УДК 42.72/.73:519

ТАРАН О.В., *доктор юридичних наук, професор*, провідний науковий співробітник наукової лабораторії з проблем протидії злочинності НАВС.
ORCID: https://orcid.org/0000-0003-4752-9924.
ГАВЛОВСЬКИЙ В.Д., *кандидат юридичних наук, с.н.с.*,
головний науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України.
ORCID: https://orcid.org/0000-0001-7496-9904.

ПРАВОВЕ РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ЄВРОПЕЙСЬКОМУ СОЮЗІ ТА УКРАЇНІ: ОСНОВНІ ПІДХОДИ ТА ПРАВА ЛЮДИНИ

***Анотація**. У статті здійснено аналітичний огляд низки міжнародних та національних документів, що стосуються різних аспектів правового регулювання штучного інтелекту. Акцентується увага на проблемах нормативних і практичних підходів до забезпечення та дотримання прав людини на всіх етапах життєвого циклу штучного інтелекту.*

***Ключові слова**: штучний інтелект, правове регулювання, нормативні документи, права людини, стандарти, збройний конфлікт.*

***Summary.** The article provides an analytical review of a number of international and national documents relating to various aspects of the legal regulation of artificial intelligence. Attention is focused on the problems of regulatory and practical approaches to ensuring and observing human rights at all stages of the life cycle of artificial intelligence.*

***Keywords:** artificial intelligence, legal regulation, regulatory documents, human rights, standards, armed conflict.*

Постановка проблеми. Сьогодні не викликає сумніву, що прогрес у галузі технологій штучного інтелекту (далі – ШІ) відкриває широкі перспективи для розвитку різноманітних сфер людської діяльності та значно впливає на них. Потенціал застосування ШІ вражає – від можливостей автоматизації рутинних процесів до оптимізації складних операцій, персоналізації послуг, генерування контенту, проведення експертного аналізу великих масивів даних, ухвалення рішень в режимі реального часу без участі людини тощо. Поєднання широких функціональних можливостей, зручності та доступності систем ШІ очевидно свідчить, що популярність і використання ШІ надалі лише зростатимуть.

Водночас, поряд із безсумнівними перевагами, масштабне впровадження технологій ШІ актуалізує низку проблемних питань правового, етичного та соціального характеру. Зокрема, дедалі більшу увагу привертає правове регулювання сфер, пов’язаних із розробкою, впровадженням та визначенням відповідальності у сфері ШІ.

Поточний стан правової регламентації ШІ можна окреслити як такий, що перебуває у стадії становлення. Водночас, деякі з чинних регуляторних механізмів можуть бути екстрапольовані на цю сферу. Можна також констатувати процес формування ШІ як окремого об’єкта комплексного правового регулювання, що зумовлено його специфікою та потребує уваги до узгодження з суміжними сферами, захисту персональних даних, авторського права, інших прав людини, відповідальності, створення гнучких та дієвих механізмів правового реагування для постійної актуалізації нормативної бази, тощо.

Результати аналізу наукових публікацій. Різні аспекти функціонування та правового регулювання ШІ розглядали О. Баранов, О. Жидкова, О. Кармаза, Д. Кушерець, О. Костенко, В. Костенко, О. Кривецький, О. Радутний, К. Токарєва, О. Турута, Н. Шишка та ін.

Незважаючи на підвищену увагу до цієї тематики, залишаються дискусійними та потребують вирішення деякі проблеми щодо обсягу та змісту правового регулювання ШІ на міжнародному та національному рівні. Особливо гостро постає питання забезпечення та захисту прав людини на всіх етапах життєвого циклу ШІ.

Метою статті є аналітичний огляд низки нормативних актів у сфері ШІ, визначення стану правового регулювання у частині забезпечення і дотримання прав людини.

Виклад основного матеріалу. 21 квітня 2021 року Європейською Комісією було запропоновано Закон про штучний інтелект (Artificial Intelligence Act, AI Act) (далі – Закон) [1] політична домовленість між Європейським Парламентом і Радою щодо якого була досягнута у грудні 2023 року [2]. Цей Закон визначає комплексний та системний підхід, який охоплює широке коло застосування ШІ, у його основі – ризик-орієнтований підхід із диференціацією на мінімальний, високий, неприйнятний, конкретний ризик порушення прозорості. Для систем з високим ризиком передбачені жорсткі вимоги з управління ризиками, забезпечення точності, безпеки, захисту даних, також встановлюються обмеження щодо можливостей застосування окремих технологій (наприклад, дистанційної біометричної ідентифікації).

У Законі (стаття 3) сформульовані визначення ключових понять, серед яких: “система ШІ”, що означає програмне забезпечення, яке розроблене із використанням одного або декількох визначених в цьому Законі методів та підходів та можуть для заданого набору визначених людиною цілей генерувати вихідні дані, такі як контент, прогнози, рекомендації або рішення, що впливають на середовище, з яким вони взаємодіють; “біометричні дані” означають персональні дані, отримані в результаті спеціальної технічної обробки, що стосуються фізичних, фізіологічних або поведінкових характеристик фізичної особи, які дозволяють або підтверджують унікальну ідентифікацію цієї фізичної особи, наприклад, зображення обличчя або дактилоскопічні дані; “серйозний інцидент” – будь-який інцидент, який прямо або опосередковано призвів, міг призвести або може призвести до будь якої з подій: (а) смерть людини або серйозна шкода здоров’ю людини, майну або навколишньому середовищу, (в) серйозне і незворотне порушення управління і експлуатації критично важливої інфраструктури та ін. [3].

З огляду на структуру та зміст Закону, він має широку сферу охоплення і поширюється на різні категорії систем та компонентів ШІ: програмне забезпечення, алгоритми, дані, процеси навчання і валідації таких систем.

Регулюванню підлягають як суто програмні рішення, так і пов’язані з ними фізичні пристрої або компоненти. Закон також поширюється на різні стадії життєвого циклу таких систем – від розробки до розгортання, інтеграції та використання.

Тобто, законодавець намагався максимально широко і всеохоплююче визначити сферу дії регулювання ШІ і Закон фактично враховує усі ключові етапи створення та експлуатації систем ШІ.

Що стосується прав людини, то ключовими положеннями цього документа є те, що забезпечення дотримання прав і свобод людини визначено однією з головних цілей регулювання сфери ШІ. Документ прямо посилається як на загальні норми захисту прав людини в ЄС, так і на конкретні їх аспекти, зокрема повагу до приватного життя, особистої гідності, недискримінацію тощо, що означає необхідність їх дотримання під час розробки і використання ШІ. Відповідно до ризик-орієнтованого підходу, застосування

високоризикових систем ШІ має супроводжуватися незалежним аудитом з оцінки їх впливу на права людини. Також передбачені спеціальні механізми тестування ШІ-систем на предмет можливої дискримінації, расизму чи інших форм упередженості, це має запобігти проявам можливої алгоритмічної дискримінації та посилити соціальну справедливість, інклюзивність системи ШІ.

Отже, такий підхід, що передбачає визначення захисту прав людини як ключової мети Закону, впливає на увесь подальший зміст документа, ставить права людини в центр системи норм у сфері ШІ.

Очевидно, що ці положення можуть і мають бути орієнтиром для формування відповідних правових механізмів на національному рівні.

Водночас, привертає увагу і те, що Європейська Комісія у проекті запиту на стандартизацію до Європейського комітету зі стандартизації (CEN), Європейського комітету з електротехнічної стандартизації (CENELEC) у контексті Закону визначає такі стандарти, які необхідно розробити: система управління ризиками для систем ШІ, управління і якість набору даних, які використовуються для створення систем ШІ, ведення обліку за допомогою систем ШІ, прозорість і надання інформації користувачам ШІ, нагляд людини за системами ШІ, характеристики точності ШІ, специфікація надійності ШІ, кібербезпека ШІ, управління якістю для постачальників систем ШІ, включаючи процес після маркетингового моніторингу, оцінка відповідності систем ШІ (термін прийняття цих стандартів встановлено до 31 січня 2025 року) [4]. У цьому документі, який визначає пріоритетні галузі стандартизації, не передбачено розроблення стандартів для забезпечення і захисту прав людини як окремого напряму. Не міститься стандартів, аудиту або відповідних механізмів і у інших офіційних документах. Мають місце тільки загальні вказівки про важливість забезпечення прав людини, без конкретизації та визначення замовлення на розробку необхідних інструментів (за аналогією з технічними стандартами) на вирішення цієї проблеми. Таким чином, існує ризик, що деякі норми Закону, що стосуються прав людини матимуть декларативний характер, а їх практичне застосування може виявитися проблематичним.

Загальну позицію країн G7 та ЄС щодо розвитку і правового регулювання ШІ сформульовано в межах Хіросімського процесу з ШІ у Міжнародних керівних принципах для організацій з розробки передових систем ШІ [5] та Кодексу поведінки для організацій з розробки передових систем ШІ [6]. Ця позиція в цілому узгоджується з положеннями Закону.

Організація економічного співробітництва та розвитку (OECD) 8 листопада 2023 року схвалила Рекомендації щодо ШІ [7] (перший міжурядовий стандарт OECD щодо ШІ було ухвалено 22 травня 2019 року, його особливістю є сформульовані принципи ШІ: інклюзивне зростання, сталий розвиток та благополуччя; людино-орієнтовані цінності та справедливість; прозорість і пояснюваність; надійність, захищеність та безпека; підзвітність), у якому на основі власних аналітичних та емпіричних досліджень констатувала необхідність створення стабільного політичного середовища на міжнародному рівні для забезпечення довіри та сприйняття ШІ суспільством, що передбачає розвиток людино-центричного підходу до надійного ШІ.

Цей документ має рекомендаційний характер, його положення, що сформульовані у 2019 році, були враховані у Концепції розвитку штучного інтелекту в Україні (далі – Концепція) [8].

У Концепції, серед іншого, зазначено, що принципами розвитку та використання технологій ШІ є розроблення та використання систем ШІ лише за умови дотримання верховенства права, основоположних прав та свобод людини і громадянина,

демократичних цінностей, а також забезпечення відповідних гарантій під час використання таких технологій; відповідність діяльності та алгоритму рішень систем штучного інтелекту вимогам законодавства про захист персональних даних, а також додержання конституційного права кожного на невтручання в особисте і сімейне життя у зв'язку з обробкою персональних даних [8].

Аналізуючи Концепцію з точки зору захисту прав людини, можна зазначити, що серед ключових прав людини, що згадуються у документі, виділено право на захист персональних даних та право на недискримінацію. Це положення є особливо актуальним у контексті розвитку систем ШІ, які часто оперують значними обсягами даних користувачів, тому необхідно запобігти зловживанням та забезпечити безпеку персональних даних під час їх обробки. Захист від дискримінації має запобігти алгоритмічній дискримінації, прихованим упередженням та викривленням у процесі роботи ШІ.

Задекларовано також неприпустимість використання технологій ШІ для порушення прав і свобод людини чи створення загроз громадській безпеці.

Для забезпечення реалізації цих прав передбачено розробку спеціальних етичних правил (Етичного кодексу ШІ) та стандартів (забезпечення функціонування та діяльності технічних комітетів стандартизації відповідно до вимог 7.1.5 ДСТУ 1.14:2015 "Національна стандартизація. Процедури створення, діяльності та припинення діяльності технічних комітетів стандартизації" за напрямом штучного інтелекту), а також формування нормативно-правової бази (опрацювання питання щодо необхідності врегулювання суспільних відносин у сфері розвитку штучного інтелекту на законодавчому рівні), що регулюватиме сферу ШІ з огляду на європейське законодавство. Таким чином, стандартизація та правила застосування ШІ мають забезпечити наскрізне дотримання й захист прав людини на усіх етапах – від розробки до експлуатації систем ШІ. Прикладом може слугувати європейська регуляторна практика у цій сфері.

Отже, можна зробити висновок, що попри певну декларативність, Концепція передбачає вимоги щодо забезпечення захисту прав людини в процесі розвитку сфери ШІ в Україні, але так само, як і інші документи, не визначає конкретні заходи та механізми для забезпечення таких гарантій. Така ж проблема існує і з визначенням відповідальності.

7 жовтня 2023 року Міністерство цифрової інформації презентувало дорожню карту з регулювання ШІ в Україні [9]. Серед іншого, передбачається, що Україна повинна буде імплементувати AI Act Європейського Союзу як одну з умов євроінтеграції в цифровій сфері, а також впровадження (на кінцевому етапі) регуляції, яка пропонує найвищий у світі рівень захисту прав людини від ризиків та зловмисного використання ШІ.

Примітно також, що у презентації зауважено про важливість використання ШІ у сфері військових технологій [10], проте у самому документі відповідних положень не міститься.

Продовжуючи цю актуальну для України і світу тему, потрібно зауважити, що поряд з розвитком правового регулювання ШІ у "цивільній" сфері, правове регулювання ШІ в умовах збройного конфлікту фактично відсутнє. Як убачається, засоби міжнародного права, міжнародного гуманітарного права (далі – МГП) та національного права очевидно недостатні, оскільки прямо не регулюють питання застосування зброї, керованої ШІ (автономна зброя).

Тобто існуючі норми не встановлюють чітких правил щодо застосування автономних систем озброєння на основі ШІ. Це створює значні ризики, адже такі системи можуть діяти непередбачувано, поза людським контролем, що суперечить принципам МГП, а передусім – пропорційності та вибірковості.

Актуальним залишається питання відповідальності за помилки чи злочини із застосуванням автономної зброї, що передбачає необхідність визначити коло суб'єктів, відповідальних за розгортання та застосування автономних систем озброєння.

Відсутність правового регулювання автономної зброї також стимулює гонку озброєнь у цій сфері, що на відміну від, наприклад, гонки ядерних озброєнь, яка традиційно вважається найбільшою загрозою міжнародній безпеці та стабільності, вкрай складно контролювати, оскільки розроблення автономної зброї не потребує залучення специфічних ресурсів обіг яких обмежений та контролюється.

Для прав людини, які мають бути забезпечені навіть в умовах збройного конфлікту, правове регулювання автономної зброї потрібне для захисту цивільного населення, цивільних об'єктів, дотримання прав комбатантів та інших осіб та об'єктів захисту у розумінні МГП. Обмеження та заборони необхідні для запобігання застосуванню систем ШІ, рішення яких неможливо дослідити, оскаржити та забезпечити відповідальність. Це суперечить принципам прийнятності, пропорційності та верховенства права.

Групою урядових експертів (Австралія, Канада, Японія, Республіка Корея, Сполучене Королівство, США) з нових технологій у галузі летальних автономних систем озброєння подано проект нормативного акта про автономні системи озброєння та інші регуляторні заходи на основі МГП [11].

В цьому документі зазначено, що дослідження і розроблення нових технологій у сфері ШІ розвивається швидкими темпами, потенційно дозволяючи створювати новітню і більш досконалу зброю з автономними функціями, зокрема системи озброєння, які після активації можуть ідентифікувати, обирати і уражати цілі із застосуванням летальної сили без подальшого втручання оператора.

На підставі цього був розроблений проект статей щодо заборон та регуляторних заходів, які повинні забезпечити дотримання цих вимог МГП державами під час застосування автономних систем озброєння у збройному конфлікті. Йдеться про заборони розробки систем, що за своєю природою не можуть використовуватися у відповідності з МГП; вимоги дотримання принципів розрізнення, пропорційності та запобіжних заходів під час атак із застосуванням автономних систем; регуляторні заходи для забезпечення підзвітності та відповідальності за використання таких систем зброї; системи повинні функціонувати під контролем людини і на підставі наказу командувача.

Таким чином, проект статей має на меті визначення правової основи застосування МГП до автономних систем озброєння та належне регулювання цих систем у збройних конфліктах в інтересах захисту цивільного населення та забезпечення відповідальності за застосування такої зброї.

Водночас, в контексті захисту прав людини у цьому документі не конкретизовано, як саме має здійснюватися оцінка дотримання системами принципів МГП, не визначено мінімально необхідного рівня втручання людини-оператора для забезпечення належного контролю над системами, а також відсутні механізми реалізації та контролю за дотриманням наведених вимог державами.

Висновки.

Активна нормативна діяльність у сфері забезпечення правового регулювання ШІ відображає нагальну необхідність такого регулювання, де чільне місце належить забезпеченню і захисту прав людини. Водночас, через недостатність уваги до конкретних механізмів та інструментів контролю, саме права людини виявляються найбільш вразливою ланкою у правовому регулюванні. Оскільки наразі не передбачено стандартизованих механізмів виявлення впливу ШІ на права людини, тому це має розглядатися як пріоритетне завдання розвитку правового регулювання ШІ. При цьому

правова основа має забезпечувати гарантії дотримання прав людини та забезпечувати можливості для правового захисту.

Ефективність цієї діяльності потребує узгоджених зусиль міжнародної спільноти, окремих держав, науковців, громадянського суспільства та компаній, що розробляють і впроваджують технології ШІ.

Першочерговими завданнями є формування чітких міжнародних правових норм у цій сфері та імплементація їх положень в національні законодавства. Обов'язковими складовими регулювання мають стати оцінки впливу на права людини, регулярні аудити алгоритмів і систем ШІ, процедури оскарження автоматизованих рішень, відшкодування шкоди у разі порушень. Лише за умови дотримання цих принципів ШІ слугуватиме інтересам людства, не порушуючи прав окремої людини.

Окрему увагу потрібно приділити застосуванню технологій ШІ під час збройних конфліктів. Тут має забезпечуватись неухильне дотримання норм МГП, зокрема щодо принципів ведення бойових дій та захисту цивільного населення, а також міжнародного права прав людини Необхідно розробити регламенти використання озброєнь з ШІ, що забезпечуватимуть відповідність цим вимогам.

Використана література

1. Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682

2. Європейська Комісія вітає політичну домовленість щодо Закону про штучний інтелект. Представництво Європейського Союзу в Україні. – (11 грудня 2023 року). URL: https://www.eeas.europa.eu/delegations/ukraine

3. Artificial Intelligence Act. URL: https://artificialintelligenceact.com

4. Draft standardisation request to the European Standardisation Organisations in support of safe and trustworthy artificial intelligence. Document date: 05.12.2022. URL: https://ec.europa.eu/docsroom/documents/52376?locale=en

5. Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI System. On 30 October (JST) 2023. URL: https://www.mofa.go.jp/files/100573471.pdf

6. Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems. On 30 October (JST) 2023. URL: https://www.mofa.go.jp/files/100573473.pdf

7. Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449. URL: https://legalinstruments.oecd.org/api/print?ids=648&lang=en

8. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження КМУ від 02.12.20 р. № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text

9. Дорожня карта з регулювання штучного інтелекту в Україні. Bottom-Up Підхід. URL: https://cms.thedigital.gov.ua/storage/uploads/files/page/community/docs_compressed.pdf

10. Регулювання штучного інтелекту в Україні: презентуємо дорожню карту. – (Міністерство цифрової трансформації України, 07.10.23 р.). URL: https://thedigital.gov.ua/news/ regulyuvannya-shtuchnogo-intelektu-v-ukraini-prezentuemo-dorozhnyu-kartu

11. Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects. United Nations Office for Disarmament Affairs 13 March 2023. URL: https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons-Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2023)/CCW_GGE1_2023_WP.4_Rev1.pdf

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~