

*Редченко Я. О.,**аспірант кафедри міжнародного та європейського права,  
Національного університету «Одеська юридична академія»*

## ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У РЕГУЛЮВАННІ ЦИФРОВИХ АКТИВІВ КРІЗЬ ПРИЗМУ МІЖНАРОДНО-ПРАВОВИХ ГАРАНТІЙ ПРАВ ЛЮДИНИ

**Анотація.** У статті досліджується використання штучного інтелекту у сфері регулювання цифрових активів крізь призму міжнародно-правових гарантій прав людини. Обґрунтовується, що цифровізація фінансових ринків, поширення криптоактивів, стейблкоїнів, токенизованих прав та інших форм цифрової вартості зумовили істотне ускладнення механізмів правового регулювання і контролю. У відповідь на це держави, міжнародні організації, фінансові регулятори та приватні постачальники послуг дедалі частіше застосовують системи штучного інтелекту для автоматизованого моніторингу транзакцій, оцінювання ризиків, виявлення шахрайства, санкційного скринінгу, процедур KYC/AML та ринкового нагляду.

Примітно, що використання ШІ у цій сфері дає подвійний ефект. З одного боку, алгоритмічні системи істотно збільшують швидкість і масштаб обробки даних, дозволяють виявляти приховані зв'язки між операціями, прогнозувати підозрілі схеми поведінки та посилювати ефективність фінансового моніторингу. З іншого боку, вони створюють ризики для основоположних прав людини. Передусім для права на приватність, захист персональних даних, майнові права, право на належну правову процедуру та право на ефективний засіб юридичного захисту.

Доведено, що правомірність використання штучного інтелекту у сфері цифрових активів повинна оцінюватися не лише крізь призму фінансового законодавства, а й у світлі міжнародних стандартів захисту прав людини. Особливого значення набувають Рамкова конвенція Ради Європи про штучний інтелект, права людини, демократію та верховенство права, Регламент ЄС про штучний інтелект (AI Act), Регламент MiCA, Загальний регламент про захист даних (GDPR) [5], позиції Європейської ради із захисту даних, стандарти UNESCO та підходи системи ООН у сфері прав людини і нових цифрових технологій. Саме сукупність цих актів формує сучасну міжнародно-правову рамку, в якій має розвиватися алгоритмізоване регулювання цифрових активів.

**Ключові слова:** штучний інтелект, цифрові активи, криптоактиви, права людини, міжнародне право, MiCA, AI Act, приватність, захист персональних даних.

**Постановка проблеми.** Сучасний розвиток цифрової економіки зумовив перехід від традиційних форм фінансового обігу до середовища, у якому дедалі більшу роль відіграють цифрові активи. Їхнє правове значення давно вийшло за межі суто технологічного феномену. Тепер цифрові активи виступають не лише об'єктом інвестування або інноваційним платіжним інструментом. Вони вже є складовою глобальної інфраструктури вартості, що перетинає межі держав, валютних систем і класичних механізмів юридичного контролю. Саме такі особливості й зумовлюють потребу в нових регуляторних інструментах,

здатних працювати з великими масивами даних у режимі реального часу [1, с. 117].

У зв'язку з цим штучний інтелект став одним із ключових технологічних інструментів, за допомогою яких відбувається сучасне регулювання цифрових активів. Алгоритмічні системи вже використовуються не лише у приватному секторі, а й у діяльності регуляторів та наглядових органів. Йдеться про автоматизований фінансовий моніторинг, виявлення нетипових транзакційних патернів, встановлення зв'язків між криптогаманцями, перевірку користувачів, верифікацію документів, аналіз поведінкових характеристик та виявлення ймовірних порушень санкційного, податкового чи антикорупційного законодавства [2, с. 148].

Однак така технологізація породжує новий рівень юридичної складності. Якщо раніше основна проблема полягала у визначенні правової природи цифрових активів та побудові належного режиму їхнього обігу, то нині до неї додається питання про допустимість алгоритмічного втручання у сферу прав людини. Автоматизовані рішення можуть впливати на доступ особи до фінансових сервісів, обмежувати операції, блокувати транзакції, зумовлювати посилений моніторинг або визначати статус користувача як «ризикового». За відсутності належних гарантій це створює небезпеку непрозорого втручання у права людини [3, с. 56].

Саме тому постає принципово важливе питання: чи можна вважати використання ШІ у сфері цифрових активів правомірним лише на тій підставі, що воно сприяє боротьбі з шахрайством, відмиванням коштів або санкційними порушеннями? Відповідь на нього має бути негативною. Ефективність регуляторного контролю сама по собі не усуває обов'язку держави та приватних суб'єктів поважати міжнародні стандарти прав людини. Навпаки, чим глибшим є втручання алгоритмів у фінансову автономію особи, тим вищими повинні бути гарантії законності, пропорційності, прозорості, підзвітності та оскаржуваності таких рішень.

У вітчизняній юридичній літературі проблема цифрових активів зазвичай розглядається крізь призму цивільного, господарського та фінансового права. І. Ю. Гулейков у дисертаційному дослідженні аналізує цифрові активи як об'єкти цивільного обороту та підкреслює, що їхній правовий режим не може бути адекватно описаний у межах лише однієї класичної категорії майна [4]. С. М. Защипас звертає увагу на необхідність розмежування понять «цифрові активи», «віртуальні активи» та «криптоактиви», оскільки від коректності термінології залежить якість законодавчого регулювання [5].

Проблематика штучного інтелекту і прав людини в українській правовій доктрині також набуває дедалі більшої уваги. І. М. Берназюк підкреслює, що ШІ створює нові виклики для людської гід-

ності, автономії, приватності та рівності, якщо його використання не супроводжується достатніми юридичними запобіжниками [6]. О. С. Котуха наголошує, що цифровізація права та державного управління об'єктивно вимагає створення нового покоління правових гарантій, які були б здатні обмежувати непрозорі автоматизовані рішення та забезпечувати належний захист особи [7].

У зарубіжній науковій літературі Joseph Lee аналізує застосування ШІ у фінансових послугах як сферу, де поєднуються переваги інновацій і ризики для доступу до фінансових сервісів, захисту даних та справедливості автоматизованих рішень [8, с. 742]. Dirk Zetzsche, досліджуючи режим МіСА, звертає увагу на те, що європейське регулювання криптоактивів спрямоване на посилення ринкової стабільності, прозорості та захисту інвестора, але в практичній площині неминуче поєднується з цифровими засобами контролю [9].

Водночас варто відзначити, що питання саме міжнародно-правових гарантій прав людини в умовах використання ШІ для регулювання цифрових активів залишається недостатньо розробленим. Наявні дослідження здебільшого або зосереджуються на правовій природі цифрових активів, або окремо аналізують правове регулювання ШІ. Менш дослідженою лишається саме точка їхнього перетину. У цьому, по суті, і полягає наукова актуальність цієї статті.

**Мета статті** полягає у визначенні особливостей використання штучного інтелекту у регулюванні цифрових активів та виявленні міжнародно-правових гарантій прав людини, які повинні застосовуватися у цій сфері.

Цифрові активи становлять неоднорідну категорію. У широкому сенсі до них можуть належати криптоактиви, стейблкоїни, токенизовані права вимоги, деякі форми цифрових фінансових інструментів, а також інші об'єкти вартості, що існують і обертаються в цифровому середовищі. Саме ця неоднорідність ускладнює побудову єдиного правового режиму та спонукає законодавця до функціонального підходу.

Найбільш системною сучасною моделлю секторального регулювання криптоактивів є правовий режим Європейського Союзу, закріплений у МіСА [10]. Застосування МіСА в повному обсязі розпочалося з 30 грудня 2024 року, а сам режим став важливим кроком до створення єдиної нормативної рамки для крипторинку ЄС. ESMA у грудні 2024 року окремо підкреслила, що початок застосування МіСА є значним кроком до впорядкування крипторинку, хоча сам новий режим не усуває всі ризики волатильності та невизначеності [10].

Значення МіСА полягає не лише у встановленні правил для постачальників криптоактивних послуг, а й у створенні середовища, де діяльність із цифровими активами стає об'єктом регулярного контролю, комплаєнсу, звітності й нагляду. Саме на цьому рівні і починає відігравати важливу роль ШІ. Чим більш формалізованим та інтенсивним є регулювання, тим більшою стає практична потреба в інструментах автоматизованої обробки інформації.

Отже, цифрові активи нині є не просто об'єктом цивільного або фінансового обороту. Вони є об'єктом алгоритмізованого регулювання, де правове значення має не тільки сам актив, а й спосіб технологічного контролю за його обігом. Коротко кажучи, змінився не лише предмет регулювання, а й інструментарій.

Використання ШІ у сфері цифрових активів має комплексний характер. Найпоширенішим напрямом є процедури KYC та цифрової ідентифікації. Алгоритми застосовуються для розпізнавання

документів, перевірки їхньої справжності, зіставлення зображення особи з документальними даними, аналізу поведінкових та технічних індикаторів. Такі системи дозволяють прискорити верифікацію клієнтів, але водночас пов'язані з обробкою чутливих персональних даних та ризиками помилкової ідентифікації [11].

Другим напрямом є AML/CFT-моніторинг. Сектор віртуальних активів визнається на міжнародному рівні таким, що потребує підвищеної уваги у сфері боротьби з відмиванням коштів та фінансуванням тероризму. У своєму targeted update 2025 року FATF вказала, що, попри певний прогрес, глобальне впровадження стандартів щодо віртуальних активів і VASP залишається нерівномірним, а багато юрисдикцій і досі мають фундаментальні прогалини у виконанні Recommendation 15 та супровідних вимог [12]. У цих умовах алгоритмічний аналіз операцій, адрес, зв'язків між суб'єктами та поведінкових патернів стає інструментом, який дає змогу хоча б частково компенсувати складність контролю за транскордонними потоками цифрової вартості.

Третім напрямом є blockchain analytics і wallet-risk scoring. Йдеться про побудову алгоритмічних моделей, які визначають рівень ризику конкретної адреси або користувача на основі історії транзакцій, зв'язків із іншими адресами, участі у змішувальних сервісах, взаємодії з певними протоколами чи платформами, а іноді й на основі зовнішніх санкційних або комплаєнс-списків. Юридично це особливо важливо, оскільки такі оцінки можуть мати прямі наслідки для доступу особи до послуг.

Четвертим напрямом є ринковий нагляд. На крипторинку, як і на традиційних фінансових ринках, існує ризик маніпулювання цінами, wash trading, spoofing та інших форм недобросовісного поведінки. Алгоритми можуть виявляти нетипові патерни торгівлі й сигналізувати про ймовірні порушення. З правового погляду це позитивна функція, однак її реалізація не повинна бути відірвана від гарантій справедливості та точності автоматизованого аналізу.

П'ятим напрямом є внутрішній комплаєнс постачальників криптопослуг. Суб'єкти ринку дедалі більше покладаються на ШІ для сортування ризиків, ранжування клієнтів, визначення рівня контролю, необхідності посиленої перевірки та навіть для пріоритизації кейсів для внутрішніх служб безпеки. Це означає, що алгоритмічні рішення дедалі частіше передують юридично значущим діям.

Сучасна міжнародно-правова рамка цієї сфери має багатовірневий характер. Її перший рівень становлять акти, безпосередньо присвячені цифровим активам та їх регулюванню, зокрема МіСА і стандарти FATF. Другий рівень становлять акти, що регулюють ШІ та автоматизовані системи, насамперед AI Act та Рамкова конвенція Ради Європи. Третій рівень включає загальні акти про фундаментальні права, зокрема GDPR, Хартію основних прав ЄС, а також міжнародні документи soft law та підходи ООН [10-17].

Особливого значення набуває Рамкова конвенція Ради Європи про штучний інтелект, права людини, демократію та верховенство права [3]. Рада Європи прямо визначає її як перший у світі міжнародно-правово зобов'язальний договір у сфері ШІ. Конвенцію було ухвалено 17 травня 2024 року, а для підписання її відкрито 5 вересня 2024 року [15]. Її головна цінність полягає в тому, що вона виводить дискусію про ШІ за межі суто технічного чи ринкового регулювання і прямо підпорядковує використання систем ШІ вимогам прав людини, демократії та верховенства права.

Для України значення Конвенції є особливо важливим, оскільки у травні 2025 року держава приєдналася до неї. Міністерство цифрової трансформації України зазначило, що цей документ визначає принципи, яких держава повинна дотримуватися у формуванні законодавства та застосуванні ШІ-продуктів, зокрема повагу до людської гідності, прозорість, недискримінацію, захист приватності, надійність і безпеку. Це надає досліджуваній проблемі безпосереднього значення і для української правової системи.

Не менш важливим є AI Act [15]. Його завдання полягає у встановленні гармонізованих правил для безпечного та надійного ШІ у межах ЄС. З правової точки зору варто звернути увагу на те, що AI Act від початку сконструйований як акт, спрямований не лише на розвиток інновацій, а й на забезпечення високого рівня захисту здоров'я, безпеки та фундаментальних прав [15]. Для сфери цифрових активів це означає, що автоматизовані системи, які можуть істотно впливати на правове становище особи, не можуть розглядатися виключно як технічний інструмент комплаєнсу.

GDPR і позиції EDPB [16] надають цій системі ще більшої конкретики. У грудні 2024 року EDPB прийняла Opinion 28/2024, де розглянула питання правової підстави використання персональних даних для AI-моделей, межі анонімізації та наслідки незаконної обробки даних на етапі розробки моделей [16]. Це має безпосереднє значення для цифрових активів, оскільки в цій сфері моделі ШІ часто навчаються або працюють на великих масивах поведінкових, транзакційних і технічних даних.

Важливу орієнтуючу роль відіграють і міжнародні стандарти soft law. UNESCO у своїй Recommendation on the Ethics of Artificial Intelligence наголошує, що захист прав людини та людської гідності є основою етичного регулювання ШІ, а серед базових принципів прямо називає прозорість, справедливість, підзвітність і людський нагляд [18]. OHCHR у Mapping Report 2024 року систематизує підходи системи ООН до нових цифрових технологій, включно зі штучним інтелектом, і підкреслює, що цифрові технології повинні оцінюватися крізь призму їхнього впливу на права людини.

Найочевиднішим правом, що опиняється під впливом алгоритмізованого регулювання цифрових активів, є право на приватність. Теза про те, що блокчейн нібито гарантує анонімність, давно втратила абсолютний характер. У сучасних умовах поєднання blockchain analytics, KYC-процедур, технічної телеметрії, пристроєвих даних, IP-адрес, історії транзакцій та зовнішніх баз даних створює високий потенціал ідентифікації особи. Якщо ж до цього додаються моделі ШІ, які прогнозують «ризиковану поведінку» або будують профіль користувача, відбувається перехід від простої фіксації фінансових дій до глибокого поведінкового аналізу. Це становить суттєву небезпеку для приватності, оскільки особа стає об'єктом не лише нагляду, а й імовірного оцінювання. У такій ситуації особливої ваги набувають принципи мінімізації даних, обмеження мети, пропорційності та законності обробки, закріплені у GDPR.

EDPB у своїй новітній позиції щодо AI-моделей прямо наголошує, що використання персональних даних при створенні та функціонуванні AI-моделей не виводить таку обробку за межі вимог європейського законодавства про захист даних [16]. Це означає, що жоден фінансово-комплаєнсний інтерес не скасовує потреби в чіткій правовій підставі, належній документації, прозорості та обмеженні надмірного втручання.

Наступним критично важливим виміром є право на недискримінацію. У випадку цифрових активів дискримінація далеко не завжди проявляється прямо. Вона може мати прихований алгоритмічний характер, коли певні моделі систематично відносять до підвищеної категорії ризику окремі групи користувачів на основі географічних, поведінкових, технічних або непрямих соціальних індикаторів.

Така ситуація особливо небезпечна тим, що дискримінаційний ефект може бути непомітним для самої особи. Користувачеві можуть просто відмовити у доступі до сервісу, затримати операцію, вимагати додаткову перевірку або застосувати до нього жорсткіші процедури комплаєнсу, не розкриваючи логіки рішення. У результаті формально нейтральне алгоритмічне рішення набуває змісту фактичної нерівності.

UNESCO прямо підкреслює, що системи ШІ повинні оцінюватися на предмет fairness і non-discrimination [19]. У міжнародно-правовому сенсі це означає, що суб'єкти, які використовують ШІ в регулюванні цифрових активів, повинні не просто тестувати точність моделей, а й перевіряти їх на предмет непропорційного негативного впливу на різні групи користувачів. Саме тому технічна ефективність моделі не може розглядатися як достатній критерій її правомірності.

Сфера цифрових активів безпосередньо пов'язана з майновими інтересами особи. Тому будь-яке алгоритмічне рішення, що впливає на можливість користування криптоактивом, проведення транзакції, доступ до облікового запису чи сервісу, має розглядатися не лише як технічна дія, а і як юридично значущий акт.

Коли особа не може розпоряджатися активом через алгоритмічне блокування, відбувається втручання у сферу майнових прав. Якщо при цьому відсутня можливість отримати обґрунтування, звернутися до людини-оператора, оперативного переглянути рішення та оскаржити його, виникає проблема не тільки власності, а й належної правової процедури. Рамкова конвенція Ради Європи про ШІ приділяє особливу увагу процедурним гарантіям у випадках, коли система ШІ істотно впливає на права людини. Саме ця логіка є особливо релевантною для ринку цифрових активів.

Тому правомірне використання ШІ у цій сфері передбачає щонайменше такі процесуальні вимоги: можливість людського перегляду рішень, документування підстав втручання, наявність audit trail, фіксацію джерел даних та реальну доступність механізмів оскарження. Без цих елементів алгоритмічне регулювання цифрових активів може перетворитися на форму непрозорого приватного або публічного примусу.

Окремо слід підкреслити, що підвищений ризик використання віртуальних активів у незаконних фінансових операціях є реальним. Саме цим пояснюється посилена увага FATF, національних фінансових розвідок і регуляторів до цього сектору [13]. Разом із тим боротьба з фінансовими злочинами не створює для держави або приватних суб'єктів «правового імунітету» від стандартів захисту прав людини.

Правильнішим видається підхід, за якого AML/CFT-логіка та human rights-based approach не протиставляються, а поєднуються. Іншими словами, ефективний фінансовий контроль має бути не просто суворим, а правозахисно сумісним. Лише така модель здатна зберегти баланс між безпекою фінансової системи та свободою особи.

На підставі проведеного аналізу можна сформулювати систему базових принципів.

Перший принцип - законність. Будь-яке алгоритмічне втручання у права та інтереси особи повинно мати чітку правову основу.

Другий принцип - пропорційність. Масштаб обробки даних, рівень автоматизації та інтенсивність контролю мають відповідати законній меті.

Третій принцип - цільове обмеження і мінімізація даних. Збирання та використання даних не повинні виходити за межі того, що об'єктивно необхідно.

Четвертий принцип - прозорість. Особа повинна бути поінформована про те, що щодо неї застосовується алгоритмічна оцінка, і мати змогу зрозуміти її загальне значення.

П'ятий принцип - людський контроль. Рішення, які здатні істотно вплинути на права особи, не повинні бути суто машинними.

Для України ця проблематика має особливу актуальність. По-перше, українське право перебуває у фазі інтенсивної цифровізації та наближення до європейських стандартів. По-друге, інтеграція до європейського правового простору об'єктивно означає необхідність врахування MiCA, AI Act, GDPR-логіки та загальних правозахисних стандартів Європи. По-третє, підписання Україною у 2025 році Рамкової конвенції Ради Європи про ШІ створює нормативно-політичну передумову для більш системного законодавчого підходу.

Отже, майбутня українська модель регулювання цифрових активів не повинна обмежуватися лише визначенням правового статусу віртуальних активів чи механізмів фінансового моніторингу. Вона має включати окремий блок гарантій прав людини у випадках, коли в цій сфері використовуються системи штучного інтелекту. Саме це дасть змогу уникнути ситуації, коли інноваційність регулювання досягається ціною зниження стандартів правового захисту особи.

Проведене дослідження дає підстави стверджувати, що використання штучного інтелекту у регулюванні цифрових активів є об'єктивною тенденцією розвитку сучасного фінансового права. ШІ вже став інструментом транзакційного моніторингу, ризик-скорингу, KYC/AML-процедур, ринкового нагляду, blockchain analytics та внутрішнього комплаєнсу. Утім його використання не може оцінюватися виключно через призму ефективності чи технологічної доцільності.

Цифрові активи перебувають у сфері підвищеного регуляторного інтересу, однак саме через це вони потребують підвищеного рівня правозахисних гарантій. Автоматизовані рішення здатні впливати на приватність, захист персональних даних, доступ до фінансових послуг, рівність ставлення, майнові права та процесуальні гарантії особи. Отже, сучасне правове регулювання повинно поєднувати фінансовий контроль із міжнародними стандартами прав людини.

Підбиваючи підсумок, правомірне використання штучного інтелекту у сфері цифрових активів можливе лише за умов дотримання принципів законності, пропорційності, прозорості, мінімізації даних, людського контролю, недискримінації, підзвітності та ефективного оскарження. Саме така модель дозволяє поєднати інноваційний розвиток цифрових фінансів, безпеку фінансової системи та належний рівень захисту прав людини.

Перспективи подальших досліджень полягають у спеціальному аналізі застосування AI Act до окремих фінансових сервісів, пов'язаних із цифровими активами, у дослідженні правового режиму blockchain analytics, у розробці критеріїв

оцінки алгоритмічного ризик-скорингу, а також у виробленні моделі імплементації міжнародних та європейських стандартів у законодавство України. Особливо важливо надалі дослідити, яким чином гарантії прав людини мають бути інтегровані у діяльність постачальників криптоактивних послуг і наглядових органів у процесі практичного використання систем ШІ.

#### Література:

1. Яценко Д. П. Управління ризиками в цифрову епоху: роль штучного інтелекту. *Фінанси України*. 2023. № 5. С. 112–121.
2. Марутян Р. Р. Інформаційні технології інтелектуального управління у публічно-управлінській практиці: зарубіжний та вітчизняний досвід. *Вісник Національного університету цивільного захисту України*, 2018. № 2. С. 146–153.
3. Ткаленко О. М., Макаренко А. О., Полоневич О. В. Інтелектуальні технології та системи штучного інтелекту для підтримки прийняття рішень. *Телекомунікаційні та інформаційні технології*. 2019. № 2. С. 53–59.
4. Гулейков І. Ю. Цифрові активи в цивільному обороті України : дис. ... д-ра філософії з права : 081. Київ, 2025. 243 с.
5. Защипас С.М. Ендогенна та екзогенна природа грошової пропозиції в умовах розвитку віртуальних активів. *Сучасні виклики сталого розвитку бізнесу: тези виступів VI Міжнар. наук.-практ. конф.* – Житомир: Житомирська політехніка, 2025. 463 с.
6. Берназюк Ян. Штучний інтелект та система правосуддя України: результати співпраці у році, що минув URL: <https://so.supreme.court.gov.ua/authors/934/shtuchnyi-intelekt-ta-systema-pravosuddia-ukrainy-rezultaty-spi-pratsi-urotsi-sh%D1%81ho-mynuv>
7. Подорожна Т. С., Котуха О. С. Цифровізація нормотворчої діяльності: сучасний стан і перспективи розвитку. *Альманах права*. 2024. Вип. 15. С. 155–163. URL: <http://jnas.nbuv.gov.ua/article/UJRN-0001525894>
8. Lee J. Access to Finance for Artificial Intelligence Regulation in the Financial Services Industry. *European Business Organization Law Review*. 2020. Vol. 21. P. 731–757.
9. Zetzsche D. Crypto custody. *Capital Markets Law Journal*. 2024. Volume 19. Issue 3. July 2024. P.207–229 URL: <https://doi.org/10.1093/cmlj/kmae010>
10. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1114>
11. Новікова Н.Л., Бойко Л.В. Цифровізація та національна безпека: тенденції та виклики. *Національна безпека та публічне управління*. 2024. № 1. С. 19–32. DOI: <https://doi.org/10.51369/3083-5917-2024-1-8>
12. Understanding Crypto Money Laundering Methods: The Cryptocurrency Crime <https://financialcrimeacademy.org/cryptocurrency-moneylaundering-methods/>
13. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (The FATF Recommendations). Paris, France, 2012–2025. URL: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html>
14. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>
15. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. 2024. URL: <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence>

16. European Data Protection Board. Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models. 18 December 2024. URL: [https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects\\_en](https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en)
17. Charter of Fundamental Rights of the European Union. 2012/C 326/02. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>
18. UNESCO, "Recommendation on the ethics of artificial intelligence," 2021, acceso feb. 2023. URL: <https://bsu.buap.mx/b2m>
19. UNESCO. Recommendation on the Ethics of Artificial Intelligence. Paris, 2021. URL: <https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence>

**Redchenko Ya. The Use of Artificial Intelligence in the Regulation of Digital Assets through the Prism of International Legal Guarantees of Human Rights**

**Summary.** The article examines the use of artificial intelligence in the field of regulation of digital assets through the prism of international legal guarantees of human rights. It is shown that the digitalization of financial markets, the spread

of crypto-assets, stablecoins and tokenized rights have not only complicated the mechanisms of legal control, but also made algorithmic tools an almost integral part of modern supervision. It is noteworthy that AI systems simultaneously increase the efficiency of transaction monitoring, risk assessment and compliance procedures and, at the same time, create new challenges for the right to privacy, personal data protection, non-discrimination, property rights and due process.

Particular attention is paid to the significance of MiCA, AI Act, GDPR, the Council of Europe Framework Convention on Artificial Intelligence, as well as the approaches of UNESCO, OHCHR and the European Data Protection Board. To sum up, we can conclude that the legitimate use of artificial intelligence in the field of digital assets is possible only if the principles of legality, proportionality, transparency, data minimization, human control, accountability, and effective redress are adhered to.

**Key words:** artificial intelligence, digital assets, cryptoassets, human rights, international law, MiCA, AI Act, privacy, personal data protection.

Дата першого надходження статті до видання: 10.03.2026

Дата прийняття статті до друку після рецензування: 05.04.2026

Дата публікації (оприлюднення) статті: 27.05.2026



Стаття поширюється на умовах ліцензії відкритого доступу (CC BY 4.0)