ЯВТУШЕНКО О. В.,
аспірант кафедри цивільного права
(Навчально-науковий інститут права Київського національного університету імені Тараса Шевченка)

УДК 347.1
DOI https://doi.org/10.32842/2078-3736/2024.3.17

ТЕОРЕТИКО-ПРАВОВИЙ АНАЛІЗ РИЗИК-ОРІЄНТОВАНОГО ПІДХОДУ В АКТІ ПРО ШТУЧНИЙ ІНТЕЛЕКТ ТА ОЦІНКА ЙОГО ВПЛИВУ НА РОЗВИТОК СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ У БЕЗПІЛОТНИКАХ В ЄВРОПЕЙСЬКОМУ СОЮЗІ

У статті досліджується вплив Акту про штучний інтелект на правове регулювання безпілотних транспортних засобів у Європейському союзі та аналіз основних положень цього нормативно-правового акту, зокрема щодо відповідальності розробників та операторів систем штучного інтелекту (ШІ). У дослідженні розглянуто ключові аспекти гармонізації правил для ШІ, що регулюють розвиток, впровадження та використання так званих систем штучного інтелекту «високого ризику», до яких відносяться безпілотні транспортні засоби.

Акт про штучний інтелект, прийнятий Європейським Парламентом 13 березня 2024 року, має на меті встановлення єдиного правового поля для ШІ систем у Європейському Союзі, що сприятиме захисту здоров'я, безпеки та основних прав осіб, а також підтримці інновацій та розвитку ШІ технологій. Основні положення акту включають вимоги щодо прозорості, технічної документації, оцінки ризиків та управління ними, а також дотримання вимог безпеки та захисту даних. Дослідження обов'язків розробників та операторів ШІ систем в рамках згаданого нормативно-правового акту показало, що розробники зобов'язані забезпечити прозорість та інформування користувачів про функціонування ШІ системи, її можливості та обмеження. Вони також повинні вести детальну технічну документацію та зберігати записи про роботу системи для ретроспективного аналізу та виявлення можливих помилок. Оператори, у свою чергу, зобов'язані використовувати ШІ системи відповідно до інструкцій розробників, забезпечити належне навчання персоналу та постійний моніторинг роботи систем, а також дотримуватися вимог щодо захисту персональних даних та конфіденційності.

Для досягнення мети дослідження були використані загальнонаукові методи наукового пізнання, включаючи діалектичний, історичний, формально-логічний (догматичний), метод системного аналізу, синтезу, дедукції, індукції, а також спеціально-наукові методи, такі як формально-юридичний, порівняльно-правовий, метод аналогії та метод правового моделювання.

Ключові слова: *безпілотники, безпілотні транспортні засоби, БПЛА, дрони, IT право, об'єкти цивільних прав, правове регулювання, правовий режим, цивільно-правова відповідальність, штучний інтелект.*

Yavtushenko O. V. The impact of the Artificial intelligence act on the legal regulation of unmanned vehicles in the EU: a civil law analysis

This article explores the impact of the Artificial Intelligence Act on the legal regulation of unmanned vehicles (UVs) in the European Union and analyzes the main provisions of this regulatory act, particularly regarding the responsibilities of developers

and operators of artificial intelligence (AI) systems. The study examines key aspects of the harmonization of AI rules governing the development, deployment, and use of so-called «high-risk» AI systems, which include unmanned vehicles.

The Artificial Intelligence Act, adopted by the European Parliament on March 13, 2024, aims to establish a unified legal framework for AI systems within the European Union, promoting the protection of health, safety, and fundamental rights, as well as supporting innovation and the development of AI technologies. The main provisions of the act include requirements for transparency, technical documentation, risk assessment and management, as well as compliance with safety and data protection standards.

The analysis of the responsibilities of AI system developers and operators under this regulatory act revealed that developers are required to ensure transparency and inform users about the functioning of AI systems, their capabilities, and limitations. They must also maintain detailed technical documentation and keep records of system operations for retrospective analysis and the identification of potential errors. Operators, in turn, are obligated to use AI systems in accordance with developers' instructions, provide adequate training for personnel, continuously monitor system performance, and adhere to data protection and confidentiality requirements.

To achieve the research objectives, general scientific methods of knowledge were used, including dialectical, historical, formal-logical (dogmatic), systems analysis, synthesis, deduction, induction, as well as specialized scientific methods such as formal-legal, comparative-legal, analogy method, and legal modeling.

Key words: *artificial Intelligence (AI), civil liability, drones, IT law, legal regime, legal regulation, objects of civil rights, unmanned aerial vehicles (UAVs), unmanned vehicles (UVs).*

Вступ. Швидкий розвиток технологій штучного інтелекту (далі також – ШІ) створює нові можливості для різних секторів економіки, включаючи транспортну галузь. Однією з найбільш перспективних областей застосування ШІ є безпілотні транспортні засоби (далі також – БПТЗ), які обіцяють значно підвищити ефективність і безпеку транспортних систем. Однак, використання БПТЗ також ставить перед правовою системою нові виклики, що вимагають чіткої регламентації та визначення правових рамок для забезпечення належного рівня безпеки, захисту прав користувачів та інших учасників дорожнього руху.

Оскільки базовою технологією для функціонування та розвитку БПТЗ є штучний інтелект, то прийняття Європейським Парламентом Акту про штучний інтелект 13 березня 2024 року стало важливим кроком у гармонізації правил для ШІ систем у Європейському Союзі. Цей нормативно-правовий акт спрямований на створення єдиного правового поля для розробки, впровадження та використання ШІ технологій, включаючи безпілотні транспортні засоби. Акт передбачає комплекс вимог щодо прозорості, технічної документації, оцінки ризиків та управління ними, а також дотримання вимог безпеки та захисту даних. Особлива увага приділяється відповідальності розробників та операторів ШІ систем, що є ключовим аспектом для забезпечення належного функціонування БПТЗ.

Аналіз останніх досліджень і публікацій показує, що значна кількість наукових праць присвячена розробці технічних аспектів ШІ та безпілотних транспортних засобів, а також їх правовому регулювання і впливу цієї технології на права людини. Серед закордонних вчених значну увагу цим питанням у своїх роботах приділяють Лаура Осса, Патрісіа Гомез, Йонас Талберг, Магнус Лудгрен та деякі інші. На вітчизняному рівні питанню правового регулювання ШІ значну увагу приділяють Шишка Н.В., Мічурін Є.О. та інші. Водночас, з огляду на стрімкий розвиток технології, нам видається, що згадане питання є недостатньо дослідженим як на національному, так і на міжнародному рівні і потребує додаткового доктринального опрацювання.

Незважаючи на наявність численних досліджень, залишаються невирішеними деякі аспекти правового регулювання БПТЗ, зокрема питання цивільно-правової відповідальності розробників та операторів ШІ систем.

Постановка завдання. Метою цієї статті є аналіз ризик-орієнтованого підходу Акту про штучний інтелект та дослідження його впливу на правове регулювання безпілотних транспортних засобів у Європейському Союзі. Цілями статті є аналіз основних положень Акту про штучний інтелект, що регулюють розвиток, впровадження та використання «high-risk» систем ШІ, зокрема безпілотних транспортних засобів, визначення відповідальності розробників та операторів цих систем, а також оцінка правових наслідків впровадження Акту для безпілотних транспортних засобів у Європейському Союзі. Окрім того, стаття має на меті розробити рекомендації щодо удосконалення правового регулювання БПТЗ для забезпечення більшої безпеки та підтримки інновацій у сфері ШІ в Україні. У роботі також зосереджено увагу на визначенні відповідальності розробників та операторів, що є ключовим для забезпечення безпеки та ефективності використання БПТЗ, їх комерційного використання та визначення рівня оборотоздатності.

Результати дослідження. Акт про ШІ складається з 13 розділів та 113 статей. Цей нормативно-правовий акт спрямований на вдосконалення європейського ринку шляхом сприяння використанню штучного інтелекту, який є безпечним, поважає права людини та захищає здоров'я, безпеку та навколишнє середовище. Він встановлює правила продажу, використання та моніторингу штучного інтелекту в ЄС, а також забороняє певні практики застосування ШІ. Він також встановлює конкретні правила для систем штучного інтелекту з високим ступенем ризику та їхніх операторів і вимагає, щоб певні системи штучного інтелекту були прозорими. Акт також містить правила продажу моделей ШІ загального призначення та заходи з підтримки інновацій, особливо для малого бізнесу та стартапів.

Першою важливою новелою Акту про штучний інтелект стало те, що законодавець уперше на загальноєвропейському нормативному рівні (фактично у статусі закону, а не Білої книги як це було раніше у 2020 році) дав визначення поняттю системи штучного інтелекту, яка відповідно до пункту 1 статті 3 «означає машинну систему, яка розроблена для роботи з різним рівнем автономності та може демонструвати адаптивність після розгортання, і яка, для явних або неявних цілей, робить висновки на основі отриманих вхідних даних, яким чином генерувати вихідні дані, такі як прогнози, контент, рекомендації або рішення, які можуть впливати на фізичне або віртуальне середовище» [1]. Водночас, акт не дає визначення поняттю «штучний інтелект», а оперує категорією «ШІ система».

Науковці, які працювали над Актом про ШІ, зокрема Йохан Лаукс, Сандра Вахтер та Брендт Міттерштадт зазначають, що «зусилля, спрямовані на розробку «надійного ШІ» за допомогою регуляторних законів, таких як Закон про ШІ, визнають необхідність довіри до ШІ для його широкого впровадження. Це, очевидно, передбачає, що ШІ може бути можливим об'єктом довіри» [7]. Група експертів високого рівня зі штучного інтелекту (AI HLEG), експертна група, призначена для консультування Європейської комісії щодо її стратегії у сфері штучного інтелекту, у своїх «Керівних принципах етики для надійного ШІ» 2019 року [5, с. 4] визначає «довіру» як не що інше, як «фундамент суспільства». Дослідження показують, що довіра пов'язана з такими позитивними змінами, як вищий рівень економічного зростання, вищий рівень громадянської активності, вища якість державного управління та нижчий рівень злочинності й корупції. Акт про штучний інтелект покликаний стати інструментом регулювання ризиків, спрямованого на зміцнення довіри до штучного інтелекту, обидва причинно-наслідкові зв'язки мають важливе значення. По-перше, якщо довіра до інституцій визначає прийнятність ризиків, пов'язаних зі штучним інтелектом, то для того, щоб Акт про штучний інтелект був успішним (правозастосовним), він сам повинен викликати довіру. По-друге, якщо сприйняття прийнятності ризиків визначає довіру, то вирішальне значення матимуть фактичні результати застосування ШІ та ставлення суспільства до цієї технології в цілому.

Закон про штучний інтелект спирається на складну мережу довірчих відносин, які він лише неявно і недостатньо диференціює. Стаття 3 Акту про штучний інтелект визначає такі ролі як «провайдер», «користувач», «розповсюджувач», «нотифікований орган» тощо. Ця таксономія суб'єктів у сфері штучного інтелекту не є чіткою. Ролі провайдерів і користувачів «можуть легко переплітатися, наприклад, коли користувач надає розробнику навчальні дані» [8]. Більше того, не існує визначеної «ролі» для адресатів або суб'єктів рішення чи прогнозу ШІ. Такими суб'єктами можуть бути громадяни, від яких, ймовірно, очікується довіра до системи регулювання ШІ «у цілому». Це ставить під сумнів так звану патерналістську (партисипативну) модель регулювання ризиків, яка була обрана Європейською комісією.

Найважливішою концепцією Акту про ШІ є ризик-орієнтований підхід з чотирма рівнями ризику для систем ШІ:

1) Системи неприйнятного ризику (регламентується главою 2 Акту) [2].

Системи штучного інтелекту з неприйнятними ризиками будуть заборонені на території ЄС через шість місяців після набуття чинності. До таких систем належать такі (з певними винятками):

– використання підсвідомих, маніпулятивних або оманливих методів, що спотворюють поведінку та заважають ухваленню обґрунтованих рішень, завдаючи значної шкоди;

– використання вразливостей, пов'язаних з віком, інвалідністю або соціально-економічними обставинами, з метою спотворення поведінки, що (з достатньою ймовірністю) спричиняє значну шкоду;

– біометричні системи категоризації, що виводять чутливі атрибути;

– соціальний скоринг, тобто оцінка або класифікація осіб або груп на основі соціальної поведінки або особистих характеристик, що спричиняє шкідливе або несприятливе ставлення до цих людей;

– оцінка ризику вчинення особою кримінальних правопорушень виключно на основі профайлінгу або особистісних рис і характеристик;

– створення баз даних розпізнавання осіб шляхом нецільового зчитування;

– визначення емоцій на робочих місцях або в навчальних закладах, за винятком систем штучного інтелекту з медичних міркувань та міркувань безпеки;

– дистанційна біометрична ідентифікація в режимі реального часу в публічно доступних місцях для правоохоронних органів (за винятком випадків, коли її використання є суворо необхідним у певних визначених сценаріях).

2) Системи високого ризику (регламентується главою 3 Акту) [3].

До систем штучного інтелекту з високим ступенем ризику Акт про штучний інтелект встановлює детальні та всеосяжні зобов'язання та вимоги, які застосовуються переважно до постачальників і розповсюджувачів цих систем. Ці зобов'язання стосуються широкого кола заходів з управління ШІ та технічних втручань (зокрема, прозорості, управління ризиками, підзвітності, управління даними, людського нагляду, точності, надійності та кібербезпеки), які необхідно впроваджувати на етапах проектування та розробки, а також контролювати та підтримувати протягом усього життєвого циклу ШІ. Існує дві основні групи систем ШІ з високим рівнем ризику:

Системи, регламентовані Додатком II, тобто системи, призначені для використання в якості компонента безпеки продукту або які самі є продуктом, на який поширюється законодавство ЄС в Додатку II і який повинен пройти оцінку відповідності; це, як правило, системи ШІ, що використовуються в контексті схильних до ризику, суворо регульованих продуктів.

Системи, регламентовані Додатком III, тобто системи ШІ, призначені для служіння спеціальним цілям, переліченим у Додатку III, зокрема:

– незаборонені біометричні дані;

– критична інфраструктура;

– освіта та професійна підготовка, включаючи системи для визначення доступу або вступу, оцінки результатів навчання, моніторингу та виявлення забороненої поведінки під час тестів;

– зайнятість, управління працівниками та доступ до самозайнятості, включаючи системи найму, відбору, моніторингу, звільнення або просування по службі;

– доступ до основних державних і приватних послуг та користування ними, включаючи кредитний скоринг, а також ціноутворення у сфері медичного страхування та страхування життя;

– правоохоронна діяльність;

– управління міграцією, наданням притулку та прикордонним контролем;

– відправлення правосуддя та демократичні процеси, включно зі штучним інтелектом, що впливає на вибори, наприклад, алгоритми рекомендацій у соціальних мережах.

Якраз до цієї категорії варто також відносити і ШІ системи, на базі яких побудовані безпілотні транспортні засоби. Постачальники високоризикових систем штучного інтелекту повинні реєструвати їх у спеціалізованій базі даних [6] перед виходом на ринок. Ця база буде створена та керуватиметься Комісією, яка також забезпечить технічну та адміністративну підтримку постачальникам. Відомості, що містяться у базі даних ЄС, будуть відкриті для громадськості.

Відповідно до ст.ст. 8–17 Акту, постачальники систем ШІ з високим ступенем ризику повинні впровадити систему управління ризиками протягом усього життєвого циклу системи ШІ з високим ступенем ризику; здійснювати управління даними, гарантуючи, що навчальні, валідаційні та тестові набори даних є релевантними, достатньо репрезентативними та, наскільки це можливо, не містять помилок і є повними відповідно до цільового призначення; складати технічну документацію для демонстрації відповідності та надавати органам влади інформацію для оцінки цієї відповідності; розробити систему штучного інтелекту для ведення обліку високих ризиків, щоб вона могла автоматично реєструвати події, важливі для виявлення ризиків на національному рівні, а також суттєві модифікації протягом життєвого циклу системи; надати інструкції з використання для подальшого розгортання системи, щоб забезпечити її відповідність нормативним вимогам; запровадити систему управління якістю для забезпечення відповідності вимогам.

3) Системи обмеженого ризику (регламентується главою 5 Акту) [4].

Системи ШІ з обмеженим ризиком повинні відповідати мінімальним вимогам щодо прозорості та/або маркування. Зобов'язання щодо прозорості стосуються насамперед систем ШІ, призначених для безпосередньої взаємодії з фізичними особами. Крім того, компромісний текст вимагає від постачальників систем ШІ, що генерують синтетичний аудіо-, відео- або текстовий контент, забезпечити маркування вихідних даних систем ШІ в машиночитному форматі, щоб їх можна було виявити як штучно створені або підроблені. Ці провайдери повинні також забезпечити ефективність, інтероперабельність, стійкість і надійність своїх технічних рішень. Додаткові зобов'язання щодо прозорості та маркування існують для розробників певних систем ШІ (які уможливлюють розпізнавання емоцій або біометричну категоризацію, глибокі підробки або маніпуляції з текстами, що становлять суспільний інтерес). Інші системи ШІ з мінімальними ризиками можуть бути охоплені майбутнім добровільним кодексом поведінки, який буде створений відповідно до Закону про ШІ.

4) Системи загального призначення (регламентується главою 5 Акту) [4].

Класифікація систем ШІ на основі ризиків доповнена правилами для моделей ШІ загального призначення (GPAI), які були введені в текст у відповідь на появу фундаментальних моделей, таких як «великі мовні моделі» («LLMs»). Конкретні зобов'язання для цих моделей можна згрупувати в наступні чотири категорії – з додатковими зобов'язаннями для таких моделей ШІ загального призначення, які тягнуть за собою системні ризики: складання та підтримка в актуальному стані технічної документації моделі, включаючи процес навчання, тестування та результати оцінки; забезпечення прозорості для постачальників систем, які бажають інтегрувати модель у власну систему ШІ; впровадження політики дотримання законодавства про авторські права та публікація детального звіту про навчальні дані, використані під час розробки моделі.

Провайдери GPAI з системним ризиком (який буде оцінюватися на основі технічних порогових значень, що вказують на високий рівень впливу, який буде розвиватися в майбутньому) повинні додатково проводити оцінку моделей, впроваджувати заходи з оцінки та зменшення ризиків, підтримувати процедури реагування на інциденти та звітування про них, а також забезпечувати належний рівень захисту кібербезпеки. Комісія ЄС може ухвалювати підзаконні НПА для зміни порогових значень.

Акт про штучний інтелект також передбачає широкі правозастосовні повноваження та потенційно високі штрафи. Штрафи повинні бути ефективними, пропорційними та стримуючими і можуть мати значний вплив на бізнес. Вони варіюються від 7,5 до 35 млн євро або від 1,5 до 7% світового річного обороту (залежно від того, яка з цих сум вища – у випадку МСП, включаючи стартапи, залежно від того, яка з них нижча), залежно від тяжкості порушення.

Висновки. Акт про штучний інтелект є важливим кроком у гармонізації правового регулювання ШІ в Європейському Союзі. Він встановлює чіткі вимоги щодо прозорості, технічної документації, управління ризиками, безпеки та захисту даних для систем ШІ, включаючи вимоги до провайдерів та постачальників ШІ систем на базі яких побудовані сучасні безпілотні транспортні засоби. Основна мета цього акту – забезпечення високого рівня захисту прав людини та безпеки, а також підтримка інновацій у сфері ШІ. Важливою новелою є впровадження ризик-орієнтованого підходу, що класифікує системи ШІ на чотири рівні ризику, зокрема, системи високого ризику, які потребують особливої уваги та дотримання строгих вимог.

Акт також акцентує увагу на відповідальності розробників та операторів ШІ систем, що є ключовим для забезпечення безпеки та ефективності. Україна, з огляду на обраний нею євроінтеграційний шлях, повинна буде з часом також імплементувати ці норми у свою правову систему. Це забезпечить гармонізацію українського законодавства з європейським, сприятиме розвитку інноваційних технологій, зокрема безпілотних транспортних засобів, та підвищить рівень захисту прав людини і безпеки. Така імплементація вимагатиме значних зусиль та ресурсів, але буде важливим кроком на шляху до європейської інтеграції та розвитку технологічного потенціалу країни.

Саме тому, уже зараз є сенс розробити і прийняти дорожню карту змін до національного законодавства і, у першу чергу, до затвердженої в грудні 2021 року Концепції розвитку штучного інтелекту в Україні. Робота над такими змінами дозволить не просто підсилити євроінтеграційні процеси, але і закладе правові підвалини для створення в Україні технологічного хабу розробки рішень на базі штучного інтелекту.

Список використаних джерел:

1. Article 3: Definitions | EU Artificial Intelligence Act. EU Artificial Intelligence Act | Up-to-date developments and analyses of the EU AI Act. URL: https://artificialintelligenceact.eu/article/3/ (date of access: 08.06.2024).

2. Article 5: Prohibited Artificial Intelligence Practices | EU Artificial Intelligence Act. EU Artificial Intelligence Act | Up-to-date developments and analyses of the EU AI Act. URL: https://artificialintelligenceact.eu/article/5/ (date of access: 08.06.2024).

3. Chapter III: High-Risk AI System | EU Artificial Intelligence Act. EU Artificial Intelligence Act | Up-to-date developments and analyses of the EU AI Act. URL: https://artificialintelligenceact.eu/chapter/3/ (date of access: 08.06.2024).

4. Chapter V: General Purpose AI Models | EU Artificial Intelligence Act. EU Artificial Intelligence Act | Up-to-date developments and analyses of the EU AI Act. URL: https://artificialintelligenceact.eu/chapter/5/ (date of access: 08.06.2024).

5. Ethics guidelines for trustworthy AI. Shaping Europe's digital future. URL: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419 (date of access: 08.06.2024).

6. EUR-Lex – 52021PC0206 – EN – EUR-Lex. EUR-Lex – Access to European Union law. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0206#:~:text=

title%20vii-,EU%20DATABASE%20FOR%20STAND-ALONE%20HIGH-RISK%20AI%20SYSTEMS,-Article%2060 EU (date of access: 08.06.2024).

7. Laux J., Wachter S., Mittelstadt B. Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk. Regulation & Governance. 2023. URL: https://doi.org/10.1111/rego.12512 (date of access: 08.06.2024).

8. Zarra A., de Andrade N. N. G. Artificial Intelligence Act: A Policy Prototyping Experiment: Operationalizing the Requirements for AI Systems – Part I. Search eLibrary: SSRN. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4365515 (date of access: 08.06.2024).