DOI: https://doi.org/10.32782/2524-0072/2026-83-192

УДК 347.73/.74:341.22(477)

ІНТЕГРАЦІЯ ШТУЧНОГО ІНТЕЛЕКТУ У БІЗНЕС-ПРОЦЕСИ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ: БАЛАНС ЗАБЕЗПЕЧЕННЯ ПРАВ ЛЮДИНИ ТА СОЦІАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ

THE INTEGRATION OF ARTIFICIAL INTELLIGENCE INTO THE BUSINESS PROCESSES OF ECONOMIC ENTITIES: BALANCING THE PROTECTION OF HUMAN RIGHTS AND SOCIAL RESPONSIBILITY

Петруненко Ярослав Вікторович
доктор юридичних наук, професор, провідний науковий співробітник,
Державна установа «Інститут економіко-правових досліджень
імені В.К. Мамутова Національної академії наук України»
ORCID: https://orcid.org/0000-0002-1186-730X

Гудіма Тетяна Степанівна
доктор юридичних наук, професор, заступник завідувача відділу,
Державна установа «Інститут економіко-правових досліджень
імені В.К. Мамутова Національної академії наук України»
ORCID: https://orcid.org/0000-0003-1509-5180

Petrunenko Iaroslav, Hudima Tetiana
State Organization «V. Mamutov Institute of Economic and Legal Research
of the National Academy of Sciences of Ukraine»

У статті науково обґрунтовано, що у сучасному світі інтеграція штучного інтелекту в бізнес-процеси суб'єктів господарювання набуває дедалі більшого значення, забезпечуючи численні переваги, зокрема автоматизацію, підвищення ефективності та інноваційний розвиток. Проте, паралельно із вказаними перевагами, виникають й значні виклики, пов'язані із захистом прав людини та забезпеченням соціальної відповідальності. Представлена стаття аналізує основні аспекти інтеграції штучного інтелекту у бізнес-процеси суб'єктів господарювання, зокрема етичні, правові та соціальні питання, що виникають у зв'язку з використанням цієї технології. У статті досліджено вплив штучного інтелекту на робочі місця, підкреслено потенційні загрози для зайнятості, такі як автоматизація та роботизація, що можуть призвести до масового вивільнення робочої сили. Розглянуто способи пом'якшення зазначених наслідків через розвиток нових навичок, перекваліфікацію та створення нових робочих місць, орієнтованих на взаємодію з технологіями штучного інтелекту. Особливу увагу приділено питанням конфіденційності та безпеки даних, які є ключовими при використанні штучного інтелекту у бізнесі. Здійснено аналіз правових норм, що регулюють використання персональних даних, та роль компаній у забезпеченні дотримання вказаних норм. Зокрема, досліджено питання прозорості алгоритмів штучного інтелекту та забезпечення доступу до правосуддя для осіб, права яких можуть бути порушені внаслідок автоматизованих рішень. Крім того, розглянуто питання соціальної відповідальності компаній, що впроваджують штучний інтелект, зокрема у контексті етичного поводження та забезпечення інклюзивності. Підкреслено важливість розробки етичних кодексів та стандартів, що регулюють використання штучного інтелекту, а також роль компаній у сприянні сталому розвитку та захисту прав людини. Загалом, стаття надає комплексний огляд поточних тенденцій та викликів, пов'язаних з інтеграцією штучного інтелекту у бізнес-процеси суб'єктів господарювання, у ній висвітлюються важливі питання, які повинні бути враховані при розробці та впровадженні політик і стратегій використання штучного інтелекту, аби забезпечити баланс між інноваційним розвитком, захистом прав людини та соціальною відповідальністю. Значну увагу приділено аналізу законодавства ЄС про штучний інтелект та шляхи імплементації його положень в національну правову систему України.

Ключові слова: штучний інтелект, соціальна справедливість, права людини, бізнес-процеси, суб'єкти господарювання, соціальна відповідальність, сталий розвиток, інновації, інноваційний розвиток, європейська інтеграція.

The article provides a scientific rationale for the growing importance, in today's world, of integrating artificial intelligence into the business processes of economic entities, as it offers numerous benefits, including automation, increased efficiency and innovative development. However, alongside these benefits, significant challenges arise concerning the protection of human rights and the assurance of social responsibility. This article analyses the key aspects of integrating artificial intelligence into the business processes of economic entities, in particular the ethical, legal and social issues arising from the use of this technology. This article examines the impact of artificial intelligence on the workplace and highlights potential threats to employment, such as automation and robotisation, which could lead to mass redundancies. It examines ways to mitigate these consequences through the development of new skills, reskilling and the creation of new jobs focused on interaction with artificial intelligence technologies. Particular attention is paid to issues of data privacy and security, which are key considerations when using artificial intelligence in business. An analysis has been carried out of the legal provisions governing the use of personal data and the role of companies in ensuring compliance with these provisions. In particular, the report examines the issue of transparency in artificial intelligence algorithms and ensuring access to justice for individuals whose rights may be infringed as a result of automated decisions. Furthermore, it addresses the issue of social responsibility among companies implementing artificial intelligence, particularly in the context of ethical conduct and ensuring inclusivity. The importance of developing codes of ethics and standards governing the use of artificial intelligence was emphasised, as was the role of companies in promoting sustainable development and protecting human rights. Overall, the article provides a comprehensive overview of current trends and challenges associated with the integration of artificial intelligence into business processes, It highlights key issues that must be taken into account when developing and implementing policies and strategies for the use of artificial intelligence, in order to ensure a balance between innovative development, the protection of human rights and social responsibility. Considerable attention is paid to the analysis of EU legislation on artificial intelligence and ways of implementing its provisions into Ukraine's national legal system.

Keywords: artificial intelligence, social justice, human rights, business processes, economic entities, social responsibility, sustainable development, innovation, innovative development, European integration.

Постановка проблеми. Стрімкий розвиток штучного інтелекту ставить перед демократією та державно-суспільними відносинами унікальні виклики, що у підсумку призводить до суттєвої трансформації характеру безпекової парадигми, особливо у сфері забезпечення прав людини. Штучний інтелект є універсальною технологією, яка впливає практично на всі інші сектори технологій, а також на сектори фінансів і комунікацій. Сама природа штучного інтелекту також змінює способи здійснення й підтримки влади, впливаючи на соціальні та психологічні важелі, що підтримують і зміцнюють цю владу. Власне, подібні зміни безпосередньо впливають на процеси державного управління по всьому світу, створюючи нові форми тиску на права людини та основоположні свободи, оскільки дедалі більше держав покладаються на нові технології для посилення контролю над суспільствами і даними.

Верховний комісар ООН з прав людини Фолькер Тюрк влучно зазначив: «Безпрецедентний прогрес у цифрових технологіях, включаючи генеративний штучний інтелект, відкриває перед нами раніше неймовірні можливості для просування забезпечення прав людини та сприяння досягненню цілей Порядку денного на період до 2030 року» [1].

Питання штучного інтелекту були у центрі уваги на п'ятому щорічному глобальному самміті *AI for Good Global Summit*, який проходив у травні 2024 р. у Женеві. Самміт є провідною орієнтованою на дії платформою ООН для просування штучного інтелекту для покращення здоров'я, клімату, гендерних питань, інклюзивного процвітання, сталої інфраструктури та інших пріоритетів глобального розвитку [2].

Технологія штучного інтелекту стрімко змінює наш світ, відкриваючи нові можливості для покращення життя людей. Від надання освіти та медичних послуг у віддалених районах до оптимізації сільського господарства та попередження стихійних лих – штучний інтелект може стати (і уже стає) могутнім інструментом для досягнення сталого розвитку.

Втім, аби реалізувати зазначений потенціал, необхідно розробити нормативні рамки штучного інтелекту, який буде етичним, безпечним та доступним для всіх. Як справедливо зауважував Генеральний секретар ООН Антоніу Гутерреш, «нам потрібен штучний інтелект, який зменшує упередженість, дезінформацію та загрози безпеці, а не посилює їх» [1].

Вказане вимагає комплексного підходу, що включає:

– *зменшення упередженості* (розробку алгоритмів штучного інтелекту, які не дискримінують та не обмежують певні групи людей);

– *боротьбу з дезінформацією* (використання штучного інтелекту з метою виявлення і протидії фейковим новинам та пропаганді);

– *забезпечення безпеки* (впровадження ефективних заходів для захисту від кіберзлочинів та інших кіберзагроз, пов'язаних зі штучним інтелектом);

– *підтримку країн*, *що розвиваються* (допомога країнам, що розвиваються, у розробці власних можливостей штучного інтелекту й інтеграції цієї технології у свої економіки та суспільства);

– *глобальну координацію* (створення міжнародних механізмів співпраці для цілей регулювання штучного інтелекту та забезпечення його етичного й відповідального використання).

Представляється, що лише завдяки спільним зусиллям ми матимемо змогу розкрити потенціал штучного інтелекту для покращення життя людей та створення більш сталого і справедливого світу. Власне, ось чому місія ООН з прав людини у 2019 р. започаткувала важливий проєкт «*Бізнес і права людини в технологіях*» (*B-Tech Project*) [3] як спосіб вирішення цих проблем шляхом надання авторитетної дорожньої карти для застосування Керівних принципів ООН з питань бізнесу і прав людини (*UNGP*) [4] до розробки та використання цифрових технологій.

Завдяки проєкту *B-Tech* Управління Верховного комісара ООН з прав людини співпрацює безпосередньо з такими компаніями, як *Microsoft*, *Hewlett Packard Enterprise*, *Google* і *Meta*, серед інших, над вирішенням проблем із правами людини, включно з генеративним штучним інтелектом. Проєкт співпрацює не лише з приватними партнерами, але й з урядами, академічними колами і громадянським суспільством, надаючи безпечний простір для взаємодії та навчання один у одного.

Та пропри все це у штучного інтелекту є й зворотна сторона – це його стрімкий розвиток й відсутність належного контролю за використанням і, як наслідок, неможливість спрогнозувати усі ризики та загрози. Ілон Маск ще у 2018 р. під час конференції *South by Southwest* в Остіні (штат Техас, США) зазначив, що штучний інтелект є небезпечнішим за ядерну зброю [5]. В результаті, у листопаді 2023 р. майже 30 країн підписали так звану «*декларацію Блетчлі*» в перший день самміту з безпеки штучного інтелекту, організованого урядом Великої Британії. Країни таким чином домовилися про спільну роботу над дослідженнями безпеки штучного інтелекту [6]. Дещо раніше, у жовтні 2023 р. адміністрація президента США опублікувала розпорядження, згідно з яким американські компанії штучного інтелекту, такі як *OpenAI* і *Google*, повинні ділитися з урядом результатами своїх тестів безпеки перед випуском моделей штучного інтелекту [7]. Та попри це, вже у січні 2024 р. компанія *OpenAI* змінила політику *ChatGPT*, фактично дозволивши використовувати свої технології у військових цілях [8].

У зазначеному контексті необхідно підтримати думку колег з Української Гельсінської спілки з прав людини з приводу того, що «війна в Україні – це своєрідна «перша світова війна з використанням технологій». Штучний інтелект активно застосовується для ведення війни за допомогою програмного забезпечення, використання дронів, для розпізнавання і розшифрування супутникових знімків, розпізнавання цілей на полі бою і прогнозування засобів, якими вони можуть бути уражені, для розпізнавання облич та ідентифікації військових злочинців або виявлення, ідентифікації жертв війни та повернення тіл загиблих їхнім сім'ям тощо» [9]. Втім, ми вже зараз маємо усвідомлювати усю важливість й відповідальність питань використання штучного інтелекту у військових цілях та шукати механізм забезпечення балансу з соціальною відповідальністю для безпеки майбутніх поколінь.

Аналіз останніх досліджень і публікацій. При написанні наукової статті здійснено аналіз міжнародних нормативно-правових актів у сфері регулювання штучного інтелекту, а також наукових праць, аналітичних оглядів, експертних оцінок авторства Audrey Azoulay, Sam Biddle, Ryan Calo, Zach Campbell, Caitlin L. Chandler, Steve Feldstein, Eva Galperin, Brian Kot, Patrick Howell O'Neill, Thaima Samman, Benjamin De Vanssay та інших, чиї роботи стали достойним підґрунтям для переосмислення авторами досліджуваної проблематики, а також формулювання власних результатів, висновків і пропозицій по результатах проведеного дослідження.

Формулювання цілей статті. *Метою* представленої наукової статті є визначення та наукове обґрунтування ключових засад і норм, які мають бути враховані для забезпечення прав людини та соціальної відповідальності при використанні штучного інтелекту. Для досягнення визначеної мети передбачається вирішення таких *дослідницьких завдань*: дослідити теоретичні основи етики штучного інтелекту, включаючи принципи етики штучного інтелекту, права людини та соціальну відповідальність; визначити ключові фактори, які впливають на етичне використання

штучного інтелекту у різних сферах бізнесу; розробити рекомендації щодо впровадження штучного інтелекту у бізнес-процеси суб'єктів господарювання, які сприятимуть забезпеченню балансу між ефективністю, етикою та соціальною відповідальністю.

Представлена наукова стаття підготовлена авторами в рамках наукового дослідження «*Комплексне наукове дослідження інвестиційно-інноваційної детермінанти сталого економічного розвитку України*», що реалізується відповідно до договору про виконання наукового дослідження, науково-технічної (експериментальної) розробки державною установою, яка за результатами державної атестації за науковим напрямом «Суспільний» віднесена до групи А, укладеного між Державною установою «Інститут економіко-правових досліджень імені В.К. Мамутова Національної академії наук України» та Міністерством освіти і науки України від 10 жовтня 2025 р. № БФ/С22-2025 за рахунок коштів, передбачених наказом Міністерства освіти і науки України «Про затвердження Переліку державних наукових установ, яким за результатами державної атестації спрямовуються бюджетні кошти у 2025 році, разом з відповідними обсягами фінансування для кожної державної наукової установи» від 25 серпня 2025 р. № 1174.

Виклад основного матеріалу. Наукова сфера досліджень штучного інтелекту бере свій початок щонайменше з 1950-х років, однак разом з тим ця технологія все ще знаходиться на ранньому етапі свого життєвого циклу. Успішні програми в таких сферах, як охорона здоров'я і транспорт, є відносно новими явищами. Вони стали можливими завдяки збільшенню обчислювальної потужності і доступу до навчальних даних, що сприяло прогресу в машинному навчанні, підгалузі штучного інтелекту. Проте, існують перешкоди для більш широкого впровадження штучного інтелекту в приватних і державних установах. Однією з таких перешкод є відсутність стандартизації [10].

21 березня 2024 р. Генеральна Асамблея ООН прийняла історичну резолюцію, присвячену штучному інтелекту. Зазначена резолюція, A/78/L.49 «*Використання можливостей безпечних*, *надійних і таких*, *що заслуговують на довіру*, *систем штучного інтелекту для сталого розвитку*», закликає держави до розробки міжнародних принципів для мінімізації ризиків та максимізації переваг штучного інтелекту. Вона знаменує собою важливий потужний крок у регулюванні штучного інтелекту на міжнародному рівні й визнає як потенціал цієї технології для покращення життя людей, так і потенційні загрози, які вона несе, якщо її використовувати безвідповідально. Резолюція підкреслює, що штучний інтелект може призвести до порушення прав людини, посилити упередження та поставити під загрозу захист персональних даних, якщо не вжити відповідних заходів. З цієї причини країнам-членам ООН та іншим зацікавленим сторонам рекомендується «утримуватися або припинити використання систем штучного інтелекту, які не можуть функціонувати відповідно до міжнародного права прав людини або які створюють надмірні ризики для реалізації прав людини» [11].

Інтеграція штучного інтелекту у бізнес-процеси широкого кола суб'єктів господарювання стає дедалі все більш актуальною темою в сучасному світі, бо штучний інтелект може значно підвищити ефективність і продуктивність компаній. Але разом із відзначеними перевагами виникають і серйозні виклики, зокрема щодо забезпечення прав людини та соціальної відповідальності. На цих фактах, зокрема наголошується у доповіді Спеціального доповідача ООН з питань сприяння та захисту права на свободу думки і вираження поглядів [12]. У доповіді також акцентовано увагу на тому, як цифрові технології, особливо ті, що працюють на базі штучного інтелекту, становлять значну проблему для свободи слова.

Одна з провідних організацій у сфері захисту цифрових прав, *Access Now*, звертає увагу на сувору реальність державних відключень Інтернету, називаючи їх зухвалою формою цифрових репресій. Однак, крім цих явних дій, вони також висвітлюють більш тонкі, але не менш руйнівні тактики, такі як посилене спостереження за допомогою штучного інтелекту, що може визначати та ізолювати активістів, а також цілеспрямовані цифрові напади на людей, які не згодні з політикою влади [13].

ЄС запровадив суворий експортний контроль, спрямований на обмеження постачання передових технологій до авторитарних країн, щоб запобігти їх використанню в алгоритмічному авторитаризмі. Однак, вже були зафіксовані непоодинокі випадки, коли європейські високотехнологічні експортні товари перепрофільовувалися для авторитарних цілей у третіх країнах. Більше того, європейські компанії продовжують продавати передові системи

спостереження країнам з поганим досвідом у сфері прав людини [14]. Сьогодні, коли інфраструктура спостереження значною мірою підсилює можливості штучного інтелекту для стеження, провести чітку межу між цими технологіями практично неможливо.

Європейські компанії неодноразово піддавалися критиці за експорт технологій спостереження, які зрештою використовувалися авторитарними режимами для масового стеження та придушення інакомислення. Наприклад, понад десять років тому європейські компанії звинуватили у продажу інструментів шпигунства авторитарним режимам у Сирії, Єгипті та Лівії. Відомо, що ці технології у подальшому використовувалися проти журналістів, правозахисників та опозиційних груп для придушення демократичних рухів, зокрема під час «Арабської весни» 2010 р. [15].

Попри зусилля ЄС запровадити більш суворий контроль над експортом таких технологій, деякі країни-члени, зокрема Швеція, Фінляндія та колишні члени Сполученого Королівства, перебували під впливом бізнес-інтересів, що призвело до послаблення гарантій захисту прав людини.

Окремим прикладом є шведська компанія *MSAB*, відома своєю діяльністю у галузі цифрової криміналістики. *MSAB* отримала державне фінансування ЄС через флагманську програму технологічних досліджень «*Горизонт Європа*» і брала участь у проєкті «*Formobile*» [16]. Вказаний проєкт мав на меті розробити технологію для розблокування мобільних пристроїв без згоди користувачів та аналізу даних для кримінальних розслідувань. Проте, виникли занепокоєння, коли технологія, розроблена в рамках проєкту, була продана поліції М'янми, яка на той час перебувала під цивільним правлінням, але згодом опинилася під військовим контролем після державного перевороту 2021 р. Відтак, цей продаж поставив під сумнів доцільність нормативних актів щодо експорту технологій спостереження та криміналістики до регіонів із високим ризиком зловживань.

Ще одним важливим й не менш ілюстративним прикладом є шведський телекомунікаційний гігант *TeliaSonera*, якого близько десяти років тому звинуватили у продажу високотехнологічного обладнання для спостереження авторитарним режимам у таких країнах, як Білорусь, Узбекистан, Азербайджан, Таджикистан, Грузія та Казахстан. Вказане обладнання дозволяло урядам цих країн шпигувати за журналістами, профспілковими лідерами та членами політичної опозиції. Обладнання, надане *TeliaSonera*, дозволяло здійснювати безперешкодний моніторинг усіх комунікацій, включаючи Інтернет-трафік, телефонні дзвінки та текстові повідомлення. На широкий загал проблема стала відомою після розслідування шведської новинної програми, яка розкрила масштаби використання цієї технології для масового стеження та придушення інакомислення [17].

Узагальнимо, що вищезазначені випадки актуалізують та підкреслюють необхідність:

– *суворого контролю експорту*, зокрема впровадження жорстких правил для запобігання продажу технологій стеження країнам із поганим дотриманням прав людини;

– *ретельної перевірки покупців*, тобто компанії-виробники мають ретельно перевіряти потенційних покупців своїх технологій, аби запобігти їх можливому використанню з метою порушення прав людини.

Продаж технологій стеження авторитарним режимам є серйозною загрозою правам людини, відтак необхідно вживати заходів для запобігання зловживанню цими технологіями.

Надалі варто зауважити про створення складної та мінливої картини міжнародних ініціатив щодо розробки правил і керівних органів для штучного інтелекту. У зазначеному процесі задіяні численні учасники: ЄС, ООН, Рада Європи, а також інші міжнародні і регіональні організації, окремі держави та їх об'єднання (наприклад, G7).

Для запобігання потенційним порушенням прав людини необхідною є прозорість у застосуванні штучного інтелекту, особливо в чутливих сферах, таких як безпека та правоохоронна діяльність, кібербезпека і приватність. Тому актуальним залишається застереження генерального директора ЮНЕСКО з приводу того, що «Штучний інтелект – це новий рубіж людства. Як тільки цей кордон буде перетнуто, штучний інтелект призведе до нової форми людської цивілізації. Керівний принцип штучного інтелекту – не стати автономним або замінити людський інтелект. Але ми повинні переконатися, що він розвивається через гуманістичний підхід, заснований на цінностях і правах людини. Перед нами постає важливе питання: яке суспільство ми хочемо бачити завтра? Революція штучного інтелекту відкриває нові захоплюючі перспективи, але антропологічні та соціальні потрясіння, які вона несе за собою, вимагають ретельного розгляду» [18].

Власне, саме тому ефективне управління цим процесом потребує обов'язкового всебічного та інклюзивного діалогу між експертами з технологій, правозахисниками, політиками та представниками громадськості. Подібна співпраця є критично важливою для глибокого розуміння впливу штучного інтелекту на фундаментальні права людини та гарантування того, що розробка й застосування цієї технології відбуватиметься відповідально, етично та з повагою до гідності і недоторканності особи.

Найвпливовіші глобальні компанії, які сьогодні домінують в економічних рейтингах і на ринках, усі мають одну спільну рису: це великі технологічні платформи, що надають цифрові послуги та продукти, базуючи свої бізнес-моделі на даних, їх цінності та корисності. Встановлення правил для природно глобалізованої та децентралізованої цифрової економіки вимагає політичного впливу на наднаціональному рівні. Виходячи у тому числі й з таких міркувань, 21 травня 2024 р. Рада ЄС остаточно схвалила регламент про штучний інтелект, прийнятий Європейським парламентом 13 березня 2024 р., який 01 серпня 2024 р. набув чинності [19].

Положення вказаного акту впроваджуються поетапно, починаючи з 02 лютого 2025 р., з поступовим посиленням регуляторних норм: до 02 лютого 2025 р. – заборона на використання систем штучного інтелекту, що становлять неприйнятний ризик, й до цієї категорії належать інструменти, котрі здатні до маніпулювання людьми, обману або класифікації за соціальними рейтингами; до 02 серпня 2025 р. – запровадження положень для регулювання систем штучного інтелекту загального призначення, й тут, зокрема, передбачено, що вказані положення визначатимуть загальні принципи та вимоги до розробки і використання систем штучного інтелекту; до 02 серпня 2026 р. – введення обмежувальних правил для систем штучного інтелекту «високого ризику», й до цієї категорії належать системи, що використовуються правоохоронними та державними органами, а також інструменти для біометричної ідентифікації і розпізнавання емоцій.

Примітно, що вказаний акт класифікує системи штучного інтелекту *за категоріями ризику*: *низький ризик*: такі моделі штучного інтелекту як спам-фільтри або відеоігри, які не потребують регулювання; *обмежувальний ризик*: чат-боти та інші системи, що генерують текст і зображення, підпадають під цю категорію, для них встановлюються певні вимоги щодо прозорості та звітності; *високий ризик*: системи, що використовуються правоохоронними та державними органами, а також інструменти для біометричної ідентифікації і розпізнавання емоцій, відносяться до цієї категорії, й для них передбачаються більш суворі вимоги та контроль з боку відповідних органів; *неприйнятний ризик*: системи, які можуть обманювати людей, маніпулювати ними або оцінювати їх на основі соціальної поведінки чи особистих якостей, заборонені до використання.

При цьому, поетапне впровадження регулювання штучного інтелекту дозволяє:

– *забезпечити плавний перехід*, що надає можливість учасникам ринку адаптуватися до нових вимог та впровадити необхідні зміни у своїх системах;

– *мінімізувати негативні наслідки*, зокрема поетапний підхід допомагає уникнути різких змін, які можуть призвести до економічних чи соціальних проблем;

– *зібрати дані та досвід*, власне поступове впровадження регулювання дає можливість накопичити емпіричну базу, що у підсумку допоможе вдосконалити регуляторні норми в майбутньому.

Представляється, що поетапне впровадження регулювання штучного інтелекту є важливим кроком на шляху до забезпечення його безпечного, етичного й відповідального використання. Такий підхід дозволяє максимізувати потенційні переваги штучного інтелекту, мінімізуючи при цьому ризики, пов'язані з його розвитком та застосуванням.

Регламент забороняє використання біометричних систем ідентифікації правоохоронними органами, за винятком чітко визначених випадків. Системи ідентифікації в режимі реального часу можуть застосовуватися лише за умови суворого дотримання заходів безпеки, зокрема таких як обмеження за часом і географією, а також наявність попередньої судової або адміністративної згоди. Приклади таких випадків можуть включати пошук зниклих осіб чи запобігання терористичним актам. Проте, слід звернути увагу, що використання цих систем в інших випадках вважається надзвичайно ризикованим і потребує судового дозволу, пов'язаного з кримінальною справою.

Окрім того, також встановлені чіткі вимоги для інших високоризикових систем штучного інтелекту через їх досить значний потенціал заподіяти шкоду здоров'ю, безпеці, осно-

вним правам, навколишньому середовищу, демократії та верховенству права. Приклади подібного високоризикового використання штучного інтелекту включають критичну інфраструктуру, освіту та професійну підготовку, працевлаштування, основні приватні та державні послуги (зокрема, у таких сферах як охорона здоров'я, банківська діяльність), деякі системи правоохоронних органів, управління міграцією та кордонами, правосуддя і демократичні процеси (наприклад, вплив на вибори). Такі системи повинні оцінюватися на предмет ризиків, й тут же також необхідно вживати заходів щодо зменшення ризиків при їх використанні (наприклад, вести облік доступу і використання), вони мають бути прозорими і точними, а також забезпечувати нагляд з боку людини, зокрема йдеться про створення умов, за яких громадяни матимуть право подавати скарги на системи штучного інтелекту та отримувати пояснення щодо рішень, заснованих на високоризикових системах штучного інтелекту, які впливають на їх права.

Тож затвердження Європейським парламентом регламенту про штучний інтелект безумовно свідчить на користь посилення регулювання і контролю за використанням штучного інтелекту в ЄС. Вказаний документ встановлює нові зобов'язання для систем штучного інтелекту на основі їх потенційних ризиків та впливу на суспільство, що відображає зростаючу необхідність забезпечення етичного й безпечного використання цієї технології.

Регламент пропонує широке визначення штучного інтелекту, яке охоплює «будь-яку машинну систему, розроблену для роботи з різними рівнями автономності та яка може проявляти адаптивність після розгортання та яка, для явних чи неявних цілей, робить висновок, на основі вхідних даних, які вона отримує, як генерувати результати, такі як передбачення, вміст, рекомендації або рішення, які можуть впливати на фізичне чи віртуальне середовище».

Документ розрізняє два типи систем штучного інтелекту, а саме: *системи штучного інтелекту* (охоплює всі системи, що відповідають згаданому вище визначенню штучного інтелекту) та *моделі штучного інтелекту загального призначення* (*GPAI*) (тип моделі штучного інтелекту, навченої на величезному наборі даних з використанням методів масштабного самоконтролю, такі моделі здатні виконувати широкий спектр завдань). При цьому, передбачається кілька винятків із загальних правил, зокрема: системи та моделі штучного інтелекту, призначені для військових цілей, оборони і національної безпеки; системи та моделі штучного інтелекту, розроблені та введені в експлуатацію виключно для наукових досліджень і розробок; дослідницька, тестова або розробна діяльність щодо систем або моделей штучного інтелекту до їх розміщення на ринку або введення в експлуатацію; також системи штучного інтелекту, котрі випущені за безкоштовними ліцензіями та ліцензіями з відкритим вихідним кодом, за винятком випадків, коли вони підпадають під заборону і вимоги щодо прозорості для генеративних систем штучного інтелекту.

Варто зауважити, що документ має значний вплив на наукову роботу в галузі штучного інтелекту. Науковці, котрі розробляють, досліджують або впроваджують системи штучного інтелекту в ЄС, повинні бути ознайомлені з цим законом та його положеннями [20], він є комплексним документом, який встановлює рамки для регулювання штучного інтелекту на території ЄС.

Зважаючи на затвердження переговорних рамок щодо вступу України в ЄС, наша країна повинна враховувати, що європейські регулятори активно працюють над впровадженням повноцінного регулювання штучного інтелекту в ЄС, і аналогічні обмеження в майбутньому будуть застосовані і в Україні під час безпосередньої інтеграції. Ми маємо кілька років до того моменту, коли зазначені заходи стануть обов'язковими для імплементації в Україні, що надає нам можливість здобути значну перевагу на міжнародній арені та визначити майбутнє професійних послуг у нашій країні. Перед нами відкривається дійсно унікальна можливість успішно скористатися швидким розвитком технологій та забезпечити собі конкурентні переваги у цій сфері. У вказаному аспекті слід зауважити про те, що Міністерство цифрової трансформації України, завчасно готуючись до нових реалій регламенту ЄС про штучний інтелект, 07 жовтня 2023 р. презентувало Дорожню карту з регулювання штучного інтелекту в Україні [21]. Одним із пріоритетів Дорожньою картою визначено захист прав українців у цифровому просторі для створення безпечного середовища, де штучний інтелект не становитиме додаткових загроз.

Підсумовуючи проведене дослідження, відмітимо, що основна концепція регламенту ЄС про штучний інтелект полягає в тому, що

широке впровадження цифрових технологій, таких як штучний інтелект, є соціально та економічно вигідним для компаній і споживачів. Компанії можуть оптимізувати власні виробничі моделі та краще прогнозувати ринкові тенденції, тоді як споживачі отримують вигоди від персоналізованих продуктів. Однак, цифрові ринки потребують певних умов для свого процвітання. Зусилля з насильницького впровадження зазначених технологій у національний контекст за допомогою специфічних правил можуть просто знищити їх порівняльну перевагу, створену завдяки мережевому ефекту масштабу. Ця визначальна риса цифрових ринків служить виправданням для поширення основоположного принципу ЄС щодо ринкової інтеграції на нову цифрову сферу.

У вказаному контексті ЄС виступає як рушійна сила для розвитку ринку, встановлюючи загальні правила, аби забезпечити зникнення віртуальних кордонів на єдиному цифровому ринку, що приносить користь усім. Важливо, що у пропозиції регламенту про штучний інтелект, ЄС представлений як гарант «*правової визначеності*», запроваджуючи лише «*мінімально необхідні вимоги*» для ринків. Крім того, ЄС також виконує роль захисника «*основних міркувань суспільного інтересу та прав осіб на всьому внутрішньому ринку*». Це вказує на необхідність балансу між посиленням ринкової інтеграції та забезпеченням соціального захисту: єдині зобов'язання для операторів лежать в основі єдиного захисту для людей.

Висновки. По результатах проведеного дослідження видається можливим сформулювати низку важливих висновків і пропозицій.

Із прийняттям регламенту про штучний інтелект, ЄС претендує на встановлення правил емансипації та соціального захисту для цифрових ринків, одночасно визначаючи, що означають емансипація та соціальний захист і як їх слід застосовувати в контексті цифрового середовища. При цьому, доцільно констатувати, що документ не пропонує рішень для безпосереднього залучення соціальних учасників до процесу прийняття рішень. Таким чином, хоча основні положення регламенту спрямовані на емансипацію, у ньому відсутні елементи процедурних рішень, які б надавали повноваження особам і організаціям, що представляють інтереси суспільства. Відтак, у вказаному контексті вважаємо, що основні зусилля в Україні, у ході імплементації стандартів ЄС в національне законодавство з питань щодо регулювання штучного інтелекту, мають бути сконцентровані на зміщення балансу між посиленням і формуванням ринку в бік емансипації.

Примітно, що ЄС намагається створити для себе нову нормативну роль, коли справа доходить до формування ринку через регулювання цифрової економіки. Зрештою ж, те, як регуляторні пропозиції ЄС збалансовують маркетизацію, соціальний захист і емансипацію, є питанням інтересу не лише для самого ЄС, оскільки норми, прийняті ЄС, часто стають шаблоном, якого дотримуються інші країни та організації. Аналізуючи потрійний рух у контексті цифровізації та враховуючи роль, яку у вказаному процесі відіграє регламент, варто зосередитися на ЄС як важливому а́кторові, що намагається розробити регуляторні стандарти в цій сфері.

Незважаючи на низку дискусійних аспектів, нормативно-правова база ЄС у сфері штучного інтелекту слугує орієнтиром для національних законодавчих ініціатив. Вказане визначається наступним:

– *глобальний вплив*: ЄС – один з найважливіших економічних та політичних блоків у світі, тому його норми мають значний вплив на інші країни;

– *комплексний підхід*: нормативно-правова база ЄС охоплює широкий спектр аспектів, пов'язаних зі штучним інтелектом, зокрема від розробки та впровадження до етики та відповідальності;

– *фокус на етиці*: ЄС ставить етику в пріоритет при регулюванні штучного інтелекту, що робить його норми актуальними та соціально відповідальними.

Як зазначалося, нові технології штучного інтелекту також створюють й нові виклики, які потребують чіткої та послідовної стратегії регулювання. Один із ключових викликів, з якими стикається ЄС, – це знайти баланс між свободою вираження поглядів та міркуваннями безпеки. Так, штучний інтелект ризикує використовуватися для поширення дезінформації і пропаганди, що може становити загрозу для демократії та суспільного добробуту. Відтак, важливо розробити правила, які б захищали свободу вираження поглядів, але водночас запобігали зловживанню штучним інтелектом.

Інтеграція штучного інтелекту в бізнес-процеси суб'єктів господарювання дійсно може принести значну користь, однак важливо здійснювати її етично та відповідально. З цією метою на національному рівні необхідно

розробити та впровадити етичні норми, проводити оцінку ризиків, забезпечувати прозорість, захищати дані та залучати до процесу всіх зацікавлених сторін.

Варто пам'ятати, що штучний інтелект – це надпотужний інструмент, який може бути використаний як на благо, так і на шкоду, відтак важливо використовувати його максимально відповідально, аби не завдати шкоди людям і суспільству.

Представляється, що баланс забезпечення прав людини та соціальної відповідальності у процесі інтеграції штучного інтелекту у бізнес-процеси суб'єктів господарювання можливий за умови дотримання системного підходу до таких сфер:

– *стратегії інтеграції*: компанії мають розробляти такі стратегії інтеграції штучного інтелекту, котрі враховуватимуть як економічну ефективність, так і соціальну відповідальність, й цей процес передбачає етичні перевірки, аудит алгоритмів і активну участь зацікавлених сторін у процесі прийняття рішень;

– *регулювання та стандарти*: державні органи та міжнародні організації розробляють регулювання та стандарти для використання штучного інтелекту, компанії ж повинні неухильно дотримуватися цих стандартів, аби забезпечити баланс між інноваціями й відповідальністю;

– *співпраця з громадськістю*: уявляється важливим, аби компанії активно взаємодіяли з громадськістю, пояснювали свою політику щодо використання штучного інтелекту та прислухалися до зворотного зв'язку від споживачів і працівників.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Human Rights: A Path for Solutions. *United Nations High Commissioner for Human Rights*. 2024. URL: https://www.ohchr.org/sites/default/files/2024-09/hc-visionstatement-2024-en.pdf

2. The AI for Good Global Summit. URL: https://aiforgood.itu.int/summit24

3. Developing safer digital technologies for all. *United Nations High Commissioner for Human Rights*. URL: https://www.ohchr.org/en/stories/2023/10/developing-safer-digital-technologies-all

4. Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework. *United Nations High Commissioner for Human Rights*. URL: https://www.ohchr.org/en/publications/reference-publications/guiding-principles-business-and-human-rights

5. Elon Musk on danger of Artificial Intelligence. https://www.youtube.com/watch?v=KQs2KtVWQHI

6. The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023. URL: https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023

7. Biden hails 'bold action' of US government with order on safe use of AI. *The Guardian*. URL: https://www.theguardian.com/technology/2023/oct/30/biden-orders-tech-firms-to-share-ai-safety-test-results-with-us-government

8. Sam Biddle. OpenAI quietly deletes ban on using ChatGPT for "military and warfare". *The Intercetp*. URL: https://theintercept.com/2024/01/12/open-ai-military-ban

9. Коваленко Ю., Войнов М. Штучний інтелект та права людини: орієнтири та обмеження у контексті національної безпеки та оборони. *Українська Гельсінська спілка з прав людини*. 2024. URL: https://www.helsinki.org.ua/wp-content/uploads/2024/05/Preview_AI_human_right_A4-1.pdf

10. Ryan Calo. Artificial Intelligence Policy: A Primer and Roadmap. URL: https://lawreview.sf.ucdavis.edu/sites/g/files/dgvnsk15026/files/media/documents/51-2_Calo.pdf

11. United Nations General Assembly, Resolution A/78/L.49 Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development. URL: https://digitallibrary.un.org/record/4040897?v=pdf

12. A Global Digital Compact – an Open, Free and Secure Digital Future for All. URL: https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-gobal-digi-compact-en.pdf

13. Ban biometric surveillance. *AccessNow*. URL: https://www.accessnow.org/campaign/ban-biometric-surveillance

14. Steve Feldstein, Brian Kot. Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses. *Carnegie Endowment for International Peace*. URL: https://carnegieendowment.org/research/2023/03/why-does-the-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses?lang=en

15. Patrick Howell O'Neill. French spyware bosses indicted for their role in the torture of dissidents. *MIT Technology Review*. URL: https://www.technologyreview.com/2021/06/22/1026777/france-spyware-amesys-nexa-crimes-against-humanity-libya-egypt

16. Zach Campbell, Caitlin L. Chandler. Tools for repression in Myanmar expose gap between EU tech investment and regulation. *The Intercetp*. URL: https://theintercept.com/2021/06/14/myanmar-msab-eu-technology-regulation

17. Eva Galperin. Swedish Telcom Giant TeliaSonera Caught Helping Authoritarian Regimes Spy on Their Citizens. *The Electronic Frontier Foundation*. URL: https://www.eff.org/deeplinks/2012/05/swedish-telcom-giant-teliasonera-caught-helping-authoritarian-regimes-spy-its

18. Audrey Azoulay. Towards an Ethics of Artificial Intelligence. *UN Chronicle*. URL: https://www.un.org/en/chronicle/article/towards-ethics-artificial-intelligence

19. 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). Document 32024R1689. EUR-Lex. *European Union*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401689

20. Thaima Samman, Benjamin De Vanssay. What to take away from the European law on artificial intelligence. *The Robert Schuman Foundation*. URL: https://www.robert-schuman.eu/en/european-issues/757-what-to-take-away-from-the-european-law-on-artificial-intelligence

21. Регулювання штучного інтелекту в Україні: Мінцифри презентувало дорожню карту. *Урядовий портал*. URL: https://www.kmu.gov.ua/news/rehuliuvannia-shtuchnoho-intelektu-v-ukraini-mintsyfry-prezentuvalo-dorozhniu-kartu

REFERENCES:

1. United Nations High Commissioner for Human Rights. (2024). *Human rights: A path for solutions*. Available at: https://www.ohchr.org/sites/default/files/2024-09/hc-visionstatement-2024-en.pdf

2. International Telecommunication Union. (2024). *The AI for Good Global Summit*. Available at: https://aiforgood.itu.int/summit24

3. United Nations High Commissioner for Human Rights. (2023, October). *Developing safer digital technologies for all*. Available at: https://www.ohchr.org/en/stories/2023/10/developing-safer-digital-technologies-all

4. United Nations High Commissioner for Human Rights. (2012, January 01). *Guiding principles on business and human rights: Implementing the United Nations* "*Protect*, *Respect and Remedy*" *framework*. Available at: https://www.ohchr.org/en/publications/reference-publications/guiding-principles-business-and-human-rights

5. Musk, E. (2018). *Elon Musk on danger of artificial intelligence* [Video]. YouTube. Available at: https://www.youtube.com/watch?v=KQs2KtVWQHI

6. The Bletchley Declaration by countries attending the AI Safety Summit, 1–2 November 2023. (2023). GOV.UK. Available at: https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023

7. The Guardian. (2023, October 30). *Biden hails* '*bold action*' *of US government with order on safe use of AI*. Available at: https://www.theguardian.com/technology/2023/oct/30/biden-orders-tech-firms-to-share-ai-safety-test-results-with-us-government

8. Biddle, S. (2024, January 12). *OpenAI quietly deletes ban on using ChatGPT for* "*military and warfare*". The Intercept. Available at: https://theintercept.com/2024/01/12/open-ai-military-ban

9. Kovalenko, Y., & Voinov, M. (2024). *Shtuchnyi intelekt ta prava liudyny*: *Oriientyry ta obmezhennia u konteksti natsionalnoi bezpeky ta oborony* [Artificial Intelligence and Human Rights: Guidelines and Limitations in the Context of National Security and Defence]. Ukrainian Helsinki Human Rights Union. Available at: https://www.helsinki.org.ua/wp-content/uploads/2024/05/Preview_AI_human_right_A4-1.pdf [in Ukrainian]

10. Calo, R. (n.d.). *Artificial intelligence policy*: *A primer and roadmap*. Available at: https://lawreview.sf.ucdavis.edu/sites/g/files/dgvnsk15026/files/media/documents/51-2_Calo.pdf

11. United Nations General Assembly. (2024). *Resolution A*/*78*/*L*.*49*: *Seizing the opportunities of safe*, *secure and trustworthy artificial intelligence systems for sustainable development*. Available at: https://digitallibrary.un.org/record/4040897?v=pdf

12. United Nations. (2023, May). *A global digital compact*: *An open*, *free and secure digital future for all*. Available at: https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-gobal-digi-compact-en.pdf

13. AccessNow. (n.d.). *Ban biometric surveillance*. Available at: https://www.accessnow.org/campaign/ban-biometric-surveillance

14. Feldstein, S., & Kot, B. (2023, March). *Why does the global spyware industry continue to thrive*? *Trends*, *explanations*, *and responses*. Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/research/2023/03/why-does-the-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses?lang=en

15. Howell O'Neill, P. (2021, June 22). *French spyware bosses indicted for their role in the torture of dissidents*. MIT Technology Review. Available at: https://www.technologyreview.com/2021/06/22/1026777/france-spyware-amesys-nexa-crimes-against-humanity-libya-egypt

16. Campbell, Z., & Chandler, C. L. (2021, June 14). *Tools for repression in Myanmar expose gap between EU tech investment and regulation*. The Intercept. Available at: https://theintercept.com/2021/06/14/myanmar-msab-eu-technology-regulation

17. Galperin, E. (2012, May). *Swedish telecom giant TeliaSonera caught helping authoritarian regimes spy on their citizens*. Electronic Frontier Foundation. Available at: https://www.eff.org/deeplinks/2012/05/swedish-telcom-giant-teliasonera-caught-helping-authoritarian-regimes-spy-its

18. Azoulay, A. (2018, December 21). *Towards an ethics of artificial intelligence*. UN Chronicle. Available at: https://www.un.org/en/chronicle/article/towards-ethics-artificial-intelligence

19. European Union. (2024). *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*). *Document 32024R1689*. EUR-Lex. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401689

20. Samman, T., & De Vanssay, B. (2024, July 16). *What to take away from the European law on artificial intelligence*. Robert Schuman Foundation. Available at: https://www.robert-schuman.eu/en/european-issues/757-what-to-take-away-from-the-european-law-on-artificial-intelligence

21. Uriadovyi portal. (2023, October 07). *Rehuliuvannia shtuchnoho intelektu v Ukraini*: *Mintsyfry prezentuvalo dorozhniu kartu* [Regulation of artificial intelligence in Ukraine: the Ministry of Digital Transformation has presented a roadmap]. Available at: https://www.kmu.gov.ua/news/rehuliuvannia-shtuchnoho-intelektu-v-ukraini-mintsyfry-prezentuvalo-dorozhniu-kartu [in Ukrainian]

Дата надходження статті: 30.01.2026
Дата прийняття статті: 24.02.2026
Дата публікації статті: 27.03.2026