УДК 340.13
DOI https://doi.org/10.24144/2788-6018.2025.03.3.44

АКТ ПРО ШТУЧНИЙ ІНТЕЛЕКТ (ARTIFICAL INTELIGENCE ACT, AI ACT) ЯК ОСНОВА ПРАВОВОГО РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ЄС: ОГЛЯД ОСНОВНИХ ПОЛОЖЕНЬ

Забокрицький І.І.,
доктор юридичних наук, доцент,
доцент кафедри теорії права та конституціоналізму
Інституту права, психології та інноваційної освіти
НУ «Львівська політехніка»

Забокрицький І.І. Акт про Штучний Інтелект (Artifical Inteligence Act, AI Act) як основа правового регулювання штучного інтелекту в ЄС: огляд основних положень.

В даній статті здійснено огляд основних положень Акту про штучний інтелект (Artificial Intelligence Act або AI Act) який набув чинності як Регламент ЄС в 2014 році. Вказано, що одна з головних світових тенденцій останніх років – це активний розвиток штучного інтелекту, його застосування та стверджується, що оскільки AI Act є одним із перших в світі правових актів, який покликаний регулювати штучний інтелект, а також враховуючи курс України на євроінтеграцію, важливо дослідити основні питання, які врегульовуються в AI Act, оскільки його положення також можуть лягти в основу українського законодавства, предметом регулювання якого буде штучний інтелект. Зроблено висновок, що поділ на види ризику, який лежить в основі діяльності тої чи іншої системи штучного інтелекту та є базовим для AI Act є надзвичайно вдалим підходом, який розділяє рівні регулювання в залежності від того, який саме ризик лежить в основі системи штучного інтелекту.

Зроблено короткий огляд основних положень та перелічено суб'єктів, до яких застосовується AI Act. Зроблено висновок, що коло суб'єктів визначено надзвичайно широко. Мета такого широкого визначення є зрозумілою – широкий перелік суб'єктів необхідний для запобігання ухиленню від регулювання будь-якими способами, в першу чергу непрямими. Сам факт використання систем штучного інтелекту в ЄС, навіть якщо розробники, постачальники таких систем розміщені поза межами Європейського Союзу, вже є достатнім щоб такі суб'єкти підпадали під регулювання. Це саме стосується суб'єктів, які знаходяться в ЄС, а також будь-яких імпортерів, дистриб'юторів, представників.

Зроблено висновок, що окремі практики застосування штучного інтелекту є забороненими, хоча для певних із них, такі як використання систем дистанційної біометричної ідентифікації в режимі реального часу у загальнодоступних місцях для цілей правоохоронної діяльності, передбачено виключення, які базуються на принципі пропорційності та за умови наявності легітимної мети використання штучного інтелекту в такому випадку. Це дозволяє гнучко підходити до правового регулювання штучного інтелекту – запобігати ризикам, разом з тим не обмежуючи ті випадки, коли використання таких систем є доцільним та корисним для суспільства.

Ключові слова: Акт про штучний інтелект, AI Act, ЄС, правове регулювання штучного інтелекту.

Zabokrytskyy I.I. The Artificial Intelligence Act (AI Act) as the basis for legal regulation of artificial intelligence in the EU: review of the main provisions.

This article reviews the main provisions of the Artificial Intelligence Act (AI Act), which entered into force as an EU Regulation in 2014. It is indicated that one of the main global trends in recent years is the active development of artificial intelligence and its application, and it is argued that since the AI Act is one of the first legal acts in the world designed to regulate artificial intelligence, and also taking into account Ukraine's course towards European integration, it is important to examine the main issues regulated in the AI Act, since its provisions may also form the basis of Ukrainian legislation, the subject of regulation of which will be artificial intelligence. It is concluded that the division into types of risk that underlies the activities of a particular artificial intelligence system and is the basis for the AI Act is an extremely successful approach that separates the levels of regulation depending on the specific risk that underlies the artificial intelligence system.

A brief overview of the main provisions is made and the subjects to which the AI Act applies are listed. It is concluded that the range of subjects is defined extremely broadly. The purpose of such a broad definition is clear – a wide list of subjects is necessary to prevent evasion of regulation by any means, primarily indirect ones. The very fact of using artificial intelligence systems in the EU, even

if the developers and suppliers of such systems are located outside the European Union, is already sufficient for such subjects to be subject to regulation. This applies to subects located in the EU, as well as any importers, distributors, representatives.

It is concluded that certain practices of using artificial intelligence are prohibited, although for some of them, such as the use of remote biometric identification systems in real time in public places for law enforcement purposes, exceptions are provided for, which are based on the principle of proportionality and provided that there is a legitimate purpose for using artificial intelligence in such a case. This allows for a flexible approach to the legal regulation of artificial intelligence – to prevent risks, while not limiting those cases where the use of such systems is appropriate and beneficial to society.

Key words: Artificial Intelligence Act, AI Act, EU, legal regulation of artificial intelligence.

Постановка проблеми. Одна з головних світових тенденцій останніх років – це активний розвиток штучного інтелекту, його застосування. З тих пір як в 2022 році дебютував відомий чат-бот ChatGPT [1], його використання стає все більш поширеним. За одними з останніх даних у світі є більше ніж 180 мільйонів користувачів ChatGPT [2]. І це лише кількість користувачів цього чат-бота. Загалом же ж кількість різноманітних мовних моделей, тощо, стає все більшою. Ці дані свідчать про беззаперечний факт – використання штучного інтелекту стає масовим, а його розвиток – стрімким. Саме тому важливо, щоб правове регулювання не відставало від розвитку штучного інтелекту, оскільки потрібно, щоб існували належні рамки, в межах яких такий розвиток відбувається, для того щоб мінімізувати ризики та загрози, які можуть виникнути як для користувачів, так і для суспільства. Одним із правових актів, які з'явились в цій сфері є Закон про штучний інтелект – Artificial Intelligence Act (надалі – AI Act), який був остаточно прийнятий 21 травня 2024 року та набув чинності 1 серпня 2024 року [3]. Оскільки AI Act є одним із перших в світі правових актів, який покликаний регулювати штучний інтелект, а також враховуючи курс України на євроінтеграцію, важливо дослідити основні питання, які врегульовуються в AI Act, оскільки його положення також можуть лягти в основу українського законодавства, предметом регулювання якого буде штучний інтелект.

Відтак, **метою** даної статті є огляд основних положень та узагальнення AI Act, виокремлення основних питань які він регулює та їх аналіз.

Щодо стану опрацювання проблематики, то оскільки як сам AI Act був прийнятий лише нещодавно, так і розвиток штучного інтелекту, чат-ботів, мовних моделей інтенсифікувався лише з 2022 р., то опрацювання проблематики перебуває лише на зародковому рівні.

Виклад основного матеріалу. 1 серпня 2024 р. Європейська Комісія опублікувала прес-реліз щодо набуття чинності AI Act, в якому вказано, що AI Act спрямований на усунення потенційних ризиків для здоров'я, безпеки та основоположних прав громадян. Він надає розробникам і впроваджувачам чіткі вимоги та зобов'язання щодо конкретних видів використання штучного інтелекту, водночас зменшуючи адміністративний і фінансовий тягар для бізнесу. AI Act запроваджує єдині рамки для всіх країн ЄС, засновані на перспективному визначенні штучного інтелекту та підході, що ґрунтується на оцінці ризиків:

- Мінімальний ризик: більшість систем штучного інтелекту, таких як спам-фільтри та відеоігри зі штучним інтелектом, не несуть жодних зобов'язань відповідно до AI Act, але компанії можуть добровільно прийняти додаткові кодекси поведінки.
- Ризик недостатньої прозорості: такі системи, як чат-боти, повинні чітко інформувати користувачів про те, що вони взаємодіють з машиною, а певний контент, створений штучним інтелектом, повинен бути позначений як такий.
- Високий ризик: системи штучного інтелекту з високим ступенем ризику, такі як медичне програмне забезпечення на основі штучного інтелекту або системи штучного інтелекту що використовуються для підбору персоналу, повинні відповідати суворим вимогам, включаючи системи зниження ризиків, високу якість наборів даних, чітку інформацію для користувачів, людський нагляд тощо.
- Неприйнятний ризик: наприклад, системи штучного інтелекту, які дозволяють урядам або компаніям проводити «соціальний скоринг», вважаються явною загрозою основним правам людини і тому заборонені [4].

На наше переконання, такий поділ на види ризику, які лежать в основі AI Act є надзвичайно вдалим підходом, який розділяє рівні регулювання в залежності від того, який саме ризик лежить в основі системи штучного інтелекту. Зрозуміло, що у випадку низького ризику, наприклад щодо відеоігор зі штучним інтелектом, не є доцільним застосовувати значні регуляції та покладати адміністративний тягар на компанії, які розробляють такі ігри. Разом з тим, якщо ризик високий, як у випадку систем штучного інтелекту, що використовуються для підбору персоналу, то використання

таких систем несе значні ризики на практиці для конкретних осіб. Наприклад, системи для підбору персоналу можуть бути наперед натреновані на певних даних, які демонструють упередженість щодо тієї чи іншої категорії осіб, а отже посилювати дискримінацію, і не надавати рівний доступ до отримання роботи для заявників, які історично були дискриміновані. Тому, якщо ці системи будуть використовуватись неналежним чином, то це несе загрозу порушення прав людини.

Отже, ми погоджуємось з думкою Європейської Комісії, яка вказує що «ЄС прагне стати світовим лідером у сфері безпечного штучного інтелекту. Розробляючи міцну регуляторну базу, засновану на правах людини та фундаментальних цінностях, ЄС може створити екосистему штучного інтелекту, яка принесе користь усім. Це означає кращу охорону здоров'я, безпечніший та чистіший транспорт, а також покращені державні послуги для громадян. Це пропонує інноваційні продукти та послуги, зокрема в енергетиці, безпеці та охороні здоров'я, а також вищу продуктивність та ефективніше виробництво для бізнесу, тоді як уряди можуть скористатися перевагами дешевших та більш сталих послуг, таких як транспорт, енергетика та управління відходами» [4].

Наведемо короткий огляд та аналіз основних положень AI Act. Так, ч. 2 ст. 1 цього Регламенту вказує, що Цей Регламент встановлює:

- гармонізовані правила розміщення на ринку, введення в експлуатацію та використання систем штучного інтелекту в Союзі;
- заборони на певні види практик ШІ;
- спеціальні вимоги до систем ШІ з високим рівнем ризику та зобов'язання для операторів таких систем;
- гармонізовані правила прозорості для певних систем ШІ;
- гармонізовані правила розміщення на ринку моделей ШІ загального призначення;
- правила моніторингу ринку, ринкового нагляду, управління та правозастосування;
- заходи для підтримки інновацій, з особливим акцентом на підприємства малого та середнього бізнесу, включаючи стартапи [3].

Щодо суб'єктів, до яких він застосовується, то їхнє коло визначено в ч. 1 ст. 2 Регламенту, а саме:

- постачальники, що розміщують на ринку або вводять в експлуатацію системи штучного інтелекту, або розміщують на ринку моделі штучного інтелекту загального призначення в Союзі, незалежно від того, чи ці постачальники зареєстровані або розташовані в Союзі, чи в третій країні;
- розгортачі систем штучного інтелекту, які мають місцезнаходження або розташовані в Союзі;
- постачальники та розгортачі систем штучного інтелекту, які мають місцезнаходження або розташовані в третій країні, де результат, вироблений системою штучного інтелекту, використовується в Союзі;
- імпортери та дистриб'ютори систем штучного інтелекту;
- виробники продукції, що розміщують на ринку або вводять в експлуатацію систему штучного інтелекту разом зі своїм продуктом та під своїм ім'ям або торговою маркою;
- уповноважені представники постачальників, які не зареєстровані в Союзі;
- зацікавлені особи, які розташовані в Союзі [3].

Як бачимо, коло суб'єктів визначено надзвичайно широко. Мета такого широкого визначення є зрозумілою – широкий перелік суб'єктів необхідний для запобігання ухиленню від регулювання будь-якими способами, в першу чергу нерпямими. Сам факт використання систем штучного інтелекту в ЄС, навіть якщо розробники, постачальники таких систем розміщені поза межами Європейського Союзу, вже є достатнім щоб такі суб'єкти підпадали під регулювання. Це саме стосується суб'єктів, які знаходяться в ЄС, а також будь-яких імпортерів, дистриб'юторів, представників.

Окремо вважаємо за необхідне звернути увагу на практики використання штучного інтелекту, які є забороненими. Такі практики визначені в ст. 5 Регламенту. Не будемо перелічувати всі із них, а натомість опишемо ті, які найкраще ілюструють мету регулювання

- розміщення на ринку, введення в експлуатацію або використання системи штучного інтелекту, яка використовує підсвідомі методи поза свідомістю людини або цілеспрямовано маніпулятивні чи оманливі методи, з метою або наслідком суттєвого спотворення поведінки особи або групи осіб шляхом суттєвого порушення їхньої здатності приймати обґрунтоване рішення, що змушує їх приймати рішення, яке вони б інакше не прийняли, таким чином, що це завдає або обґрунтовано ймовірно завдасть цій особі, іншій особі або групі осіб значної шкоди (ч. 1 (а)) – такі системи штучного інтелекту розглядаються як маніпулятивні і несуть значні ризики порушення прав людини, а також загрози демократії;
- розміщення на ринку, введення в експлуатацію або використання системи штучного інтелекту, яка використовує будь-яку вразливість фізичної особи або певної групи осіб через їхній вік,

інвалідність або певну соціальну чи економічну ситуацію, з метою або наслідком суттєвого спотворення поведінки цієї особи або особи, що належить до цієї групи, таким чином, що це завдає або обґрунтовано ймовірно завдасть цій особі або іншій особі значної шкоди (ч. 1 (b)) – як бачимо, ці системи несуть значну загрозу дискримінації тієї чи іншої групи осіб, а отже є забороненими;

- розміщення на ринку, введення в експлуатацію або використання систем штучного інтелекту для оцінки або класифікації фізичних осіб або груп осіб протягом певного періоду часу на основі їхньої соціальної поведінки або відомих, виведених або передбачуваних особистих чи особистісних характеристик (ч. 1 (c)) – такі способи використання штучного інтелекту, до яких вдаються деякі держави (наприклад Китай) несуть значні ризики обмеження свободи слова, вираження думки, а також порушенню інших прав людини, а отже є забороненими згідно AI Act;
- розміщення на ринку, введення в експлуатацію для цієї конкретної мети або використання системи штучного інтелекту для проведення оцінки ризиків фізичних осіб з метою оцінки або прогнозування ризику вчинення фізичною особою кримінального злочину, виключно на основі профілювання фізичної особи або оцінки її рис та характеристик особистості (ч. 1 d)) – такі системи штучного інтелекту несуть ризики використання так званого профайлінгу – систему оцінювання, яка прогнозує схильність до вчинення тих чи інших діянь. Профайлінг сам по собі несе загрозу упередженого ставлення, оскільки діяння ще не відбулось, але ту чи іншу людину (яка, цілком можливо, навіть і в думці може не мати вчиняти певне діяння), вже оцінюють негативно, що може виразитись у зміні ставлення до неї.

Окрему увагу хочемо звернути на приклад, який демонструє як заборону, так і винятки із такої заборони, коли використання системи штучного інтелекту має легітимну мету. Ця заборона передбачена в ч. 1 (h) – використання систем дистанційної біометричної ідентифікації в режимі реального часу у загальнодоступних місцях для цілей правоохоронної діяльності, окрім випадків, коли таке використання є суворо необхідним для однієї з наступних цілей: (i) цільовий пошук конкретних жертв викрадення, торгівлі людьми або сексуальної експлуатації людей, а також пошук зниклих безвісти осіб; (ii) запобігання конкретній, суттєвій та безпосередній загрозі життю або фізичній безпеці фізичних осіб або реальній та поточній чи реальній та передбачуваній загрозі терористичного нападу; (iii) виявлення місця розташування або ідентифікація особи, підозрюваної у скоєнні кримінального злочину, з метою проведення кримінального розслідування або кримінального переслідування, або виконання кримінального покарання за злочини, зазначені в Додатку II (цей додаток передбачає список злочинів, таких як тероризм, вбивство, викрадення людини, згвалтування, тощо – *прим. Автора*), які караються у відповідній державі-члені позбавленням волі або постановою про тримання під вартою на максимальний строк не менше чотирьох років. Вважаємо, що це є надзвичайно збалансований підхід, який впроваджує принцип пропорційності у регулювання, оскільки насправді таке використання штучного інтелекту, яке має легітимну мету, може бути надзвичайно корисним для суспільства та для запобігання злочинів, а отже повна заборона не є доцільною. Разом з тим, використання таких систем належним чином, з достатнім рівнем контролю (в тому числі адміністративного та судового) є необхідним для того, щоб принцип пропорційності був справді дотриманим.

Окрему увагу пропонуємо звернути на регулювання тих систем штучного інтелекту, які вважаються з високим ризиком. Обов'язки для провайдерів таких систем є розширеними, та включають в себе наступне (такі обов'язки визначені в статтях 8–17 Регламенту):

- Створити систему управління ризиками протягом усього життєвого циклу системи ШІ з високим рівнем ризику;
- Здійснювати управління даними, забезпечуючи, щоб набори даних для навчання, валідації та тестування були релевантними, достатньо репрезентативними та, наскільки це можливо, без помилок та повними відповідно до цільового призначення.
- Розробити технічну документацію для демонстрації відповідності та надати органам влади інформацію для оцінки цієї відповідності.
- Розробити свою систему ШІ з високим рівнем ризику для ведення обліку, щоб вона могла автоматично фіксувати події, що стосуються виявлення ризиків національного рівня, та суттєві зміни протягом життєвого циклу системи.
- Надавати інструкції з використання для наступних розробників, щоб забезпечити відповідність останніх вимогам.
- Розробити свою систему ШІ з високим рівнем ризику, щоб розробники могли здійснювати людський нагляд.
- Розробити свою систему ШІ з високим рівнем ризику для досягнення належного рівня точності, надійності та кібербезпеки.
- Створити систему управління якістю для забезпечення відповідності [5].

При цьому важливо зазначити, що стаття 96 Регламенту передбачає санкції, які в залежності від порушення варіюються від 1 до 7% загального річного доходу або ж від 7 500 000 до 35 000 000 євро, в залежності від того, що є вищим. Відмітимо, що такий підхід до санкцій певної мірою схожий до підходу, який існує в Загальному регламенті про захист персональних даних – GDPR.

Зрозуміло, що AI Act зараз знаходиться лише на початкових етапах його впровадження і існують певні недоліки . Так, такі науковці як Хенрік Нолте, Міріам Ратейке, Мішель Фінк вказують, що існують правові проблеми та недоліки в положеннях, пов'язаних із стійкістю та кібербезпекою для систем ШІ високого ризику (стаття 15 AI Act) та моделей ШІ загального призначення (стаття 55 AI Act) а також оцінюють потенційні проблеми у впровадженні цих положень у світлі останніх досягнень у літературі з машинного навчання (ML) [6]. Такі ж автори як Міхал Арашкевич, Гжегож Я. Налепа та Радослав Палош вважають, що стверджують, що підхід AI Act, який переважно ґрунтується на правилах, може недостатньо збалансувати захист основних прав із заохоченням інновацій. Вони виділяють три основні проблеми: недостатній захист фундаментальних прав через жорстке застосування правил, можливість надмірного навантаження на зобов'язані сторони через жорсткі структури управління та можливість постачальників штучного інтелекту обходити класифікацію високого ризику через нечіткі винятки [7].

Висновки. Як висновки, можемо стверджувати наступне. Прийняття AI Act є надзвичайно прогресивним і нагальним кроком у сфері регулювання штучного інтелекту в ЄС. Враховуючи список суб'єктів, до яких він застосовується, екстериторіальну дію (аналогічно до GDPR), належне вивчення та дослідження AI Act є необхідним для української науки та практики. Зрозуміло, що практика покаже як саме буде застосовуватись AI Act, разом з тим окремі його положення та принципи вже виглядають як такі, що гнучко підходять до правового регулювання, зокрема відмінності в підходах в залежності від того, якою є оцінка ризику тої чи іншої системи. Саме для цього є передбачені розширені обов'язки для провайдерів систем штучного інтелекту, які вважаються з високим ризиком. Важливо також наголосити на підходах до санкцій, які теж є схожими до тих, які наявні в GDPR, і варіюються в залежності від виду порушень, а базою для обчислення розміру санкцій є загальний річний дохід порушника. Окремі ж практики застосування штучного інтелекту є забороненими, хоча для певних із них, такі як використання систем дистанційної біометричної ідентифікації в режимі реального часу у загальнодоступних місцях для цілей правоохоронної діяльності, передбачено виключення, які базуються на принципі пропорційності та за умови наявності легітимної мети використання штучного інтелекту в такому випадку. Це дозволяє гнучко підходити до правового регулювання штучного інтелекту – запобігати ризикам, разом з тим не обмежуючи ті випадки, коли використання таких систем є доцільним та корисним для суспільства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. ChatGPT URL: https://chatgpt.com.
2. How Many Users on ChatGPT? URL: https://seo.ai/blog/how-many-users-does-chatgpt-have.
3. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.
4. AI Act enters into force. Directorate-General for Communication. URL: https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en.
5. High-level summary of the AI Act. URL: https://artificialintelligenceact.eu/high-level-summary.
6. Nolte, H., Rateike, M., & Finck, M. (2025). Robustness and Cybersecurity in the EU Artificia l Intelligence Act. arXiv. URL: https://arxiv.org/abs/2502.16184:contentReference[oaicite:2]{index=2}.
7. Araszkiewicz, M., Nalepa, G.J., & Pałosz, R. (2024). The Artificial Intelligence Act: Taking normative imbalances seriously. *Internet Policy Review*, 13(4). URL: https://policyreview.info/articles/news/artificial-intelligence-act-taking-normative-imbalances-seriously/1817:contentReference[oaicite:2]{index=2}.