

КОНДРАТЕНКО В. М.,

доктор юридичних наук, професор,
професор кафедри права
та правоохоронної діяльності
(Центральноукраїнський державний
університет імені Володимира
Винниченка)

МАНЖУЛА А. А.,

доктор юридичних наук, професор,
професор кафедри права
та правоохоронної діяльності
(Центральноукраїнський державний
університет імені Володимира
Винниченка)

УДК 342.951:351.746:004.9

DOI <https://doi.org/10.32842/2078-3736/2025.3.1.27>

АДМІНІСТРАТИВНО-ПРАВОВІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ БАЛАНСУ МІЖ ДОСТУПОМ ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ ТА ЗАХИСТОМ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В УМОВАХ РОЗВИТКУ ІНФОРМАЦІЙНОГО ПРОСТОРУ

У статті представлено комплексний аналіз адміністративно-правових механізмів, спрямованих на забезпечення балансу між правом громадян на доступ до публічної інформації та захистом національної безпеки. Автори наголошують на тому, що цифровізація публічного управління, поширення інтернет-комунікацій та використання відкритих даних як елементів прозорості влади супроводжуються серйозними загрозами безпеці, особливо в умовах гібридної війни.

Проаналізовано чинне законодавство у сфері доступу до інформації, та інші нормативні акти, що регламентують обмеження інформації в інтересах державної безпеки. Визначено коло суб'єктів, уповноважених обмежувати доступ до відомостей, критерії такого обмеження та процедурні аспекти їхнього застосування.

Увага зосереджена на важливості забезпечення балансу між відкритістю інформації як інструментом забезпечення підзвітності влади, боротьби з корупцією та залучення громадськості до публічного управління та необхідністю недопущення витоку даних, які становлять державну, службову чи комерційну таємницю. Детально розглянуто питання класифікації інформації за рівнями доступу, ролі кібербезпеки, а також механізми функціонування державних кіберінституцій і цифрової інфраструктури в умовах воєнного стану.

Аргументовано необхідність посилення ролі адміністративного судочинства, інституційного контролю (омбудсмен, незалежні комісії), розвитку електронних сервісів та впровадження прозорих алгоритмів прийняття рішень у сфері доступу до публічної інформації.

У результаті дослідження запропоновано низку практичних рекомендацій з удосконалення нормативно-правової бази, стандартизації адміністративних процедур, розвитку електронних платформ відкритих даних і гармонізації вітчизняного законодавства з міжнародними стандартами. Підкреслено, що



досягнення балансу між відкритістю інформації та захистом національних інтересів потребує не статичних рішень, а постійного адаптивного перегляду механізмів адміністративного регулювання згідно до змін безпекового середовища.

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

Kondratenko V. M., Manzhula A. A. Administrative and legal mechanisms for ensuring the balance between access to public information and the protection of national security in the context of the development of the information space

This article provides an in-depth legal and administrative analysis of mechanisms designed to strike a balance between the constitutional right of citizens to access public information and the imperative to safeguard Ukraine's national security in the context of a rapidly evolving digital environment. The authors highlight that the digitalization of public governance, the proliferation of internet communications, and the increasing use of open data as a transparency tool generate significant security challenges, particularly amid hybrid warfare and information threats.

The study explores current Ukrainian legislation and relevant regulatory acts governing information access and national security restrictions. It outlines the legally authorized actors responsible for restricting access to information, the legal grounds and procedural safeguards for such restrictions, and the principles of proportionality and legitimacy.

Special emphasis is placed on the dual necessity of promoting information openness to enhance governmental accountability and citizen engagement, while simultaneously protecting sensitive data related to state, official, or commercial secrecy. The article examines key issues such as information classification, cybersecurity infrastructure, the role of digital platforms, and the operations of national cyber institutions.

The authors offer practical recommendations for improving the legal framework, automating administrative processes, advancing digital platforms for open data, and aligning national legislation with international legal standards. It is argued that maintaining the balance between transparency and security demands a dynamic, adaptive approach to regulation, responsive to ongoing transformations in the national and global information security landscape.

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

Вступ. Активне розширення інформаційно-комунікаційних технологій, інформаційне оновлення сфери державного адміністрування призвели до виникнення актуальних загроз, що стосуються як забезпечення можливості на отримання відкритих даних, так і забезпечення державної безпеки. У контексті повномасштабної гібридної агресії, саме цифрове середовище перетворився на ключову арену протистояння. Недобросовісні суб'єкти міжнародного права активно використовують цифрові ресурси для поширення дезінформації, психологічного впливу, формування наративів і підриву стабільності. До найнебезпечніших проявів цих загроз належать хакерські атаки, маніпуляції у соціальних мережах, витіки конфіденційної чи стратегічної інформації та ін.

У таких умовах перед органами публічної влади постає нагальна потреба у формуванні ефективної системи адміністративно-правового регулювання, яка б, з одного боку, гарантувала належний рівень прозорості, а з іншого забезпечувала захист державної таємниці,



безпеку критичної інфраструктури й стратегічних даних. Особливого значення набувають засоби адміністративно-правового регулювання, покликані встановлювати прозорі та передбачувані процедури доступу, обмеження, класифікації та захисту інформації, визначати правові критерії віднесення даних до категорій з обмеженим доступом, а також передбачати відповідальність за порушення таких вимог.

Питання забезпечення рівноваги між відкритістю публічної інформації та потребами державної безпеки активно досліджується в сучасній правовій доктрині. У центрі наукових пошуків перебувають юридичні засади регулювання доступу до інформації та засоби адміністративно-правового регулювання протидії інформаційним загрозам. В. Діхтєвський аналізує проблематику правового забезпечення доступу до публічної інформації. Окрема група науковців серед яких О. Бандурка, Т. Качур, О. Золотухін звертає увагу на інформаційну безпеку як ключовий об'єкт адміністративно-правового регулювання. У низці досліджень акцентовано на особливостях формування інформаційної політики, протидії кібератакам і мінімізації негативного впливу інформаційних операцій.

М. Бліхар зосереджує увагу на питаннях інформаційної безпеки в інтернет-середовищі. Він підкреслює необхідність формування цілісного адміністративно-правового механізму, що забезпечує взаємодію між органами влади, громадянським суспільством і приватним сектором у сфері захисту інформаційного простору. Зі свого боку, В. Сенік досліджує правові механізми захисту інформації з обмеженим доступом у діяльності Національної поліції України.

В окремих працях О. Плужника і Л. Кириченка піднімається питання забезпечення інформаційної безпеки громадян у період воєнного стану. Отже, вітчизняна правова наука перебуває на етапі формування міждисциплінарного підходу до піднятої проблематики. Водночас дослідження вказують на необхідність поглибленої розробки саме адміністративно-правових механізмів, які б дозволили ефективно зрівноважити відкритість державної інформації з потребами захисту в умовах викликів інформаційного суспільства.

Метою статті є всебічне дослідження адміністративно-правових механізмів досягнення рівноваги між реалізацією права на отримання публічної інформації та необхідністю захисту державної безпеки на тлі еволюції інформаційного простору; визначення ключових проблем у правовому регулюванні цієї сфери, а також обґрунтування напрямів його ефективного вдосконалення.

Виклад основного матеріалу. У демократичних державах право на отримання публічної інформації визнається базовою гарантією відкритості та прозорості публічного адміністрування. Варто відзначити, що імплементація європейських стандартів підзвітності та публічності в українському законодавстві часто стикається з проблемами на етапі практичної реалізації. Існують випадки, коли формальні норми не забезпечують реальної прозорості, а контроль громадськості носить декларативний характер. Це зумовлює необхідність розробки дієвих механізмів внутрішнього та зовнішнього аудиту рішень органів влади.

Громадська потреба на максимальну відкритість публічної інформації зростає, коли громадяни очікують на оперативний і повний доступ до відомостей про діяльність державних органів, ухвалення рішень, використання бюджетних коштів, стан екології, безпеку, соціальні послуги тощо. Особливої гостроти це питання набуває під час кризових ситуацій, воєнного стану або надзвичайних подій, коли довіра до влади формується через відкритість інформаційної взаємодії. З іншого боку, надмірна або необґрунтовано широка відкритість інформації може створювати додаткові ризики для державної безпеки. Ситуацію ускладнює динамічний розвиток інформаційних технологій, коли інформація миттєво поширюється не лише в національних, а й у глобальних масштабах, а механізми контролю та регулювання часто не встигають за цими процесами.

Сучасна правова доктрина пропонує низку моделей організації доступу до інформації, серед яких особливої актуальності для України набувають європейські стандарти, рекомендації Ради Європи, практика Європейського суду з прав людини, а також досвід держав, що пройшли шлях цифрової трансформації державного адміністрування. Водночас у реаліях



воєнного стану, постійної гібридної агресії та інформаційних атак специфічним залишається питання встановлення меж і підстав для обмеження доступу до окремих категорій інформації. На адміністративно-правовому рівні закладаються запобіжники зловживання владою, необґрунтованого обмеження прав громадян і забезпечення адекватної відповіді на сучасні виклики.

Наукові дискусії точаться навколо ефективності існуючої моделі регулювання доступу до публічної інформації, проблем формалізму в діяльності органів влади, потреби в розвитку єдиних електронних сервісів, механізмів громадського контролю та прозорого моніторингу дотримання інформаційних прав. Питання досягнення балансу між відкритістю публічної інформації та захистом державної безпеки є однією з найскладніших проблем сучасної правової науки та практики державного адміністрування. Для його розв'язання необхідний комплексний аналіз фундаментальних положень адміністративного права, конституційних гарантій, а також урахування специфіки розвитку інформаційного суспільства [1, с. 157–158; 2].

На доктринальному рівні виокремлюють кілька підходів до визначення сутності такого балансу. Один із них включає концепцію примату відкритості, згідно з якою право на отримання відкритих даних розглядається як невід'ємна складова демократії, прозорості влади і боротьби з корупцією [3, с. 90]. Відкритість виступає базовою цінністю, а будь-які обмеження цього права можливі лише у виняткових, прямо визначених законом випадках. Реалізація принципу відкритості, за сучасними дослідниками, є не лише юридичним, а й моральним імперативом для демократичної держави.

Проте поряд із цим підходом існує й концепція обґрунтованого обмеження, яка визнає, що повна відкритість інформації не завжди є можливою або доцільною. В умовах гібридних загроз, воєнних дій, поширення дезінформації чи кібератак держава має обов'язок обмежувати доступ до певних категорій інформації задля захисту державної безпеки, громадського порядку, прав і свобод інших осіб. Такі обмеження повинні бути визначені законом, відповідати принципу пропорційності й бути виправданими легітимною метою. Європейський суд з прав людини неодноразово підкреслював, що обмеження прав мають бути необхідними в демократичному суспільстві й відповідати принципу пропорційності.

Сучасна правова доктрина дедалі більше спирається на теорію зважування цінностей, згідно з якою жодна з цінностей не є абсолютною. Кожен конкретний випадок оцінюється індивідуально з урахуванням потенційної користі чи шкоди для суспільства. Цей підхід знаходить відображення в практиці Конституційного Суду України щодо обмеження прав під час воєнного стану та захисту державної таємниці [4, с. 18–21].

Європейські правові системи орієнтуються на інтеграцію принципу прозорості з інтересами безпеки через чітку регламентацію процедур доступу, диференціацію рівнів інформації, а також посилення ролі незалежних інституцій через омбудсменів, спеціальних комісій, судового контролю. У багатьох країнах ЄС створено електронні платформи, які автоматизують процеси доступу до інформації та мінімізують суб'єктивізм посадовців [5, с. 163].

У вітчизняному законодавстві простежується прагнення досягти балансу між дотриманням демократичних стандартів відкритості, закріплених, зокрема у Законі України «Про доступ до публічної інформації» [6], та необхідністю захисту державної, службової, конфіденційної інформації, особливо в умовах воєнного стану й гібридної агресії. Водночас залишається невирішеною проблема чіткого визначення меж між відкритою та обмеженою інформацією, а також створення дієвих запобіжників проти зловживань з боку органів влади [7, с. 47].

Значущою є міжнародно-правова складова. Міжнародні стандарти (рекомендації Ради Європи, Конвенція про доступ до офіційних документів, стандарти ОБСЄ та ООН) встановлюють, що обмеження права на доступ до інформації мають бути законними, обґрунтованими та мінімально необхідними для захисту конкретних легітимних інтересів. У підсумку, принципи відкритості, прозорості та підзвітності є основою публічного адміністрування, але забезпечення безпеки держави та суспільства потребує чітко визначених, пропорційних



і контрольованих обмежень доступу до інформації. Баланс між цими цінностями не слугує статичною нормою, а радше гнучкою системою, яка постійно вдосконалюється відповідно до нових інформаційних викликів, технологічного прогресу та змін у безпековому середовищі.

Новітній адміністративно-правовий механізм реалізації права на отримання інформації формується під впливом двох взаємозалежних чинників: потреби забезпечення максимальної прозорості публічної влади та необхідності гарантування національної та інформаційної безпеки держави. Законодавча основа таких механізмів визначена передусім Законом України «Про доступ до публічної інформації», який закріплює основні принципи відкритості, прозорості, неупередженості та своєчасності доступу до інформації для всіх заінтересованих осіб. До механізмів реалізації такого права належать чітко визначений перелік суб'єктів, які зобов'язані надавати інформацію, процедура подання й розгляду інформаційних запитів, встановлення строків надання відповідей, вимоги щодо форми та способу оприлюднення інформації.

Чинне законодавство містить низку винятків, які передбачають обмеження доступу до інформації, якщо її поширення може завдати шкоди національним інтересам, обороноздатності, економічній безпеці або міжнародним відносинам України. Обґрунтованість таких обмежень визначається на основі принципу, коли інформація стосується легітимного інтересу; розголошення може завдати суттєвої шкоди цьому інтересу; шкода від оприлюднення перевищує суспільну користь від відкритості. Ключовим елементом виступає дотримання вимог пропорційності, обґрунтованості й мінімальної достатності обмеження.

Засоби адміністративно-правового регулювання, спрямовані на захист інформаційної та державної безпеки, передбачають запровадження спеціальних адміністративних процедур і технологічних рішень. Це, зокрема, класифікація інформації за рівнями доступу, ведення державних реєстрів інформації з обмеженим доступом, застосування систем контролю доступу, кібербезпеки, шифрування даних, а також обов'язкова експертиза відомостей, які можуть становити таємницю [8; 9].

За період 2022–2024 років СБУ зафіксувала понад 150 кібератак на державні органи, значна частина яких була спрямована на отримання даних із закритих реєстрів. У деяких випадках наслідки таких атак мали вплив не лише на державну безпеку, а й на діяльність місцевих громад (наприклад, у ситуації з DDoS-атаками на реєстри Мін'юсту у квітні 2023). Це підкреслює важливість розробки адаптивних протоколів реагування. Зростає частка тимчасового блокування доступу до окремих категорій інформації (наприклад, про переміщення ЗСУ, роботу критичної інфраструктури, мобілізаційних процесів тощо). Практика свідчить, що такі заходи є обґрунтованими за умови чіткого дотримання норм законодавства. Важливим інструментом адміністративно-правового захисту інформаційної безпеки стала розбудова кіберінфраструктури держави: впровадження комплексних систем захисту інформації в органах державної влади, створення Національного координаційного центру кібербезпеки при РНБО, запровадження стандартів захисту критичних інформаційних ресурсів [10].

Крім цього, значна увага приділяється вдосконаленню електронних сервісів доступу до публічної інформації, які забезпечують не лише зручність для громадян, а й унеможливають несанкціонований доступ до чутливих даних. Розвиток платформ «Дія», державних порталів відкритих даних, автоматизація процесів розгляду запитів є прикладами застосування сучасних адміністративних та інформаційно-технологічних механізмів, що одночасно посилюють і відкритість, і безпеку [11; 12]. Водночас, у практиці реалізації адміністративно-правових механізмів виявляються низка проблем: формалізм при розгляді інформаційних запитів, зловживання правом на відмову в доступі, нечіткість критеріїв віднесення інформації до обмеженої, недостатній рівень цифрової грамотності посадових осіб та брак ефективного зовнішнього контролю.

Висновки. Означені виклики сьогодення вимагають постійного вдосконалення адміністративно-правових механізмів у сфері доступу до публічної інформації й інформаційної безпеки. На нашу думку, наявні законодавчі зміни не повністю враховують реальну



швидкість трансформації інформаційних загроз. Відтак, одним із перспективних напрямів є створення оперативних міжвідомчих груп, що здатні на практиці забезпечити аналіз ризиків і формування дієвих алгоритмів обмеження інформації. Такий підхід дозволить мінімізувати розрив між появою нових загроз і реакцією державних інституцій.

Іншими ключовими напрямками удосконалення є: уточнення категорій інформації й критеріїв її обмеження, впровадження прозорих стандартів прийняття рішень, стандартизація та автоматизація адміністративних процедур, розвиток електронних сервісів і порталів відкритих даних. Необхідно посилювати кіберзахист систем органів публічної влади, впроваджувати багаторівневий контроль доступу й протоколи реагування на інциденти.

Важливо також розширювати повноваження незалежних інституцій, залучати громадськість до контролю, а державним службовцям забезпечувати сучасну цифрову освіту та підвищення кваліфікації. Гармонізація із міжнародними стандартами має ґрунтуватися на детальному аналізі вітчизняних ризиків і потенціалу цифрової інфраструктури. Зокрема, впровадження стандартів ISO/IEC 27001 та регулярний аудит інформаційних систем допоможуть не лише формально відповідати глобальним трендам, а й реально посилити стійкість українських електронних платформ. Сукупність цих заходів створює адаптивну систему адміністративно-правових механізмів, здатну забезпечити доступність публічної інформації та захист національних інтересів в інформаційному суспільстві.

Список використаних джерел:

1. Бліхар М.М. Інформаційна безпека в інтернет-просторі: правові засади. *Вісник Львівського університету. Серія юридична*. 2022. № 74. С. 154–162.
2. Рішення Конституційного Суду України від 20.04.2022 № 3-р/2022. <https://zakon.rada.gov.ua/laws/show/v003p710-22#Text>
3. Качур Т.М. Баланс відкритості та безпеки: європейський досвід для України. *Журнал європейського права*. 2023. № 3. С. 87–97.
4. Діхтієвський В.П. Адміністративно-правове регулювання доступу до публічної інформації монографія. Харків: Право, 2023. 152 с.
5. Transparency and Accountability in Public Administration: Comparative Legal Aspects. *Journal of Public Policy*. 2024. Vol. 7. P. 150–167.
6. 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>.
7. Плужник О.П., Кириченко Л.В. Інформаційна безпека громадянина у період воєнного стану: правові аспекти. *Право України*. 2023. № 5. С. 45–58.
8. Про інформацію Закон України від 02.10.1992 № 2657-XII (у редакції від 15.11.2024). URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>.
9. 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>.
10. Національний координаційний центр кібербезпеки при РНБО України. URL: <https://www.ncscc.gov.ua/>.
11. Офіційний портал відкритих даних України. URL: <https://data.gov.ua/>.
12. Міністерство цифрової трансформації України. Електронні сервіси. URL: <https://thedigital.gov.ua/>.

