УДК 34:004.8(477)

ПРАВОВЕ РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В УКРАЇНІ

Кирило Музиченко[1], Валентин Петрик[2], Саченко Юлія[1]

[1] Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації, Україна
[2] Державний Університет «Київський авіаційний інститут», Україна

Анотація. *У даній статті запропоновано науково обґрунтовані рекомендації щодо майбутнього спеціального законодавства про штучний інтелект в Україні з урахуванням євроінтеграційного курсу держави. Результати дослідження свідчать, що станом на початок 2026 року правове регулювання ШІ в Україні залишається фрагментарним. Спеціальний закон відсутній, а правовідносини регулюються загальними нормами цивільного, інформаційного та адміністративного законодавства. Розпорядженням Кабінету Міністрів України № 457-р від 09.05.2025 затверджено План заходів з реалізації Концепції розвитку штучного інтелекту на 2025–2026 роки, проте цей документ має виключно програмний характер і не містить регуляторних норм. Порівняльний аналіз з EU AI Act виявив суттєві прогалини: в Україні не запроваджено ризик-орієнтованого підходу, класифікації систем ШІ, механізмів обов'язкової сертифікації та незалежного нагляду.*

Ключові слова: *штучний інтелект, правове регулювання, Україна, Регламент ЄС про ШІ, гармонізація законодавства, ризик-орієнтований підхід, цифровізація, відповідальність за ШІ.*

Вступ

Стрімкий розвиток технологій штучного інтелекту (далі — ШІ) зумовлює принципові зміни в економічних, соціальних і правових відносинах на національному та міжнародному рівнях. Системи ШІ дедалі активніше використовуються в охороні здоров'я, правосудді, державному управлінні, фінансовому секторі та медіапросторі, що породжує нові правові ризики: порушення конфіденційності персональних даних, дискримінацію за алгоритмічними критеріями, проблеми юридичної відповідальності за рішення, прийняті автономними системами, а також загрози національній безпеці внаслідок зловживання технологіями. Водночас технологічний прогрес у цій сфері суттєво випереджає нормотворчу реакцію держав, що формує критичний регуляторний розрив.

В Україні відсутність спеціального законодавства про ШІ станом на 2026 рік є однією з найбільш актуальних проблем у сфері правового регулювання цифрових технологій. Правовідносини, пов'язані з розробкою, впровадженням та застосуванням систем ШІ, регулюються загальними нормами Цивільного кодексу України (зокрема, інститутами деліктної відповідальності та договірного права), Закону України «Про захист персональних даних», Закону України «Про інформацію», а також галузевими нормативними актами — без єдиної термінологічної бази, системи класифікації ризиків і спеціальних механізмів нагляду [1; 2]. Такий стан речей породжує правову невизначеність як для суб'єктів господарювання, що впроваджують ШІ-рішення, так і для фізичних осіб, чиї права можуть бути порушені внаслідок автоматизованих рішень.

Особливої ваги проблема набуває у контексті євроінтеграції. Україна як держава-кандидат на членство в Європейському Союзі зобов'язана здійснювати поступову гармонізацію національного законодавства з Acquis communautaire, зокрема з Регламентом ЄС № 2024/1689 про штучний інтелект (EU AI Act), що набув чинності 01.08.2024 та поетапно застосовується з лютого 2025 по серпень 2026 року [3]. Крім того, у 2025 році Україна підписала Рамкову конвенцію Ради Європи про штучний інтелект та права людини, демократію і верховенство права (Framework Convention on AI), що є першим міжнародно-правовим зобов'язанням у цій сфері та слугує додатковим стимулом для системного оновлення регуляторного середовища.

Водночас Кабінет Міністрів України розпорядженням від 09.05.2025 № 457-р затвердив план заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025–2026 роки, який передбачає розробку законопроекту про ШІ [4]. Проте зараз законопроект перебуває на стадії підготовки, а проблема його концептуального наповнення залишається відкритою і дискусійною. Зазначені обставини визначають актуальність цього дослідження.

Мета дослідження— здійснити комплексний аналіз правового регулювання ШІ в Україні, виявити системні прогалини та суперечності чинного законодавства, а також розробити

конкретні науково обґрунтовані рекомендації для майбутнього спеціального закону.

Досягнення поставленої мети передбачає вирішення таких завдань: 1) проаналізувати нормативно-правову базу регулювання ШІ в Україні, включаючи стратегічні документи та галузеве законодавство; 2) провести порівняльний аналіз із регуляторними підходами ЄС, передусім з EU AI Act; 3) виявити ключові виклики та прогалини правового регулювання; 4) сформулювати пропозиції щодо структури та змісту майбутнього Закону України про штучний інтелект.

Об'єктом дослідження є суспільні відносини, що виникають у зв'язку з розробкою, впровадженням та використанням систем штучного інтелекту.

Предметом — норми права, що регулюють ці відносини в Україні та Європейському Союзі.

Методологічну основу складають доктринальний, порівняльно-правовий, формально-юридичний методи та системний аналіз.

Аналіз існуючих досліджень

У сучасній українській правовій науці значна увага приділяється дослідженню загальних підходів до формування правового режиму штучного інтелекту. Зокрема, у працях українських дослідників підкреслюється, що формування ефективного правового регулювання повинно забезпечувати баланс між інноваційним розвитком технологій та захистом основоположних прав і свобод людини. Так, у дослідженнях, присвячених правовому регулюванню штучного інтелекту в Україні, наголошується на необхідності створення чітких правових механізмів відповідальності за використання ШІ та визначення правового статусу результатів його діяльності.

Важливим напрямом досліджень є питання співвідношення правового регулювання штучного інтелекту із захистом персональних даних. Науковці зазначають, що широке використання алгоритмів машинного навчання пов’язане з обробкою значних масивів інформації, що створює ризики порушення права на приватність. У відповідних роботах наголошується на необхідності інтеграції норм щодо захисту персональних даних у систему правового регулювання ШІ та узгодження національного законодавства із міжнародними стандартами у цій сфері.

Окрему групу становлять дослідження, присвячені порівняльному аналізу українського та європейського підходів до правового регулювання штучного інтелекту. Дослідники підкреслюють, що Україна орієнтується на правові стандарти Європейського Союзу, зокрема на положення Регламенту ЄС щодо штучного інтелекту (AI Act), який встановлює ризик-орієнтований підхід до регулювання систем ШІ. Водночас науковці наголошують на необхідності адаптації цих норм з урахуванням національних особливостей правової системи України.

У процесі дослідження застосовано низку методів: доктринальний (для аналізу наукових концепцій і юридичних категорій у сфері ШІ), порівняльно-правовий (для зіставлення українського законодавства з Регламентом ЄС про штучний інтелект № 2024/1689), формально-юридичний (для тлумачення чинних нормативно-правових актів) та системний аналіз (для виявлення прогалин і суперечностей у регуляторному середовищі).

Основна частина дослідження

Формування регуляторного середовища у сфері штучного інтелекту в Україні розпочалося з ухвалення Концепції розвитку штучного інтелекту в Україні, схваленої розпорядженням Кабінету Міністрів України від 02.12.2020 № 1556-р. Цей документ заклав базові засади державної політики у сфері ШІ: визначив пріоритетні напрями розвитку технологій, окреслив роль держави як регулятора та замовника ШІ-рішень, а також запропонував первинне описове визначення штучного інтелекту як сукупності технологічних рішень, що імітують когнітивні функції людини. Принципово важливо, що ця дефініція так і не набула статусу законодавчої норми — вона залишилася виключно в межах програмного документа, позбавленого юридично зобов'язувальної сили.

Наступним кроком у системі стратегічного планування стало затвердження розпорядженням Кабінету Міністрів України від 09.05.2025 № 457-р Плану заходів з реалізації Концепції розвитку штучного інтелекту на 2025–2026 роки. Цей документ передбачає розробку законопроекту про ШІ, запровадження механізмів регуляторних «пісочниць» для тестування інноваційних рішень, а також проведення оцінки регуляторного впливу на ринок ШІ. Водночас План заходів є документом організаційно-виконавчого характеру: він встановлює строки та відповідальних виконавців, але не породжує безпосередніх прав і обов'язків для суб'єктів господарювання. Доповнює цю систему «Біла книга» Мінцифри з питань регулювання ШІ, яка

окреслила концептуальні підходи до майбутнього закону, зокрема доцільність ризик-орієнтованого підходу та принципу «regulation by design», однак також не має обов'язкової юридичної сили [5; 6].

За відсутності спеціального закону правовідносини у сфері ІІІ регулюються комплексом загальних норм різних галузей права, що породжує суттєві труднощі у правозастосуванні. Питання цивільно-правової відповідальності за шкоду, заподіяну внаслідок функціонування ІІІ-систем, вирішуються на підставі загальних норм деліктного права Цивільного кодексу України — зокрема статей 1166–1187 щодо відшкодування шкоди, заподіяної джерелом підвищеної небезпеки [1]. Однак класична конструкція деліктної відповідальності ґрунтується на встановленні причинно-наслідкового зв'язку між діянням конкретного суб'єкта та шкідливим наслідком, що є вкрай складним завданням стосовно автономних самонавчальних систем, чия поведінка визначається не безпосередньо людиною, а алгоритмічними процесами. Відтак чинне законодавство не містить жодного спеціального механізму розподілу відповідальності між розробником, оператором та користувачем системи ІІІ — а це означає, що при виникненні реальної шкоди суд змушений застосовувати норми, які не враховують технологічної природи відносин.

Захист персональних даних у контексті ІІІ регулюється Законом України «Про захист персональних даних» від 01.06.2010 № 2297-VI, який закріплює принципи законності, мети та пропорційності обробки даних [2]. Втім, цей Закон не містить спеціального регулювання автоматизованого прийняття рішень та профілювання, аналогічного статті 22 Загального регламенту ЄС про захист даних (GDPR), що унеможливлює ефективний захист громадян від наслідків алгоритмічної дискримінації. Загальні вимоги до захисту та безпеки інформаційних систем, що поширюються і на ІІІ-системи, встановлюють Закон України «Про інформацію» та Закон України «Про захист інформації в інформаційно-комунікаційних системах», проте й вони не враховують специфіки машинного навчання, генеративних моделей та автономних агентів [7; 8]. Закон України «Про електронні довірчі послуги» від 05.10.2017 № 2155-VIII регулює суміжну проблематику електронної ідентифікації, однак питання юридичної сили документів, підписаних чи сформованих системами ІІІ, залишаються повністю невирішеними [9]. Принциповою прогалиною є відсутність нормативно закріпленого визначення «системи штучного інтелекту». Внаслідок цього суди, органи влади та суб'єкти господарювання позбавлені єдиного правового орієнтиру при кваліфікації технологічних рішень, розмежуванні ІІІ від звичайного програмного забезпечення та встановленні кола суб'єктів регуляторних зобов'язань.

Нижче наведео схему нормативно-правової бази регулювання ІІІ в Україні станом на 2026 рік. Наведена схема унаочнює трирівневу архітектуру чинного регулювання — від програмних документів через галузеве законодавство до міжнародних зобов'язань та підкреслює системну прогалину: відсутність спеціального закону як верхнього рівня ієрархії.

Переходячи до порівняльного аналізу, слід констатувати, що Регламент Європейського Парламенту і Ради ЄС № 2024/1689 від 13.06.2024 про штучний інтелект (EU AI Act) є першим у світі комплексним горизонтальним нормативно-правовим актом у цій сфері [3]. Він набув чинності 01.08.2024 і запровадив поетапне застосування своїх положень: з 02.02.2025 — норми щодо заборонених практик; з 02.08.2025 — положення про моделі ІІІ загального призначення; повне застосування до високоризикових систем очікується з 02.08.2026. Регламент визначає систему ІІІ як машинну систему, здатну генерувати результати — прогнози, рекомендації, рішення або контент, — що впливають на реальне або віртуальне середовище. Дефініція є технологічно нейтральною та функціональною, що дозволяє охопити широкий спектр як наявних, так і майбутніх технологічних рішень.

Принциповою методологічною особливістю EU AI Act є ризик-орієнтований підхід, що передбачає диференційовані регуляторні вимоги залежно від потенційної шкоди. Системи з неприйнятним рівнем ризику — когнітивні маніпулятивні системи, системи соціального рейтингування громадян, дистанційна біометрична ідентифікація в реальному часі у публічних місцях — є безумовно забороненими з 02.02.2025. Системи високого ризику, що охоплюють сфери охорони здоров'я, правосуддя, зайнятості та управління критичною інфраструктурою, підпадають під обов'язкову оцінку відповідності, реєстрацію у централізованій базі даних ЄС та постмаркетинговий моніторинг. Системи обмеженого ризику — зокрема чат-боти та генератори синтетичного контенту — зобов'язані інформувати користувачів про

взаємодію із ШІ. Більшість систем мінімального ризику не підпадають під обов'язкове регулювання, хоча й заохочуються до добровільного дотримання кодексів поведінки [3].

Важливим нормативним нововведенням є вимога прозорості та пояснюваності рішень ШІ. Постачальники та оператори зобов'язані надавати особам, щодо яких приймаються автоматизовані рішення, зрозумілі пояснення логіки таких рішень та забезпечити реальне право на їх оскарження. EU AI Act також формує розгалужену інституційну архітектуру: Офіс ШІ ЄС при Єврокомісії здійснює наднаціональний нагляд, а національні компетентні органи кожної держави-члена забезпечують ринковий нагляд і правозастосування. За порушення заборонених практик передбачені санкції до 35 мільйонів євро або 7% річного глобального обороту.

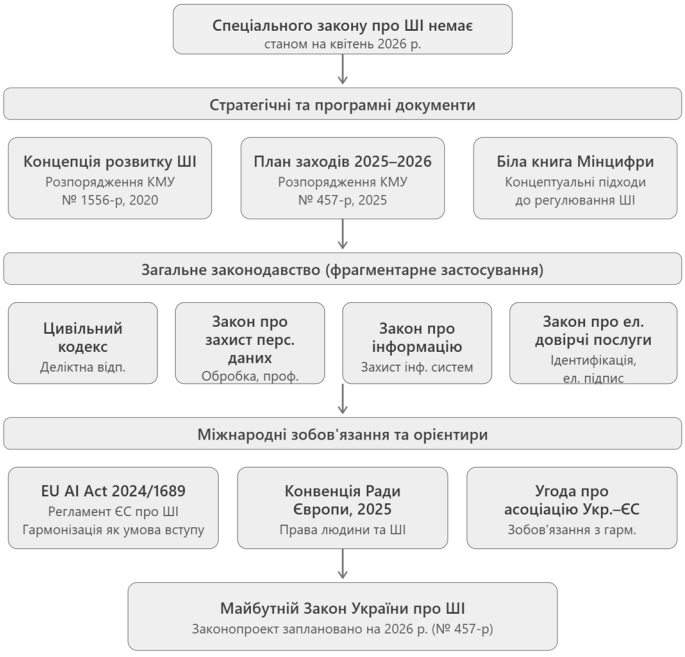

Рис. 1. Схема нормативно-правової бази регулювання ШІ в Україні станом на 2026 рік

Для України як держави-кандидата на членство в ЄС гармонізація з EU AI Act є водночас стратегічним завданням і юридичним зобов'язанням у рамках Угоди про асоціацію та переговорного процесу щодо вступу [10]. Підписання у 2025 році Рамкової конвенції Ради Європи про штучний інтелект та права людини додає ще один рівень міжнародно-правових зобов'язань: держави-сторони мають гарантувати верховенство права, недискримінацію, прозорість і підзвітність систем ШІ [11]. На відміну від EU AI Act, Конвенція поширюється і на приватний сектор у тій мірі, яку визначає кожна держава-сторона, надаючи ширший імплементаційний простір.

Порівняльний аналіз засвідчує глибокий розрив між стандартами ЄС та поточним станом регулювання в Україні: відсутня законодавча класифікація систем ШІ за рівнями ризику, не передбачено обов'язкової оцінки відповідності та сертифікації, не створено незалежного наглядового органу, не врегульовано права громадян щодо автоматизованих рішень. Подолання цього розриву є необхідною умовою як для успішного руху до членства в ЄС, так і для реального захисту прав людини в умовах прискореної цифровізації.

Аналіз нормативно-правової бази та порівняльне дослідження засвідчили глибокі системні прогалини вітчизняного регулювання. Їх природа є не випадковою, а структурною — вони зумовлені самою логікою фрагментарного підходу, за якого суспільні відносини у сфері ШІ регулюються нормами, створеними для принципово інших технологічних реалій. У цьому контексті доцільно детально проаналізувати ключові виклики, що постають перед українським законодавцем, та сформулювати конкретні рекомендації щодо їх подолання.

Першим і найбільш фундаментальним викликом є відсутність єдиної термінологічної та класифікаційної системи. Без законодавчого визначення поняття «система штучного інтелекту» неможливо встановити ані суб'єктний склад регульованих відносин, ані межі застосування спеціальних норм. Ця проблема має практичний вимір: суди вже сьогодні стикаються з необхідністю кваліфікувати спірні правовідносини, пов'язані з автоматизованими системами прийняття рішень, — і змушені робити це в умовах правової невизначеності, спираючись на загальні норми без будь-якого технологічно орієнтованого тлумачення. Відсутність класифікації ризиків унеможливлює диференційований регуляторний підхід: усі системи ШІ — від простих рекомендаційних алгоритмів до систем автономного прийняття рішень у сфері кримінального правосуддя — перебувають в однаковому правовому вакуумі, що є очевидним регуляторним нонсенсом.

Не менш гострою є проблема визначення суб'єкта юридичної відповідальності за шкоду, заподіяну ШІ-системою. Ланцюжок відносин у типовому сценарії є багатоланковим: розробник алгоритму, постачальник хмарної інфраструктури, оператор, що налаштовує і впроваджує систему, та кінцевий користувач — усі вони тією чи іншою мірою можуть бути

причетні до заподіяння шкоди. Чинне деліктне право, орієнтоване на класичну двосторонню модель «заподіювач — потерпілий», не здатне адекватно врегулювати таку розподілену причинність. Особливої складності це питання набуває у випадку самонавчальних систем, поведінка яких може суттєво відхилятися від початково закладеної розробником логіки внаслідок навчання на нових даних. У науковій доктрині пропонуються різні підходи до вирішення цієї проблеми — від запровадження об'єктивної відповідальності оператора за принципом «strict liability» до створення галузевих компенсаційних фондів за аналогією з ядерною або авіаційною відповідальністю [12; 13]. Жоден із цих підходів наразі не знайшов відображення в українському законодавстві.

Окремим викликом є захист основоположних прав людини в умовах алгоритмічного управління. Системи ШІ, що застосовуються у сферах кредитного скорингу, рекрутингу, медичної діагностики та правоохоронної діяльності, здатні відтворювати і навіть посилювати соціальну дискримінацію, якщо навчальні дані містять системні упередження. Так зване «алгоритмічне упередження» (algorithmic bias) є задокументованою проблемою: дослідження засвідчують, що системи розпізнавання облич демонструють суттєво вищий рівень помилок щодо осіб із темнішим кольором шкіри, а системи прогнозування рецидивізму відтворюють расові стереотипи, закладені в історичних даних [14]. Українське законодавство не містить жодних спеціальних норм щодо аудиту алгоритмів на предмет дискримінаційних патернів, права осіб вимагати пояснення автоматизованих рішень або механізмів їх оскарження. Закон про захист персональних даних, як зазначалося, не відтворює гарантій статті 22 GDPR, що є критичною прогалиною з огляду на масштаби впровадження ШІ в публічному секторі України в умовах воєнного стану та повоєнної відбудови.

Етичний вимір регулювання, попри свій позаправовий характер, безпосередньо впливає на якість нормотворення. Відсутність інституційних механізмів етичної експертизи ШІ-систем — незалежних комітетів з оцінки, процедур громадського обговорення, стандартів прозорості — означає, що рішення про впровадження потенційно небезпечних технологій приймаються виключно на розсуд їх замовників і постачальників. Це особливо актуально для застосування ШІ в умовах збройного конфлікту та систем спостереження, де ціна помилки є надзвичайно високою, а громадський контроль — мінімальним.

Враховуючи сукупність виявлених викликів, першочерговим завданням є прийняття спеціального Закону України про штучний інтелект. Строки, встановлені Планом заходів 2025–2026 років, роблять прийняття такого закону до кінця 2026 року реалістичним завданням за умови належної політичної волі та якісної підготовки законопроекту. При цьому принципово важливим є не механічне перенесення тексту EU AI Act, а його адаптоване впровадження з урахуванням українських правових традицій, інституційних можливостей та соціально-економічного контексту.

Концептуальною основою майбутнього закону має слугувати ризик-орієнтований підхід, адаптований до українських реалій. Пропонована чотирирівнева класифікація систем ШІ — за рівнями неприйнятного, високого, обмеженого та мінімального ризику — повинна враховувати не лише технічні характеристики систем, але й специфіку сфер їх застосування в Україні. Зокрема, з огляду на тривалий збройний конфлікт, до категорії ризику доцільно віднести системи автономного ураження цілей без належного людського контролю та системи масового стеження, що не відповідають стандартам верховенства права. До категорії високого ризику — системи ШІ у сферах охорони здоров'я, судочинства, соціального захисту та управління критичною інфраструктурою.

Закон має закріпити право фізичних осіб на отримання зрозумілого пояснення будь-якого автоматизованого рішення, що суттєво впливає на їхні права та законні інтереси, а також право на оскарження такого рішення із залученням людини-оператора. Це право має кореспондувати з обов'язком операторів систем ШІ забезпечити технічну можливість такого пояснення вже на етапі проєктування — відповідно до принципу «explainability by design». Для систем високого ризику слід запровадити обов'язкову попередню оцінку відповідності та реєстрацію у національному реєстрі ШІ-систем, що адмініструватиметься уповноваженим органом.

Створення незалежного національного органу з нагляду у сфері ШІ є необхідною інституційною передумовою ефективного правозастосування. Такий орган міг би функціонувати або як окремий регулятор, або як структурний підрозділ розширеного мандату Уповноваженого Верховної Ради України з прав людини чи Національної комісії з питань

захисту персональних даних. Його ключовими функціями мають бути: ведення реєстру систем ШІ, проведення аудитів і розслідувань, накладення санкцій за порушення, надання роз'яснень і методичних рекомендацій, а також координація з Офісом ШІ ЄС у рамках майбутньої інтеграції.

Механізм регуляторних «пісочниць», передбачений Планом заходів 2025–2026 років, заслуговує законодавчого закріплення як інструмент стимулювання інновацій при збереженні регуляторного контролю. За цим механізмом підприємства, що розробляють або впроваджують ШІ-системи, могли б тестувати їх у контрольованому правовому середовищі з тимчасовим відступом від окремих регуляторних вимог — за умови посиленого моніторингу з боку уповноваженого органу та обов'язкового звітування про результати. Аналогічні моделі успішно функціонують у Великій Британії, Сингапурі та Іспанії [15].

Нарешті, імплементація Рамкової конвенції Ради Європи про штучний інтелект потребує не лише адаптації матеріального законодавства, але й перегляду процесуальних механізмів захисту прав. Конвенція зобов'язує держави-сторони забезпечити ефективні засоби правового захисту для осіб, чиї права порушені внаслідок застосування ШІ-систем, — що потребує відповідних змін до процесуального законодавства та формування спеціалізованої судової практики. У цьому контексті доцільним є запровадження освітніх програм для суддів та адвокатів із питань технологічного права, а також розробка методичних рекомендацій щодо розгляду справ, пов'язаних із застосуванням ШІ.

Висновки

Проведене дослідження дозволяє сформулювати систему висновків, що відображають як теоретичний внесок роботи, так і її практичне значення для розвитку вітчизняного законодавства у сфері штучного інтелекту.

Насамперед підтверджено вихідну гіпотезу дослідження: правове регулювання штучного інтелекту в Україні станом на 2026 рік є фрагментарним і системно недостатнім для забезпечення належного захисту прав людини, стимулювання інновацій та виконання міжнародно-правових зобов'язань держави. Чинна нормативна база — розпорошена між нормами цивільного, інформаційного та адміністративного права — не утворює цілісної регуляторної системи, оскільки була створена для принципово інших технологічних реалій і не враховує специфіки автономних самонавчальних систем. Стратегічні документи — Концепція розвитку ШІ 2020 року та План заходів 2025–2026 років — окреслюють напрями реформування, проте самі по собі не мають регуляторної сили і не можуть замінити спеціального закону.

У межах дослідження було виконано всі поставлені завдання. Проведений аналіз нормативно-правової бази виявив ключові прогалини: відсутність законодавчого визначення системи ШІ, відсутність класифікації ризиків, неврегульованість питань відповідальності в ланцюжку «розробник — оператор — користувач», а також відсутність механізмів аудиту алгоритмів та права громадян на оскарження автоматизованих рішень. Порівняльний аналіз із EU AI Act 2024/1689 та Рамковою конвенцією Ради Європи 2025 року дав змогу встановити конкретний регуляторний розрив між стандартами ЄС і поточним станом українського законодавства, а також визначити параметри необхідної гармонізації. Виявлені системні виклики — проблема розподіленої відповідальності, алгоритмічна дискримінація, відсутність інституційного нагляду — були структуровані та проаналізовані з позицій як доктринального, так і порівняльно-правового методу. Нарешті, сформульовано оригінальні рекомендації щодо структури та змісту майбутнього Закону України про штучний інтелект, що є самостійним науковим результатом роботи.

Наукова новизна дослідження визначається кількома аспектами. По-перше, здійснено комплексний аналіз чинної нормативно-правової бази регулювання ШІ в Україні саме в контексті актуального стану — після підписання Рамкової конвенції Ради Європи та на етапі підготовки національного законопроекту, — що відрізняє цю роботу від попередніх досліджень, які не могли враховувати зазначених змін. По-друге, запропоновано оригінальну модель адаптованого впровадження ризик-орієнтованого підходу з урахуванням українського контексту, зокрема необхідності регулювання ШІ в умовах збройного конфлікту. По-третє, обґрунтовано інституційну архітектуру національного нагляду у сфері ШІ із визначенням конкретних функцій уповноваженого органу та його місця в системі органів державної влади.

Практичне значення одержаних результатів є багатовимірним. Для законодавця сформульовані рекомендації можуть слугувати концептуальною основою при розробці

законопроекту про ШІ, що відповідає вимогам Плану заходів 2025–2026 років. Для суб'єктів господарювання — розробників та операторів ШІ-систем — результати дослідження окреслюють очікуваний регуляторний контур і дозволяють завчасно адаптувати бізнес-процеси до майбутніх вимог. Для наукової спільноти стаття визначає актуальний порядок денний досліджень у сфері інформаційного та технологічного права: питання алгоритмічної відповідальності, процесуальних механізмів захисту прав в умовах автоматизованого прийняття рішень та конституційно-правових меж застосування ШІ в публічному секторі потребують подальшого самостійного опрацювання.

Підсумовуючи, слід наголосити, що правове регулювання штучного інтелекту є не технічним, а глибоко ціннісним завданням: воно відповідає на питання про те, яким суспільством прагне бути Україна в умовах цифрової трансформації — суспільством, де технологічний прогрес підпорядкований верховенству права та захисту гідності людини, чи суспільством, де регуляторна інертність відкриває простір для зловживань. Своєчасне прийняття якісного спеціального закону є не лише євроінтеграційним зобов'язанням, але й вираженням конституційного обов'язку держави гарантувати права і свободи людини в усіх сферах суспільного життя, включно з тими, що визначаються алгоритмами. Тому для успішної гармонізації з законодавством ЄС та забезпечення захисту прав людини в умовах цифровізації Україна має невідкладно прийняти спеціальний Закон про штучний інтелект, який запровадить ризик-орієнтовану класифікацію систем, чітку відповідальність операторів, право на оскарження автоматизованих рішень та створення незалежного регуляторного органу.

Література

[1] Vaswani A. Attention is all you need / A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. Gomez, Ł. Kaiser, I. Polosukhin // Advances in Neural Information Processing Systems. – 2017. – Vol. 30. – P. 5998–6008.

[2] Brown T. Language models are few-shot learners / T. Brown, B. Mann, N. Ryder et al. // Advances in Neural Information Processing Systems. – 2020. – Vol. 33. – P. 1877–1901.

[3] Goodfellow I. Generative adversarial nets / I. Goodfellow, J. Pouget-Abadie, M. Mirza et al. // Advances in Neural Information Processing Systems. – 2014. – Vol. 27. – P. 2672–2680.

[4] Kingma D. Auto-encoding variational Bayes / D. Kingma, M. Welling // International Conference on Learning Representations (ICLR). – 2014. – 14 p.

[5] Hochreiter S. Long short-term memory / S. Hochreiter, J. Schmidhuber // Neural Computation. – 1997. – Vol. 9, No. 8. – P. 1735–1780.

[6] Kaplan J. Scaling laws for neural language models / J. Kaplan, S. McCandlish, T. Henighan et al. // arXiv preprint arXiv:2001.08361. – 2020. – 26 p.

[7] Wardle C. Information disorder: Toward an interdisciplinary framework for research and policy making / C. Wardle, H. Derakhshan. – Strasbourg: Council of Europe, 2017. – 108 p.

[8] Floridi L. Artificial intelligence, deepfakes and a future of epistemic instability / L. Floridi // Philosophy & Technology. – 2020. – Vol. 33. – P. 1–6.

[9] Chesney R. Deep fakes: A looming challenge for privacy, democracy, and national security / R. Chesney, D. Citron // California Law Review. – 2019. – Vol. 107. – P. 1753–1820.

[10] Ferrara E. Manipulation and abuse on social media / E. Ferrara // ACM Computing Surveys. – 2020. – Vol. 53, No. 1. – P. 1–38.

[11] Russell S. Artificial intelligence: A modern approach / S. Russell, P. Norvig. – 4th ed. – Hoboken: Pearson Education, 2021. – 1152 p.

[12] Mitchell M. Artificial intelligence: A guide for thinking humans / M. Mitchell. – New York: Farrar, Straus and Giroux, 2019. – 336 p.

[13] Kahneman D. Thinking, fast and slow / D. Kahneman. – New York: Farrar, Straus and Giroux, 2011. – 499 p.

[14] Sunstein C. #Republic: Divided democracy in the age of social media / C. Sunstein. – Princeton: Princeton University Press, 2017. – 320 p.

[15] O'Neil C. Weapons of math destruction: How big data increases inequality and threatens democracy / C. O'Neil. – New York: Crown Publishing Group, 2016. – 272 p.

[16] European Parliament Research Service. Artificial intelligence and disinformation: Challenges for democracy. – Brussels: European Parliament, 2025. – 92 p.

[17] UNESCO. Guidelines for the governance of digital platforms and artificial intelligence. – Paris: UNESCO Publishing, 2023. – 156 p.

[18] World Economic Forum. Global risks report 2026. – Geneva: World Economic Forum, 2026. – 104 p.

[19] NATO Strategic Communications Centre of Excellence. Artificial intelligence and information warfare. – Riga: NATO StratCom COE, 2023. – 148 p.

[20] Stanford Internet Observatory. Synthetic media and information integrity report 2026. – Stanford: Stanford University, 2026. – 78 p.

LEGAL FRAMEWORK FOR ARTIFICIAL INTELLIGENCE IN UKRAINE

Abstract. This article proposes scientifically grounded recommendations for the future development of special legislation on artificial intelligence in Ukraine, taking into account the state's European integration course. The results of the study indicate that, as of early 2026, the legal regulation of artificial intelligence in Ukraine remains fragmented. A specific law is absent, and legal relations are governed by general provisions of civil, information, and administrative legislation. By Order of the Cabinet of Ministers of Ukraine No. 457-r dated May 9, 2025, the Action Plan for the implementation of the Concept for the Development of Artificial Intelligence for 2025–2026 was approved; however, this document has an exclusively programmatic character and does not contain regulatory provisions. A comparative analysis with the EU AI Act revealed significant gaps: Ukraine has not yet introduced a risk-based approach, classification of AI systems, mechanisms of mandatory certification, or independent oversight.

Keywords: artificial intelligence, legal regulation, Ukraine, EU AI Act, harmonization of legislation, risk-based approach, digitalization, liability for AI.

МУЗИЧЕНКО Кирило Миколайович, *Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації.*

MUZYCHENKO Kyrylo Mykolayovych, State Scientific and Research Institute of Cybersecurity Technologies and Information Protection.

E-mail: kirilmuzychenkho@gmail.com

Orcid: 0009-0004-0738-6273

ПЕТРИК Валентин Михайлович*, к. н. з держ. управл., доцент, доцент кафедри кібербезпеки,* Державний університет «Київський авіаційний інститут».

PETRYK Valentyn Mykhailovych, PhD in Public Administration, Associate Professor, Department of Cybersecurity, State University "Kyiv Aviation Institute"

E-mail: iszzi_open@ukr.net

Orcid: 0000-0003-2662-0876

САЧЕНКО Юлія Миколаївна*, Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації.*

SACHENKO Yulia Mykolaivna, State Scientific and Research Institute of Cybersecurity Technologies and Information Protection.

E-mail: Sachenko_yulia0307@ukr.net

Orcid: 0009-0005-6028-2550