УДК 342.951:351.74:004.9
DOI https://doi.org/10.24144/2307-3322.2025.89.2.69

АДМІНІСТРАТИВНО-ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ДОСТУПУ ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ В ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ СЕКТОРУ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Кондратенко В.М.,
доктор юридичних наук, професор,
професор кафедри права та правоохоронної діяльності,
Центральноукраїнський державний університет
імені Володимира Винниченка

Сокуренко О.А.,
кандидат юридичних наук, доцент,
доцент кафедри права та правоохоронної діяльності,
Центральноукраїнський державний університет
імені Володимира Винниченка

Кондратенко В.М., Сокуренко О.А. Адміністративно-правові засади забезпечення інформаційної безпеки та доступу до публічної інформації в діяльності правоохоронних органів сектору національної безпеки.

Стаття присвячена системному аналізу адміністративно-правових засад забезпечення інформаційної безпеки та реалізації права на доступ до публічної інформації в діяльності правоохоронних органів сектору національної безпеки. В умовах цифрової трансформації та триваючої гібридної агресії значення інформаційного захисту та відкритості публічної влади набуває критичного характеру. Відкритість державного управління, прозорість процедур, доступність даних про діяльність органів влади є невід'ємними чинниками демократичного ладу, потребують обережного балансування із вимогами безпеки та захисту критичної інформації.

У роботі розглянуто функціональну подвійність правоохоронних структур, які одночасно зобов'язані гарантувати захист інформаційного простору від загроз, реагувати на кібератаки, втручання в інформаційні системи, поширення дезінформації та водночас забезпечувати реалізацію конституційного права громадян на доступ до публічної інформації.

Зроблено акцент на важливості впровадження прозорих процедур обмеження доступу до інформації, створення ефективного механізму контролю за дотриманням інформаційних прав, посилення ролі незалежних наглядових структур. Окрема увага приділена викликам, пов'язаним із формалізмом у відповіді на інформаційні запити, зловживанням правом відмови, нечіткістю критеріїв класифікації відомостей та проблемам міжвідомчої координації.

Аналізується роль цифрових інструментів у забезпеченні доступності публічної інформації, зокрема функціонування державних порталів відкритих даних, електронних сервісів та систем документообігу. Визначено необхідність формування внутрішньої культури відкритості у публічному секторі, яка передбачає дотримання формальних вимог і наявність внутрішніх мотивацій до прозорості, звітності, діалогу з суспільством.

На основі комплексного підходу обґрунтовано, що ефективність інформаційної політики держави у сфері безпеки та відкритості залежить від здатності поєднати швидке реагування на інформаційні загрози з демократичними стандартами публічного управління. Досягнення балансу між правом громадян на інформацію і потребою захисту національних інтересів є ключовою умовою безпечного функціонування держави в інформаційну епоху. Запропоновано концептуальні напрями удосконалення адміністративно-правового регулювання відповідної сфери.

Ключові слова: адміністративно-правовий механізм, безпекове середовище, доступ до публічної інформації, інформаційна безпека, цифрове середовище, інформаційні загрози, кіберпростір, національна безпека, правоохоронні органи, публічна влада, публічна інформація.

Kondratenko V.M., Sokurenko O.A. Administrative and legal foundations for ensuring information security and access to public information in the activities of law enforcement agencies within the national security sector.

This article presents a systematic analysis of the administrative and legal framework for safeguarding information security and ensuring the right of access to public information in the operations of law enforcement agencies within the national security sector. In the context of digital transformation and ongoing hybrid aggression, the dual imperative of protecting the informational domain and maintaining transparency in public governance has become critically important. Openness of state institutions, procedural transparency, and public access to government activities are integral to democratic governance, yet they require careful balancing with national security demands and the protection.

The study examines the dual functional nature of law enforcement bodies, which are simultaneously responsible for defending the information space against cyberattacks, system intrusions, and disinformation, while also ensuring the constitutional right of citizens to access public information. Emphasis is placed on the need for transparent procedures when restricting access to information, the development of robust oversight mechanisms for safeguarding information rights.

Particular attention is paid to challenges such as formalistic responses to information requests, abuse of exemption clauses, ambiguous classification criteria, and inter-agency coordination gaps. The role of digital tools is also analyzed, with a focus on the functionality of open data platforms, e-governance services, and electronic document management systems.

The article underlines the importance of fostering an internal culture of transparency within the public sector one that goes beyond formal compliance and embraces intrinsic motivation toward openness, accountability, and civic engagement. Through an integrated approach, the study argues that the effectiveness of state information policy in security and openness hinges on its capacity to reconcile rapid responses to threats with democratic standards of public governance. Achieving equilibrium between citizens' right to information and the imperative of national security is essential for ensuring the resilience and legitimacy of the state in the digital era.

Key words: administrative regulation, administrative and legal mechanism, administrative and legal principles, security environment, access to public information, information security, information threats, cyberspace, law enforcement agencies, national security, public authority, public information.

Постановка проблеми. Сучасне інформаційне суспільство висуває нові вимоги до держави та її органів, насамперед у питаннях захисту інформації та забезпечення відкритості. Використання цифрових технологій дало поштовх для швидкого обміну даними, спростило доступ до важливих відомостей, дозволило громадянам брати активну участь у контролі за роботою влади. У таких умовах право на доступ до публічної інформації стало реальною складовою демократичного устрою, підвищило рівень прозорості, сприяло розвитку довіри до державних інституцій.

Однак водночас із новими можливостями зросли й ризики. Значна частина даних, які опиняються у відкритому доступі, може бути використана зловмисниками для завдання шкоди державі, окремим громадянам або організаціям. Особливо небезпечною є діяльність, спрямована на поширення неправдивої інформації, втручання у роботу державних інформаційних систем, отримання доступу до закритих реєстрів, поширення відомостей.

Правоохоронні органи сектору національної безпеки опинилися в ситуації, коли необхідно поєднувати відкритість і підзвітність із обов'язком захищати дані, які можуть бути використані проти інтересів країни. На практиці це означає необхідність вироблення чітких правил, що регулюють доступ до публічної інформації, визначення категорій відомостей, які підлягають захисту, а також встановлення відповідальності за порушення цих правил. Особливо гостро ця проблема проявилася в умовах воєнного стану та постійної інформаційної агресії, коли навіть незначний витік може призвести до серйозних наслідків для обороноздатності.

З огляду на це, актуальним є комплексний аналіз адміністративно-правових засад діяльності правоохоронних органів у питаннях інформаційної безпеки та публічності. Потрібно не лише правильно визначити межі допустимого розкриття відомостей, а й забезпечити дієвий механізм

контролю за дотриманням цих меж, передбачити запобіжники від зловживань та надати інструменти захисту як державним інтересам, так і правам громадян.

Ступінь наукової розробки проблеми дослідження. Розвиток цифрових технологій та ускладнення інформаційного простору поставили перед юридичною наукою нові завдання у сфері забезпечення інформаційної безпеки та врегулювання доступу до публічної інформації. Ці питання привернули значну увагу науковців, що підтверджується численними монографіями, науковими статтями та доповідями на спеціалізованих конференціях. Зокрема, дослідженням адміністративно-правових аспектів інформаційної безпеки, регулювання доступу до публічної інформації та діяльності правоохоронних органів сектору національної безпеки займаються такі вітчизняні та зарубіжні вчені, як О.П. Плужник, Л.В. Кириченко, В.П. Діхтієвський, Т.М. Качур, О. Бандурка, А.П. Гетьман, С.В. Ківалов, О.Ф. Андрійко, В.М. Шаповал, Ю.П. Битяк, М.П. Орзіх.

Науковці досліджують різні аспекти правового захисту інформаційних прав громадян, адміністрування електронних сервісів, діяльності спеціалізованих правоохоронних органів у сфері інформаційної безпеки, а також впровадження міжнародних стандартів у цій галузі. Окремо варто відзначити праці О.Ю. Наливайка, О.В. Дзюби, О.М. Стародубцевої, які аналізують виклики захисту інформації та проблеми цифрової безпеки.

Метою статті є визначення основних адміністративно-правових засад забезпечення інформаційної безпеки та порядку доступу до публічної інформації в діяльності правоохоронних органів сектору національної безпеки, а також аналіз наявних проблем і розробка пропозицій для підвищення ефективності правового регулювання у цій сфері з урахуванням сучасних викликів цифрового середовища.

Виклад основного матеріалу. У демократичних державах право на доступ до публічної інформації є невід'ємною складовою системи стримувань і противаг, що забезпечує реальну підзвітність органів влади перед суспільством. Це не лише юридично закріплене право, а й ефективний інструмент, який дозволяє громадянам контролювати діяльність посадових осіб, отримувати об'єктивну інформацію про управлінські процеси, критично оцінювати державну політику. Дає можливість впливати на її формування. Відкритість інформаційних потоків у сфері публічного управління сприяє підвищенню інституційної відповідальності, попередженню зловживань та спрямуванню державної політики на задоволення потреб населення [1, с. 74; 2, с. 63-64].

Право на доступ до публічної інформації нерозривно пов'язане з визнанням людини як активного суб'єкта у сфері публічного управління. Його реалізація дозволяє переходити від моделі пасивного споживача владних рішень до моделі свідомого і поінформованого учасника, який здатен впливати на якість публічних послуг, легітимність політичних процесів і напрямок розвитку держави.

Для України, яка продовжує боротьбу проти зовнішньої агресії в умовах гібридної війни, а також проводить масштабні внутрішні трансформації, доступ до публічної інформації набуває виняткової ваги. Це питання більше не зводиться до реалізації окремого суб'єктивного права, а виходить на рівень забезпечення національної безпеки, стабільності державного управління та збереження довіри громадян до влади [3, с. 347]. Поширення достовірної інформації, відкритість процедур ухвалення рішень, прозорість у використанні бюджетних коштів, усе це створює бар'єри для деструктивного зовнішнього впливу, сприяє внутрішній консолідації та зміцнює легітимність дій державних інституцій.

У цьому контексті особливе значення має формування ефективного адміністративно-правового механізму забезпечення доступу до публічної інформації. Мова йде про наявність чітких процедур, гарантій відповідальності за ненадання інформації, функціонування незалежних інституцій, які контролюють дотримання прав громадян, і належну цифрову інфраструктуру, що дозволяє спростити доступ до відкритих даних для всіх соціальних груп. Запровадження принципів відкритого врядування, розвиток електронних сервісів, цифровізація документообігу та відкриття державних реєстрів, усе це має бути не винятком, а стандартом у роботі органів публічної влади.

З огляду на зазначене, розширення і вдосконалення правових, організаційних та технічних інструментів реалізації права на доступ до публічної інформації повинно розглядатися як стратегічний пріоритет державної політики. Забезпечення формальної відповідності європейським стандартам та створення внутрішньої культури відкритості – середовища, в якому прозорість, підзвітність і діалог із суспільством є нормою функціонування кожної владної інституції. Такий

підхід зміцнює державність, підвищує ефективність публічного адміністрування й формує передумови для побудови якісно нової моделі взаємодії влади й громадян.

Однак на практиці впровадження стандартів відкритості та підзвітності нерідко стикається з низкою проблем. Формальне виконання законодавчих вимог щодо доступу до інформації не завжди означає реальну прозорість роботи органів влади. Часто відсутній належний громадський контроль, а механізми аудиту рішень органів влади залишаються малоефективними. Особливого значення набуває діяльність правоохоронних органів сектору національної безпеки, які покликані не лише захищати державні інтереси, але й контролювати дотримання прав громадян на отримання інформації, своєчасно реагувати на зловживання, втручання у роботу інформаційних систем та інші порушення у сфері доступу до даних [4, с. 95; 5].

Громадська потреба у відкритості влади, у тому числі правоохоронних структур, зростає в умовах кризових ситуацій, під час воєнного стану, масових соціальних змін [6]. Громадяни дедалі частіше вимагають доступу до інформації про діяльність органів влади, силових відомств, перебіг реформ, розподіл державних фінансів, безпеку, екологію, роботу судів. Довіра до влади в такі періоди значною мірою залежить від оперативного та повного доступу до достовірної інформації. Водночас, надмірна відкритість чи безконтрольне поширення відомостей може спричинити ризики для безпеки держави, полегшити діяльність зовнішніх загроз, створити додаткові можливості для дезінформації, маніпуляцій та кібератак.

Цифровізація державного управління, впровадження сучасних електронних сервісів, масове поширення цифрових технологій різко підвищили швидкість і масштаби поширення інформації. В умовах глобальної мережі дані можуть миттєво потрапити за межі країни, що ускладнює роботу органів контролю і підвищує ризик витоку чутливих відомостей. Кіберінциденти, хакерські атаки, незаконний доступ до державних реєстрів, маніпуляції у соціальних мережах стали повсякденною реальністю [7; 8]. Саме тому правоохоронні органи сектору національної безпеки мають діяти комплексно, поєднувати функції реагування на інформаційні загрози, розслідування порушень, виявлення джерел кібератак, притягнення до відповідальності посадових осіб за зловживання або бездіяльність, а також захищати конституційні права громадян на доступ до публічної інформації.

У наукових підходах до організації доступу до інформації значну увагу приділяють рекомендаціям Ради Європи, рішенням Європейського суду з прав людини, досвіду держав із розвиненою цифровою інфраструктурою. Утім, в умовах гібридної війни, інформаційних кампаній, активних кібератак особливого значення набуває правильне поєднання принципу прозорості з механізмами захисту. В українському законодавстві, зокрема у Законах України «Про доступ до публічної інформації», «Про Службу безпеки України» [9; 10] визначені як загальні принципи відкритості, так і чіткі підстави для обмеження доступу, якщо розкриття інформації може завдати шкоди національній безпеці, обороноздатності, міжнародним відносинам чи правам інших осіб. Правоохоронні органи на практиці забезпечують дотримання цих процедур, проводять розслідування у разі порушень, координують діяльність інших відомств, ініціюють притягнення до відповідальності за незаконні обмеження прав громадян чи навпаки безпідставне розкриття державних таємниць.

Останні роки продемонстрували стрімке зростання складних кіберінцидентів та спроб несанкціонованого доступу до захищених державних даних. Зокрема, за даними Служби безпеки України, лише у 2022–2024 роках зафіксовано понад 150 спроб кібератак на державні органи, значна частина яких була спрямована на отримання доступу до критичних реєстрів та баз даних [11]. В окремих випадках наслідки таких атак відчувалися не лише на рівні функціонування органів влади, а й впливали на діяльність місцевих громад, доступ до соціальних послуг, реалізацію оборонних програм. У відповідь правоохоронні органи впроваджують спеціальні протоколи захисту, тимчасово обмежують доступ до певних категорій інформації (даних про переміщення військових частин, роботу об'єктів критичної інфраструктури), проводять роз'яснювальну роботу серед посадових осіб, вимагають жорсткого дотримання кібергігієни та інформаційної безпеки [12].

Значну увагу приділено розвитку електронних сервісів, державних порталів відкритих даних, автоматизації розгляду запитів. Сучасні цифрові платформи підвищують зручність для громадян, але одночасно висувають нові вимоги до захисту даних від несанкціонованого втручання. Правоохоронні органи у цій системі виконують функції контролю, реагування на інциденти, розслідування зловживань, а також сприяють підвищенню цифрової грамотності державних службовців, розробляють практичні інструкції для роботи з інформацією.

Водночас залишається низка проблем: формалізм під час розгляду інформаційних запитів, зловживання правом на відмову у наданні інформації, нечіткість критеріїв віднесення відомостей до обмежених, недостатній рівень незалежного зовнішнього контролю, недоліки координації між органами влади та правоохоронними структурами. На практиці трапляються ситуації, коли розголошення інформації або відмова у її наданні завдають шкоди як державним, так і приватним інтересам. Це вимагає постійного вдосконалення адміністративно-правових механізмів, оновлення процедур, підвищення кваліфікації персоналу, розвитку системи моніторингу та аудиту.

Комплексний підхід до організації інформаційної безпеки й доступу до публічної інформації у діяльності правоохоронних органів сектору національної безпеки повинен враховувати як потреби громадянського суспільства у відкритості, так і реальні ризики сучасного інформаційного простору. Ефективне законодавче та адміністративне забезпечення у цій сфері має поєднувати гнучкість, швидкість реагування на загрози, контроль за дотриманням процедур і чітке розмежування відповідальності між різними органами влади. В умовах воєнного стану й постійного оновлення інформаційних викликів держава має оперативно удосконалювати правові підходи до захисту даних, активно залучати правоохоронні органи до розробки та реалізації політики інформаційної безпеки, підвищувати рівень взаємодії з громадськістю і міжнародними партнерами. Тільки такий підхід дозволить зберегти баланс між відкритістю, захистом прав людини і забезпеченням національної безпеки.

Висновки. Проведене дослідження підтвердило, що забезпечення балансу між відкритістю публічної інформації та захистом національної безпеки є однією з ключових проблем сучасного етапу розвитку адміністративного права в умовах цифрової трансформації державного управління. Право громадян на доступ до публічної інформації виступає базовою демократичною цінністю, інструментом забезпечення прозорості, підзвітності органів публічної влади та участі суспільства у процесах ухвалення рішень. Стрімке зростання кіберзагроз, активізація гібридних форм агресії, зокрема в умовах воєнного стану, суттєво ускладнюють реалізацію цього права й актуалізують потребу у формуванні чіткої системи адміністративно-правових гарантій захисту інформації.

Правоохоронні органи сектору національної безпеки мають діяти як суб'єкти подвійної функції: з одного боку захищати державні інтереси й протидіяти кіберзагрозам, з іншого гарантувати реалізацію права громадян на інформацію. Ефективне функціонування цієї моделі можливе лише за умови чіткого розмежування повноважень, створення механізмів зовнішнього контролю, прозорих процедур прийняття рішень щодо обмеження інформації та впровадження принципів відкритого врядування.

У підсумку, адміністративно-правовий механізм у сфері інформаційної безпеки та доступу до публічної інформації потребує постійного адаптивного перегляду відповідно до змін безпекового середовища, цифрових технологій і суспільних запитів. Його вдосконалення має ґрунтуватися на дотриманні балансу між відкритістю влади та захистом національних інтересів, що є запорукою ефективного, безпечного й демократичного існування держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Ліховіцький Я.О. Адміністративно-правові засади доступу до публічної інформації в Україні: *монографія*. Ужгород: ТОВ «РІК-У». 2024. 140 с.
2. Сибіга О.М. Право особи на доступ до публічної інформації: адміністративно-правове забезпечення і захист: монографія. Херсон: Видавничий дім «Гельветика», 2019. 370 с.
3. Національна безпека: світоглядні та теоретико-методологічні засади: монографія / за заг. ред. О.П. Дзьобаня. Харків: Право, 2021. 776 с.
4. Боровик А.В. Адміністративно-правовий механізм взаємодії суб'єктів сектору безпеки й оборони щодо забезпечення національної безпеки: питання теорії та практики: монографія. Одеса: Видавництво «Юридика», 2024. 186 с.
5. Інформаційна безпека: філософське та організаційно-правове підґрунтя рефлексії національних інтересів України: *монографія* / за ред. О.Г. Данильяна. Харків: Право, 2024. 224 с.
6. Національний координаційний центр кібербезпеки при РНБО України. URL: https://www.ncscc.gov.ua.

7. Офіційний портал відкритих даних України. URL: https://data.gov.ua.
8. Міністерство цифрової трансформації України. Електронні сервіси. URL: https://thedigital.gov.ua.
9. Про доступ до публічної інформації : Закон України « від 13.01.2011 № 2939-VI (у редакція від 08.10.2023). URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text.
10. Про Службу безпеки України : Закон України від 25.03.1992 № 2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text.
11. Звіти, доповіді та інша інформація державних органів та посадових осіб / Офіційний веб-портал парламенту України. URL: https://www.rada.gov.ua/documents/reports_list.
12. Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах: Постанова Кабінету Міністрів України від 29.03.2006 № 373 (у редакція від 18.04.2025). URL: https://zakon.rada.gov.ua/laws/show/373-2006-п#Text.