компетентності працівників правоохоронних органів.

Удосконалення за цими напрямами сприятиме переходу Служби безпеки України від реактивної моделі протидії загрозам до проактивної системи управління інформаційною безпекою, здатної забезпечити технологічну, правову та організаційну стійкість держави у цифровому середовищі.

Національна поліція України, окрім діяльності Кіберполіції, також здійснює заходи з підтримання інформаційної безпеки. Зокрема, її підрозділи розслідують злочини, пов’язані з розповсюдженням шкідливого програмного забезпечення, фінансовими махінаціями у мережі, незаконним обігом персональних даних та поширенням забороненого контенту. В умовах воєнного стану особливої актуальності набуває моніторинг інтернет-простору на предмет виявлення закликів до насильства, екстремізму чи тероризму, що дозволяє своєчасно локалізувати потенційні інформаційні загрози [118].

Для забезпечення постійного функціонування органів (закладів, установ) поліції у сфері трудових, соціальних, фінансових, управлінських відносин, відносин документообігу створюються відповідні бази даних, а також міжвідомчі інформаційно-аналітичні та інформаційно-телекомунікаційні системи, необхідні для виконання покладених на поліцію повноважень. Зважаючи на це, інформація, яка акумулюється в них, і самі інформаційні обліки набувають статусу критичної інформаційної інфраструктури, що потребує належного захисту [126, с. 11; 127].

У контексті сучасних кіберзагроз саме інформаційні ресурси поліції становлять основу функціональної спроможності правоохоронної системи. Їхня вразливість може призвести не лише до витоку персональних даних, а й до дестабілізації діяльності державних органів, тому питання безпеки баз даних поліції має розглядатися як складова національної безпеки.

Відповідно до ч. 2 ст. 25 Закону України «Про Національну поліцію» поліція в рамках інформаційно-аналітичної діяльності: формує реєстри та бази (банки) даних, що входять до Єдиної інформаційної системи Міністерства внутрішніх справ України; здійснює інформаційно-пошукову та інформаційно-аналітичну роботу; користується реєстрами та базами (банками) даних Міністерства внутрішніх справ України та інших органів державної влади; надає до Єдиного державного реєстру призовників, військовозобов'язаних та резервістів в електронній формі необхідні відомості; здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями [127; 128].

Така система обміну даними створює передумови для побудови інтегрованого інформаційного простору правоохоронних органів, проте водночас потребує чітких правил доступу, зберігання і передачі інформації. Доцільно посилити правові гарантії захисту персональних даних, а також запровадити незалежний аудит безпеки інформаційних систем МВС із залученням Держспецзв'язку.

Інформаційно-аналітична робота поліції – це творча, дослідницька, цілеспрямована й спеціально організована діяльність, що проводиться на основі методів пізнання та призначена здійснювати: збір, накопичення й обробку даних; пошук, аналіз і узагальнення інформації про стан правопорядку та діяльність поліції; отримання нових спеціальних знань щодо підвищення ефективності протидії злочинності; підвищення ефективності управлінської діяльності поліції на різних рівнях щодо забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку [127; 129, с. 139].

Як бачимо, інформаційно-аналітична діяльність поліції має не лише технічний, а й стратегічний характер, оскільки слугує базою для прийняття управлінських рішень і формування аналітичних прогнозів безпеки. Вважаємо доцільним удосконалити систему підготовки кадрів для цієї сфери,

запровадивши в навчальних закладах МВС спеціалізовані модулі з аналітичної обробки даних, кіберрозвідки та інформаційного менеджменту.

До правоохоронних повноважень Національної поліції України у сфері забезпечення інформаційної безпеки належить комплекс дій, спрямованих на попередження, виявлення та розслідування правопорушень, що становлять загрозу інформаційному простору держави. Зокрема, йдеться про превентивну та профілактичну діяльність, спрямовану на недопущення порушень у сфері інформації, а також на усунення причин і умов, які сприяють їх виникненню.

Поліція уповноважена вживати заходів для захисту життя, здоров'я громадян і публічної безпеки у разі, коли інформаційні злочини створюють реальні ризики для суспільства. До її компетенції також належать виявлення кримінальних та адміністративних правопорушень у сфері інформаційної безпеки, проведення досудового розслідування, розшук осіб, які ухиляються від слідства чи суду, а також застосування адміністративних стягнень у випадках, передбачених законом [127; 130, с. 170–171].

Такі функції засвідчують, що поліція фактично є операційною ланкою державної системи кібер- та інформаційної безпеки, яка реалізує практичні механізми виявлення й реагування на загрози. Однак аналіз чинної практики показує, що превентивна діяльність ще не має належної системності: більшість заходів є постфактумними, а взаємодія з органами сектора безпеки відбувається переважно шляхом запитів, а не автоматизованого обміну інформацією.

У межах структур Національної поліції реалізація цих повноважень здійснюється усіма підрозділами відповідно до їх компетенції – Департаментом інформаційно-аналітичної підтримки [127; 131], Департаментом патрульної поліції [127; 132], Департаментом організаційно-аналітичного забезпечення та оперативного реагування [127; 133], Департаментом превентивної діяльності [127; 134], Департаментом карного розшуку [127; 135], а також слідчими підрозділами [127; 136].

З огляду на розгалужену систему підрозділів важливо забезпечити єдину координаційну платформу для інформаційного обміну, що дозволить уникнути дублювання повноважень, підвищити швидкість реагування на кіберінциденти та підсилити аналітичну спроможність поліції. Доцільно також розробити єдині методичні стандарти дій підрозділів поліції у сфері інформаційної безпеки, гармонізовані з рекомендаціями Європолу та INTERPOL Cybercrime Directorate.

Проаналізувавши діяльність правоохоронних органів та нормативну базу їх закріплення в забезпеченні національної безпеки в інформаційному просторі, зазначимо, що попри наявність законодавчих основ ще спостерігаються, як зазначено вище, прогалини у чіткому розмежуванні компетенцій та координації між суб'єктами цієї діяльності. Тому підведемо підсумки з обґрунтуванням.

Аналіз чинної нормативно-правової бази та діяльності правоохоронних органів у сфері забезпечення інформаційної безпеки засвідчує фрагментарність компетенцій та відсутність чіткого розмежування повноважень між суб'єктами цієї сфери.

Відповідно до ст. 12 Закону України «Про національну безпеку України» [23], до сектору безпеки і оборони належать, зокрема, Служба безпеки України, Національна поліція, Державна служба спеціального зв'язку та захисту інформації України, а також інші органи виконавчої влади, які беруть участь у забезпеченні національної безпеки. Однак ні зазначений закон, ні профільні нормативні акти – зокрема, Закони України «Про Службу безпеки України» [98], «Про Національну поліцію» [128], «Про основні засади забезпечення кібербезпеки України» [47] – не встановлюють єдиної, узгодженої системи розмежування функцій у межах інформаційно-комунікаційної сфери.

Закон України «Про основні засади забезпечення кібербезпеки України» [47] лише загально визначає суб'єктів забезпечення кібербезпеки, серед яких – Служба безпеки України та Національна поліція, однак не конкретизує їх функціональну спеціалізацію. Як наслідок, у правозастосовній практиці

простежується дублювання компетенцій, зокрема у реагуванні на кібератаки на об’єкти критичної інформаційної інфраструктури, коли обидва органи можуть одночасно ініціювати кримінальне провадження або здійснювати оперативно-технічні заходи.

Подібна ситуація суперечить принципу чіткого розподілу повноважень і відповідальності між суб’єктами сектору безпеки, закріпленому у статті 4 Закону України «Про національну безпеку України» [23], та зумовлює неузгодженість дій під час реагування на масштабні кіберінциденти. Така фрагментарність негативно позначається на швидкості реагування, знижує рівень координації між інституціями сектору безпеки та, відповідно, зменшує ефективність системи національної кіберстійкості.

З науково-практичного погляду, потребує вдосконалення нормативна модель розмежування компетенцій між органами сектору безпеки в інформаційній сфері. З огляду на це важливо підвищити ефективність функціонування координаційного механізму – Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України.

Попри наявність цього центру, який виконує функції стратегічного планування, моніторингу та реагування на кіберінциденти, на практиці спостерігаються проблеми узгодженості дій між Службою безпеки України, Національною поліцією, Державною службою спеціального зв’язку та захисту інформації та іншими суб’єктами сектору безпеки. Це спричинено відсутністю чітких процедур оперативної взаємодії, недостатнім нормативним регулюванням повноважень, бюрократичною інерційністю міжвідомчої координації.

Пріоритетним напрямом удосконалення державної системи кібербезпеки має стати розширення повноважень та інституційної спроможності НКЦК через:

– законодавче закріплення його статусу як центрального координатора у сфері кіберзахисту;

- запровадження єдиних протоколів обміну інформацією між усіма суб’єктами кібербезпеки;
- інтеграцію інформаційних систем реагування на кіберінциденти в єдиний державний простір;
- створення механізмів громадсько-приватного партнерства для залучення операторів критичної інфраструктури до процесів оцінювання ризиків і розроблення заходів реагування.

Удосконалення діяльності НКЦК дозволить не лише оптимізувати координацію між основними суб’єктами сектору безпеки, але й сформувати єдиний національний простір оперативного реагування на кіберзагрози, що відповідатиме європейським стандартам кіберстійкості та принципам NIS2 Директиви ЄС.

Також, слід наголосити на недостатній правовій визначеності статусу Департаменту кіберполіції. На підзаконному рівні діяльність підрозділу врегульована Наказом МВС України від 15 жовтня 2015 р. № 1251 «Про проведення конкурсу на заміщення вакантних посад у Департаменті кіберполіції», а також Положенням про Департамент кіберполіції Національної поліції України, затвердженим наказом МВС № 1234 від 23.11.2015 р., однак у Законі України «Про Національну поліцію» (далі – Закон) відсутні прямі норми, які б визначали правовий статус цього підрозділу, його структуру, повноваження, підзвітність і принципи взаємодії з іншими органами.

Відповідно до ч. 2 ст. 25 Закону, поліція має право формувати реєстри, бази (банки) даних і здійснювати інформаційно-аналітичну діяльність, однак не конкретизовано повноваження саме у сфері кіберзлочинності, що створює ризики неоднозначного тлумачення меж компетенції. Департамент кіберполіції де-факто виконує функції центрального координатора у боротьбі з кіберзлочинністю, але де-юре не має статусу спеціалізованого органу, що обмежує можливості у сфері

міжнародного співробітництва (зокрема, взаємодії з Europol EC3, INTERPOL Cybercrime Centre) та унеможливлює створення свого бюджету в системі МВС.

Правова невизначеність статусу кіберполіції суперечить принципу інституційної прозорості, закріпленому у ст. 3 Закону України «Про національну безпеку України», і знижує ефективність міжвідомчої координації у сфері кіберзахисту.

Безпосередньо прослідковується дисбаланс між реагуванням на вже здійснені кіберзагрози та системною роботою із запобігання їх виникненню. У більшості випадків діяльність органів сектору безпеки спрямована на фіксацію інциденту, розслідування фактів порушень та мінімізацію наслідків, тоді як механізми прогнозування, оцінювання ризиків і раннього попередження загроз залишаються фрагментарними або взагалі відсутніми.

Згідно зі Стратегією інформаційної безпеки України (Указ Президента України від 28.12.2021 р. № 685/2021) [107], ключовим завданням державної політики визначено переорієнтацію системи безпеки на запобігання інформаційним і кіберзагрозам. Проте на практиці правоохоронні органи здебільшого діють реактивно, тобто лише після настання події.

Наявна нормативна база не містить вимог до створення прогнозно-аналітичних структур або механізмів моніторингу ризиків у режимі реального часу. У Законі «Про Службу безпеки України» [98] вжито лише загальне формулювання «здійснює інформаційно-аналітичну роботу», що не визначає ані інструментів, ані методів прогнозування. Відсутність законодавчо врегульованого механізму превентивного аналізу вразливостей створює умови для того, що значна частина кіберінцидентів виявляється після завдання шкоди.

Таке становище спричинено недостатнім розвитком аналітичної інфраструктури держави, відсутністю чітких вимог до міжвідомчого обміну інформацією про потенційні ризики. Зокрема, чинне законодавство не передбачає створення на постійній основі спеціалізованих центрів моніторингу

інформаційного простору чи національних платформ прогнозного аналізу кіберзагроз, які б забезпечували інтеграцію даних від державних органів, провайдерів критичної інфраструктури та приватного сектора.

Наслідком цього є низький рівень ситуаційної обізнаності органів державної влади щодо процесів у кіберпросторі, що унеможливлює своєчасне реагування на атаки, інформаційні кампанії чи деструктивний контент.

Розв'язання проблеми передбачає перехід до проактивної (превентивної) моделі управління ризиками, заснованої на системному моніторингу, аналізі поведінкових аномалій у кіберсередовищі та прогнозуванні потенційних загроз. Для цього доцільно:

- запровадити національну систему раннього виявлення кіберінцидентів (за аналогією з моделлю Early Warning Systems ЄС);
- створити аналітичні підрозділи з оцінювання ризиків при ключових суб'єктах сектору безпеки, які б працювали на основі даних кіберрозвідки (cyber threat intelligence);
- забезпечити інституційну інтеграцію таких підрозділів із Національним координаційним центром кібербезпеки при РНБО України для формування єдиного аналітичного простору;
- розробити державну методологію оцінювання кіберризиків, що враховуватиме не лише технічні, а й соціально-психологічні аспекти інформаційного впливу.

Перехід до превентивної моделі управління інформаційною безпекою дасть змогу змістити акцент з реагування на загрози – на їх попередження, що відповідає принципам сучасних стратегій кіберстійкості НАТО та Європейського Союзу. Це не лише підвищить адаптивність національної системи безпеки до динамічних умов гібридного протистояння, а й сприятиме формуванню культури інформаційної безпеки на державному рівні.

Однією з найактуальніших і водночас найменш врегульованих проблем у системі державного забезпечення інформаційної безпеки є обмежена підзвітність та інституційна закритість Служби безпеки України (СБУ) у сфері кібербезпеки. Цей аспект набуває особливого значення в умовах гібридної агресії проти України, коли довіра суспільства та ефективність міжвідомчої координації виступають критичними чинниками національної стійкості.

Згідно із ст. 6 Закону України «Про національну безпеку України» (2018), у державі запроваджується демократичний цивільний контроль за діяльністю сектору безпеки та оборони. Його метою є забезпечення прозорості, підзвітності та легітимності діяльності силових органів через парламентський, громадський, судовий та фінансовий нагляд. Цей принцип відображає міжнародні стандарти, зокрема Рекомендації Ради Європи № CM/Rec(2016)5 «Про правовий нагляд і підзвітність служб безпеки», згідно з якими ефективна розвідка чи контррозвідка у демократичній державі можлива лише за умов інституційної відкритості та зовнішнього контролю за дотриманням прав людини, однак чинний Закон України «Про Службу безпеки України» (в редакції 1992 р.) не містить жодної норми, що зобов'язувала б Службу звітувати про стан кіберзагроз, результати контррозвідувальної діяльності чи ефективність заходів з кіберзахисту державних інформаційних ресурсів. Наявна система підзвітності обмежується внутрішнім контролем Президента України та Ради національної безпеки і оборони, тобто перебуває у виключно закритому управлінському контурі.

Таке становище створює дисбаланс між принципом державної таємниці і суспільним правом на інформацію, що є порушенням статті 34 Конституції України та ст. 19 Закону України «Про доступ до публічної інформації» [73], якою передбачено, що обмеження доступу до інформації можливе лише за умови доведеності наявності реальної шкоди національним інтересам.

Відсутність законодавчо визначеного обов'язку щодо публічного або хоча б парламентського звітування призводить до дефіциту суспільної довіри та

перешкоджає формуванню партнерських відносин між СБУ, науковою спільнотою, IT-сектором і громадськими організаціями, які залучені до проєктів кіберосвіти й протидії дезінформації. Ізольованість суперечить європейським підходам democratic security governance, за якими ефективність системи безпеки оцінюється за результативністю дій і за їх легітимністю для суспільства.

Окрім того, нормативна закритість СБУ має і функціональні наслідки:

- ускладнено оперативну взаємодію з Державною службою спеціального зв'язку та захисту інформації України (ДССЗЗІ) під час координації кіберінцидентів, бо обмін даними між відомствами не врегульовано на рівні закону, а організовано на основі відомчих листів і протоколів;
- знижується ефективність спільних операцій із Національною поліцією, адже відсутні процедурні механізми погодження спільної підслідності у «змішаних» кіберсправах, де одночасно присутній і кримінально-правовий, і контррозвідувальний аспекти;
- обмежується можливість зовнішнього аудиту кіберзахисних заходів у системі державного управління, що не відповідає сучасним вимогам стандартів NIS2 (Директива ЄС 2022/2555) та ISO/IEC 27001:2022 щодо незалежного оцінювання кіберстійкості).

Непрозорість і відсутність системної підзвітності СБУ у сфері кібербезпеки становить організаційно-управлінську й правову прогалину, що обмежує ефективність державної політики у сфері інформаційної безпеки. З урахуванням цього доцільно передбачити в новій редакції Закону України «Про Службу безпеки України» такі норми:

1. Обов'язок СБУ подавати щорічний відкритий звіт до Верховної Ради України про стан кіберзагроз, тенденції у сфері інформаційної безпеки та результати міжнародного співробітництва у сфері кіберзахисту (з урахуванням вимог державної таємниці).

2. Визначення форми парламентського контролю, передбачивши створення при Комітеті ВРУ з питань національної безпеки, оборони та розвідки підкомітету з питань інформаційної та кібербезпеки, уповноваженого запитувати звіти та оцінювати ефективність СБУ у цій сфері.
3. Запровадження механізму незалежного аудиту інформаційної безпеки, який здійснювався б за участі сертифікованих фахівців ДССЗЗІ, Мінцифри та академічних установ.

Реалізація таких змін забезпечить баланс між безпековими інтересами держави і принципами демократичного управління, зміцнить довіру суспільства до Служби безпеки України, а також наблизить національну практику до європейських стандартів відкритого та підзвітного сектору безпеки.

Отже, роль правоохоронних органів у забезпеченні національної безпеки в інформаційному просторі полягає у реалізації організаційно-правових, аналітичних, оперативно-розшукових і превентивних заходів для виявлення, попередження та нейтралізацію інформаційних і кібернетичних загроз, що посягають на суверенітет, стабільність і правопорядок держави. Їхня діяльність охоплює моніторинг інформаційного середовища, встановлення джерел деструктивного впливу, документування протиправної діяльності, розслідування кіберзлочинів та забезпечення взаємодії з іншими суб’єктами сектору безпеки.

Належно організована діяльність правоохоронних структур забезпечує формування цілісної державної системи реагування на інформаційні загрози, спрямованої на підтримання стійкості національного інформаційного простору, ефективний захист цифрових ресурсів, своєчасне управління кіберінцидентами та забезпечення безперервності роботи критичної інформаційної інфраструктури. Водночас така система функціонує на засадах верховенства права, підзвітності та демократичного контролю, що є важливими умовами розвитку безпечного й правового цифрового середовища.

2.3. Механізми адміністративно-правового реагування та запобігання інформаційним загрозам

Дослідження механізмів адміністративно-правового реагування на інформаційні загрози базується на положеннях сучасної теорії адміністративного права, концептуальних засадах інформаційної безпеки держави, нормах чинного законодавства України, що регулює відносини у сфері інформаційної політики та кібербезпеки, а також на результатах аналізу практики діяльності органів публічної адміністрації.

Для того щоб розкрити поняття «механізм адміністративно-правового реагування та запобігання інформаційним загрозам», визначити його основні ознаки та структурні елементи, доцільно, застосовуючи метод аналізу, звернутися до з'ясування сутності первинних базових категорій, насамперед поняття «механізм». Первісно цей термін виник у межах природничих наук, насамперед механіки, де позначав систему взаємопов'язаних елементів, що забезпечують функціонування певного процесу чи явища. Згодом розвиток наукового знання призвів до поширення цього поняття в інші галузі – соціальні, політичні та юридичні науки [138].

Поняття «механізм» посідає важливе місце в різних сферах суспільного життя. У юридичній науці ця категорія почала активно застосовуватися від початку 2000-х років, коли вчені почали переосмислювати її методологічний потенціал у контексті правових досліджень. Як зазначає К. В. Шундіков, використання поняття «механізм» у правознавстві виявилося продуктивним, адже воно дозволило глибше зрозуміти інструментальну природу та внутрішню структуру правових явищ. Водночас дослідник зауважує, що нерідко характеристика певного правового феномена як «механізму» сприймається занадто формально – як суто логічний прийом, який не завжди забезпечує належний методологічний рівень аналізу. Унаслідок цього поняття, утворені на основі родової абстракції «механізм», переважно відображають масштабні

регулятивні системи – своєрідні юридичні макроконструкції, які охоплюють значний комплекс як правових, так і позаправових явищ [139, с. 12–21; 140].

У сучасній правовій доктрині активно застосовуються такі категорії, як «механізм правового забезпечення», «механізм правового регулювання», «механізм адміністративно-правового забезпечення» тощо. Аналіз наукових праць свідчить, що ці поняття нерідко використовуються як взаємозамінні, а отже – частково ототожнюються за своїм змістом. Зокрема, С. Діденко, досліджуючи поняття та елементи механізму адміністративно-правового забезпечення обігу та застосування зброї в Україні, зазначає, що адміністративно-правове забезпечення полягає у формуванні правових засад і засобів реалізації адміністративно-правових відносин у відповідній сфері, а також у гарантуванні та охороні прав, свобод і законних інтересів їх учасників. Виходячи з цього, науковець пропонує розглядати механізм адміністративно-правового забезпечення крізь призму механізму правового регулювання, покладаючи останній в основу теоретичного осмислення досліджуваного явища [141; 138].

Разом із тим, поняття механізму правового забезпечення сформувалося як результат наукової дискусії щодо сутності самого правового забезпечення, під яким у загальнотеоретичному сенсі розуміють цілеспрямований вплив на суспільні відносини та поведінку людей за допомогою правових (юридичних) засобів [142, с. 327; 144]. Якщо розглядати сферу правового забезпечення як сукупність правил і процедур управління, що підлягають впорядкуванню за допомогою правових норм та інструментів, то термін «правове забезпечення» може тлумачитися у двох взаємопов’язаних аспектах.

По-перше, воно може розумітися як управлінська діяльність органів публічної влади та їх посадових осіб, спрямована на виконання визначених законом функцій, пов’язаних із реалізацією правових приписів. По-друге, правове забезпечення може розглядатися як результат цієї діяльності, що

виявляється у фактичному виконанні норм права, забезпеченні прав і свобод громадян, підтриманні правопорядку [143, с. 165; 144].

Безсумнівно, механізм адміністративно-правового реагування та запобігання інформаційним загрозам доцільно розглядати як комплексну систему юридичних, організаційних і процедурних засобів, за якими держава здійснює превентивний, контрольний і примусовий вплив на інформаційні процеси для забезпечення відповідності вимогам безпеки й законності.

На відміну від механізму правового регулювання, який має переважно нормативно-статичний характер, механізм адміністративно-правового реагування є динамічною конструкцією для на виявлення, попередження й нейтралізацію інформаційних загроз у реальному часі. Його функціонування передбачає активну діяльність суб'єктів публічної адміністрації – передусім Національної поліції України, Служби безпеки України, Міністерства цифрової трансформації, Національного центру кібербезпеки при РНБО тощо.

У цьому контексті механізм адміністративно-правового реагування та запобігання інформаційним загрозам можна визначити як цілісну систему правових норм, адміністративних процедур, форм і методів діяльності уповноважених органів, спрямовану на забезпечення інформаційної стабільності держави, захист прав людини в цифровому середовищі та підтримання публічної безпеки у сфері інформаційних відносин.

Безперечно особливого значення набуває формування ефективного адміністративно-правового механізму реагування та запобігання інформаційним загрозам. Йдеться про створення чітких адміністративних процедур, які регламентують порядок виявлення, фіксації, оцінювання та нейтралізації таких загроз, визначають повноваження відповідних органів публічної адміністрації та встановлюють взаємодію між ними.

Цей механізм має забезпечувати узгодженість дій державних інституцій, своєчасне прийняття управлінських рішень, а також ефективний контроль за

дотриманням законності у сфері інформаційної безпеки. Важливою складовою виступає система правових гарантій і відповідальності за неналежне виконання обов'язків щодо захисту інформаційного простору, розголошення службової чи конфіденційної інформації, поширення дезінформації або створення умов для інформаційних атак.

Крім того, дієвий адміністративно-правовий механізм має передбачати функціонування спеціалізованих органів контролю та моніторингу, упровадження сучасних технологічних рішень для аналізу інформаційних потоків, а також налагодження міжвідомчої комунікації в умовах кризових чи надзвичайних ситуацій. Лише за наявності таких правових, організаційних і технічних елементів можливо забезпечити стійкість національного інформаційного простору, ефективне реагування на інформаційні виклики та захист прав громадян у цифровому середовищі.

Система адміністративно-правових механізмів реагування на інформаційні загрози є багаторівневою та комплексною, що передбачає застосування взаємопов'язаних правових, організаційних і технічних інструментів державного впливу. Її головна мета – забезпечити стійкість національного інформаційного простору, своєчасне попередження, локалізацію та усунення наслідків деструктивних інформаційних впливів.

Відповідно до функціонального призначення та характеру правового впливу доцільно виокремити три основні види адміністративно-правових механізмів реагування: превентивні, оперативно-реагувальні та юрисдикційні.

Одним із фундаментальних елементів системи адміністративно-правового забезпечення інформаційної безпеки держави виступають превентивні механізми, призначені для запобігання виникненню інформаційних загроз, мінімізації кіберризиків та формування стійкої архітектури національного інформаційного простору. Їх сутність полягає у цілеспрямованій діяльності уповноважених суб'єктів публічної адміністрації, спрямованій на створення

правових, організаційних, технічних і освітніх передумов, за яких можливість реалізації деструктивних інформаційних впливів є мінімальною.

Нормативно-правову основу превентивних адміністративно-правових механізмів становить Конституція України [46], де закріплено засади захисту інформаційного простору як елементу національної безпеки та гарантування права особи на захист від незаконного втручання в особисте і сімейне життя. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. № 2163-VIII [47], визначено обов'язки державних органів щодо забезпечення постійного моніторингу кіберінцидентів, здійснення оцінки вразливостей інформаційних систем, а також впровадження превентивних заходів у межах національної системи кібербезпеки.

У Законі України «Про національну безпеку України» від 21 червня 2018 р. № 2469-VIII [23] принцип превентивності визначено одним із засадничих принципів державної політики безпеки, що орієнтує сектор безпеки й оборони на запобігання загрозам, а не лише на реагування на їх наслідки. На рівні стратегічного планування цей підхід розвинуто у Стратегії кібербезпеки України до 2025 року (Указ Президента України від 26 серпня 2021 р. № 447/2021) [92], якою визначено пріоритет переходу до моделі випереджального управління ризиками та формування культури безпеки в цифровому середовищі.

На думку О. Проневич, превентивний напрям у діяльності держави передбачає відхід від репресивної, інтервенційної моделі правоохоронної політики та орієнтацію на соціально-правове партнерство між державою і суспільством. Учений наголошує, що ефективна протидія правопорушенням неможлива без визнання особливої соціальної значущості превентивної діяльності, а також без налагодження тісної взаємодії державних і комунальних суб'єктів поліцейської діяльності з інститутами громадянського суспільства у сфері інформаційно-роз'яснювальної роботи, спрямованої на коригування деструктивної поведінки громадян та усунення чинників, що детермінують

правопорушення [145, с. 639–640; 147]. Тобто, дослідник підкреслює, що превенція, на відміну від карального впливу, діє на ранніх стадіях розвитку небезпечних тенденцій, коли ще не відбулося посягання на права і свободи людини, що охороняються державою.

У цьому контексті до превентивних адміністративно-правових механізмів належать кілька взаємопов'язаних напрямів діяльності, кожен із яких має власне правове регулювання, організаційні форми реалізації та аналітичне забезпечення. Ключовим елементом таких механізмів виступає безперервний інформаційний моніторинг, спрямований на своєчасне виявлення ознак кіберінцидентів, інформаційних атак, поширення дезінформації або маніпулятивних технологій у публічному просторі.

Відповідно до ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України», суб'єкти сектору безпеки зобов'язані забезпечувати постійне спостереження за інформаційними потоками, фіксацію та аналітичну оцінку подій у кіберпросторі, а також здійснювати обмін інформацією про загрози через національні інформаційно-аналітичні системи. Саме цей вид превентивної діяльності створює підґрунтя для оперативного реагування на ризики інформаційної дестабілізації та гарантує сталість функціонування критичної інформаційної інфраструктури держави.

Як слушно зауважує Д. Булатін, у сучасній науковій та управлінській практиці поняття «превентивна діяльність» іноді трактується нетипово – не лише як попередження правопорушень, а й як запобігання виникненню кризових або несприятливих станів у певній сфері адміністрування чи управлінському процесі [146; 147]. Водночас у межах адміністративно-правової науки доцільно зберігати класичне розуміння превентивної діяльності – як системи заходів, спрямованих на попередження вчинення правопорушень, що реалізується насамперед

Національною поліцією України та іншими суб'єктами публічної адміністрації. Такий підхід узгоджується із загальною концепцією безпеки, у якій превенція виступає не лише інструментом охорони правопорядку, а й важливим чинником формування правової свідомості та підвищення рівня довіри до держави.

У контексті нашого предмета дослідження – адміністративно-правового реагування та запобігання інформаційним загрозам – концепція превентивної діяльності, запропонована О. Проневичем, набуває особливої актуальності. Вона вимагає переходу від виключно реактивної моделі протидії інформаційним правопорушенням до системи попереджувальних заходів, зорієнтованих на раннє виявлення і нейтралізацію загроз у цифровому середовищі.

Превентивний складник адміністративно-правового механізму в інформаційній безпеці полягає у створенні правових, організаційних і технологічних умов, що унеможливлюють негативний інформаційний вплив на суспільство. Це передбачає постійний моніторинг інформаційного простору, аналітичну оцінку ризиків, просвітницьку роботу серед населення, підвищення рівня медіаграмотності й інформаційної культури громадян.

Важливою рисою такого підходу є співпраця органів публічної адміністрації з громадянським суспільством, експертними спільнотами та представниками ІТ-сектору. Саме через інтеграцію державних і недержавних ресурсів можливо забезпечити комплексний моніторинг, оперативне реагування на кіберінциденти та ефективне поширення достовірної інформації.

У межах нашого дослідження превентивна діяльність розглядається як ключовий напрям адміністративно-правового реагування на інформаційні загрози, який поєднує правове регулювання, управлінську координацію та соціальну комунікацію. Її метою є не лише усунення наслідків інформаційних атак, а й створення стійкої системи інформаційної безпеки держави, що

ґрунтується на принципах відкритості, законності, партнерства та довіри між владою і суспільством.

Функціональну реалізацію цього механізму здійснюють урядова команда реагування на комп'ютерні надзвичайні події CERT-UA, Національний координаційний центр кібербезпеки при РНБО України, Служба безпеки України та Державна служба спеціального зв'язку та захисту інформації України. CERT-UA, як визначено виконує функції з ідентифікації, обліку, класифікації та інформування про кіберінциденти, а також забезпечує міжнародну координацію з аналогічними структурами (FIRST, ENISA).

Разом із тим, аналіз чинної нормативної бази свідчить про відсутність єдиного регламенту обміну даними про кіберінциденти між суб'єктами системи кібербезпеки, що призводить до дублювання дій і зниження оперативності реагування. Окремої уваги заслуговує той факт, що на сьогодні вже діє Наказ Служби безпеки України та Міністерства внутрішніх справ України від 13 жовтня 2022 р. № 360/657, яким затверджено Порядок електронної інформаційної взаємодії Служби безпеки України, Міністерства внутрішніх справ України та центральних органів виконавчої влади, діяльність яких спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України [148]. Зазначений нормативний акт визначає організаційно-технічні засади обміну інформацією між відповідними суб'єктами, встановлює вимоги до форматів електронних даних, способів їх захисту, а також процедури фіксації, зберігання та обліку інформаційних запитів.

Дія цього Порядку є міжвідомчо обмеженою, оскільки регламентує інформаційну взаємодію лише між СБУ, МВС та підпорядкованими йому центральними органами виконавчої влади. У сучасних умовах цифрової трансформації та зростання масштабів кіберзагроз виникає необхідність створення єдиного нормативного механізму координації інформаційних потоків між усіма ключовими суб'єктами національної системи кібербезпеки – СБУ,

Державною службою спеціального зв'язку та захисту інформації України, Міністерством внутрішніх справ, Міністерством цифрової трансформації та Національним координаційним центром кібербезпеки при РНБО України.

Доцільно ухвалити постанову Кабінету Міністрів України, яка встановить порядок інформаційної взаємодії між зазначеними органами, унормувавши формати, періодичність і технічні стандарти обміну аналітичними даними, а також визначила єдині протоколи реагування на виявлені кіберінциденти. Це дозволило б забезпечити системність і оперативність у сфері адміністративно-правового реагування на інформаційні загрози, посилити міжвідомчу координацію та уникнути дублювання функцій.

Наступним напрямом превентивної діяльності є аудит стану кіберзахисту, що охоплює оцінювання рівня інформаційної безпеки державних органів, підприємств та операторів критичної інфраструктури. Відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 р. № 80/94-ВР [149], власники систем зобов'язані впроваджувати заходи технічного й криптографічного захисту інформації, а контроль за їх реалізацією здійснює ДССЗЗІ.

Відповідно до Положення про ДССЗЗІ до її повноважень належить проведення державної експертизи у сфері технічного захисту інформації, атестація об'єктів і розроблення нормативів безпеки. Практична реалізація аудиту полягає у виявленні вразливостей, тестуванні систем на проникнення, перевірці ефективності політик кіберзахисту, що дає змогу виявляти загрози до їх фактичного прояву.

Водночас законодавство України не містить норм, які б встановлювали обов'язковість регулярного аудиту для всіх суб'єктів критичної інфраструктури, як це передбачено в законодавстві Європейського Союзу. У зв'язку з цим доцільно передбачити в національному законодавстві вимогу щодо проведення

періодичного аудиту інформаційної безпеки не рідше одного разу на два роки та затвердити єдині державні стандарти його здійснення.

Сучасний етап розвитку інформаційних технологій зумовлює необхідність запровадження аналітичних систем прогнозування ризиків і кіберзагроз. Нормативне підґрунтя напряму – у Концепції розвитку цифрової економіки й суспільства України (розпорядження Кабінету Міністрів України від 17 січня 2018 р. № 67-р) [150], що передбачає створення механізмів управління ризиками на основі аналізу великих даних (Big Data) й інструментів штучного інтелекту.

Проте аналіз чинної правової бази засвідчує відсутність нормативно визначеного статусу аналітичних центрів прогнозування кіберзагроз, а також юридичних вимог до формування національної системи ризик-менеджменту у сфері інформаційної безпеки. З метою підвищення ефективності превентивних механізмів доцільно передбачити створення державної системи прогнозного аналізу кіберзагроз на базі НКЦК при РНБО України за аналогією до Європейської системи раннього попередження. Такі аналітичні інструменти мають забезпечувати оцінювання тенденцій розвитку кіберзагроз, прогнозування потенційних атак на критичні об’єкти, формування сценаріїв реагування та надання пропозицій органам влади щодо запобіжних дій.

Важливою складовою превентивної політики є формування цифрової компетентності та культури безпеки населення, що безпосередньо впливає на стійкість інформаційного середовища. У Стратегії кібербезпеки України (2021 р.) [107] зазначено, що підвищення рівня цифрової грамотності є одним з ключових завдань національної системи кіберзахисту.

Зазначений напрям реалізується через державну програму «Дія. Цифрова освіта», а також через Концепцію розвитку цифрових компетентностей (розпорядження КМУ від 23 грудня 2020 р. № 1642-р) [151]. Утім, зазначені акти мають переважно рекомендаційний характер і не містять імперативних приписів

щодо підготовки державних службовців та працівників сектору безпеки з питань інформаційної безпеки.

З огляду на це доцільно передбачити в Законах України «Про державну службу» та «Про службу в органах місцевого самоврядування» положення про обов'язкове проходження курсів підвищення кваліфікації з кібербезпеки, що сприятиме формуванню єдиної професійної культури інформаційної безпеки серед представників публічної адміністрації.

Превентивні адміністративно-правові механізми є системоутворювальним елементом державної політики забезпечення інформаційної безпеки. Вони охоплюють інформаційний моніторинг і раннє виявлення загроз; аудит стану кіберзахисту; прогнозування ризиків і моделювання кіберзагроз; підвищення цифрової грамотності як елемент соціальної стійкості.

Водночас нормативна база, що регламентує реалізацію цих механізмів, потребує подальшого вдосконалення, зокрема в частині уніфікації процедур міжвідомчої взаємодії, встановлення єдиних стандартів аудиту інформаційної безпеки, закріплення механізмів прогнозного аналізу та правового статусу аналітичних центрів.

Посилення превентивного складника дозволить забезпечити перехід від реактивної до проактивної моделі державного управління кібербезпекою, що відповідає принципам сталості, інтегрованості та відповідальності, визначеним у європейських стандартах.

Якщо превентивні адміністративно-правові механізми спрямовані на упередження та мінімізацію ризиків інформаційних загроз, то оперативно-реагувальні – забезпечують безпосереднє реагування держави на вже реалізовані кіберінциденти, відновлення стабільності інформаційного середовища та нейтралізацію наслідків порушень. Таким чином, обидва блоки механізмів взаємопов'язані: превентивні – формують потенційну стійкість системи, тоді як реагувальні – забезпечують її функціональну живучість у кризових ситуаціях.

Оперативно-реагувальні механізми є динамічним елементом системи адміністративно-правового забезпечення кібербезпеки, що активізується у разі фіксації інформаційних атак, кібершпигунства, дезінформаційних кампаній або порушень у функціонуванні критичної інформаційної інфраструктури. Їх зміст розкривається через правові, організаційні та технічні дії уповноважених органів, спрямовані на локалізацію загроз, відновлення працездатності інформаційних систем та притягнення винних осіб до відповідальності.

Оперативно-реагувальні механізми реалізуються завдяки комплексу правових, організаційних і техніко-процедурних дій, спрямованих на локалізацію кіберінцидентів, нейтралізацію загроз і відновлення цілісності інформаційного середовища. Їхня структура охоплює декілька взаємопов’язаних компонентів.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» [47], Служба безпеки України, Департамент кіберполіції, Державна служба спеціального зв’язку та захисту інформації, а також Національний координаційний центр кібербезпеки забезпечують спільні дії з ідентифікації, локалізації та усунення наслідків кіберінцидентів. Такі заходи включають ізоляцію уражених сегментів мережі, блокування каналів несанкціонованого доступу, ліквідацію шкідливого програмного забезпечення, а також технічне відновлення працездатності інформаційних систем.

Практика реагування на масштабні кібератаки, зокрема NotPetya (2017) та Industroyer2 (2022), продемонструвала ефективність міжвідомчої координації між суб’єктами кібербезпеки, проте виявила дефіцит єдиного оперативного центру кризового управління, здатного забезпечити централізоване управління реагуванням у реальному часі. Створення центру є нагальною потребою з огляду на зростання складності та гібридного характеру сучасних інформаційних атак.

Перед початком широкомасштабної збройної агресії Російської Федерації проти України кібератаки були чітко скоординованими. 14 січня 2022 р. на державні органи та установи України було спрямовано шкідливе програмне

забезпечення WhisperGate, яке маскувалося під програму-вимагач, однак мало на меті знищення критично важливих даних, подібно до механізмів NotPetya. Уже 23 лютого 2022 р. щонайменше п’ять українських організацій стали жертвами HermeticWiper, додаткові компоненти – HermeticWizard і HermeticRansom – поширювалися для ускладнення процесів відновлення систем [152].

Наведені приклади засвідчують, що локалізаційно-усувальні заходи мають технічний та адміністративно-правовий вимір. Їх ефективність залежить від оперативності ухвалення управлінських рішень, узгодженості дій між суб’єктами публічної адміністрації, а також від наявності нормативно визначених процедур кризового реагування. Відтак доцільним є прийняття комплексного підзаконного акта, який би унормував порядок координації локалізаційно-усувальних заходів, визначив би чіткі етапи, відповідальних суб’єктів, терміни реагування та механізми обміну аналітичними даними між органами системи кібербезпеки.

Контентно-блокувальні заходи. Закон «Про інформацію» [76] дозволяє обмеження доступу до ресурсів, поширення яких може завдати шкоди національній безпеці. Такі рішення, ухвалені РНБО й уведені в дію указами Президента, застосовуються для нейтралізації інформаційно-психологічних операцій та ворожої пропаганди. Однак відсутність спеціального закону про процедури обмеження контенту в кіберпросторі зумовлює ризики надмірного втручання в інформаційну свободу. З огляду на це, доцільним є нормативне врегулювання пропорційності таких заходів із закріпленням судового контролю.

Згідно з постановою Кабінету Міністрів України № 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури» [153], суб’єкти критичної інформаційної інфраструктури зобов’язані реалізовувати комплекс технічних і адміністративних дій із відновлення працездатності інформаційних систем, документування наслідків кіберінциденту та звітування до CERT-UA. Такі заходи спрямовані на забезпечення неперервності державного

управління та стабільного функціонування життєво важливих галузей, зокрема фінансової, енергетичної, транспортної, комунальної та оборонної сфер.

Відновлювальні дії охоплюють поетапне відновлення критичних сервісів, перевірку цілісності резервних копій, впровадження оновлених політик безпеки й аналіз причин інциденту для запобігання повторним атакам. З огляду на це доцільним є розроблення стандарту адміністративних дій з відновлення кіберстійкості, що поєднає технічні вимоги, нормативні приписи та організаційні процедури реагування у межах єдиної системи кіберзахисту держави.

Оперативно-реагувальні адміністративно-правові механізми є невід'ємною складовою системи інформаційної безпеки держави, що забезпечує її здатність до швидкого відновлення після кіберінцидентів і підтримання функціональної безперервності інформаційної інфраструктури. Ефективність залежить від рівня нормативної деталізації, міжвідомчої координації і технологічної модернізації.

Юрисдикційні механізми відіграють правовідновлювальну та каральну роль у системі реагування на інформаційні загрози. Їх сутність полягає у притягненні винних осіб до адміністративної відповідальності за правопорушення у сфері інформаційної безпеки, а також у відновленні порушених прав суб'єктів інформаційних відносин.

Адміністративна відповідальність є ефективним засобом реагування на правопорушення у сфері інформаційної безпеки. Вона реалізується через механізми притягнення порушників до відповідальності шляхом накладення штрафів, застосування адміністративного арешту, попереджень тощо, що виконує як каральну, так і превентивну функцію [154; 155]

Крім притягнення до відповідальності, юрисдикційні механізми охоплюють контрольні та наглядові функції – перевірку дотримання вимог інформаційної безпеки органами державної влади, суб'єктами господарювання та провайдерами послуг зв'язку. Їх ефективне застосування сприяє утвердженню

принципу невідворотності відповідальності та забезпеченню дисципліни у сфері поводження з інформаційними ресурсами.

До важливих адміністративно-правових інструментів належать також механізми ліцензування та дозвільної діяльності. Вони забезпечують допуск до окремих видів діяльності лише тих суб'єктів, які відповідають визначеним критеріям безпеки, зокрема під час обробки конфіденційної чи захищеної інформації. Водночас системна робота з інформування та навчання кадрів є передумовою ефективного функціонування всієї системи інформаційної безпеки. Проведення освітніх заходів, професійної перепідготовки й підвищення кваліфікації персоналу сприяє зменшенню кількості кіберінцидентів та загроз людського фактору. Окреме місце посідає сертифікація технічних і програмних засобів захисту інформації, діяльності, пов'язаної із забезпеченням охорони державної таємниці. Це має бути максимально жорстко регламентованим та контрольованим з боку держави, оскільки йдеться про національну безпеку [155].

Реєстраційний метод, у свою чергу, виступає складовою контрольно-наглядової діяльності виконавчої влади. Наприклад, згідно зі ст. 4 Закону України «Про друковані засоби масової інформації (пресу) в Україні», державна реєстрація ЗМІ є обов'язковою передумовою для початку їхньої діяльності. Процедура включає подання заяви, її розгляд протягом встановленого терміну, ухвалення рішення про реєстрацію або відмову, а також повідомлення про виявлені недоліки в документах [154; 155].

Отже, адміністративно-правові механізми реагування на інформаційні загрози становлять комплексну систему, у якій кожен вид виконує окрему, але взаємопов'язану функцію: превентивні забезпечують своєчасне попередження загроз та підвищення кіберстійкості; оперативно-реагувальні гарантують швидке усунення наслідків інцидентів і відновлення функціонування систем; юрисдикційні формують правову основу невідворотності відповідальності й підтримання правопорядку в інформаційному просторі.

Їх інтеграція в єдиний державний механізм забезпечує ефективну реалізацію принципів законності, пропорційності та балансу між захистом національної безпеки й дотриманням прав людини у цифровому середовищі.

ВИСНОВКИ ДО РОЗДІЛУ 2

У другому розділі дисертації досліджено адміністративно-правові механізми забезпечення національної безпеки у публічно-інформаційній сфері. У межах розділу розкрито функціональну роль органів публічної влади у формуванні та реалізації державної політики інформаційної безпеки, проаналізовано діяльність правоохоронних органів у протидії загрозам інформаційного характеру, схарактеризовано механізми адміністративно-правового реагування на шкідливі інформаційні впливи.

1. Уточнено понятійний апарат, відповідно до якого суб’єкти публічної влади у публічно-інформаційній сфері національної безпеки обґрунтовано як інтегровану систему державних, самоврядних і недержавних інституцій, наділених публічно-правовою компетенцією та інструментами впливу. Така концептуалізація забезпечує цілісне бачення розподілу відповідальності за захист інформаційного простору, мінімізує можливі прогалини між рівнями влади та створює передумови для скоординованої безпекової політики.

2. Розкрито трирівневу структуру управління у сфері інформаційної безпеки (стратегічно-керівний, операційно-виконавчий і суспільно-громадський рівні) з чітким визначенням функцій, підзвітності та каналів взаємодії кожного рівня. Така архітектура переводить управління від інституційної роз’єднаності до керованої координації, забезпечує послідовність рішень і створює організаційне підґрунтя для єдиного циклу державного планування, включно зі щорічним урядовим планом, визначеним через показники результативності (KPI).

3. Посилено суспільний вимір безпеки шляхом обґрунтування підвищення інституційної ваги Центру стратегічних комунікацій та інформаційної безпеки.

Запропоновано надання йому міжвідомчого статусу, встановлення прямої підзвітності Кабінету Міністрів, створення платформи вироблення стратегічних наративів і впровадження системних програм з медіаграмотності. Такий підхід закріплює whole-of-society security approach і формує стійкість суспільства до дезінформаційних впливів на стратегічному рівні.

4. Визначено роль правоохоронних органів як інтегрованого складника державного механізму кіберзахисту. Показано, що їхня діяльність поєднує контррозвідувальні, профілактичні, аналітичні та техніко-оперативні напрями, які забезпечують охоплення всіх етапів захисту інформаційного середовища — від виявлення та моніторингу загроз до їх нейтралізації та мінімізації наслідків.

5. Удосконалено наукове тлумачення компетенцій Служби безпеки України, Національної поліції та Державної служби спеціального зв'язку та захисту інформації шляхом уточнення їхніх функцій, рівнів відповідальності й зон взаємодії. Запропоновано диференціацію повноважень між аналітичним, оперативним і технічним рівнями забезпечення безпеки, що сприяє підвищенню ефективності міжвідомчої координації.

6. Дістало подальшого розвитку обґрунтування необхідності переходу від реактивної до превентивної моделі діяльності правоохоронних органів у сфері кіберзахисту. Запропоновано впровадження національної системи раннього виявлення кіберінцидентів, інтегрованої з аналітичними платформами сектору безпеки, а також створення єдиного прогнозно-аналітичного центру оцінювання інформаційних ризиків, спроможного формувати проактивні рекомендації для державної політики.

7. Виявлено основні проблеми правового регулювання: фрагментарність компетенцій між суб'єктами інформаційної безпеки, недостатню правову визначеність статусу Департаменту кіберполіції, а також обмежену прозорість діяльності СБУ у сфері кібербезпеки. Аргументовано важливість законодавчого закріплення механізмів парламентського контролю й публічної звітності.

8. Запропоновано напрями вдосконалення правового та організаційного забезпечення, зокрема нормативне розмежування повноважень між СБУ, Національною поліцією, ДССЗЗІ та Мінцифрою; гармонізацію нормативно-технічних стандартів з вимогами ISO/IEC та NIS2; розбудову міжвідомчої системи обміну інформацією; запровадження незалежного аудиту кіберзахисту.

9. Визначено структуру адміністративно-правових механізмів реагування на інформаційні загрози, що включає превентивні, оперативно-реагувальні та юрисдикційні компоненти. Така структура дозволяє розглядати інформаційну безпеку як багаторівневу систему державного управління з узгодженими функціями кожного механізму.

10. Розкрито зміст превентивних механізмів, які охоплюють інформаційний моніторинг, аудит інформаційних систем, прогнозування ризиків і розвиток цифрової грамотності населення. Доведено, що превентивна модель забезпечує проактивне управління ризиками та формує кіберстійкість держави.

11. Схарактеризовано оперативно-реагувальні механізми як комплекс правових, організаційних і технічних дій, спрямованих на локалізацію, усунення та мінімізацію наслідків інформаційних інцидентів. Обґрунтовано потребу у створенні єдиного кризового центру реагування на кіберзагрози для координації дій СБУ, ДССЗЗІ, Кіберполіції, Мінцифри та НКЦК при РНБО України.

12. Удосконалено підхід до формування єдиного адміністративно-правового механізму забезпечення інформаційної безпеки держави, що поєднує нормативні, організаційні та технологічні засоби реагування. Підкреслено, що його ефективність можлива лише за умов міжвідомчої координації, підзвітності органів сектору безпеки, гармонізації законодавства з європейськими стандартами та дотримання принципу верховенства права у цифровому середовищі.

РОЗДІЛ 3
ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ВДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ У ПУБЛІЧНО-ІНФОРМАЦІЙНІЙ СФЕРІ

3.1. Досвід зарубіжних країн у забезпеченні національної безпеки у публічно-інформаційній сфері

У сучасних умовах глобалізації, динамічного розвитку цифрових технологій і поширення гібридних загроз питання інформаційної безпеки постає як пріоритетне у системі національної безпеки кожної держави. Вивчення зарубіжного досвіду дозволяє окреслити ефективні моделі, що забезпечують стійкість інформаційного простору, та окреслити вектори подальшого розвитку для країн, які прагнуть адаптувати ці практики, зокрема для України [156].

Однією з найрозвиненіших є модель Сполучених Штатів Америки, яка ґрунтується на інтеграції зусиль державних, військових та приватних структур у межах уніфікованої стратегії. Основними інституціями є Департамент внутрішньої безпеки (DHS), Національне агентство з безпеки (NSA) та Командування кіберпростору США (USCYBERCOM). Ці органи забезпечують координацію заходів щодо захисту критичної інфраструктури, інформаційних систем, а також протидію зовнішньому втручанню в демократичні процеси. У США існує розвинена система стратегічних комунікацій, що забезпечує оперативне реагування на спроби дезінформації. Законодавчо закріплено принципи кібергігієни, відповідальність цифрових платформ, а також налагоджено ефективну міжвідомчу взаємодію. Особливої уваги заслуговує масштабне фінансування досліджень у сфері штучного інтелекту, який застосовується для автоматизованого аналізу інформаційних потоків, виявлення аномалій і загроз у реальному часі.

Система забезпечення інформаційної безпеки США є однією з найрозвиненіших у світі, що зумовлено як історичними передумовами, так і сучасними викликами цифрової доби. Її формування розпочалося з ухвалення Закону про національну безпеку США 1947 року, який заклав основи створення нормативної бази для діяльності у сфері національної розвідки, захисту інформації та кіберпростору [165].

У США сформовано широку систему стандартів, таких як Федеральний стандарт обробки інформації (FIPS), який визначає технічні вимоги до криптографічного захисту державних інформаційних систем. Такий підхід забезпечує законодавче підґрунтя для впровадження надійних засобів інформаційного захисту, що є фундаментом безпечного функціонування цифрової економіки та державного управління.

Розвиток цифрових технологій зробив США світовим лідером в електронному врядуванні, але водночас – об'єктом масштабних кібератак, які здатні впливати не лише на національну, а й глобальну економічну та політичну стабільність, тому захист конфіденційної інформації, персональних даних, державних і комерційних секретів розглядається як стратегічний пріоритет національної безпеки [165].

В управлінні кібербезпекою беруть участь численні державні інституції, зокрема: Федеральне агентство з кібербезпеки та інфраструктурної безпеки (CISA); Агентство національної безпеки (NSA); Федеральне бюро розслідувань (FBI); Міністерство оборони (DoD); Рада національної безпеки (NSC).

Ключову роль відіграє Агентство національної безпеки (АНБ), створене у 1952 р., яке займається збором, аналізом і захистом розвідувальної інформації, а також розробкою криптографічних стандартів і протоколів для безпечного обміну даними між урядом, союзниками по НАТО й міжнародними партнерами. В структурі АНБ функціонує Управління розвідки сигналів (SIGINT), що

забезпечує моніторинг електронних сигналів, а також Центральна служба безпеки (CH/CSS), яка координує діяльність у сфері військової криптографії.

Важливою складовою інформаційної політики США є освітній та науково-технічний напрям. АНБ активно співпрацює з університетами та науковими центрами. Прикладом є Консорціум з дослідження інформаційної безпеки та політики (CRISP), створений спільно зі Стенфордським університетом. Цей проєкт став платформою для наукових досліджень та розробки механізмів захисту критичної інформаційної інфраструктури [165].

США приділяють значну увагу міжнародному співробітництву у сфері інформаційної безпеки. Як член НАТО, країна бере участь у створенні спільних стратегій та навчань з кіберзахисту, зокрема у роботі Центру передових технологій кібероборони (CCDCOE) в Естонії. На саміті НАТО у Вільнюсі (2023) США підтримали розширення спроможностей Альянсу щодо реагування на кіберінциденти (VCISC), підкресливши важливість колективної кіберстійкості.

Окрім того, США розвивають партнерства з ЄС, Ізраїлем, Японією, Південною Кореєю та Австралією, що дозволяє обмінюватися технологіями, досвідом і стандартами кіберзахисту. Така міжнародна інтеграція формує єдину систему протидії глобальним інформаційним загрозам.

З-поміж основних напрямів інформаційної політики США варто виокремити:

1. Розвиток сильного національного кіберзахисту шляхом інвестицій у технології виявлення й нейтралізації загроз.
2. Співпрацю на міжнародному рівні для створення єдиних стандартів кібербезпеки.
3. Підготовку кваліфікованих кадрів через систему освіти, сертифікацій і стажувань.
4. Боротьбу з кіберзлочинністю у взаємодії з іншими державами та приватним сектором.

5. Систему оперативного реагування на кібератаки з метою мінімізації наслідків для критичної інфраструктури.

Досвід США демонструє, що ефективне забезпечення національної безпеки у публічно-інформаційній сфері потребує поєднання правових, технічних, освітніх та міжнародно-координаційних механізмів. Саме комплексний, інституційно інтегрований підхід дозволив США вибудувати найпотужнішу систему кіберзахисту у світі, яка є орієнтиром для інших держав.

Європейський Союз реалізує модель гармонізації підходів до інформаційної безпеки на рівні держав-членів. У 2001 році Європейська Комісія представила перший документ під назвою «Мережева та інформаційна безпека: європейський політичний підхід» [156; 157; 158]. Цей документ, презентований Європейською Комісією у 2001 році, став важливим кроком у формуванні загальноєвропейської стратегії забезпечення інформаційної безпеки. У ньому було визначено основні проблеми, що виникають у зв'язку з інформаційною безпекою, та запропоновано політичний підхід до їх розв'язання на рівні ЄС.

Документ заклав фундамент для подальших ініціатив і розробок у цій сфері, ставши своєрідним орієнтиром для держав-членів ЄС у побудові їхніх національних стратегій. Основні ідеї та підходи, викладені в документі, стали базисом для розроблення подальших політик та нормативних актів у сфері мережевої та інформаційної безпеки в ЄС. Вони вплинули на створення такої ініціативи, як Директива про безпеку мережевих та інформаційних систем (NIS Directive), яку прийнято у 2016 р. і яка зобов'язує держави-члени ЄС впроваджувати мінімальні стандарти кібербезпеки на національному рівні [157; 158]. У межах ЄС активно впроваджуються програми підвищення цифрової грамотності громадян, а також інтегруються модулі інформаційної безпеки до системи загальної та вищої освіти. Особливе значення надається прозорості державної політики, доступу громадян до інформації і громадському контролю.

Франція трактує інформаційну безпеку як невід'ємну складову стратегії національної безпеки. Основи цієї політики викладені у так званих Білих книгах оборони та національної безпеки. З 1972 р. у документах послідовно розвивається концепція інтегрованої безпеки, що охоплює як оборонний, так і цивільний виміри. Після завершення холодної війни акценти змістилися на зовнішні військові операції, професіоналізацію армії та інформаційну безпеку. У Білій книзі 2008 року вперше докладно проаналізовано загрози, що походять від кіберзлочинності, масштабних атак на інформаційні системи, використання ЗМІ та інтернету як інструментів маніпуляції, шпіонажу та стратегічного впливу.

Франція має один із найрозвиненіших у Європі підходів до правового регулювання інформаційної безпеки та протидії дезінформації, що є складовою системи забезпечення національної безпеки у публічно-інформаційній сфері. Французький законодавець ще наприкінці XIX століття визнав небезпеку поширення неправдивих повідомлень для суспільства. Зокрема, Закон про свободу преси від 29 липня 1881 р. (Loi sur la liberté de la presse) містить ст. 27, яка встановлює кримінальну відповідальність за оприлюднення або поширення фальшивих новин (nouvelles fausses), що здатні порушити громадський порядок. За такі дії передбачено штраф у розмірі 45 000 євро, а якщо дезінформація створює загрозу моральному стану чи дисципліні армії або перешкоджає оборонним зусиллям держави – до 135 000 євро.

Попри суворість норм, експерти наголошують, що довести безпосередній зв'язок між публікацією та порушенням громадського спокою доволі складно, тому ці положення застосовуються обмежено [164].

Важливим складником сучасного французького правового механізму інформаційної безпеки є Закон про довіру в цифровій економіці (Loi pour la confiance dans l'économie numérique, LCEN), ухвалений 21 червня 2004 р. Він визначає правові засади боротьби з незаконним контентом в Інтернеті, зокрема з матеріалами, що розпалюють ненависть або дискримінацію. Закон надає судовим

органам повноваження вимагати видалення з цифрового простору інформації, яка порушує національне законодавство [164].

Новий етап розвитку інформаційної безпеки Франції пов'язаний із прийняттям у 2015 р. Національної стратегії цифрової безпеки (Stratégie nationale pour la sécurité du numérique). У ній підкреслено, що цифрові платформи та соціальні мережі можуть суттєво впливати на формування суспільної думки, а також використовуватися для поширення дезінформації та пропаганди, що загрожує основоположним інтересам держави. Діяльність таких платформ підпадає під дію норм законодавства про національну безпеку та оборону [164].

Французька стратегія кібербезпеки базується на п'яти стратегічних цілях, спрямованих на формування «цифрової республіки» з високим рівнем довіри та захисту інформаційного простору:

1. Захист основоположних національних інтересів у кіберпросторі, зокрема державних інформаційних систем і критичної інфраструктури.
2. Забезпечення конфіденційності та захисту персональних даних, розроблення вітчизняних продуктів для кіберзахисту та надання правової і технічної допомоги.
3. Підвищення рівня кіберграмотності населення і зміцнення національного потенціалу у сфері кібербезпеки.
4. Формування сприятливого середовища для ІКТ-бізнесу, інновацій та інвестицій у сферу цифрових технологій.
5. Розроблення «дорожньої карти» для досягнення європейської цифрової автономії, що дозволяє зменшити залежність від зовнішніх технологічних впливів.

Загалом у Франції діє розгалужена інституційна система: ANSSI координує заходи з кіберзахисту, DISIC відповідає за державні комунікації, а спеціалізовані служби займаються контрпропагандою та інформаційною протидією [156; 159, с. 189].

Французький досвід демонструє ефективну інтеграцію правових, технологічних і освітніх інструментів у забезпечення інформаційної безпеки. Він може бути корисним для України при формуванні власної системи протидії дезінформації та гібридним загрозам у публічно-інформаційній сфері.

Естонію визнано однією з найрозвиненіших країн Європи у сфері кіберзахисту та інформаційної безпеки, зокрема серед держав Балтії. Цей статус вона здобула завдяки послідовній державній політиці у сфері цифрової безпеки, яка поєднує законодавчі, організаційні та технологічні механізми забезпечення стійкості до кіберзагроз.

Одним із перших кроків Естонії у цьому напрямі стало ухвалення Національної стратегії кібербезпеки, яка була інтегрована в міжнародно-правові рамки. Уже у 2014 р. уряд прийняв оновлений документ – «Cyber Security Strategy 2014–2017», що визначив стратегічні пріоритети держави у цій сфері. Як зазначає Звоздецька, основними цілями стратегії стали створення багаторівневої системи безпекових заходів, з особливим акцентом на захист критичної інформаційної інфраструктури та формування правового регулювання кіберпростору. Така модель забезпечує цілісність архітектури національної безпеки, сприяє впровадженню інноваційних технологій і підвищує ефективність використання інформаційно-комунікаційних систем у державному управлінні [167].

До 2011 р. політика у сфері кібербезпеки координувалася Міністерством оборони Естонії, однак після цього відповідальність була передана Міністерству економічних питань та комунікацій, що підкреслило перехід від виключно оборонного підходу до комплексного – публічно-управлінського. Саме в структурі цього міністерства діє Управління інформаційних систем Естонії (EISA), створене у 2011 р. Воно охоплює низку підрозділів, відповідальних за різні напрями кіберзахисту:

– Департамент із захисту критичних інформаційних інфраструктур (CIIP);

– Інфраструктуру відкритих ключів (PKI), що забезпечує надійність цифрових підписів і аутентифікацію;
– Центр обміну документами (DEC);
– IT-інфраструктуру, яка гарантує безперервність роботи державних інформаційних систем навіть у кризових ситуаціях.

Важливу роль у координації міжвідомчої діяльності відіграє Рада з кібербезпеки Естонії, створена при урядовому Комітеті з питань безпеки. Вона забезпечує стратегічне узгодження дій між різними органами державної влади.

Ключовою інституцією оперативного реагування стала CERT Estonia, утворена ще у 2006 році, яка відповідає за управління кіберінцидентами. Вона є однією з найефективніших структур такого типу в Європі, адже поєднує державний і приватний сектори у виявленні та ліквідації кіберзагроз [167].

Подальше зміцнення міжнародної взаємодії Естонії у сфері кібербезпеки відбулося після створення у 2008 році в місті Таллінн Центру передового досвіду НАТО з кіберзахисту (NATO CCDCOE). Ця міждержавна військова організація стала науково-аналітичним та освітнім хабом, який займається підготовкою фахівців, розробкою навчальних програм і моделюванням кібервійськових операцій. Визнання кіберпростору операційним середовищем НАТО означало прирівняння кіберзагроз до військових викликів, що заклало підґрунтя для інтеграції цифрової оборони в систему колективної безпеки [167].

Безсумнівно, досвід Естонії демонструє, що ефективне забезпечення національної безпеки у публічно-інформаційній сфері потребує інституційної координації, міжнародної співпраці та безперервного розвитку людського капіталу. Естонська модель побудована на взаємодії державних структур, громадянського суспільства й технологічних компаній, що дозволяє підтримувати високий рівень кіберстійкості. Для України цей досвід є надзвичайно цінним, оскільки доводить, що безпека інформаційного простору

має формуватися як комплексна політика, де оборонний, економічний і освітній аспекти діють у взаємозв'язку.

Республіка Польща послідовно приділяє значну увагу розбудові системи інформаційної безпеки як на рівні державного управління, так і в приватному секторі. Формування відповідної правової та організаційної основи відбувалося поступово – від концепцій корпоративної безпеки до комплексного підходу, орієнтованого на захист інформаційного простору держави.

Ще на початку 2000-х років польські науковці, зокрема Л. Кільтика, акцентували на необхідності вдосконалення управління інформаційною безпекою у різних організаціях, звертаючи увагу на потребу стандартизації процедур захисту інформації, запровадження нормативно-правових механізмів і розробку політик багаторівневої безпеки. Подальший імпульс розвитку системи інформаційного захисту був наданий після впровадження міжнародного стандарту ISO/IEC 27001:2005, що визначив вимоги до систем управління інформаційною безпекою на основі оцінки ризиків. Польські дослідники Я. Лучак і М. Тибурський слушно відзначали, що зростання обсягів обробки даних і динамічний розвиток інформаційних технологій потребують від держави системного підходу до управління інформацією, який би враховував не лише технологічні, а й правові та соціальні ризики [166].

З огляду на конституційні положення Республіки Польща (зокрема ст. 47 і 51 Конституції 1997 р.), що гарантують право на приватність, захист честі та персональних даних, інформаційну безпеку розглядають складником правового статусу особи. Такий підхід є основою для розбудови цілісної національної моделі захисту інформаційного простору в персональному й публічному вимірі.

Новий етап розвитку польської інформаційної політики настав із прийняттям Стратегії національної безпеки Республіки Польща від 20 травня 2020 року, яка визнає інформаційну та кібербезпеку невід'ємними складовими національної безпеки. У документі зазначено, що держава забезпечує умови для

реалізації національних інтересів – зокрема незалежності, безпеки громадян, дотримання прав і свобод людини, верховенства права та міжнародного правопорядку. Важливо, що інформаційній безпеці присвячено два з п'яти підрозділів першого розділу Стратегії, що свідчить про пріоритетність цього напряму у державній політиці [166].

Розділ «Кібербезпека» визначає головну мету – підвищення стійкості державних і приватних інформаційних систем до кіберзагроз, розвиток національних спроможностей для запобігання, виявлення та реагування на них, а також формування суспільної свідомості у сфері безпечного користування цифровими технологіями. Особливу увагу польський законодавець приділяє людському фактору, визнаючи, що ефективність будь-якої системи кіберзахисту залежить від рівня інформаційної культури громадян.

Шість стратегічних напрямів реалізації політики кібербезпеки Польщі охоплюють:

- зміцнення стійкості державних, військових і приватних інформаційних систем;
- розвиток оборонного потенціалу у кіберпросторі;
- створення умов для ведення повного спектру кібероперацій;
- формування національної інфраструктури тестування й сертифікації рішень у сфері кіберзахисту;
- просування освіти, підвищення обізнаності та компетентностей громадян щодо інформаційних ризиків;
- стимулювання досліджень, інновацій і державно-приватного партнерства у сфері сучасних технологій (зокрема штучного інтелекту, Інтернету речей, мобільних мереж 5G).

П'ятий підрозділ Стратегії – «Інформаційний простір» – визначає мету забезпечення безпечного функціонування держави та громадян у цифровому

середовищі. Польський підхід базується на розумінні інформаційного простору як поєднання віртуального, фізичного та когнітивного вимірів, що дозволяє комплексно реагувати на загрози, зокрема дезінформацію. Серед ключових інструментів реалізації політики – створення єдиної системи стратегічних комунікацій, розвиток механізмів співпраці держави з медіа та громадськими організаціями, а також освітні ініціативи щодо підвищення рівня інформаційної грамотності населення [166].

Досвід Республіки Польща демонструє інтегрований і людиноцентричний підхід до забезпечення інформаційної безпеки, у якому акцент робиться не лише на технологічних рішеннях, але й на формуванні інформаційної культури громадян як основи національної стійкості. Польська модель може бути корисною для України, зокрема у частині розвитку правових механізмів стратегічних комунікацій, освітніх програм з кіберграмотності та взаємодії держави з громадянським суспільством у протидії дезінформації.

У Німеччині правовою основою для формування політики кібербезпеки є Закон про посилення безпеки IT-систем від 2015 р., який закріплює визначення критичної інфраструктури (енергетика, транспорт, охорона здоров’я тощо) та надає Федеральному відомству з безпеки у сфері IT (BSI) провідну роль у захисті державних і приватних цифрових систем. Командування стратегічної розвідки Бундесверу здійснює управління сучасними супутниковими системами SAR-Lupe та SATCOMBw, які забезпечують високоточну розвідку й безпечний зв’язок. Споживче маркування IT-безпеки для комерційних продуктів є свідченням комплексного підходу до безпеки цифрового простору [159, с. 189].

Ізраїль реалізує концепцію активного кіберзахисту, що включає не лише оборону, але й превентивні дії. Тісна інтеграція армії, спецслужб, наукових інститутів і стартапів забезпечує розробку інноваційних рішень, які дозволяють ефективно захищати критичну інфраструктуру.

Сучасна інфраструктура кібербезпеки в Ізраїлі охоплює приблизно 450 компаній, включаючи відомі фірми, такі як «Check Point», а також численні стартапи та венчурні фонди, зокрема «Jerusalem Venture Partners (JVP) Cyber Labs», що активно інвестують у цю галузь. Крім того, значну роль відіграють науково-дослідні проєкти, які сприяють співпраці між високотехнологічними компаніями та дослідницькими центрами [161, с. 79]

У 2017 р. інвестиції у сферу кіберзахисту в Ізраїлі становили 10,8 мільйона доларів, що на 26% більше порівняно з 2016 р. Нині Ізраїль є другим за обсягом експортером програмного забезпечення після США, тобто Ізраїль перетворюється на міжнародний центр високих технологій і найперше стає одним із провідних світових лідерів у галузі кібербезпеки [162, с. 79; 162].

У червні 2018 р. Ізраїльський національний кібердиректорат (INCD) оприлюднив проєкт закону про кібербезпеку для обговорення громадськістю. Цей проєкт закону спрямований на регулювання діяльності INCD відповідно до рішень уряду та є завершальною стадією створення національної кібербезпекової структури. Документ складається з трьох основних розділів: 1) організаційний розділ визначає структуру та організаційні аспекти INCD; 2) оперативний розділ описує повноваження щодо виявлення та реагування на кібератаки; 3) регуляторний розділ встановлює національні та секторальні регуляції, спрямовані на підвищення стійкості різних секторів та визначає роль INCD як національного регулятора у сфері кібербезпеки [161, с. 79; 7].

Очевидно, що ізраїльська модель кібербезпеки є прикладом ефективного синтезу державної політики, технологічного розвитку й стратегічного мислення, оскільки ґрунтується на активному, а не реактивному підході до кіберзагроз, що дозволяє Ізраїлю швидко реагувати на атаки та запобігати потенційним загрозам.

Протягом 2019-2020 рр. INCD провів понад 30 зустрічей із зацікавленими сторонами, установами та урядовими міністерствами для обговорення коментарів щодо цього проєкту закону. На основі обговорень у березні 2021 р.

опубліковано доопрацьований проєкт закону, який значно критикували через надані INCD повноваження і питання захисту приватності громадян [163].

Китай, навпаки, базує свою модель на концепції «кіберсуверенітету». Це означає, що держава володіє повним контролем над інформаційним середовищем у межах своїх кордонів. Такий підхід передбачає фільтрацію контенту, блокування доступу до окремих ресурсів, регулювання цифрових компаній та використання потужної системи моніторингу – «Золотого щита». Китайський досвід є прикладом централізованого управління цифровим простором як інструменту ідеологічного впливу та безпеки.

Отже, зарубіжні моделі забезпечення інформаційної безпеки, попри відмінності в організації та політико-правових підходах, мають низку сильних сторін — від технологічного лідерства та високого рівня кіберготовності до соціальної інклюзивності та правової адаптивності. Спільним для них є трактування інформаційної безпеки як багатоаспектного явища, що охоплює законодавчий, технологічний, організаційний, освітній та міжнародний рівні. В умовах зростання гібридних викликів особливого значення набуває міжнародна співпраця, що передбачає обмін кіберінформацією, розроблення узгоджених стандартів і координацію реагування на інциденти.

Усі розглянуті моделі демонструють важливість комплексного, стратегічного та динамічного підходу до захисту національного інформаційного простору. Їх аналіз дозволяє виокремити низку позитивних елементів, релевантних для адаптації в Україні:

1. Інституційна інтеграція: створення єдиного національного координаційного центру з інформаційної безпеки з міжвідомчим статусом (за прикладом США) з функціями стратегічного планування, управління інцидентами та аналітичного забезпечення.
2. Гармонізація законодавства: приведення українського нормативного регулювання у відповідність до стандартів ЄС, зокрема NIS2, що

сприятиме інтеграції в європейський цифровий простір і посиленню нормативної визначеності.

3. Цифрова освіта: розширення програм цифрової грамотності й медіаграмотності, інтеграція компонентів інформаційної безпеки в навчальні програми різних рівнів освіти (досвід Естонії та ЄС).
4. Безпечне електронне урядування: впровадження єдиної системи цифрової ідентифікації громадян, захищених державних сервісів і довірчих цифрових платформ.
5. Підготовка фахівців: розвиток кіберрезерву, підтримка спеціалізованих ІТ-освітніх програм і партнерств між державою, університетами та приватним сектором (практика Ізраїлю).
6. Міжнародна кооперація: активна участь у міжнародних кіберструктурах, підвищення рівня інформаційного обміну, проведення спільних тренувань і впровадження уніфікованих стандартів реагування.
7. Громадський контроль: забезпечення прозорості державної політики, інклюзивності процесів і системного залучення громадянського суспільства до моніторингу інформаційного простору.

Зарубіжний досвід засвідчує, що ефективна система забезпечення національної безпеки у публічно-інформаційній сфері можлива за умови чіткої стратегії, узгоджених дій між суб’єктами безпеки, прозорої взаємодії із суспільством і постійного вдосконалення відповідних механізмів. Україна має потенціал для адаптації найкращих практик передусім для розвитку кіберінфраструктури, посилення правового регулювання, підвищення цифрової та медіаграмотності, забезпечення стійкості інформаційного середовища до зовнішніх впливів. Важлива також розбудова системи підготовки фахівців у сфері інформаційної безпеки, створення міжвідомчих аналітичних центрів і розширення участі у міжнародних ініціативах із кіберзахисту.

3.2. Напрями вдосконалення адміністративно-правового регулювання національної безпеки у публічно-інформаційній сфері

Сучасні трансформаційні процеси у сфері публічного управління, стрімкий розвиток цифрових технологій та зростання складності інформаційних загроз зумовлюють необхідність переосмислення існуючих механізмів забезпечення національної безпеки у публічно-інформаційному просторі. В умовах гібридної агресії проти України, глобалізації комунікаційних мереж і збільшення залежності державних інституцій від інформаційно-комунікаційних технологій адміністративно-правове регулювання сфери набуває пріоритетного значення.

У наукових дослідженнях С. Єсімова підкреслено, що подальший розвиток і вдосконалення інформаційного законодавства України у сфері забезпечення інформаційної безпеки безпосередньо пов'язані зі створенням нових законів і нормативно-правових актів. Такі акти слід спрямувати на усунення прогалин у правовому регулюванні суспільних відносин в інформаційній сфері шляхом упровадження до законодавства сучасних категорій і термінів, що відображають специфіку інформаційно-телекомунікаційних технологій, а також гармонізації внутрішнього законодавства з міжнародними зобов'язаннями України [97; 168].

На основі положень Стратегії розвитку інформаційного суспільства в Україні та Окінавської хартії глобального інформаційного суспільства [168; 169] С. Єсімов виокремлює ключові напрями удосконалення національного законодавства у відповідній сфері. До них належать:

1. Розвиток державної системи забезпечення інформаційної безпеки. Наголошено на необхідності формування цілісної та керованої системи, здатної забезпечувати належну оцінку рівня інформаційної безпеки, ефективну координацію й контроль діяльності всіх суб'єктів цієї сфери. Важливими є чіткий розподіл повноважень між органами державної влади та місцевого самоврядування, визначення процедур участі громадських об'єднань і громадян

у заходах із захисту інформаційного простору, а також створення регіональних структур забезпечення інформаційної безпеки.

2. Створення ефективної системи управління державними інформаційними ресурсами. Запропоновано нормативне закріплення функцій щодо формування, зберігання, передачі та захисту державних інформаційних ресурсів, удосконалення системи сертифікації інформаційної продукції відповідно до вимог безпеки, а також розширення механізмів ліцензування діяльності у сфері надання інформаційних послуг. Це сприятиме підвищенню керованості та безпеки інформаційних процесів.

3. Забезпечення реалізації конституційних прав громадян в інформаційній сфері. Передбачає нормативне закріплення пріоритету права на недоторканність приватного життя над правом на свободу інформації, визначення правової природи відомостей, що можуть завдати шкоди честі, гідності чи діловій репутації особи, установлення юридичної відповідальності за незаконне збирання або поширення персональних даних. Також наголошено на формуванні системи обмежень доступу до інформації з огляду на захист національної безпеки, моралі та прав інших осіб.

4. Посилення протидії правопорушенням в інформаційній сфері. Напрям охоплює уточнення правових норм, що регулюють відповідальність за несанкціонований доступ до інформації, копіювання, спотворення або незаконне використання, за поширення недостовірних відомостей чи розкриття конфіденційної інформації. Важливо вдосконалити оперативно-розшукової діяльності для протидії кіберзлочинності й нормативного обмеження використання імпортних засобів криптографічного захисту.

5. Пріоритетний розвиток національної інформаційної інфраструктури. Ідеться про підтримку вітчизняного виробництва комп’ютерної техніки, телекомунікаційних мереж, супутникових систем зв’язку, інноваційних інформаційно-телекомунікаційних технологій, а також про зміцнення наукової та

виробничої бази у сфері інформаційної безпеки як ключового чинника національної стійкості.

6. Захист прав інтелектуальної власності. Передбачає врегулювання питань охорони секретних винаходів, корисних моделей, промислових зразків, ноу-хау й інших результатів інтелектуальної діяльності, а також визначення співвідношення прав держави та виконавців робіт, що фінансуються за рахунок державного бюджету. Належне правове забезпечення у цій сфері є передумовою інноваційного розвитку та технологічного суверенітету держави.

7. Інтеграція інформаційного простору України у світовий інформаційний простір. Реалізація цього напряму вимагає розроблення нормативних положень щодо статусу інформації, що передається транскордонними мережами, визначення прав та обов'язків користувачів, а також закріплення правового статусу телекомунікаційних провайдерів. Такий підхід забезпечить збалансоване входження України до міжнародного інформаційного середовища.

8. Підвищення якості нормативно-правових актів. Охоплює ревізію чинного законодавства, усунення внутрішніх неузгодженостей, удосконалення механізмів реалізації правових норм, розроблення нових підзаконних актів і проведення наукової експертизи ефективності законодавства, що потрібно для формування сучасної й адаптивної нормативної бази в інформаційній сфері.

Як бачимо, С. Єсімов обґрунтовує важливість комплексного оновлення законодавчої бази у сфері інформаційної безпеки, що передбачає одночасне зміцнення правових, організаційних та технологічних механізмів захисту національного інформаційного простору та його інтеграцію в глобальні інформаційні процеси.

Ці пропозиції до вдосконалення системи забезпечення інформаційної безпеки України зберігають надзвичайно високий рівень актуальності, а в умовах триваючої збройної агресії Російської Федерації та стрімкої цифровізації державного управління набувають навіть більшої значущості, ніж на момент їх

первинного формулювання. Усі окреслені напрями, по суті, віддзеркалюють структурні дисфункції національного інформаційного простору, які протягом тривалого часу залишаються неврегульованими.

Передусім цілком виправданою є пропозиція щодо розбудови цілісної державної системи забезпечення інформаційної безпеки, адже в Україні досі відсутній єдиний координуючий центр, здатний формувати та реалізовувати уніфіковану політику у цій сфері. Фрагментарність повноважень між органами сектору безпеки та оборони супроводжується відсутністю узгодженої термінології та єдиних стандартів, що суперечить підходам НАТО та Європейського Союзу й знижує рівень національної стійкості. Так само обґрунтованою є необхідність створення системи комплексного управління державними інформаційними ресурсами, оскільки їх розпорошеність, технічна неоднорідність і нестача захищених інфраструктур створюють передумови для витоків даних, технічних збоїв і зовнішнього втручання.

Надзвичайно важливим напрямом, який визначив С. Єсімов, є забезпечення реалізації конституційних прав особи у цифровому середовищі. Європейські стандарти захисту приватності та персональних даних передбачають високий рівень правових гарантій, що зумовлює потребу в нормативному уточненні категорій, пов’язаних з честю, гідністю та репутацією, а також у формуванні збалансованої моделі співвідношення приватності та національної безпеки. У сучасних умовах масової цифровізації державних послуг такі положення становлять фундамент демократичного правопорядку.

Підтвердженої сучасними реаліями потребує і посилення відповідальності за правопорушення в інформаційній сфері, зокрема у зв’язку з масштабними кібератаками, дезінформаційними кампаніями та спробами зовнішнього впливу на державні інформаційні системи.

Стратегічно значущим є й пріоритет розвитку національної інформаційної інфраструктури, зважаючи на надмірну залежність України від іноземного

програмного забезпечення, сервісів і технологічних платформ. Створення власних технічних рішень здатне підвищити кіберстійкість держави, мінімізувати ризики втручання та забезпечити контроль над критичними об’єктами інфраструктури. Не менш актуальним, у контексті інноваційного розвитку та модернізації оборонного сектору, є питання захисту інтелектуальної власності, що потребує збалансування інтересів держави та виконавців науково-дослідних проєктів відповідно до міжнародних стандартів.

Пропозиції щодо інтеграції України до глобального інформаційного простору також мають очевидну логічну обґрунтованість, адже транскордонні потоки даних, діяльність цифрових платформ і транснаціональні інформаційні загрози потребують чітких правил регулювання. У цьому контексті особливо важливою є гармонізація законодавства з нормами Європейського Союзу, зокрема тими, що стосуються цифрових послуг, ринків та захисту даних. Нарешті, підвищення якості нормативно-правових актів у сфері інформаційної безпеки становить необхідну передумову усунення суперечливості, застарілості та неузгодженості правового регулювання, що багато в чому стримує ефективність державної політики.

Концептуальні підходи С. Єсімова формують цілісну систему стратегічних орієнтирів, які перебувають у повній відповідності з сучасними міжнародними тенденціями розвитку інформаційного права, кібербезпеки та цифрового врядування. Усі запропоновані напрями є не лише актуальними, а й критично необхідними для формування стійкої, інституційно збалансованої системи національної безпеки України в умовах гібридної війни та зростання інформаційних загроз.

Подібні позиції простежуються і в роботах В. Антонюка, який наголошує на стратегічній важливості нормативно-правового підґрунтя інформаційної безпеки. Учений зауважує, що розвиток інформаційних технологій значно випереджає інституційні можливості держави, що спричиняє правову

інерційність, фрагментарність регулювання й створює умови для зловживань у цифровому середовищі. Ключовим завданням є приведення законодавства у відповідність до міжнародних стандартів і забезпечення його динамічності, тобто здатності оперативно реагувати на нові загрози [170].

Дослідник також акцентує на необхідності нормативного впорядкування відносин щодо створення, використання та захисту інформаційних ресурсів на всіх рівнях та визначення вимог до технічної інфраструктури, програмного забезпечення й діяльності у сфері електронних комунікацій. Він підкреслює важливість розроблення стандартів та удосконалення системи сертифікації й ліцензування у сфері інформаційних технологій як передумови належного функціонування єдиного інформаційного простору держави.

Концепції С Єсімова та В. Антонюка взаємодоповнюють одна одну, утворюючи цілісний підхід до модернізації національної системи інформаційної безпеки. Позицію С. Єсімова зосереджено на стратегічних напрямах і структурній трансформації нормативно-правової бази, концепція В. Антонюка підкреслює техніко-правові параметри цієї модернізації та важливість гнучкого правового реагування. Разом вони формують теоретичний підмурівок для створення сучасної, адаптивної та інституційно збалансованої системи забезпечення національної безпеки в інформаційній сфері.

У цьому контексті варто також врахувати пропозиції В. Калетніка щодо трансформації адміністративно-правового забезпечення інформаційної безпеки України. На нашу думку, його підхід є надзвичайно актуальним і системно обґрунтованим. Науковець підкреслює потребу в перегляді понятійно-категоріальної бази, доповнення Закону України «Про інформацію» поняттям «інформаційна безпека» та усунення невідповідностей щодо переліку суб’єктів інформаційних відносин у різних законах. Така уніфікація термінології є передумовою ефективного правового регулювання, дозволяє створити єдину

основу для координації діяльності суб’єктів інформаційної безпеки та формування цілісного інформаційного простору держави [171].

Особливо доречною є пропозиція щодо приведення у відповідність нормативно-правових актів різного рівня щодо суб’єктів національної системи кібербезпеки та визначення структури системи кібероборони, включаючи склад, функції та завдання її учасників, а також перелік об’єктів кібероборони. Реалізація цих заходів сприятиме усуненню дублювання повноважень, підвищенню узгодженості дій органів влади та створенню передумов для швидкого і скоординованого реагування на кіберзагрози, що особливо актуально в умовах триваючої гібридної війни та зростаючого інформаційного впливу з боку зовнішніх суб’єктів [171].

Законодавче закріплення механізмів протидії дезінформації та діяльності агентів впливу, яке запропоновав В. Калетнік, також заслуговує на підтримку. У сучасних умовах цифрового середовища, де інформаційні потоки використовують для маніпуляцій та впливу на суспільну думку, наявність чітких нормативних інструментів для ідентифікації і нейтралізації таких загроз є першорядною умовою забезпечення національної безпеки. Важливо забезпечити баланс між протидією шкідливому впливу й дотриманням конституційних прав громадян – свободи слова й діяльності громадських об’єднань.

Не менш суттєвою є пропозиція щодо забезпечення динамічності нормативно-правової бази, що дозволяє оперативно генерувати нові регуляторні рішення та адаптуватися до темпів розвитку інформаційного суспільства. Такий підхід відповідає сучасним вимогам гібридної безпеки та цифровізації державного управління, оскільки дозволяє реагувати на нові загрози та підтримувати стійкість державних інститутів.

Як бачимо, пропозиції В. Калетніка доповнюють і конкретизують концептуальні підходи, які сформулювали С. Єсімов та В. Антонюк, та разом формують єдину систему стратегічних заходів для удосконалення законодавчого

та адміністративного забезпечення інформаційної безпеки України. Їх реалізація сприятиме підвищенню рівня кіберстійкості держави, інтеграції національного інформаційного простору у глобальні інформаційні процеси та ефективному протидіянню сучасним інформаційним загрозам.

У дослідженнях В. Кондратенка та О. Сокуренко акцентовано на стрімкому зростанні складних кіберінцидентів і спроб несанкціонованого доступу до державних інформаційних ресурсів, що підтверджується практичними даними СБУ за 2022–2024 рр. Науковці підкреслюють, що наслідки таких атак позначаються не лише на функціонуванні центральних органів виконавчої влади, а й безпосередньо впливають на роботу місцевих громад, доступність соціальних послуг, реалізацію оборонних програм та загальну стійкість публічного управління. У відповідь на зростання загроз правоохоронні органи впроваджують спеціальні протоколи кіберзахисту, обмежують доступ до окремих категорій службової інформації, здійснюють превентивну роз'яснювальну діяльність, контролюють дотримання вимог кібергігієни та інформаційної безпеки, а також підвищують цифрову компетентність державних службовців [172].

Автори наголошують, що розвиток електронних сервісів і державних цифрових платформ істотно розширює можливості для громадян, водночас створюючи нові ризики для захисту інформації. Зокрема, вони виокремлюють низку проблем, характерних для сучасної практики публічного управління: формалізм при розгляді інформаційних запитів, зловживання правом на відмову в наданні інформації, нечіткі критерії віднесення даних до обмежених, недостатній рівень зовнішнього контролю та слабку координацію між органами влади й правоохоронними структурами [172].

Ключовим у висновках дослідників є твердження про необхідність забезпечення балансу між відкритістю публічної інформації та захистом національних інтересів. На їхню думку, правоохоронні органи мають реалізовувати подвійний функціональний мандат: гарантувати доступ громадян

до інформації, дотримуючись вимог законності й прозорості, та одночасно забезпечувати кібербезпеку й захист державних інформаційних ресурсів. Ефективність такого механізму можлива лише за умов чіткого розмежування повноважень, унормованих процедур прийняття рішень і наявності дієвих інструментів зовнішнього демократичного контролю.

Отже, В. Кондратенко та О. Сокуренко підкреслюють, що адміністративно-правовий механізм забезпечення інформаційної безпеки повинен залишатися адаптивним до динаміки інформаційних загроз, розвитку цифрових технологій і зростання суспільних очікувань щодо прозорості публічної влади.

Продовжуючи аналіз наукових підходів до вдосконалення системи інформаційної безпеки України, слід зазначити, що в дисертації М. Баран запропоновано суттєве розширення підходів до нормативної бази в цій сфері. Авторка пропонує виділяти широке та вузьке значення поняття нормативної бази, включаючи не лише нормативно-правові акти, а й документи стратегічного планування, акти тлумачення, нормативно-технічні документи та матеріали правозастосовної практики. Такий підхід забезпечує комплексну оцінку стану інформаційної безпеки та інтеграцію багаторівневих компонентів у єдину систему нормативного забезпечення [173].

Значну увагу М. Баран приділяє важливості побудови єдиної системи нормативного забезпечення інформаційної безпеки, що передбачає інтеграцію однорідних, взаємопов’язаних компонентів, залучаючи широкий спектр суб’єктів – державні органи, органи місцевого самоврядування та інші учасники інформаційного простору. Система передбачає використання сучасних цифрових технологій для забезпечення ефективності управління та оперативного реагування на загрози.

Важливим напрямом є внесення змін до чинних законів України, зокрема: до Закону «Про інформацію» – введення окремої статті про забезпечення інформаційної безпеки; до Закону «Про адміністративні послуги» – доповнення

ст. 5 нормами щодо обов'язкової організації інформаційної безпеки; до Закону «Про публічні електронні реєстри» – встановлення спеціальних вимог щодо захисту інформації; до Закону «Про хмарні послуги» – державний нагляд за дотриманням вимог інформаційної безпеки провайдерами [173].

Дослідниця також пропонує створити національну систему інформаційної безпеки на платформній основі, що забезпечує інтеграцію державних інформаційних ресурсів, цифрових сервісів та механізмів адміністрування, підвищуючи рівень захищеності інформаційного простору.

Водночас учена окреслює прогалини, що потребують подальшого розвитку, серед яких відсутність базових засад інформаційної безпеки у законодавстві, недостатня регламентація питань захисту даних у державних реєстрах, хмарних сервісах та цифрових адміністративних послугах, потреба у зміцненні правових та організаційних механізмів протидії деструктивному інформаційному впливу та необхідність розроблення окремого Закону України «Про захист від деструктивного інформаційного впливу на населення».

Особливу увагу авторка приділяє розгляду інформаційної безпеки як стратегічного ресурсу держави, у межах якого розвиток правової інформатизації, цифровізація публічного управління та формування єдиного інформаційно-правового простору постають ключовими елементами державної політики переходу до «суспільства знань» [173]. Такий підхід підкреслює, що інформаційна безпека не зводиться до технічного захисту, а інтегрує правові, організаційні, технологічні та соціальні складові, які визначають здатність держави забезпечувати стійкість та інноваційний розвиток у цифрову епоху.

Окремо сформульовано напрями подальшого розвитку інформаційного законодавства, що передбачають: розширення правових механізмів забезпечення інформаційно-психологічної безпеки; удосконалення юридичної техніки, процедур правового моніторингу й оцінювання ефективності нормативних актів; посилення контролю якості цифрових сервісів і стандартів державних

інформаційних систем; інтеграцію публічних інформаційних ресурсів із сучасними цифровими технологіями; формування культури інформаційної безпеки та підвищення цифрової грамотності населення як базової умови стійкості інформаційного середовища.

У наукових напрацюваннях Ю. Лісовська обґрунтовує комплексний підхід до модернізації механізмів адміністративно-правового забезпечення інформаційної безпеки України, визначаючи низку нормативних, інституційних, організаційних та міжнародно-правових кроків, необхідних для формування цілісної та ефективної системи захисту інформаційного простору держави [174].

Насамперед авторка акцентує на необхідності нормативно-правового удосконалення, пропонуючи розробити та прийняти спеціальний Закон України «Про інформаційну безпеку України». Цей акт має закріпити правові засади діяльності у сфері інформаційної безпеки, визначити статус і порядок функціонування національних та іноземних інституцій, що діють в українському інформаційному просторі, а також усунути прогалини в законодавстві.

За твердженням Ю. Лісовської, потрібно реформувати адміністративно-деліктне законодавство, зокрема в частині відповідальності за посягання на інформаційну безпеку, а також комплексно модернізувати інформаційне законодавство з урахуванням нових викликів цифрової трансформації та міжнародних стандартів. Важливим складником є удосконалення правового забезпечення доступу до публічної інформації, що передбачає розвиток програм відкритих даних та створення ефективних механізмів їхнього отримання [174].

Друга група пропозицій стосується інституційно-організаційного розвитку, де дослідниця порушує питання створення спеціалізованого державного органу (служби), відповідального за координацію діяльності всіх суб’єктів у сфері інформаційної безпеки. Окрему увагу вона приділяє інституціоналізації участі громадянського суспільства шляхом закріплення механізмів взаємодії недержавних організацій з органами державної влади у процесі формування та

реалізації державної політики інформаційної безпеки. Доповненням до цього є пропозиції щодо реформування системи електронного урядування з урахуванням вимог сервісності, захисту інформації та прозорості. У цьому контексті Лісовська наголошує на потребі формування цілісної, системної та динамічної державної політики інформаційної безпеки, що орієнтується на багатовимірність сучасних загроз і специфічні геополітичні умови України.

Значна частина напрацювань авторки присвячена інформаційно-комунікаційним та медійним механізмам. Лісовська пропонує створити власні потужні інформаційні структури, включно з державними та недержавними інформаційними агенціями, здатними забезпечувати збір, аналіз, обробку та поширення інформації, що відображає інтереси України. Однією з ключових ініціатив є створення повноцінного телеканалу зовнішнього мовлення, покликаного формувати позитивний міжнародний імідж держави та забезпечувати інформаційну присутність України в глобальному медіапросторі. Важливим елементом є також розробка стратегічних комунікацій і системи превентивних заходів, спрямованих на протидію пропаганді, дезінформації та інформаційному впливу іноземних держав [174].

Особливе місце у системі запропонованих заходів посідає кадрово-освітній напрям, у межах якого авторка акцентує на необхідності формування національного кадрового потенціалу у сфері інформаційної безпеки, здатного ефективно реагувати на сучасні інформаційні та кіберзагрози. Підкреслюється стратегічна роль освіти, науки і виховання як інструментів зміцнення інтелектуального ресурсу держави, а також наголошується на важливості інтеграції проблематики інформаційної безпеки у програми формальної, неформальної та післядипломної освіти.

Зрештою, Ю. Лісовська окреслює міжнародно-правові та інтеграційні орієнтири розвитку, наголошуючи на доцільності використання досвіду ЄС і провідних держав світу у вибудові національної системи інформаційної безпеки.

Йдеться про участь України у формуванні спільної європейської стратегії захисту інформаційного простору, посилення спроможності держави у протидії кібервійнам, інформаційному тероризму та кіберзлочинності. Важливим вектором визначено також поглиблення співпраці з інституціями Ради Європи, Європейської телерадіомовної спілки та іншими міжнародними організаціями з метою інтеграції України у спільний європейський інформаційний простір.

Концептуальні підходи Ю. Лісовської вирізняються багатовимірністю та стратегічною зорієнтованістю, а розроблені пропозиції охоплюють увесь спектр актуальних проблем інформаційної безпеки – від законодавчої модернізації та інституційного реформування до розвитку стратегічних комунікацій, зміцнення кадрового потенціалу й активізації міжнародної кооперації.

Не менш значущими для сучасної наукової дискусії є підходи О. Пугачова, який сформував комплексне бачення удосконалення адміністративно-правового, організаційного й інформаційно-технічного забезпечення інформаційної безпеки України. На наш погляд, запропоновані напрями вирізняються практичною спрямованістю та орієнтацією на адаптацію вітчизняної моделі інформаційної безпеки до сучасних глобальних тенденцій і євроатлантичних стандартів [175].

Передусім заслуговує на увагу наголос дослідника на гармонізації національного законодавства з міжнародними стандартами. Такий підхід є об’єктивно виправданим, оскільки інформаційні загрози є транскордонними, поширюються зі швидкістю цифрових комунікацій і вимагають координації на міжнародному рівні. Підхід О. Пугачова передбачає не лише формальне імплементацію положень ЄС, НАТО та інших міжнародних організацій, а й розбудову інституційних форматів співпраці, що фактично орієнтує Україну на модель колективної кіберстійкості та спільної відповідальності за безпеку інформаційного простору.

Важливим є також акцент автора на розробленні спеціалізованих нормативно-правових актів для регламенту окремих сегментів інформаційної

безпеки, зокрема механізми кіберзахисту критичної інформаційної інфраструктури, протидію інформаційним війнам і шкідливим інформаційним впливам. На наш погляд, така деталізація законодавства сприятиме усуненню існуючих прогалин у правовому регулюванні, забезпечить чіткість адміністративних процедур і визначеність повноважень органів публічної влади.

Дослідник також акцентує на потребі посилення механізмів контролю та юридичної відповідальності в інформаційній сфері, що видається актуальним в умовах різкого зростання кількості кіберінцидентів та інформаційних операцій. Неефективність реагування на такі загрози, як обґрунтовує О. Пугачов, безпосередньо впливає на функціонування державних інститутів, стійкість економіки й безпеку громадян, тому потребує підвищення рівня інституційної спроможності й технологічної оснащеності органів публічної влади [175].

Значущими для розвитку національної системи інформаційної безпеки є й пропозиції щодо удосконалення організаційного забезпечення. У розвідці дослідника обґрунтовано наголошено на потребі у створенні єдиного координаційного центру для забезпечення цілісності, узгодженості й безперервності дій різних суб’єктів у сфері інформаційної безпеки. Така модель відповідає провідним зарубіжним практикам (NCSC у Великій Британії, CISA у США) та дає змогу мінімізувати дублювання функцій, подолати фрагментацію управлінських процесів і підвищити ефективність міжвідомчої взаємодії. Сформульовані дослідником пропозиції щодо розвитку єдиних протоколів реагування та підвищення рівня взаємної підзвітності суб’єктів сфери інформаційної безпеки видаються обґрунтованими, оскільки забезпечують оперативність, передбачуваність і скоординованість дій у разі виникнення інформаційних інцидентів [175].

Окремого акценту заслуговує ідея щодо ширшого залучення приватного сектору та інститутів громадянського суспільства, що узгоджується з міжнародною практикою багатостейкхолдерного управління у сфері кібер- та

інформаційної безпеки. Така взаємодія сприяє мобілізації додаткової експертизи, використанню інноваційних технологій, доступу до аналітичних ресурсів і формуванню стійкішої загальнонаціональної моделі інформаційного захисту. Створення кризових центрів і спеціалізованих оперативних груп є логічним для підвищення готовності держави до реагування на масштабні інформаційні інциденти та відновлення функціонування критично важливих систем.

Актуальними є підходи вченого до інформаційно-технічного забезпечення. Розвиток інфраструктури кіберзахисту, технічна модернізація критичних інформаційних систем, упровадження технологій штучного інтелекту й машинного навчання, створення та розвиток національних CERT-структур відповідають найкращим міжнародним стандартам та є ключовими умовами формування сучасної, стійкої та адаптивної архітектури інформаційної безпеки. Особливо важливим видається акцентування на розвитку резервних систем, здатних гарантувати безперервність роботи критичної інфраструктури у разі масштабних кіберінцидентів або деструктивних інформаційних впливів [175].

Загалом пропозиції О. Пугачова вирізняються стратегічною глибиною, комплексністю та орієнтацією на довгостроковий розвиток системи забезпечення інформаційної безпеки. На нашу думку, їх імплементація у практику державного управління може стати підґрунтям для формування більш стійкої, технологічно розвиненої та ефективної моделі протидії кібер- та інформаційним загрозам.

Узагальнення наукових підходів, представлених у працях С. Єсімова, В. Антонюка, В. Калетніка, Ю. Лісовської, М. Баран, О. Пугачова, В. Кондратенка, О. Сокуренко, засвідчує наявність сформованої концептуальної основи модернізації адміністративно-правового забезпечення національної безпеки у публічно-інформаційній сфері. Водночас сучасні трансформаційні процеси, зумовлені цифровізацією публічного управління, широким упровадженням штучного інтелекту, платформізацією комунікацій та еволюцією гібридних загроз, актуалізують потребу подальшого розвитку відповідних

підходів через їх конкретизацію, ризик-орієнтацію та посилення людиноцентричної складової. Запропоновані авторські напрями вдосконалення продовжують, поглиблюють і систематизують наявні доктринальні позиції.

По-перше, обґрунтовується доцільність переходу від переважно декларативно-фактологічної моделі правового регулювання інформаційної безпеки до ризик-орієнтованого підходу. Йдеться про необхідність нормативного закріплення класифікації інформаційних систем і процесів за рівнями ризику для національної безпеки (критичні, високого, середнього й низького ризику) із подальшою диференціацією вимог до організаційно-технічного захисту, звітності та контролю. Такий підхід кореспондує із сучасними європейськими практиками кібербезпеки, забезпечує раціональний розподіл ресурсів та дає змогу зосередити державні зусилля на найбільш уразливих сегментах публічно-інформаційного простору. Також доцільним є запровадження обов'язкової оцінки впливу на інформаційну безпеку (information security impact assessment) для державних цифрових проєктів, систем електронного урядування та державно-приватних цифрових ініціатив, що сприятиме превентивному виявленню загроз ще на етапі проєктування та ухвалення управлінських рішень.

По-друге, виникає потреба у створенні цілісної системи управління державними інформаційними ресурсами, яка в науковій літературі, як правило, окреслюється лише загально. У цьому зв'язку пропонується інституціоналізація управління даними (data governance) у публічному секторі шляхом законодавчого запровадження інституту уповноваженого з управління даними (Chief Data Officer) у ключових органах державної влади. Така посадова особа має забезпечувати якість, цілісність, безпеку та повторне використання даних, узгоджувати політику відкритих даних із вимогами інформаційної безпеки та координувати реалізацію внутрішніх стандартів обігу інформації. Додатково необхідно нормативно врегулювати повний життєвий цикл даних у державних інформаційних системах (створення, збирання, зберігання, використання,

передавання, архівація, видалення) з обов'язковою фіксацією операцій доступу (логуванням) як передумовою ефективної відповідальності за правопорушення.

По-третє, рівень цифрової трансформації публічного управління зумовлює потребу у впровадженні спеціального адміністративно-правового режиму застосування алгоритмічних систем та систем штучного інтелекту органами публічної влади. На відміну від наявних підходів, що розглядають ШІ переважно як інструмент кіберзахисту, необхідно передбачити створення реєстру державних алгоритмічних систем, установлення вимог до прозорості логіки автоматизованого прийняття рішень у випадках, коли такі рішення впливають на права, свободи та обов'язки осіб, а також запровадження обов'язкової людиноцентричної процедури перегляду рішень, ухвалених на основі автоматизованого аналізу даних. Окремої регламентації потребує оцінка впливу систем ШІ на права людини та національну безпеку як складова впровадження відповідних технологій у сферу публічного управління.

По-четверте, з огляду на ключову роль глобальних цифрових платформ у формуванні інформаційного середовища й здійсненні інформаційного впливу, актуалізовано потребу в розвитку механізмів співрегулювання й саморегулювання. Уважаємо за доцільне законодавчо закріпити модель співрегулювання з великими цифровими платформами (соціальними мережами, відеохостингами, месенджерами) на основі кодексів поведінки щодо протидії дезінформаційним та пропагандистським кампаніям, узгоджених протоколів позначення та обмеження шкідливого контенту, а також регулярної звітності перед національним регулятором щодо координованих інформаційних операцій і політичної реклами. Паралельно необхідно стимулювати створення галузевих саморегульованих організацій (медійних, ІТ, телекомунікаційних), відповідальних за розроблення кодексів інформаційної безпеки, етичних стандартів і надання експертної підтримки державній політиці.

По-п’яте, у контексті децентралізації публічного управління та зростання ролі територіальних громад важливого значення набуває концепція мультирівневого забезпечення інформаційної безпеки. Потрібно нормативно закріпити роль органів місцевого самоврядування як суб’єктів забезпечення інформаційної безпеки, передбачивши створення регіональних центрів кіберстійкості, розроблення та реалізацію місцевих програм цифрової грамотності посадових осіб, включення питань інформаційної безпеки до стратегій розвитку територіальних громад. Інструментом реалізації підходу є «інформаційний аудит громад» як форма державного нагляду й методичної підтримки, спрямована на оцінку захищеності локальних інформаційних систем і практик роботи з публічною інформацією та відкритими даними.

По-шосте, розвиток людиноцентричного виміру адміністративно-правового регулювання національної безпеки в публічно-інформаційній сфері обумовлює потребу в посиленні інституційних гарантій інформаційних прав людини. У цьому контексті обґрунтовується доцільність створення інституту омбудсмана з цифрових прав та інформаційної безпеки (у структурі Уповноваженого Верховної Ради України з прав людини або як окремого суб’єкта), уповноваженого розглядати скарги на порушення прав у цифровому середовищі, здійснювати моніторинг практики державних органів і цифрових платформ щодо обмеження контенту, а також готувати щорічні доповіді про стан інформаційних прав і свобод. Важливо також забезпечити уніфікацію й публічність критеріїв обмеження доступу до інформації, запровадити стандартизовані форми мотивованих відповідей на запити та ефективні механізми адміністративного оскарження.

По-сьоме, динаміка інформаційних загроз зумовлює потребу в розвитку аналітичної та прогностичної складових системи інформаційної безпеки. Доцільним є законодавче закріплення створення національного центру моніторингу інформаційних операцій як окремого елемента системи

національної безпеки, уповноваженого здійснювати автоматизований моніторинг інформаційних кампаній, координованої неавтентичної поведінки, діяльності бот-мереж, а також готувати стратегічні аналітичні звіти для суб'єктів сектору безпеки й оборони. Додатково необхідно нормативно врегулювати прогностичну функцію інформаційної безпеки через підготовку щорічних національних доповідей про ризики в публічно-інформаційній сфері та сценарне планування можливих траєкторій ескалації інформаційних загроз.

Отже, запропоновані напрями вдосконалення адміністративно-правового регулювання національної безпеки у публічно-інформаційній сфері поглиблюють існуючі доктринальні підходи, переводячи їх із площини загальних стратегічних орієнтирів у площину конкретних, операціоналізованих механізмів правового впливу. Реалізація ризик-орієнтованої моделі регулювання, інституціоналізація управління даними, формування правового режиму алгоритмічних систем, розвиток співрегулювання з цифровими платформами, упровадження мультирівневих моделей інформаційної безпеки, посилення інституційних гарантій інформаційних прав людини та розбудова аналітико-прогностичної підсистеми створюють підґрунтя для формування стійкої, динамічної та людиноцентричної моделі національної безпеки України у публічно-інформаційній сфері.

ВИСНОВКИ ДО РОЗДІЛУ 3

1. На підставі аналізу зарубіжних моделей (США, ЄС, Франції, Німеччини, Естонії, Польщі, Ізраїлю, Китаю) установлено, що забезпечення національної безпеки в публічно-інформаційній сфері потрібно розглядати як стратегічний пріоритет, інтегрований у систему правових, інституційних, технологічних, освітніх і міжнародно-координаційних механізмів. Інформаційну безпеку визначено як комплексний політико-правовий феномен, який охоплює технічні, організаційні та гуманітарні аспекти захисту держави в цифровому середовищі.

2. Доведено, що однією з ключових передумов ефективності системи інформаційної безпеки є розвинена інституційна архітектура, яка включає спеціалізовані національні агентства (CISA, NSA, ANSSI, BSI, INCD та ін.), урядові CERT-структури, координаційні ради та центри передового досвіду. Ці інституції забезпечують міжвідомчу взаємодію, стратегічне управління, аналіз і реагування на кіберінциденти, а також формують канали кооперації з міжнародними партнерами та глобальними мережами кіберзахисту.

3. Засвідчено, що провідні держави поєднують оборонний і превентивний виміри інформаційної безпеки: поряд з реагуванням на кіберінциденти суттєву увагу звертають на формування культури інформаційної безпеки, цифрової та медіаграмотності населення, підготовку висококваліфікованих фахівців, зміцнення людського капіталу, а також підтримку науково-дослідних ініціатив у сфері інформаційного захисту, штучного інтелекту та технологій кіберстійкості.

4. Узагальнення практик ЄС, Франції, Естонії, Польщі та Німеччини дає підстави стверджувати, що ефективна політика у публічно-інформаційній сфері потребує системної нормативної бази, гармонізованої із міжнародними та європейськими стандартами (зокрема NIS/NIS2), а також чітко окреслених процедур захисту критичної інфраструктури, прозорих механізмів державної політики, розвинених інструментів протидії дезінформації й стратегічних комунікацій.

5. Установлено, що моделі США, Ізраїлю та Китаю віддзеркалюють різні парадигми управління інформаційним простором: від інституційно-інтегративної та моделі активного кіберзахисту до концепції «кіберсуверенітету», що передбачає домінування державного контролю. З огляду на це вибір конкретної моделі інформаційної безпеки залежить від поєднання безпекових потреб, політико-правових засад та ціннісної орієнтації кожної держави.

6. З’ясовано, що важливою передумовою стійкості національного інформаційного простору є розвинута міжнародна співпраця, щоохоплює участь

у структурах НАТО та ЄС, діяльність у межах центрів передового досвіду (зокрема CCDCOE); проведення спільних навчань, обмін розвідувальною інформацією та кращими практиками; вироблення спільних стандартів і протоколів реагування на кіберзагрози, оскільки саме міжнародна кооперація формує основу для зміцнення національної кіберстійкості та інтеграції до європейського безпекового простору.

7. Обґрунтовано, що для України особливо релевантними є ті елементи зарубіжного досвіду, які поєднують інституційну координацію, правову визначеність, потужний освітній і науково-дослідний компоненти та активну міжнародну взаємодію. Адаптація цих підходів може стати основою подальшого вдосконалення національної системи забезпечення безпеки у публічно-інформаційній сфері й підсилити її стійкість до гібридних загроз.

8. Систематизовано й здійснено порівняльний аналіз моделі забезпечення національної безпеки у публічно-інформаційній сфері провідних зарубіжних держав (США, країн ЄС, зокрема Франції, Німеччини та Естонії, Республіки Польща, Ізраїлю та Китаю) з виокремленням їх інституційних, нормативно-правових, технологічних та освітніх компонентів. Такий аналіз дав змогу окреслити загальні тенденції, спільні риси та ключові відмінності різних підходів до управління інформаційною безпекою.

9. Проаналізовано загальні наукові підходи, представлені в працях С. Єсімова, В. Антонюка, В. Калетніка, Ю. Лісовської, М. Баран, О. Пугачова, В. Кондратенка та О. Сокуренко; засвідчено наявність сформованої концептуальної бази модернізації адміністративно-правового забезпечення національної безпеки в публічно-інформаційній сфері. Водночас сучасні трансформаційні процеси, пов’язані з цифровізацією публічного управління, широким упровадженням штучного інтелекту, платформізацією комунікацій та еволюцією гібридних впливів, потребують подальшого розвитку цих підходів, їх

конкретизації, переходу до ризик-орієнтованої моделі та посилення людиноцентричного виміру управління.

10. За результатами дослідження запропоновано авторські напрями вдосконалення адміністративно-правового регулювання, які послідовно розвивають і систематизують наявні доктринальні положення. З-поміж ключових пропозицій: нормативне закріплення класифікації інформаційних систем за рівнями ризику; запровадження оцінки впливу цифрових проєктів на інформаційну безпеку; інституціоналізація управління державними інформаційними ресурсами через уповноваженого з управління даними та регламентація повного життєвого циклу даних; формування правового режиму використання алгоритмічних систем і штучного інтелекту з людиноцентричними процедурами перегляду рішень; розвиток механізмів співрегулювання й саморегулювання цифрових платформ; нормативне визначення ролі органів місцевого самоврядування в забезпеченні інформаційної безпеки та впровадження мультирівневого управління; посилення гарантій інформаційних прав людини через створення інституту омбудсмана з цифрових прав; розвиток аналітико-прогностичної підсистеми національної безпеки та формування національного центру моніторингу інформаційних операцій.

11. Реалізація запропонованих напрямів забезпечує формування стійкої, динамічної та людиноцентричної моделі адміністративно-правового забезпечення національної безпеки у публічно-інформаційній сфері України, здатної ефективно протидіяти сучасним кібер- та інформаційним загрозам і відповідати вимогам європейських безпекових стандартів та принципам цифрового врядування.

ВИСНОВКИ

1. Систематизація здобутих результатів засвідчує, що в процесі розкриття поняття, змісту й сутності національної безпеки в публічно-інформаційній сфері уточнено її змістове наповнення та теоретичні межі. Національна безпека у цій сфері є комплексним, міждисциплінарним і світоглядним феноменом, що охоплює техніко-організаційні механізми захисту інформаційного простору й гуманітарний вимір, пов'язаний із духовною, культурною та ціннісною стійкістю суспільства. Інформаційні процеси дедалі більше впливають на формування політичних рішень, суспільних настроїв та національної ідентичності, а відтак їхня захищеність стає визначальною умовою державної стабільності.

Національна безпека в інформаційній сфері виявляється в здатності держави забезпечити захищеність критичної інформаційної інфраструктури, цілісність державних інформаційних ресурсів, безпечність комунікаційного простору й створити умови для інформаційної взаємодії, заснованої на достовірності, правдивості й відповідальності. Актуальною стає протидія інформаційним маніпуляціям, пропагандистським впливам та деструктивним практикам, спрямованим на підрив національної єдності, спотворення історичної пам'яті та девальвацію демократичних засад суспільного життя.

Сутність національної безпеки в публічно-інформаційній сфері полягає у формуванні стійкого, збалансованого й самодостатнього інформаційного середовища, що забезпечує безперервність функціонування державних інститутів, захист прав і свобод людини, підтримку демократичних процесів і розвиток громадянського суспільства. Національна безпека є інструментом державної політики та інтегрованим правовим і ціннісним феномен, що визначає напрям модернізації держави в умовах цифрової трансформації та глобальної інформаційної конкуренції.

2. Обґрунтовано, що система адміністративно-правового регулювання інформаційної безпеки постає як структурно впорядкований комплекс

нормативних, інституційних і процедурних елементів, спрямованих на забезпечення цілісності та захищеності національного інформаційного простору, реалізацію державної політики у сфері національної безпеки й утвердження принципів правової держави в умовах цифрової трансформації. Її концептуальна сутність полягає в поєднанні правових норм й управлінських механізмів, що формують цілісну модель правового впливу, засновану на принципах законності, публічності, пропорційності й ефективності.

У результаті дослідження встановлено, що принципи адміністративно-правового регулювання інформаційної безпеки мають нормативно-доктринальну природу, оскільки водночас віддзеркалюють законодавчу волю держави та науково-теоретичне осмислення специфіки публічного управління в інформаційній сфері. Аналіз загальноправових, адміністративно-правових і спеціальних принципів дав змогу сформувати авторську класифікацію, релевантну сучасним викликам інформаційної політики й тенденціям європейського правового розвитку.

У стислому вигляді така класифікація охоплює три рівні: за сферою дії – загальноправові (верховенство права, законність, пріоритет прав людини); адміністративно-правові (публічність, відкритість, підзвітність, ефективність); спеціальні (достовірність та цілісність даних, баланс свободи інформації та захисту, технологічна адаптивність); за функціональним призначенням – регулятивні, гарантійні, превентивно-захисні, інтеграційно-координаційні; за змістовно-ціннісною орієнтацією – демократично-правові, безпеково-захисні, етико-гуманітарні. Сформована система принципів забезпечує теоретичне підґрунтя для подальшого розроблення ефективних механізмів державної інформаційної політики, удосконалення правового забезпечення кібербезпеки й зміцнення стійкості інформаційного середовища України в умовах наростання гібридних загроз.

3. Аналіз нормативно-правових актів, що регулюють забезпечення національної безпеки в інформаційній сфері України, засвідчує наявність розгалуженої, проте фрагментованої й недостатньо узгодженої системи правового забезпечення. Попри існування значної кількості законів, підзаконних актів, стратегічних документів і секторальних політик, їх результативність обмежена через наявність концептуальних, термінологічних і процедурних невідповідностей.

Виявлені процедурно-нормативні колізії підтверджують системність проблеми, що охоплює термінологічний, інституційний, процедурний та ієрархічний рівні правового регулювання. Неузгодженість ключових категорій (інформаційна безпека, кібербезпека, інформаційний простір, критична інформаційна інфраструктура) ускладнює правозастосування та спричиняє дублювання повноважень між органами влади. Додатковою проблемою є відсутність єдиного координаційного механізму реагування на інформаційні та кіберзагрози.

Для подолання структурних недоліків і підвищення ефективності державної політики у сфері інформаційної безпеки важливо впровадити комплекс взаємодоповнювальних заходів, зокрема ухвалити базовий закон «Про інформаційну безпеку», який забезпечить системність, прозорість і внутрішню узгодженість нормативного поля; гармонізувати українське законодавство з європейськими стандартами (NIS 2, GDPR, Cybersecurity Act), що сприятиме адаптації національної моделі безпеки до найкращих міжнародних практик; забезпечити інституційну консолідацію, зокрема створити єдиний координуючий орган при РНБО для узгодження діяльності суб’єктів сектора безпеки й оборони; стандартизувати процедури реагування, моніторингу й оцінювання інформаційних загроз, що дозволить підвищити оперативність і передбачуваність державних дій; формувати державний реєстр кіберінцидентів як інструмент ризик-менеджменту та оперативного управління інцидентами.

Стверджено, що нормативно-правова база в сфері інформаційної безпеки України потребує глибокої модернізації, спрямованої на її систематизацію, узгодження та увідповіднення із сучасними викликами цифрової епохи. Реалізація запропонованих заходів стане ключовою передумовою підвищення стійкості держави до інформаційних загроз і наближення України до європейських стандартів безпеки.

4. Дослідження діяльності органів публічної влади у сфері забезпечення національної безпеки в публічно-інформаційному просторі засвідчило, що ефективність системи інформаційної безпеки України забезпечується взаємодією державних, муніципальних і суспільних інститутів та чітким розмежуванням їхніх повноважень.

Для підвищення ефективності управління інформаційною безпекою запропоновано функціональне розмежування суб'єктів на три взаємопов'язані рівні: стратегічно-керівний рівень – Президент України, Верховна Рада України, РНБО, Кабінет Міністрів України, які формують державну політику, визначають пріоритети, ухвалюють стратегічні рішення та затверджують нормативні документи у сфері інформаційної безпеки; операційно-виконавчий рівень – органи державної влади та правоохоронні структури (Мінцифра, ДССЗЗІ, СБУ, Національна поліція тощо), що реалізують державну політику, забезпечують кіберзахист, здійснюють оперативне реагування на інформаційні загрози та координують міжвідомчу діяльність; суспільно-громадський рівень – інститути громадянського суспільства, засоби масової інформації, освітні й аналітичні установи, що здійснюють демократичний контроль, підвищують рівень медіаграмотності населення та формують культуру інформаційної безпеки.

Запропонована трирівнева типологія дає змогу чітко визначити сфери відповідальності, повноваження і канали взаємодії суб'єктів інформаційної безпеки, поєднуючи інституційний і функціональний підходи, а також враховуючи рівень управлінської компетентності. Її практичне впровадження

може стати основою для розроблення Концепції єдиної системи управління інформаційною безпекою, що забезпечить узгодженість дій між державними, муніципальними та громадськими структурами.

У межах удосконалення правового регулювання обґрунтовано доцільність внесення змін до Закону «Про національну безпеку України» для чіткого визначення відповідальності держави, бізнесу та громадян; оновлення Закону України «Про основні засади забезпечення кібербезпеки України», зокрема шляхом упровадження регулярної сертифікації державних ІТ-систем тощо.

5. З’ясовано роль правоохоронних органів у забезпеченні безпеки інформаційного простору держави й установлено, що їх діяльність є ключовим складником національної системи інформаційної безпеки, оскільки саме ці органи здійснюють виявлення, документування, припинення та розслідування правопорушень у кіберсфері, протидію інформаційним загрозам, а також координацію державних заходів із захисту цифрового простору.

На підставі проведеного аналізу сформульовано висновок про важливість комплексного вдосконалення діяльності Служби безпеки України та інших правоохоронних органів у сфері інформаційної безпеки. Запропоновані заходи спрямовано на перехід від фрагментарного й реактивного реагування до цілісної, проактивної й ризик-орієнтованої моделі захисту інформаційного простору держави. Зокрема, обґрунтовано такі напрями вдосконалення: нормативне уточнення повноважень СБУ та чітке розмежування компетенцій між основними суб’єктами інформаційної безпеки для уникнення дублювання функцій; інтеграція інформаційних систем і створення єдиної захищеної платформи обміну даними, що забезпечить оперативність реагування на кіберінциденти; гармонізація нормативно-технічної бази СБУ з міжнародними стандартами кіберзахисту та впровадження незалежного аудиту технічних засобів безпеки; підвищення прозорості діяльності шляхом уведення щорічного відкритого звіту СБУ щодо стану кіберзагроз і результатів їх нейтралізації; удосконалення

кадрової системи, створення сучасної моделі підготовки фахівців із кібербезпеки в співпраці із закладами вищої освіти.

Особливу увагу приділено ролі Національного координаційного центру кібербезпеки (НКЦК), інституційну спроможність якого запропоновано посилити шляхом законодавчого закріплення статусу центрального координатора у сфері безпеки, упровадження єдиних протоколів інформаційної взаємодії, інтеграції систем реагування в межах єдиного національного простору оперативного реагування; розвитку громадсько-приватного партнерства.

Такі кроки сприятимуть формуванню національної моделі оперативного реагування на кіберінциденти відповідно до вимог NIS2 та сучасних європейських стандартів кіберстійкості.

Окремо підкреслено важливість переходу до превентивної моделі управління кіберризиками, що передбачає створення систем раннього виявлення кіберінцидентів, формування аналітичних підрозділів кіберрозвідки, їх інтеграцію з НКЦК та розроблення національної методології оцінювання кіберризиків. Такий підхід забезпечить своєчасне виявлення загроз і зміцнить загальну стійкість держави до деструктивних інформаційно-кібернетичних впливів.

6. У результаті дослідження встановлено, що механізми адміністративно-правового реагування та запобігання інформаційним загрозам становлять цілісну багаторівневу систему, що поєднує юридичні, організаційні та процедурні інструменти впливу держави на інформаційні процеси. Їх призначення полягає у створенні правових умов для забезпечення відповідності функціонування інформаційного простору вимогам національної безпеки, стабільності та законності. На підставі проведеного аналізу уточнено зміст механізму адміністративно-правового реагування, який доцільно розглядати як комплекс превентивного, контрольного та примусового впливу, що забезпечує своєчасне

виявлення загроз, локалізацію їх наслідків та гарантування невідворотності юридичної відповідальності.

Удосконалено підхід до класифікації адміністративно-правових механізмів, визначено їх як превентивні, оперативно-реагувальні та юрисдикційні, кожен із них виконує самостійну, проте взаємопов'язану функцію в державній системі інформаційної безпеки. Інтеграція цих механізмів інтеграція забезпечує дотримання принципів законності, пропорційності, публічності та збалансування між інтересами національної безпеки й правами людини у цифровому середовищі. Сформована модель створює передумови для побудови ефективної адміністративно-правової інфраструктури реагування на інформаційні загрози та підвищує кіберстійкість держави в умовах динамічних викликів сучасного інформаційного простору.

7. Узагальнення результатів аналізу зарубіжних моделей забезпечення національної безпеки в публічно-інформаційній сфері засвідчує, що провідні держави світу розглядають інформаційну безпеку як стратегічний пріоритет, інтегрований у ширший комплекс правових, інституційних, технологічних, освітніх та міжнародно-координаційних механізмів. Незалежно від національної специфіки інформаційну безпеку витлумачено не як вузько технічне, а як багатовимірне політико-правове явище, що вимагає системної інституційної архітектури. що вимагає наявності стабільної інституційної архітектури та чітко визначених державних повноважень. Ключова роль у таких моделях належить спеціалізованим національним агентствам, урядовим CERT-структурам, координаційним радам та центрам передового досвіду, які забезпечують стратегічне планування, міжвідомчу взаємодію, реагування на кіберінциденти й кооперацію з міжнародними партнерами.

Аналіз практик США, ЄС, Франції, Німеччини, Естонії, Польщі, Ізраїлю та Китаю засвідчує, що ефективна політика в інформаційному просторі можлива лише за умов: наявності чіткої нормативної бази, узгодженої зі світовими

стандартами; розвинених процедур захисту критичної інфраструктури; системних механізмів протидії дезінформації та маніпулятивному впливу; сформованої культури інформаційної та цифрової грамотності населення. При цьому різні держави реалізують відмінні парадигми управління інформаційним простором: від демократичної, інституційно-координаційної моделі до концепції «кіберсуверенітету», орієнтованої на посилений державний контроль. Спільним для всіх є визнання того, що стійкість національного інформаційного простору не можлива без міжнародної кооперації, обміну розвідувальними даними, участі в міжнародних структурах кібербезпеки та формування спільних стандартів реагування на загрози. Для України найбільш релевантними є ті елементи зарубіжного досвіду, які поєднують інституційну координацію, правову визначеність, освітньо-науковий розвиток та активну міжнародну співпрацю, що може стати фундаментом подальшого зміцнення національної публічно-інформаційної безпеки в умовах гібридних загроз та інтеграції до європейського безпекового простору.

8. Дослідження засвідчує, що сучасні трансформаційні виклики – цифровізація публічного управління, упровадження штучного інтелекту, розвиток глобальних цифрових платформ і поширення гібридних загроз – зумовлюють потребу в переході від декларативної моделі правового регулювання до комплексного, ризик-орієнтованого та людиноцентричного підходу. У цих умовах особливої ваги набуває формування єдиної системи управління державними інформаційними ресурсами, визначення правового режиму алгоритмічних систем і штучного інтелекту, розвиток механізмів співрегулювання з цифровими платформами та посилення інституційних гарантій інформаційних прав людини.

Запропоновано авторські напрями вдосконалення ключових складників публічно-інформаційної безпеки, з-поміж яких ризик-орієнтоване регулювання інформаційних систем; інституціоналізація управління даними шляхом

створення інституту уповноважених із data governance; установлення прозорого та людиноцентричного режиму застосування алгоритмічних систем і ШІ; розвиток механізмів співрегулювання й саморегулювання цифрових платформ; нормативне закріплення мультирівневого управління інформаційною безпекою та створення регіональних центрів кіберстійкості; посилення гарантій інформаційних прав людини; розвиток аналітико-прогностичних механізмів державного реагування на загрози. Реалізація цих заходів сприятиме формуванню стійкої, динамічної та людиноцентричної моделі національної безпеки в публічно-інформаційній сфері України, що відповідає європейським стандартам, принципам NIS2 та сучасним вимогам ефективного публічного адміністрування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Ізбаш К. С., Деревянкін С. Л. Національна безпека України в умовах воєнного стану: сучасний стан. *Південноукраїнський правничий часопи*с. 2024. № 1. С. 213–217. URL : https://surl.li/uhgqxg.
2. Ціцерон М. Т. Тускуланські бесіди. Про обов'язки. Пер. з англ. В. Литвинов. Ви-во Апріорі. 2021. 440 с.
3. Коломієць Б. С. Еволюція поняття безпеки : від класичних теорій до сучасних підходів. *ECONOMICS: time realities.* № 6(76), 2024. С. 47–54. URL : https://economics.net.ua/files/archive/2024/No6/47.pdf.
4. Plato. The Republic. Translated by Benjamin Jowett. Project Gutenberg, 1998. URL :https://www.gutenberg.org/files/1497/1497-h/1497-h.htm.
5. Гоббс Т. Левіафан, або Суть, будова і повноваження держави церковної та цивільної / пер. з англ. Київ : Дух і Літера, 2000. С. 601. URL : https://surl.li/wgdbst.
6. Вовк О. О. Теоретико-правовий аналіз співвідношення понять державної та зовнішньої безпек. *Часопис Київського університету права*. 2013. № 2. С. 43–48.
7. Настюк В. Я. Сучасні підходи до визначення сутності та поняття державної безпеки. *Сучасний стан та перспективи розвитку сектору безпеки України: публічно-приватні аспекти*: матеріали III міжнар. наук.-практ. конф., м. Харків, 16 квітня 2015 р. Харків, 2015. С. 56–58.
8. Янчук А. О. Особливості вдосконалення нормативно-правового забезпечення державної безпеки України в сучасних умовах. *Науковий вісник Львівського державного університету внутрішніх справ. Серія «Юридична».* 2016. Вип. 1. С. 342–355.
9. Козьяков І. Законодавче визначення державної безпеки: проблеми теорії та практики. *Підприємництво, господарство і право.* 2019. № 9. С. 160–164. URL : http://pgp-journal.kiev.ua/archive/2019/9/27.pdf.

10. Воротнюк М. О. Концепція людської безпеки: теоретичні аспекти. URL : https://surl.li/ddeksm.
11. Воротнюк М., Сушко О. Людська безпека як імператив сучасної епохи: переніс фокусу з держави на людину / Фонд ім. Фрідріха Еберта: представництво в Україні. Київ; Бонн, 2011. 18 с. URL : https://library.fes.de/pdf-files/bueros/ukraine/07749.pdf.
12. Білий В. І., Михальчук В. М. Основні напрями забезпечення національної безпеки держави. *Інвестиції: практика та досвід.* 2021. № 17. С. 92–98.
13. Маркович Х. М. Національна безпека України: понятійно-категоріальне осмислення. *Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична*. 2023, Вип. 38. С. 10–15.
14. Собакарь А. О., Ковалів М. В. Адміністративно-правові засади діяльності державних органів у сфері забезпечення національної безпеки. *Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки*. 2016. № 845. С. 156–160.
15. Ізбаш К. С., Деревянкін С. Л. Національна безпека України в умовах воєнного стану: сучасний стан. *Південноукраїнський правничий часопис.* 2024. № 1. С. 213–217.
16. Корж І. Безпека: методологічні підходи до поняття. *Журнал юридичних наук.* 2019. № 4 (ч. 1). С. 111–124. URL : https://surl.li/wufdgy.
17. Мельниченко Б., Фігель Н. Основні підходи до розуміння поняття «національна безпека». *Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки*. 2016. № 2(30). С. 68–72. URL : https://science.lpnu.ua/sites/default/files/journal-paper/2021/aug/24795/11.pdf.
18. Загуменна Ю. О. Концептуалізація феномену національної безпеки: правовий аспект. *Форум права.* 2021. Вип. 1. С. 37–55. URL : https://forumprava.pp.ua/files/037-055-2021-1-FP-Zagumenna_6.pdf.

19. Прохожев А. А. Національна безпека: до єдиного розуміння суті термінів. *Безпека.* 1995. № 9 (29). С. 23.
20. Національна безпека: світоглядні та теоретико-методологічні засади : монографія / за заг. ред. О. П. Дзьобаня. Харків : Право, 2021. 776 с.
21. Кузнецова М. Ю. Сфера публічної інформації: поняття, структура, загальна характеристика суспільних та правових відносин. *Юридичний науковий електронний журнал.* 2014. № 4. С. 148–152. URL : http://www.lsej.org.ua/4_2014/38.pdf.
22. Крушеніцький В. С. Публічно-інформаційна сфера як складова системи національної безпеки України. *Право і суспільство.* 2023. С. 585–590. URL : http://pravoisuspilstvo.org.ua/archive/2023/3_2023/88.pdf.
23. Про національну безпеку України: Закон України від 21.06.2018. № 2469-VIII. URL : https://zakon.rada.gov.ua/laws/show/2469-19#Text.
24. Горбенко О. І. Інформаційна та кібербез-пека: концептуальні засади та практичні аспекти. Харків : видавництво «Фоліо». 2017. 320 с.
25. Гончаренко Г. А. До проблеми визначення та розмежування дефініцій «інформаційна безпека» і «кібербезпека». *Електронне наукове видання «Аналітично-порівняльне правознавство».* С. 466 471. URL : http://journal-app.uzhnu.edu.ua/article/view/313097/304139.
26. Морозов С. П. Стратегії забезпечення інформаційної та кібербезпеки держави. Дніпро : Акцент. 2018. 268 с.
27. Ткаченко І. В. Кібербезпека та захист інформаційних систем. Вінниця: видавництво «Нова книга». 2015. 298 с.
28. Звіти – Центр протидії дезінформації при Раді національної безпеки та оборони України. Центр протидії дезінформації. URL : https://cpd.gov.ua/category/reports/.
29. Поліщук А. «Інтерв'ю із засновницею волонтерської ініціативи «Як не стати овочем» Оксаною Мороз. «День». 2020. 19 берез.

30. Чайкун Е. С. Проблема інформаційного імунітету та викликів інфодемії. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Філологія. Журналістика.* 2023. Том 34 (73) № 1 Ч. 2. С. 244–253. URL : https://surl.li/qtltzu.
31. Шестак В. С. Роль адміністративного права у правовому забезпеченні реалізації окремих функцій держави суб'єктами публічного управління (на прикладі культурної функції). *Науковий вісник Ужгородського національного університету. Серія : Право*. 2015. Вип. 34(2). С. 151–154.
32. Надьон О. В. Адміністративно-правове забезпечення фінансової безпеки банків: поняття та необхідні ознаки. *Науковий вісник Ужгородського національного університету. Серія : Право.* 2016. Вип. 39(2). С. 17–21.
33. Матвійчук А. В. Адміністративно-правое забезпечення державної регуляторної політики. *Підприємництво, господарство і право*. 2019. № 1. С. 108–111.
34. Гумін О. М., Пряхін Є. В. Адміністративно-правове забезпечення: поняття та структура. *Наше право.* 2014. № 4. С. 46–50.
35. Моргунов О. А. Поняття та механізм адміністративно-правового регулювання публічного адміністрування сфер фізичної культури і спорту. *Юридичний науковий електронний журнал.* 2019. № 3. С. 274–277. URL : http://www.lsej.org.ua/3_2019/72.pdf.
36. Теремецький В. І. Поняття адміністративно-правового регулювання у сфері оподаткування. *Держава та регіони. Серія «Право».* 2012. № 1(35). С. 50–54.
37. Литовченко П. В. Поняття адміністративно-правового регулювання у сфері комунального господарства. *Митна справа*. 2012. № 2(80). частина 2, кн. 2. 130 с.
38. Стеценко С. Г. Адміністративне право України : навчальний посібник. Київ : Атіка, 2007. 624 с.

39. Буга Г. С., Кузьменко С. Г. Поняття адміністративно-правового регулювання підприємницької діяльності. *Право та державне управління.* 2023. № 4. С. 317–321. URL : https://surl.li/yxewda.
40. Баран М. В. Інформаційна безпека як предмет адміністративно-правового регулювання. URL : https://surl.li/jqtcvo.
41. Трансформаційні процеси безпекового середовища у воєнний час. (м. Кам'янське, 20 березня 2025 р. Кам'янське : ГО «Молодіжна Організація Починаючих Лідерів «ГО МОПЛ», 2025.
42. Данильян О. Г., Тараненко В. М. Філософія: підручник. Харків : Право, 2010. 312 с.
43. Большой энциклопедический словарь : в 2 т. / под ред. А. М. Прохорова. М. : Сов. энцикл., 1991. Т. 2. 768 с.
44. Прангишвили И. В. Системный подход и общесистемные закономерности. М. : СИНТЕГ, 2000. 528 с.
45. Тарасенко В. С. Система адміністративно-правового регулювання статусу Кабінету Міністрів України у сфері наукової і науково-технічної діяльності в Україні. Вісник ХНУВС. 2021. № 2(93). С. 203-212. URL : https://surl.li/kmslvz.
46. Конституція України від 28.06.1996 р. № 254к/96-ВР. URL : https://surl.li/gskasv.
47. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL : https://surl.li/oasxeb.
48. Горбулін В. П. Рада національної безпеки і оборони України (РНБО України). URL : https://surl.lu/urdavq.
49. Шедяков В. Поліцентризм як принцип суспільного структурування. *Collection of Scientific Papers «SCIENTIA»*, (April 14, 2023; Bern, Switzerland), 21–25. Retrieved from. URL : https://surli.cc/bywyvi.

50. Безпалова О. Сутність та значення координаційних органів як суб'єктів реалізації державної політики. *Підприємництво, господарство і право.* 2020. № 6. С. 105–109. URL http://pgp-journal.kiev.ua/archive/2020/6/20.pdf.
51. Сівков С. «Взаємодія» і «координація»: масштабність понять. *Закон и жизнь*. 2013. № 6. С. 27–29. URL : https://surl.li/tmerub
52. Білоус В. Т. Координація боротьби з економічною злочинністю : монографія. Ірпінь : Академія держ. подат. служби, 2012. 449 с.
53. Адміністративне право України (загальна частина): навчальний посібник / О. І. Остапенко, М. В. Ковалів, С. С. Єсімов і інші. Львів: Національний університет «Львівська політехніка», 2019. 504 с.
54. Баран М. В. Принципи правового регулювання інституту інформаційної безпеки. *Науковий вісник Ужгородського Національного Університету*. 2021. Випуск 66. С. 129–134. URL : https://surl.lu/agzdtn.
55. Свиридюк Н. П., Цюприк Н. О. Принципи адміністративно-правового регулювання у сфері гендерної політики держави. Південноукраїнський правничий часопис. Одеса, ОДУВС. 2017 № 3. С. 121–125, С. 122.
56. Теорія держави і права: навч. посіб. / С. К. Бостан, С. Д. Гусарєв, Н. М. Пархоменко та ін. Київ: ВЦ «Академія», 2013. 348 с.
57. Музика С. С. Принципи адміністративно-правового режиму конфіденційної інформації в національній поліції України. *Юридичний науковий електронний журнал.* 2022. № 1. С. 405–408. URL : http://lsej.org.ua/1_2022/101.pdf.
58. Олійник О. В. Принципи забезпечення інформаційної безпеки України. *Науковий вісник Ужгородського університету. Серія ПРАВО.* 2012. Вип. 18. С. 170−173.
59. Александрова М. В. Адміністративно-правове забезпечення інформаційної безпеки у сфері електронного урядування : дис. ... д-ра філософії : 081 –

Право / ПрАТ «Вищий навчальний заклад «Міжрегіональна академія управління персоналом» ; наук. кер. Ю. П. Тимошенко. Київ, 2024. 245 с.

60. Чубарук Т. В. Конституційні засади правового регулювання інформаційної сфери. Правова інформатика, 2010 р. URL : https://surl.li/tllfgb.
61. Шемчук В. В. Конституційно-правові засади розвитку інформаційного суспільства в Україні. *Науковий вісник Національної академії внутрішніх справ.* № 3(108), 2018 р. URL : https://surli.cc/gzhljx.
62. Коментарі до проекту Закону України «Про інформаційну безпеку України» (від 22.09.2004 № 5732). Харківська правозахисна група. URL : https://surl.li/smooda.
63. Шевчук М. О. До питання конституційних засад інформаційної безпеки держави. *Електронне наукове видання «Аналітично-порівняльне правознавство».* 2025. № 1. С. 563–568. URL : https://app-journal.in.ua/wp-content/uploads/2025/02/96.pdf.
64. Про затвердження Порядку отримання дозволу суду на здійснення заходів, які тимчасово обмежують права людини, та використання добутої інформації: Постанова Кабінету Міністрів України від 26 вересня 2007 р. № 1169. URL : https://zakon.rada.gov.ua/laws/show/1169-2007-%D0%BF#Text.
65. Тоцький Б. А. Принцип пропорційності: історичний аспект і теоретичні складові. *Часопис Київського університету права.* 2013. № 3. С. 70–74. URL : http://nbuv.gov.ua/UJRN/Chkup_2013_3_18.
66. Завидняк І. І. Обмеження прав людини і основоположних свобод у контексті принципу пропорційності (на прикладі конституційних засад діяльності Служби безпеки України). *Науковий вісник Ужгородського національного університету. Серія «Право».* 2012. Вип. 19. Т. 1. С. 164–167. URL : https://surl.li/exseug.

67. Майданик Р. А. Пропорційність (співрозмірність) і право власності: доктрина і судова практика. *Право України.* 2016. № 1. С. 41–54. URL : https://surl.li/nfwzvm.
68. Шинкан Т. Застосування принципу пропорційності в заходах інформаційної безпеки та встановлення в інтересах національної безпеки обмежень щодо реалізації права на інформацію. *Наука і правоохорона*. 2025. Вип. 1–2. С. 67–68.
69. Манжула А. А. Адміністративно-правові засади організації діяльності науково-дослідних установ в Україні: автореф. дис. ... доктора. юрид. наук : 12.00.07. Харківський національний університет внутрішніх справ. Харків, 2016. 40 с.
70. Пирожкова Ю. В. Адміністративно-правове регулювання у сфері автомобілебудування в Україні: дис. ... канд. юрид. наук : 12.00.07. Ірпінь, 2007. 233 с.
71. Ківалов С. В. Адміністративне право України: Підручник. Одеса : Юрид. літ., 2003. 896 с.
72. Тюря Ю. І. Визначення принципів публічного адміністрування діяльності зі створення, впровадження та використання штучного інтелекту в Україні. *Приватне та публічне право*. 2022. № 2. С. 73 –78.
73. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI. URL : https://zakon.rada.gov.ua/laws/show/2939-17#Text.
74. Мілевський А. Характеристика принципів адміністративних послуг, що надаються підрозділами Міністерства юстиції України. *Підприємництво, господарство і право.* 2019. № 6. С. 173–177. URL : https://surl.li/sduxld.
75. Конвенція про захист прав людини і основоположних свобод від 04.11.1950. URL : https://zakon.rada.gov.ua/laws/show/995_004#Text.
76. Про інформацію : Закон України від 02.10.1992 № 2657-XII. URL : https://zakon.rada.gov.ua/laws/show/2657-12#Text.

77. Про захист персональних даних : Закон України від 01.06.2010 № 297-VI. URL : https://zakon.rada.gov.ua/laws/show/2297-17/ed20180130#Text.
78. Директива Європейського Парламенту і Ради(ЄС) 2022/2555 від 14 грудня 2022 р. про заходи для високого спільного рівня кібербезпеки на всій території Союзу, якою вносяться зміни до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972 і скасовується Директива (ЄС) 2016/1148 (Директива NIS 2). URL : https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text.
79. Пащенко Є. М., Корольов С. С., Гашенко С. В., Мороховський М. Л., Прозванюк О. В. Правові основи інформаційної безпеки, інформатизації та зв'язку в електромагнітному середовищі та кіберпросторі як складова забезпечення виконання завдань підрозділами сил оборони і безпеки України. *Юридичний науковий електронний журнал.* 2024. № 12. С. 456–459. URL : http://lsej.org.ua/12_2024/107.pdf.
80. Handyside v. the United Kingdom : Judgment of 7 December 1976 : Application no. 5493/72 // European Court of Human Rights. Series A. No 24. URL : https://hudoc.echr.coe.int/eng?i=001-57499.
81. Sunday Times v. the United Kingdom (No. 1) : Judgment of 26 April 1979 : Application no. 6538/74 // European Court of Human Rights. Series A. No 30. URL : https://hudoc.echr.coe.int/eng?i=001-57584.
82. Про медіа : Закон України від 13.12.2022 № 2849-IX. URL : https://zakon.rada.gov.ua/laws/show/2849-20#Text.
83. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX. URL : https://zakon.rada.gov.ua/laws/show/1089-20#Text.
84. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII. URL : https://zakon.rada.gov.ua/laws/show/2155-19#Text.

85. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. URL : https://zakon.rada.gov.ua/laws/show/1882-20#Text.
86. Конвенція Ради Європи № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» від 28 січня 1981 р. URL : https://zakon.rada.gov.ua/laws/show/994_326#Text.
87. Регламент (ЄС) 2016/679 Європейського парламенту і Ради від 27 квітня 2016 р. «Про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних, а також про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних – GDPR»). URL : https://surl.li/igtgji.
88. Дзюкевич К. Адаптація єдиного ринку ЄС до епохи цифровізації. Економіка та суспільство. 2023. Вип. 54. URL : https://surl.li/rfuqrf.
89. Директива (ЄС) 2022/2557 Європейського парламенту і Ради від 14 грудня 2022 р. «Про стійкість критичних суб'єктів та про скасування Директиви Ради 2008/114/ЄС». URL : https://surl.li/kcnbey.
90. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» від 25 лютого 2017 р.: Указ Президента України № 47/2017. URL : https://surl.lt/ftxpol.
91. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : указ Президента України № 392/2020. URL : https://surl.li/rdqqvr.
92. Про рішення Ради національної безпеки і оборони України від 14.05.2021 «Про Стратегію кібербезпеки України»: указ Президента України № 447/2021. URL : https://zakon.rada.gov.ua/laws/show/447/2021#Text.
93. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : постанова Кабінету Міністрів України від 19.06.2019 № 518. URL : https://zakon.rada.gov.ua/laws/show/47/2017#Text.

94. Деякі питання об’єктів критичної інформаційної інфраструктури: Постанова Кабінету Міністрів України від 09.10.2020 № 943. URL : https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text.

95. Європейська конвенція про захист прав людини і основоположних свобод від 04.11.1950 (ратифікована Законом України від 17.07.1997 № 475/97-ВР). URL : https://zakon.rada.gov.ua/laws/show/995_004#Text.

96. Будапештська конвенція про кіберзлочинність від 23.11.2001 (ратифікована Законом України від 07.09.2005 № 2824-IV). URL : https://zakon.rada.gov.ua/laws/show/994_575#Text.

97. Про схвалення Стратегії розвитку інформаційного суспільства в Україні : розпорядження Кабінету Міністрів України від 15.05.2013. № 386-2013-р. URL : https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80#n8.

98. Про Службу безпеки України : Закон України від 25.03.1992 № 2229-XII. URL : https://zakon.rada.gov.ua/laws/show/2229-12/ed20000225.

99. Питання Міністерства цифрової трансформації України: постанова Кабінету Міністрів України від 18.09.2019 № 856. URL : https://surl.li/ncpzrk.

100. Європейський парламент і Рада Європейського Союзу. Регламент (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв’язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних, GDPR) // Офіційний вісник Європейського Союзу. 2016. L 119. С. 1–88. URL : https://eur-lex.europa.eu/eli/reg/2016/679/oj.

101. Глобенко І. О. Особливості адміністративно-правового статусу суб’єктів публічної адміністрації в Україні. *Науковий вісник публічного та приватного права*. 2020. Вип. 4. С. 82 –86.

102. Волох Д. О. Поняття та ознаки суб’єктів публічного права. *Наукові записки. Серія: Право.* 2025. Вип. 18. С. 190–195.

103. Про основи національної безпеки України : Закон України від 19.06.2003 № 964-IV. URL: https://zakon.rada.gov.ua/laws/show/964-15.

104. Нестеренко О. В. Система суб'єктів забезпечення національної безпеки і оборони України. *Право і безпека.* 2020. № 2(77). С. 33–39. URL : file:///C:/Users/HP/Downloads/gekova,+6.pdf.

105. Олійник О. В. Теоретико-методологічні засади адміністративно-правового забезпечення інформаційної безпеки України: монографія. Київ: Укр. пріоритет, 2012. 400 с.

106. Стебловський В. В. Суб'єкти побудови безпекового середовища в інформаційній сфері: поняття, види. *Науковий вісник Ужгородського Національного Університету. Серія Право.* 2025. Вип. 89: Ч. 3. С. 112–116. URL : https:// isnyk-juris-uzhnu.com/wp-content/uploads/2025/07/18-3.pdf

107. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021року «Про Стратегію інформаційної безпеки»: указ Президента України 28.12.2021 №685/2021. URL : https://surl.li/itgbeq.

108. Питання Міністерства цифрової трансформації: постанова Кабінету Міністрів від 18.09.2019 № 856. URL : https://surl.li/iwtcrg .

109. Розпаченюк А. С. Міністерство цифрової трансформації як суб'єкт публічно управлінської діяльності: правовий аспект. *Ірпінський юридичний часопис: науковий журнал.* 2024. Вип. 2 (15). С. 182–189. URL : file:///C:/Users/HP/Downloads/20.pdf

110. Міністерство цифрової трансформації / Офіційний вебсайт. URL : https://thedigital.gov.ua/ministry.

111. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 № 3475-IV URL : https://zakon.rada.gov.ua/laws/show/3475-15#Text.

112. Коц Д. В. Повноваження державної служби спеціального зв'язку та захисту інформації України щодо нормативно-правового регулювання

захисту інформації з обмеженим доступом. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право.* Випуск 2(50) 2021. С. 138–142. URL : https://zakon.rada.gov.ua/laws/show/3475-15#Text.

113. Уряд доручив Адміністрації Держспецзв'язку організовувати акредитацію з питань безпеки українських інформаційно-комунікаційних систем для оброблення інформації НАТО з обмеженим доступом. Державна служба спеціального зв'язку та захисту інформації України : вебсайт. URL : https://surl.li/wfsoqc.

114. Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації : постанова Кабінету Міністрів України від 03.09.2014 № 411 URL : https://surl.li/kjbsmv.

115. Петров С. Г. Проблеми захисту державних електронних інформаційних ресурсів у контексті цифрових трансформацій і цифровізації в Україні. *Електронне наукове видання «Порівняльно-аналітичне право».* 2020. № 3. С. 126–132.

116. Щиголь Ю. Національну безпеку монетизувати не можна. URL : https://surl.li/xthost.

117. Про затвердження Положення про Міністерство культури України: постанова Кабінету Міністрів України від 03.09.2014 № 495. URL : https://zakon.rada.gov.ua/laws/show/495-2014-%D0%BF#Text.

118. Батраченко Т. С., Розгон О. Г., Єфімова І. В. Роль правоохоронних органів у забезпеченні інформаційної безпеки держави. *Науковий вісник Університету митної справи та фінансів. Серія: Право.* 2025. № 3(44). С. 25–31. URL : https://surl.li/pzuuia.

119. Лихова С. Я., Сисоєва В. П. Діяльність правоохоронних органів України у сфері забезпечення інформаційної безпеки. *Юридичний вісник*. 2022. № 3(64). С. 102–107. URL :file:///C:/Users/HP/Downloads/16.pdf.

120. Про утворення територіального органу Національної поліції : постанова Кабінету Міністрів України від 13.10.2015 № 831. URL : https://zakon.rada.gov.ua/laws/show/831.

121. Про проведення позачергового атестування осіб начальницького складу підрозділів боротьби з кіберзлочинністю: наказ МВС України від 15.10.2015 № 1250. URL : https://zakon.rada.gov.ua/laws/show/1250.

122. Про проведення конкурсу на заміщення вакантних посад старших інспекторів, інспекторів і спеціальних агентів інформаційних технологій міжрегіонального територіального органу Департаменту кіберполіції Національної поліції: наказ МВС України від 15.10.2015 року № 1251. URL : https://zakon.rada.gov.ua/laws/show/1251.

123. Харченко Н. Кіберполіція України як суб'єкт забезпечення інформаційної функції держави. *Матеріали міжнародної науково-практичної конференції*. Київ: Національна академія внутрішніх справ, 2023. С. 164–166. URL : https://surl.lu/fuzbcm.

124. Казанчук І., Яценко В. Особливості правового регулювання діяльності Національної поліції України у сфері забезпечення інформаційної безпеки в Україні. *Право і безпека.* 2020. № 4(79). С. 32–38. URL : https://surl.li/unuohw.

125. Макарчук В. В. Повноваження правоохоронних органів при реалізації державної політики щодо забезпечення інформаційної безпеки. *Юридичний науковий електронний журнал.* 2022. № 8. С. 324–326. URL : http://lsej.org.ua/8_2022/71.pdf.

126. Нікулін Є. Ю. Адміністративно-правове забезпечення інформаційної безпеки Національної поліції України : дис. … канд. юрид. наук. : 12.00.07. Київ. 2021. 133 с. URL : https://surl.li/rqrjqu.

127. Моргун Н. С., Шевчук О. О., Марчевський С. В. Щодо визначення поняття інформаційної безпеки у діяльності Національній поліції України.

Електронне наукове видання «Аналітично-порівняльне правознавство». С. 409–415. URL : https://surli.cc/mixxbf.

128. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII. URL : https://zakon.rada.gov.ua/laws/show/580-19#Text.
129. Закон України «Про Національну поліцію» : наук.-практ. коментар / кер. авт. кол. д-р юрид. наук, доц. Т. П. Мінка. Дніпро : Дніпропетр. держ. ун-т внутр. справ, 2017. 480 с.
130. Негодченко В. О. Інформаційна безпека в органах Національної поліції України: адміністративно-правове забезпечення. Право і суспільство. № 6. 2020. С. 167–174. DOI : https://doi.org/10.32842/2078- 3736/2020.6.1.24.
131. Про затвердження Положення про Департамент інформаційно-аналітичної підтримки Національної поліції України : наказ Національної поліції України від 31.01.2020 № 77. URL : https://surl.li/yddnle.
132. Про затвердження Положення про Департамент патрульної поліції : наказ Національної поліції України від 06.11.2015 № 73. URL : https://surli.cc/yvdbnw.
133. Про затвердження Положення про Департамент організаційно-аналітичного забезпечення та оперативного реагування Національної поліції України : наказ Національної поліції України від 27.11. 2015 № 126.
134. Про затвердження Положення про Департамент превентивної діяльності Національної поліції України : наказ Національної поліції України від 27 листоп. 2015 № 123. URL : https://surl.li/afsqfk.
135. Про затвердження Положення про Департамент карного розшуку Національної поліції України : наказ Національної поліції України від 14.11.2015. № 90. URL : https://surl.li/dmbcvq.
136. Про організацію діяльності слідчих підрозділів Національної поліції України : наказ МВС України від 06.07.2017 № 570. URL : https://zakon.rada.gov.ua/laws/show/z0918-17#Text.

137. Руснак О. В. Національна безпека в інформаційній сфері: функції та повноваження правоохоронних органів в її забезпеченні. *Правова інформатика.* 2013. № 4(40). С. 72–78. URL : https://surl.li/poifjs.

138. Плескач М. В. Сутність поняття та основні елементи механізму адміністративно-правового забезпечення кібернетичної безпеки людини. *Часопис Київського університету права.* 2020. № 4. С. 201–209. URL : https://chasprava.com.ua/index.php/journal/article/view/568/540.

139. Шундиков К. В. Правові механізми: основи теорії. *Держава і право.* 2006. № 12. С.12–21.

140. Соф'їн М. І. До проблеми визначення поняття механізму адміністративно-правового регулювання здійснення фіскальної політики в Україні. *Юридичний бюлетень.* 2018. Вип. 8. С. 258–264. URL : http://www.lawbulletin.oduvs.od.ua/archive/2018/8_2018/39.pdf.

141. Діденко С. В. Поняття та елементи механізму адміністративно-правового забезпечення обігу та застосування зброї в Україні. *Наукові праці Національного університету «Одеська юридична академія».* 2015. Т. 16. С. 463–469. С. 464. URL : https://surl.lu/wrdamz.

142. Цвік М. В. Загальна теорія держави і права: підруч / М. В. Цвік, В. Д. Ткаченко, Л. Л. Рогачова, О. В. Петришин, С. М. Олейников; М. В. Цвік (ред.). Харків: Право, 2002. 432 с.

143. Пашинський В. Й. Адміністративно-правове забезпечення оборони України: теорія і практика: дис … д-ра юрид. наук: 12.00.07. Київ, 2020. 520 с.

144. Фоменко О. О. До питання про визначення поняття механізму адміністративно-правового забезпечення продовольчої безпеки держави. Право та державне управління. 2022, № 3. С. 392–398. URL : http://pdu-journal.kpu.zp.ua/archive/3_2022/60.pdf.

145. Проневич О. С. Проактивна діяльність поліції (міліції) як складова сучасної парадигми охорони правопорядку. *Форум права :* електрон. наук. фах. вид. 2011. № 3. С. 639–643.

146. Булатін Д. О. Поняття «превенція» і «превентивна діяльність» в адміністративно-правовому аспекті. *Вісник Чернівецького факультету Національного університету «Одеська юридична академія».* 2018. Вип. 1. С. 15–22.

147. Сулацький В. С. Адміністративно-правовий механізм превентивної діяльності Національної поліції України : дис. ... д-ра філософії : 08 – Право; МВС України, Нац. акад. внутр. справ. Київ, 2022. 219 с. URL : https://surl.li/wvecoa.

148. Про затвердження Порядку електронної інформаційної взаємодії Служби безпеки України, Міністерства внутрішніх справ України та центральних органів виконавчої влади, діяльність яких спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України: наказ від 13.10.2022 № 360/657. URL : https://zakon.rada.gov.ua/laws/show/z1327-22#Text.

149. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. URL : https://surl.li/kluzfx.

150. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації: розпорядження Кабінету Міністрів України від 17.01.2018 № 67–р. URL : https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text.

151. Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації: розпорядження КМУ від 23.12.2020 № 1642-р. URL : https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80#Text.

152. Рік руйнівних кібератак в Україні: як загрози атакували користувачів та організації. URL : https://surl.li/wdaycz.

153. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: постанова Кабінету Міністрів України від 19.06.2019 № 518. URL : https://surl.li/rdsbxl.

154. Чистоклетов Л. Г., Хитра О. Л. Адміністративно-правові засоби у забезпеченні інформаційної безпеки Україні. *IT-право: проблеми та перспективи розвитку в Україні* : зб. матеріалів II-ї Міжнар. наук.- практ. конф. (Львів, 17 листоп. 2017 р.). Львів, 2017. С. 212–217. URL : http://aphd.ua/publication-349/.

155. Крушеніцький В. С. Адміністративно-правові механізми реагування на інформаційні загрози: теоретико-правовий аспект. *Право та державне управління*. 2024, № 4. С. 468–472. URL : http://www.pdu-journal.kpu.zp.ua/archive/4_2024/66.pdf.

156. Крушеніцький В. С. Зарубіжний досвід забезпечення національної безпеки у публічно-інформаційній сфері. *Науковий вісник Сіверщини.* 2025. Серія: Право № 3(26). С. 19–28. URL : https://surl.li/hzwezd.

157. Пугачов О. І. Зарубіжний досвід забезпечення інформаційної безпеки держави. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. 2024. № 13. URL : https://surl.li/bxhdro.

158. Network and Iinformation security: proposal for a European policy approach (2014). URL : https://www.steptoe.com/a/web/485/811.pdf.

159. Шемчук В. В. Зарубіжний досвід забезпечення інформаційної безпеки держави. *Порівняльно-аналітичне право*. 2019. № 2. С. 188–191.

160. Климчук О. О., Ткачук Н. А. Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки. *Інформаційна безпека людини, суспільства, держави.* 2015. № 3. С. 75–83. URL : https://surl.lt/aixnaj.

161. Дзеньків В. Кібербезпека в умовах сучасних загроз: ізраїльський досвід і його застосування в Україні. *Науковий вісник Ужгородського національного університету. Серія Право*. 2024. Вип. 84. Ч. 3. С. 77–83.

162. Гребенюк М. В., Леонов Б. Д. Досвід Ізраїлю у сфері забезпечення кібербезпеки. *Інформація і право.* 2018. № 2 (25). С. 45–52.

163. Stancu A.-I., Pavel T. Unveiling Israel's Cyber Legal Landscape: A Comprehensive Analysis of Cybersecurity Regulations and Policies. Perspectives of Law and Public Administration. 2023. № 12 (4). P. 643–650.

164. Фурсай О. Система забезпечення інформаційної безпеки Франції. *Вісник Львівського університету. Серія філос.-політолог. студії*. 2021. Вип. 34. С. 222–227. URL : http://fps-visnyk.lnu.lviv.ua/archive/34_2021/31.pdf.

165. Білоусов О. С., Татакі Д. Д., Татакі О. О. Міжнародна інформаційна безпека в США. *Філософія та політологія в контексті сучасної культури*. 2023. Т. 15. № 2. С. 82–89. URL : https://surl.li/izedpo .

166. Онопрієнко С. Г. Проблеми інформаційної безпеки стратегії національної безпеки республіки Польща. *Правовий Часопис ДонБасу.* 2022. № 4(81) Ч. 1. С. 119–122. URL : https://surl.li/fnnrdi.

167. Кавин С. Нормативно-правові механізми забезпечення кібербезпеки в країнах Балтії. *Підприємництво, господарство і право.* 2020. № 12. С. 315–320.

168. Єсімов С. С. Шляхи удосконалення нормативно-правового регулювання в сфері інформаційної безпеки. URL : https://surl.li/vycxjp.

169. Окинавская хартия глобального информационного общества. (Окинава, 22 июля 2000 года). URL : http://zakon4.rada.gov.ua/laws/show/998_163.

170. Антонюк В. В. Механізми державного реагування на сучасні виклики та загрози інформаційній безпеці. *Державне управління: удосконалення та розвиток.* 2014. № 8. URL : http://www.dy.nayka.com.ua/?op=1&z=747.

171. Калетнік В. В. Сучасний стан адміністративно-правового забезпечення інформаційної безпеки в Україні: теоретико-правовий аналіз. *Юридичний вісник*. 2021. 2 (59). С. 70–77.

172. Кондратенко В. М., Сокуренко О. А. Адміністративно-правові засади забезпечення інформаційної безпеки та доступу до публічної інформації в діяльності правоохоронних органів сектору національної безпеки. *Науковий вісник Ужгородського Національного Університету. Серія Право.* 2025. Вип. 89: Ч. 2. С. 452–457. URL : https://surl.li/munhpj.

173. Баран М. В. Адміністративно-правове забезпечення інформаційної безпеки в Україні: дис. … д-ра філос. наук: 081 «Право». Львів, 2022. 242 с.

174. Лісовська Ю. П. Адміністративно-правове забезпечення інформаційної безпеки в Україні: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. Київ, 2017. 21 с.

175. Пугачов О. І. *Удосконалення державних механізмів забезпечення інформаційної безпеки України* : дис. … доктора філософії : 281 »Публічне управління та адміністрування» / Таврійський національний університет імені В. І. Вернадського. Київ, 2025. С. 242 URL : https://surl.li/pqoldu.

176. Про затвердження Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України: постанова Кабінету Міністрів України від 03.09.2014 № 411. URL : https://surl.li/gnnbgl.

177. Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять [...]: постанова Кабінету Міністрів України від 19.10.2016 № 736. URL : https://surl.li/omeoli.

178. Розуміння сутності національної безпеки: світоглядно-понятійні й науково-теоретичні засади (частина 1). URL : https://surl.lt/haevyf.

ДОДАТКИ

ДОДАТОК 1

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ,

у яких опубліковано основні наукові результати дисертації:

6. Крушеніцький В. С. Публічно-інформаційна сфера як складова системи національної безпеки України. *Право і суспільство.* 2023. № 3. С. 585–590. URL: https://doi.org/10.32842/2078-3736/2023.3.88.

7. Крушеніцький В. С. Органи публічної влади як суб'єкти формування та реалізації політики національної безпеки в інформаційному просторі. *Наукові записки. Серія: Право.* 2024. № 17. С. 252–256. URL: https://doi.org/10.36550/2522-9230-2024-17-252-256.

8. Крушеніцький В. С. Адміністративно-правові механізми реагування на інформаційні загрози: теоретико-правовий аспект. *Право та державне управління.* 2024. № 4. С. 468–472. URL : https://doi.org/10.32782/pdu.2024.4.64.

9. Крушеніцький В.С. Зарубіжний досвід забезпечення національної безпеки у публічно-інформаційній сфері. *Науковий вісник Сіверщини. Серія: Право.* 2025. №3(26). С. 19–28. URL: https://doi.org/10.32755/sjlaw.2025.03.019.

10. Крушеніцький В. С. Роль Ради національної безпеки і оборони України у формуванні державної політики інформаційної безпеки. *Наукові записки. Серія: Право.* 2025. № 18. С. 164–167. URL: https://doi.org/10.36550/2522-9230-2025-18-164-167.

які засвідчують апробацію матеріалів дисертації:

5. Крушеніцький В. С. Роль правоохоронних органів у забезпеченні національної безпеки в інформаційному просторі. *Сектор безпеки України: актуальні питання науки та практики:* збірник наукових статей, тез доповідей та повідомлень за матеріалами XIII Міжнародної науково-практичної конференції (27 березня 2025 р., Національний юридичний університет імені

Ярослава Мудрого, м. Харків). У 2-х частинах. Частина 1. Серія «Сектор безпеки України». Вип. 54. Харків: Друкарня Мадрид, 2025. С. 54–58.

6. Крушеніцький В. С. Принципи адміністративно-правового регулювання інформаційної безпеки в Україні: сучасний стан і перспективи розвитку. *Актуальні проблеми національного законодавства:* збірник матеріалів Міжнародної науково-практичної конференції, м. Кропивницький. 17 квітня 2025 р. Частина 1. Кропивницький, 2025. С. 104–106.

7. Крушеніцький В. С. Сутність та особливості національної безпеки у сфері публічної інформації. *Актуальні питання адміністративного права та адміністративного судочинства*: збірник наукових статей, тез доповідей та повідомлень за матеріалами II Міжнародної науково-практичної конференції (15 травня 2025 р., Національний юридичний університет імені Ярослава Мудрого, м. Харків). Серія «Сектор безпеки України». Вип. 55. Харків: Друкарня Мадрид, 2025. С. 64–69.

8. Крушеніцький В. С. Адміністративно-правові засоби забезпечення національної безпеки у публічно-інформаційній сфері. *Сталий розвиток економіки, права та державного управління в умовах глобальних викликів.* Міжнародна науково-практична конференція. 28 травня 2025 р. м. Анже, Франція. Видавництво Scholarly Publisher ICSSH. 2025. С. 66–68.

ДОДАТОК 2

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІМЕНІ ВОЛОДИМИРА ВИННИЧЕНКА

вул. Шевченка, 1, м. Кропивницький, 25006, тел. (0522) 32-08-89, факс (0522) 24-85-44
E-mail: mails@cuspu.edu.ua, код ЄДРПОУ 02125415

20 травня 2025 р. № 35/1-К

На № _____ від _____

ДОВІДКА

про впровадження результатів наукового дослідження здобувача третього (освітньо-наукового) рівня вищої освіти Центральноукраїнського державного університету імені Володимира Винниченка Крушеніцького Владислава Сергійовича на тему: «Адміністративно-правові засади забезпечення національної безпеки у публічно-інформаційній сфері», в освітній процес Центральноукраїнського державного університету імені Володимира Винниченка

Матеріали дисертації Крушеніцького Владислава Сергійовича на тему: «Адміністративно-правові засади забезпечення національної безпеки у публічно-інформаційній сфері» впроваджено в освітній процес Центральноукраїнського державного університету імені Володимира Винниченка протягом 2024–2025 навчального року.

Теоретичні положення дисертації є актуальними, мають значний науковий і практичний інтерес, що зумовило їх використання у викладанні лекційного та семінарського матеріалу з навчальних дисциплін «Сучасні аспекти міжнародного публічного права», «Актуальні проблеми адміністративного права України», «Сучасні проблеми міжнародного приватного права», для здобувачів другого (магістерського) рівня вищої освіти за спеціальностями 081 «Право» та 262 «Правоохоронна діяльність».

Практичне застосування результатів дисертаційної роботи в освітньому процесі забезпечило істотне підвищення якості підготовки здобувачів вищої освіти. Зокрема, отримані наукові результати були інтегровані у підготовку та проведення тематичних лекцій, розробку практичних і семінарських занять, створення методичних рекомендацій та тестових завдань для студентів. Опрацювання основних положень і висновків дисертації дозволило забезпечити цілісне та системне розуміння актуальних проблем адміністративно-правового забезпечення національної безпеки у публічно-інформаційній сфері, від медіаграмотності та протидії інформаційним загрозам — до регулювання діяльності органів публічної влади у сфері кібербезпеки та публічних

комунікацій. Це дало можливість сформувати у студентів сучасне бачення ролі держави у захисті інформаційного простору, розвинути їх здатність до комплексного аналізу нормативно-правових механізмів забезпечення інформаційної безпеки, а також підвищити їхню компетентність щодо вирішення практичних завдань у сфері виявлення, запобігання та нейтралізації інформаційних загроз.

Результати дослідження були впроваджені під час організації студентських наукових гуртків, проведення круглих столів і науково-практичних конференцій на факультеті. Особливу увагу приділено інтеграції напрацювань дисертації у форматах, присвячених аналізу сучасних загроз у публічно-інформаційній сфері, ролі органів публічної влади в забезпеченні інформаційної безпеки, а також механізмам протидії дезінформації та інформаційно-психологічним операціям.

Під час викладання відповідних розділів особливий акцент було зроблено на міждисциплінарному підході, який поєднує адміністративне право, теорію національної безпеки, інформаційне право, кібербезпеку та міжнародні відносини. Студенти отримали можливість опрацьовувати практичні кейси щодо організації міжвідомчої взаємодії у сфері національної безпеки, механізмів міжнародної інформаційної співпраці, а також практики координації діяльності органів державної влади під час реагування на інформаційні інциденти та взаємодії з іноземними партнерами у сфері кіберзахисту.

З урахуванням зазначеного, впровадження результатів дисертації Крушеніцького Владислава Сергійовича в освітній процес сприяло розширенню професійних знань і навичок здобувачів, формуванню їхнього сучасного правового світогляду, підвищенню рівня підготовки фахівців у галузі адміністративного та міжнародного права.

Довідку обговорено на засіданні кафедри права та правоохоронної діяльності (протокол № 10 від 25 квітня 2025 року).

Проректор з наукової роботи
Центральноукраїнського державного
університету імені Володимира Винниченка,
доктор психологічних наук, професор **Лілія КЛОЧЕК**

ДОДАТОК 3

ЗАТВЕРДЖУЮ
В.о. Президента Науково-дослідного інституту публічного права,
доктор юридичних наук, професор

Сергій КОРОЄД
«15» вересня 2025 року

А К Т

впровадження результатів дисертаційного дослідження Крушеніцького Владислава Сергійовича на тему: «Адміністративно-правові засади забезпечення національної безпеки у публічно-інформаційній сфері», поданого на здобуття ступеня доктора філософії зі спеціальності 081«Право» у науково-дослідну діяльність Науково-дослідного інституту публічного права

Комісія в складі: завідувача відділу докторантури і аспірантури, доктора юридичних наук, професора Сороки Лариси 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 Крушеніцького Владислава Сергійовича на тему: «Адміністративно-правові засади забезпечення національної безпеки у публічно-інформаційній сфері», (на здобуття ступеня доктора філософії зі спеціальності 081«Право») 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 забезпечення національної безпеки у публічно-інформаційній сфері, 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 Крушеніцького Владислава Сергійовича на тему: «Адміністративно-правові засади забезпечення національної безпеки у публічно-інформаційній сфері», вважати впровадженими у науково-дослідну діяльність Науково-дослідного інституту публічного права, під час проведення загальнотеоретичних і галузевих досліджень, спрямованих на вирішення теоретико-методологічних проблем забезпечення національної безпеки у публічно-інформаційній сфері.

Голова комісії: **Лариса СОРОКА**

Члени комісії: **Леся ЛУЦЕНКО-МИСЬКІВ**

Костянтин ШКАРУПА

ДОДАТОК 4

ЗАТВЕРДЖУЮ
В.о. Президента Науково-дослідного інституту публічного права,
доктор юридичних наук, професор

Сергій КОРОЄД
«15» вересня 2025 року

АКТ
упровадження результатів дисертаційного дослідження Крушеніцького Владислава Сергійовича на тему: «Адміністративно-правові засади забезпечення національної безпеки у публічно-інформаційній сфері», поданого на здобуття ступеня доктора філософії зі спеціальності 081«Право» в освітній процес Науково-дослідного інституту публічного права

Комісія в складі: завідувача відділу докторантури і аспірантури, доктора юридичних наук, професора Сороки Лариси 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 Крушеніцького Владислава Сергійовича на тему: «Адміністративно-правові засади забезпечення національної безпеки у публічно-інформаційній сфері» (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 забезпечення національної безпеки у публічно-інформаційній сфері» Крушеніцького Владислава Сергійовича вважати впровадженими в освітній процес Науково-дослідного інституту публічного права з дисципліни «Адміністративне право та процес: доктринальні та практичні проблеми».

Голова комісії: **Лариса СОРОКА**

Члени комісії: **Леся ЛУЦЕНКО-МИСЬКІВ**

Костянтин ШКАРУПА