



УДК 342.9

DOI <https://doi.org/10.32782/cuj-2026-1-16>**Шопіна Ірина Миколаївна**

доктор юридичних наук, професор,
професор кафедри адміністративно-правових дисциплін
Львівського державного університету внутрішніх справ
Scopus ID: 57210888060
ORCID: 0000-0003-3334-7548

ВИКОРИСТАННЯ СУБ'ЄКТАМИ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ: ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ

Метою статті є визначення особливостей використання суб'єктами правоохоронної діяльності технологій штучного інтелекту (далі – ШІ) з позиції правового регулювання. З'ясовано, що нині вже напрацьована певна теоретико-методологічна база для подальшого вивчення та розвитку правового забезпечення використання технологій ШІ. Однак у контексті правового статусу правоохоронних органів мають місце суттєві прогалини.

Визначено, що використання суб'єктами правоохоронної діяльності технологій ШІ може бути пов'язано з ризиками порушення прав людини, втручання у приватне життя, витоку персональних даних, дискримінації, а також зі створенням загроз національній та воєнній безпеці держави. Водночас повна відмова від використання таких технологій в умовах цифровізації злочинності, розвитку кіберзагроз та застосування ШІ суб'єктами протиправної діяльності призвела б до істотного зниження ефективності правоохоронної системи.

Аргументовано необхідність внесення змін до законодавчих актів, які визначають правовий статус правоохоронних органів, з метою доповнення їх наступними положеннями: правові підстави застосування ШІ у діяльності правоохоронних органів; критерії допустимості використання конкретних технологічних рішень, заснованих на технологіях ШІ; механізми зовнішнього і внутрішнього контролю за використанням ШІ у правоохоронній діяльності; юридична відповідальність за неправомірне використання ШІ.

Обґрунтовано доцільність встановлення законодавчої заборони на використання правоохоронними органами тих систем ШІ, щодо яких відсутня можливість аудиту алгоритмів, контролю за потоками даних або гарантій кібербезпеки. В умовах повномасштабної збройної російської агресії ці вимоги мають розглядатися як елемент забезпечення національної, воєнної та інформаційної безпеки.

Аргументовано, що мають бути ліквідовані правові прогалини, пов'язані зі здійсненням недержавної правоохоронної діяльності, що потребує прийняття законів про приватну детективну діяльність та про службу безпеки суб'єктів господарювання. У цих правових актах мають знайти своє відображення підстави, умови, порядок і контроль за використанням технологій ШІ.

Ключові слова: штучний інтелект, правоохоронна діяльність, правоохоронні органи, інформаційна безпека, кібербезпека, інформаційна діяльність, інформаційні технології, інформаційні загрози, інформаційні ризики, правове регулювання.

Shopina I. M. The use of artificial intelligence technologies by law enforcement subjects: peculiarities of legal regulation

This article examines the legal dimensions of implementing artificial intelligence (AI) technologies within law enforcement operations. While a foundational theoretical framework for AI integration exists, the study identifies critical legislative gaps regarding the specific legal status of law enforcement agencies in this domain.

The research highlights that AI deployment carries inherent risks, including potential human rights infringements, privacy violations, data breaches, and algorithmic bias, which may threaten national and military security. Conversely, the author argues that a categorical rejection of AI is untenable; given the rapid digitalization of criminal activity and the rise of AI-driven cyber threats, law enforcement must adopt these tools to maintain systemic efficacy.

To address these challenges, the paper proposes comprehensive legislative reforms to define the legal grounds for AI application. Key recommendations include establishing admissibility criteria for AI-based solutions, implementing

© Шопіна І. М., 2026

robust internal and external oversight mechanisms, and defining liability for misuse. Furthermore, the study advocates for a statutory ban on AI systems that lack transparency, auditability, or sufficient cybersecurity guarantees. In the context of ongoing Russian military aggression, these measures are framed as vital components of Ukraine's national and information security. Finally, the article stresses the need to regulate non-state law enforcement, specifically by establishing AI-related guidelines for private detective and corporate security services.

Key words: *artificial intelligence, law enforcement, law enforcement agencies, information security, cybersecurity, information activity, information technologies, information threats, information risks, legal regulation.*

Вступ. Технології штучного інтелекту досить швидко стали невід'ємною частиною української реальності. Вони активно використовуються в різних видах діяльності, розробляються і затверджуються правила етичної поведінки щодо застосування штучного інтелекту у закладах освіти, засобах медіа, ІТ-компаніях тощо. Однак правове регулювання в означеній сфері значно відстає від активного розвитку технологій ШІ. Особливо помітним є таке відставання у сфері правового забезпечення правоохоронної діяльності. Саме правоохоронні органи здійснюють повноваження, безпосередньо пов'язані із застосуванням заходів процесуального примусу та спеціальних технічних засобів, а також з обробкою значних масивів персональних даних. За таких умов використання технологій штучного інтелекту без чітко визначених правових рамок створює ризики порушення прав людини і громадянина та може негативно вплинути на забезпечення національної та воєнної безпеки. Вказане слугує підтвердженням актуальності теми цієї статті.

Матеріали та методи. Проблеми використання штучного інтелекту у правоохоронній діяльності привертають увагу як зарубіжних, так і українських вчених. У дослідженні британських дослідниць Я. Еззеддін, П. С. Байерл та Х. Гібсон з'ясовано, що у світлі сучасного технологічного прогресу на штучний інтелект (далі – ШІ) покладаються надії щодо покращення продуктивності, підвищення ефективності та максимізації результатів. Для правоохоронних органів він може виявитися цінним для оптимізації аналізу доказів та впровадження проактивних заходів запобігання злочинності. Проте громадяни висловлюють закономірне занепокоєння щодо втручання в приватне життя, упередженості, нерівності та неточних рішень. У дослідженні, в якому було використано інтерв'ю 111 громадян для

визначення їх поглядів на використання ШІ поліцією, було вивчено існуючі суспільні занепокоєння та сформульовано пропозиції щодо заходів захисту від негативних наслідків використання ШІ правоохоронними органами в контексті кіберзлочинності та тероризму [1].

К. К. Апостолакис, Н. Дімітріу, Г. Маргетіс, С. Нтоа, Д.Цоварас і К. Стефанідіс у своєму дослідженні представили екосистему DARLENE, яка поєднує доповнену реальність (далі – AR) та ШІ, що дозволяє покращити можливості співробітників правоохоронних органів на місцях, дозволяючи своєчасно аналізувати численні потоки даних за допомогою масштабованої архітектури ШІ та персоналізоване, адаптивне представлення результатів ШІ через AR. Зокрема, предметом аналізу стали такі можливості DARLENE, як аналіз конфігурації тіла кожної людини після об'єднання обчислених теплових карт. Це може допомогти правоохоронцям краще аналізувати події, що відбуваються, навіть за бетонними стінами, а також дозволить виконувати завдання комп'ютерного зору вищого рівня для розпізнавання та відстеження людської діяльності. Водночас вчені наголошують на тому, що успіх DARLENE значною мірою залежить від створення надійної етичної бази відповідно до чинного законодавства та етичних принципів як під час його розробки, так і під час впровадження. З цією метою розробка DARLENE постійно перевіряється внутрішніми та зовнішніми експертами з етики [2].

О. В. Турута і О. П. Турута у своєму дослідженні дійшли висновку, що неправомірне використання алгоритмів ШІ створює безліч проблем, таких, як порушення права на життя, права на недоторканність приватного життя, обмеження свободи слова та думки, порушення права на справедливий судовий розгляд та презумпцію невинності, права на

рівні можливості і недискримінацію, права на працю тощо. Оскільки технології ШІ використовують певні набори даних, то найчастіше спостерігається порушення прав певних груп населення. Це можуть бути жінки та діти, а також певні етнічні, расові чи релігійні групи тощо. Уряди країн світу та компанії, які використовують технології ШІ, на думку вчених, мають усвідомлювати недосконалість даних, на основі яких технологія навчається, та дбати про недопущення дискримінації і порушень прав людини, бути готовими надати своєчасні та ефективні засоби правового захисту у випадках, коли рішення, прийняті машинами, виявляються невірними [3].

Можна констатувати, що нині вже напрацьована певна теоретико-методологічна база для подальшого вивчення та розвитку правового забезпечення використання технологій ШІ. Однак у контексті правового статусу правоохоронних органів це питання вивчено ще недостатньо, що обумовлює спрямованість подальших наукових пошуків.

У роботі використано формально-догматичний, порівняльно-правовий методи, а також метод правового моделювання.

Метою статті є визначення особливостей використання суб'єктами правоохоронної діяльності технологій штучного інтелекту з позиції правового регулювання.

Результати. Динамічний розвиток інформаційних технологій обумовлює кардинальні зміни у сфері правоохоронної діяльності. Відкриття доступу до технологій ШІ мало своїми наслідками його використання суб'єктами протиправної діяльності у багатьох державах, які легко обходять закладені у програмні продукти обмеження [4]. За таких умов відмова правоохоронних органів використовувати такі технології означала б суттєве зниження ефективності їх діяльності щодо розкриття, розслідування та попередження кримінальних правопорушень, забезпечення публічного порядку тощо.

Однак широке впровадження технологій ШІ у всі сфери суспільних відносин, у тому числі у правоохоронну, пов'язано не лише зі здобутками, а й з численними ризиками. Такі ризики охоплюють велику кількість

політичних, економічних, психологічних, екологічних та інших чинників, проте найбільш важливими з них є, на нашу думку, правові. Саме право легітимізує застосування різних технологій державними інституціями, створює нормативний каркас їх діяльності, встановлює обмеження та заборони, спрямовані у першу чергу на забезпечення конституційних прав і свобод людини та громадянина.

Аналізуючи правові аспекти використання ШІ у правоохоронній діяльності, перш за все хотілося б зупинитися на наявності правових підстав їх застосування. Як відомо, відповідно до ч. 2 ст. 6 Основного Закону органи законодавчої, виконавчої та судової влади здійснюють свої повноваження у встановлених цією Конституцією межах і відповідно до законів України [5]. Не всі правоохоронні органи є органами виконавчої влади, однак Основний Закон також включає положення про те, що організація і порядок діяльності правоохоронних органів визначаються законом (ч. 3 ст. 17) [5]. Тобто законодавець наголошує на наявності законодавчих рамок функціонування правоохоронних органів та здійснення ними своєї діяльності. Ці положення, на нашу думку, повністю поширюються на інформаційне забезпечення означених інституцій, у тому числі й на використання ними ШІ.

Однак аналіз більшості законів України, які регулюють правовий статус правоохоронних органів, свідчить, що у сфері їх правомочностей використовувати інформаційні технології мають місце суттєві прогалини. Переважно право правоохоронного органу та його співробітників здійснювати інформаційну діяльність визначається у законодавстві дуже вузько, точково, в контексті окремих робочих операцій. Так, у Законі України «Про прокуратуру» присутні окремі згадування, в яких визначено права прокурорів використовувати у своїй діяльності деякі інформаційні технології. У ч. 8 ст. 23 закріплено, що з метою виявлення необґрунтованих активів та збору доказів їх необґрунтованості в межах своєї компетенції прокурор у порядку, визначеному законодавством, має прямий доступ до автоматизованих інформаційних і довідкових систем, реєстрів та банків даних, держателем (адміністратором)

яких є державні органи або органи місцевого самоврядування [6]. Як можна побачити, згадані у цій нормі ресурси адмініструються державою або органами місцевого самоврядування. Однак технології ШІ створені та розповсюджуються комерційними структурами інших держав, а українські органи публічної влади не мають впливу ані на принципи їх роботи, ані на доступ для контролю якості.

Безумовно, і Європейський Союз, і Сполучені Штати Америки мають безперечні правові здобутки у сфері забезпечення безпеки держави, суспільства і громадян у зв'язку із використанням технологій ШІ. Однак предметом регулювання цих правових актів є у першу чергу безпека громадян, суспільства та урядів цих країн. Для українського споживача, у тому числі для правоохоронних органів, таке використання здійснюється у зоні ризиків. До таких ризиків слід віднести неправомірне поширення персональних даних, підвищення вразливості державних та єдиних реєстрів, інших інформаційно-телекомунікаційних систем, дані з яких використовуються при роботі з ШІ. В умовах руйнування архітектури міжнародної безпеки та повернення деяких держав до силових методів міжнародної взаємодії слід також з усією серйозністю розглядати можливість використання прихованих для українського користувача алгоритмів ШІ для дестабілізації ситуації в правоохоронній системі та у державі в цілому.

Отже, використання ШІ у правоохоронній діяльності має бути перш за все безпечним. Надання ШІ доступу до відомостей та даних правоохоронної спрямованості, до систем відеоспостережень, у тому числі у режимі онлайн, має здійснюватися лише за умови контролю за використанням і розповсюдженням таких даних розробниками. Безумовно, це суттєво обмежить кількість ресурсів ШІ, якими зможуть скористатися українські правоохоронці. Однак в аспекті забезпечення національної та воєнної безпеки такі заходи не здаються нам надмірними. Враховуючи процитовані вище положення Конституції України, має бути встановлена законодавча заборона користуватися засобами ШІ, відносно яких відсутня можливість контролю. Ці положення мають знайти своє відображення у правових актах,

які регулюють правовий статус суб'єктів правоохоронної діяльності.

Вказане вимагає відповіді на питання про віднесення тих чи інших інституцій до правоохоронних. Проблема визначення поняття та ознак суб'єктів, які здійснюють правоохоронну діяльність, не є новою. Протягом трьох десятиліть існування української держави їй приділяло увагу багато науковців, які намагалися створити об'єктивні та логічні критерії віднесення певних інституцій до категорії правоохоронних. Однак головна проблема, яка обумовлює потребу у постійному доктринальному аналізі та виробленні правових позицій, так і залишилася невирішеною.

Легальне визначення правоохоронних органів у Законі України «Про державний захист працівників суду і правоохоронних органів» має відкритий характер і містить сумнівні критерії віднесення певних суб'єктів до означеної категорії. Разом з тим, у правових актах, які визначають компетенцію посадових осіб та інших працівників державних інституцій та органів місцевого самоврядування, досить часто згадуються правоохоронні органи в контексті обов'язкового повідомлення їм певної інформації, залучення їх до здійснення певної діяльності тощо.

Велика Палата Верховного Суду у постанові від 30 серпня 2023 року по справі № 633/195/17 (провадження № 13-39 кс 23) визначила, що критеріями віднесення органів державної влади до правоохоронних є інституційно-функціональні ознаки, що визначають правовий статус такого органу у системі органів державної влади. На відміну від інших органів державної влади, які можуть також здійснювати правоохоронну функцію, для правоохоронних органів вона є основною. При цьому при віднесенні того чи іншого органу державної влади до правоохоронного слід звернути увагу насамперед на те, чи визначено відповідний орган у спеціальному нормативно-правовому акті, який регламентує його правовий статус, як правоохоронний, а також на повноваження, які цей орган здійснює, тобто на закріплену за ними на законодавчому рівні правоохоронну функцію [7]. На нашу думку, така правова позиція породжує більше питань,

ніж відповідей, оскільки звернення до доктринальної категорії «правоохоронні функції» дозволяє переконатися у неоднорідному її розумінні у різних теоретичних джерелах.

Зокрема, існують протилежні позиції щодо виконання правоохоронної функції недержавними інституціями. Думка про відсутність монополії держави на правоохоронну діяльність є достатньо поширеною серед правників. Хоча, безумовно, існують вчені, які не поділяють таку позицію. До недержавних правоохоронних інституцій на доктринальному рівні відносять приватні охоронні підприємства, служби безпеки установ, підприємств та організацій, приватних детективів та їх агенції, громадські формування з охорони громадського порядку та державного кордону [8; 9 та ін.]. Охоронна діяльність та функціонування громадських формувань з охорони громадського порядку та державного кордону врегульовані на законодавчому рівні. Про якість такого регулювання можна сперечатися, в аспекті використання ШІ також наявні прогалини. Так, суб'єкти охоронної діяльності мають право застосовувати технічні засоби охорони – технічні засоби, що використовуються під час здійснення охоронної діяльності: системи, прилади та обладнання для виявлення, оповіщення і попередження про наявність небезпеки для життя людей та / або майна [10]. Як свідчить наведений вище аналіз системи DARLENE, технічні засоби охорони нового покоління можуть базуватися на технологіях ШІ і доповненої реальності, що значно підвищує їх ефективність. Однак питання про коло суб'єктів, які будуть мати доступ до даних відеоспостереження, залишається поза межами правового регулювання. Додамо, що у 2025 році у Тайвані, Австралії, Італії та деяких урядових структурах США з міркувань безпеки було заборонено використовувати ШІ китайського стартапу DeerSeek [11; 12].

Особливу небезпеку несе у собі використання ШІ суб'єктами, які здійснюють правоохоронну діяльність поза межами правового регулювання. В Україні нині надають послуги десятки тисяч приватних детективів та детективних агенцій (код за КВЕД 80.30 – проведення розслідувань). Їх діяльність включає розшук людей, пошук власності, перевірку

конкурентів, встановлення фактів шлюбної зради, перевірки на поліграфі тощо і здійснюється відповідно до загальних вимог до господарської діяльності, без урахування правоохоронної специфіки. Як відомо, прийнятий у 2017 році Верховною Радою України Закон України «Про приватну детективну (розшукову) діяльність» так і не було підписано Президентом України. Подальші спроби визначити статус приватних детективів на законодавчому рівні також не дали результатів [8]. Отже, ризики відсутності адекватного правового забезпечення розслідувань приватних детективів поєднуються з ризиками використання ними можливостей ШІ. Схожа ситуація спостерігається і у сфері діяльності служб безпеки підприємств, установ та організацій.

Висновки. Використання суб'єктами правоохоронної діяльності технологій ШІ може бути пов'язано з ризиками порушення прав людини, втручання у приватне життя, витоку персональних даних, дискримінації, а також зі створенням загроз національній та військовій безпеці держави. Водночас повна відмова від використання таких технологій в умовах цифровізації злочинності, розвитку кіберзагроз та застосування ШІ суб'єктами протиправної діяльності призвела б до істотного зниження ефективності правоохоронної системи.

Це потребує внесення змін до законодавчих актів, які визначають правовий статус правоохоронних органів, з метою доповнення їх наступними положеннями: правові підстави застосування ШІ у діяльності правоохоронних органів; критерії допустимості використання конкретних технологічних рішень, заснованих на технологіях ШІ; механізми зовнішнього і внутрішнього контролю за використанням ШІ у правоохоронній діяльності; юридична відповідальність за неправомірне використання ШІ.

Особливої актуальності набуває питання встановлення законодавчої заборони на використання правоохоронними органами тих систем ШІ, щодо яких відсутня можливість аудиту алгоритмів, контролю за потоками даних або гарантій кібербезпеки. В умовах повномасштабної збройної російської агресії ці вимоги мають розглядатися як елемент забезпечення національної, воєнної та інформаційної безпеки.

Крім того, мають бути ліквідовані правові прогалини, пов'язані зі здійсненням недержавної правоохоронної діяльності, що потребує прийняття законів про приватну детективну діяльність та про службу безпеки суб'єктів господарювання. У цих правових актах мають знайти своє відображення підстави, умови, порядок і контроль за використанням технологій ШІ.

Література

1. Ezzeddine Y., Bayerl P. S., Gibson H. Citizen Perspectives on Necessary Safeguards to the Use of AI by Law Enforcement Agencies. arXiv. 2023. DOI: <https://doi.org/10.48550/arXiv.2306.01786> (дата звернення: 24.01.2026).
2. Apostolakis K. C., Dimitriou N., Margetis G., Ntoa S., Tzovaras D., Stephanidis C. DARLENE – Improving situational awareness of European law enforcement agents through a combination of augmented reality and artificial intelligence solutions. *Open Res Eur*. 2022. Jan 21;1:87. DOI: 10.12688/openreseurope.13715.2.
3. Турута О. В., Турута О. П. Штучний інтелект крізь призму фундаментальних прав людини. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2022. № 71. С. 49–54. DOI: <https://doi.org/10.24144/2307-3322.2022.71.7>
4. Мягких С. В., Шопіна Ю. О. Проблеми використання штучного інтелекту для вчинення кіберзлочинів. *Кібербезпека в дії: від особистого захисту до національного: матеріали наук.-практ. круглого столу* (Київ, 15 жовт. 2025 р.). Київ, 2025. С. 75–80.
5. Конституція України : Закон від 28.06.1996 р. № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254k/96-вр> (дата звернення: 25.01.2026).
6. Про прокуратуру : Закон України від 14 жовт. 2014 р. № 1697-VII. URL: <https://zakon.rada.gov.ua/laws/show/1697-18#Text> (дата звернення: 25.01.2026).
7. Постанова Великої Палати Верховного Суду від 30 серпня 2023 року по справі № 633/195/17 (провадження № 13-39 кс 23). URL: <https://reyestr.court.gov.ua/Review/113396900> (дата звернення: 25.01.2026).
8. Мулявка Д. Г. Проблеми адміністративно-правового забезпечення приватної детективної та недержавної охоронної діяльності в Україні: монографія. Ірпінь : Університет державної фіскальної служби України, 2020. 404 с.
9. Завальний М. В. Адміністративно-правові засади діяльності та взаємодії державних та недержавних суб'єктів правоохорони в Україні : монографія. Харків : Стильна типографія, 2018. 320 с.
10. Про охоронну діяльність: Закон України від 22 берез. 2012 р. № 4616-VI. URL: <https://zakon.rada.gov.ua/laws/show/4616-17#Text> (дата звернення: 25.01.2026).
11. Taiwan bans government departments from using DeepSeek AI Reuters. 2025. 3 Feb. URL: <https://www.reuters.com/technology/taiwan-bans-government-departments-using-deepseek-ai-2025-02-03/> (дата звернення: 23.01.2026).
12. Italy blocks Chinese AI app DeepSeek over data concerns Associated Press. 2025. 30 Jan. URL: <https://apnews.com/article/dc7e87835ed7a125b5e46614d8bd80d0> (дата звернення: 23.01.2026).

References

1. Ezzeddine, Y., Bayerl, P. S., & Gibson, H. (2023). Citizen perspectives on necessary safeguards to the use of AI by law enforcement agencies. arXiv. DOI: <https://doi.org/10.48550/arXiv.2306.01786>
2. Apostolakis, K. C., Dimitriou, N., Margetis, G., Ntoa, S., Tzovaras, D., & Stephanidis, C. (2022). DARLENE – Improving situational awareness of European law enforcement agents through a combination of augmented reality and artificial intelligence solutions. *Open Research Europe*, 1 (87). DOI: <https://doi.org/10.12688/openreseurope.13715.2>
3. Turuta, O. V., & Turuta, O. P. (2022). Shtuchnyi intelekt kriz pryzmu fundamentalnykh prav liudyny [Artificial intelligence through the prism of fundamental human rights]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Serii: Pravo*, (71), 49–54. DOI: <https://doi.org/10.24144/2307-3322.2022.71.7> [in Ukrainian].
4. Miakkykh, S. V., & Shopina, Yu. O. (2025). Problemy vykorystannia shtuchnoho intelektu dlia vchynennia kibezlochyniv [Problems of using artificial intelligence to commit cybercrimes]. In *Kiberbezpeka v dii: vid osobystoho zakhystu do natsionalnoho: materialy nauk.-prakt. kruhloho stolu*, 75–80. Kyiv [in Ukrainian].
5. Konstitutsiia Ukrainy [Constitution of Ukraine]: Zakon vid 28.06.1996 No. 254k/96-VR. (1996). URL: <https://zakon.rada.gov.ua/laws/show/254k/96-вр> [in Ukrainian]
6. Pro prokuraturu [On the Prosecutor's Office]: Zakon Ukrainy vid 14 zhovtnia 2014 roku No. 1697-VII. (2014). URL: <https://zakon.rada.gov.ua/laws/show/1697-18#Text> [in Ukrainian].

7. Postanova Velykoi Palaty Verkhovnoho Sudu vid 30 serpnia 2023 roku po spravi No. 633/195/17 (provadzhennia No. 13-39 ks 23) [Resolution of the Grand Chamber of the Supreme Court of August 30, 2023 in case No. 633/195/17]. (2023). URL: <https://reyestr.court.gov.ua/Review/113396900> [in Ukrainian].

8. Muliavka, D. H. (2020). Problemy administratyvno-pravovoho zabezpechennia pryvatnoi detektyvnoi ta nederzhavnoi okhoronnoi diialnosti v Ukraini [Problems of administrative and legal support of private detective and non-state security activities in Ukraine: monograph]. Irpin : Universytet derzhavnoi fiskalnoi sluzhby Ukrainy. [in Ukrainian].

9. Zavalnyi, M. V. (2018). Administratyvno-pravovi zasady diialnosti ta vzaiemodii derzhavnykh ta nederzhavnykh subiektiv pravookhorony v Ukraini [Administrative and legal framework for the activity and interaction of state and non-state law enforcement entities in Ukraine : monograph]. Kharkiv : Styl'na typohrafiia. [in Ukrainian].

10. Pro okhoronnu diialnist [On security activities]: Zakon Ukrainy vid 22 bereznia 2012 roku No. 4616-VI. (2012). URL: <https://zakon.rada.gov.ua/laws/show/4616-17#Text> [in Ukrainian].

11. Reuters. (2025, February 3). Taiwan bans government departments from using DeepSeek AI. URL: <https://www.reuters.com/technology/taiwan-bans-government-departments-using-deepseek-ai-2025-02-03/>

12. Associated Press. (2025, January 30). Italy blocks Chinese AI app DeepSeek over data concerns. URL: <https://apnews.com/article/dc7e87835ed7a125b5e46614d8bd80d0>

Дата першого надходження статті до видання: 04.02.2025
Дата прийняття статті до друку після рецензування: 17.03.2026
Дата публікації (оприлюднення) статті: 20.04.2026