

УДК / UDC: 34:004.8

DOI: [https://doi.org/10.37750/2616-6798.2026.1\(56\).357177](https://doi.org/10.37750/2616-6798.2026.1(56).357177)**Олег Анатолійович Заярний**Державна наукова установа “Інститут інформації, безпеки і права  
Національної академії правових наук України”

Київ, Україна,

Навчально-науковий інститут права Київського національного  
університету імені Тараса Шевченка

Київ, Україна

ResearcherID: S-3358-2018

ORCID: <https://orcid.org/0000-0003-4549-7201>

## ДО ПИТАННЯ ЗАБЕЗПЕЧЕННЯ ПРАВ ЛЮДИНИ ПРИ ФОРМУВАННІ ЗАКОНОДАВЧИХ ЗАСАД РОЗРОБКИ І ЗАСТОСУВАННЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ В УКРАЇНІ

***Анотація.** У статті досліджуються окремі проблеми забезпечення дотримання прав людини у контексті формування в Україні законодавчих засад регулювання суспільних відносин, пов'язаних із розробкою і застосуванням систем штучного інтелекту. З огляду на стрімкий розвиток алгоритмічних систем та їхню інтеграцію у сфери публічного управління, судочинства та приватноправових відносин, у статті значну увагу приділено ризико-орієнтованому підходу, закладеному в Регламенті ЄС 2024/1689 (AI Act). Поряд з цим, у роботі проаналізовано статистичні показники системних ризиків для фундаментальних прав людини, зокрема права на приватність, недискримінацію у зв'язку із застосуванням штучного інтелекту та на кібербезпеку у цифровому середовищі. Висвітлено авторський погляд щодо структури майбутнього Закону України “Про регулювання штучного інтелекту” та охарактеризовано систему засобів правового забезпечення дотримання прав людини у відповідній сфері правового регулювання.*

*Також, у статті розвинено науковий погляд про необхідності гармонізації національного законодавства з Рамковою конвенцією Ради Європи “Про штучний інтелект, права людини, демократію і верховенство права” та стандартами Європейського Союзу у сфері прав людини.*

*У висновках викладено рекомендації щодо розробки майбутнього Закону України “Про регулювання штучного інтелекту”, запропонований комплекс заходів, спрямованих на практичну реалізацію ризико-орієнтованого підходу в управлінні і регулюванні систем штучного інтелекту.*

***Ключові слова:** штучний інтелект, права людини, законодавче регулювання, цифрова трансформація, кібербезпека, Акт про ШІ, європейська інтеграція, ризико-орієнтований підхід.*

**Oleh A. Zaiarnyi**

State Scientific Institution "Institute of Information, Security and Law  
of the National Academy of Legal Sciences of Ukraine"

Kyiv, Ukraine

Institute of Law of Taras Shevchenko National University of Kyiv

Kyiv, Ukraine

ResearcherID: S-3358-2018

ORCID: <https://orcid.org/0000-0003-4549-7201>

## ON ENSURING HUMAN RIGHTS IN THE FORMATION OF THE LEGISLATIVE FRAMEWORK FOR THE DEVELOPMENT AND APPLICATION OF ARTIFICIAL INTELLIGENCE SYSTEMS IN UKRAINE

***Summary.** This article explores key challenges in safeguarding human rights in the context of the emerging legislative framework governing the development and deployment of artificial intelligence systems in Ukraine. Against the backdrop of the rapid evolution of algorithmic technologies and their growing integration into public administration, judicial decision-making, and private-law relations, particular emphasis is placed on the risk-based regulatory approach embodied in Regulation (EU) 2024/1689 (the AI Act).*

*The study further examines statistical evidence of systemic risks posed by artificial intelligence to fundamental human rights, with a specific focus on the right to privacy, the principle of non-discrimination, and cybersecurity in the digital environment. The article articulates the author's conceptual vision for the structure of a prospective Law of Ukraine "On the Regulation of Artificial Intelligence" and outlines a coherent system of legal instruments to ensure effective human rights protection in this regulatory domain.*

*In addition, the article advances the scholarly argument for aligning national legislation with the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, as well as with relevant European Union human rights standards.*

*The conclusions offer practical recommendations for drafting the future Law of Ukraine "On the Regulation of Artificial Intelligence" and propose a comprehensive set of measures to operationalize a risk-based approach to the governance and regulation of artificial intelligence systems.*

***Keywords:** artificial intelligence, human rights, legislative regulation, digital transformation, cybersecurity, AI Act, European integration, risk-based approach.*

**Постановка проблеми.** Сучасний етап розвитку інформаційного суспільства характеризується широким впровадженням систем штучного інтелекту (далі — ШІ) у різні сфери діяльності. Алгоритмічні системи стають невід'ємною складовою соціально-економічного, науково-технічного та оборонного розвитку сучасної держави і суспільства. Це особливо відчутно в умовах цифрової трансформації України, яка відбувається на тлі повномасштабної війни та європейської інтеграції [1].

Згідно із останніми аналітичними дослідженнями розвитку ІТ-індустрії в Україні, національний ІТ-сектор демонструє активність у розробці ШІ-рішень, зокрема у сфері кібербезпеки та технологій оборонного призначення [2].

Водночас, поряд із широкими можливостями для розвитку електронного урядування, цифрової економіки та інноваційних напрямів промисловості, ШІ створює значні ризики для прав людини. У зв'язку з цим, перед Україною, аналогічно до більшості сучасних держав гостро постала проблема щодо необхідності формування ефективного законодавчого підґрунтя регулювання суспільних відносин, пов'язаних з розробкою і застосуванням систем ШІ у різних сферах суспільного життя.

Відсутність цілісного нормативного регулювання у цій сфері породжує низку інституційних проблем. Їх сутність передусім проявляється через відсутність чітких законодавчих правил реалізації ризико-орієнтованого підходу у застосуванні ШІ, невизначеності регуляторних підходів до здійснення підприємницької діяльності у сфері розробки і впровадження автоматизованих рішень на основі ШІ, необхідності запровадження спеціальних заходів з протидії кіберзагрозам на рівні проектування усіх ІТ-систем та технічного захисту даних за принципом безпечної обробки [3, с. 211].

Незважаючи на здійснення міжнародними організаціями, зокрема, Радою Європи, Організацією з економічного співробітництва і розвитку системи заходів, спрямованих на подолання основних груп ризиків, пов'язаних із розвитком ШІ, глобальні статистичні дані демонструють стрімке зростання системних ризиків для фундаментальних прав людини [4, с. 18].

Згідно з аналітичними матеріалами Європейської комісії, близько 60% інструментів ШІ, що використовуються у сфері рекрутингу та найму, потенційно можуть посилювати гендерні або етнічні упередження за відсутності належного моніторингу [5, с. 16].

У фінансовому секторі дослідження 2024 року виявило, що 43% автоматизованих кредитних рішень містять необґрунтовані розбіжності, які негативно впливають на маргіналізовані групи населення [6, с. 14]. Більш того, звіти Європолу (ІОСТА 2024, 2025) вказують на те, що ШІ стає активним засобом вчинення кіберзлочинів: від створення високоякісних фішингових кампаній до генерації дипфейків з метою вимагання та поширення матеріалів сексуального насильства над дітьми [7, с. 9; 8, с. 17].

Для України, як кандидата на вступ до Європейського Союзу, адаптація національного законодавства до Регламенту ЄС 2024/1689 (далі – Акт “Про штучний інтелект”) [9] та Рамкової конвенції Ради Європи “Про штучний інтелект, права людини, демократію і верховенство права” [10] є не лише юридичним зобов'язанням, а й стратегічною передумовою захисту національних інтересів у цифровому просторі. Це потребує глибокого доктринального аналізу та розробки правових механізмів, які б забезпечували баланс між стимулюванням інновацій та неухильним дотриманням прав і свобод людини.

**Аналіз останніх досліджень і публікацій.** На сьогоднішній день, проблема забезпечення дотримання прав людини у сфері розробки і застосування систем ШІ є предметом наукових досліджень багатьох вчених-правників і практиків у галузі інформаційного права.

Так, М. В. Дубняк проводить системний аналіз законодавства ЄС про штучний інтелект, визначаючи ключові напрями гармонізації національного механізму правового регулювання у цій сфері діяльності суспільства. У своїх роботах дослідниця робить значний акцент на проблемах визначення правового режиму об'єктів, створених за допомогою нейромереж, та правових аспектах цифрової трансформації юридичних послуг. Її підхід ґрунтується на необхідності запровадження критеріїв поділу технологій за ступенем ризику та забезпечення кібербезпеки в інформаційних системах [11; 12].

Досліджуючи проблематику, порушену у межах цієї статті, В.Г. Пилипчук зосереджується серед іншого на питаннях інформаційної безпеки та етичних засадах використання алгоритмічних систем. У наукових роботах під його редакцією досліджуються проблеми протидії системним кіберзагрозам, викликаним застосуванням ШІ та розробки стратегій розвитку галузі з урахуванням національної безпеки [13].

У своїх публікаціях Я. О. Берназюк детально висвітлює виклики, які ШІ становить для процесуальних прав сторін судових спорів, ефективності здійснення правосуддя

загалом. Його дослідження акцентують увагу на неприпустимості зловживання процесуальними правами через використання ШІ та необхідності збереження людського контролю над судовими рішеннями відповідно до статті 6 Конвенції Про захист прав людини і основоположних свобод [14; 15].

У свою чергу, О.В. Костенко досліджує вплив розвитку ШІ на право на приватність, підкреслюючи загрози масового збору даних та втрати контролю над особистою інформацією. Його праці присвячені правовим аспектам Інтернету речей (IoT), метавсесвіту та цифровій ідентичності, що є критично важливим для розуміння нових форм порушень прав людини [16].

Питанням дотримання прав людини у відносинах, які виникають при застосуванні систем ШІ також присвячені окремі публікації С. В. Кравчука [17].

Незважаючи на значний інтерес до проблематики забезпечення дотримання прав людини у контексті формування законодавчих засад розвитку систем ШІ в Україні, існують окремі дискусійні аспекти порушеної проблематики, які вимагають проведення додаткового наукового дослідження. Йдеться, зокрема, про питання законодавчого закріплення комплексу заходів, спрямованих на легалізацію ризико-орієнтованого підходу у виборі моделей ШІ, які можуть бути застосовані до людини, визначення системи гарантій захисту прав людини від безпідставного застосування ШІ, формулювання структурних частин майбутнього проекту Закону України “Про регулювання штучного інтелекту”, предмет регулювання яких буде безпосередньо спрямований на дотримання прав людини при застосуванні цифрових рішень на основі алгоритмічних систем.

**Метою статті** є дослідження правових засад забезпечення прав людини при формуванні законодавчого регулювання розробки та застосування систем штучного інтелекту в Україні, визначення основних викликів, зумовлених алгоритмічними ризиками, та розробка рекомендацій щодо структури майбутнього спеціального закону на основі міжнародних стандартів та вітчизняної правової доктрини.

**Виклад основного матеріалу.** Однією із основних передумов формування законодавчих засад регулювання ШІ в Україні є системний аналіз реальних та потенційних загроз, які ця технологія несе в собі для прав людини, правопорядку і національної безпеки загалом.

За своєю природою Системи ШІ належать до непрозорих технологій, часто із подвійним суспільним призначенням, що створює труднощі в оцінці логіки прийняття рішень та визначенні відповідальних осіб у разі заподіяння шкоди [18, с. 24].

Згідно з дослідженнями Агентства ЄС з фундаментальних прав (FRA), використання ШІ у сферах з високим ризиком — таких як правосуддя, правоохоронна діяльність, освіта та соціальне забезпечення — може призвести до системних порушень права на недискримінацію, приватність та людську гідність. Статистичні показники демонструють, що ризики є цілком реальними та мають тенденцію до масштабування [19, с. 27; 20, с. 14 - 17].

**Таблиця 1. Ризики ШІ для прав людини: статистичний огляд**

Сфера застосування ШІ	Тип ризику / Статистичний показник	Джерело даних
<b>Фінансовий сектор</b>	43% автоматизованих кредитних рішень виявляють необґрунтовану дискримінацію маргіналізованих груп	EU Oversight Study 2024

Сфера застосування ШІ	Тип ризику / Статистичний показник	Джерело даних
Рекрутинг та HRM	60% інструментів відбору кандидатів можуть посилювати гендерні або етнічні упередження	European Commission Analysis 2024
Правоохоронна діяльність	72% опитаних правоохоронців ЄС вказують на етичні та правові обмеження як бар'єр для використання ШІ	ALIGNER Project / FRA 2024
Кібербезпека	Зростання кількості повідомлень про ШІ-генерацію CSAM на 380% у 2024 році порівняно з попереднім роком	Europol / IWF 2024
Охорона здоров'я	Прогноз зростання витрат на цифровізацію до 4,8% ВВП ЄС до 2060 року при ризиках цифрової нерівності	JOLAS / World Bank 2024

У контексті наведених статистичних показників порушення прав людини істотну занепокоєність викликає застосування систем ШІ для біометричного спостереження у громадських місцях, на робочих місцях, у секторі надання послуг.

Такі заходи за своїм проявом не лише можуть мати наслідком надмірне втручання у приватне життя людини, але і викликати ризики безпідставного обмеження інших фундаментальних громадянських прав, зокрема, на мирні зібрання, на вираження власних переконань, свободу вибору форми отримання інформації, тощо [21].

За своїм змістом поняття “дотримання прав людини” в контексті ШІ означає не лише формальне утримання держави від втручання у права осіб, а й позитивне зобов'язання щодо формування такої правової і технічної основи, яка б забезпечувала захист гідності, свободи та рівності людини на кожному етапі життєвого циклу систем ШІ.

Спираючись на раніше отримані нами результати наукових досліджень проблематики правового регулювання у сфері застосування ШІ [22, с. 2369], можна стверджувати, що підґрунтя для нормативної і технічної основи дотримання прав людини можуть складати саме нормативний, правозастосовчий і фактичний критерії оцінки правомірності поведінки з відповідною технологією. При цьому, важливо, щоб спираючись на існуючі законодавчі підходи до регулювання штучного інтелекту, вказані критерії оцінювалися у кожному конкретному випадку спираючись на ризико-орієнтований, людиноцентричний підхід до застосування систем ШІ.

Міжнародні технічні стандарти перед усім виходять з того, що надійність системи ґрунтується на трьох компонентах: законність, етичність та технічна стійкість.

Разом з тим, практичне втілення усіх трьох із перелічених компонентів, на нашу думку може бути ефективним у контексті дотримання прав людини лише за умови впровадження механізмів “людського нагляду”, які дозволяють втручатися в роботу системи та скасовувати її рішення [23].

Україна, яка є членом Спеціального комітету із штучного інтелекту при Раді Європи, у жовтні 2019 року приєдналася до Рекомендацій Організації економічного співробітництва і розвитку з питань штучного інтелекту, що діють в редакції від 23 березня 2024 року [24].

Поряд з цим, як рекомендацій цієї міжнародної організації, зокрема від 08 квітня 2020 року “Про вплив алгоритмічних систем на права людини [25]”.

Зазначені міжнародні акти м'якого права закріплюють ряд правових засобів, спрямованих на забезпечення дотримання прав людини у сфері розробки і застосування систем ШІ.

Поряд із необхідністю впровадження людського нагляду на всіх стадіях життєвого циклу вказаних технологій, акти міжнародного права передбачають правила про необхідність обов'язкової поінформованої згоди про застосування ШІ, встановлення гарантій захисту від автоматизованого прийняття рішень, права на заборону автоматизованої обробки даних з використанням ШІ, запровадження механізму розмежування юридичної відповідальності розробників, постачальників, операторів і замовників рішень, заснованих на вказаних технологіях.

Єдиним законодавчим актом на рівні ЄС, що комплексно унормовує застосування ШІ) та має екстериторіальну дію, є Акт ЄС “Про ШІ” [9], який набрав чинності 1 серпня 2024 року.

До ухвалення Закону та вироблення уніфікованих підходів до унормування використання ШІ вирізнялися комплексністю й ґрунтувалися на низці актів рекомендаційного характеру, прийнятих керівними інституціями ЄС, серед яких: Резолюція Європейського Парламенту з рекомендаціями Комісії з норм цивільного права щодо робототехніки 2015/2103(INL) [26], Повідомлення Європейської Комісії до Європейського Парламенту, Європейської Ради, Ради Європейського економічного та соціального Комітету та Комітету регіонів “Штучний інтелект для Європи” [27], Рекомендації Експертної групи високого рівня з штучного інтелекту з етики для надійного ШІ [28], Рекомендація Комітету міністрів Ради Європи Cm/res (2020)1 державам-членам щодо впливу алгоритмічних систем на права людини [29], Звіт Європейської Комісії про наслідки для безпеки і відповідальності ШІ, Інтернету речей та робототехніки [30].

Враховуючи потенційні ризики та можливі негативні впливи використання ШІ у площині гарантування й забезпечення основних прав людини та етичних норм, всі ці документи містять пропозиції щодо їх дотримання. Зокрема, Резолюція Європейського Парламенту 2015/2103 (INL) стала підґрунтям для запровадження єдиних правових стандартів і розробки конкретних правових інструментів використання ШІ на території ЄС. У ній передбачені засади неухильного дотримання законодавства про захист персональних даних та способи подолання проблем залежності людини від технічних приладів. У Рекомендаціях Експертної групи високого рівня з ШІ з етики для надійного ШІ також визначені основні принципи його використання: орієнтованість на людину, тобто системи ШІ повинні розроблятися, використовуватися й контролюватися, забезпечуючи дотримання основних прав людини та етичних норм. “Надійний ШІ” вимагає, щоб алгоритми були законними, безпечними, надійними та досить стійкими, щоб справлятися з помилками або невідповідностями на всіх етапах циклу системи ШІ. Рекомендації містять 7 ключових вимог, яким мають відповідати системи ШІ, щоб вважатися надійними: 1) людські права та нагляд; 2) технічна надійність і безпека; 3) конфіденційність й управління даними; 4) прозорість; 5) різноманітність, відсутність дискримінації та справедливості; 6) суспільне та екологічне благополуччя; 7) підзвітність. Рекомендація Комітету Міністрів Ради Європи Cm/res (2020)1 державам-членам щодо впливу алгоритмічних систем на права людини містить зобов'язання держав щодо захисту й заохочення прав людини та основних свобод у контексті алгоритмічних систем.

Базуючись на цих напрацюваннях, положеннями Акту “Про ШІ” встановлено єдині зобов’язання для операторів і гарантії однакового захисту суспільного інтересу та прав осіб на всьому внутрішньому ринку на основі статті 114 Договору про функціонування ЄС.

Нормами Акту “Про ШІ” передбачено диференційоване законодавче регулювання використання систем ШІ залежно від так званої “зони ризику”: неприйнятний ризик, високий ризик, обмежений ризик та мінімальний ризик. Залежно від “зони ризику”, у розділі II Закону викладено заборонені практики використання систем ШІ на території ЄС. Заборони охоплюють практики, які мають значний потенціал для маніпулювання людьми за допомогою підсвідомих методів або використання вразливості конкретних груп, зокрема дітей чи осіб з обмеженими можливостями, з метою суттєвого спотворення їх поведінки таким чином, що це може спричинити шкоду їх психологічному чи фізичному здоров’ю та/або негативно вплинути на інших.

Загалом, підхід, який застосовується у положеннях Акту “Про ШІ” стосовно прав людини при використанні систем ШІ, виявляється в тому, що ці системи не можуть створювати істотніші ризики для людини порівняно з традиційними підходами гарантування її прав та свобод, які реалізуються у традиційний спосіб.

У нормах Акту “Про ШІ”, серед іншого, заборонено дізнаватися про расову приналежність людини, її сексуальну орієнтацію чи переконання за допомогою біометричних даних. Також правоохоронні органи не повинні використовувати ШІ для прогнозування злочинів.

Прийняття Європейським Парламентом уніфікованого, комплексного законодавчого акту, обов’язкового для усіх держав-членів ЄС фактично стало підґрунтям для розробки і прийняття перших міжнародних договорів зобов’язального характеру у цій сфері правового регулювання.

Першим міжнародним юридично обов’язковим договором, що регулює ШІ, стала Рамкова Конвенція Ради Європи “Про права людини, штучний інтелект, демократію та верховенство права” [10], яку Україна підписала 15 травня 2025 року.

Метою цієї Конвенції є забезпечення дотримання прав людини, принципів демократії та верховенства права у всьому життєвому циклі систем ШІ.

Конвенція містить низку ключових зобов’язань для держав-учасниць:

1) **Обов’язки держав щодо регулювання ШІ.** Встановлення належного законодавчого та адміністративного регулювання відповідно до рівня ризиків, пов’язаних із ШІ.

2) **Принципи відповідального використання ШІ.** Прозорість, підзвітність, недискримінація, захист приватності та безпека алгоритмічних систем.

3) **Захист демократичних інституцій.** Запобігання використанню ШІ для маніпуляцій громадською думкою, цензури або незаконного стеження.

4) **Право на оскарження рішень ШІ.** Користувачі повинні мати доступ до інформації про використання ШІ та механізмів оскарження рішень, прийнятих системами ШІ.

5) **Нагляд та міжнародна співпраця.** Створення незалежного наглядового механізму в кожній країні та обмін досвідом між державами-учасницями.

На нашу думку, виконання Україною зобов’язань за вказаною Конвенцією буде сприяти формуванню чіткого, послідовного механізму законодавчого забезпечення розробки і застосування систем ШІ, заснованого на засадах пріоритету прав людини, верховенства права, дотримання моральних засад розвитку суспільства.

Відповідно до Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, для України, як кандидата у прийняття до Європейського Союзу, адаптація національного законодавства до законодавства Європейського Союзу є пріоритетним завданням внутрішньої і зовнішньої політики, зокрема і щодо сфери розвитку систем ШІ.

Розв'язання вказаних та багатьох інших проблем у сфері цифрової трансформації суспільства, держави, територіальних громад і національної економіки загалом потребує прийняття окремого Закону України, нормами якого будуть врегульовані особливості розробки і застосування систем ШІ в різних сферах суспільного життя, визначені обмеження і заборони на використання цієї технології у випадку створення значних ризиків для прав і свобод людини, закладені спеціальні умови обробки персональних даних і управління великими даними на основі цієї технології.

У цьому контексті Україна демонструє активну державну позицію. У 2020 році Розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р була схвалена Концепція розвитку штучного інтелекту в Україні [31].

Проте справжня інтенсифікація процесу відбулася у 2023–2024 роках, коли Міністерство цифрової трансформації презентувало Дорожню карту регулювання ШІ та “Білу книгу” [32; 33].

Стратегія України передбачає двоетапний підхід: спочатку створення інструментів м'якого права, а згодом — розробка та прийняття Закону України про штучний інтелект, який буде гармонізований з Актом ЄС “Про ШІ”. Важливою ініціативою є використання “регуляторних пісочниць”, що дозволяють компаніям тестувати ШІ-рішення під наглядом держави.

Регуляторна пісочниця передбачає створення контрольованого середовища, де інноваційні ШІ-рішення можуть тестуватися з тимчасовим послабленням окремих регуляторних вимог. Це дозволяє державі отримувати практичний досвід застосування технологій, а бізнесу — перевіряти свої рішення до їх масового впровадження. Така модель успішно функціонує в країнах ЄС, Великій Британії та Сінгапурі.

Для України запровадження регуляторних пісочниць може стати важливим інструментом забезпечення балансу між інноваціями та захистом прав людини.

Разом із легалізованими в нормах міжнародного права засобами дотримання прав людини, вказані інноваційні рішення можуть створити ефективне правове, економічне і технічне підґрунтя для зниження ризиків порушення прав людини на усіх стадіях розробки і застосування ШІ.

Водночас, на нашу думку, важливо, щоб поряд із реалізацією законодавчих ініціатив, правозастосовчою діяльністю у сфері застосування ШІ відбувалося дотримання професійних етичних норм у відповідній сфері регулювання.

**Висновки.** Проведене дослідження дозволяє сформулювати наступні висновки і рекомендації:

1. Законодавче забезпечення ШІ в Україні є фундаментальною умовою цифрової трансформації держави та її інтеграції до європейського правового простору. Наявність ефективного механізму правового регулювання у цій сфері буде сприяти зниженню кількості порушень прав людини, обумовлених застосуванням ШІ та створить передбачуване середовище для розробників і користувачів ШІ-систем.

2. На нашу думку, ризико-орієнтований підхід Акту про ШІ має стати основою для національної законодавчої ініціативи, з чітким розмежуванням сфер застосування



ШІ за ступенем небезпеки. Класифікація систем за рівнями ризику дозволить диференціювати регуляторні вимоги та забезпечити пропорційність втручання держави.

3. Статистичні дані підтверджують зростання системних ризиків алгоритмічної дискримінації (43% у фінансовому секторі, 60% у сфері найму) та кіберзлочинності (зростання ШІ-генерованого CSAM на 380%), що вимагає впровадження обов'язкової оцінки впливу на фундаментальні права людини для систем високого ризику.

4. Дотримання прав людини має трактуватися як позитивне зобов'язання держави забезпечити підконтрольність, прозорість та підзвітність алгоритмічних систем через механізми людського нагляду. Це включає право на пояснення автоматизованих рішень, можливість їх оскарження та чіткі процедури визначення відповідальності.

5. Запровадження регуляторних пісочниць є необхідним кроком для забезпечення балансу між стимулюванням інновацій та забезпеченням безпеки. Контрольоване середовище для тестування дозволить накопичити практичний досвід регулювання до масового впровадження технологій.

6. Створення Національного агентства з ШІ та координація з європейськими структурами забезпечить ефективну імплементацію регуляторних вимог та сприятиме інтеграції України до єдиного цифрового ринку ЄС.

**ПОДЯКИ:** Немає

**КОНФЛІКТ ІНТЕРЕСІВ:** Немає

### Список використаних джерел

1. Як Україна використовує штучний інтелект у війні з Росією — The Economist. *Texty.org.ua*. 2024. URL: <https://texty.org.ua/fragments/112210/> (дата звернення: 19.01.2026).

2. Штучний інтелект може бути ключем до перемоги України у війні – західні експерти. *Радіо Свобода*. 2024. URL: <https://www.radiosvoboda.org/a/32785722.html> (дата звернення: 19.01.2026).

3. Заярний О. А. Законодавче забезпечення розробки і застосування технологій штучного інтелекту в умовах війни та європейської інтеграції України *Правове забезпечення євроінтеграції: загальноправовий та галузевий аспекти* : колективна монографія. – Рига : Baltija Publishing, 2025. – С. 207–224. URL: <http://www.baltijapublishing.lv/omp/index.php/bp/catalog/view/597/16071/33923-1> (дата звернення: 19.01.2026)

4. Risk Management Profile for Artificial Intelligence and Human Rights: Profile. *U.S. Department of State*. 2024. 32 p. URL: <https://2021-2025.state.gov/risk-management-profile-for-ai-and-human-rights/> (дата звернення: 19.01.2026).

5 Assessing High-risk Artificial Intelligence: Fundamental Rights Risks. *European Union Agency for Fundamental Rights (FRA)*. 2024. 74 p. URL: <https://fra.europa.eu/en/publication/2024/assessing-high-risk-artificial-intelligence-fundamental-rights-risks> (дата звернення: 19.01.2026).

6. AI regulations to watch in 2026: a complete and plain-language guide to Europe's changing AI rules. *Accurate Legal Billing*. 2024. URL: <https://www.accuratelegalbilling.com/articles/ai-regulations-to-watch-in-2026-a-complete-and-plainlanguage-guide-to-europes-changing-ai-rules> (дата звернення: 19.01.2026).

7. Internet Watch Foundation. AI-generated CSAM reports rise 380% in 2024. *RedCompass Labs Insights*. 2025. URL: <https://www.redcompasslabs.com/insights/child-exploitation-payments-europols-iocta-report/> (дата звернення: 19.01.2026).

8. Internet Organised Crime Threat Assessment (IOCTA) 2024. *Europol*. 2024. URL: <https://www.europol.europa.eu/publications-events/main-reports/iocta-report> (дата звернення: 19.01.2026).

9. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (дата звернення: 19.01.2026).

10. Рамкова Конвенція Ради Європи «Про штучний інтелект, права людини, демократію та верховенство права». Відкрита для підписання 26.03.2024 року. URL: <https://rm.coe.int/-1493-10-1b-committee-on-artificial-intelligence-cai-b-draft-framework/1680aee411> (дата звернення: 19.01.2026).

11. Дубняк М. В. Відкриті дані та пояснювальний штучний інтелект: правові перспективи. *Інформація і право*. 2024. № 2 (49). С. 102–117. URL: <http://il.ippi.org.ua/article/view/306147> (дата звернення: 19.01.2026).

12. Дубняк М. В., Соловійова В. С. Цифрова трансформація юридичних послуг. *Інформація і право*. 2022. № 2 (41). С. 52–57. URL: <http://il.ippi.org.ua/article/view/270363> (дата звернення: 19.01.2026).

13. Пилипчук В. Г., Баранов О. А., Гиляка О. С. Проблема правового регулювання у сфері штучного інтелекту в контексті розвитку законодавства Європейського Союзу. *Вісник Національної академії правових наук України*. 2022. Т. 329, № 2. С. 35 – 61.

14. Берназюк Я. Штучний інтелект та система правосуддя України: результати співпраці у році, що минув. *Constitutionalist*. 2024. URL: <https://so.supreme.court.gov.ua/authors/934/shtuchnyi-intelekt-ta-systema-pravosuddia-ukrainy> (дата звернення: 19.01.2026).

15. Берназюк Я. Ера ШІ й роль верховних судів у цифровій трансформації правосуддя. *Юридична Газета*. 2024. URL: <https://yur-gazeta.com/publications/practice/sudova-praktika/era-shi-y-rol-verhovnih-sudiv-u-cifroviy-transformaciyi-pravosuddya.html> (дата звернення: 19.01.2026).

16. Костенко О. В. Електронна юрисдикція, метавесвіт, штучний інтелект, цифрова особистість: теорія, практика, перспективи. *Наукові інновації та передові технології*. 2022. № 4. С. 75–90.

17. Кравчук С. В. Вплив штучного інтелекту на права людини та загальні рекомендації для сталого втілення. *Вісник Національного університету “Львівська політехніка”*. Серія: “Юридичні науки”. – 2024. – № 3 (43). – С. 101–110. – URL: <https://science.lpnu.ua/sites/default/files/journal-paper/2024/oct/36048/17.pdf>. – DOI: <http://doi.org/10.23939/law2024.43.101>. (science.lpnu.ua)

18. The Effects of Artificial Intelligence on Human Rights: Report. *Western Balkans Fund*. 2024. 34 p. URL: <https://westernbalkansfund.org/wp-content/uploads/2024/12/ITS-The-Effects-of-Artificial-Intelligence-on-Human-Rights-Final-EN.pdf> (дата звернення: 19.01.2026).

19. Assessing High-risk Artificial Intelligence: Fundamental Rights Risks. *European Union Agency for Fundamental Rights (FRA)*. 2024. 74 p. URL:

<https://fra.europa.eu/en/publication/2024/assessing-high-risk-artificial-intelligence-fundamental-rights-risks> (дата звернення: 19.01.2026).

20. Digitalising Justice: A fundamental rights-based approach. *European Union Agency for Fundamental Rights (FRA)*. 2024. 68 p. URL: <https://fra.europa.eu/en/publication/2024/digitalising-justice-fundamental-rights-based-approach> (дата звернення: 19.01.2026).

21. ALIGNER Fundamental Rights Impact Assessment: Ensuring compliance of law enforcement AI systems. *AI and Ethics*. 2024. Vol. 4. P. 1569–1582. URL: <https://doi.org/10.1007/s43681-024-00445-5> (дата звернення: 19.01.2026).

22. Oleh A. Zaiarnyi. Assessment criteria for the lawfulness of artificial intelligence technologies application in health care. *Wiadomości Lekarskie* 2019, tom LXXII, nr 12 cz. II. P. 2568–2572. URL: [https://www.researchgate.net/publication/339723357\\_Assessment\\_criteria\\_for\\_the\\_lawfulness\\_of\\_artificial\\_intelligence\\_technologies\\_application\\_in\\_health\\_care](https://www.researchgate.net/publication/339723357_Assessment_criteria_for_the_lawfulness_of_artificial_intelligence_technologies_application_in_health_care) (дата звернення: 19.01.2026).

23. Recommendation of the Council on Artificial Intelligence: OECD/LEGAL/0449. *Organisation for Economic Co-operation and Development*. 2024. 12 p. URL: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> (дата звернення: 19.01.2026).

24. World Organization for Security and Economic Development. Recommendations of the Artificial Intelligence Council of the World Organization for Security and Economic Development on the guidelines of artificial intelligence, 22 May 2019. Available at: <https://legalinstruments.oecd.org/> (дата звернення: 19.01.2026).

25. Рада Європи. Рекомендація CM/Rec(2020)1 Комітету Міністрів державам-членам щодо впливу алгоритмічних систем на права людини: ухвалено Комітетом Міністрів 8 квітня 2020 р. URL: [https://search.coe.int/cm/Pages/result\\_details.aspx?ObjectId=09000016809e1154](https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016809e1154) (дата звернення: 19.01.2026)

26. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). URL: [https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html) (дата звернення: 19.01.2026).

27. European Commission. (2018). Communication Artificial Intelligence for Europe. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN> (дата звернення: 19.01.2026).

28. AI HLEG. (2019). Ethics guidelines for a trustworthy AI. URL: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai> ; Ethics guidelines for trustworthy AI. URL: <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> (дата звернення: 19.01.2026).

29. European Commission. (2020). White Paper On Artificial Intelligence – A European approach to excellence and trust, Brussels, 19.02.2020, COM (2020) 65 final. URL: [https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust\\_en](https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en) (дата звернення: 19.01.2026).

30. European Commission. (2020). Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics. COM/2020/64 final. URL: <https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1593079180383&uri=CELEX%3A52020DC0064> (дата звернення: 19.01.2026).

31. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. *Урядовий портал*. 2020. URL: <https://www.kmu.gov.ua/npras/pro-shvalennya-koncersiyi-rozvitku-shtuchnogo-intelektu-v-ukrayini-s21220> (дата звернення: 19.01.2026).

32. Дорожня карта з регулювання штучного інтелекту в Україні. *Міністерство цифрової трансформації України*. 2023. URL: <https://thedigital.gov.ua/news/regulyuvannya-shtuchnogo-intelektu-v-ukraini-prezentuemo-dorozhnyu-kartu> (дата звернення: 19.01.2026).

33. Біла книга з регулювання ШІ в Україні: бачення Мінцифри. *Міністерство цифрової трансформації України*. 2024. URL: <https://thedigital.gov.ua/news/regulyuvannya-shtuchnogo-intelektu-v-ukraini-prezentuemo-bilu-knigu> (дата звернення: 19.01.2026).

### **Олег Анатолійович Заярний**

доктор юридичних наук, професор

головний науковий співробітник наукової лабораторії інформаційних прав та безпеки людини наукового центру інформації і права Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України»

04053, Україна, м. Київ, пров. Несторівський, 4

професор кафедри інтелектуальної власності та інформаційного права Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка

01601, Україна, м. Київ, вул. Володимирська, 60

*email: oleganalitik.knu@gmail.com*

### **Oleh A. Zaiarnyi**

Doctor of Law, Professor

Chief Research Fellow of the Research Laboratory of Information Rights and Human Security, Research Center of Information and Law

State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine"

4 Nestorivskyi Lane, Kyiv, 04053, Ukraine

Professor of the Department of Intellectual Property and Information Law

Institute of Law of Taras Shevchenko National University of Kyiv

60 Volodymyrska Street, Kyiv, 01601, Ukraine

*email: oleganalitik.knu@gmail.com*

**Рекомендоване цитування:** Заярний О.А. До питання забезпечення прав людини при формуванні законодавчих засад розробки і застосування систем штучного інтелекту в Україні. *Інформація і право*. № 1(56)/2026. 2026. С. 42-53. [https://doi.org/10.37750/2616-6798.2026.1\(56\).357177](https://doi.org/10.37750/2616-6798.2026.1(56).357177)

**Suggested Citation:** Zaiarnyi O.A. (2026) On Ensuring Human Rights in the Formation of the Legislative Framework for the Development and Application of Artificial Intelligence Systems in Ukraine. *Information and Law*. 1(56)/2026. 42-53. [https://doi.org/10.37750/2616-6798.2026.1\(56\).357177](https://doi.org/10.37750/2616-6798.2026.1(56).357177)

Дата надходження статті до редакції: 05.02.2026 р.

Дата прийняття статті до друку після рецензування: 09.02.2026 р.

Дата публікації (оприлюднення): 01.04.2026 р.