МАНЖУЛА А. А.,
доктор юридичних наук, професор,
професор кафедри права
та правоохоронної діяльності
(Центральноукраїнський державний університет ім. Володимира Винниченка)

СОКУРЕНКО О. А.,
кандидат юридичних наук, доцент,
доцент кафедри права та правоохоронної діяльності
(Центральноукраїнський державний університет ім. Володимира Винниченка)

УДК 351.746
DOI https://doi.org/10.32842/2078-3736/2025.4.1.27

АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В ПУБЛІЧНО-ІНФОРМАЦІЙНІЙ СФЕРІ: ФОРМУВАННЯ БЕЗПЕКОВОГО СЕРЕДОВИЩА, ПРОТИДІЯ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ ТА ГАРАНТУВАННЯ ДОСТУПУ ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ В УМОВАХ ДІЯЛЬНОСТІ ПУБЛІЧНОЇ ВЛАДИ

У науковій статті здійснено комплексний аналіз адміністративно-правового реагування на інформаційні загрози в контексті забезпечення національної безпеки України. Автор виходить із того, що трансформація глобального інформаційного простору, цифровізація державного управління, зростання впливу соціальних мереж і кібертехнологій сприяють не лише позитивним зрушенням у сфері комунікацій, але й створюють нові, часто гібридні загрози для державності, демократичного ладу та правопорядку. Особливої актуальності проблема набуває в умовах збройної агресії проти України, коли інформаційна зброя активно використовується як складова військово-політичної стратегії супротивника.

З позицій адміністративного права досліджено сутність публічно-інформаційної сфери як об'єкта правового регулювання та захисту. Публічно-інформаційна сфера розглядається як сукупність правовідносин, що виникають у процесі створення, зберігання, поширення, обробки, використання інформації органами публічної влади, а також взаємодії цих органів з іншими суб'єктами інформаційної діяльності. Показано, що національна інформаційна безпека залежить не лише від технічного захисту інфраструктури, а й від ефективності інституційного, організаційного та правового реагування на загрози.

У центрі уваги – діяльність органів публічної адміністрації у сфері виявлення, фіксації, блокування та локалізації шкідливого інформаційного впливу, включаючи фейки, маніпуляції, інформаційно-психологічні операції та деструктивну пропаганду. Розкрито функціональну роль таких суб'єктів, як Служба безпеки України, Національна поліція, Державна служба спеціального зв'язку та захисту інформації, інші органи виконавчої влади, уповноважені забезпечувати інформаційну безпеку.

У статті охарактеризовано особливості нормативно-правового забезпечення захисту інформаційного простору, включаючи основні законодавчі та підзаконні акти, які визначають порядок взаємодії органів влади, межі їх компетенції, інструменти адміністративного впливу та процедури притягнення до відповідальності за поширення шкідливої інформації. Зроблено акцент на проблемах імплементації міжнародних стандартів у сфері кібербезпеки та інформаційного захисту в національне законодавство.

На основі проведеного аналізу сформульовано висновки щодо стану адміністративно-правового реагування на інформаційні загрози в Україні, окреслено проблемні аспекти правозастосовної практики та надано загальні рекомендації щодо посилення спроможності держави у сфері інформаційної безпеки.

Ключові слова: *адміністративно-правове забезпечення, національна безпека, публічно-інформаційна сфера, безпекове середовище, інформаційні загрози, доступ до публічної інформації, публічна влада, адміністративно-правове регулювання, інформація, інформаційний простір, кіберпростір.*

Manzhula A. A., Sokurenko O. A. Administrative and legal support of national security in the public information sphere: formation of a security environment, counteraction to information threats and guaranteeing access to public information in the conditions of public authority activities

The scientific article provides a comprehensive analysis of the administrative and legal response to information threats in the context of ensuring the national security of Ukraine. The author proceeds from the fact that the transformation of the global information space, the digitalization of public administration, the growing influence of social networks and cyber technologies contribute not only to positive developments in the field of communications, but also create new, often hybrid threats to statehood, democratic order and law and order. The problem becomes particularly relevant in the context of armed aggression against Ukraine, when information weapons are actively used as a component of the enemy's military-political strategy.

From the standpoint of administrative law, the essence of the public information sphere as an object of legal regulation and protection is studied. The public information sphere is considered as a set of legal relations that arise in the process of creating, storing, distributing, processing, using information by public authorities, as well as the interaction of these authorities with other subjects of information activity. It is shown that national information security depends not only on the technical protection of the infrastructure, but also on the effectiveness of institutional, organizational and legal response to threats.

The focus is on the activities of public administration bodies in the field of detecting, recording, blocking and localizing harmful information influence, including fakes, manipulations, information and psychological operations and destructive propaganda. The functional role of such entities as the Security Service of Ukraine, the National Police, the State Service for Special Communications and Information Protection, and other executive bodies authorized to ensure information security is revealed.

The article describes the features of the regulatory and legal support for the protection of the information space, including the main legislative and regulatory acts that determine the procedure for interaction between authorities, the boundaries of their competence, instruments of administrative influence and procedures for bringing to justice for the dissemination of harmful information. Emphasis is placed on the problems of implementing international standards in the field of cybersecurity and information protection into national legislation.

Based on the analysis, conclusions are formulated on the state of administrative and legal response to information threats in Ukraine, problematic aspects of law enforcement practice are outlined, and general recommendations are provided for strengthening the state's capacity in the field of information security.

Key words: *administrative and legal support, national security, public information sphere, security environment, information threats, access to public information, public authority, administrative and legal regulation, information, information space, cyberspace.*

Постановка проблеми та її актуальність. В умовах гібридної війни, інформаційної експансії та цифровізації всіх сфер суспільного життя питання забезпечення національної безпеки у публічно-інформаційній сфері набуває особливої актуальності. Публічна влада водночас виконує функції гаранта інформаційної безпеки, організатора ефективної комунікації з суспільством та суб'єкта, що зобов'язаний забезпечувати доступ до публічної інформації. Однак сучасна реальність в Україні свідчить про низку проблем: зростання масштабів інформаційної агресії з боку іноземних держав, недосконаліть правових механізмів протидії дезінформації, правовий нігілізм у сфері доступу до інформації, а також нерівномірний розвиток інституційного потенціалу органів публічної влади.

Існує об'єктивна потреба у вдосконаленні адміністративно-правових механізмів, спрямованих на формування стійкого безпекового середовища, яке не суперечить демократичним стандартам відкритості влади та свободи слова. Водночас викликом залишається гармонізація забезпечення інформаційної безпеки з гарантуванням конституційного права громадян на доступ до публічної інформації. Це зумовлює необхідність комплексного наукового аналізу та нормативно-правового удосконалення адміністративно-правового регулювання у сфері національної безпеки в інформаційному просторі.

Стан опрацювання цієї проблематики. Проблематика адміністративно-правового забезпечення національної безпеки в інформаційній сфері досліджувалася в роботах як українських, так і зарубіжних науковців. Зокрема, ґрунтовні теоретико-правові засади інформаційної безпеки та її місце в системі національної безпеки висвітлені у працях В. П. Горбатенка, В. М. Мандрика, І. О. Брижко, О. П. Заєць, де аналізується державна інформаційна політика та загрози в інформаційному просторі.

Питання правового регулювання доступу до публічної інформації та відкритості публічної влади досліджували Є. Б. Сташевський, І. С. Шевченко, О. І. Остапенко, які акцентують увагу на реалізації конституційного права громадян на інформацію в умовах демократичної держави.

Окрему увагу у науковій літературі приділено темі боротьби з дезінформацією, кіберзагрозами та інформаційною агресією, про що свідчать праці А. В. Литвиненка, К. В. Скубака, С. В. Кравченка, які вивчають питання інформаційної безпеки в умовах воєнного конфлікту та гібридної війни.

Мета дослідження полягає в теоретико-правовому обґрунтуванні сутності та особливостей адміністративно-правового забезпечення національної безпеки в публічно-інформаційній сфері, з урахуванням викликів інформаційної війни, цифровізації суспільства та необхідності забезпечення балансу між гарантуванням інформаційної безпеки й реалізацією конституційного права громадян на доступ до публічної інформації.

Виклад основного матеріалу. Адміністративно-правове забезпечення національної безпеки у публічно-інформаційній сфері постає як багаторівнева система заходів, механізмів та правових інструментів, які спрямовані на захист національних інтересів у сфері інформації, а також на формування стабільного безпекового середовища в умовах демократичного функціонування органів публічної влади. З огляду на стрімкий розвиток цифрових технологій, кіберпростору та телекомунікацій, інформаційна сфера дедалі частіше виступає не лише інструментом комунікації, але й самостійним полем виникнення загроз державній безпеці. У цьому контексті адміністративне право відіграє роль основного

регулятора відносин між публічною владою, суспільством та суб'єктами, що діють у сфері обігу інформації. Сучасна концепція національної безпеки у публічно-інформаційній сфері ґрунтується на принциповій необхідності забезпечення балансу між захистом інформаційного простору держави та гарантуванням фундаментальних прав і свобод людини, зокрема права на доступ до публічної інформації, свободи вираження поглядів і думки, захисту персональних даних та ін.

Формування безпекового середовища в публічно-інформаційній сфері є одним із ключових напрямів державної політики у сфері національної безпеки. Цей процес реалізується шляхом упровадження комплексу адміністративно-правових заходів, що охоплюють удосконалення нормативно-правової бази, функціонування спеціалізованих інституцій (зокрема, Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації, Національного центру оперативно-технічного управління мережами зв'язку), а також розвиток механізмів інформаційного моніторингу, кіберзахисту, протидії деструктивному контенту та систем запобігання поширенню недостовірної інформації. Необхідною умовою ефективного забезпечення інформаційної безпеки виступає також нормативна конкретизація базових понять, таких як «інформаційна загроза», «дезінформація», «фейкові новини», «гібридна інформаційна атака», що дозволить забезпечити юридичну визначеність і уніфіковане правозастосування в межах національного інформаційного простору.

У зазначеному контексті стратегічного значення набуває офіційне визначення поняття «інформаційна загроза». Відповідно до Указу Президента України від 15 жовтня 2021 року «Про рішення Ради національної безпеки і оборони України «Про Стратегію інформаційної безпеки», інформаційна загроза – це «потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні» [1]. Таке визначення встановлює нормативні межі для ідентифікації ризиків в інформаційному просторі, сприяє формуванню скоординованої державної політики протидії деструктивному впливу та забезпечує правові підстави для створення національного механізму реагування в умовах гібридної війни.

Особливої уваги потребує феномен дезінформації як системного інструменту дестабілізації внутрішнього інформаційного порядку. Згідно з визначенням Кембриджського словника, дезінформація – це неправдива інформація, яка поширюється з метою введення в оману. Цей підхід узгоджується з позицією міжнародних організацій: у Спільній декларації ООН, ОБСЄ та інших суб'єктів наголошується, що дезінформація є свідомо викривленою інформацією, спрямованою на маніпулювання громадською думкою, дискредитацію політичних опонентів або отримання економічної вигоди. Згідно з доповіддю Спеціального доповідача ООН із захисту свободи думки (2021), дезінформація становить серйозну загрозу соціальній стабільності, оскільки здатна провокувати недовіру до демократичних інституцій, медіа та урядових структур [2].

Фейкові новини, як специфічна форма дезінформації, значною мірою посилилися внаслідок цифровізації інформаційного простору та зниження рівня довіри до традиційних ЗМІ. Соціальні мережі, які водночас є інструментом демократизації доступу до інформації, стали середовищем, у якому активно поширюються неправдиві повідомлення, що мають на меті спотворити громадське сприйняття суспільно-політичних процесів. У зв'язку з цим надзвичайно актуальним є впровадження національних і міждержавних механізмів для боротьби з фейками, зокрема формування ефективної стратегії інформаційної гігієни, посилення цифрової медіаграмотності населення, нормативного контролю за поширенням недостовірної інформації [3, с. 77].

Важливу загрозу в інформаційному просторі становлять також гібридні атаки, які поєднують кібернетичні, інформаційно-психологічні та технічні методи впливу. У контексті кібербезпеки гібридна атака передбачає синергію декількох векторів впливу: соціальної

інженерії, впровадження шкідливого програмного забезпечення, експлуатації вразливостей цифрової інфраструктури. Такий комплексний підхід суттєво ускладнює виявлення джерел загрози, потребуючи високого рівня координації зусиль між суб'єктами публічної влади, а також запровадження дієвих правових засобів превенції, виявлення та реагування [4].

У цьому контексті особливого значення набуває адміністративно-правове регулювання відповідальності за порушення у сфері медіа, інформації та кібербезпеки. Відповідні правові норми мають бути чіткими, пропорційними та відповідати стандартам Європейського суду з прав людини щодо обмеження свободи вираження. Тільки за умови дотримання балансу між безпековими інтересами держави та гарантіями основоположних прав людини можливо сформувати ефективну модель національного інформаційного суверенітету в умовах цифрової трансформації та зростання глобальних інформаційних ризиків.

У цьому контексті надзвичайно актуальним є питання формування єдиної системи реагування на інформаційні загрози, яка б поєднувала функції попередження, нейтралізації, ліквідації наслідків і правового притягнення до відповідальності. Основоположним елементом такої системи має стати розбудова ефективного адміністративно-правового механізму, що передбачатиме оперативну взаємодію між ключовими суб'єктами публічної адміністрації – Службою безпеки України, Державною службою спеціального зв'язку та захисту інформації, Міністерством цифрової трансформації, Національною поліцією України, Міністерством оборони (у частині кіберзахисту збройних сил), а також органами судової влади в частині оперативного контролю за законністю обмежувальних заходів у цифровому середовищі.

Правова база у сфері протидії інформаційним загрозам досі залишається недостатньо розвиненою, що зумовлює нормативну фрагментарність, дублювання повноважень, а інколи – їхню невизначеність. Зокрема, чинне законодавство України не містить чітких класифікацій інформаційних інцидентів, критеріїв розмежування їх за рівнем небезпеки (низький, середній, високий, критичний), а також порядку ескалації відповідних адміністративних дій. Водночас на практиці інформаційні атаки можуть мати катастрофічні наслідки, зокрема – паралізацію критичних об'єктів інфраструктури, поширення паніки, підрив легітимності державної влади.

З метою підвищення ефективності реагування на інформаційні загрози доцільно передбачити на рівні закону запровадження Єдиного реєстру інформаційних інцидентів, доступ до якого матимуть визначені законом суб'єкти. У цьому реєстрі фіксуватимуться всі випадки інформаційного впливу, включно з їх джерелами, характером, рівнем загрози, результатами реагування. Це дозволить уніфікувати підходи до обробки даних, сформувати єдину аналітичну базу для подальшої розробки державної політики у сфері інформаційної безпеки та забезпечити належний моніторинг тенденцій загроз.

Окремим напрямом адміністративно-правового вдосконалення має стати розробка процедурного кодексу в сфері інформаційної безпеки, який унормує: порядок ініціювання процедур реагування на інформаційні атаки; строки адміністративних рішень про блокування контенту; критерії співмірності втручання з огляду на стандарти свободи вираження; механізми апеляції та перегляду рішень у судовому чи адміністративному порядку.

У межах цього кодексу доцільним є закріплення принципів пропорційності, обґрунтованості, необхідності та найменшого втручання, відповідно до практики Європейського суду з прав людини, а також створення інституційного механізму незалежного нагляду, наприклад, у формі окремого підрозділу Уповноваженого Верховної Ради з прав людини або спеціалізованої незалежної наглядової ради при РНБО.

У сфері міжнародної взаємодії Україна має активніше імплементувати положення Будапештської конвенції про кіберзлочинність [5], а також адаптувати положення Директиви (ЄС) 2022/2555 (NIS2) [6], яка передбачає комплексну систему кіберризик-менеджменту та обов'язки операторів критично важливих послуг щодо попередження і реагування на кіберінциденти. Ратифікація та інтеграція цих міжнародних стандартів дозволить Україні гармонізувати власне адміністративне законодавство з європейськими вимогами, що особливо важливо в контексті євроінтеграційного курсу.

Таким чином, удосконалення адміністративно-правового регулювання протидії інформаційним загрозам потребує не лише оновлення нормативно-правової бази, але й перегляду концептуальних підходів до інформаційної безпеки як до динамічної багаторівневої системи. Це передбачає поєднання превентивних, оперативних, наглядових і контрольних функцій в єдиній інституційній моделі з прозорими процедурами та чітким розподілом відповідальності. Упровадження таких підходів сприятиме зміцненню національної стійкості до гібридних загроз, збереженню довіри до демократичних інституцій і посиленню авторитету правової держави.

Паралельно з безпековими аспектами, важливим компонентом адміністративно-правового регулювання виступає забезпечення права на доступ до публічної інформації як одного з базових елементів демократичної правової держави. Закон України «Про доступ до публічної інформації» установлює загальні правила відкритості у діяльності суб'єктів владних повноважень, визначає категорії інформації з обмеженим доступом та регламентує процедури подання, розгляду й оскарження запитів [7]. Проте на практиці нерідко виникають конфлікти між потребою у відкритості та необхідністю забезпечення державної чи публічної безпеки, що вимагає пошуку справедливого балансу між правом на інформацію та інтересами національної безпеки. Адміністративне право має забезпечувати можливість ефективного захисту як публічного інтересу, так і приватних прав суб'єктів, шляхом встановлення чітких, недискримінаційних та передбачуваних процедур доступу до інформації.

Особливої актуальності ці питання набули в умовах воєнного стану, коли обмеження доступу до окремих категорій інформації можуть бути об'єктивно зумовлені потребами оборони, однак повинні залишатися співмірними, обґрунтованими та тимчасовими. В цьому контексті важливо враховувати міжнародні стандарти, зокрема рекомендації Ради Європи та практику Європейського суду з прав людини, зокрема рішення у справі «Володимир Торбіч проти України» (2023), яке підтверджує, що обмеження права на доступ до інформації можливе лише за умов дотримання принципу пропорційності. Ратифікація Україною Конвенції Ради Європи про доступ до офіційних документів (Тромсе) вимагає адаптації національного законодавства до європейських підходів, у тому числі шляхом застосування трискладового тесту при обґрунтуванні відмов у наданні інформації. Водночас саме адміністративні суди мають гарантувати, що державні органи не зловживають міркуваннями безпеки для обмеження відкритості, а відповідні обмеження є дійсно необхідними в демократичному суспільстві. Таким чином, адміністративно-правовий механізм повинен забезпечувати ефективний захист як публічного інтересу, так і приватних прав громадян навіть у складних умовах збройного конфлікту [8].

Висновок. Таким чином, адміністративно-правове забезпечення національної безпеки в публічно-інформаційній сфері в умовах діяльності публічної влади має базуватися на поєднанні захисних механізмів протидії інформаційним загрозам із гарантованим дотриманням конституційних прав громадян на свободу слова, доступ до публічної інформації та безпеку в цифровому середовищі. Формування безпекового інформаційного середовища потребує впровадження ефективної системи адміністративно-правового реагування, нормативного врегулювання базових понять і класифікацій загроз, а також налагодження взаємодії між ключовими суб'єктами публічної адміністрації. Зростання масштабів гібридних загроз і дезінформаційних кампаній вимагає від держави стратегічної цілісності та високого рівня інституційної спроможності. Публічна влада має діяти не лише як інструмент захисту інформаційного простору, але і як гарант прозорості, відкритості та правової визначеності в комунікації з суспільством. Лише за таких умов можливе ефективне функціонування системи інформаційної безпеки, що відповідає викликам часу та принципам демократичної правової держави.

Список використаних джерел:

1. Стратегія інформаційної безпеки : Указ Президента України від 28 грудня 2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення 20.07.2025)
2. Дезінформація: як розпізнати та боротися. URL: https://law.chnu.edu.ua/dezinformatsiia-yak-rozpiznaty-ta-borotysia/ (дата звернення 29.07.2025)
3. Доскіч Л. С. Фейкові новини як новітній засіб маніпуляції та дезінформації. *Бібліотекознавство. Документознавство. Інформологія.* 2022. № 4. С. 72–77. (дата звернення 15.07.2025)
4. Гібридна атака. URL: https://www.vpnunlimited.com/ua/help/cybersecurity/hybrid-attack?srsltid=AfmBOoqLO4U7kSJPpVfmjkAv4eoTdo6G1zOSY6bf9-rrznRgk-sxhc3e (дата звернення 16.07.2025)
5. Конвенція про кіберзлочинність від 23 листопада 2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення 20.07.2025)
6. Директива Європейського Парламенту і Ради (ЄС) 2022/2555 від 14 грудня 2022 року про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972 та скасування Директиви (ЄС) 2016/1148 (Директива NIS 2) URL: https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text (дата звернення 20.07.2025)
7. Про доступ до публічної інформації: Закон України від 13 січня 2011 року № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення 20.07.2025)
8. Про забезпечення права на доступ до публічної інформації в умовах правового режиму воєнного стану. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1696751/ (дата звернення 19.07.2025)

Дата першого надходження рукопису до видання: 23.07.2025
Дата прийнятого до друку рукопису після рецензування: 18.08.2025
Дата публікації: 26.09.2025