БОРИСЕНКО С. І.,
викладач кафедри права
(Вищий навчальний приватний заклад «Дніпровський гуманітарний університет»)

УДК 347.65
DOI https://doi.org/10.32842/2078-3736/2025.5.1.7

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ДЖЕРЕЛО ПІДВИЩЕНОЇ НЕБЕЗПЕКИ: ПРОБЛЕМИ ДЕЛІКТНОЇ ВІДПОВІДАЛЬНОСТІ

У статті вивчається деліктна відповідальність за шкоду, завдану штучним інтелектом (ШІ) та автоматизованими системами, що є вкрай актуальним у контексті цифровізації та впровадження автономних технологій у транспорт, охорону здоров'я, оборону та фінансову сферу. Автор аналізує проблеми визначення суб'єктів відповідальності, адже традиційна цивільно-правова концепція делікту передбачає наявність фізичної або юридичної особи, здатної контролювати свої дії та нести за них відповідальність. Автономні системи, самонавчальні, непередбачувані та непрозорі (так званий «чорний ящик»), ускладнюють встановлення причинно-наслідкового зв'язку між їхніми діями та завданою шкодою.

Розглянуто коло потенційних суб'єктів відповідальності: розробники, виробники, оператори, власники систем, а також третіх осіб, що можуть впливати на функціонування ШІ. Проаналізовано міжнародні підходи до регулювання відповідальності, зокрема законодавчі ініціативи ЄС та досвід Польщі, включно з концепцією «анонімної вини», яка дозволяє застосовувати цивільно-правові санкції до юридичних осіб без встановлення конкретного винного працівника.

В Україні законодавчий регулювання щодо деліктної відповідальності за шкоду, завдану ШІ, перебуває на стадії становлення, проте вже існують нормативні ініціативи: «Концепція розвитку ШІ» та «Дорожна карта з регулювання ШІ». Автор підкреслює необхідність адаптації діючих норм цивільного права, застосування положень про деліктну відповідальність і джерела підвищеної небезпеки, а також інтеграції механізмів страхування ризиків, аудиту алгоритмів та оцінки впливу на права людини.

Особлива увага приділяється питанням відповідальності у воєнний час та шкоді від автономних систем у сфері оборони, логістики та критичної інфраструктури, що вимагає додаткового законодавчого врегулювання. Дослідження доводить, що ефективна модель деліктної відповідальності за шкоду від ШІ можлива лише за комплексного підходу, який поєднує адаптацію діючих норм, створення спеціальних положень та застосування запобіжних заходів. Висновки статті можуть бути використані для вдосконалення цивільного законодавства України та гармонізації його з міжнародними стандартами.

Ключові слова: *деліктна відповідальність, штучний інтелект, автономні системи, цивільне право, ризик, безпека, правове регулювання, стандарти ISO, аудит алгоритмів, страхування ризиків.*

Borysenko S. I. Tort liability for damage caused by artificial intelligence or automated systems

the article examines tort liability for damage caused by artificial intelligence (AI) and automated systems, which is highly relevant in the context of digitalization and the implementation of autonomous technologies in transportation, healthcare,

defense, and the financial sector. The author analyzes the challenges in identifying liable parties, as the traditional civil law concept of tort assumes the presence of a natural or legal person capable of controlling their actions and bearing responsibility for them. Autonomous systems, which are self-learning, unpredictable, and opaque (the so-called "black box"), complicate the establishment of a causal link between their actions and the damage caused.

The study considers potential liable parties, including developers, manufacturers, operators, system owners, as well as third parties who may influence AI operations. International approaches to regulating liability are analyzed, particularly EU legislative initiatives and the experience of Poland, including the concept of "anonymous fault," which allows civil liability to be applied to legal entities without identifying a specific culpable employee.

In Ukraine, legal regulation regarding tort liability for damage caused by AI is still at an early stage, but there are already normative initiatives, such as the "Concept for the Development of AI" and the "Roadmap for AI Regulation." The author emphasizes the need to adapt existing civil law provisions, apply rules on tort liability and sources of heightened risk, and integrate mechanisms for risk insurance, algorithm auditing, and human rights impact assessments.

Special attention is given to issues of liability in wartime and damage caused by autonomous systems in defense, logistics, and critical infrastructure, which require additional legislative regulation. The study demonstrates that an effective model of tort liability for AI-related damage is possible only through a comprehensive approach that combines adaptation of current legal norms, creation of specialized provisions, and implementation of preventive measures. The findings of the article may be used to improve Ukraine's civil legislation and harmonize it with international standards.

Key words: *tort liability, artificial intelligence, autonomous systems, civil law, risk, safety, legal regulation, ISO standards, algorithm auditing, risk insurance.*

Вступ. Стрімкий розвиток цифрових технологій та активне впровадження штучного інтелекту у різні сфери суспільного життя актуалізують питання належного правового регулювання. Автономні системи все частіше використовуються у транспорті, медицині, фінансовому секторі, сфері оборони та безпеки, що зумовлює виникнення нових ризиків завдання шкоди. У цих умовах постає необхідність у переосмисленні традиційних цивільно-правових конструкцій деліктної відповідальності, які виходять з припущення про контрольованість поведінки суб'єкта та можливість покладення на нього обов'язку відшкодувати збитки. Автономність і самонавчальні властивості ШІ ускладнюють встановлення суб'єкта відповідальності, що зумовлює потребу в пошуку нових підходів до правового регулювання.

Стан дослідження теми. Питання цивільно-правової відповідальності за шкоду, завдану ШІ, знаходяться у центрі сучасних наукових дискусій як в Україні, так і за її межами. Значний внесок у розробку даної проблематики зроблено у працях М. Великанової, А. Кирилюка, Є. Мічуріна, О. Співака та інших дослідників. Наукова література акцентує увагу на кількох можливих доктринальних підходах: застосування інституту джерела підвищеної небезпеки, концепції «анонімної вини», створення спеціального делікту. Європейський Союз, а також Польща, досвід якої розглядається як релевантний для України, виробляють власні моделі правового врегулювання.

Методи дослідження. Методологічною основою дослідження є загальнонаукові та спеціально-правові методи. Застосовано формально-догматичний метод для аналізу чинних норм цивільного законодавства; порівняльно-правовий метод – для вивчення досвіду Європейського Союзу та окремих європейських держав; системний метод – для з'ясування особливостей функціонування автономних систем і їхнього впливу на інститут деліктних зобов'язань; метод логіко-правового моделювання – для формування пропозицій щодо вдосконалення цивільного законодавства України.

Актуальність теми. Актуальність обраної теми зумовлюється трансформацією цивільних правовідносин під впливом розвитку автономних технологій. Відсутність спеціальних норм у законодавстві України щодо визначення підстав і меж відповідальності за шкоду, завдану ШІ, створює правову невизначеність і ставить під загрозу ефективний захист прав потерпілих. Додаткової актуальності дослідження набуває у зв'язку з воєнними подіями, адже використання роботизованих систем у сфері оборони та критичної інфраструктури створює підвищені ризики для суспільства.

Мета статті. Метою дослідження є з'ясування особливостей деліктної відповідальності за шкоду, завдану штучним інтелектом та автоматизованими системами, аналіз сучасних доктринальних підходів та зарубіжного досвіду, а також вироблення пропозицій щодо вдосконалення цивільного законодавства України у цій сфері.

Постановка завдання. Для досягнення поставленої мети необхідно визначити проблемні аспекти застосування традиційних інститутів деліктного права до автономних систем, також проаналізувати міжнародний досвід регулювання деліктної відповідальності у сфері використання ШІ, зокрема ініціативи ЄС та законодавчу практику Польщі. Окрім цього виникає необхідність дослідити можливості застосування аналогій у чинному цивільному законодавстві України ну і в підсумку запропонувати напрями вдосконалення національної правової системи шляхом створення спеціальних деліктів, розробки стандартів безпеки та запровадження механізмів страхування ризиків.

Виклад основного матеріалу. У сучасних умовах тотальної діджиталізації важко уявити людину поза цифровим середовищем: повсякденне використання смартфонів, розумних годинників, соціальних мереж та Інтернету стало невід'ємною частиною суспільного життя. Технології, які ще донедавна сприймалися як елементи наукової фантастики, зокрема самокеровані автомобілі, «розумні» будинки, віртуальні асистенти та концепція «розумних» міст, нині становлять реалії сьогодення. Процеси цифровізації значно прискорилися під впливом глобальної пандемії COVID-19, а в умовах війни в Україні вони набули ще більшої актуальності, оскільки цифрові технології забезпечують не лише комунікацію та освітній процес, а й відіграють ключову роль у сфері безпеки, оборони та протидії інформаційним загрозам. Саме тому розвиток і впровадження систем штучного інтелекту відбувається особливо інтенсивними темпами, формуючи нові напрями суспільного та наукового поступу.

І саме через це виникає необхідність в досліджені питання цивільної відповідальності за шкоду, скоєну алгоритмами чи автоматичними системами. Традиційне цивільно-правове уявлення про делікт спирається на можливість особи регулювати свої особисті дії, прогнозувати наслідки та нести за них відповідальність. Але коли дія чи бездіяльність, що призводять до шкоди, здійснюється ШІ, постає проблема визначення кола суб'єктів відповідальності: чи це буде власник системи, її розробник, оператор, чи сам «штучний агент» – якщо йому надати правосуб'єктність. Важливим є також питання доказів – виявлення причинно-наслідкового зв'язку між функціонуванням системи ШІ і шкодою, особливо якщо алгоритм працює на основі машинного навчання й приймає рішення у закритих, «чорних ящиках».

Другий аспект – обмежувальні заходи або запобіжники, необхідні для підтримання балансу між новаціями і захистом прав потерпілих. Потрібно розробити ясні правові інструменти, які встановлюватимуть:

(а) яким чином виконується контроль за системою ШІ;

(б) які стандарти безпеки та етики мають бути встановлені;

(в) яким чином оцінюється небезпека перед запуском системи в експлуатацію;

(г) які засоби відшкодування або компенсації доступні для потерпілих. Закон має передбачати не лише відповідальність, а й запобіжні засоби аудит алгоритмів, обов'язкові оцінки впливу, страхування ризиків – щоб запобігати шкоді заздалегідь [1].

Як зауважує А. В. Кирилюк, по мірі розвитку автономних юнітів ШІ збільшується складність пов'язати результати їх дій з конкретною особою-творцем або оператором. У випадках, коли ШІ-система функціонує на принципах самонавчання та автономності, її поведінка може виходити за межі початкових програмних чи інженерних передбачень,

і тоді докази умислу чи навіть недбалості з боку людини-оператора стають вкрай складними для встановлення. Кирилюк також наголошує, що існує високий ризик, особливо для органів державної влади або для сфер, де рішення ШІ мають суспільне значення, оскільки помилки ШІ можуть призвести до значної шкоди відсутності чітких регуляторних гарантій [2].

При застосуванні технологій ШІ виникає низка юридичних проблем, зумовлених особливостями природи таких систем: автономністю, здатністю до самонавчання, неповною передбачуваністю і непрозорістю (так званий «чорний ящик»). Ці характеристики ускладнюють ідентифікацію суб'єкта відповідальності та встановлення причинно-наслідкового зв'язку між діями (або бездіяльністю) ШІ-системи і завданою шкодою. В Україні ці виклики ще посилюються тим, що чинне законодавство не містить спеціальних норм, які б прямо регулювали відповідальність за шкоду, спричинену штучним інтелектом, хоча в Концепції розвитку ШІ і в концепті оновлення цивільного кодексу вже йдеться про потребу введення таких норм.

У контексті європейського права спостерігається тенденція до формування чіткішого, ризик-орієнтованого підходу. Так, ЄС працює над законодавчими ініціативами, такими як Пропозиція щодо Директиви про цивільну відповідальність за ШІ, яка має на меті встановлення єдиного режиму відповідальності, спрощення доказування, розмежування обов'язків між виробниками, розробниками, операторами, а також захисту прав споживачів. Це дає змогу більш ефективно компенсувати шкоду, уникнути ситуацій, коли потерпілі залишаються без можливості відшкодування збитків, а також стимулює розвиток безпечних та етичних систем ШІ [3].

Цікавим є досвід судової практики в країнах ЄС, де вже розглядалися випадки шкоди, завданої автономними транспортними засобами чи алгоритмами фінансового трейдингу. Так, у низці справ суди віддавали перевагу концепції "strict liability" (об'єктивної відповідальності), коли власник чи оператор системи несе відповідальність незалежно від вини, оскільки саме він отримує вигоду від використання ризиконесучої технології. Такий підхід, як відзначають дослідники, найбільш прийнятний і для України, оскільки дозволяє забезпечити належний рівень захисту потерпілих, не чекаючи на довготривале й часто малоефективне з'ясування причинної залежності між діями алгоритму та шкодою. Водночас необхідним є комплексне реформування цивільного законодавства: від внесення змін до глави про деліктні зобов'язання до запровадження інституту страхування відповідальності за шкоду, завдану штучним інтелектом. Це дасть можливість сформувати збалансовану модель, яка одночасно стимулюватиме інновації та гарантуватиме належний рівень захисту прав громадян [4].

У теоретичних дискусіях щодо відповідальності за шкоду, заподіяну роботами із штучним інтелектом (далі – роботи), одним із ключових є питання: чи можуть такі роботи визнаватись суб'єктами цивільного права, чи вони лише об'єкти, за дії яких відповідальність несе їх власник, розробник чи оператор. Згідно із дослідженнями вітчизняних науковців, зокрема Стефанишин та Схаб-Бучинської, роботи/ШІ нині в переважній більшості визнаються об'єктами цивільних прав, а не суб'єктами, оскільки існують суттєві труднощі із закріпленням правосуб'єктності таких систем у чинному законодавстві.

Вони вказують, що відповідальність найчастіше покладається на володільця чи оператора робота, особливо в разі шкоди, спричиненої дефектами системи або неналежним її обслуговуванням.

Також наукова література звертає увагу на норми цивільного законодавства, які можна застосовувати як аналогії: наприклад, норми про деліктну відповідальність (відповідальність за шкоду чужою дією) або про відповідальність за джерело підвищеної небезпеки.

При цьому виникають дискусії: чи достатньо сучасні правові норми та практика для регулювання шкіл, які можуть виникати внаслідок автономних рішень робота, особливо коли такі рішення не контролюються безпосередньо людиною, або коли роботи навчаються і модифікують свою поведінку.

В Україні вже зроблено певні кроки в нормативному регулюванні питань, пов'язаних із ШІ та робототехнікою – зокрема, Концепція розвитку штучного інтелекту, прийнята Кабінетом Міністрів, яка встановлює визначення, принципи і напрямки розвитку ШІ в державі.

У міжнародному праві (зокрема, Європейському Союзі) існують такі ініціативи, як Резолюція Європейського парламенту щодо цивільного правового регулювання робототехніки з включенням поняття «електронна особа». Ця концепція передбачає, що в разі подальшого розвитку автономності робота можуть бути встановлені форми відповідальності, подібні до тих, що застосовуються до юридичних осіб.

Проте, важливо зазначити, що міжнародний досвід також містить застереження: законодавці та науковці вказують на необхідність чіткіших визначень понять «штучний інтелект», «робот», «автономна система», «оператор» тощо; а також на необхідність створення спеціальних правил (стандартів), які врегульовуватимуть безпеку, експлуатацію, відповідальність виробників, розробників і користувачів. Наприклад, в працях із правового регулювання ШІ обговорюється, щоб виробник був відповідальним за проектування, а оператор – за використання і технічне обслуговування.

Війна в Україні створює особливі умови, в яких питання цивільно-правової відповідальності за роботи набуває підвищеного значення. ШКОДА, яка може бути спричинена роботизованими системами у сфері оборони, логістики, безпеки або інфраструктури, потребує законодавчого врегулювання з урахуванням ризиків, пов'язаних з бойовими діями, знищенням техніки, перериванням ланцюгів постачання, кібератаками чи пошкодженнями, викликаними чужим втручанням.

В цих умовах має сенс розглянути методи законодавчого моделювання, які передбачали б спеціальні правила або адаптацію чинних інститутів (наприклад, інституту форс-мажору, відповідальності за шкоду від підвищеної небезпеки, правил страхування) до реалій війни. Крім того, в умовах збройного конфлікту особливо актуальним є встановлення процедур доказування вини/факту шкоди та ступеню автономності роботи (чи системи ШІ), технічної надійності і можливості зовнішнього (людського) втручання або контролю [4].

Аналіз сучасних досліджень свідчить, що питання деліктної відповідальності за шкоду, завдану штучним інтелектом, перебуває у центрі уваги як українських, так і європейських науковців. Зокрема, у працях Є. Мічуріна наголошується на наявності трьох доктринальних підходів до регламентації такої відповідальності:

1) застосування норм про джерело підвищеної небезпеки;

2) використання загальних чи спеціальних деліктів залежно від рівня ризику;

3) формування концепції спеціального делікту, який потребує самостійного законодавчого врегулювання.

Такий підхід дозволяє комплексно розглядати різні ситуації, пов'язані з автономними системами, які здатні діяти незалежно від безпосереднього контролю людини.

Законодавство Європейського Союзу пропонує низку рішень, що можуть бути корисними для національної правової системи України. Зокрема, у Резолюції Європейського парламенту від 20 жовтня 2020 р. визначено необхідність встановлення суворої відповідальності для систем штучного інтелекту з високим рівнем ризику, тоді як до інших систем застосовуються положення про відповідальність на основі вини. Водночас у новоприйнятому Акті про штучний інтелект (2024 р.) деталізуються вимоги до якості, безпеки та маркування таких систем, що створює додаткові гарантії захисту прав потерпілих. Українська доктрина цивільного права у цьому контексті загалом узгоджується з європейськими тенденціями, однак потребує подальшого вдосконалення, зокрема шляхом імплементації механізмів обов'язкового страхування у сферах підвищеного ризику, як-от транспорт, безпілотні літальні апарати та автоматизовані виробничі комплекси.

Таким чином, наукова дискусія засвідчує, що формування ефективного режиму деліктної відповідальності за шкоду, завдану штучним інтелектом або автоматизованими системами, можливе лише за умови комплексного підходу. Він має охоплювати як адаптацію чинних положень цивільного законодавства, так і створення нових правових конструкцій, що

враховуватимуть специфіку автономності, здатності до самонавчання та непередбачуваності поведінки таких систем [5].

Співак О. М. в своїй науковій роботі зазначив, що наприкінці 2020 року Кабінет Міністрів України ухвалив «Концепцію розвитку штучного інтелекту в Україні», що окреслює мету, принципи та напрями застосування ШІ у науково-технологічних дослідженнях. Водночас законодавче регулювання ШІ в Україні перебуває на етапі становлення, подібно до інших європейських країн, зокрема Польщі. У наукових дослідженнях підкреслюється необхідність врахування міжнародних вимог під час розроблення та застосування технологій ШІ, а також при регулюванні наслідків їх використання, включаючи обробку персональних даних громадян ЄС відповідно до Загального регламенту про захист даних (GDPR). Крім того, застосування стандартів ISO/IEC 27701:2019, ISO/IEC 42001:2023 та IEEE P7003™ забезпечує методологічні та етичні підходи до створення та впровадження систем ШІ, а національні ініціативи, як «Дорожня карта з регулювання штучного інтелекту», спрямовані на оцінку впливу ШІ на права людини та маркування систем.

З погляду цивільно-правової відповідальності, польський досвід демонструє труднощі застосування традиційних норм до автономних систем. Зокрема, деліктна відповідальність за ст. 415 Цивільного кодексу Польщі базується на принципі вини, що передбачає наявність суб'єкта із визначеною поведінкою. Оскільки ШІ не має правоздатності, відповідальність покладається на фізичних або юридичних осіб, залучених до розробки, використання або обслуговування системи. Водночас концепція «анонімної вини» дозволяє застосовувати цивільно-правові санкції до юридичних осіб без встановлення конкретного винного працівника, з можливістю спростування презумпції у випадку належної організації діяльності або дій третьої сторони (наприклад, хакера). Проте у випадках автономних дій ШІ традиційні положення цивільного законодавства стають неадекватними, що підкреслює необхідність оновлення правового регулювання та інтеграції спеціалізованих норм для ШІ [6].

Висновки. Дослідження аспектів деліктної відповідальності за шкоду, завдану штучним інтелектом та автоматизованими системами, вказує на наявність значних проблем для сучасного цивільного права. Самостійність, можливість самонавчання та не зрозумілість алгоритмів ускладнюють конвенційні підходи до ідентифікації учасників відповідальності та виявлення причинно-наслідкового зв'язку. Водночас вивчення іноземного досвіду, зокрема правових ініціатив ЄС та практики Польщі, показує потенціал застосування наявних доктринальних моделей (відповідальність за джерело підвищеної небезпеки, концепція «анонімної вини», сувора відповідальність), а також необхідність створення нових спеціалізованих деліктних інститутів.

В Україні, регулювання відповідальності за шкоду, завдану ШІ, перебуває в процесі формування, стає важливішим впровадження міжнародних стандартів, створення механізмів обов'язкового страхування ризиків та впровадження процедур аудиту алгоритмів і оцінки їх впливу на права людини. Все охоплююче реформування цивільного законодавства дасть можливість не лише захистити потерпілих, а й створити передумови для безпечного і етичного розвитку технологій штучного інтелекту.

Отже, створення ефективної моделі деліктної відповідальності в галузі ШІ можливе лише за умов поєднання адаптації існуючих норм, розробки нових правових механізмів і впровадження профілактичних інструментів. Такий підхід створить баланс між стимулюванням інновацій і гарантіями захисту прав людини, що відповідає як національним, так і міжнародним правовим тенденціям.

Список використаних джерел:

1. Великанова М.М. Використання шкоди, завданої використанням технологій штучного інтелекту, як спеціальний делікт. *Нове українське право*. 2021. № 3. С. 17–21.

2. Кирилюк А. В. Відповідальність штучного інтелекту. *Правове життя сучасної України : у 3 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 15 трав. 2020 р.)* / відп. ред. М. Р. Аракелян. Одеса : Гельветика, 2020. Т. 3. С. 511–514.

3. Щодо відшкодування шкоди, завданої використанням технологій штучного інтелекту: стан правового регулювання в Україні та досвід ЄС. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/21a0030c-d502-4614-bda8-c7ca7a3aad2a/content (дата звернення: 15.09.2025)

4. Штучний інтелект в системі об'єктів цивільних прав. URL: https://app-journal.in.ua/wp-content/uploads/2023/07/25.pdf?utm_source=chatgpt.com (дата звернення: 17.09.2025)

5. Мічурін Є. Суб'єкти цивільно-правової відповідальності за шкоду, завдану з використанням штучного інтелекту, за законодавством ЄС та України. *Університетські наукові записки*. 2025. № 4 (106). С. 4–13.

6. Співак О.М. Правові засади регулювання штучного інтелекту в Україні та Польщі. *Юридичний науковий електронний журнал.* 2024. № 4. С. 815–817.

Дата першого надходження рукопису до видання: 23.09.2025
Дата прийнятого до друку рукопису після рецензування: 30.10.2025
Дата публікації: 28.11.2025