

Андрій Тарасюк,

доктор філософії у галузі права,
учений секретар ПВНЗ «Інститут екології
економіки і права».

ORCID: <https://orcid.org/0009-0008-7115-1072>

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В ЕЛЕКТРОННІЙ СИСТЕМІ ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ

У статті розкрито правові та організаційні особливості використання технологій штучного інтелекту в електронній системі охорони здоров'я України та пов'язаних із нею електронних медичних інформаційних системах. Окреслено основні напрями застосування таких технологій: опрацювання електронних медичних записів, аналіз медичних зображень, прогнозування ризиків захворювань, персоналізація лікування, підтримка телемедичних послуг, управління ресурсами та виявлення кіберзагроз. Проаналізовано ризики, пов'язані з недостатньою якістю та репрезентативністю даних, алгоритмічною упередженістю, непрозорістю автоматизованих висновків, порушенням конфіденційності медичної інформації, неправомірним доступом до персональних даних і невизначеністю юридичної відповідальності. Наголошено, що системи штучного інтелекту повинні виконувати допоміжну функцію та не підміняти професійне клінічне рішення медичного працівника.

Методологічну основу дослідження становили формально-юридичний, системно-структурний і порівняльно-правовий методи, а також методи аналізу, синтезу та узагальнення. Їх застосування дало змогу проаналізувати національне та європейське правове регулювання, визначити місце систем ШІ в інфраструктурі електронної охорони здоров'я та обґрунтувати авторські пропозиції щодо ризик-орієнтованої моделі їх інтеграції.

Запропоновано ризик-орієнтовану модель правового регулювання, за якої обсяг вимог залежатиме від призначення системи, ступеня її автономності, характеру оброблюваних даних і можливих наслідків для життя, здоров'я та прав пацієнтів. Така модель має передбачати класифікацію систем за рівнем ризику, технічне і клінічне оцінювання, аудит якості та репрезентативності навчальних даних, забезпечення прозорості й пояснюваності алгоритмічних результатів, належний людський контроль, журналювання операцій і постійний моніторинг.

Сформульовано поетапний порядок інтеграції технологій штучного інтелекту в інфраструктуру електронної охорони здоров'я та запропоновано створення реєстру систем, допущених до використання. Визначено підходи до розмежування відповідальності між медичним працівником, закладом охорони здоров'я, розробником, постачальником програмного продукту й суб'єктом, що забезпечує функціонування електронної медичної інформаційної системи. Виокремлено принципи законності, людиноцентричності, мінімально необхідного використання медичних даних, недискримінаційності, безпечності, прозорості, підзвітності та простежуваності автоматизованих операцій.

Ключові слова: штучний інтелект, електронна система охорони здоров'я, електронні медичні інформаційні системи, електронні медичні дані, правове регулювання, захист персональних даних, належний людський контроль, юридична відповідальність.

Tarasiuk A.

The USE of artificial intelligence technologies in the electronic healthcare system of Ukraine

The article examines the legal and organizational aspects of the use of artificial intelligence technologies in Ukraine's electronic healthcare system and the electronic medical information systems integrated with it. The principal areas of application of these technologies are outlined, including the processing of electronic health records, medical image analysis, disease risk prediction, personalized treatment, support for telemedicine services, healthcare resource management, and cyberthreat detection. The study analyses the risks associated with insufficient data quality and representativeness, algorithmic bias, the lack of transparency of automated outputs, breaches of medical data confidentiality, unauthorized access to personal data, and uncertainty regarding legal liability. It is emphasized that artificial intelligence systems should perform an auxiliary function and must not replace the professional clinical judgment of healthcare practitioners.

The methodological basis of the study comprised formal-legal, systemic-structural and comparative-legal

methods, as well as methods of analysis, synthesis and generalization. Their application made it possible to analyse national and European legal regulation, determine the place of AI systems in the electronic healthcare infrastructure, and substantiate proposals for a risk-based model of their integration.

A risk-based model of legal regulation is proposed, under which the scope of applicable requirements should depend on the intended purpose of the system, its degree of autonomy, the nature of the data processed, and the potential consequences for patients' lives, health, and rights. Such a model should provide for the classification of systems according to their level of risk, technical and clinical assessment, auditing of the quality and representativeness of training data, transparency and explainability of algorithmic outputs, meaningful human oversight, logging of operations, and continuous monitoring.

A phased procedure for integrating artificial intelligence technologies into the electronic healthcare infrastructure is formulated, and the establishment of a register of systems authorized for use is proposed. Approaches to the allocation of liability among healthcare practitioners, healthcare institutions, developers, software providers, and entities responsible for operating electronic medical information systems are identified. The principles of legality, human-centeredness, data minimization, non-discrimination, safety, transparency, accountability, and traceability of automated operations are specified.

Keywords: *artificial intelligence, electronic healthcare system, electronic medical information systems, electronic health data, legal regulation, personal data protection, meaningful human oversight, legal liability.*

Постановка проблеми. Цифрова трансформація сфери охорони здоров'я України, розвиток електронної системи охорони здоров'я та накопичення значних обсягів електронних медичних даних формують передумови для впровадження штучного інтелекту в електронну систему охорони здоров'я (далі – ЕСОЗ) та інтегровані з нею електронні медичні інформаційні системи (далі – ЕМІС) [1, с. 83; 23, с. 55–56]. Технології ШІ можуть використовуватися для оброблення і систематизації медичної інформації, аналізу результатів обстежень, прогнозування ризиків захворювань, персоналізації лікування, автоматизації адміністративних операцій та підтримки клінічних і управлінських рішень [2, с. 119]. Їх застосування потребує належного правового, організаційного й технічного забезпечення, оскільки результати алгоритмічного аналізу можуть впливати на здоров'я людини, якість медичної допомоги та використання ресурсів [4, с. 145].

Окремим напрямом є використання ШІ в медичній освіті та професійній підготовці лікарів, зокрема для моделювання клінічних ситуацій, персоналізації навчання й оцінювання практичних навичок [9, с. 430]. Використання для таких цілей інформації з електронних медичних систем має здійснюватися за наявності належної правової підстави та з дотриманням вимог законодавства про захист персональних даних [6].

Водночас застосування ШІ в інфраструктурі електронної охорони здоров'я супроводжується правовими, етичними, організаційними та інформаційно-технологічними ризиками: використанням неповних або упереджених даних, формуванням помилкових рекомендацій, непрозорістю алгоритмічних моделей, порушенням конфіденційності медичної інформації, неправомірним доступом до персональних даних, кіберзагрозами та невизначеністю меж юридичної відповідальності [7, с. 36; 24, с. 165–166].

Особливої уваги потребує роль медичного працівника: рекомендації, прогнози та висновки, сформовані ШІ, мають виконувати допоміжну функцію і не підміняти професійне клінічне рішення [23, с. 58]. Не менш важливим є формування цифрових компетентностей медичних працівників, необхідних для критичного оцінювання можливостей, обмежень і ризиків відповідних технологій [1, с. 94].

Чинне нормативно-правове регулювання визначає загальні засади функціонування ЕСОЗ, обміну медичною інформацією, захисту персональних даних і розвитку ШІ [6; 8; 10; 12], однак не формує цілісного спеціального механізму інтеграції систем ШІ в інфраструктуру електронної охорони здоров'я [4, с. 149]. Планом заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025–2026 роки передбачено розроблення та подання Кабінетові Міністрів України відповідного законопроекту у IV кварталі 2026 року [25].

Отже, актуальність дослідження визначається необхідністю формування комплексних правових та організаційних засад інтеграції технологій штучного інтелекту в електронну систему охорони здоров'я України, які забезпечували б поєднання їх інноваційного потенціалу із захистом прав пацієнтів, безпекою медичних даних, збереженням професійної самостійності лікаря та належним людським контролем за алгоритмічними висновками.

Мета статті полягає у визначенні особливостей правового регулювання використання технологій штучного інтелекту в електронній системі охорони здоров'я України та обґрунтуванні пропозицій щодо

встановлення вимог до доступу й оброблення медичних даних, людського контролю за алгоритмічними висновками, захисту прав пацієнтів і юридичної відповідальності учасників відповідних правовідносин.

Аналіз останніх досліджень і публікацій. Проблематика застосування ШІ у сфері охорони здоров'я має міждисциплінарний характер. У наукових працях досліджуються функціональні можливості інтелектуальних систем, їх інтеграція в медичну практику, використання електронних медичних даних, захист персональних даних, етичні обмеження та правове забезпечення. Окремим напрямом є використання ШІ в медичній освіті та професійній підготовці лікарів-інтернів [9, с. 430].

Медичні й технологічні напрями використання ШІ висвітлено у працях О. М. Бойченко та Т. Д. Бублій [14, с. 137–139], А. Б. Горкуненка [7, с. 35–41], І. П. Кривенка та К. О. Чалого [1, с. 81–96], В. О. Короткої та В. А. Мокринського [2, с. 119–121], А. В. Вовк [5]. Управлінський потенціал відповідних технологій досліджували О. В. Карпенко, Ю. В. Карпенко та Є. А. Кульгінський [16], а їх застосування в телемедицині й громадському здоров'ї – Ю. О. Пилипець та співавтори [19, с. 190–195] і Я. В. Першегуба [17, с. 128–136].

Правові аспекти застосування ШІ у сфері охорони здоров'я досліджували О. В. Россильна [15, с. 156–162], І. В. Діордіца та О. М. Коваль [3, с. 87–97], А. В. Сидорук [4, с. 143–151]. Проблемам розвитку єдиного медичного інформаційного простору та захисту конфіденційної медичної інформації присвячено праці В. І. Теремецького у співавторстві [23, с. 55–60; 24, с. 161–168].

Отже, наявні наукові праці сформували достатнє підґрунтя для розуміння технологічних, управлінських і правових аспектів використання ШІ в медицині. Водночас недостатньо дослідженими залишаються правові та організаційні умови його інтеграції безпосередньо в електронну систему охорони здоров'я України, зокрема порядок доступу алгоритмічних моделей до електронних медичних даних, вимоги до їх розроблення, навчання, валідації та оцінювання безпечності, документування автоматизованих операцій, інформування пацієнтів, забезпечення людського контролю та визначення підстав і меж юридичної відповідальності учасників відповідних правовідносин.

Виклад основного матеріалу дослідження. Використання ШІ в ЕСОЗ слід розглядати в контексті електронної охорони здоров'я. Відповідно до ст. 3 Основ законодавства України про охорону здоров'я та Порядку функціонування електронної системи охорони здоров'я, затвердженого постановою Кабінету Міністрів України від 25.04.2018 № 411, ЕСОЗ є інформаційно-комунікаційною системою, до складу якої входять центральна база даних та ЕМІС, між якими забезпечується автоматичний обмін інформацією, даними і документами через відкритий програмний інтерфейс (API) [8; 10]. Концепція розвитку електронної охорони здоров'я орієнтує розвиток галузі на формування єдиного медичного інформаційного простору та сумісність інформаційних ресурсів [11; 23, с. 55–56]. Тому ЕСОЗ не слід ототожнювати з усією інфраструктурою електронної охорони здоров'я.

ЕСОЗ є ключовим компонентом електронної охорони здоров'я, тоді як ширше цифрове середовище охоплює також ЕМІС, електронні реєстри, телемедичні платформи, діагностичні комплекси, системи підтримки клінічних рішень, мобільні застосунки та інші програмно-технічні засоби. Відповідно, ШІ може застосовуватися як у функціональних компонентах ЕСОЗ, так і в інтегрованих із нею системах.

Концепція розвитку штучного інтелекту в Україні визначає ШІ як організовану сукупність інформаційних технологій, застосування якої дає змогу виконувати складні комплексні завдання за допомогою алгоритмів оброблення інформації, формувати бази знань і моделі прийняття рішень [12]. У межах цього дослідження використання ШІ в електронній охороні здоров'я розуміється як автоматизований аналіз медичних та адміністративних даних для формування прогнозів, рекомендацій чи інших інформаційних результатів, що підтримують діяльність медичних працівників, закладів охорони здоров'я й органів публічного управління. Накопичення електронних медичних даних та розвиток механізмів їх обміну створюють фактичну основу для такої інтеграції.

Функціональне призначення таких систем не зводиться лише до діагностики. У науковій літературі до напрямів застосування ШІ відносять прогнозування, аналіз і класифікацію інформації, автоматизовану діагностику, оброблення природної мови, чат-боти та робототехніку [13, с. 107–108]. Для цілей цього дослідження відповідні можливості доцільно узагальнити в інформаційно-аналітичний, клініко-діагностичний, лікувально-прогностичний, організаційно-управлінський, профілактичний та інформаційно-безпековий напрями.

Першочерговим напрямом є автоматизоване оброблення електронних медичних записів. Технології оброблення природної мови дають змогу структурувати текстову інформацію, виявляти неповні або суперечливі записи та формувати проєкти узагальнених висновків. І. П. Кривенко та К. О. Чалий зазначають,

що медичні моделі можуть опрацьовувати електронні медичні записи, клінічні протоколи, наукові статті, медичні зображення, сигнальні та геномні дані, а їх інтеграція створює інформаційне середовище для підтримки клінічних рішень [1, с. 83].

У межах ЕСОЗ системи штучного інтелекту потенційно можуть використовуватися для автоматизованого пошуку дубльованих записів, перевірки логічної узгодженості медичної інформації, виявлення відсутніх реквізитів, зіставлення призначень із клінічними протоколами та формування повідомлень про можливі невідповідності. Водночас алгоритмічне виявлення помилки не повинно автоматично призводити до зміни або видалення медичного запису. Остаточне рішення має приймати уповноважений медичний працівник, а факт автоматизованої перевірки та подальші дії користувача повинні фіксуватися в системі.

Одним із найбільш розвинених напрямів є аналіз медичних зображень. Алгоритми комп'ютерного зору застосовуються для опрацювання результатів рентгенографії, комп'ютерної та магнітно-резонансної томографії, мамографії й гістологічних досліджень, сприяючи виявленню патологічних змін і стандартизації первинного опису результатів обстеження [14, с. 137].

ІІІ також може застосовуватися для прогнозування ризику розвитку захворювань і персоналізації лікування шляхом аналізу анамнезу, лабораторних показників, генетичних даних та динаміки стану здоров'я [15, с. 156]. Водночас алгоритмічний результат не слід визнавати самостійним медичним рішенням: система ІІІ має доповнювати, а не замінювати професійне рішення медичного працівника [23, с. 58].

ІІІ може використовуватися і для організації діяльності закладів охорони здоров'я: прогнозування навантаження, оптимізації графіків і черг, планування використання обладнання, аналізу потреб у лікарських засобах та оцінювання використання ресурсів [16]. До управлінських напрямів застосування медичного ІІІ також відносять адміністративну підтримку, управління робочими процесами та виявлення шахрайських операцій [7, с. 39].

Водночас автоматизована оптимізація ресурсів не повинна зводитися до механічного скорочення витрат. Управлінські алгоритми можуть безпосередньо впливати на доступ пацієнтів до обстежень, лікування або лікарських засобів. Тому критеріями їх роботи мають бути не лише економічна ефективність, а й медична обґрунтованість, рівність доступу, недискримінаційність і врахування потреб уразливих груп населення.

На популяційному рівні ІІІ може застосовуватися для прогнозування спалахів інфекційних захворювань, оцінювання ризиків для громадського здоров'я, виявлення територій із підвищеною потребою в медичних послугах і планування профілактичних заходів. Я. В. Першегуба звертає увагу на ризик алгоритмічної упередженості та її вплив на справедливість управлінських рішень [17, с. 129], тому оцінювати слід не лише статистичну точність, а й соціальні наслідки застосування алгоритму.

Після змін, внесених Законом України від 09.08.2023 № 3301-ІХ, Основи законодавства України про охорону здоров'я визначають телемедицину як складову електронної охорони здоров'я [18]. У телемедичних системах ІІІ може використовуватися для дистанційного моніторингу, медичного сортування та підтримки рішень під час надзвичайних ситуацій [19, с. 191], а в умовах воєнного стану – також для медичної логістики, екстреної допомоги та підтримки евакуаційних рішень [20, с. 55].

Водночас використання автоматизованих систем у невідкладних ситуаціях підвищує вимоги до надійності, швидкості, доступності та здатності працювати за нестабільного зв'язку. Система повинна передбачати резервний порядок дій у разі технічної несправності, відсутності доступу до даних або неможливості перевірити сформовану рекомендацію.

Основним ресурсом для функціонування систем ІІІ є дані, а якість алгоритмічного результату залежить від їх повноти, актуальності, репрезентативності та достовірності. Відомості про стан здоров'я належать до персональних даних, щодо оброблення яких ст. 7 Закону України «Про захист персональних даних» установлює особливі вимоги та обмеження [6]. У науковій літературі також підкреслюється, що медичні дані є складовою персональних даних і підлягають відповідному правовому захисту [24, с. 162]. Сам факт технічної можливості аналізувати інформацію не є достатньою правовою підставою для її використання.

Необхідно розмежовувати оброблення даних для безпосереднього надання медичної допомоги та їх вторинне використання для розроблення або навчання алгоритмічних моделей. У другому випадку слід окремо визначати правову підставу і мету оброблення, необхідний обсяг даних, коло осіб із доступом до них та належні заходи захисту, а за потреби застосовувати знеособлення або псевдонімізацію. Псевдонімізація сама по собі не виключає можливості ідентифікації особи за допомогою додаткової інформації, тому потребує розмежування доступу й належного документування операцій.

Окремою проблемою є якість навчальних даних: недостатнє представлення окремих груп пацієнтів або використання історичних даних, що відображають нерівність у доступі до медичної допомоги, може знижувати точність алгоритмів і відтворювати упередження. Для високоризикових систем Акт ЄС про штучний інтелект передбачає вимоги до управління даними та їх якості [22]. Для документування походження, структури, обмежень і призначення даних та моделі доцільно використовувати паспорти набору даних і алгоритмічної моделі.

Важливими вимогами є пояснюваність алгоритмічних висновків та людський контроль. Медичний працівник повинен мати достатню інформацію про основні фактори, що вплинули на результат, рівень упевненості моделі та відомі обмеження, а пацієнт – отримувати зрозумілу інформацію про роль ШІ у процесі надання медичної допомоги. Обсяг відповідних вимог має залежати від рівня ризику та впливу алгоритмічного результату на діагностику, лікування, права і безпеку пацієнта.

Використання ШІ створює додаткові ризики для конфіденційності медичної інформації, зокрема несанкціонований доступ до навчальних наборів, повторну ідентифікацію особи, використання даних за межами визначеної мети та витік інформації через зовнішні програмні сервіси. Проблеми захисту конфіденційної медичної інформації в електронних медичних системах та пов'язані з ними ризики докладно аналізувалися В. І. Теремецьким і співавторами [24, с. 165–166].

Водночас технології ШІ можуть застосовуватися для посилення захисту медичних даних. І. В. Діордіца та О. М. Коваль обґрунтовують можливість використання машинного навчання для виявлення аномальної поведінки користувачів, несанкціонованого доступу, підозрілої активності та прогнозування кіберзагроз [3, с. 89]. У межах ЕСОЗ та ЕМІС сигнал такої системи має бути підставою для додаткової перевірки уповноваженим працівником, а не автоматичним підтвердженням порушення.

Вимоги інформаційної безпеки мають ураховуватися вже на етапі проєктування системи. Закон України «Про захист інформації в інформаційно-комунікаційних системах» визначає загальні правові засади захисту інформації під час її оброблення в таких системах [21]. На організаційно-технічному рівні доцільними є розмежування прав доступу, шифрування, багатофакторна автентифікація, журналювання операцій, резервне копіювання, тестування вразливостей та реагування на інциденти [3, с. 95]. Окремої оцінки потребує передавання медичних даних до зовнішніх генеративних моделей за межі контрольованої інформаційної інфраструктури закладу охорони здоров'я, ЕСОЗ або ЕМІС.

У клінічно значущих процесах належний людський контроль має забезпечувати реальну можливість медичного працівника оцінити, перевірити й за потреби відхилити алгоритмічну рекомендацію; ШІ має доповнювати, а не замінювати професійне рішення [23, с. 58]. Це не означає автоматичного покладення на лікаря відповідальності за всі негативні наслідки використання системи. У чинному праві України спеціальної правосуб'єктності систем ШІ не встановлено; у науковій літературі статус «електронної особи» розглядається лише як можливий майбутній підхід [15, с. 157].

У межах запропонованої моделі юридичну відповідальність доцільно диференціювати залежно від характеру порушеного обов'язку, можливості відповідного суб'єкта контролювати ризик і причинного зв'язку із заподіяною шкодою. Медичний працівник має нести відповідальність у межах установлених законом професійних обов'язків за власне клінічне рішення; заклад охорони здоров'я – за належну організацію використання технології, підготовку персоналу, контроль доступу та реагування на інциденти; розробник і постачальник – за якість програмного продукту, документації та оновлень; суб'єкт, що забезпечує функціонування ЕМІС, – за технічну сумісність, захищений інформаційний обмін і фіксацію операцій. Така диференціація є пропозицією для майбутнього спеціального регулювання, а не констатацією вже встановленої законодавством моделі.

Виявлені прогалини свідчать про доцільність переходу від фрагментарного регулювання окремих складників електронної охорони здоров'я до комплексної моделі, яка враховуватиме призначення системи ШІ, характер оброблюваних даних, ступінь автономності та можливі наслідки для прав і безпеки пацієнтів [4, с. 149].

Важливим орієнтиром для вдосконалення національного законодавства є Регламент (ЄС) 2024/1689 (Акт про штучний інтелект), який загалом застосовується в ЄС з 2 серпня 2026 року, тоді як ст. 6(1) та пов'язані з нею обов'язки застосовуватимуться з 2 серпня 2027 року [22]. Не кожна медична система ШІ автоматично є високоризиковою: для систем, що є продуктами або компонентами безпеки продуктів, застосовуються умови ст. 6(1), а до переліку законодавства в Додатку I включено, зокрема, акти ЄС про медичні вироби та медичні вироби для діагностики *in vitro*. Для України Регламент є орієнтиром гармонізації, а не актом прямої дії. Запозичення ризик-орієнтованого підходу доцільно здійснювати з

урахуванням призначення системи, чутливості даних, автономності, впливу на клінічне рішення, тяжкості потенційної шкоди та можливості перевірки результату.

З огляду на ці критерії інтеграцію ІІІ в ЕСОЗ та ЕМІС пропонується здійснювати у п'ять взаємопов'язаних етапів: 1) визначення призначення системи, користувачів, категорій даних, автономності та попереднього рівня ризику; 2) оцінювання правомірності оброблення, якості, репрезентативності й захищеності даних; 3) технічне та клінічне оцінювання точності, пояснюваності, надійності й безпечності; 4) обмежене пілотне впровадження за участю підготовлених медичних працівників і з людським контролем; 5) постійний моніторинг, реєстрація інцидентів, оновлення та повторне оцінювання після істотних змін системи.

Доцільним є також створення реєстру систем ІІІ, допущених до використання в інфраструктурі електронної охорони здоров'я, із відомостями про розробника, версію, призначення, сферу застосування, рівень ризику, результати оцінювання, відомі обмеження, істотні оновлення та зареєстровані інциденти.

Таким чином, інтеграція технологій ІІІ в ЕСОЗ має ґрунтуватися на принципах законності, людиноцентричності, цільового та мінімально необхідного використання медичних даних, прозорості, пояснюваності, недискримінаційності, безпечності, підзвітності та простежуваності автоматизованих операцій.

Висновки. Розвиток ЕСОЗ і накопичення електронних медичних даних створюють передумови для використання ІІІ під час оброблення інформації, прогнозування ризиків, персоналізації лікування та підтримки клінічних і управлінських рішень. Водночас у клінічно значущих процесах ІІІ має виконувати допоміжну функцію та не підміняти професійне рішення медичного працівника.

Чинне регулювання визначає загальні засади функціонування ЕСОЗ, захисту персональних даних та державної політики у сфері ІІІ, але не встановлює цілісного спеціального механізму інтеграції алгоритмічних систем у електронну охорону здоров'я. Потребують подальшого врегулювання доступ до медичних даних, вимоги до навчальних наборів, технічного і клінічного оцінювання, пояснюваності, кібербезпеки, документування операцій, інформування пацієнтів та розподілу відповідальності.

Доцільно запровадити ризик-орієнтовану модель, що передбачатиме класифікацію систем за рівнем ризику, перевірку якості й репрезентативності даних, технічне та клінічне оцінювання, належний людський контроль, постійний моніторинг і реєстр систем, допущених до використання. Розподіл обов'язків і відповідальності між медичним працівником, закладом охорони здоров'я, розробником, постачальником та суб'єктом, що забезпечує функціонування ЕМІС, має визначатися з урахуванням фактичного контролю відповідного ризику та причинного зв'язку із заподіяною шкодою.

Перспективи подальших наукових досліджень полягають у розробленні спеціальних адміністративно-правових вимог до клінічного використання систем ІІІ в ЕСОЗ та ЕМІС, зокрема критеріїв їх ризиковості, процедур оцінювання, постійного моніторингу й розподілу відповідальності між учасниками відповідних правовідносин.

Список використаних джерел

1. Кривенко І. П., Чалий К. О. Функціональні можливості медичного штучного інтелекту для галузі охорони здоров'я та професійної освіти. *Медична інформатика та інженерія*. 2024. № 3–4. С. 81–96. DOI: <https://doi.org/10.11603/mie.1996-1960.2024.3-4.15462>.
2. Коротка В. О., Мокринський В. А. Технології штучного інтелекту в сучасній медицині: впровадження та проблематика. *Український медичний часопис*. 2024. № 5 (163). С. 119–121. DOI: <https://doi.org/10.32471/umj.1680-3051.163.257497>.
3. Діордіца І. В., Коваль О. М. Інтеграція штучного інтелекту в системи захисту персональних даних у сфері охорони здоров'я. *Наука і техніка сьогодні*. 2024. № 5 (33). С. 87–97. DOI: [https://doi.org/10.52058/2786-6025-2024-5\(33\)-87-97](https://doi.org/10.52058/2786-6025-2024-5(33)-87-97).
4. Сидорук А. В. Державна політика цифровізації охорони здоров'я: адміністративно-правові засади розвитку медичних інформаційних технологій і використання штучного інтелекту. *Київський часопис права*. 2026. № 2. С. 143–151. DOI: <https://doi.org/10.32782/klj/2026.2.20>.
5. Вовк А. В. Використання штучного інтелекту в медицині. Молодь в науці: дослідження, проблеми, перспективи (МН-2024): матеріали Всеукраїнської науково-практичної інтернет-конференції. Вінниця, 2024. URL: <https://conferences.vntu.edu.ua/index.php/mn/mn2024/paper/download/21267/17612> (дата звернення: 08.05.2026).
6. Про захист персональних даних: Закон України від 01 червня 2010 р. № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення: 08.05.2026).

7. Горкуненко А. Б. Штучний інтелект у медицині: масштаби ринку та напрями розвитку. *Вісник соціальної гігієни та організації охорони здоров'я України*. 2025. № 1 (103). С. 35–41. DOI: <https://doi.org/10.11603/1681-2786.2025.1.15340>.
8. Деякі питання електронної системи охорони здоров'я: постанова Кабінету Міністрів України від 25 квітня 2018 р. № 411. URL: <https://zakon.rada.gov.ua/laws/show/411-2018-%D0%BF#Text> (дата звернення: 08.05.2026).
9. Гряділь Т. І. Можливості використання штучного інтелекту в освітньому процесі лікарів-інтернів. *Відкрита наука України: візійний дискурс в умовах воєнного стану: матеріали Міжнародної міждисциплінарної науково-практичної конференції, м. Ужгород, 26–28 квітня 2023 р.* Ужгород : ДВНЗ «Ужгородський національний університет», 2023. С. 429–431. URL: <https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/54739/1/OSU2023.pdf> (дата звернення: 10.05.2026).
10. Основи законодавства України про охорону здоров'я: Закон України від 19 листопада 1992 р. № 2801-XII. URL: <https://zakon.rada.gov.ua/laws/show/2801-12#Text> (дата звернення: 08.05.2026).
11. Про схвалення Концепції розвитку електронної охорони здоров'я: розпорядження Кабінету Міністрів України від 28 грудня 2020 р. № 1671-р. URL: <https://zakon.rada.gov.ua/laws/show/1671-2020-%D1%80#Text> (дата звернення: 07.0.2026).
12. Про схвалення Концепції розвитку штучного інтелекту в Україні: розпорядження Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. URL: <https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text> (дата звернення: 09.05.2026).
13. Кий-Кокарева В. Г., Заславський Д. Д. Деякі аспекти використання штучного інтелекту в охороні здоров'я. *Громадське здоров'я в Україні: проблеми та способи їх вирішення: матеріали V науково-практичної конференції з міжнародною участю, м. Харків, 28 жовтня 2022 р.* Харків, 2022. С. 106–108. DOI: <https://doi.org/10.5281/zenodo.7327653>.
14. Бойченко О. М., Бублій Т. Д. Перспективи використання штучного інтелекту в медичній сфері. *Актуальні проблеми сучасної медицини*. 2024. Т. 24, вип. 3 (87). С. 137–139. DOI: <https://doi.org/10.31718/2077-1096.24.3.137>.
15. Россильна О. В. Правові засади застосування штучного інтелекту у правовідносинах у сфері персоналізованої медицини. *Юридичний вісник*. 2022. № 2. С. 156–162. DOI: <https://doi.org/10.32837/uv.v0i2.2334>.
16. Карпенко О. В., Карпенко Ю. В., Кульгінський Є. А. Застосування технологій штучного інтелекту у реформуванні сфери охорони здоров'я. *Державне управління: удосконалення та розвиток*. 2021. № 11. DOI: <https://doi.org/10.32702/2307-2156-2021.11.2>.
17. Першегуба Я. В. Методологічні підходи до застосування штучного інтелекту в системі громадського здоров'я. *Спортивна медицина, фізична терапія та ерготерапія*. 2024. № 2. С. 128–136. DOI: <https://doi.org/10.32782/spmed.2024.2.128-136>.
18. Про внесення змін до деяких законодавчих актів України щодо функціонування телемедицини: Закон України від 9 серпня 2023 р. № 3301-IX. URL: <https://zakon.rada.gov.ua/laws/show/3301-20#Text> (дата звернення: 08.05.2026).
19. Пилипець Ю. О., Павлов С. В., Ярославський Я. І., Костюк С. В., Урсан М. І. Особливості застосування телемедичних технологій на основі штучного інтелекту в медицині катастроф. *Оптико-електронні інформаційно-енергетичні технології*. 2024. Т. 48, № 2. С. 190–195. DOI: <https://doi.org/10.31649/1681-7893-2024-48-2-190-195>.
20. Савицький В. Л., Печиборщ В. П., Коробкін В. Ф., Добровольська Н. А., Печиборщ О. В., Волянський О. П. Шляхи застосування штучного інтелекту у військовій медицині в умовах воєнного стану. *Український журнал військової медицини*. 2025. Т. 6, № 2. С. 54–64. DOI: [https://doi.org/10.46847/ujmm.2025.2\(6\)-054](https://doi.org/10.46847/ujmm.2025.2(6)-054).
21. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 5 липня 1994 р. № 80/94-ВР. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text> (дата звернення: 08.05.2026).
22. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*. 2024. URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> (дата звернення: 08.05.2026).

23. Teremetskyi V. I., Frolova O. H., Batryn O. V., Myrza S. S., Matviichuk A. V., Ryzhenko O. S. Vectors of development of the unified medical information space. *Georgian Medical News*. 2024. No. 6 (351). P. 55–60. URL: https://www.geomednews.com/Articles/2024/6_2024/55-60.pdf.
24. Onishchenko N. M., Teremetskyi V. I., Kolesnikov A. P., Kovalchuk O. Ya., Shabalin A. V., Romas M. I. Protection of Confidential Medical Information in Ukraine: Problems of Legal Regulation. *Georgian Medical News*. 2024. No. 4 (349). P. 161–168. URL: https://www.geomednews.com/Articles/2024/4_2024/161-168.pdf.
25. Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025–2026 роки : розпорядження Кабінету Міністрів України від 09.05.2025 № 457-р. URL: <https://zakon.rada.gov.ua/laws/show/457-2025-p#Text> (дата звернення: 08.05.2026).

References

1. Kryvenko, I. P. & Chalyi, K. O. (2024). Funktsionalni mozhlyvosti medychnoho sztuchnoho intelektu dlia haluzi okhorony zdorovia ta profesiinoi osvity [Functional capabilities of medical artificial intelligence for healthcare and professional education]. *Medychna informatyka ta inzheneriia – Medical Informatics and Engineering*, 3–4, 81–96. DOI: <https://doi.org/10.11603/mie.1996-1960.2024.3-4.15462> [in Ukrainian].
2. Korotka, V. O. & Mokrynskyi, V. A. (2024). Tekhnolohii sztuchnoho intelektu v suchasni medytsyni: vprovadzhennia ta problematyka [Artificial intelligence technologies in modern medicine: implementation and issues]. *Ukrainskyi medychnyi chasopys – Ukrainian Medical Journal*, 5(163), 119–121. DOI: <https://doi.org/10.32471/umj.1680-3051.163.257497> [in Ukrainian].
3. Diorditsa, I. V. & Koval, O. M. (2024). Intehratsiia sztuchnoho intelektu v systemy zakhystu personalnykh danykh u sferi okhorony zdorovia [Integration of artificial intelligence into personal data protection systems in healthcare]. *Nauka i tekhnika sohodni – Science and Technology Today*, 5(33), 87–97. [https://doi.org/10.52058/2786-6025-2024-5\(33\)-87-97](https://doi.org/10.52058/2786-6025-2024-5(33)-87-97) [in Ukrainian].
4. Sydoruk, A. V. (2026). Derzhavna polityka tsyfrovizatsii okhorony zdorovia: administratyvno-pravovi zasady rozvytku medychnykh informatsiinykh tekhnolohii i vykorystannia sztuchnoho intelektu [State policy of healthcare digitalization: administrative and legal foundations for the development of medical information technologies and the use of artificial intelligence]. *Kyivskyi chasopys prava – Kyiv Law Journal*, 2, 143–151. DOI: <https://doi.org/10.32782/klj/2026.2.20> [in Ukrainian].
5. Vovk, A. V. (2024). Vykorystannia sztuchnoho intelektu v medytsyni [Use of artificial intelligence in medicine]. *Molod v nautsi: doslidzhennia, problemy, perspektyvy (MN-2024) – Youth in Science: Research, Problems, Prospects (MN-2024): materialy Vseukrainskoi naukovo-praktychnoi internet-konferentsii. Vinnytsia*. Retrieved from <https://conferences.vntu.edu.ua/index.php/mn/mn2024/paper/download/21267/17612> [in Ukrainian].
6. Verkhovna Rada Ukrainy (2010, June 1). *Pro zakhyst personalnykh danykh: Zakon Ukrainy № 2297-VI [On Personal Data Protection: Law of Ukraine No. 2297-VI]*. Retrieved from <https://zakon.rada.gov.ua/laws/show/2297-17#Text> [in Ukrainian].
7. Horkunenko, A. B. (2025). Shtuchnyi intelekt u medytsyni: masshtaby rynku ta napriamy rozvytku [Artificial intelligence in medicine: market scale and development directions]. *Visnyk sotsialnoi hihiieny ta orhanizatsii okhorony zdorovia Ukrainy – Bulletin of Social Hygiene and Health Protection Organization of Ukraine*, 1(103), 35–41. <https://doi.org/10.11603/1681-2786.2025.1.15340> [in Ukrainian].
8. Kabinet Ministriv Ukrainy (2018, April 25). *Deiaki pytannia elektronnoi systemy okhorony zdorovia: postanova № 411 [Some issues of the electronic healthcare system: Resolution No. 411]*. Retrieved from <https://zakon.rada.gov.ua/laws/show/411-2018-%D0%BF#Text> [in Ukrainian].
9. Hriadii, T. I. (2023). Mozhlyvosti vykorystannia sztuchnoho intelektu v osvithomu protsesi likariv-interniv [Opportunities for using artificial intelligence in the educational process of medical interns]. *Vidkryta nauka Ukrainy: viziinyi dyskurs v umovakh voiennoho stanu – Open Science of Ukraine: Visionary Discourse under Martial Law: materialy Mizhnarodnoi mizhdysyplinarnoi naukovo-praktychnoi konferentsii, Uzhhorod*, 429–431. Retrieved from <https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/54739/1/OSU2023.pdf> [in Ukrainian].
10. Verkhovna Rada Ukrainy (1992, November 19). *Osnovy zakonodavstva Ukrainy pro okhoronu zdorovia: Zakon Ukrainy № 2801-XII [Fundamentals of Ukrainian legislation on healthcare: Law of Ukraine No. 2801-XII]*. Retrieved from <https://zakon.rada.gov.ua/laws/show/2801-12#Text> [in Ukrainian].
11. Kabinet Ministriv Ukrainy (2020, December 28). *Pro skhvalennia Kontseptsii rozvytku elektronnoi okhorony zdorovia: rozporiadzhennia № 1671-r [On approval of the Concept for the development of*

- electronic healthcare: Order No. 1671-r*]. Retrieved from <https://zakon.rada.gov.ua/laws/show/1671-2020-%D1%80#Text> [in Ukrainian].
12. Kabinet Ministriv Ukrainy (2020, December 2). *Pro skhvalennia Kontseptsii rozvytku shturnoho intelektu v Ukraini: rozporiadzhennia № 1556-r [On approval of the Concept for the development of artificial intelligence in Ukraine: Order No. 1556-r]*. Retrieved from <https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text> [in Ukrainian].
 13. Kyi-Kokarieva, V. H. & Zaslavskiy, D. D. (2022). Deiaki aspekty vykorystannia shturnoho intelektu v okhoroni zdorovia [Some aspects of the use of artificial intelligence in healthcare]. *Hromadske zdorovia v Ukraini: problemy ta sposoby yikh vyrishennia – Public Health in Ukraine: Problems and Ways to Solve Them: materialy V naukovo-praktychnoi konferentsii z mizhnarodnoiu uchastiu*. Kharkiv, 106–108. DOI: <https://doi.org/10.5281/zenodo.7327653> [in Ukrainian].
 14. Boichenko, O. M. & Bublil, T. D. (2024). Perspektyvy vykorystannia shturnoho intelektu v medychnii sferi [Prospects for the use of artificial intelligence in the medical field]. *Aktualni problemy suchasnoi medytsyny – Current Problems of Modern Medicine*, 24, 3(87), 137–139. DOI: <https://doi.org/10.31718/2077-1096.24.3.137> [in Ukrainian].
 15. Rossylina, O. V. (2022). Pravovi zasady zastosuvannia shturnoho intelektu u pravovidnosynakh u sferi personalizovanoi medytsyny [Legal foundations for the use of artificial intelligence in legal relations in personalized medicine]. *Yurydychnyi visnyk – Law Herald*, 2, 156–162. <https://doi.org/10.32837/yuv.v0i2.2334> [in Ukrainian].
 16. Karpenko, O. V., Karpenko, Yu. V. & Kulhinskyi, Ye. A. (2021). Zastosuvannia tekhnolohii shturnoho intelektu u reformuvanni sfery okhorony zdorovia [Application of artificial intelligence technologies in healthcare reform]. *Derzhavne upravlinnia: udoskonalennia ta rozvytok – Public Administration: Improvement and Development*, 11. <https://doi.org/10.32702/2307-2156-2021.11.2> [in Ukrainian].
 17. Pershehuba, Ya. V. (2024). Metodolohichni pidkhody do zastosuvannia shturnoho intelektu v systemi hromadskoho zdorovia [Methodological approaches to the use of artificial intelligence in the public health system]. *Sportyvna medytsyna, fizychna terapiia ta erhoterapiia – Sports Medicine, Physical Therapy and Occupational Therapy*, 2, 128–136. <https://doi.org/10.32782/spmed.2024.2.128-136> [in Ukrainian].
 18. Verkhovna Rada Ukrainy (2023, August 9). *Pro vnesennia zmin do deiakyykh zakonodavchykh aktiv Ukrainy shchodo funktsionuvannia telemedytsyny: Zakon Ukrainy № 3301-IX [On amendments to certain legislative acts of Ukraine regarding the functioning of telemedicine: Law of Ukraine No. 3301-IX]*. Retrieved from <https://zakon.rada.gov.ua/laws/show/3301-20#Text> [in Ukrainian].
 19. Pylypets, Yu. O., Pavlov, S. V., Yaroslavskiy, Ya. I., Kostiuk, S. V. & Ursan, M. I. (2024). Osoblyvosti zastosuvannia telemedychnykh tekhnolohii na osnovi shturnoho intelektu v medytsyni katastrof [Features of the application of artificial intelligence-based telemedicine technologies in disaster medicine]. *Optyko-elektronni informatsiino-enerhetychni tekhnolohii – Optoelectronic Information-Power Technologies*, 48(2), 190–195. <https://doi.org/10.31649/1681-7893-2024-48-2-190-195> [in Ukrainian].
 20. Savyskiy, V. L., Pechyborshch, V. P., Korobkin, V. F., Dobrovol'ska, N. A., Pechyborshch, O. V. & Volianskiy, O. P. (2025). Shliakhy zastosuvannia shturnoho intelektu u viiskovii medytsyni v umovakh voiennoho stanu [Ways of using artificial intelligence in military medicine under martial law]. *Ukrainskyi zhurnal viiskovoi medytsyny – Ukrainian Journal of Military Medicine*, 6(2), 54–64. [https://doi.org/10.46847/ujmm.2025.2\(6\)-054](https://doi.org/10.46847/ujmm.2025.2(6)-054) [in Ukrainian].
 21. Verkhovna Rada Ukrainy (1994, July 5). *Pro zakhyst informatsii v informatsiino-komunikatsiinykh systemakh: Zakon Ukrainy № 80/94-VR [On Information Protection in Information and Communication Systems: Law of Ukraine No. 80/94-VR]*. Retrieved from <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text> [in Ukrainian].
 22. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). (2024). *Official Journal of the European Union*. Retrieved from <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>. [in English].
 23. Teremetskiy, V. I., Frolova, O. H., Batryn, O. V., Myrza, S. S., Matviichuk, A. V. & Ryzhenko, O. S. (2024). Vectors of development of the unified medical information space. *Georgian Medical News*, 6(351), 55–60. Retrieved from https://www.geomednews.com/Articles/2024/6_2024/55-60.pdf [in English].
 24. Onishchenko, N. M., Teremetskiy, V. I., Kolesnikov, A. P., Kovalchuk, O. Ya., Shabalin, A. V. & Romas, M. I. (2024). Protection of Confidential Medical Information in Ukraine: Problems of Legal

Regulation. Georgian Medical News, 4(349), 161–168. Retrieved from https://www.geomednews.com/Articles/2024/4_2024/161-168.pdf [in English].

25. Kabinet Ministriv Ukrainy (2025, May 9). *Pro zatverdzhennia planu zakhodiv z realizatsii Kontseptsii rozvytku sztuchnoho intelektu v Ukraini na 2025–2026 roky: rozporiadzhennia № 457-r* [On approval of the action plan for implementing the Concept for the development of artificial intelligence in Ukraine for 2025–2026: Order No. 457-r]. Retrieved from <https://zakon.rada.gov.ua/laws/show/457-2025-%D1%80#Text> [in Ukrainian].