ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ВАРИНСЬКИЙ ВЛАДИСЛАВ ОЛЕКСІЙОВИЧ

УДК 342.9:34:004.8(477)

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ТА ПРАВОВІ ЗАСАДИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В УКРАЇНІ

12.00.07 «Адміністративне право і процес; фінансове право;
інформаційне право»

Реферат
дисертації на здобуття наукового ступеня
доктора юридичних наук

Одеса – 2026

Дисертацією є кваліфікаційна наукова праця на правах рукопису.

Робота підготовлена здобувачем самостійно.

Опоненти: доктор юридичних наук, професор,
КУДІНОВ Сергій Сергійович,
Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського",
головний науковий співробітник науково-дослідного центру Інституту спеціального зв'язку та захисту інформації;

доктор юридичних наук, професор
ВАСИЛЕНКО Віктор Михайлович,
Харківський національний університет внутрішніх справ, перший проректор;

доктор юридичних наук, професор
ТЕТЕРЯТНИК Ганна Костянтинівна,
Одеський державний університет внутрішніх справ,
завідувач кафедри кримінального процесу та криміналістики факультету підготовки фахівців для органів досудового розслідування Національної поліції України

Захист відбудеться 20 серпня 2026 р. о 10:00 годині на засіданні спеціалізованої вченої ради Д 41.884.04 в Одеському державному університеті внутрішніх справ за адресою: 65014, місто Одеса, вул. Успенська, 1.

З дисертацією можна ознайомитись на офіційному сайті https://oduvs.edu.ua/ та в науковій бібліотеці Одеського державного університету внутрішніх справ за адресою: 65014, місто Одеса, провулок Сабанський, 4.

Вчений секретар
спеціалізованої вченої ради **О.В. Ковальова**

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Обґрунтування вибору теми дослідження. Стрімкий розвиток технологій штучного інтелекту (далі – ШІ) став одним із визначальних чинників сучасної цифрової трансформації суспільства, державного управління та економіки. Системи штучного інтелекту дедалі активніше використовуються у сфері публічного адміністрування, правосуддя, охорони здоров'я, фінансової діяльності, оборони, національної безпеки, освіти, транспортної інфраструктури та інших сферах, у яких результати їх функціонування безпосередньо впливають на реалізацію прав, свобод і законних інтересів людини. Водночас розширення масштабів використання ШІ зумовлює виникнення якісно нових суспільних відносин, які потребують адекватного правового регулювання.

Сучасний розвиток ШІ характеризується переходом від допоміжних інформаційних технологій до автономних систем, здатних приймати рішення, що мають юридично значущі наслідки. Така трансформація зумовлює необхідність переосмислення традиційних підходів до правового регулювання, оскільки існуючі правові механізми були сформовані для регулювання діяльності людини та класичних інформаційних систем і не враховують особливостей функціонування автономних алгоритмічних моделей, генеративного штучного інтелекту, великих мовних моделей та інших сучасних AI-систем.

Особливої актуальності зазначена проблема набуває в умовах інтеграції України до Європейського Союзу та необхідності гармонізації національного законодавства із Регламентом (ЄС) 2024/1689 про встановлення гармонізованих правил щодо штучного інтелекту (AI Act), який започаткував принципово нову ризик-орієнтовану модель правового регулювання використання штучного інтелекту. Водночас імплементація європейських стандартів не може обмежуватися формальним перенесенням положень AI Act до національного законодавства, оскільки вони повинні бути адаптовані до особливостей системи публічного адміністрування України, структури органів державної влади, національного законодавства та існуючих механізмів реалізації владних повноважень.

Базовим документом державної політики в Україні в сфері регулювання ШІ залишається Концепція розвитку штучного інтелекту в Україні**,** затверджена Кабінетом Міністрів України ще у 2020 році, на її виконання Кабінет Міністрів України у 2025 році затвердив План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025–2026 роки.

Україна демонструє вражаючі темпи цифрової трансформації, що створює фундамент для впровадження ШІ: 1-ше місце у світі за Індексом електронної участі ООН (E-Participation Index), що свідчить про найвищий рівень залучення громадян до демократичних процесів через цифрові інструменти[1]; 5-те місце у світі за Індексом онлайн-послуг ООН (Online

[1] Міністерство цифрової трансформації України**.** Ukraine's GovTech Topping Global Rankings. URL: https://digitalstate.gov.ua/news/govtech/ukraines-govtech-topping-global-rankings

Services Index) у 2024 році Україна піднялася на 97 позицій з 2018 року[2]; 40-ве місце серед 195 країн у Government AI Readiness Index 2025 від Oxford Insights, при цьому показник цифровізації державних послуг досяг 99,63%, що відносить Україну до 10-ки країн Східної Європи у сфері розвитку ШІ[3]. Отже, досягнутий Україною рівень цифрової трансформації створює об'єктивні передумови для масштабного використання технологій ШІ. Масштабність та невідворотність цього процесу підтверджуються останніми макроекономічними та соціологічними маркерами 2025 – 2026 років. На глобальному рівні, за прогнозами аналітичних агентств Gartner та MarketsandMarkets, світові витрати на ШІ, які у 2025 році становили 1,48 трлн дол. США, вже у 2026 році перетнули межу у 2 трлн дол. США, демонструючи стрімку капіталізацію ринку з тенденцією досягнення 2,4 трлн дол. США до 2032 року[4].

На національному рівні зазначені тенденції віддзеркалюються у безпрецедентній динаміці залученості населення: за даними дослідницьких компаній Gradus Research та KMIC (січень – березень 2026 року), до 85% українців використовують ШІ регулярно або фрагментарно, причому найвища залученість фіксується серед молоді віком 18–29 років (58% регулярних користувачів)[5]. Концентрація споживчого попиту навколо безкоштовних версій домінуючих мультимодальних сервісів (ChatGPT, Gemini) у поєднанні з низькою готовністю індивідуальних користувачів інвестувати у платний контент (лише 6%) свідчить про те, що масова інтеграція технологій ШІ в Україні відбувається стихійно та переважно поза межами корпоративного або суворого відомчого контролю. Водночас це актуалізує необхідність формування сучасних теоретико-методологічних і правових засад їх використання.

Попри активний розвиток міжнародного та європейського правового регулювання використання ШІ, в Україні досі відсутня цілісна концепція правового забезпечення його використання. Чинне законодавство чітко не визначає системи суб'єктів публічного адміністрування у сфері штучного інтелекту, їх компетенції, повноважень, адміністративно-правового статусу, порядку взаємодії, механізмів державного контролю, розподілу юридичної відповідальності, реалізації принципу змістовного людського контролю **(**meaningful human oversight**)** та адміністративно-правових гарантій захисту прав людини при використанні систем ШІ. Необхідність імперативного втручання

---

[2] Міністерство цифрової трансформації України .Україна посіла 5-те місце за індексом онлайн-сервісів у глобальному рейтингу ООН. URL: https://digitalstate.gov.ua/news/govtech/ukraines-govtech-topping-global-rankings

[3] Україна піднялася на 14 позицій у світовому рейтингу зі штучного інтелекту: допомогла цифровізація держпослуг. URL: https://forbes.ua/news/ukraina-pidnyalasya-na-14-pozitsiy-u-svitovomu-reytingu-zi-shtuchnogo-intelektu-posivshi-40-te-mistse-23122025-35066

[4] Artificial Intelligence Market Trends 2025: Generative AI, AI Chips, and Cloud AI Platforms Fuel Industry Expansion. MarketsandMarkets Blog. 2026. 19 May. URL: https://www.marketsandmarketsblog.com/artificial-intelligence-market-trends-2025-generative-ai-ai-chips-and-cloud-ai-platforms-fuel-industry-expansion.html; Gartner Says Worldwide AI Spending Will Total $1.5 Trillion in 2025. *Gartner*. 2025. 17 Sept. URL: https://www.gartner.com/en/newsroom/press-releases/2025-09-17-gartner-says-worldwide-ai-spending-will-total-1-point-5-trillion-in-2025

[5] Скільки українців користуються ШІ та чи готові платити за нього. *Факти ICTV*. 08 квіт. 2026. URL: https://fakty.com.ua/ua/styl-zhyttia/nauka-tekhnolohii/20260408-skilky-ukrayinczіv-korystuyutsya-shi-ta-chy-gotovi-platyty-za-nogo/

публічної адміністрації та побудови жорстких правових бар'єрів обумовлюється стрімкою ескалацією правопорушень та інцидентів, пов'язаних із деструктивним або технічно недосконалим функціонуванням алгоритмічних моделей. Згідно з верифікованими даними глобальних моніторингових платформ AI Incident Database, OECD та MIT AI Risk Repository, кількість інцидентів у сфері ШІ зростає на 35–45% щороку, причому понад 58% із них безпосередньо зумовлені генеративними технологіями[6].

Тільки за останній звітний період зафіксовано сотні критичних інцидентів, архітектоніка яких чітко диференціюється за категоріями правової шкоди: дезінформація та деструктивний контентний вплив (28%), алгоритмічна дискримінація й упередженість (22%), а також прямі помилки у сфері фізичної та цифрової безпеки (14%)[7]. Особливу небезпеку для правопорядку становлять протиправні прояви у вигляді дипфейків (технології підробки голосу та відео), які виступають інструментарієм у понад 80% випадків масштабного кібершахрайства та фінансових махінацій. Ба більше, фіксація випадків генерації чат-ботами небезпечного контенту, що призводив до закликів до насильства або депресивних станів користувачів (зокрема, за участю найбільш поширеного інструменту ChatGPT), свідчить про наявність латентних екзистенційних та безпекових ризиків навіть у межах найбільш технологічно захищених систем[8].

Не менш важливою є необхідність формування сучасної доктрини адміністративно-правового регулювання використання штучного інтелекту, яка враховуватиме не лише технологічні особливості AI-систем, а й конституційні засади діяльності держави, принцип верховенства права, пріоритет прав і свобод людини, принципи належного врядування, цифрової трансформації та людиноцентризму. Відсутність таких доктринальних підходів істотно ускладнює вироблення ефективної державної політики у сфері використання штучного інтелекту, побудову дієвого механізму адміністративно-правового регулювання та визначення місця штучного інтелекту в системі публічного адміністрування.

Актуальність дисертаційного дослідження обумовлюється також практичними потребами держави. Використання систем ШІ вже сьогодні є одним із ключових напрямів цифровізації публічного управління, розвитку електронного урядування, цифрових адміністративних послуг, систем підтримки прийняття управлінських рішень, правоохоронної діяльності, оборонного сектору та відновлення України. За таких умов виникає об'єктивна необхідність створення ефективного адміністративно-правового механізму, який забезпечуватиме баланс між стимулюванням інноваційного розвитку та належним рівнем захисту прав людини, суспільних інтересів і національної безпеки.

---

[6] Ramanath. AI Incident Database Statistics 2026. *Presenc AI*. Updated May 2026. URL: https://presenc.ai/research/ai-incident-database-statistics-2026

[7] Ramanath. AI Incident Database Statistics 2026. *Presenc AI*. Updated May 2026. URL: https://presenc.ai/research/ai-incident-database-statistics-2026

[8] Ramanath. AI Incident Database Statistics 2026. *Presenc AI*. Updated May 2026. URL: https://presenc.ai/research/ai-incident-database-statistics-2026

Таким чином, актуальність теми дослідження зумовлена сукупністю взаємопов'язаних чинників: відсутністю цілісної адміністративно-правової доктрини використання штучного інтелекту в Україні; необхідністю адаптації європейських стандартів AI Governance до національної системи публічного адміністрування; потребою у формуванні теоретико-методологічних засад адміністративно-правового регулювання використання штучного інтелекту, а також практичною необхідністю вдосконалення механізму державного управління процесами створення, впровадження, використання та контролю за застосуванням систем ШІ.

Ступінь наукової розробленості проблеми. Аксіолого-правовий та методологічний фундамент роботи побудовано на засадах людиноцентричного розуміння права, пріоритетності фундаментальних свобод особи та її захисту від ризиків алгоритмічної автономізації. Вихідним орієнтиром у цьому контексті стали загальнотеоретичні підходи П. Рабіновича щодо людиноцентричного розуміння права, які в умовах зростання технологічних загроз, пов’язаних із використанням автономних цифрових систем, безпосередньо корелюють із західними концепціями відповідальності за технологічне майбутнє Г. Йонаса (H. Jonas), Х. Дрейфуса (H. Dreyfus) та доктриною проєктування, чутливого до ціннісних імперативів (Value Sensitive Design – Б. Фрідман (B. Friedman), Д. Генрі (D. G. Hendry), А. Борнінг (A. Borning).

На цьому фундаментальному підґрунті в українській юридичній науці сформувався напрям, присвячений концептуалізації цифрового правопорядку та визначенню правової природи штучного інтелекту, базові засади якого закладено у загальнотеоретичних працях О. Баранова, М. Карчевського та О. Костенка. Поряд із цим, на осмислення конкретних онтологічних та правових викликів функціонування алгоритмічних систем зорієнтовані дослідження К. Некіт, О. Радутного та О. Харитонової. Напрацювання зазначених авторів, присвячені проблематиці правової природи штучного інтелекту, відсутності у нього автономної юридичної волі та специфіці цивільно-правових ризиків, дозволяють чітко диференціювати штучний інтелект як самостійний цифровий феномен від суміжних технологічних систем, насамперед Інтернету речей (IoT).

У свою чергу, питання модернізації правової політики держави в умовах цифровізації та адаптації національного законодавства до європейських стандартів висвітлено у працях Д. Бєлова, О. Ковальчук, О. Олійник, В. Пилипчука, О. Павлюк, Т. Попової, Є. Тимошенко, Ю. Тюрі.

Доктринальні положення та окремі аспекти адміністративно-правового й інформаційно-правового характеру щодо формування та реалізації державної політики були предметом вивчення таких вчених як: В. Авер’янов, О. Баранов, К. Бєляков, Ю. Битяк, В. Василенко, В. Галунько, В. Грохольський, А. Денисова, Д. Журавльов, Д. Калаянов, Р. Калюжний, В. Колпаков, С. Кудінов, М. Корнієнко, В. Пядишев, Н. Свиридюк, В. Стефанюк, С. Тімченко, , Т. Тур, Т. Фулей, І. Цюприк, Ю. Шемшученко, М. Янишівського, Х. Ярмакі та ін. На галузевому рівні найбільш розробленими у вітчизняній доктрині є питання алгоритмізації та деліктних ризиків у діяльності органів судової влади, що

відображено у працях Я. Берназюка, О. Гиляки, О. Карпушової, та В. Рядінської. Водночас процесуальні загрози, межі предиктивного моделювання та ризики порушення фундаментальних прав особи у сфері кримінальної юстиції, правоохоронної діяльності та забезпечення безпеки стали предметом ґрунтовного вивчення у дослідженнях Н. Глинської, І. Гловюк, Д. Клепки, А. Нікітіна, Ю. Рєпіної, Н. Савінової, Г. Тетерятник, І. Тітка та О. Торбаса. Окреслена галузева проблематика суттєво розширюється зарубіжним доктринальним досвідом. Зокрема, у працях М. Еберса (M. Ebers), А. Ренди (A. Renda), а також у доповідях OECD та Ada Lovelace Institute обґрунтовано необхідність секторальних обмежень використання ШІ у сферах охорони здоров'я, національної оборони та освіти і науки.

Водночас аналіз сучасного стану наукової розробленості проблематики свідчить, що переважна більшість досліджень присвячена окремим правовим аспектам використання ШІ: визначенню його правової природи, питанням цивільної, кримінальної чи інформаційно-правової відповідальності, захисту персональних даних, етичним засадам функціонування алгоритмічних систем або аналізу окремих положень AI Act. Такий підхід не забезпечує цілісного розуміння систем ШІ як об'єкта адміністративно-правового та інформаційного регулювання та не дозволяє сформувати комплексну модель державного впливу на процеси його створення, впровадження, використання й контролю. Саме тому предметом цього дослідження є не окремі правові інститути, а теоретико-методологічні та правові засади використання штучного інтелекту, які розглядаються крізь призму механізму адміністративно-правового регулювання, системи його суб'єктів, принципів, форм, методів, адміністративно-правових режимів та гарантій забезпечення прав людини. Такий підхід дозволяє перейти від дослідження окремих правових проблем до формування цілісної доктринальної концепції адміністративно-правового забезпечення використання систем ШІ в Україні.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Тема дисертаційного дослідження узгоджується з положеннями: 1) п. 4 розділу 1 та 47 розділу 3 Стратегії національної безпеки України (Указ Президента України від 14.09.2020 р. № 392/2020); 2) п.п. 4 та 5 Стратегії кібербезпеки України (Указ Президента України від 26.08.2021 р. № 447/2021); 3) п. 1.2 розділу ІІ Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 27 роки (Указ Президента України від 11.05.2023 р. № 273/2023); 4) п. 16 Плану заходів на 2025 рік реалізації Стратегії кібербезпеки України (Розпорядження КМУ від 07.03.2025 р. № 204-р); 5) п.п. 3, 7, 11, 13 Тематики наукових досліджень та науково-технічних (експериментальних) розробок на 2025–2029 роки (наказ МВС від 21.05.2024 р. № 326); 6) темою науково-дослідних робіт Одеського державного університету внутрішніх справ «Пріоритетні напрямки розвитку реформування правоохоронних органів в умовах розгортання демократичних процесів у державі» (номер державної реєстрації 0123U103538), Тем кафедри адміністративного права та адміністративного процесу ОДУВС «Забезпечення адміністративно-правовими засобами прав і свобод людини і

громадянина в Україні» (реєстраційний номер 0125U001209), кафедри кримінального аналізу та інформаційних технологій ОДУВС «Інформаційні технології: сучасний стан, особливості в умовах війни та післявоєнний період» (реєстраційний номер 0123U103748).

Мета і завдання дослідження. *Метою дослідження* є формування теоретико-методологічних та правових засад використання штучного інтелекту в Україні, а також обґрунтування напрямів удосконалення національного законодавства відповідно до європейських стандартів правового регулювання штучного інтелекту.

Для досягнення зазначеної мети поставлено такі *завдання:*

- дослідити ґенезу інформаційно-правового регулювання систем штучного інтелекту та його співвідношення з Інтернетом речей;
- розкрити аксіологічні засади використання систем штучного інтелекту та визначити систему цінностей, що підлягають охороні в процесі його створення, впровадження та використання;
- проаналізувати соціальні очікування, ризики та суспільні перестороги щодо використання штучного інтелекту як емпіричну основу формування ризик-орієнтованої моделі правового регулювання;
- систематизувати міжнародно-правові стандарти безпечного, відповідального та людиноцентричного використання систем штучного інтелекту та визначити механізми їх імплементації в національну правову систему;
- розкрити особливості правового статусу суб'єктів створення, впровадження та використання систем штучного інтелекту;
- провести комплексний аналіз стану правового регулювання використання систем штучного інтелекту в Україні;
- встановити соціально-правові передумови обмеження використання систем штучного інтелекту в окремих сферах суспільних відносин;
- визначити правові межі використання систем штучного інтелекту в автономних системах озброєння;
- охарактеризувати особливості правового регулювання та обмеження використання систем штучного інтелекту у сфері охорони здоров’я;
- розкрити особливості правового регулювання використання штучного інтелекту у правоохоронній діяльності та діяльності спеціальних служб;
- визначити межі допустимого використання систем штучного інтелекту у сфері правосуддя та гарантії забезпечення людського контролю під час ухвалення юридично значущих рішень;
- з’ясувати особливості правового регулювання використання систем штучного інтелекту в освіті та науковій діяльності;
- обґрунтувати концептуальні засади ризик-орієнтованої правової політики та адміністративних процедур у сфері використання штучного інтелекту в Україні;
- розробити сучасну інституційну модель публічного адміністрування використання систем штучного інтелекту в Україні в умовах європейської

інтеграції та визначити напрями вдосконалення її адміністративно-правового забезпечення;

- сформулювати комплекс пропозицій щодо вдосконалення законодавства України та механізмів публічного адміністрування у сфері використання систем штучного інтелекту.

Об'єкт та предмет дослідження. *Об'єктом* дослідження *є* суспільні відносини, що виникають у процесі розроблення, впровадження та використання систем штучного інтелекту в Україні, а також у зв'язку з необхідністю мінімізації їхнього деструктивного впливу на права і свободи людини, національну безпеку та демократичні інститути в умовах цифрової трансформації соціуму

Предмет дослідження – теоретико-методологічні та правові засади використання штучного інтелекту в Україні

Методологічна основа дослідження. Методологічну основу дослідження становить комплекс загальнонаукових та спеціально-юридичних методів, системне застосування яких зумовлене специфікою правового регулювання використання штучного інтелекту, міждисциплінарною природою алгоритмічних систем і потребою модернізації вітчизняного законодавства.

Застосування *діалектичного методу* дозволило розкрити суперечливі тенденції інтеграції штучного інтелекту – посилення його технологічного потенціалу за одночасного зростання ризиків для прав людини й національної безпеки, а також простежити еволюцію правової політики від реактивного регулювання до проактивних ризик-орієнтованих моделей (розділи 1 – 4).

За допомогою *системного методу* досліджено внутрішні та зовнішні зв'язки між фундаментальними засадами конституційного, адміністративного та інформаційного права України й нормами спеціального законодавства, що регулює стратегічні сфери суспільних відносин, а також визначено місце секторальних обмежень використання алгоритмічних систем у загальній структурі публічно-правового регулювання (розділи 2 – 4).

Структурно-функціональний та *аксіологічний методи* застосовано для правової оцінки ціннісних засад обмеження використання штучного інтелекту крізь призму імперативів людської гідності, свободи, справедливості, недискримінації та пропорційності. Це дозволило обґрунтувати ризик-орієнтовану модель як легітимний та ефективний превентивний інструмент забезпечення балансу інтересів особи, суспільства й демократичної держави (розділи 1 – 4).

Застосування *когнітивного методу* дозволило дослідити специфіку сприйняття автономності алгоритмічних систем у сучасній правовій свідомості та здійснити концептуальне переосмислення юридичних категорій у сфері цифровізації (розділи 1 – 4).

Завдяки *емпірико-соціологічним методам* (анкетуванню, аналізу результатів авторських опитувань та узагальненню емпіричних даних інших дослідників) з'ясовано реальний стан суспільних очікувань і занепокоєнь щодо інтеграції штучного інтелекту в Україні. Отримані результати дозволили емпірично обґрунтувати вектори та межі нормативних обмежень і правових

гарантій на національному рівні (підрозділи 1.3, 3.1).

Використання *прогностичного методу* уможливило визначення довгострокових векторів розвитку цифрового простору в Україні та обґрунтування орієнтирів проактивної правової політики держави, спрямованої на випередження потенційних технологічних загроз (розділи 2 – 4).

Історико-правовий метод дав змогу простежити ґенезу науково-доктринальних уявлень про штучний інтелект та еволюцію підходів до юридичного визначення його правової природи на різних етапах технологічного розвитку. Це дозволило виявити закономірності переходу від загальних декларативних принципів до сучасних комплексних моделей правового обмеження використання алгоритмічних систем (розділ 1 – 2).

Порівняльно-правовий метод використано для зіставлення вітчизняних підходів із правом Європейського Союзу (насамперед Регламентом ЄС про штучний інтелект), стандартами Ради Європи та правовими моделями окремих іноземних держав (США, Японії, Великої Британії) щодо встановлення заборонених і високоризикових практик використання ШІ (розділи 2 – 4).

Формально-юридичний метод та *метод правового моделювання* застосовано для критичного аналізу чинних і проєктних нормативно-правових актів, з'ясування доктринального змісту юридичних дефініцій, виявлення системних прогалин і колізій, а також побудови авторської секторальної моделі обмежень використання штучного інтелекту та формулювання концептуальних пропозицій щодо вдосконалення правового регулювання (розділи 1 – 4).

Емпіричну базу дисертаційного дослідження становлять матеріали офіційних звітів, аналітичних доповідей, рекомендацій та експертних висновків міжнародних і європейських інституцій, практику Європейського суду з прав людини, документи Європейської комісії, Європейської ради з питань штучного інтелекту, національних регуляторних органів держав-членів Європейського Союзу, рішення судів, результати соціологічних, статистичних та аналітичних досліджень, присвячених суспільному сприйняттю, ризикам та особливостям використання технологій штучного інтелекту в різних сферах суспільних відносин, а також результати проведеного автором опитування 1092 респондентів з питань використання ШІ в Україні.

Наукова новизна отриманих результатів. Наукова новизна дисертаційного дослідження полягає в тому, що воно є першою в Україні комплексною теоретико-прикладною розвідкою, у якій на основі аксіологічних імперативів людиноцентризму та стандартів Європейського Союзу сформовано теоретико-методологічні та правові засади використання штучного інтелекту й визначено стратегічні орієнтири проактивної правової політики держави в умовах цифровізації суспільних відносин.

Найбільш вагомі результати дослідження, що визначають його наукову новизну та винесені на захист, полягають у такому:

уперше:

- сформульовано авторську дефініцію штучного інтелекту як правової категорії, відповідно до якої його визначено як високотехнологічну автономну інтелектуальну систему машинного походження, що характеризується

внутрішньою здатністю до динамічної адаптації (самонавчання на основі великих масивів даних) і функціональною спроможністю безпосередньо або опосередковано формувати, оптимізувати чи реалізовувати алгоритмічні рішення (прогнози, рекомендації), які мають юридично значущий характер та можуть створювати потенційні ризики для фундаментальних прав і свобод людини, національної безпеки, демократичного врядування та публічного порядку;

- запропоновано та обґрунтовано концептуальні основи адміністративно-правового механізму використання систем ШІ, який визначено як багаторівневу динамічну систему взаємопов'язаних принципів, суб'єктів, правових режимів та засобів контролю; визначено нормативну архітектуру цього механізму, що реалізується через розроблену комплексну трирівневу модель (горизонтальний рамковий Закон України «Про безпечне та відповідальне використання систем штучного інтелекту», системні зміни до базового процесуального й інформаційного законодавства та підзаконні акти Кабінету Міністрів України);
- визначено адміністративно-правове зонування (межі) допустимості використання систем ШІ, відповідно до якого правомірність застосування алгоритмічних систем визначається не галузевою сферою їх функціонування, а динамічним співвідношенням ступеня автономності технології, рівня ризику, інтенсивності втручання у права людини та спроможності здійснення ефективного людського контролю;
- розроблено авторський аксіологічний ризик-орієнтований тест адміністративно-правової оцінки допустимості використання систем штучного інтелекту, який, на відміну від ринково-функціональної моделі класифікації AI Act, ґрунтується на конституційній ієрархії правових благ та передбачає послідовне оцінювання потенційного впливу систем ШІ на: 1) життя і здоров'я людини; 2) національну безпеку та стійкість держави; 3) фундаментальні права, свободи та законні інтереси особи; 4) демократичне врядування, верховенство права й інституційну спроможність публічної влади;
- обґрунтовано новий правовий принцип – принцип пропорційності адміністративно-правового впливу при використанні ШІ, відповідно до якого інтенсивність регуляторного тиску, державного контролю та імперативність адміністративних процедур перебувають у прямій залежності від ступеня потенційної загрози, яку конкретна система ШІ створює для об'єктів адміністративно-правової охорони;
- розроблено засади адміністративної процедури використання високоризикових систем ШІ, яка інтегрує в єдиний послідовний адміністративний процес інвентаризацію, оцінювання ризиків, оцінку відповідності, оцінювання впливу на основоположні права людини (HRIA/FRIA), державну реєстрацію, алгоритмічний аудит, змістовний людський контроль, післяринковий моніторинг та реагування на інциденти;
- запропоновано гібридну мережеву інституційну модель публічного адміністрування у сфері ШІ, яка визначає функціональну систему та правила взаємодії суб'єктів формування державної політики (Кабінет Міністрів України,

Мінцифри), незалежного нагляду й контролю (Національний компетентний орган, секторальні регулятори), парламентського правозахисного контролю (Уповноважений ВРУ з прав людини) та судового захисту;

- запропоновано систему адміністративно-правових інструментів супроводу життєвого циклу ШІ, до складу якої включено паспорт ризику системи ШІ, інтегроване адміністративне досьє, Державний реєстр високоризикових систем, алгоритмічний аудит та модель «відтворюваного алгоритмічного сліду» в адміністративному провадженні;

удосконалено:

- класифікацію етапів та моделей міжнародно-правового реагування на технологічні виклики, яку побудовано з урахуванням еволюції регуляторних моделей від етичного саморегулювання (soft law) до юридично обов'язкового ризик-орієнтованого регулювання (hard law) систем штучного інтелекту, що дало змогу визначити закономірності трансформації міжнародних стандартів у національний правовий механізм;
- наукові підходи до формування понятійно-категоріального апарату дослідження шляхом уточнення змісту та юридичного наповнення категорій «штучний інтелект як об’єкт публічного адміністрування», «механізм адміністративно-правового регулювання використання ШІ», «адміністративно-правовий режим системи штучного інтелекту», «високоризикова система ШІ» та «адміністративно-правовий ризик»;
- класифікацію систем штучного інтелекту в контексті правового регулювання шляхом її доповнення кумулятивними юридично значущими критеріями: рівнем автономності, здатністю до адаптивності, класом ризику, процесуальним контекстом сфери застосування та моделлю необхідного людського контролю;
- функціонально-правовий підхід до оцінки людського контролю за використанням автономних систем озброєння та військових технологій ШІ, відповідно до якого визначальним критерієм визначено не технічну архітектуру взаємодії людини і алгоритму (human-in/on/out-of-the-loop), а реальну здатність військової посадової особи здійснювати змістовний юридично значущий контроль над прийняттям рішення про застосування сили та нести персональну відповідальність за його наслідки;
- теоретичні підходи до визначення адміністративно-правового статусу суб'єктів створення та експлуатації систем ШІ на основі їх функціонального розмежування залежно від конкретної ролі у життєвому циклі технології та рівня їхньої спроможності контролювати алгоритмічні й правові ризики (розробників, постачальників, розгортувачів та органів нагляду);
- розуміння системи правових засобів регулювання використання систем ШІ шляхом їх групування за функціональним призначенням на регулятивні, превентивні, контрольно-наглядові, інформаційні, процедурні та гарантійні інструменти;
- наукові бачення щодо реалізації ризикоорієнтованої державної правової політики у сфері ШІ шляхом адаптації положень *AI Act* та Рамкової

конвенції Ради Європи до правової системи України з урахуванням викликів відновлення держави та режиму воєнного стану;

дістало подальшого розвитку:

- концептуальний дуалізм аксіолого-правового виміру використання систем ШІ, який полягає у доктринальному співіснуванні гуманістичної та трансгуманістичної моделей технологічного розвитку, що дозволило довести визначальну роль права у забезпеченні пріоритету прав людини, людської автономії та суспільного контролю над використанням автономних алгоритмічних систем;
- теоретико-методологічна доктрина адміністративно-правового регулювання систем ШІ, яка базується на інтеграції людиноцентричної, ризик-орієнтованої, сервісної та безпекової парадигм публічного адміністрування і визначає систему принципів, режимів та інструментів забезпечення правомірного функціонування цифрових технологій;
- доктринальні положення щодо людиноцентричного адміністративно-правового регулювання використання систем ШІ як фундаментальної основи забезпечення балансу між прискореним технологічним розвитком, загальносуспільними інтересами та превентивним захистом прав особи;
- теоретичні засади адміністративно-правового забезпечення алгоритмічної прозорості, підзвітності, пояснюваності та алгоритмічної справедливості як базових юридичних гарантій захисту прав громадян від упередженості чи помилок систем штучного інтелекту;
- диференційована адміністративно-правова модель допустимої автономії медичного штучного інтелекту, відповідно до якої встановлено правові режими та межі використання систем ШІ залежно від етапу надання медичної допомоги із обов'язковим збереженням остаточного клінічного розсуду за лікарем-людиною;
- концепція правової недопустимості алгоритмічної деформації дискреційних повноважень правоохоронних і судових органів, відповідно до якої впровадження систем ШІ не може призводити до заміщення індивідуального суддівського розсуду чи дискреційної юрисдикції органів правопорядку автоматизованими алгоритмічними висновками, а вимагає обов'язкового збереження персональної відповідальності суб’єкта владних повноважень;
- наукові підходи до визначення меж допустимого використання систем ШІ в освітньому та науковому просторі, що передбачають чітку диференціацію правомірного інформаційно-технічного супроводу від недопустимого заміщення системами ШІ самостійної когнітивної діяльності й академічної свободи.

Практичне значення отриманих результатів полягає в тому, що сформульовані в роботі висновки, рекомендації та пропозиції можуть бути безпосередньо використані:

– у правотворчій діяльності – при підготовці змін до законодавства України, розробленні спеціальних нормативно-правових актів у сфері використання ШІ, а також при формуванні проактивних секторальних напрямів

державної правової політики (лист народної депутатки, голови підкомітету з питань вищої освіти Комітету ВРУ з питань освіти, науки та інновацій, д.ю.н., професора Юлії Гришиної від 22.04.2026; при розробленні процедур, стандартів і внутрішніх регламентів використання систем ШІ, а також при впровадженні процедур оцінювання впливу на фундаментальні права людини (FRIA) (довідка про провадження результатів дослідження до Association «METAVERSE-UA», підписана Phd, старшим офіційним членом міжнародної Робочої групи з нагляду за етикою штучного інтелекту, що входить до складу Комітету зі стандартів штучного інтелекту (C/AISC) Асоціації стандартів Інституту інженерів з електротехніки та електроніки (IEEE SA) О. Костенком № 140720266-07-14 від 14.07.2026);

– у діяльності судових та правоохоронних органів – для запобігання забороненим практикам застосування ШІ у сфері правопорядку та здійснення правосуддя, розподілу відповідальності між суб'єктами їх розроблення, впровадження і використання, а також оцінки доказів, оброблених за допомогою таких систем;

– в освітньому процесі – при викладанні навчальних дисциплін «Кримінальний аналіз», «Пошук інформації з відкритих джерел (OSINT) працівниками кримінальної поліції», «Протидія кіберзлочинності» для здобувачів першого (бакалаврського) рівня вищої освіти за спеціальністю «Правоохоронна діяльність», «Інформаційна та кібернетична безпека» для здобувачів другого (магістерського) рівня вищої освіти за спеціальністю «Системний аналіз», розроблення освітніх програм, навчально-методичного забезпечення, а також у науково-дослідній роботі здобувачів вищої освіти (акт впровадження в освітній процес ОДУВС від 15.07.2026 б/н);

– у науковій діяльності – при виконанні НДР «Пріоритетні напрями реформування правоохоронних органів в умовах розвитку демократичних процесів у державі» (реєстраційний номер 0123U103538) та теми кафедри кримінального аналізу та інформаційних технологій ОДУВС «Інформаційні технології: сучасний стан, особливості в умовах війни та післявоєнний період» (реєстраційний номер 0123U103748) (акт впровадження у наукову діяльність ОДУВС від 15.07.2026 б/н)

Апробація результатів дослідження. Висновки і положення дисертаційного дослідження обговорювалися на кафедрі адміністративного права та процесу Одеського державного університету внутрішніх справ, а також міжкафедральному семінарі. Основні положення дисертаційного дослідження оприлюднені на міжнародних та всеукраїнських конференціях, засіданнях круглих столів, у тому числі: «Наукові читання, присвячені пам'яті професора Т.А. Денисової» (м. Запоріжжя, 10 березня 2022 р.); «Людина має право: соціально-гуманітарний дискурс у контексті реформаційних процесів в Україні» (м. Одеса, 17 листопада 2022 р.); «Вдосконалення правового регулювання прав та основних свобод людини і громадянина» (м. Івано-Франківськ, 5-6 травня 2023 р.); «Створювальне знання: освіта для майбутнього» (м. Одеса, 9 червня 2023 р.); «Сучасна парадигма публічного управління» (м. Львів, 30 листопада – 2 грудня 2023 р.); «Штучний інтелект у

правовій практиці: межі та можливості» (м. Львів, 15 березня 2024 р.); «Проблеми інформаційного забезпечення та розвитку парламентського контролю в контексті Європейської та Євроатлантичної інтеграції України» (м. Київ, 25 квітня 2024 р.); «Україна в умовах соціальної та цифрової трансформації: шляхи до сталого розвитку та повоєнної відбудови» (м. Київ, 22 листопада 2024 р.); «Трансформаційні процеси правотворчої діяльності та парламентського контролю» (м. Київ, 30 жовтня 2025 р.); «Україна в умовах соціальної та цифрової трансформації: теоретичні моделі правового регулювання штучного інтелекту» (м. Київ, 5 листопада 2025 р.).

Публікації. Результати наукового дослідження висвітлено в 30 публікаціях, серед них: 1 розділ в колективній монографії; 13 статей у наукових виданнях, включених до Переліку наукових фахових видань України; 4 – у виданнях, що індексовані в міжнародних наукометричних базах даних Scopus та Web of Science; 2 – у наукових періодичних виданнях інших держав із напряму, з якого підготовано дисертацію; 10 – тези доповідей на наукових, науково-практичних конференціях, семінарах та засіданнях круглих столів.

Особистий внесок здобувача. Висновки та пропозиції, викладені у дисертації становлять особистий здобуток автора.

У статті «Information security and information hygiene on internet media» (авторський внесок 60 %) з А. Варинською, М. Костицьким, Н. Кушаковою-Костицькою автором проаналізовано поняття інформаційної безпеки та правові механізми протидії фейковій інформації. У статті з «Use of the “electronic court” service as a means of citizens' access to the judiciary» (авторський внесок 50 %) з Н. Шелевер, М. Янковим, В. Пилип, О. Анталовці здобувачем охарактеризовано основні правові ризики використання штучного інтелекту та цифрових технологій у сфері правосуддя й обґрунтовано необхідність забезпечення балансу між цифровізацією судочинства, захистом прав людини та принципом верховенства права. У статті «The potential and prospects of artificial intelligence use in strategic planning: issues of security and defense» (авторський внесок 45 %) з О. Руденко, І. Рафальським, О. Єрмак, Ю. Конопля дисертантом обґрунтовано необхідність людиноорієнтованого підходу до розроблення та застосування штучного інтелекту в оборонній сфері з урахуванням вимог прозорості, підзвітності та мінімізації правових ризиків. У статті «Digitization of local self-government based on the use of artificial intelligence in the context of sustainable development» (авторський внесок 45 %) з О. Руденко, О. Заїка, І. Кульчій, А. Мирошниченко автором розглянуто можливості використання штучного інтелекту для аналізу даних та підвищення ефективності правоохоронної діяльності за умови забезпечення належного захисту прав людини. У статті «Artificial intelligence in education: tool, object, «subject» of learning» (авторський внесок 80 %) з І. Донніковою та Н. Савіновою дисертантом розкрито особливості використання штучного інтелекту у сфері освіти, визначено потенційні ризики його застосування та окреслено механізми правового регулювання. У статті «Electronic means of ensuring fair justice: contemporary and development prospects» (авторський внесок 50 %) з Н. Шелевер, М. Бурдоносовою, О. Рогач, В. Пилип проаналізовано концепцію

цифровізації судочинства в сучасних умовах та виокремлено основні групи ризиків використання штучного інтелекту у забезпеченні справедливого правосуддя. У дисертації ідеї та матеріали кандидатської дисертації не використовувалися.

Структура та обсяг дисертації. Структура роботи зумовлена метою та завданнями дослідження і складається зі вступу, чотирьох розділів, що включають 14 підрозділів, висновків до розділів, загальних висновків, списку використаних джерел і додатків. Загальний обсяг дисертації становить 562 сторінки. Із них основний текст займає 403 сторінки, список використаних джерел (531 найменування) – 64 сторінки, додатки – 73 сторінки.

ОСНОВНИЙ ЗМІСТ РОБОТИ

Вступна частина містить обґрунтування актуальності обраної тематики, демонструє зв'язок дослідження з відповідними науковими програмами, планами та темами. У вступі сформульовано мету та завдання роботи, визначено об'єкт і предмет дослідження, описано застосовані методи дослідження. Розкрито наукову новизну отриманих результатів та їхнє практичне застосування, подано відомості про апробацію результатів дослідження, а також про висвітлення ключових положень і висновків дисертаційного дослідження у наукових публікаціях. Надано характеристику структури дисертаційної роботи.

У розділі 1 «Теоретико-методологічні засади інформаційно-правового та адміністративно-правового регулювання штучного інтелекту» здійснено системний аналіз генезису та еволюції доктринальних і регуляторних підходів до юридичного осмислення ШІ. Обґрунтовано трансформацію предмета інформаційного права від статичного регулювання обігу інформації як самостійного феномену (наприкінці XX ст.) до комплексного врегулювання суспільних відносин, пов'язаних із процесами її автоматизованого створення, інтерпретації та генерації високоавтономними системами.

У *підрозділі 1.1 «Ґенеза інформаційно-правового регулювання штучного інтелекту та його співвідношення з Інтернетом речей»* досліджено еволюцію поняття «інформація» у вітчизняному законодавчому дискурсі та типізовано три ключові доктринальні вектори осмислення ШІ: функціональний (Л. Флориді, О. Баранов), субстанційний (Л. Солум, О. Радутний) та антропоцентричний (Ф. Паскуале, П. Рабінович). Проаналізовано світовий прагматичний досвід дефініювання ШІ (США, Південна Корея, КНР, Естонія, Німеччина) та доведено методологічну небезпеку «розмивання» поняття системи ШІ до будь-якої алгоритмізованої системи. На цій основі запропоновано авторську правову дефініцію ШІ. Здійснено чітке правове розмежування ШІ та Інтернету речей (IoT), де IoT визначено як цифрову інфраструктуру обміну даними, яка зберігає людиноорієнтовану модель і позбавлена когнітивних функцій прийняття нелінійних рішень.

У *підрозділі 1.2 «Аксіологічний вимір використання штучного інтелекту»* розкрито ціннісно-правові засади функціонування алгоритмічних моделей крізь призму концепції ціннісно-чутливого проєктування (*Value Sensitive Design* Б. Фрідман) та «етики відповідальності» Г. Йонаса. Аргументовано, що автономні системи не є аксіологічно нейтральними, оскільки здійснюють опосередковану ієрархізацію альтернативних рішень на основі закладених у них нормативних установок. Доведено необхідність підпорядкування прагматичної ефективності технологій вимогам захисту людської гідності та збереження обов'язкового людського контролю (*human-in-the-loop*). Проаналізовано аксіолого-правові виклики генеративного ШІ (на прикладі ChatGPT та законопроєкту № 15379 щодо криміналізації шахрайства із використанням ШІ) й обґрунтовано, що за умов девальвації моральних імперативів саме право має виступати ключовим механізмом встановлення меж допустимого втручання технологій у приватне життя особи.

У *підрозділі 1.3 «Соціальні очікування і перестороги щодо впровадження штучного інтелекту як емпірична основа ризикоорієнтованого правового регулювання»* презентовано емпіричні результати авторського соціолого-правового опитування (1092 респонденти), яке виявило глибоку амбівалентність суспільного сприйняття ШІ в Україні. Застосовуючи синергетичний підхід, ШІ досліджено як складну систему, що стихійно самоорганізується у споживчому секторі станом на 2026 рік (на основі даних Gradus та KMIC). З урахуванням зафіксованих суспільних побоювань щодо цифрового контролю, структурного безробіття та деградації мислення, узагальнено глобальну динаміку інцидентів ШІ (на основі даних AI Incident Database та OECD) і сформовано соціально-правову карту ризиків ШІ в Україні. Верифіковано п'ять найбільш аксіологічно чутливих сфер, які вимагають секторально диференційованого правового регулювання та обмежень (воєнна сфера, медицина, правоохоронна діяльність, правосудді, освіта і наука), що визначає подальший вектор дослідження.

У розділі 2 «Міжнародні та національні правові засади правового регулювання використання штучного інтелекту» обґрунтовано доцільність дослідження міжнародних і національних засад використання систем ШІ із застосуванням методологічного підходу, заснованого на категорії механізму правового регулювання (МПР) як цілісної системи взаємопов'язаних елементів. Проаналізовано доктринальні підходи до сутності МПР. Доведено, що розвиток технологій ШІ зумовлює необхідність розширення класичної моделі МПР шляхом включення до його структури таких елементів, як управління ризиками, оцінка відповідності, алгоритмічна прозорість, незалежний аудит, сертифікація та державний нагляд. Визначено чотири структурні компоненти дослідження цього розділу: міжнародно-правові стандарти; суб'єктний склад правовідносин; система правових засобів та інструментів (зокрема *AI Act*); національна модель правового регулювання в Україні.

У *підрозділі 2.1 «Міжнародно-правові стандарти безпечного та відповідального використання штучного інтелекту»* розглянуто міжнародні акти ООН (Окінавська хартія, Декларація тисячоліття ООН, Женевська

декларація принципів 2003 р., Порядок денний у сфері сталого розвитку до 2030 року). Констатовано, що вказані документи тривалий час не виокремлювали ШІ як самостійний сегмент правового регулювання, розглядаючи його в межах сектору ІКТ. На рівні європейського права зафіксовано формування спеціалізованого регулювання (Етична хартія про використання ШІ в судових системах 2018 р., Рекомендація Ради Європи *CM/Rec (2020)1, Ethics Guidelines for Trustworthy AI 2019 р.*, Блетчлійська декларація 2023 р., Резолюція ГА ООН *A/RES/78/265* 2024 року). Досліджено ризик-орієнтовану модель *AI Act*, яка класифікує системи ШІ на чотири групи (неприпустимий, високий, обмежений та мінімальний ризик), встановлює процедури оцінки відповідності (*conformity assessment*), людського нагляду (*human oversight*) та оцінки впливу на фундаментальні права (*FRIA*). Визначено специфіку регулювання ШІ в США (децентралізована модель) та КНР (Національний план 2017 р., *Personal Information Protection Law 2021 р.*, проєкт Тимчасових заходів Адміністрації кіберпростору Китаю 2025 року щодо інтерактивних послуг). Звернуто увагу на інтеграцію *AI Act* із цифровою інфраструктурою ЄС (*VIS, Eurodac, EES, ETIAS, ECRIS-TCN*).

У *підрозділі 2.2 «Правовий статус суб'єктів створення, впровадження та використання штучного інтелекту»* систематизовано доктринальні підходи до правосуб'єктності, концепцію «електронної особи» та доведено її неделіктоздатність через відсутність у ШІ автономної правової волі, правосвідомості та психоемоційного компонента вини. Обґрунтовано підпорядкування систем ШІ правовому режиму джерела підвищеної небезпеки та «мислячої речі» (*res cogitans*), де загальний тягар ризиків покладається на його володільця. Запропоновано розмежування на *неавтономний ШІ* (стадія інституційного навчання під телеологічним контролем людини) та *автономний ШІ* (здатний виконувати завдання під системним наглядом людини, але без її покрокового керування). На основі *AI Act* охарактеризовано правовий статус ключових юридичних суб'єктів життєвого циклу ШІ: розробника (*Developer*), постачальника (*Provider*), оператора (*Deployers*) та користувача.

У *підрозділі 2.3 «Стан адміністративно-правового та інформаційно-правового регулювання використання штучного інтелекту в Україні»* оцінено вітчизняне нормативне середовище, що базується на Конституції України, законах «Про інформацію», «Про захист персональних даних», «Про доступ до публічної інформації», «Про адміністративну процедуру» та стратегічних документах (Концепція розвитку ШІ в Україні 2020 р., Дорожня карта та Біла книга Мінцифри, запуск експериментального *Sandbox* у 2025 р., План заходів на 2025-2026 роки). З урахуванням підписання Україною Рамкової конвенції Ради Європи про ШІ 15 травня 2025 року, автором виявлено сім ключових прогалин національного регулювання: 1) понятійна невизначеність категорії ШІ в законах загальної дії; 2) відсутність законодавчої класифікації ризиків; 3) інституційна невизначеність органу ринкового та адміністративного нагляду; 4) відсутність обов'язкової процедури оцінювання впливу системи на основоположні права до її використання публічною владою; 5) недостатність індивідуальних гарантій особи (права знати про використання ШІ, права на

пояснення та перегляд рішення людиною); 6) невизначеність і фрагментарність розподілу відповідальності в ланцюгу суб'єктів; 7) відсутність спеціально врегульованого режиму використання ШІ під час воєнного стану в правоохоронній та оборонній сферах.

Для усунення прогалин обґрунтовано трирівневу модель нормативного вдосконалення: першим рівнем визначено рамковий Закон України «Про безпечне та відповідальне використання систем штучного інтелекту»; другим – внесення узгоджених змін до чинних базових законів; третім – прийняття процедурних підзаконних актів Кабінету Міністрів України.

У розділі 3 «Обмеження використання штучного інтелекту в окремих сферах правовідносин» обґрунтовано, що збалансоване та таргетоване нормативне обмеження використання систем ШІ в окремих сферах суспільних відносин виступає більш ефективною модельною безпечного розвитку технологій, ніж надмірна превентивна зарегульованість, яка здатна стримувати прогрес ще до повноцінної інтеграції відповідних систем у суспільні процеси. Доведено, що традиційні людські когнітивні механізми у високоризикових сферах дедалі частіше доповнюються або частково замінюються алгоритмічними моделями, що якісно змінює характер супутніх ризиків та актуалізує вимоги до правового контролю, роблячи потребу у спеціальних обмежувальних механізмах прагматичною та галузевою.

У *підрозділі 3.1 «Соціальні передумови обмеження використання штучного інтелекту в окремих сферах життєдіяльності людини»* виявлено закономірність взаємозв'язку між соціальними побоюваннями та позитивними очікуваннями: суспільство остерігається саме тих властивостей систем ШІ, які забезпечують їхні переваги порівняно з людськими можливостями. Результати опитування представників ІТ-сфери засвідчили зближення позицій фахової та нефахової аудиторій щодо визначення сфер підвищеного ризику.

Для розуміння меж допустимої алгоритмізації проаналізовано класичну критику ШІ Х'юберта Дрейфуса крізь призму чотирьох фундаментальних припущень: біологічного, психологічного, епістемологічного та онтологічного. Аргументовано, що розвиток сучасних нейромережевих архітектур та генеративних моделей змушує переоцінити категоричність біологічного та психологічного припущень через ефект «чорної скриньки» та здатність свідомості адаптуватися до віртуальних середовищ. Визначено провідною позицію щодо неможливості повного заміщення людського досвіду, контекстуального розуміння та морального судження алгоритмами у сферах охорони здоров'я, правосуддя та публічного управління.

Узагальнено застереження представників трансгуманістичного напряму та експертів (Н. Бостром, І. Маск, С. Рассел, М. Тегмарк, Р. Курцвейл). Виокремлено три ключові проблеми за Н. Бостромом: проблему контролю, проблему узгодження цінностей (value alignment) та ризики конкурентних перегонів. Систематизовано підходи І. Маска щодо цивілізаційних ризиків автономних систем, загрози їх використання у протиправних цілях та структурного безробіття. Досліджено концепцію С. Рассела «ШІ як хорошого партнера» та проблему алгоритмічної упередженості (algorithmic bias). Оцінено

застереження М. Тегмарка щодо мілітаризації ШІ й використання повністю автономних систем озброєння (*LAWS*), а також прогноз Р. Курцвейла щодо настання Технологічної Сингулярності між 2029 та 2045 роками.

Виокремлено шість ключових етико-правових пересторог, які мають виступати критеріями нормативного обмеження систем ШІ: 1) приватність та захист персональних даних; 2) неупередженість та справедливість (*fairness assessment*); 3) підзвітність та алгоритмічна прозорість (*black box*); 4) автономія людини та людський контроль; 5) безпека та надійність систем (включаючи засоби аварійного блокування *emergency stop*); 6) соціально-економічна безпека та адаптація суспільства до автоматизації.

У *підрозділі 3.2 «Правове регулювання використання штучного інтелекту в автономній зброї»* констатовано, що регулювання в автономних системах озброєння (АСО) та летальних автономних системах озброєння (ЛАСО) суттєво відрізняється від цивільних сфер, оскільки *AI Act* встановлює для них імперативне виключення (ч. 3 ст. 2). Нормативно-правові обмеження застосування систем ШІ у військовій сфері зафіксовані у комплексі джерел, серед яких: міжнародне гуманітарне право (Женевські конвенції 1949 р., Додаткові протоколи 1977 р., Конвенція про конкретні види звичайної зброї 1980 р.), позиційні документи МКЧХ, матеріали Групи урядових експертів ООН (схвалені 11 Керівних принципів щодо ЛАСО) та Резолюції ГА ООН № 78/241 (2023 р.) і № 79/77 (2024 р.).

Повномасштабне російське вторгнення в Україну у 2022 році загострило питання дотримання базових принципів МГП – розрізнення та пропорційності. Систематизовано визначені науковцями категорії ризиків розробки та експорту АСО: ризик порушення норм МГП, ризик атрибуції відповідальності («вакуум/прогалина у відповідальності»), ризик порушення міжнародного права щодо застосування сили (ст. 2 та ст. 51 Статуту ООН) та ризик недостатності міжнародно-правового регулювання.

Досліджено впровадження АСО крізь призму концепцій Інтернету військових речей (*IoMT*) та Інтернету речей поля бою (*IoBT*), що розробляються в НАТО, США (програма DEVCOM ARL, мікро-БПЛА *Perdix*), Ізраїлі (*Iron Dome*), КНР, Південній Кореї та РФ. Проаналізовано три базові моделі інтеграції людського оператора в контур управління АСО та пов'язані з ними загрози: 1) людина «в контурі управління» (human-in-the-loop)*:* обмежує швидкість реакції всієї системи, зумовлює психофізіологічне перевантаження, ментальну втому оператора та колосальне психоемоційне навантаження; 2) людина «над контуром управління» (human-on-the-loop)*:* створює ілюзію контролю, яка нівелюється затримками передачі даних через РЕБ, кібератаки та надмірний масив вхідних сигналів у щільній міській забудові; 3) людина «поза контуром управління» (human-out-of-the-loop)*:* пов'язана з найвищими ризиками помилок розрізнення, виникнення accountability gap та вразливості до зовнішнього кібервтручання за відсутності механізмів віддаленого відключення.

Окрему увагу приділено феномену «упередження автоматизації», який полягає в надмірній довірі людини до рішень автоматизованої системи й ігноруванні операційних аномалій.

У *підрозділі 3.3 «Правове регулювання обмеження використання штучного інтелекту в медицині»* досліджено нормативно-етичний баланс медичного ШІ.

Проаналізовано шість фундаментальних принципів ВООЗ (захист автономії, сприяння добробуту та безпеці, прозорість, підвищення відповідальності, інклюзивність, просування гнучкого ШІ) та механізми їх правової кодифікації через обов'язкове ведення системних логів, клінічну оцінку та інститут «значущого людського нагляду».

Диференційовано межі допустимості технологій штучного інтелекту залежно від операційного контексту: 1) у *сфері діагностики:* допускається автономна робота систем у режимі *human-out-of-the-loop* на етапах первинного скринінгу, тріажу (ранжування) пацієнтів, популяційного моніторингу та збору інформації за умови захисту даних (GDPR). Проте встановлення остаточного діагнозу та деонтологічна комунікація вимагають реалізації схеми *human-in-the-loop*; 2) у сфері терапії (планування лікування)*:* через непередбачуваність перебігу патологій та коморбідні чинники, ухвалення рішень з боку ШІ в автономному режимі повністю виключається; моделювання персоналізованої терапії допустиме виключно в межах моделі *human-in-the-loop*; 3) у *фармакології та клінічних дослідженнях:* модель *human-out-of-the-loop* є правомірною лише на етапах доклінічного моделювання та наукової розвідки (Big Data), тоді як безпосереднє втручання у лікування реальних пацієнтів та моніторинг експериментальних груп вимагають режимів *human-in-the-loop* або *human-on-the-loop*.

Окреслено трансформацію інституту інформованої згоди пацієнта в умовах використання ШІ. Визначено базові орієнтири для української правової політики: закріплення розширеної форми згоди з розкриттям ролі ШІ; утвердження людиноцентричного стандарту медичної допомоги (ШІ як засіб підтримки, а не заміни клінічного розсуду); побудова моделі розподіленої відповідальності у технологічному ланцюгу «розробник–постачальник–заклад охорони здоров'я–лікар»; запровадження особливого правового режиму захисту медичних даних в інтегрованих системах *eHealth* з акцентом на деідентифікацію.

У *підрозділі 3.4 «Правове регулювання обмеження використання штучного інтелекту в правоохоронній діяльності та діяльності спецслужб»* констатовано наявність інституційних та інфраструктурних бар'єрів в Україні, пов'язаних із фрагментарністю відомчих ресурсів та відсутністю єдиного цифрового простору. Обґрунтовано, що концепція «юстиції штучного інтелекту» у правоохоронній сфері має полягати у створенні жорсткої системи правового контролю, законності, необхідності та пропорційності, де системи ШІ виступають виключно допоміжним інструментом аналітичної підтримки.

Охарактеризовано світовий досвід впровадження систем правопорядку: аналітичної платформи *Qlik Sense* у Великій Британії, системи превенції

злочинності *Dejaview* у Південній Кореї, а також використання системи розпізнавання облич *Clearview AI* правоохоронними органами США та її результативне застосування Національною поліцією України з 2022 року для перевірки осіб на блокпостах та ідентифікації причетних до агресії.

Здійснено критичний аналіз ризиків алгоритмічної упередженості на прикладі американської системи оцінювання ризиків рецидивів *COMPAS*, яка продемонструвала уявну «об'єктивність» та расову дискримінацію. Досліджено загрози масового нагляду без згоди громадян, ризики витоку та деанонімізації персональних даних.

Висвітлено ризик-орієнтовний підхід європейського *AI Act* (ст. 5), який поділяє використання ШІ органами правопорядку на дві категорії: 1) п*рактики, які підлягають прямій забороні:* системи сублімінального маніпулювання; соціальне рейтингування (*social scoring*); біометрична категоризація за чутливими ознаками (раса, релігія, орієнтація); використання віддаленої біометричної ідентифікації в режимі «real-time» у публічних місцях (за винятком чітко визначених випадків, що потребують судового контролю); 2) в*исокоризикові системи (high-risk):* застосування яких допускається за умови побудови системи ризик-менеджменту, забезпечення репрезентативності даних, ведення технічної документації, обов'язкового автоматизованого логування журналів подій та реалізації людського нагляду за моделями *human-in-the-loop* або *human-on-the-loop*.

У *підрозділі 3.5 «Правове регулювання обмеження використання штучного інтелекту в правосудді»* обґрунтовано, що судове рішення за своєю природою є актом оцінки та внутрішнього переконання судді, через що повна автономізація судового розсуду несумісна з принципом верховенства права. Окреслено трансформацію сучасного судочинства, де ШІ еволюціонує від допоміжного інструменту документообігу та пошуку практики до систем прогнозування рішень та оцінки доказів. Стверджується, що переваги швидкості обробки великих масивів інформації найгостріше стикаються з правовими вимогами незалежності, мотивованості судових рішень, вимогою їх прийняття за внутрішнім переконанням на підставі дослідження матеріалів справ та збереження реального людського контролю.

У *підрозділі 3.6 «Правове регулювання обмеження використання штучного інтелекту в освіті та науці»* досліджено адміністративно-правові засади та межі використання технологій штучного інтелекту в освіті та науковій діяльності як сферах, що безпосередньо пов'язані з реалізацією права на освіту, академічною свободою та забезпеченням академічної доброчесності. Особливістю цих сфер є поєднання значного потенціалу цифрових технологій із високим рівнем ризику для прав людини та фундаментальних академічних цінностей. Аналіз результатів авторського соціологічного дослідження засвідчив наявність суперечливого ставлення академічної спільноти до використання систем штучного інтелекту. З одного боку, респонденти високо оцінюють можливості персоналізації навчання, адаптивного консультування, автоматизації адміністративних процесів та підтримки наукової діяльності, а з іншого – висловлюють занепокоєння щодо поширення академічної

недоброчесності, втрати навичок критичного мислення та надмірної залежності від алгоритмічних систем.

У результаті дослідження систематизовано основні ризики використання ШІ в освіті та науці. Першу групу становлять ризики академічної недоброчесності, пов'язані з використанням генеративних моделей для імітації інтелектуальної діяльності та прихованого запозичення результатів чужої праці. Другу групу ризиків становлять алгоритмічні похибки під час оцінювання результатів навчання. Третій блок ризиків пов'язаний із захистом персональних даних і кібербезпекою. Окрему групу становлять ризики для академічної свободи та професійної автономії педагогічних і науково-педагогічних працівників.

На підставі проведеного дослідження сформульовано основні напрями вдосконалення правового регулювання використання штучного інтелекту в освіті та науці: внесення змін до законодавства про освіту й академічну доброчесність; запровадження процедур перевірки доброчесності та використання генеративного штучного інтелекту; забезпечення алгоритмічної прозорості й права особи на пояснення та оскарження рішень, ухвалених із використанням алгоритмічних систем; посилення гарантій академічної свободи; удосконалення механізмів кіберзахисту та захисту персональних даних.

У розділі 4 «Формування сучасної інституційної моделі публічного адміністрування використання штучного інтелекту в Україні в умовах євроінтеграції» обґрунтовано, що побудова правової моделі використання систем ШІ в Україні не може зводитися до механічного перенесення іноземного законодавства чи фрагментарного доповнення чинних законів поодинокими згадками про алгоритмічні системи. Доведено необхідність переходу до цілісної державної правової політики, яка одночасно виконує три функції: правозахисну, безпекову та інноваційно-стимулюючу. Конституційним ядром цієї політики визначено положення ст. ст. 3, 8, 19, 32, 34 і 55 Конституції України. Зазначено, що чим істотніше алгоритмічний результат впливає на права та законні інтереси особи, тим вищими є вимоги до нормативної визначеності, обґрунтування мети, якості даних, людського контролю, документування та можливості оскарження.

У *підрозділі 4.1 «Ризик-орієнтована правова політика та адміністративні процедури обмеження використання штучного інтелекту в Україні»* аргументовано, що в умовах технологічної невизначеності ризик-орієнтований підхід виступає найбільш ефективним інструментом управління. Спираючись на наукові розробки вітчизняних науковців, адаптовано методологічні положення FATF та концепцію трирівневої моделі аналітичної діяльності для побудови теоретико-методологічної моделі використання ШІ. Виокремлено чотири базові методологічні положення ризик-орієнтованої правової політики ШІ: 1) пріоритет попередньої оцінки ризиків перед вибором адміністративно-правових засобів реагування; 2) принцип пропорційності державного впливу рівню ризику; 3) динамічний (безперервний) характер оцінки ризиків; 4) циклічність регулювання.

Узагальнено європейські правові орієнтири і констатовано, що адаптація європейського підходу в Україні не повинна бути механічним копіюванням, оскільки національна модель має додатково враховувати правовий режим воєнного стану, потреби оборони і розвідки, обмежені фінансові ресурси та стан державних реєстрів.

З урахуванням концептуальних підходів О. А. Баранова обґрунтовано перехід від реагування на наслідки до попереднього виявлення небезпек протягом усього життєвого циклу технології.

Визначено п'ять груп критеріїв для оцінювання ризику: об'єкт впливу, інтенсивність впливу, технологічні властивості системи, процесуальний контекст та характеристики суб'єктів (враховуючи вразливість дітей, пацієнтів, затриманих, військовослужбовців тощо). Запропоновано закріпити на законодавчому рівні п'ять категорій систем та моделей: 1) заборонені практики неприйнятного ризику (маніпулятивне застосування ШІ, експлуатація вразливостей, соціальне оцінювання громадян владою, невибіркове збирання біометричних зображень, категоризація за чутливими ознаками, оцінка ризику правопорушень виключно на основі профілю особи); 2) високоризикові системи (компоненти безпеки продукції або системи у сферах біометрії, критичної інфраструктури, освіти, працевлаштування, соцзахисту, охорони здоров'я, правоохоронної діяльності, міграції, правосуддя, виборів та оборони); 3) системи обмеженого ризику (із застосуванням спеціальних вимог прозорісті та маркування контенту); 4) системи мінімального ризику; 5) моделі ШІ загального призначення (включаючи моделі із системним ризиком).

Запропоновано аксіологічний ризик-орієнтований тест адміністративно-правової оцінки, який, на відміну від функціонального підходу AI Act, базується на ієрархії правових благ і включає чотири послідовні рівні: 1) оцінка ризику заподіяння шкоди життю та здоров'ю людини; 2) встановлення потенційного впливу на національну безпеку та стійкість держави; 3) оцінка впливу на основоположні права, свободи та законні інтереси людини у сфері публічного адміністрування та цифрових послуг; 4) оцінка впливу на функціонування демократичного врядування, забезпечення принципу верховенства права та інституційну спроможність держави (на основі концепції AI Governance).

У *підрозділі 4.2 «Напрями розвитку інституційної моделі публічного адміністрування та вдосконалення законодавства України у сфері використання штучного інтелекту в умовах євроінтеграції»* доведено, що розв'язання проблеми розпорошеності повноважень між державними суб'єктами вимагає нормативно узгодженого розподілу функцій. Визначено зміст інституційної моделі публічного адміністрування ШІ та структуровано її функціонал за п'ятьма напрямами: нормотворчий, координаційний, сервісно-інформаційний, контрольно-наглядовий та юрисдикційно-захисний.

У результаті аналізу трьох варіантів розбудови інституцій (створення окремого ЦОВВ зі спеціальним статусом; покладення всіх функцій на Мінцифри; побудова мережевої моделі), обґрунтовано оптимальність мережевої (гібридної) інституційної моделі, яка усуває інституційний конфлікт

цілей між підтримкою інновацій та захистом прав людини. Модель передбачає чіткий розподіл ролей за допомогою законодавчо закріпленої функціональної матриці компетенції: Кабінет Міністрів України – загальне спрямування політики, затвердження урядових порядків; Міністерство цифрової трансформації України – центральний координатор, розробник стратегічної політики, типових методик та адміністратор відкритої інфраструктури; Національний компетентний орган нагляду – ЦОВВ зі спеціальним статусом, функціонально незалежний під час проведення планових і позапланових перевірок, розгляду інцидентів та застосування фінансових санкцій чи приписів; секторальні регулятори здійснюють змістовну оцінку специфічних ризиків в окремих сферах; Уповноважений Верховної Ради України з прав людини здійснює правозахисний та інформаційно-правовий контроль; органи стандартизації, акредитації та оцінки відповідності забезпечують технічну складову, суди гарантують остаточний контроль законності.

Розроблено багаторівневий узгоджений пакет нормативно-правових актів, який об'єднує: рамковий Закон України «Про безпечне та відповідальне використання систем штучного інтелекту», проєкт Закону України про внесення змін до деяких законодавчих актів України, що адаптує суміжні режими; процедурні постанови Кабінету Міністрів України.

Систематизовано дванадцять взаємопов'язаних адміністративних процедур, що охоплюють увесь життєвий цикл системи ШІ: інвентаризація та попередня класифікація; перевірка законної мети та менш обмежувальних альтернатив; оцінювання впливу високоризикової системи на основоположні права (HRIA/FRIA); управління даними та їх мінімізація; оцінка відповідності технічним вимогам; публічна закупівля системи ШІ (з оцінкою вартості всього життєвого циклу); державна реєстрація (із запровадженням паспорта ризику та єдиного адміністративного досьє системи); забезпечення змістовного людського контролю; постійний правовий та технічний моніторинг; повідомлення про серйозні інциденти протягом 72 годин; застосування пропорційних коригувальних заходів; забезпечення індивідуальних прав.

Доведено, що особливості воєнного стану не повинні означати повного вилучення сфер оборони, розвідки та безпеки з правового поля; для них мають застосовуватися прискорені або спеціальні закриті процедури із обов'язковим збереженням законності, пропорційності, документування, змістовного людського контролю та персональної відповідальності.

Визначено ключові ризики впровадження моделі (інституційне дублювання, дефіцит міждисциплінарних фахівців, формалізація оцінок, регуляторне захоплення) та інструменти їх мінімізації. Запропоновано здійснювати розгортання інституційної моделі поетапно (підготовчий, законодавчий, інституційний та повний операційний етапи) з оцінкою її результативності за системою якісних та кількісних індикаторів у межах щорічного циклу правового моніторингу.

ВИСНОВКИ

За результатами дослідження вирішено наукову проблему щодо розробки теоретико-методологічних та правових засад використання штучного інтелекту в Україні:

1. Обґрунтовано закономірну трансформацію предмета інформаційного права від регулювання відносин щодо обігу інформації до регулювання суспільних відносин, пов'язаних із функціонуванням автономних інтелектуальних систем, здатних формувати юридично значущі рішення.

Необхідним є концептуальне розмежування у межах інформаційно-правового дискурсу загального доктринального поняття «штучний інтелект», що позначає науково-технологічний напрям та систему когнітивних методів обробки інформації, від нормативно-дефінітивної категорії «система штучного інтелекту». ШІ виступає лише концептуальним фундаментом, тоді як саме система ШІ як матеріалізований програмно-апаратний комплекс є безпосереднім об'єктом публічного адміністрування, державного контролю та правового обмеження, оскільки її функціонування здатне генерувати реальні ризики для прав особи.

ШІ як правова категорія являє собою високотехнологічну автономну інтелектуальну систему машинного походження, що характеризується внутрішньою здатністю до динамічної адаптації (самонавчання на основі великих масивів даних) і функціональною спроможністю безпосередньо або опосередковано формувати, оптимізувати чи реалізовувати алгоритмічні рішення (прогнози, рекомендації), які мають юридично значущий характер та можуть створювати потенційні ризики для фундаментальних прав і свобод людини, національної безпеки, демократичного врядування та публічного порядку.

Інтернет речей забезпечує виключно цифрову й апаратну інфраструктуру автоматизованого збирання, первинного передавання та транскордонного обміну даними між пристроями, тоді як штучний інтелект здійснює їх глибокий інтелектуальний аналіз, когнітивне моделювання та кінцеву реалізацію владних, сервісних або управлінських рішень. Це зумовлює відмінність їхньої правової природи, предмета регулювання, ризиків і доводить вимогу спрямування ризик-орієнтованої правової політики держави не на регулювання технології ШІ як абстрактного явища, а на встановлення суворих процедурних меж та обов'язків для суб'єктів життєвого циклу конкретних систем штучного інтелекту

2. Аксіолого-правовий вимір використання систем ШІ формується під впливом гуманістичної та трансгуманістичної моделей технологічного розвитку, співіснування яких визначає сучасні тенденції правового регулювання автономних інтелектуальних систем. Це обумовлює необхідність побудови адміністративно-правового механізму використання штучного інтелекту на засадах людиноцентризму, що забезпечує пріоритет прав людини, збереження людської автономії та належний суспільний контроль за прийняттям юридично значущих рішень із використанням систем штучного інтелекту.

3. Результати проведеного аналізу соціальних очікувань, ризиків і суспільних пересторог щодо використання ШІ відображають не лише рівень суспільної довіри до автономних алгоритмічних систем, а й виконують функцію емпіричних індикаторів юридично значущих ризиків, пов'язаних із можливим порушенням фундаментальних прав людини, втратою людського контролю над алгоритмічним прийняттям рішень, виникненням алгоритмічної упередженості, розмиванням юридичної відповідальності, загрозами академічній доброчесності, цифровій приватності та суспільній довірі до державних інституцій. Вони повинні враховуватися під час визначення меж адміністративно-правового регулювання.

Ризик-орієнтована модель правового регулювання систем ШІ має формуватися на основі поєднання правового аналізу із результатами емпіричних соціологічних досліджень, що дає змогу визначати найбільш соціально чутливі сфери застосування ШІ, забезпечувати диференціацію правових режимів залежно від рівня потенційних ризиків та своєчасно адаптувати державну правову політику до суспільних очікувань щодо безпечного використання інтелектуальних систем.

4. Виявлено закономірність еволюції міжнародно-правового регулювання систем ШІ від інструментів «м'якого права» (soft law), заснованих на етичних принципах і саморегулюванні, до формування юридично обов'язкової (hard law) ризик-орієнтованої моделі. Кульмінацією цього процесу визначено AI Act, який закріпив екстериторіальний підхід, диференціацію обов'язків суб'єктів за рівнями ризику та систему державного контролю. Сформульовано методологічні засади імплементації цих стандартів у правову систему України з метою інтеграції до єдиного європейського цифрового ринку та забезпечення безпекових вимог в умовах воєнного стану.

5. Сучасна модель адміністративно-правового регулювання використання систем ШІ ґрунтується на функціональному розмежуванні компетенції суб'єктів відповідно до їх ролі у життєвому циклі системи ШІ та рівня впливу на ризики її функціонування. Адміністративно-правовий статус таких суб'єктів визначається не лише сукупністю їх прав і обов'язків, а й покладеними на них функціями щодо створення, постачання, розгортання, використання, оцінювання відповідності, здійснення державного нагляду та управління ризиками. В умовах сучасної людиноцентричної моделі правового регулювання ШІ не набуває самостійної правосуб'єктності, а юридична відповідальність за його функціонування покладається на людину-суб’єкта та інституційних суб'єктів, які здійснюють проєктування, впровадження, експлуатацію та контроль відповідних систем.

Нормативна модель, закріплена в AI Act, трансформувала підхід до визначення адміністративно-правового статусу учасників цих правовідносин, замінивши традиційне визначення суб'єктів за їх організаційно-правовою належністю функціональною моделлю розподілу компетенції, юридичних обов'язків і відповідальності залежно від місця суб'єкта у життєвому циклі системи штучного інтелекту. Функціональна роль у життєвому циклі системи

та обсяг ризиків, на управління якими вони здатні впливати зумовлює диференціацію їх компетенції, юридичних обов'язків і відповідальності

6. Чинне законодавство України: Конституція України, Закони України «Про інформацію», «Про захист персональних даних», «Про адміністративну процедуру», «Про доступ до публічної інформації», «Про публічні електронні реєстри», інші акти інформаційного та адміністративного законодавства, а також Концепція розвитку штучного інтелекту в Україні, програмно-стратегічні документи Міністерства цифрової трансформації України формують нормативні й організаційні передумови використання систем ШІ, однак не утворюють завершеного адміністративно-правового механізму їх регулювання, оскільки не забезпечують комплексного врегулювання всіх елементів життєвого циклу ШІ, процедур оцінювання відповідності, державного нагляду, управління ризиками та спеціального розподілу юридичної відповідальності.

Імплементація міжнародних стандартів має відбуватися не через механічне копіювання норм AI Act, а шляхом побудови цілісної нормативної архітектури: рамкового закону про систем ШІ, взаємоузгоджених змін до інформаційного й адміністративного законодавства, системи підзаконних актів та спеціальних адміністративних процедур, що забезпечить сумісність із правом ЄС та адаптованість до системи публічного адміністрування України на засадах безпечного, відповідального та людиноцентричного використання систем ШІ.

7. Соціально-правові передумови обмеження використання систем ШІ зумовлені об'єктивною необхідністю забезпечення збалансованого поєднання технологічного розвитку, публічних інтересів і належного захисту прав людини в умовах зростання автономності алгоритмічних систем. Людиноцентризм є системоутворюючим доктринальним критерієм правотворення, за яким визначаються допустимі межі алгоритмізації суспільних відносин та інтенсивність регуляторного впливу залежно від рівня ризику для прав людини і публічних інтересів.

Базовим критерієм адміністративно-правового обмеження систем ШІ є характер та інтенсивність його впливу на фундаментальні права. На цій основі обґрунтовано правову диференціацію трьох моделей інтеграції людини в контур функціонування автономних систем: «людина в контурі управління» (*human-in-the-loop*), «людина над контуром управління» (*human-on-the-loop*) та «людина поза контуром управління» (*human-out-of-the-loop*), яка потребує найсуворіших обмежень або заборони застосування у сферах реалізації основоположних прав.

Такий підхід формує теоретичну основу ризик-орієнтованої моделі адміністративно-правового регулювання використання систем ШІ, за якої форма інтеграції людини у процес функціонування алгоритмічної системи визначається ступенем її автономності, рівнем потенційного ризику та юридичною значущістю наслідків ухвалюваних рішень.

8. Сучасне міжнародно-правове регулювання використання систем ШІ в автономних системах озброєння перебуває на етапі формування та ґрунтується переважно на нормах міжнародного гуманітарного права, практиці Міжнародного Комітету Червоного Хреста, документах ООН і концепції

meaningful human control, що відображає загальну тенденцію до недопущення повної автономізації застосування летальної сили.

Обґрунтовано застосування функціонально-правового підходу до визначення меж використання систем ШІ в автономних системах озброєння, де ключовим критерієм є реальна здатність людини здійснювати юридично значущий контроль над вибором цілі, прийняттям рішення про застосування летальної сили та особисто нести персональну відповідальність за наслідки. Концепцію meaningful human control визначено не як технічну характеристику архітектури, а як самостійний функціонально-правовий стандарт оцінки допустимості застосування систем ШІ та відповідності його функціонування принципам міжнародного гуманітарного права, що виключає можливість повного делегування алгоритмам права на застосування сили.

Такий підхід забезпечує перехід від формальної оцінки моделей взаємодії людини й алгоритму до змістовної правової оцінки спроможності людини залишатися суб'єктом прийняття рішень і юридичної відповідальності, що виключає можливість делегування ШІ автономного права на застосування летальної сили.

9. Адміністративно-правова допустимість автономії медичного ШІ має оцінюватися не за ступенем автоматизації процесів, а за спроможністю забезпечення ефективного людського контролю над клінічно значущими рішеннями. Диференційовано правові режими використання систем ШІ в медицині: автономні режими визначено допустимими виключно під час виконання допоміжних аналітичних, скринінгових та дослідницьких завдань. Натомість на етапах встановлення діагнозу, вибору протоколу лікування та прийняття клінічно значущих рішень обов'язковим є збереження безпосереднього людського контролю лікаря як гаранта прав пацієнта та суб'єкта юридичної відповідальності.

10. Сформульовано концепцію правової недопустимості алгоритмічної деформації дискреційних повноважень правоохоронних органів, яка виключає існування автономного алгоритмічного правозастосування, підміну індивідуального юридичного розсуду уповноваженої особи та ухвалення рішень, що породжують правові наслідки, без їх змістовної перевірки людиною.

Правомірні межі використання систем ШІ у цій сфері визначають його як допоміжний інструмент інформаційно-аналітичної підтримки, прогнозування, біометричної ідентифікації та аналізу великих масивів даних. Допустимим застосування транскордонних баз даних розпізнавання обличчя в умовах відсічі збройній агресії (для ідентифікації військовополонених, загиблих, зниклих безвісти та воєнних злочинців) є виключно за наявності чіткої правової підстави, легітимної мети та жорстких часових і просторових обмежень. Необхідним є подолання інфраструктурної фрагментарності органів правопорядку через створення єдиного інтегрованого аналітичного простору на принципах Data Science із обов'язковим логуванням дій та деідентифікацією осіб на ранніх етапах обробки.

11. У сфері правосуддя змістовний людський контроль є самостійною процесуальною гарантією реалізації права на справедливий суд, оскільки виключно суддя здатний здійснювати індивідуалізовану оцінку обставин справи на засадах справедливості й пропорційності. Використання систем ШІ є допустимим лише як допоміжного інформаційно-аналітичного інструменту для автоматизації технічних процесів, пошуку правової інформації та підготовки проєктів документів, і не може поширюватися на оцінку доказів, формування внутрішнього переконання судді та тлумачення норм права. Застосування систем із закритою логікою, автоматизоване прогнозування чи ухвалення судових рішень створюють пряму загрозу ст. 6 Конвенції про захист прав людини і основоположних свобод, через що обов'язковими умовами використання ШІ є його пояснюваність, прозорість та можливість незалежного аудиту й відхилення алгоритмічних висновків суддею.

Сучасні міжнародні стандарти, сформовані практикою ЄСПЛ, Європейською етичною хартією CEPEJ, AI Act, рекомендаціями CNIL та іншими міжнародними документами, відображають єдину концепцію, відповідно до якої системи ШІ повинні посилювати ефективність здійснення правосуддя, але не можуть підміняти суддівський розсуд, незалежність суду та процесуальні гарантії реалізації права людини на справедливий суд.

12. Особливості правового регулювання використання систем ШІ в освіті та науковій діяльності визначаються необхідністю забезпечення балансу між цифровою модернізацією освітнього процесу та збереженням людської суб'єктності як основоположної цінності академічного середовища. Правові межі використання систем ШІ у цій сфері повинні визначатися не рівнем технологічних можливостей алгоритмічних систем, а характером їхнього впливу на самостійну когнітивну діяльність здобувачів освіти, педагогічний розсуд викладача, академічну свободу та академічну доброчесність.

Допустимими межами використання систем ШІ в освіті та науці є їх застосування для інформаційного пошуку, аналітичної обробки даних, мовного й технічного редагування, візуалізації інформації, автоматизації адміністративних процесів та інших допоміжних функцій, що не заміщують інтелектуальну діяльність людини, тоді як недопустимим є використання алгоритмічних систем для імітації авторства, підміни самостійної когнітивної діяльності, заміщення педагогічного розсуду, формування наукових результатів без належного творчого осмислення, а також прийняття остаточних рішень щодо оцінювання результатів навчання, якщо вони істотно впливають на освітню чи професійну траєкторію особи.

Академічна доброчесність в умовах поширення генеративних технологій повинна забезпечуватися не шляхом загальної заборони використання систем ШІ, а через нормативне розмежування допустимих і недопустимих способів його застосування, обов'язок декларування використання генеративних систем, прозорість алгоритмічної підтримки та збереження персональної відповідальності автора за результати освітньої й наукової діяльності.

Використання високоризикових систем ШІ для оцінювання знань, формування освітніх траєкторій, прокторингу та інших рішень, здатних

впливати на реалізацію права на освіту, потребує обов'язкового людського контролю, можливості перевірки й оскарження алгоритмічних висновків, а також забезпечення недискримінаційності, захисту персональних даних, академічної свободи та інституційної автономії закладів освіти й науки.

13. Сучасна модель адміністративно-правового регулювання використання систем ШІ повинна базуватися на ризик-орієнтованій правовій політиці, за якої інтенсивність адміністративно-правового впливу, зміст адміністративних процедур, обсяг державного контролю та характер правових обмежень визначаються не видом технології чи сферою її застосування, а рівнем потенційної загрози для життя і здоров'я людини, національної безпеки, прав і свобод людини, демократичного врядування та верховенства права.

Розроблено авторський аксіологічний ризик-орієнтований тест адміністративно-правової оцінки допустимості використання систем ШІ, який, на відміну від функціональної моделі класифікації ризиків, покладеної в основу AI Act, ґрунтується на ієрархії конституційних та міжнародно визнаних правових цінностей і передбачає послідовне оцінювання потенційного впливу ШІ на життя і здоров'я людини, національну безпеку та стійкість держави, права, свободи й законні інтереси людини, а також демократичне врядування, верховенство права та інституційну спроможність держави, що забезпечує універсальний адміністративно-правовий механізм визначення допустимості використання систем штучного інтелекту незалежно від сфери їх застосування.

Визначено принцип пропорційності адміністративно-правового впливу, який повинен визначати не лише інтенсивність державного контролю, а й зміст адміністративних процедур, обсяг документації, характер людського контролю, рівень прозорості, періодичність адміністративного аудиту, післяринкового моніторингу та реагування на інциденти відповідно до ступеня ризику конкретної системи штучного інтелекту, що забезпечує адаптивність правового регулювання до розвитку цифрових технологій і виключає застосування уніфікованих регуляторних вимог до систем із різним рівнем потенційної небезпеки.

Запропоновано розглядати ризик-орієнтовану модель адміністративно-правового регулювання як безперервний цикл адміністративного управління, який охоплює попередню ідентифікацію та класифікацію ризиків, формування паспорта ризику системи штучного інтелекту, перевірку законної мети та менш обмежувальних альтернатив, оцінювання впливу на права людини (HRIA/FRIA), оцінку відповідності, управління даними, державну реєстрацію, забезпечення змістовного людського контролю, адміністративний аудит, післяринковий моніторинг, повідомлення про інциденти, застосування коригувальних заходів та забезпечення права особи на перегляд і оскарження алгоритмічно підтриманих рішень протягом усього життєвого циклу системи.

Доцільним є запровадження паспорта ризику систем ШІ як базового адміністративного документа, що забезпечує узгодженість усіх процедур оцінювання ризиків, оцінки відповідності, HRIA/FRIA, державного нагляду та взаємодії компетентних органів. Ризик-орієнтована модель повинна передбачати динамічну перекласифікацію систем ШІ після зміни їх

функціонального призначення, рівня автономності, масштабів використання, інтеграції з державними інформаційними ресурсами або виявлення нових ризиків, а також обов'язкове документування кожного адміністративного рішення щодо допуску системи до експлуатації.

Правове регулювання використання високоризикових систем ШІ має здійснюватися у межах єдиного адміністративного досьє, яке акумулює результати класифікації ризиків, HRIA/FRIA, оцінки відповідності, державної реєстрації, адміністративних аудитів, моніторингу, повідомлень про інциденти та прийнятих адміністративних актів, забезпечуючи простежуваність усього життєвого циклу системи. Запропонована модель адміністративних процедур створює цілісний механізм AI governance, який поєднує превентивний захист прав людини, принцип людиноцентризму, належне врядування, адміністративно-процедурні гарантії, підтримку інновацій та виконання євроінтеграційних зобов'язань України шляхом імплементації найкращих міжнародних стандартів без їх механічного копіювання.

14. Сучасна вітчизняна модель публічного адміністрування використання систем ШІ повинна ґрунтуватися на мережевій (гібридній) системі управління, яка забезпечує розмежування політичних, регуляторних, контрольно-наглядових, правозахисних, експертних і судових функцій та виключає концентрацію всіх повноважень у межах одного органу. Запропоновано інституційну модель публічного адміністрування використання систем ШІ, яка визначає функціональну систему суб'єктів формування державної політики, регулювання, нагляду, контролю, сертифікації, оцінки відповідності, незалежного аудиту та захисту прав людини.

Оптимальна для України модель повинна поєднувати Кабінет Міністрів України як суб'єкта формування державної політики, Міністерство цифрової трансформації України як центрального координатора розвитку та методичного забезпечення, функціонально незалежний національний компетентний орган як суб'єкта державного нагляду і застосування заходів реагування, секторальних регуляторів, Уповноваженого Верховної Ради України з прав людини, органи стандартизації, акредитації й оцінки відповідності, незалежних аудиторів, науково-консультативну раду та адміністративні суди як взаємопов'язану систему AI governance.

Доцільним є законодавче запровадження функціональної матриці компетенції, яка визначає для кожної адміністративної процедури провідний орган, суб'єктів погодження, консультативної участі, адміністративного й судового оскарження, що забезпечує усунення дублювання повноважень, компетенційних конфліктів і фрагментарності державного регулювання.

Логічним є створення єдиного електронного адміністративного досьє високоризикової системи ШІ, яке акумулює матеріали класифікації ризиків, HRIA/FRIA, оцінки відповідності, державної реєстрації, адміністративних аудитів, повідомлень про інциденти, застосованих заходів реагування, результатів перевірок та судового контролю, забезпечуючи простежуваність адміністративних процедур протягом усього життєвого циклу системи.

Контрольно-наглядова діяльність у сфері використання систем ШІ повинна здійснюватися за ризик-орієнтованою моделлю, яка передбачає проведення планових і позапланових перевірок залежно від категорії ризику, історії інцидентів, масштабів використання, суттєвих модифікацій системи та результатів попередніх аудитів, із наданням компетентному органу права доступу до технічної документації, журналів подій, тестових середовищ і можливості застосування тимчасового обмеження використання системи у разі неможливості підтвердження її безпечності та законності.

Обґрунтовано посилення ролі Уповноваженого Верховної Ради України з прав людини шляхом надання права ініціювати перевірки, отримувати матеріали HRIA/FRIA, брати участь у розгляді системних інцидентів, звертатися до суду в інтересах осіб та подавати обов'язкові до розгляду рекомендації щодо усунення алгоритмічної дискримінації і порушень інформаційних прав.

Запропоновано комплексну модель нормативного забезпечення функціонування інституційної системи, основу якої становить розроблений проєкт рамкового Закону України «Про безпечне та відповідальне використання систем штучного інтелекту», а також взаємоузгоджений пакет законодавчих змін до Законів України «Про адміністративну процедуру», «Про захист персональних даних», «Про доступ до публічної інформації», «Про публічні електронні реєстри», «Про публічні закупівлі» та інших законодавчих актів. Передбачено законодавче врегулювання алгоритмічно підтриманих адміністративних актів шляхом доповнення Закону України «Про адміністративну процедуру» статтею 69^1, яка встановлює заборону ухвалення негативного адміністративного акта виключно на підставі результату функціонування системи штучного інтелекту за наявності дискреційних повноважень, обов'язок посадової особи здійснювати самостійну оцінку фактичних обставин і пропорційності втручання, забезпечувати фіксацію алгоритмічного сліду, людський перегляд та можливість повноцінного адміністративного й судового контролю.

Необхідним є нормативне закріплення права особи на отримання інформації про використання систем ШІ, змістовного пояснення алгоритмічно підтриманого рішення, людського перегляду, заперечення автоматизованої обробки, захисту від алгоритмічної дискримінації та оскарження результатів використання систем штучного інтелекту.

Запропоновано створення державного реєстру високоризикових систем ШІ, впровадження регуляторного експериментального середовища (AI Sandbox), спеціального порядку проведення HRIA/FRIA, інтегрованої системи повідомлення про серйозні інциденти та поетапної дорожньої карти імплементації законодавства, що забезпечує функціональну еквівалентність української моделі європейським стандартам AI Act без їх механічного відтворення.

15. Сформовано цілісну концепцію вдосконалення законодавства України та механізмів публічного адміністрування у сфері використання систем ШІ, спрямовану на формування комплексної адміністративно-правової моделі його

безпечного, людиноцентричного та ризик-орієнтованого використання, а також надані пропозиції до окремих галузевих законів зі сфер правовідносин, які були проаналізовані у дослідженні.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, у яких опубліковано основні наукові результати дисертації

Монографія

1. Варинський В. Штучний інтелект в освіті: проблеми впровадження та регулювання. *Створювальна сила знання* : монографія. Книга друга / авт. кол. ; відп. ред.: І. А. Доннікова, Н. В. Кривцова. Київ : 7БЦ, 2025. С. 145–163.

Статті у наукових виданнях, включених до Переліку наукових фахових видань України

2. Варинський В. О. Сучасні напрямки соціально-правових досліджень штучного інтелекту. *Наукові перспективи*. 2022. №. 12 (30). С. 299–310. DOI: https://doi.org/10.52058/2708-7530-2022-12(30)-299-310

3. Варинський В. О. Правосуб'єктність штучного інтелекту: міф чи реальність. *Юридична Україна.* 2024. № 11. С. 60–68. DOI: 10.37749/2308-9639-2024-11(263)-6. URL: https://yur-ukraine.com/pravosubyektnist-shtuchnogo-intelektu-mif-chy-realnist-2/

4. Варинський В. О. Правосуб’єктність штучного інтелекту: критичний погляд на автономність. *Інформація і право*. 2024. № 4 (51). С. 83–94. DOI: https://doi.org/10.37750/2616-6798.2024.4(51).317919

5. Варинський В. О. Стан правового регулювання використання штучного інтелекту у законодавстві України. *Юридична Україна.* 2025. № 1. С. 40–50. DOI: 10.37749/2308-9639-2025-1(265)-6. URL: https://yur-ukraine.com/stan-pravovogo-regulyuvannya-vykorystannya-shtuchnogo-intelektu-u-zakonodavstvi-ukrayiny

6. Варинський В. О. Соціально-правові чинники формування довіри до штучного інтелекту (Частина 1). *Право і суспільство*. 2025. № 6. С. 524–532. DOI: https://doi.org/10.32842/2078-3736/2025.6.73

7. Варинський В. О. Основні підходи правового регулювання використання штучного інтелекту в освіті. *Актуальні проблеми вдосконалення чинного законодавства України.* 2025. № 69. С. 140–151. DOI: https://doi.org/10.15330/apiclu.69.1.40-1.51

8. Варинський В. Алгоритмічне забезпечення охорони громадського порядку : правові межі застосування штучного інтелекту у діяльності правоохоронних органів. *Академічні візії*. 2025. № 48. С. 1–11. URL: https://www.academy-vision.org/index.php/av/article/view/3189

9. Варинський В.О. Нормативне регулювання використання штучного інтелекту у правосудді. Журнал східноєвропейського права. 2025. № 140. С. 291 – 299. DOI: http://doi.org/10.71404/2409-6415.140.35

10. Варинський В. О. Правова парадигма довіри до штучного інтелекту (Частина ІІ). *Право і суспільство*. 2026. № 1. С. 258–264. DOI https://doi.org/10.32842/2078-3736/2026.1.1.33

11. Варинський В. О. Етичні та правові ризики застосування штучного інтелекту у правоохоронній діяльності та діяльності спецслужб. *Вісник Пенітенціарної асоціації України*. 2026. №1 (35). С. 245–256. DOI: https://doi.org/10.34015/2523-4552.2026.1.22

12. Варинський В. О. AI Act як ризик-орієнтована модель правового обмеження застосування штучного інтелекту у правоохоронній діяльності та діяльності спецслужб. *Південноукраїнський правничий часопис*. 2026. № 1. С. 134–141. DOI : https://doi.org/10.32850/sulj.2026.1.23

13. Варинський В. Правове регулювання обмеження використання штучного інтелекту в медицині: основні міжнародні підходи. *Український часопис міжнародного права*. 2026. № 1. С. 21–33. DOI: https://doi.org/10.36952/ujil.2026.1.3

14. Варинський В. О. Оцінка впливу високоризикових систем штучного інтелекту на права людини як інструмент правової політики України. Академічні візії. 2026. Вип 53. DOI: https://doi.org/10.66556/2786-586X.53.varynskyi-v

Статті у закордонних виданнях, проіндексованих у базах даних Web of Science Core Collection та/або Scopus

15. Varynskyi V., Varynska A., Kostytsky M., Kushakova-Kostytska N. Information security and information hygiene on internet media. *Nexo Revista Científica*. 2021. Vol. 34. № 1. P. 120–128. DOI: https://doi.org/10.5377/nexo.v34i01.11291

16. Varynskyi V., Shelever N., Yankovyi M., Pylyp V., Antalovtsi O., Halahan O. Use of the “electronic court” service as a means of citizens' access to the judiciary. *Lex Humana*. 2023. Vol. 16. № 1. P. 249–266. URL: https://seer.ucp.br/seer/index.php/LexHumana/article/view/2891

17. Rudenko O., Rafalskyi I., Yermak O., Varynskyi V., Konoplia Y. The potential and prospects of artificial intelligence use in strategic planning: issues of security and defense. *AD ALTA: Journal of Interdisciplinary Research.* 2024. Vol. 14/02-XLIV. P. 6–12. URL: https://www.magnanimitas.cz/ADALTA/140244/papers/A_01.pdf

18. Rudenko O., Zaika O., Varynskyi V., Kulchii I., Myroshnychenko A. Digitization of local self-government based on the use of artificial intelligence in the context of sustainable development. *Edelweiss Applied Science and Technology*. 2024. Vol. 8. № 6. P. 1467–1480. DOI: https://doi.org/10.55214/25768484.v8i6.2263

Статті у наукових періодичних виданнях інших держав

19. Varynskyi V. Health-saving technologies in the context of globalization. *International Journal of Recent Technology and Engineering (IJRTE).* 2019. Vol. 8. Issue 4S. P. 63–67. DOI: 10.35940/ijrte.D1023.1184S19

20. Varynskyi V., Donnikova I., Savinova N. Artificial intelligence in education: tool, object, «subject» of learning. *Journal of International Legal Communication*. 2023. Vol. 10. № 3. P. 46–55. DOI: https://doi.org/10.32612/uw.27201643.2023.10.3.pp.46-55

Наукові праці, які засвідчують апробацію матеріалів дисертації

1. Варинський В.О., Савінова Н.А. Два епізоди кримінальної юстиції

майбутнього: футуристичний прогноз. *Наукові читання присвячені пам'яті професора Т.А. Денисової :* збірник матеріалів (м. Запоріжжя, 10 березня 2022 р.). Класичний приватний університет. Запоріжжя : КПУ, 2022. С. 308–311.

2. Варинський В. Філософські засади концепції інтернету речей. *Людина має право: соціально-гуманітарний дискурс у контексті реформаційних процесів в Україні:* матеріали круглого столу (м. Одеса, 17 листопада 2022 р.,). Одеса : ОДУВС, 2022. С. 15–18. URL: http://dspace.pdpu.edu.ua/jspui/bitstream/123456789/16985/1/SviRLYTSKAIA.pdf#page=16

3. Варинський В.О. Основні настанови резолюції Європарламенту про цивільно-правові норми в робототехніці та штучний інтелект: дайджест основних підходів. *Вдосконалення правового регулювання прав та основних свобод людини і громадянина :* матеріали щорічної Всеукраїнської науково-практичної конференції молодих вчених (м. Івано-Франківськ, 5-6 травня 2023 р.). Івано-Франківськ, 2023. С. 78–81. URL: https://law.cnu.edu.ua/wp-content/uploads/sites/100/2024/12/youth2023-r.pdf

4. Варинський В. Штучний інтелект та освіта. *Створювальне знання: освіта для майбутнього :* матеріали 6-го круглого столу в рамках науково-освітнього міжнародного проєкту «Створювальне знання: науково-освітні практики 3.0» (м. Одеса, 9 червня 2023 р.). Одеса : НУОМА, 2023. С. 5–8. URL: http://onma.edu.ua/wp-content/uploads/2023/09/Materialy_6-go_kruglogo-stolu_23.pdf

5. Варинський В. Штучний інтелект та проблеми безпеки. *Сучасна парадигма публічного управління :* збірник тез V Міжнародної науково-практичної конференції (м. Львів, 30 листопада – 2 грудня 2023 р.) / За наук. ред. к.е.н., доцента Стасишина А.В. Львів: ЛНУ імені Івана Франка. Львів, 2024. С. 512–515. URL: https://nung.edu.ua/sites/default/files/2024-06/Збірник_5_Парадигма_2024.pdf

6. Варинський В.О. Ризики використання елементів штучного інтелекту в розробках автономної зброї: на шляху визначень нормативних обмежень. *Штучний інтелект у правовій практиці: межі та можливості:* матеріали Всеукраїнського круглого столу (м. Львів, 15 березня 2024 р.). Львів: ЛьвДУВС, 2024. С. 45–49. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/7424/1/15_03_2024.pdf

7. Варинський В. О., Савінова Н. А. Ефективність удосконалення законодавства та штучний інтелект. *Проблеми інформаційного забезпечення та розвитку парламентського контролю в контексті Європейської та Євроатлантичної інтеграції України* : матеріали науково-практичної конференції (м. Київ, 25 квітня 2024 р.). Київ; Одеса : Фенікс, 2024. С. 107–111. URL: https://ippi.org.ua/sites/default/files/konferenciya_25.04.2024.pdf

8. Варинський В. Правосуб'єктність штучного інтелекту: впродовження ідей О. А. Баранова. *Україна в умовах соціальної та цифрової трансформації: шляхи до сталого розвитку та повоєнної відбудови :* матеріали науково-практичної конференції (м. Київ, 22 листопада 2024 р.). ДНУ «Інститут інформації, безпеки і права Національної академії правових наук України».

Київ; Одеса : Фенікс, 2024. С. 185–191. URL: https://ippi.org.ua/sites/default/files/ukrayina_v_umovah_socialnoyi_ta_cifrovoyi_transformaciyi_maket.pdf

9. Варинський В. Ризики використання ШІ в правосудді: огляд проблеми. *Трансформаційні процеси правотворчої діяльності та парламентського контролю* : матеріали науково-практичної конференції (м. Київ, 30 жовтня 2025 р.). Київ; Одеса : Фенікс, 2025. С. 97–101. URL: https://ippi.org.ua/sites/default/files/zbirnik_tez_30.10.2025.pdf

10. Варинський В. Основні критерії заборон використання ШІ за AI Act. *Україна в умовах соціальної та цифрової трансформації : теоретичні моделі правового регулювання штучного інтелекту :* матеріали науково-практичної конференції (м. Київ, 5 листопада 2025 р.). Київ; Одеса : Фенікс, 2025. С. 116–120. URL: https://ippi.org.ua/sites/default/files/zbirnik_tez_05.11.2025_1.pdf

АНОТАЦІЯ

Варинський В. О. Теоретико-методологічні та правові засади використання штучного інтелекту в Україні. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». – Одеський державний університет внутрішніх справ, Одеса, 2026.

У дисертації здійснено комплексне теоретико-правове та прикладне дослідження інформаційно-правових та адміністративно-правових засад обмеження та публічного адміністрування використання штучного інтелекту (ШІ) в Україні в умовах євроінтеграційного зближення та правового режиму воєнного стану. Обґрунтовано трансформацію предмета інформаційного права від статичного регулювання обігу інформації до комплексного врегулювання суспільних відносин, пов'язаних із процесами її автоматизованого створення, інтерпретації та генерації високоавтономними системами машинного походження.

У роботі розкрито генезис доктринальних підходів до юридичного осмислення ШІ, типізовано функціональний, субстанційний та антропоцентричний вектори його розуміння. Запропоновано авторську правову дефініцію штучного інтелекту як автономної інтелектуальної системи машинного походження, що здатна до самонавчання й динамічної адаптації, та здійснено її чітке правове розмежування з Інтернетом речей (IoT). На основі концепції ціннісно-чутливого проєктування та «етики відповідальності» розкрито аксіологічний вимір алгоритмічних моделей та доведено необхідність підпорядкування їх прагматичної ефективності вимогам захисту людської гідності й збереження обов'язкового людського контролю.

Значну увагу приділено аналізу міжнародного та європейського досвіду правового регулювання ШІ, зокрема ризик-орієнтованої моделі Регламенту (ЄС) 2024/1689 (*Artificial Intelligence Act*), Рамкової конвенції Ради Європи та

специфіки децентралізованого підходу США й централізованого превентивно-наглядового режиму КНР. На основі категоріального апарату теорії права та адміністративного права обґрунтовано необхідність розширення класичної структури механізму правового регулювання шляхом включення до неї новітніх органічно-функціональних елементів: управління ризиками, оцінки відповідності, алгоритмічної прозорості, незалежного аудиту, сертифікації та превентивного державного нагляду.

У дисертації розроблено концептуальну модель диференційованого нормативного обмеження систем ШІ у п'яти найбільш аксіологічно чутливих секторах: воєнній сфері (автономна зброя), медицині, правоохоронній діяльності, правосудді, освіті та науці. Сформульовано сутнісні критерії обмежень залежно від операційного контексту в межах моделей інтеграції людського оператора (*human-in-the-loop, human-on-the-loop, human-out-of-the-loop*) та мінімізації ризиків алгоритмічної упередженості (*algorithmic bias*) й «упередження автоматизації».

Сформовано теоретико-методологічні засади цілісної ризик-орієнтованої правової політики у сфері ШІ, визначеної як системна діяльність держави з формування диференційованих правових режимів, де зміст заборон та обов'язків корелює із масштабом, тяжкістю й оборотністю впливу конкретної системи на права людини, демократію та національну безпеку. Запропоновано авторський аксіологічний ризик-орієнтований тест адміністративно-правової оцінки ШІ, що базується на ієрархії конституційних благ і включає чотири послідовні рівні: оцінку загрози життю та здоров'ю людини; вплив на національну безпеку; ступінь ризику для реалізації фундаментальних прав; вплив на функціонування демократичного врядування та верховенство права.

Розроблено та обґрунтовано оптимальну для України мережеву (гібридну) інституційну модель публічного адміністрування ШІ, яка усуває конфлікт цілей між підтримкою інновацій та захистом прав і передбачає функціональну матрицю компетенцій між Кабінетом Міністрів України, Мінцифри, Національним компетентним органом нагляду (ЦОВВ зі спеціальним статусом), секторальними регуляторами, Уповноваженим ВРУ з прав людини та судовою системою.

Для практичного впровадження моделі сформовано трирівневий узгоджений пакет нормативно-правових актів, що складається з рамкового Закону України «Про безпечне та відповідальне використання систем штучного інтелекту», проєкту закону про внесення змін до базових актів (зокрема до ЗУ «Про адміністративну процедуру» щодо алгоритмічно підтриманих рішень та відтворюваного алгоритмічного сліду, законів про захист персональних даних, публічні закупівлі, електронні реєстри та доступ до інформації), а також процедурних постанов уряду. Систематизовано дванадцять взаємопов'язаних адміністративних процедур, що охоплюють повний життєвий цикл систем ШІ, та визначено особливості їх застосування у закритих безпекових секторах під час воєнного стану.

Ключові слова: теоретико-методологічні засади, правові засади, штучний інтелект, система штучного інтелекту, публічне адміністрування,

інформаційне право, адміністративна процедура, ризик-орієнтований підхід, аксіологія, людський контроль, мережева інституційна модель, євроінтеграція, цифровізація, механізм правового регулювання.

SUMMARY

Varynskyi V. O. Theoretical, Methodological, and Legal Framework for the Use of Artificial Intelligence in Ukraine. – Qualification scientific work manuscript.

Thesis for a Doctor of Laws (Doctor of Legal Sciences) degree in Speciality 12.00.07 "Administrative Law and Process; Financial Law; Information Law". – Odesa State University of Internal Affairs, Odesa, 2026.

The thesis provides a comprehensive theoretical and applied study of the information-legal and administrative-legal frameworks for the restriction and public administration of artificial intelligence (AI) systems in Ukraine in the context of European integration alignment and the legal regime of martial law. The dissertation substantiates the transformation of the subject matter of information law from the static regulation of information circulation into a complex regulation of social relations arising from the automated creation, interpretation, and generation of information by highly autonomous systems of machine origin.

The work reveals the genesis of doctrinal approaches to the legal conceptualisation of AI, categorising the functional, substantial, and anthropocentric vectors of its understanding. The author proposes a novel legal definition of artificial intelligence as an autonomous intellectual system of machine origin capable of self-learning and dynamic adaptation, and draws a clear legal distinction between AI and the Internet of Things (IoT). Based on the concepts of Value Sensitive Design and the "ethics of responsibility", the dissertation explores the axiological dimension of algorithmic models and demonstrates the necessity of subordinating their pragmatic efficiency to the imperatives of human dignity protection and the preservation of meaningful human control.

Significant attention is devoted to the analysis of international and European experience in the legal regulation of AI, in particular the risk-based model of Regulation (EU) 2024/1689 (Artificial Intelligence Act), the Council of Europe Framework Convention, as well as the specific features of the decentralized approach of the USA and the centralized preventive-supervisory regime of the PRC. Grounded on the categorical apparatus of the theory of law and administrative law, the study argues for the necessity of expanding the classical structure of the mechanism of legal regulation by incorporating novel organic-functional elements into it: risk management, conformity assessment, algorithmic transparency, independent audit, certification, and preventive state supervision.

The thesis develops a conceptual model for the differentiated regulatory restriction of AI systems within five most axiologically sensitive sectors: the military sphere (autonomous weapons), medicine, law enforcement, justice, education and science. The essential criteria for restrictions are formulated depending on the operational context within the models of human operator integration (*human-in-the-loop, human-on-the-loop, human-out-of-the-loop*) and the mitigation of risks associated with algorithmic bias and automation bias.

The study establishes the theoretical and methodological foundations of a holistic risk-based legal policy in the field of AI, defined as a systemic activity of the state aimed at forming differentiated legal regimes, where the scope of prohibitions and obligations correlates with the scale, severity, and reversibility of a specific system's impact on human rights, democracy, and national security. The author proposes an original axiological risk-based test for the administrative-legal assessment of AI, which is rooted in the hierarchy of constitutional goods and comprises four successive levels: assessment of threats to human life and health; impact on national security; the degree of risk to the exercise of fundamental rights; and the impact on the functioning of democratic governance and the rule of law.

The dissertation designs and substantiates a network (hybrid) institutional model of public administration of AI optimal for Ukraine. This model eliminates the conflict of objectives between supporting innovation and protecting rights, and introduces a functional matrix of competences shared among the Cabinet of Ministers of Ukraine, the Ministry of Digital Transformation, the National Competent Supervisory Authority (a central executive body with special status), sectoral regulators, the Ukrainian Parliament Commissioner for Human Rights (Ombudsman), and the judiciary.

For the practical implementation of the model, a three-tiered harmonised package of regulatory legal acts has been developed, consisting of the framework Law of Ukraine "On the Safe and Responsible Use of Artificial Intelligence Systems", a draft law on amendments to basic legislative acts (specifically to the Law of Ukraine "On Administrative Procedure" regarding algorithmically supported decisions and the reproducible algorithmic trail, and laws on personal data protection, public procurement, public electronic registries, and access to information), as well as procedural government decrees. The study systematises twelve interconnected administrative procedures covering the full lifecycle of AI systems and defines the specificities of their application in closed security sectors during martial law.

Keywords: theoretical and methodological framework, legal framework, artificial intelligence, artificial intelligence system, public administration, information law, administrative procedure, risk-based approach, axiology, human control, network institutional model, European integration, digitization, mechanism of legal regulation.