УДК 347.5:004.8
DOI https://doi.org/10.24144/2307-3322.2025.92.3.10

ПРАВОВА ВІДПОВІДАЛЬНІСТЬ ЗА ДІЇ ШТУЧНОГО ІНТЕЛЕКТУ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ РЕГУЛЮВАННЯ.

Гнідовський М.С.,
здобувач вищої освіти III курсу хіміко-технологічного факультету
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»
ORCID: 0009-0009-9953-0637
e-mail: maxhnidovskiy@ukr.net

Сергієнко М.А.,
здобувачка вищої освіти III курсу хіміко-технологічного факультету
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»
ORCID: 0009-0009-3265-3501
e-mail: sergienkomaruna06@gmail.com

Лук'янчиков Б.Є.,
кандидат юридичних наук, доцент,
доцент кафедри інформаційного, господарського та адміністративного
права Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»
ORCID: 0000-0002-4761-5980
e-mail: boryn1971@gmail.com

Гнідовський М.С., Сергієнко М.А., Лук'янчиков Б.Є. Правова відповідальність за дії штучного інтелекту:виклики та перспективи регулювання.

У статті досліджується проблема визначення правової відповідальності за шкоду, завдану системами штучного інтелекту (ШІ), з огляду на зростання їх автономності та здатності ухвалювати рішення без прямого втручання людини. Проаналізовано сучасні підходи до регулювання таких правовідносин у ЄС, США та Україні, а також тенденцію до формування глобальної моделі, що забезпечує баланс між інноваційністю технологій і захистом прав людини. Значну увагу приділено питанню розподілу відповідальності між розробниками, виробниками, постачальниками даних, власниками, операторами й користувачами, а також дискусіям щодо можливості надання автономним системам окремих елементів правосуб'єктності.

Окреслено особливості застосування ШІ у високоризикових сферах – автономному транспорті, медицині, фінансах, безпеці та державному управлінні, де технічні збої або алгоритмічна упередженість можуть спричинити значні збитки чи порушення прав людини. Проведено порівняльний аналіз моделей відповідальності: суворої (об'єктивної), спільної, пропорційної та страхової, які використовуються у провідних юрисдикціях.

На основі досвіду ЄС розглянуто ключові положення Регламенту про ШІ (AI Act), що запроваджує ризик-орієнтовану систему контролю та встановлює вимоги до прозорості, управління даними, кібербезпеки й нагляду за високоризиковими системами. Показано особливості американської моделі, що спирається на доктрини продуктової відповідальності та недбалості й дозволяє судовим органам оперативно реагувати на технологічні виклики. Зазначено, що в Україні відсутність спеціального правового регулювання ШІ створює суттєву невизначеність, насамперед у питаннях відшкодування шкоди та встановлення причинно-наслідкового зв'язку.

Обґрунтовано необхідність оновлення Цивільного кодексу України, запровадження сертифікації алгоритмів, страхування ризиків, аудиту даних і підвищення прозорості діяльності розробників.

Запропоновано гібридний підхід, який враховує рівень автономності систем і забезпечує належний захист потерпілих, не обмежуючи технологічний розвиток. Результати дослідження можуть створити базу для формування цілісної нормативно-правової моделі, що гарантуватиме безпечне й етичне застосування ШІ в Україні.

Ключові слова: правова відповідальність, цивільне право, деліктне право, правосуб'єктність, автономні системи, штучний інтелект.

Hnidovskyi M.S., Sergienko M.A., Lukianchykov B.Y. Legal liability for artificial intelligence actions: challenges and regulatory prospects.

The article examines the issue of determining legal liability for damage caused by artificial intelligence (AI) systems, given their growing autonomy and ability to make decisions without direct human intervention. It analyses current approaches to regulating such legal relations in the EU, the US and Ukraine, as well as the trend towards the formation of a global model that strikes a balance between technological innovation and the protection of human rights. Considerable attention is paid to the issue of the distribution of liability between developers, manufacturers, data providers, owners, operators and users, as well as to discussions on the possibility of granting autonomous systems certain elements of legal personality.

The article outlines the peculiarities of AI application in high-risk areas – autonomous transport, medicine, finance, security, and public administration – where technical failures or algorithmic bias can cause significant damage or human rights violations. A comparative analysis of liability models is conducted: strict (objective), joint, proportional and insurance, which are used in leading jurisdictions.

Based on the EU's experience, the key provisions of the AI Act are examined, which introduces a risk-based control system and establishes requirements for transparency, data management, cybersecurity, and oversight of high-risk systems. The features of the American model, which is based on the doctrines of product liability and negligence and allows judicial authorities to respond quickly to technological challenges, are highlighted. It is noted that in Ukraine, the absence of specific legal regulation of AI creates significant uncertainty, primarily in matters of compensation for damage and establishing causality.

The necessity of updating the Civil Code of Ukraine, introducing algorithm certification, risk insurance, data auditing, and increasing the transparency of developers' activities has been substantiated. A hybrid approach is proposed that takes into account the level of autonomy of systems and provides adequate protection for victims without restricting technological development. The results of the study can form the basis for the development of a comprehensive regulatory model that will ensure the safe and ethical use of AI in Ukraine.

Key words: legal responsibility, civil law, tort law, legal personality, autonomous systems, artificial intelligence

.

Постановка проблеми. Стрімкий розвиток технологій штучного інтелекту (далі – ШІ) створює принципово нові виклики для правової системи. Автономні транспортні засоби, медичні діагностичні системи, алгоритми прийняття фінансових рішень та інші застосування ШІ дедалі частіше стають причиною настання юридично значущих наслідків, включаючи заподіяння шкоди життю, здоров'ю та майну людей. При цій традиційній правовій конструкції відповідальність виявляється недостатньою для ефективного регулювання відносин у цій сфері [1; 5; 7, с. 60].

Актуальність дослідження зумовлена відсутністю або недосконалістю правового регулювання штучного інтелекту (в тому числі у сферах освіти, економіки, публічного управління, кібербезпеки, оборони), а також комплексного правового регулювання відповідальності за дії ШІ. Це створює правову невизначеність як для розробників і користувачів технологій, так і для потерпілих від дій автономної системи [4; 9, с. 2-3].

Стан опрацювання проблематики. Серед зарубіжних учених варто відзначити праці Л. Флоріді, Ф. Шнайдера, Т. Зіммермана, які досліджували етичні та правові аспекти автономних систем [6, с. 90; 7, с. 60; 8, с. 3] і проблеми відповідальності алгоритмів. Серед українських науковців питання правового регулювання ШІ досліджувала О. В. Корват [9, с. 4].

Мета статті – проаналізувати існуючі підходи до визначення правової відповідальності за дії ШІ та запропонувати напрями вдосконалення правового регулювання в цій сфері.

Виклад основного матеріалу: Проблема правосуб'єктності штучного інтелекту постала перед суспільством майже одночасно з появою перших автономних алгоритмів і сьогодні стала одним

із ключових викликів цифрової епохи. Сучасні системи машинного навчання здатні приймати складні рішення, взаємодіяти з середовищем, адаптувати власну поведінку й навіть демонструвати результати, які не завжди можна повністю пояснити або передбачити розробниками. Це спричиняє питання: чи можна розглядати такі системи як окремих учасників правовідносин? Традиційне розуміння суб'єктності передбачає наявність волі, інтересів та можливості усвідомлювати значення власних дій. Проте більшість науковців сходяться на думці, що навіть найскладніші моделі ШІ залишаються інструментом, а не самостійним носієм правових можливостей.

У правовій доктрині сформульовано кілька технічних характеристик ШІ – автономність у прийнятті рішень, здатність до навчання, можливість сприйняття інформації із зовнішнього середовища та непередбачуваність поведінки [9, с. 1]. Вони часто подаються як аргументи щодо потенційної можливості правового статусу ШІ, однак з юридичного погляду ці характеристики не дорівнюють волі, наміру чи правосвідомості, а отже – не створюють підстав для наділення технічної системи правосуб'єктністю. Вони лише підтверджують складність технологій і обґрунтовують потребу у спеціальному регулюванні, особливо з огляду на так звану «проблему чорної скриньки», коли функціонування глибоких нейронних мереж є настільки непрозорим, що навіть їхні творці не можуть точно пояснити, чому було прийнято те чи інше автономне рішення. У цьому контексті інструментальний підхід, згідно з яким вся відповідальність лежить на людині – розробнику, власнику або оператору, який є найпоширенішим і відповідає базовим принципам цивільного права, стикається з неспроможністю справедливо притягнути людину до відповідальності за непередбачувані алгоритмічні помилки, оскільки причинно-наслідковий зв'язок між початковим дизайном і фінальною дією ШІ є розірваним. Ця невідповідність викликає гострі дебати щодо необхідності введення концепції обмеженої (спеціальної) правосуб'єктності, яка могла б бути надана найбільш автономним системам виключно для цілей майнових правовідносин і відшкодування шкоди.

На противагу цьому, гібридний підхід передбачає диференціацію відповідальності залежно від рівня автономності системи. Для простих алгоритмів застосовується класичний правовий режим, тоді як для високоавтономних запроваджуються спеціальні механізми, такі як обов'язкове страхування та сувора відповідальність, а також додаткові вимоги до сертифікації та аудиту. Така модель є гнучкіша, але потребує точного визначення критеріїв автономності, що поки залишається проблемою для більшості країн, оскільки технологічний розвиток випереджає юридичне визначення цих меж [6, с. 95]. Третій підхід – диференційоване регулювання залежно від ризиків – збігається з логікою європейського AI Act і передбачає створення декількох правових режимів для різних типів систем. Це дозволяє уникнути надмірного регулювання для безпечних алгоритмів і водночас встановити високі вимоги до критично важливих сфер – транспорту, медицини, інфраструктури, ефективно розподіляючи регуляторне навантаження відповідно до потенційної шкоди для суспільства та фундаментальних прав людини.

Проблема відповідальності за шкоду, завдану ШІ, є особливо актуальною, оскільки класична модель солідарної відповідальності розробника, що базується на концепції дефектного продукту, виявляється недостатньо ефективною. Алгоритмічна система, яка змінюється через самонавчання, не повністю відповідає традиційному розумінню «продукту» як статичного об'єкта. У ЄС Директива 85/374/ЄЕС формально може застосовуватися до ШІ, але складність доведення дефекту та причинного зв'язку, особливо у випадку, коли помилка виникла не через початковий код, а через упередженість у навчальних даних чи непередбачуваний алгоритмічний вибір, робить її недостатньо ефективною для захисту потерпілого. Реакцією на це стала пропозиція Європейської Комісії щодо нової Директиви про відповідальність за ШІ, яка має на меті полегшити доведення причинно-наслідкового зв'язку шляхом запровадження презумпції причинного зв'язку на користь позивача за умови доведення ним порушення обов'язків оператором або постачальником системи [3].

Інша модель, що пропонує відповідальність оператора або власника системи за аналогією зі ст. 1187 ЦК України [1], яка регулює джерела підвищеної небезпеки, виглядає логічною, оскільки саме оператор має фактичний контроль над рішенням про експлуатацію системи. Такий підхід найбільш застосовний для систем, що фізично взаємодіють з навколишнім середовищем (автономний транспорт, промислові роботи). Проте у випадку надскладних автономних систем контроль може бути переважно формальним, що знову ж таки перекладає необґрунтований ризик на кінцевого користувача чи оператора, який не міг передбачити чи запобігти алгоритмічній помилці.

З огляду на ці складнощі, модель об'єктивної (безвинної) відповідальності стає необхідною для захисту потерпілого навіть у разі, якщо встановити вину розробника чи оператора неможливо. Хоча її впровадження пов'язане з економічними ризиками, оскільки змушує виробників і операторів ШІ створювати фонди або страхові механізми, що значно підвищує витрати, вона забезпечує найвищий рівень гарантії компенсації. Саме тому страхування є ключовим елементом цієї системи, і у країнах ЄС активно обговорюється створення спеціальних страхових полісів для ШІ, подібних до тих, що діють у сфері автомобільного страхування. Такий підхід дозволить ефективно розподілити ризики та компенсувати шкоду незалежно від складності технологій, знімаючи частину відповідальності з кінцевих користувачів.

Європейський AI Act встановлює саме таку ризик-орієнтовану модель, поділяючи системи на чотири категорії: неприйнятний ризик (заборонені системи, що можуть маніпулювати поведінкою), високий ризик (підлягають суворій сертифікації, включаючи транспорт і медицину), обмежений ризик (вимоги прозорості, наприклад, для чат-ботів) та мінімальний ризик [2]. Регламент детально визначає вимоги до високоризикових систем, які стосуються не лише кінцевого продукту, але й навчальних даних (для уникнення упередженості), керування якістю, аудиту, забезпечення прозорості та можливості людського контролю на всіх етапах життєвого циклу системи. Це створює комплексний механізм контролю, який зміщує фокус з пошуку вини на управління ризиками та дотримання етичних принципів.

Поглиблюючи аналіз проблеми, варто детально розглянути складний ланцюжок створення та експлуатації систем ШІ, оскільки відповідальність у ньому може бути розподілена між кількома суб'єктами. Сучасна система ШІ рідко є продуктом однієї компанії. Вона часто складається з компонентів, розроблених різними суб'єктами: постачальник базових моделей (наприклад, фундаментальних моделей на кшталт великих мовних моделей), розробник конкретного застосунку чи сервісу, та оператор або кінцевий користувач. Європейський AI Act, а також пропоновані зміни до Директиви про відповідальність за дефектну продукцію, намагаються чітко розмежувати ролі. Вони вводять поняття «постачальник» – той, хто випускає систему ШІ на ринок, незалежно від того, чи він є розробником коду, чи лише інтегратором компонентів. Постачальник несе первинну відповідальність за відповідність системи нормативним вимогам та якість її дизайну. Водночас, існує відповідальність «імпортера» та «дистриб'ютора», які також мають обов'язки перевірки та контролю. Нарешті, «оператор» – той, хто використовує систему під своїм керівництвом (наприклад, лікарня, що використовує діагностичний ШІ) – несе відповідальність за належну експлуатацію, моніторинг і забезпечення людського нагляду. Цей багаторівневий підхід до відповідальності є ключовим для забезпечення ефективного правового захисту.

Окремим, не менш гострим питанням, пов'язаним із правосуб'єктністю, є право інтелектуальної власності на контент, створений ШІ. Коли система генерує унікальні твори (музику, текст, зображення), постає питання: хто є автором і, відповідно, власником авторських прав? Традиційне законодавство про інтелектуальну власність більшості країн (зокрема, України) вимагає наявності людського творчого внеску та авторської волі. Наразі у світі домінують два підходи. Перший – твір ШІ не захищається авторським правом, оскільки не має людського автора (позиція США). Другий – власником прав є людина, яка ініціювала та контролювала процес генерації (оператор) або розробник (позиція, що набирає популярності в ЄС, де права часто прирівнюються до прав роботодавця на службовий твір) [5]. Деякі юрисдикції, наприклад, Велика Британія, вже давно мають норми, які визначають, що автором комп'ютерно-генерованого твору є особа, яка «зробила необхідні заходи для створення твору». Майбутнє законодавство, ймовірно, вимагатиме від розробників створення чіткої документації щодо використаних навчальних даних (датасетів) та алгоритмічних параметрів, щоб уникнути порушення прав на ті твори, які були використані для навчання генеративних моделей, що також є частиною проблеми прозорості.

Виклики, пов'язані з правовим регулюванням ШІ, мають глобальний характер. Система ШІ, розроблена в одній країні, може експлуатуватися в іншій, спричиняючи шкоду у третій. Це створює проблему колізії права та юрисдикції. Наприклад, чиї норми застосовуватимуться до автономного автомобіля, виготовленого в Німеччині, проданого в Україні та спричинившого ДТП у Польщі? Ефективне вирішення цієї проблеми вимагає міжнародної гармонізації законодавчих підходів. Прийняття Європейським Союзом AI Act задає певний глобальний стандарт, оскільки всі компанії, які бажають працювати на європейському ринку, повинні будуть його дотримуватися («Брюссельський ефект») [8, с. 10]. Для України, в контексті її європейської інтеграції, це означає

необхідність не просто створення власного закону, а його максимального узгодження з регуляторною рамкою ЄС. Це стосується не лише ризик-орієнтованої моделі, але й вимог до якості даних, аудиту алгоритмів та транскордонного обміну інформацією про інциденти, пов'язані з високоризиковими системами ШІ.

Тоді як у США відсутнє єдине федеральне законодавство про ШІ, судова практика активно формує підходи на основі доктрини продуктової відповідальності та недбалості, а багато штатів впровадили норми щодо автономних транспортних засобів, вимагаючи від виробників зберігати лог-файли, забезпечувати можливість ручного втручання та регулярно оновлювати програмне забезпечення. У сфері автономного транспорту ключовим викликом є встановлення, хто саме відповідає за ДТП: виробник автомобіля, розробник програмного забезпечення, компанія-оператор чи власник. Країни, такі як Німеччина та Японія, закріпили презумпцію відповідальності виробника у разі технічної несправності або програмної помилки, але вимагають детального протоколювання поведінки автомобіля, що забезпечує необхідну доказову базу для судових процесів.

Медична сфера залишається однією з найризиковіших. Невизначеність щодо того, хто відповідальний за наслідки використання систем ШІ у діагностиці чи лікуванні, стримує впровадження інновацій. Більшість країн поки залишають відповідальність за медичним працівником, навіть якщо діагноз або рекомендація були надані системою ШІ, керуючись принципом, що лікар має «останнє слово» та повинен здійснити критичну оцінку даних. Проте такий підхід створює правову невизначеність, оскільки у випадку складних діагностичних систем лікар фактично не має можливості перевірити всі висновки алгоритму, що не стимулює розвиток інновацій і може призвести до несправедливого перекладення відповідальності. Тому необхідне чітке розмежування між ШІ як консультативним інструментом і автономною системою прийняття рішень.

Використання ШІ державними органами також потребує чіткого правового регулювання, оскільки автоматизовані рішення у соціальній сфері, кримінальному правосудді чи міграційному контролі можуть призводити до дискримінації, упередженості або помилок, які важко оскаржити через непрозорість алгоритмів. Тому принцип "пояснюваності" має бути закріплений у законодавстві як базовий, гарантуючи право особи на отримання зрозумілого пояснення причини та логіки алгоритмічного рішення, що має для неї правові наслідки [7, с. 65]. Для України першочерговим завданням є прийняття спеціального закону про штучний інтелект, який має містити чіткі визначення, принципи регулювання, механізми відповідальності та вимоги до сертифікації [4]. Важливо також розробити систему незалежного аудиту алгоритмів, вимоги до документації розробки й експлуатації систем та створити спеціалізовані експертні установи для судових справ. Не менш важливим є запровадження обов'язкового страхування для операторів ризикових систем та закріплення принципу прозорості у публічному секторі, що забезпечить справедливий баланс між стимулюванням технологічного розвитку та захистом фундаментальних прав громадян.

Висновки. Проблема правової відповідальності за дії штучного інтелекту є одним із ключових викликів для сучасного права. Існуючі правові конструкції, розроблені для традиційних технологій, виявляються автономно недостатніми для ефективного регулювання відносин, пов'язаних із застосуванням інтелектуальних систем.

Аналіз міжнародного досвіду розробок у сфері правового регулювання штучного інтелекту свідчить про формування різних підходів до вирішення цієї проблеми – від створення спеціального правового статусу для систем ШІ до застосування адаптованих традиційних правових механізмів. З наведеного вбачається, що найбільш ефективним є гібридний підхід, який передбачає диференційоване регулювання залежно від рівня автономності системи штучного інтелекту. Такий підхід, з одного боку, дає змогу забезпечити належний захист прав потерпілих, а з іншого – сприяє розвитку та впровадженню інноваційних технологій, не створюючи надмірних правових обмежень.

Для України актуальним є завдання створення комплексної нормативно-правової бази регулювання ШІ, яка б враховувала кращі світові практики та особливості національної правової системи. Прийняття спеціального законодавства про відповідальність за дії ШІ дозволить зменшити правову невизначеність, сприятиме розвитку інноваційних технологій та забезпечить належний захист прав та інтересів громадян.

Перспективами подальших досліджень є детальний аналіз окремих аспектів відповідальності за дії ШІ в конкретних галузях (медицина, транспорт, фінанси), вивчення питань кримінальної

відповідальності за кримінальні правопорушення, вчинені з використанням ШІ, а також розробка конкретних законодавчих пропозицій для українських законодавців.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Цивільний кодекс України від 16.01.2003 № 435-IV.
2. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text. (дата звернення 29 жовтня 2025 р.).
3. Регламент (ЄС) 2024/1689 Європейського Парламенту та Ради про штучний інтелект (Закон про ШІ). URL:https://eur-lex.europa.eu/legal-content/en/LSU/?uri=oj%3AL_202401689&utm_source.
4. Пропозиція щодо Директиви про адаптацію правил не договірної цивільної відповідальності до штучного інтелекту (Директива про відповідальність ШІ). COM(2022) 496 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0496 (дата звернення 29 жовтня 2025 р.).
5. Концепція розвитку штучного інтелекту в Україні / Міністерство цифрової трансформації України. 2020 рік. URL: https://www.kmu.gov.ua/npas/pro-shvalennya-koncepciyi-rozvitku-shtuchnogo-intelektu-v-ukrayini-s21220 (дата звернення 29 жовтня 2025 р.).
6. Резолюція Європейського Парламенту від 16 лютого 2017 року з рекомендаціями Комісії щодо норм цивільного права з робототехніки (2015/2103(INL)). URL: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html (дата звернення 29 жовтня 2025 р.).
7. Владек Д. Машини без принципалів: правила відповідальності та штучний інтелект. *Washington Law Review.* 2014. Том 89. с. 88-115.
8. URL:https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=4799&context=wlr.
9. Distinguishing two features of accountability for AI technologies / Z. Porter, A. Zimmermann, P. Morgan, J. McDermid, T. Lawton, I. Habli. – *Nature Machine Intelligence*. 2022. Vol. 4. P. 58–74. DOI: 10.15587/2706-5448.2025.323117.
10. On the Brussels-Washington Consensus about the Legal Definition of Artificial Intelligence / L. Floridi. *Philosophy & Technology*. 2023. p. 31. DOI: https://doi.org/10.1007/s13347-023-00624-9.
11. Корват О.В. Актуальні питання правового регулювання штучного інтелекту. URL: https://openarchive.nure.ua/server/api/core/bitstreams/e023c3b3-3ad6-44ee-9099-5ba502b15c3c/content (Дата звернення 29 жовтня 2025 р.).