УДК 342.9:004.056(477)
DOI https://doi.org/10.32782/TNU-2707-0581/2026.5/21

Горєлова В. Ю.
https://orcid.org/0000-0001-6536-2422
Таврійський національний університет імені В. І. Вернадського

АДМІНІСТРАТИВНО-ПРАВОВИЙ МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ВОЄННИХ ТА ГІБРИДНИХ ЗАГРОЗ

У статті досліджуються адміністративно-правові засади забезпечення інформаційної безпеки України в умовах воєнних та гібридних загроз. Обґрунтовується необхідність комплексного підходу до захисту національного інформаційного простору з урахуванням особливостей правового режиму воєнного стану. Наголошується, що сучасні загрози охоплюють дезінформацію, пропаганду, інформаційно-психологічні операції, кібератаки, витоки даних, втручання у функціонування критичної інформаційної інфраструктури та нові ризики, пов'язані з використанням штучного інтелекту. Звертається увага на значення чіткого розмежування адміністративних, правових, організаційних і технічних засобів забезпечення інформаційної безпеки та їх узгодженої реалізації суб'єктами публічного управління. Зазначається необхідність посилення координації між державними органами, удосконалення процедур реагування на кіберінциденти та розвитку кіберзахисту. Обґрунтовується висновок про те, що ефективність адміністративно-правового забезпечення залежить не лише від нормативної бази, а й від практичної спроможності уповноважених суб'єктів своєчасно виявляти, локалізувати та нейтралізувати інформаційні загрози. У статті розроблено рекомендації щодо вдосконалення адміністративно-правових механізмів забезпечення інформаційної безпеки, підвищення інституційної спроможності суб'єктів кіберзахисту, розвитку міжвідомчої взаємодії та адаптації правових інструментів до динаміки воєнних і гібридних загроз. Особливу увагу приділено поширенню вимог кіберзахисту на приватний сектор критичної інфраструктури, а також запровадженню незалежних аудитів ефективності адміністративно-правових засобів. Доведено доцільність системного оновлення підходів до державного управління інформаційною безпекою, що має забезпечити належний баланс між безпековими потребами держави та правами людини.

Ключові слова: *інформаційна безпека, правовий режим воєнного стану, кібербезпека, кіберзахист, воєнні загрози, гібридні загрози, критична інформаційна інфраструктура, суб'єкти забезпечення інформаційної безпеки, адміністративно-правове забезпечення.*

Постановка проблеми. В умовах повномасштабної війни інформаційна безпека України стала невід'ємною складовою національної безпеки та оборони держави. Воєнні й гібридні загрози охоплюють не лише поширення дезінформації та пропаганди, а й кібератаки, інформаційно-психологічні операції, втручання у функціонування критичної інформаційної інфраструктури, витоки даних та інші форми деструктивного впливу. За таких умов адміністративно-правове забезпечення інформаційної безпеки потребує постійного вдосконалення відповідно до характеру сучасних загроз. Проблема полягає у відсутності цілісного адміністративно-правового механізму, який би забезпечував узгоджену діяльність суб'єктів публічного управління. Неузгодженість проявляється у трьох основних площинах. По-перше, спостерігається дублювання функцій між окремими органами, зокрема у сфері реагування на кіберінциденти. По-друге, відсутній єдиний центр обміну даними про загрози, що ускладнює оперативне реагування. По-третє, існують розбіжності між воєнними та цивільними підходами до організації інформаційної безпеки, що особливо помітно в умовах воєнного стану.

Аналіз останніх досліджень і публікацій. Дослідження окремих аспектів адміністративно-правового забезпечення інформаційної безпеки

© Горєлова В. Ю., 2026
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

здійснювали різні науковці. В. М. Кондратенко та О. А. Сокуренко дослідили адміністративно-правові засади доступу до публічної інформації в діяльності правоохоронних органів [1]. А. А. Васильєв і Я. О. Бакай зосередилися на регулюванні кібербезпеки критичної інформаційної інфраструктури в умовах воєнного стану [2]. А. О. Крупнова визначила систему суб'єктів адміністративно-правового забезпечення інформаційної безпеки [3]. А. М. Лисеюк і Т. В. Свінцицька проаналізували правове забезпечення кібербезпеки України в умовах воєнного стану та євроінтеграції [4]. С. Ф. Константінов розглянув адміністративно-правові засоби забезпечення інформаційної безпеки держави у воєнний період [5]. Водночас поза увагою дослідників залишлося питання узгодження компетенції цих суб'єктів та механізмів їхньої міжвідомчої взаємодії в умовах одночасного впливу воєнних і гібридних загроз.

Невирішені раніше частини загальної проблеми. Отже, попри наявність значної кількості наукових досліджень, недостатньо комплексно дослідженими залишаються питання формування цілісного адміністративно-правового механізму забезпечення інформаційної безпеки України в умовах одночасного впливу воєнних і гібридних загроз.

Постановка завдання. Метою статті є комплексне дослідження адміністративно-правових засад забезпечення інформаційної безпеки України в умовах воєнних та гібридних загроз. Для досягнення поставленої мети передбачається охарактеризувати сучасні загрози, визначити систему суб'єктів забезпечення інформаційної безпеки, проаналізувати адміністративні, правові, організаційні та технічні засоби протидії, дослідити особливості міжвідомчої взаємодії та обґрунтувати напрями вдосконалення нормативно-правового забезпечення.

Виклад основного матеріалу. Дослідження адміністративно-правового механізму забезпечення інформаційної безпеки потребує чіткої методологічної основи, оскільки йдеться про складний об'єкт, що перебуває під одночасним впливом воєнних і гібридних загроз. Саме тому системний підхід застосовано для розгляду цього механізму як цілісної системи нормативних, інституційних і процедурних елементів, що перебувають у взаємозв'язку та взаємодіють із зовнішнім безпековим середовищем [6]. Формально-юридичний метод дозволив проаналізувати норми Конституції України [7], законів України «Про національну безпеку України» [8], «Про основні засади забезпечення кібербезпеки України» [9], «Про правовий режим воєнного стану» [10] та підзаконних актів. Порівняльно-правовий метод використано для зіставлення національної моделі з практикою Європейського Союзу (зокрема діяльністю Агентства ЄС з кібербезпеки ENISA) [11] та Німеччини [12]. Такий підхід дозволив виявити спільні риси та відмінності в організації інституційної складової забезпечення інформаційної безпеки.

Сучасний стан забезпечення інформаційної безпеки України визначається одночасним впливом воєнних та гібридних загроз, які взаємно підсилюють одна одну. Повномасштабна збройна агресія російської федерації супроводжується системними кібератаками на об'єкти критичної інформаційної інфраструктури, масованими дезінформаційними кампаніями та інформаційно-психологічними операціями. З огляду на це, адміністративно-правовий механізм забезпечення інформаційної безпеки має розглядатися не як сукупність окремих заходів, а як цілісна система взаємопов'язаних елементів, до яких належать нормативна основа, інституційна складова, процедурні механізми та ресурсне забезпечення.

Сучасні воєнні та гібридні загрози інформаційній безпеці характеризуються різноманітністю форм і методів впливу. Дезінформація та пропаганда залишаються основними інструментами маніпуляції суспільною свідомістю. За даними Центру протидії дезінформації, з 2022 року зафіксовано тисячі випадків скоординованого поширення недостовірної інформації, спрямованої на підрив довіри до органів влади [13]. Кібератаки набули ознак усталеного типу військових операцій. Дослідження фахівців засвідчують, що DDoS-атаки становлять близько 87,5 відсотка всіх зареєстрованих кібератак, а найбільше їх спрямовано на фінансовий, державний та інформаційно-комунікаційний сектори [14, с. 8]. Показовим прикладом є кібератака на оператора мобільного зв'язку «Київстар» у грудні 2023 року, яка призвела до тимчасового порушення роботи мережі по всій країні. Інцидент засвідчив вразливість навіть великих приватних операторів та необхідність посилення державного нагляду за кіберзахистом критичної інфраструктури. Крім того, з'являються нові ризики, пов'язані з використанням штучного інтелекту. Зокрема, технології глибокого синтезу голосу та зображення використовуються для створення дипфейків, які ускладнюють верифікацію інформації. Відповідно до Стратегії кібербезпеки України, такі технології віднесено до нових викликів, що потребують додаткових правових інструментів реагування [15].

Окремої уваги потребують загрози, пов'язані з витоками персональних даних та втручанням у функціонування критичної інформаційної інфраструктури. Такі інциденти завдають шкоди не лише окремим громадянам, а й обороноздатності держави в цілому. Отже, правове регулювання має охоплювати весь спектр загроз, а не лише найбільш очевидні з них [16, с. 121].

Система суб'єктів забезпечення інформаційної безпеки включає кілька рівнів. Провідну роль відіграє Рада національної безпеки і оборони України, яка координує політику у сфері інформаційної безпеки. Національний координаційний центр кібербезпеки функціонує як робочий орган Ради та забезпечує загальний контроль за діяльністю суб'єктів сектору безпеки і оборони [9]. Державна служба спеціального зв'язку та захисту інформації України відповідає за технічний захист інформації, функціонування систем захищеного доступу та реагування на кіберінциденти. Служба безпеки України здійснює контррозвідувальну діяльність у кіберпросторі та протидіє кібертероризму. Національна поліція України забезпечує запобігання, виявлення та розкриття кіберзлочинів [17]. Міністерство оборони України та Генеральний штаб Збройних Сил України опікуються захистом військових інформаційних систем, а також координують діяльність кіберсил [18].

Водночас значна кількість суб'єктів ускладнює ефективний обмін інформацією про загрози та правопорушення. Наприклад, Державна служба спеціального зв'язку та захисту інформації відповідає за технічний захист, тоді як Служба безпеки України – за контррозвідувальну діяльність у кіберпросторі. На практиці виникають ситуації, коли один і той самий інцидент потребує одночасного реагування обох органів, що ускладнює визначення відповідального суб'єкта. З огляду на це, ключовим завданням є налагодження чіткої міжвідомчої взаємодії, яка б виключала дублювання повноважень та забезпечувала оперативність реагування [19, с. 173].

Певним орієнтиром тут може слугувати досвід Європейського Союзу. ENISA виконує не лише консультативну, а й координуючу функцію, готуючи щорічні звіти про стан кібербезпеки та рекомендації для держав-членів [11]. Це дозволяє формувати спільні стандарти та оперативно реагувати на транскордонні загрози. В Україні аналогічний орган (Національний координаційний центр кібербезпеки) поки що не має достатніх повноважень для впливу на галузеві центри реагування. Запозичення окремих елементів моделі ENISA, зокрема обов'язковості рекомендацій для органів влади, могло б підвищити ефективність національної системи.

Протидія інформаційним і кіберзагрозам здійснюється через поєднання адміністративних, правових, організаційних і технічних засобів. Адміністративні засоби охоплюють дозвільні процедури, ліцензування медіа, контроль контенту та координацію діяльності державних органів. Прикладом може слугувати діяльність Національної ради України з питань телебачення і радіомовлення, яка здійснює моніторинг та анулювання ліцензій для запобігання пропаганді [20]. Правові засоби формують нормативну базу для регулювання інформаційних відносин. Зокрема, Кримінальний кодекс України передбачає відповідальність за поширення завідомо неправдивих повідомлень про загрозу безпеці громадян [21], а Кодекс України про адміністративні правопорушення встановлює відповідальність за поширення неправдивих чуток, що можуть викликати паніку [22].

Організаційні засоби включають створення спеціалізованих підрозділів з кіберзахисту в органах влади, призначення керівників з кіберзахисту та функціонування національної системи реагування на кіберінциденти [23]. Технічні засоби охоплюють шифрування даних, моніторинг мереж, двофакторну аутентифікацію, застосування систем запобігання витокам даних та управління подіями безпеки. Важливим кроком стало прийняття Закону України від 27 березня 2025 року № 4336-IX, який посилив вимоги до кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури, зокрема запровадив обов'язкову перевірку постачальників програмного забезпечення [24]. Водночас поза межами цього Закону залишилося регулювання приватного сектору, який також є частиною критичної інфраструктури. Це створює розрив між державним і приватним сегментами кіберзахисту, що може бути використано агресором. Отже, доцільно поширити вимоги цього Закону й на приватних операторів критичної інфраструктури.

Особливості міжвідомчої взаємодії в умовах воєнного стану потребують окремої уваги. Практика засвідчує, що оперативність реагування залежить не лише від наявності повноважень, а й від якості комунікації між суб'єктами. Для цього доцільно запровадити єдину платформу обміну інформацією про кіберзагрози, яка б об'єднувала дані CERT-UA, кіберполіції, Служби безпеки України та галузевих центрів реагування. Крім

того, варто передбачити регулярне проведення спільних навчань і тренувань, спрямованих на відпрацювання алгоритмів реагування на комплексні гібридні атаки. Показовим є досвід Німеччини, де Національний центр кіберзахисту об'єднує представників федеральних і земельних органів влади, а також бізнесу [12]. Така модель дозволяє оперативно обмінюватися інформацією та координувати реакцію на інциденти. В Україні аналогічну роль міг би відіграти Національний координаційний центр кібербезпеки, але для цього йому потрібно надати повноваження з обов'язкового залучення представників приватного сектору.

Напрями вдосконалення нормативно-правового та організаційного забезпечення інформаційної безпеки потребують системного оновлення. Доцільно ухвалити спеціальний закон про інформаційну безпеку в умовах воєнного стану, який би систематизував чинні норми та усунув прогалини [25]. Варто законодавчо закріпити повний перелік інформаційних загроз та детермінант їх поширення, що сприятиме своєчасному виявленню та нейтралізації. Необхідно посилити юридичну відповідальність за поширення дезінформації та втручання в роботу критичної інформаційної інфраструктури. Слід розвивати співпрацю з Європейським Союзом та НАТО у сфері обміну технологіями кіберзахисту та гармонізації стандартів [26]. Важливо забезпечити регулярне підвищення кваліфікації державних службовців у сфері кібербезпеки та медіаграмотності. Нарешті, доцільно запровадити незалежні аудити ефективності адміністративно-правових засобів, що дозволить адаптувати їх до змінюваних загроз.

Таким чином, адміністративно-правовий механізм забезпечення інформаційної безпеки України в умовах воєнних та гібридних загроз потребує системного оновлення. Ефективність цього механізму залежить від узгодженості нормативної бази, інституційної спроможності суб'єктів, оперативності процедур реагування та належного ресурсного забезпечення. Лише за умови комплексного підходу можливо забезпечити належний баланс між безпековими потребами держави та правами людини, що є запорукою стійкості національного інформаційного простору.

Висновки. Проведене дослідження дозволяє сформулювати три узагальнюючі положення. Чинна модель адміністративно-правового забезпечення інформаційної безпеки формувалася переважно як відповідь на вже реалізовані загрози. Через це окремі сегменти регулювання розвивалися нерівномірно, а законодавче закріплення окремих механізмів відставало від динаміки гібридних загроз. Відтак подальший розвиток має бути спрямований на випереджальне моделювання ризиків та своєчасне оновлення нормативної бази.

Розгалуженість системи суб'єктів забезпечення інформаційної безпеки не є недоліком сама собою, однак за відсутності чітких процедур координації вона перетворюється на чинник, що уповільнює реагування. Дослідження засвідчує, що дублювання функцій між окремими органами та відсутність єдиного центру обміну даними про загрози створюють розрив між нормативним закріпленням повноважень і практичною здатністю їх реалізувати. Відтак удосконалення потребує не стільки розширення переліку суб'єктів, скільки впорядкування їхньої взаємодії.

Подальший розвиток адміністративно-правового механізму доцільно спрямувати на подолання фрагментарності регулювання. Ідеться про поширення вимог кіберзахисту на приватний сектор критичної інфраструктури, законодавче закріплення повного переліку інформаційних загроз та запровадження незалежних аудитів ефективності адміністративно-правових засобів. Перспективними напрямами подальших наукових розвідок є розроблення критеріїв оцінювання ефективності цих засобів та адаптація національного законодавства до стандартів ЄС у сфері кібербезпеки.

Список літератури:

1. 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. Т. 2, № 89. С. 452–457. DOI: 10.24144/2307-3322.2025.89.2.69.

2. Васильєв А. А., Бакай Я. О. Адміністративно-правове регулювання кібербезпеки критичної інформаційної інфраструктури в умовах воєнного стану. *Український політико-правовий дискурс.* 2025. № 11. DOI: 10.5281/zenodo.21297649.

3. Крупнова А. О. Система суб'єктів адміністративно-правового забезпечення інформаційної безпеки в Україні. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2024. Т. 2, № 83. С. 277–287. DOI: 10.24144/2307-3322.2024.83.2.40.

4. Лисеюк А. М., Свінцицька Т. В. Правове забезпечення кібербезпеки України в умовах воєнного стану та євроінтеграції. *Право та інновації*. 2024. № 4 (48). С. 32–38. DOI: 10.37772/2518-1718-2024-4(48)-4.

5. Константінов С. Ф. Адміністративно-правові засоби забезпечення інформаційної безпеки держави у воєнний період. *Вісник Харківського національного університету внутрішніх справ*. 2025. № 4 (111). С. 165–178. DOI: 10.32631/v.2025.4.13.

6. Баран М. Information Security as a Subject of Administrative and Legal Regulation. *Social and Legal Studios*. 2021. Vol. 4, No. 3. P. 50–56. DOI: 10.32518/2617-4162-2021-3-50-56.

7. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 20.09.2026).

8. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 20.09.2026).

9. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 20.09.2026).

10. Про правовий режим воєнного стану : Закон України від 12.05.2015 № 389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text (дата звернення: 20.09.2026).

11. European Union Agency for Cybersecurity (ENISA). URL: https://www.enisa.europa.eu/ (дата звернення: 20.09.2026).

12. Nationales Cyber-Abwehrzentrum (National Cyber Defence Centre), Germany. URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/Nationales-IT-Lagezentrum/Nationales-Cyber-Abwehrzentrum/nationales-cyber-abwehrzentrum_node.html (дата звернення: 20.09.2026).

13. Аналітичний звіт «Мережа російського деструктивного інформаційного впливу CopyCop». Центр протидії дезінформації. 2025. URL: https://cpd.gov.ua/reports/analitychnyj-zvit-merezha-rosijskogo-destruktyvnogo-informaczijnogo-vplyvu-copycop/ (дата звернення: 20.09.2026).

14. Duguin S., Pavlova P. The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict. Policy Department, Directorate-General for External Policies. European Union, 2023. 47 p. URL: https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2023)702.570 (дата звернення: 20.09.2026).

15. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 20.09.2026).

16. Смотрич Д. В., Браілко Л. Інформаційна безпека в умовах воєнного стану. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2023. Вип. 77, ч. 2. С. 121–127. DOI: 10.24144/2307-3322.2023.77.2.20.

17. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення: 20.09.2026).

18. Про Збройні Сили України : Закон України від 06.12.1991 № 1934-XII. URL: https://zakon.rada.gov.ua/laws/show/1934-12#Text (дата звернення: 20.09.2026).

19. Balan S., Balan L., Vorotynskyy V., Rybak I., Tarasiuk V. State information policy in the context of hybrid threats: Legal and political aspects. *Social & Legal Studios.* 2025. Vol. 8, No. 1. P. 166–177. DOI: 10.32518/sals1.2025.166.

20. Про Національну раду України з питань телебачення і радіомовлення : Закон України від 23.09.1997 № 538/97-ВР. URL: https://zakon.rada.gov.ua/laws/show/538/97-вр#Text (дата звернення: 20.09.2026).

21. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 20.09.2026).

22. Кодекс України про адміністративні правопорушення : Закон України від 07.12.1984 № 8073-X. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text (дата звернення: 20.09.2026).

23. Про затвердження Порядку функціонування національної системи реагування на кіберінциденти : Постанова Кабінету Міністрів України від 04.07.2023 № 679. URL: https://zakon.rada.gov.ua/laws/show/679-2023-%D0%BF#Text (дата звернення: 20.09.2026).

24. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27.03.2025 № 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/4336-20#Text (дата звернення: 20.09.2026).

25. Діхтієвський П. В. Адміністративно-правове забезпечення захисту персональних даних громадян в умовах воєнного стану. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування.* 2023. № 10. DOI: 10.54929/2786-5746-2023-10-01-15.

26. Semenenko O., Dobrovolskyi U., Sliusarenko M., Levchenko I., Mytchenko S. Legal aspects of the cybertechnology development and the cyberweapon use in the state defence sphere: Global and Ukrainian experience. *Social & Legal Studios.* 2023. Vol. 6, No. 4. P. 192–199. DOI: 10.32518/sals4.2023.192.

Horielova V. Yu. ADMINISTRATIVE AND LEGAL MECHANISM FOR ENSURING THE INFORMATION SECURITY OF UKRAINE IN THE CONTEXT OF MILITARY AND HYBRID THREATS

This article examines the administrative and legal principles of ensuring Ukraine's information security in the context of military and hybrid threats. It substantiates the need for a comprehensive approach to protecting the national information space, taking into account the specific features of the legal regime of martial law. The article emphasises that contemporary threats encompass disinformation, propaganda, information and psychological operations, cyberattacks, data breaches, interference with the functioning of critical information infrastructure, and emerging risks associated with the use of artificial intelligence. Attention is drawn to the importance of a clear delineation between administrative, legal, organisational, and technical means of ensuring information security, as well as their coordinated implementation by public administration entities. The article also highlights the necessity of strengthening coordination among state authorities, improving procedures for responding to cyber incidents, and developing cyber defence. The conclusion is substantiated that the effectiveness of administrative and legal frameworks depends not only on the regulatory framework but also on the practical capacity of authorised entities to identify, contain, and neutralise information threats in a timely manner. The article develops recommendations for improving the administrative and legal mechanisms for ensuring information security, enhancing the institutional capacity of cyber defence entities, developing inter-agency cooperation, and adapting legal instruments to the evolving dynamics of military and hybrid threats. Particular attention is paid to extending cyber defence requirements to the private sector of critical infrastructure, as well as to introducing independent audits of the effectiveness of administrative and legal measures. The expediency of systematically updating approaches to public administration in the field of information security is substantiated in order to ensure an appropriate balance between the state's security needs and human rights.

Keywords: *information security, legal regime of martial law, cybersecurity, cyber defence, military threats, hybrid threats, critical information infrastructure, entities responsible for ensuring information security, administrative and legal provision.*

Дата першого надходження статті до видання: 06.09.2026
Дата прийняття статті до друку після рецензування: 21.09.2026
Дата публікації (оприлюднення) статті: 18.11.2026