КОНСТИТУЦІЙНЕ ПРАВО; МУНІЦИПАЛЬНЕ ПРАВО

УДК 342.7:004.8
DOI 10.36919/3041-1149(Print).10.2025.25-31

О. О. Семенюк,
кандидат юридичних наук, доцент,
доцент кафедри права,
ПВНЗ «Європейський університет»
email: sashasemenujk@gmail.com
ORCID 0009-0007-9199-6657;
А. М. Соцький,
доктор юридичних наук, професор
email: artur.sotsky@e-u.edu.ua
ORCID 0000-0001-6836-7480

ЄВРОПЕЙСЬКИЙ ПІДХІД ДО РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ТА ЙОГО ЗНАЧЕННЯ ДЛЯ ПРАВ ЛЮДИНИ

У статті проведено комплексний аналіз теоретико-правових засад регулювання штучного інтелекту в Європейському Союзі крізь призму ухвалення EU AI Act. Досліджено трансформацію парадигми від етичних настанов до чіткого законодавчого регулювання, що базується на концепції «Trustworthy AI». Розкрито дуалістичну природу європейського регламенту, який формально є законодавством про безпеку продукції, а фактично виконує квазі-конституційну функцію захисту фундаментальних прав людини. Детально проаналізовано ризик-орієнтований підхід та механізми контролю, зокрема оцінювання впливу на права людини (FRIA). Проведено порівняльний аналіз регуляторних ландшафтів ЄС та України, виявлено відмінності між європейським підходом «hard law» та українською стратегією «soft law». Обґрунтовано потребу в застосуванні моделі «динамічної гармонізації» національного законодавства, що дасть змогу інтегруватися до Єдиного цифрового ринку ЄС, зберігши потенціал для розвитку оборонних інновацій в умовах воєнного стану.

Ключові слова: *штучний інтелект, правове регулювання, права людини, цифрова трансформація, гармонізація законодавства, правова безпека, генеративна модель.*

Постановка проблеми та її актуальність. Стрімка еволюція технологій штучного інтелекту (далі – ШІ), яка в 2022–2023 роках ознаменувалася масовим поширенням генеративних моделей загального призначення (General Purpose AI), створила безпрецедентні виклики для традиційних правових систем та архітектури прав людини. Здатність алгоритмів генерувати синтетичний контент, що не відрізняється від створеного людиною, а також самостійно приймати рішення у сферах правосуддя, медицини та бізнесу, актуалізувала проблему «алгоритмічної підзвітності» (algorithmic accountability). Якщо ще десятиліття тому дискус навколо ШІ обмежувався технічними стандартами та рамками «корпоративної соціальної відповідальності», то сьогодні він остаточно перемістився в площину чіткого законодавчого регулювання [1].

Європейський Союз (далі – ЄС), бажаючи закріпити за собою роль глобального регуляторного лідера та експортера нормативних стандартів, у травні 2024 року фіналізував ухвалення Регламенту про штучний інтелект (далі – EU AI Act) [2]. Цей документ є одним із

перших прикладів горизонтального законодавства, який регулює весь життєвий цикл систем ШІ – від розробки до виведення з експлуатації.

EU AI Act є не просто технічним регламентом з безпеки продукції, а ціннісно-орієнтованим нормативним актом, який покликаний збалансувати інноваційний розвиток і функціонування Єдиного цифрового ринку ЄС з безумовним захистом фундаментальних прав та свобод людини.

Актуальність теми дослідження зумовлена потребою в глибокому аналізі того, наскільки ефективно запропоновані ЄС механізми, зокрема класифікація ризиків та оцінювання впливу на права людини, здатні захистити право на приватність, недискримінацію та презумпцію невинуватості в епоху автоматизованих рішень.

Особливого значення це питання набуває і для України. Перебуваючи на етапі активної гармонізації національного законодавства із законодавство ЄС, наша держава одночасно стикається з унікальним викликом: петребою інтегрувати європейські гуманістичні стандарти в умовах повномасштабної війни, де новітні технології є інструментом виживання та оборони. Розуміння архітектури EU AI Act є критично важливим для побудови правової системи, яка б не лише сприяла повоєнному відновленню через інновації, але й запобігала перетворенню держави на полігон для нерегульованого цифрового стеження [3].

Аналіз останніх досліджень і публікацій. Проблематика правового регулювання ШІ вийшла за межі суто технічних наук і стала предметом міждисциплінарних дискусій у національній та іноземній науковій доктрині.

Фундаментальні засади етики ШІ, що слугували преамбулою до сучасних законодавчих ініціатив, були розроблені групою експертів високого рівня (AI HLEG) за активної участі таких дослідників, як Л. Флоріді (L. Floridi) та В. Дігнум (V. Dignum). У своїх працях вони обґрунтували концепцію «Trustworthy AI» (ШІ, що заслуговує на довіру), доводячи, що етичність технології є передумовою її соціального сприйняття, проте самої лише етики недостатньо для стримування корпоративних зловживань [4, с. 34].

Перехід від етичних настанов до юридичних зобов'язань та концепцію «ризикофікації» (riskification) права ЄС ґрунтовно досліджують А. Бредфорд (A. Bradford) та М. Веале (M. Veale). Бредфорд у роботі «Digital Empires» аналізує, як регуляторна сила ЄС змушує глобальні технологічні компанії підпорядковувати свої алгоритми європейським стандартам, навіть якщо вони діють за межами Європи [5]. М. Веале та Ф. Зуйдервін Боргезіус критично оцінюють спробу ЄС регулювати ШІ через механізми безпеки продукції (Product Safety), вказуючи на ризики, коли захист прав людини підміняється бюрократичними процедурами сертифікації [6].

У національній правовій науці питання імплементації цифрового законодавства ЄС досліджують Є. О. Харитонов, О. А. Баранов, Р. А. Майданик. Їхні роботи фокусуються на адаптації цивільного та адміністративного законодавства України до викликів цифровізації. Важливим джерелом аналітики є матеріали Міністерства цифрової трансформації України, зокрема «Біла книга» з регулювання ШІ, яка пропонує модель «м'якої» імплементації норм ЄС через регуляторні сендбокси [3].

Однак більшість існуючих українських досліджень базуються або на проєктах EU AI Act (зразок 2021 р.), або на загальних теоретичних конструкціях. На жаль, бракує комплексних праць, що аналізують остаточну редакцію Регламенту (EU) 2024/1689 [6], ухвалену весною 2024 р., та її співвідношення з новою Рамковою конвенцією Ради Європи. Тому заповнення цієї прогалини і є **метою статті.**

Виклад основного матеріалу дослідження. Європейський підхід до регулювання штучного інтелекту базується на аксіологічній концепції «ШІ, що заслуговує на довіру» (Trustworthy AI). Ця парадигма постулює, що технологія має відповідати трьом імперативам: бути законною (lawful), етичною (ethical) та технічно надійною (robust) впродовж усього життєвого циклу [7, с. 5]. Юридично EU AI Act спирається на ст. 114 Договору про функціонування ЄС (TFEU), яка стосується заходів щодо зближення законодавства держав-членів для забезпечення функціонування внутрішнього ринку. Це створює дуалістичну природу акту: формально виступаючи як законодавство про безпеку продукції (product safety legislation), за змістом він виконує квазі-конституційну функцію захисту фундаментальних прав людини [8, с. 12].

На відміну від США, де переважає децентралізований ринково-орієнтований підхід, та Китаю, де регулювання підпорядковане інтересам державної безпеки та соціального контролю, ЄС обрав «третій шлях» – людиноцентричне регулювання (human-centric approach). Стратегічна мета ЄС полягає не лише в запобіганні фрагментації єдиного цифрового ринку, але й у реалізації так званого «ефекту Брюсселя» (Brussels Effect). Цей феномен передбачає, що завдяки екстериторіальній дії регламенту та розміру європейського ринку стандарти ЄС *de facto* стануть глобальними стандартами для розробників ШІ по всьому світу [9, с. 28].

Серцевиною EU AI Act є ризик-орієнтований підхід (risk-based approach), який диференціює правові зобов'язання суб'єктів правовідносин залежно від інтенсивності потенційної шкоди, яку система ШІ може завдати основним права людини. Згідно зі ст. 6 та відповідними Додатками до EU AI Act виділяють чотири рівні ризику, що формують пірамідальну структуру регулювання:

1. *Неприйнятний ризик (Unacceptable Risk).* Практики, що прямо заборонені через їх несумісність із європейськими цінностями (ст. 5). До цього переліку, крім систем соціального скорингу (social scoring) та маніпулятивних технік, що використовують підсвідомі методи впливу, фінальна редакція тексту відносить: створення баз даних розпізнавання облич через нецільовий скрапінг (scraping) зображень з інтернету або записів камер відеоспостереження; розпізнавання емоцій на робочому місці та в закладах освіти; а також предиктивну поліцію (predictive policing), що базується виключно на профілюванні особистості без фактажу злочинної діяльності [10, с. 102].

2. *Високий ризик (High Risk).* Системи, що використовуються як компоненти безпеки продуктів або у визначених чутливих сферах (критична інфраструктура, освіта, працевлаштування, правоохоронна діяльність, управління міграцією, правосуддя). Для таких систем встановлюються імперативні вимоги *ex ante*: висока якість та репрезентативність навчальних даних (data governance), технічна прозорість, детальне логування подій, забезпечення людського нагляду (human oversight) та кіберстійкість [11, с. 45].

3. *Специфічний ризик прозорості (Specific Transparency Risk).* Категорія, що охоплює системи, які взаємодіють з людьми (чат-боти) або генерують синтетичний контент (діпфейки). Ключова вимога ст. 50 – маркування контенту та інформування користувача про взаємодію зі штучним інтелектом.

4. *Моделі загального призначення (General Purpose AI – GPAI).* Окрема новела фінального тексту, введена у відповідь на стрімкий розвиток генеративних моделей (на кшталт GPT – 4). Акт запроваджує дворівневий підхід: базові вимоги для всіх GPAI (оновлення технічної документації, дотримання авторського права) та посилені зобов'язання для моделей із «системним ризиком» (оцінювання змагальних атак, моніторинг серйозних інцидентів) [12, с. 8].

Як бачимо, ризик-орієнтований підхід EU AI Act формує багаторівневу модель регулювання, що співвідносить інтенсивність потенційної шкоди від ШІ із суворістю правових вимог. Така диференціація від повної заборони неприйнятних практик до спеціалізованих режимів для високоризикових систем, прозорісних обов'язків та окремого регулювання моделей загального призначення забезпечує адаптивність і технологічну нейтральність нормативного механізму. У результаті EU AI Act пропонує комплексну архітектуру правового контролю, орієнтовану на захист прав людини та мінімізацію системних загроз у динамічному середовищі розвитку ШІ.

Одним із найбільш дискусійних аспектів EU AI Act є регулювання віддаленої біометричної ідентифікації (RBI). Хоча використання RBI у реальному часі в публічних місцях заборонено, стаття 5 містить вичерпний перелік винятків для правоохоронних органів (пошук жертв викрадення, запобігання неминучим терористичним загрозам, розшук підозрюваних у тяжких злочинах) [13]. Тобто регулювання віддаленої біометричної ідентифікації в EU AI Act демонструє напружений баланс між завданнями безпеки та захистом фундаментальних прав. Попри формальну заборону використання RBI у реальному часі, надані винятки для правоохоронних органів і можливість постфактум отримувати судовий дозвіл фактично послаблюють гарантії приватності. Це підсилює побоювання щодо потенційної легітимації масового стеження та створення охолоджуючого ефекту для демократичних свобод, що вимагає подальшого нормативного уточнення та посиленого контролю за практиками застосування RBI.

Системи ШІ часто відтворюють і масштабують історичні упередження, імпліцитно присутні в навчальних даних. EU AI Act намагається вирішити цю проблему через вимоги ст. 10 щодо управління даними, які зобов'язують розробників виявляти та пом'якшувати можливі біаси (biases) [11, с. 52]. Однак науковці застерігають, що суто технічне «очищення» даних не здатне усунути складні соцієтальні упередження, особливо коли дискримінація відбувається через проксі-змінні (наприклад, індекс поштового відділення як маркер расової належності). Саме тому FRIA стає ключовим інструментом для виявлення потенційної дискримінації маргіналізованих груп у конкретному контексті використання ще до запуску системи.

Вимоги щодо маркування контенту, створеного ШІ, мають на меті захист інформаційного простору від дезінформації. Проте існує тонке балансування: надмірні вимоги до фільтрації контенту генеративними моделями можуть призвести до явища «надмірного блокування» (over-blocking), що фактично є формою приватної цензури. Крім того, виникає питання щодо «права на пояснення»: хоча EU AI Act вимагає прозорості функціонування систем, складність нейромереж («проблема чорної скриньки») може унеможливити надання користувачеві зрозумілого пояснення, чому система ухвалила те чи інше рішення, що прямо впливає на право на ефективний засіб правового захисту [14, с. 114].

Отже, попри намагання EU AI Act мінімізувати технічні й соціальні упередження через вимоги до управління даними та запровадження FRIA, повного усунення структурної дискримінації досягти складно. Додаткові виклики виникають у сфері інформаційної безпеки: з одного боку, маркування ШІ-контенту має стримувати дезінформацію, але з іншого – ризикує спричинити надмірне блокування. Нарешті, вимога прозорості стикається з межами пояснюваності нейромереж, що ставить під сумнів реалізацію права на ефективний засіб правового захисту.

У контексті набуття Україною статусу кандидата в члени ЄС та потреби у виконанні умов Угоди про асоціацію гармонізація національного цифрового законодавства з *acquis communautaire* ЄС стає стратегічним імперативом. Водночас поточний стан нормативно-правового забезпечення сфери ШІ в Україні демонструє суттєві концептуальні та методологічні відмінності від європейського підходу, зумовлені як економічними факторами, так і безпековими викликами.

Якщо EU AI Act репрезентує класичний приклад «жорсткого права» (hard law) з чітко визначеними імперативними нормами та санкціями, то українська модель, окреслена Міністерством цифрової трансформації України, на цьому етапі тяжіє до інструментів «м'якого права» (soft law). Згідно з «Дорожньою картою регулювання ШІ в Україні» держава обрала bottom-up approach («знизу-вгору»), який передбачає поетапний рух від добровільних етичних кодексів і рекомендацій до законодавчого закріплення норм [15, с. 5]. Така стратегія пояснюється потребою в уникненні передчасної регуляторної стагнації («regulatory chill»), яка може загальмувати розвиток національної ІТ-індустрії в умовах війни. Україна намагається знайти баланс між захистом прав громадян і створенням сприятливого інвестиційного клімату, відкладаючи прийняття аналогу AI Act до моменту, коли ринок буде готовий до імплементації складних комплаєнс-процедур.

Суттєвою відмінністю є підхід до тестування інновацій. Якщо в ЄС регуляторні пісочниці (regulatory sandboxes) вводяться паралельно з жорсткими обмеженнями для систем високого ризику, то в Україні вони розглядаються як основний механізм підготовки до регулювання. Концепція передбачає створення безпечного середовища, де компанії можуть тестувати свої продукти під наглядом регулятора без ризику отримання штрафів, що дає змогу виявити прогалини в законодавстві ще до його ухвалення [16, с. 14].

Водночас Україна декларує намір імплементувати європейську класифікацію ризиків (піраміду ризиків EU AI Act), що є критично важливим для забезпечення інтероперабельності ринків. Це означає, що українські розробники систем «високого ризику» (наприклад, у сфері MedTech або FinTech), які планують експорт до ЄС, уже сьогодні мають орієнтуватися на вимоги європейського регламенту щодо управління даними та технічної документації.

Європейська модель передбачає створення розгалуженої системи наглядових органів (AI Office, AI Board, національні компетентні органи). В Україні наразі дискутується питання щодо визначення єдиного регулятора. Експерти вказують на ризик розпорошення повноважень,

тому найбільш вірогідним сценарієм є покладання функцій нагляду на Мінцифри або створення спеціалізованої агенції на базі існуючих інституцій [15, с. 42]. Окремим аспектом є використання ШІ у сфері оборони. Оскільки EU AI Act містить винятки для систем, розроблених виключно для військових цілей, Україна, перебуваючи в стані активної війни, має унікальну можливість розвивати Military Tech без чітких обмежень цивільного регулювання, водночас гармонізуючи правила для цивільного сектору. Це створює дуалістичну систему: ліберальний режим для Defense Tech та поступове наближення до європейських стандартів (*Trustworthy AI*) для цивільного сектору.

Висновки. Викладене вище дає змогу зробити такі узагальнення:

1. Стрімкий розвиток генеративного штучного інтелекту (*General Purpose AI*) у 2022–2023 роках став каталізатором переходу від «м'якого права» (етичних кодексів і корпоративної відповідальності) до чіткого законодавчого регулювання. Проблема «алгоритмічної підзвітності» вийшла за межі технічних дискусій і набула статусу питання захисту фундаментальних прав людини, що вимагає імперативного державного втручання.

2. Встановлено, що EU AI Act не є класичним технічним регламентом безпеки продукції. За своєю сутністю він виконує квазі-конституційну функцію, встановлюючи примат фундаментальних прав (приватності, недискримінації, презумпції невинуватості) над економічною доцільністю. Ризик-орієнтований підхід є компромісним механізмом, що дає змогу мінімізувати загрози для суспільства, не зупиняючи водночас інноваційний розвиток Єдиного цифрового ринку.

3. Для України гармонізація національного законодавства з EU AI Act є безальтернативним способом у контексті євроінтеграції. Однак, враховуючи стан війни та потребу в розвитку оборонних технологій (*Military Tech*), сліпе копіювання європейських норм є ризикованим. Водночас обґрунтовано доцільність застосування Україною моделі «динамічної гармонізації»: поетапного переходу від використання регуляторних пісочниць і галузевих рекомендацій до ухвалення рамкового закону. Це дасть змогу підготувати національну IT-індустрію та систему державного управління до високих стандартів комплаєнсу, зберігаючи гнучкість для інновацій у критично важливих сферах безпеки та оборони.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ethics Guidelines for Trustworthy AI / High-Level Expert Group on Artificial Intelligence. Brussels : European Commission, 2019. 41 p.

2. EU's AI Act fails to set gold standard for human rights. European Digital Rights (EDRi). 2024. URL : https://www.edf-feph.org

3. Регулювання штучного інтелекту в Україні: Біла книга / Міністерство цифрової трансформації України. Київ, 2024.

4. How the EU Can Achieve Legally Trustworthy AI: A Response to the High-Level Expert Group on AI / N. A. Smuha et al. *Philosophy & Technology.* 2021. Vol. 34, No. 3. P. 32–55.

5. Bradford A. Digital Empires: The Global Battle to Regulate Technology. New York : Oxford University Press, 2023. 288 p.

6. Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union.* 2024.

7. Kop M. EU Artificial Intelligence Act: The European Approach to AI. Stanford – Vienna Transatlantic Technology Law Forum. *Transatlantic Antitrust and IPR Developments.* 2021. Issue No. 2. P. 1–25.

8. Bradford A. The Brussels Effect: How the European Union Rules the World. New York : Oxford University Press, 2020. 424 p.

9. 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). *Official Journal of the European Union.* 2024. L. 1689. P. 1–150.

10. Demystifying the Draft EU Artificial Intelligence Act – Analysing the good, the bad, and the unclear / M. Veale, F. Zuiderveen Borgesius. *Computer Law & Security Review*. 2021. Vol. 43. URL : https://doi.org/10.1016/j.clsr.2021.105632

11. Hacker P., Engel A., Mauer M. Regulating General Purpose AI: EU AI Act and Beyond. *Verfassungsblog.* 2023. URL : https://verfassungsblog.de/regulating-general-purpose-ai/

12. Civil society reaction to the IMCO-LIBE vote on the AI Act. EDRi Policy Paper / European Digital Rights (EDRi). May 2023. URL : https://edri.org/our-work/civil-society-reaction-imco-libe-vote-ai-act/

13. Edwards L. The EU AI Act: A Summary of the Final Text. Ada Lovelace Institute Report. 2024. 142 p.

14. Розвиток штучного інтелекту в Україні: бачення та дорожня карта / Міністерство цифрової трансформації України. Київ, 2023. 28 с. URL : https://thedigital.gov.ua/

15. Біла книга з регулювання штучного інтелекту в Україні / О. В. Борняков та ін. Київ : Мінцифра, 2024. 64 с.

16. Карчевський М. В., Бобровнік С. В. Правове регулювання штучного інтелекту: виклики для України в контексті євроінтеграції. *Право та інновації.* 2023. № 4 (44). С. 38–45. URL : https://doi.org/10.31359/2311-4894-2023-4-38

REFERENCES

1. High-Level Expert Group on Artificial Intelligence. (2019). Ethics Guidelines for Trustworthy AI. Brussels: European Commission. 41 p.

2. European Digital Rights (EDRi) (2024). EU's AI Act fails to set gold standard for human rights. URL : https://www.edf-feph.org

3. Ministry of Digital Transformation of Ukraine. (2024). Rehulyuvannya shtuchnoho intelektu v Ukrayini: Bila knyha [Regulation of artificial intelligence in Ukraine: White paper]. Kyiv [in Ukrainian].

4. Smuha, N. A. et al. (2021). How the EU Can Achieve Legally Trustworthy AI: A Response to the High-Level Expert Group on AI. *Philosophy & Technology.* Vol. 34, No. 3. 32–55.

5. Bradford, A. (2023). Digital Empires: The Global Battle to Regulate Technology. New York : Oxford University Press. 288 p.

6. Official Journal of the European Union (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

7. Kop, M. (2021). EU Artificial Intelligence Act: The European Approach to AI. Stanford – Vienna Transatlantic Technology Law Forum. *Transatlantic Antitrust and IPR Developments.* Issue No. 2. 1–25.

8. Bradford, A. (2020). The Brussels Effect: How the European Union Rules the World. New York : Oxford University Press. 424 p.

9. 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). *Official Journal of the European Union*. 2024. L. 1689. 1–150.

10. Veale, M., Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act - Analysing the good, the bad, and the unclear. *Computer Law & Security Review*. Vol. 43. URL : https://doi.org/10.1016/j.clsr.2021.105632

11. Hacker, P., Engel, A., Mauer, M. (2023). Regulating General Purpose AI: EU AI Act and Beyond. Verfassungsblog. URL : https://verfassungsblog.de/regulating-general-purpose-ai/

12. European Digital Rights (EDRi) (May 2023). Civil society reaction to the IMCO-LIBE vote on the AI Act. EDRi Policy Paper. URL : https://edri.org/our-work/civil-society-reaction-imco-libe-vote-ai-act/

13. Edwards, L. (2024). The EU AI Act: A Summary of the Final Text. Ada Lovelace Institute Report. 142 p.

14. Ministry of Digital Transformation of Ukraine. (2023). Rozvytok shtuchnoho intelektu v Ukrayini: bachennya ta dorozhnya karta [Development of artificial intelligence in Ukraine: vision and roadmap]. Kyiv. 28 p. URL : https://thedigital.gov.ua/ [in Ukrainian].

15. Bornyakov, O. V. et al. (2024). Bila knyha z rehulyuvannya shtuchnoho intelektu v Ukrayini [White paper on the regulation of artificial intelligence in Ukraine]. Kyiv : Mintsyfra. 64 p. [in Ukrainian].

16. Karchevskyy, M. V., Bobrovnik, S. V. (2023). Pravove rehulyuvannya shtuchnoho intelektu: vyklyky dlya Ukrayiny v konteksti yevrointehratsiyi [Legal regulation of artificial intelligence: challenges for Ukraine in the context of European integration]. *Pravo ta innovatsiyi.* No. 4 (44). 38–45. URL : https://doi.org/10.31359/2311-4894-2023-4-38 [in Ukrainian].

O. O. Semenuk, A. M. Sotskyi. THE EUROPEAN APPROACH TO ARTIFICIAL INTELLIGENCE REGULATION AND ITS SIGNIFICANCE FOR HUMAN RIGHTS

The article provides a comprehensive analysis of the theoretical and legal foundations of artificial intelligence regulation in the European Union through the prism of the EU AI Act adoption. The study explores the paradigm shift from ethical guidelines to binding legislation based on the "Trustworthy AI" concept. The author reveals the dual nature of the regulation, which formally acts as product safety legislation but substantively performs a quasi-constitutional function of protecting fundamental human rights. The risk-based approach and control mechanisms, particularly the Fundamental Rights Impact Assessment (FRIA), are examined in detail. A comparative analysis of the regulatory landscapes of the EU and Ukraine is conducted, highlighting the differences between the European "hard law" approach and the Ukrainian "soft law" strategy. The article substantiates the necessity of applying a "dynamic harmonization" model for national legislation, enabling integration into the EU Digital Single Market while preserving the potential for defense innovation under martial law conditions.

Key words: *artificial intelligence, legal regulation, human rights, digital transformation, harmonization of legislation, legal security, generative model.*