РОЗДІЛ ІІ. МІЖНАРОДНЕ ПРАВО

УДК 341:347.8:519.7.007.5 DOI https://doi.org/10.26661/2786-5649-2022-1-02

Визначення та правові вимоги до «високоризикованих» технологій штучного інтелекту

Тюря Ю. І.
кандидат технічних наук, доцент,
доцент кафедри цивільного, господарського та екологічного права
Національний технічний університет «Дніпровська політехніка»
пр. Дмитра Яворницького, 19, м. Дніпро, Україна
orcid.org/0000-0001-7732-3535
Tyurya.J.I@nmu.one

Ключові слова: *ризики, критерії, «високоризикований» штучний інтелект, правові вимоги, права людини, дистанційна (віддалена) біометрична ідентифікація.*

Штучний інтелект швидко завойовує всі сфери людської діяльності. Нові технології відкривають значні можливості для прискорення досліджень, творчості та організації діяльності у всіх сферах. При цьому будь-який навіть невеликий збій в алгоритмі роботи штучного інтелекту може призвести до невідворотних негативних наслідків. Отже, слід розуміти, що штучний інтелект має ряд переваг, але так само його використання супроводжується потенційними ризиками. Всі ризики необхідно передбачити та мінімізувати, що своєю чергою потребує створення належного правового поля для регламентації суспільних відносин щодо використання технологій штучного інтелекту.

Тому метою даної роботи стало визначення «високоризикованих» технологій штучного інтелекту та встановлення правових вимог до них.

У роботі висвітлено позицію Європейської Комісії щодо встановлення критеріїв, відповідно до яких технологію штучного інтелекту можливо кваліфікувати як «високоризикована» або з «високим ризиком». Комісією пропонується застосовувати пропорційне регуляторне втручання щодо використання технологій штучного інтелекту на підставі оцінки ризику, враховуючи ступінь можливого впливу цих технологій протягом їх життєвого циклу на права людини.

У статті розглянуто обов'язкові правові вимоги до «високоризикованих» технологій, які були запропоновані Європейською Комісією, з метою цілеспрямованого та пропорційного регуляторного втручання щодо використання технологій штучного інтелекту. Встановлено, що головними орієнтирами при визначенні вимог є ключові складові, характеристики, властивості та функції технологій, які є високоризикованими. До них належать: бази даних, облік даних, інформаційне забезпечення, надійність й точність, людський нагляд. З'ясовано, що використання технологій штучного інтелекту для цілей віддаленої біометричної ідентифікації можливо лише за умови, якщо таке використання є обґрунтованим належним чином, пропорційним, підлягає відповідним гарантіям та становить значний суспільний інтерес.

Definitions and legal requirements for "high risk" artificial intelligence technologies

Tiuria Yu. I.
Candidate of Technical Sciences, Associate Professor,
Associate Professor at the Department of Civil, Economic and Environmental Law
Dnipro University of Technology
Dmytra Yavornytskoho ave., 19, Dnipro, Ukraine
orcid.org/0000-0001-7732-3535
Tyurya.J.I@nmu.one

Key words: *risks, criteria, «high-risk» artificial intelligence, legal requirements, human rights, remote biometric identification*.

Artificial intelligence quickly conquers all spheres of human activity. New technologies open up significant opportunities for accelerating research, creativity and organizing activities in all fields. At the same time, any even a small failure in the algorithm of work of artificial intelligence can lead to irreversible negative risks. Therefore, it should be understood that artificial intelligence has a number of advantages, but also its use is also accompanied by potential risks. All risks must be anticipated and minimized, which in turn requires the creation of a proper legal framework for the regulation of public relations regarding the use of artificial intelligence technologies.

Therefore, the purpose of this work was to identify «high-risk» technologies of artificial intelligence and establish legal requirements for them.

The work highlights the position of the European Commission on establishing criteria according to which artificial intelligence technology can be qualified as «high risk». The Commission proposes to apply a proportionate regulatory intervention to the use of artificial intelligence technologies on the basis of a risk assessment, taking into account the extent of the potential impact of these technologies during their lifecycle on human rights.

The article examines the mandatory legal requirements for «high-risk» technologies proposed by the European Commission for the purpose of targeted and proportionate regulatory intervention to the use of artificial intelligence technologies. It has been established that the main guidelines in determining requirements are the key components, characteristics, properties and functions of high-risk technologies. These include: databases, data accounting, information support, reliability and accuracy, human supervision. The use of artificial intelligence technologies for the purpose of remote biometric identification is only possible if such use is duly justified, proportionate, subject to adequate safeguards and represents a significant public interest.

Вступ. В наш час ми спостерігаємо тенденцію щодо безпрецедентного та масштабного зростання використання цифрових додатків як найважливіших інструментів повсякденного життя, включаючи комунікацію, охорону здоров'я, освіту, економічну діяльність, транспорт тощо. Поряд з цим зростає їх роль в запровадженні у структури управління, адміністрування та розподілі матеріальних й людських ресурсів. Нині ІТ-сфера має значний потенціал для суспільно корисних інновацій та економічного розвитку держави. Але найголовнішим витвором людського інтелекту стала розробка «штучного інтелекту» (англ. artificial intelligence).

Сьогодні практично всі економічно розвинені країни світу розглядають розвиток ІТ-сфери, зокрема технологій штучного інтелекту, як найважливішу стратегію підвищення національної конкурентоспроможності у світі та забезпечення національної безпеки.

За аналітичними даними Міжнародної корпорації даних (International Data Corporation (IDC)) дохід на світовому ринку від використання технологій штучного інтелекту, включаючи програмне забезпечення, обладнання та сервіси, у 2020 році підвищився на 12,3% у порівнянні з 2019-м та становив 156,5 млрд доларів, а у 2021 році повинен був збільшитися на 35,5 % [1].

Сучасні досягнення у сфері штучного інтелекту дозволяють нам звільнити людину від рутинної роботи, для якої не потрібно бути фахівцем та мати спеціальні знання, систематизувати інформацію, обробляти великі обсяги інформації, працювати

з великими базами даних та ін. Жодна людина не здатна так багато, швидко та точно отримувати, аналізувати та давати чіткий результат, як штучний інтелект. Якщо людина може помилятися в розрахунках, зважаючи на людський фактор, то штучний інтелект запрограмований на те, щоб у максимально короткі строки надати максимально правильне рішення. Сфери застосування технологій штучного інтелекту є необмеженими – від створення роботів, які самостійно приймають рішення, до машин із можливостями самонавчання. Важливу роль відіграє штучний інтелект у роботі підприємств. Він допомагає автоматизувати процеси, які потребують чималих зусиль, і тоді участь людини залишається мінімальною. Застосування технологій штучного інтелекту безперечно надає ряд переваг, зокрема: зменшення витрат, часу, ресурсів; швидкий аналіз великих обсягів даних; підвищення та покращення продуктивності діяльності; побудова точніших прогнозів в різних сферах життєдіяльності; можливість одночасного виконання багатьох задач та ін. [2, с. 185].

Однак ці технології несуть також і значні соціально-економічні, юридичні та етичні ризики, які необхідно передбачити та мінімізувати, що своєю чергою потребує створення належного правового поля для регламентації суспільних відносин щодо використання технологій штучного інтелекту.

Тим більше, що члени Європейського Союзу, починаючи з 2017 року, дуже активно проявляють власні ініціативи. До перших кроків глобального законодавчого врегулювання питання щодо штучного інтелекту можна віднести Резолюцію Європейського Парламенту «Норми цивільного права по робототехніці» 2015/2013 (INL) від 16 лютого 2017 року (European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103INL) [3]. Цей документ став орієнтиром та одним з перших реальних кроків на шляху до законодавчого закріплення відповідних обов'язкових стандартів розробки та використання штучного інтелекту, зокрема соціальних, етичних та правових.

Останнім часом штучний інтелект став предметом кількох європейських й міжнародних програмних документів та досліджень, внаслідок чого наразі виокремився, сформувався та закріпився такий напрям, відомий як «Європейський підхід до штучного інтелекту», що ґрунтується на засадах розширення дослідницького і промислового потенціалу європейських держав та забезпеченні захисту основних прав й інтересів людей. Підґрунтям запровадження такого підходу стала необхідність формування єдиної нормативно-правової бази щодо штучного інтелекту з урахуванням потенційних ризиків використання таких технологій.

Прагнучі поширення технологій штучного інтелекту, і водночас, зважаючи на ризики, пов'язані з їх використанням, Європейська Комісія запропонувала для публічного обговорення інформаційно-аналітичний документ під назвою «Біла книга зі штучного інтелекту: Європейський підхід до досконалості та довіри» (White Paper on Artificial Intelligence: a European approach to excellence and trust, далі – Біла книга) з варіантами політик та механізмів правового регулювання штучного інтелекту [4]. «Біла книга» демонструє ризикоорієнтований підхід Єврокомісії, який широко застосовується у корпоративному управлінні. Такий підхід забезпечує ефективніше регулювання штучного інтелекту без непропорційного втручання регулятора та обтяження бізнесу.

Метою статті є визначення «високоризикованих» технологій штучного інтелекту та встановлення правових вимог до них.

Виклад основного матеріалу. Технології штучного інтелекту дедалі стають центральною ланкою кожного аспекту життя людей, тому люди повинні довіряти їм, водночас обов'язковою умовою для їх сприйняття також є надійність. Враховуючи прагнення Європи до забезпечення людських цінностей та верховенства права, а також доведену нею здатність та можливість створювати безпечні, надійні та складні інформаційні продукти й послуги від аеронавтики до енергетики, автомобільного та медичного обладнання, Європейська Комісія вважає, що формування нормативної бази щодо штучного інтелекту повинно ґрунтуватися на оцінці ризику, гарантуючи пропорційне регуляторне втручання. Однак це вимагає розроблення чітких критеріїв для встановлення відмінностей між різними технологіями штучного інтелекту, зокрема виокремлення технологій з «високим ризиком» або «високоризикованих». Критерії мають бути чіткими, легко зрозумілими та застосовними для всіх зацікавлених сторін.

Європейська Комісія запропонувала два критерії, які вважає необхідними для врахування при визначенні певної технології штучного інтелекту як «високоризикована» (з високим ризиком, небезпечна).

По-перше, варто орієнтуватися на *спрямування та характерні особливості певної сфери діяльності*, що зазвичай здійснюється за допомогою технологій штучного інтелекту, від яких можливо очікувати значних ризиків. Отже, перший критерій повинен забезпечувати регуляторне втручання саме у ті сфери діяльності, де, загалом, потенційні ризики найбільш вірогідні. Такі сфери діяльності мають бути належно визначені та зазначені у нормативній базі щодо штучного інтелекту. Зокрема, сфера охорони здоров'я, транспорту, енергетики та окремих складових державного сектору (напри-

клад, служби захисту, міграційна служба, прикордонний контроль, судова система, соціальне забезпечення та служби зайнятості). Цей перелік слід періодично переглядати та за необхідністю корегувати, враховуючи зміни практичного застосування певної технології штучного інтелекту. Таким чином за умови застосування у певній сфері діяльності технології штучного інтелекту, яка завдає шкоди, її будуть визнавати як «високоризикована». Ця шкода може бути як матеріальною (безпека та здоров'я людей, включаючи втрату життя, пошкодження майна), так і нематеріальної (втрата приватного життя, обмеження права на свободу вираження поглядів, людської гідності, дискримінація, наприклад, у доступі до роботи).

По-друге, необхідно враховувати той факт, що використання технології штучного інтелекту у сфері діяльності, віднесеної до високоризикованої, не завжди супроводжується значним ризиком. Наприклад, не зважаючи на те, що сфера охорони здоров'я загалом може бути високоризикованою, недолік у системі планування прийомів лікарів зазвичай не створює ризиків такого рівня, які потребують законодавчого втручання. При визначенні рівня ризику використання певної технології штучного інтелекту доцільно ґрунтуватися на *оцінці рівня впливу цієї технології на осіб*, які постраждали в наслідок її застосування. Зокрема це стосується використання таких технологій штучного інтелекту, які здатні створювати ризик травмування, смерті або значної матеріальної чи нематеріальної шкоди, юридичні або серйозні наслідки щодо порушення прав окремої особи чи компанії та які не можна обґрунтовано уникнути.

Європейська Комісія наполягає на необхідності встановлення обов'язкових законодавчих вимог щодо штучного інтелекту, які будуть застосовуватися лише до таких технологій, що відповідно до наведених критеріїв, кваліфіковані як високоризиковані. Таким чином застосування цих двох кумулятивних критеріїв забезпечить цільову сферу дії нормативно-правової бази та правову визначеність.

Для гарантування цілеспрямованого та пропорційного регуляторного втручання щодо технологій штучного інтелекту запропоновано визначити обов'язкові правові вимоги відповідно до ключових складових, характеристик, властивостей та функцій технологій, які є високоризикованими. Передусім це стосується: бази даних, обліку даних, інформаційного забезпечення, надійності й точності, людського нагляду та окремих конкретних вимог до певних технологій штучного інтелекту (наприклад тих, що використовують для здійснення віддаленої біометричної ідентифікації).

Бази даних. Функціонування багатьох технологій штучного інтелекту, а також їхні дії та прийняті ними рішення суттєво залежать від набору даних, відповідно до яких вони розроблювалися, налаштовувалися та вміють самостійно навчатися. Тому варто вжити необхідних заходів та передбачити певні вимоги щодо забезпечення дотримання правил і цінностей Європейського Союзу, зокрема відносно безпеки та захисту основних прав й інтересів людей, що стосуються даних. Отже, дані, на яких навчається штучний інтелект, мають бути достатньо повними та репрезентативними, забезпечувати усі релевантні сценарії для запобігання небезпечним ситуаціям, гарантувати недискримінацію та захист приватності й особистих даних.

Облік даних. Беручи до уваги окремі характеристики функціонування значної кількості технологій штучного інтелекту, зокрема складність й непрозорість та пов'язані з цим труднощі, необхідно при програмуванні алгоритму роботи таких технологій запровадити правила та вимоги щодо ведення обліку даних, які використовуються для навчання штучного інтелекту з високим ризиком, а, у певних випадках, забезпечити збереження цих даних. Ці правила та вимоги дозволять протягом усього життєвого циклу штучного інтелекту відстежувати та перевіряти потенційно проблематичні його дії або прийнятті ним рішення.

З метою реалізації зазначеного нормативно-правова база повинна передбачати правила щодо зберігання, зокрема:

– точні записи набору даних, що використовуються для навчання та тестування штучного інтелекту, включаючи опис основних характеристик та способу відбору даних;

– набори даних за необхідністю;

– документація стосовно програмування (алгоритми та методи оптимізації тощо) та методології навчання, процесів і прийомів, що використовуються для створення, тестування та перевірки штучного інтелекту, враховуючи вимоги щодо забезпечення безпеки та уникнення упередженості, яка може призвести до забороненої дискримінації.

Записи, документацію та набори даних необхідно зберігати протягом доцільного проміжку часу, щоб забезпечити ефективне виконання відповідних вимог законодавства.

Інформаційне забезпечення. З метою сприяння та підтримки використання технологій штучного інтелекту, а також зміцнення довіри та забезпечення відшкодування збитків, якщо це необхідно, важливо, щоб інформація щодо використання технологій штучного інтелекту з високим ризиком була достеменною й адекватною та надавалась у проактивній формі. Тому необхідно забезпечити інформування користувачів про можливості й обмеження технологій штучного інтелекту у випадках, коли вони з ним взаємодіють. Водночас для уникнення обтяження бізнесу, у випадках, коли використання штуч-

ного інтелекту буде очевидним користувачам, таке інформування не буде необхідним.

Надійність і точність. Технології штучного інтелекту і, безумовно, технології з високим ризиком мають бути технічно надійними та точними, аби бути безпечними. Таким чином їх потрібно розробляти відповідально та з попередньою належною оцінкою ризиків, які вони можуть спричинити. З огляду на це з метою мінімізації ризиків заподіяння шкоди варто для цього передбачити та застосовувати всіх належних заходів, щоб технології штучного інтелекту працювали безпечно. Як підсумок, високоризикові технології штучного інтелекту повинні бути достатньо надійними, вірогідно вказувати рівень точності на всіх етапах життєвого циклу, бути стійкими до зовнішніх атак і маніпуляцій з даними та алгоритмами.

Людський нагляд. Людський нагляд за штучним інтелектом дозволяє гарантувати людині автономію, безпеку, захист та уникнення негативних наслідків. Мета щодо створення надійного, етичного та орієнтованого на людину штучного інтелекту може бути досягнута лише шляхом забезпечення належної участі людей на всіх етапах життєвого циклу штучного інтелекту з високим ризиком. Тому прийняття рішення штучним інтелектом повинно здійснюватися лише з його попередньою валідацією людиною (наприклад, заявка на соціальну допомогу може бути відхилена лише людиною) або наступним постконтролем (наприклад, розгляд та прийняття рішення щодо кредитної заявки здійснюється людиною).

Окремі застосування високоризикованих технологій штучного інтелекту за певних умов можуть потребувати постійного моніторингу з можливістю негайного втручання людини або передбаченого розробниками припинення функціювання такої технології (наприклад, використання автопілотованих авто без належної розмітки, або в умовах поганої видимості тощо).

Особливі вимоги щодо дистанційної (віддаленої) біометричної ідентифікації. Збір і використання біометричних даних для цілей віддаленої ідентифікації, наприклад, за допомогою розпізнавання облич у громадських місцях, зумовлює особливий ризик щодо порушення основних прав людини, зокрема права на повагу до гідності й приватного життя та захист персональних даних. Також існує потенційний вплив на недискримінацію та права певних груп людей, таких як діти, літні люди та люди з обмеженими можливостями. Крім того, використання зазначеної технології не повинно пригнічувати свободу вираження поглядів, право на свободу мирних зібрань і свободу об'єднання.

Відповідно до п. 13 ст. 3 Law Enforcement Directive [5], п. 18 ст. 3 Regulation (EU) 2018/1725 [6] та п. 14 ст. 4 GDPR (Загальний регламент про захист даних від 04.05.2016) надано визначення щодо біометричних даних, зокрема це «персональні дані, отримані в результаті спеціального технічного опрацювання, що стосується фізичних, фізіологічних чи поведінкових ознак фізичної особи, таких як, зображення обличчя чи дактилоскопічні дані (відбиток пальця), що дозволяють однозначно ідентифікувати або підтверджують однозначну ідентифікацію фізичної особи» [7].

Оскільки передбачено розпізнавання обличчя, то у випадку ідентифікації це значить, що шаблон зображення обличчя людини порівнюється з багатьма іншими шаблонами, які зберігаються в базі даних, з метою встановлення відповідності зображення обличчя певній особі. У випадку аутентифікації (або перевірки) здійснюється порівняння двох біометричних шаблонів, які зазвичай належать одній людині, тобто встановлюється відповідність один до одного. Два біометричні шаблони порівнюються, щоб визначити, чи є особа, представлена на двох зображеннях, однією і тією ж людиною. Така процедура, наприклад, передбачена програмно-технічним комплексом автоматизації прикордонного контролю (ПТК АПК) та модернізованою автоматизованою системою інтелектуального відеоконтролю, які використовуються для прикордонного контролю в аеропортах.

Наслідки використання технологій штучного інтелекту віддаленої біометричної ідентифікації залежно від мети, контексту та сфери використання можуть значно відрізнятися.

Правила Європейського Союзу щодо захисту персональних даних в принципі забороняють обробку біометричних даних з метою однозначної ідентифікації фізичної особи, за винятком певних умов. Зокрема, згідно з п. 2 ст. 9 GDPR, така обробка може здійснюватися на певних підставах, головна з яких – з причин суттєвого суспільного інтересу [8]. Будь-яка обробка біометричних даних з метою однозначної ідентифікації фізичної особи підпадає під дію ст. 3 та ст. 8 Хартії основних прав Європейського Союзу, зокрема права на особисту недоторканність та захисту інформації особистого характеру [9]. У цьому випадку обробка біометричних даних має відбуватися на основі законодавства Європейського Союзу та/або національного законодавства з дотриманням вимог пропорційності відповідно цілі, якої прагнуть досягти, поважати сутність права на захист даних і передбачати належні та спеціальні заходи для захисту фундаментальних прав та інтересів суб'єкта даних.

Враховуючи правила захисту даних Європейського Союзу та положення Хартії основоположних прав, Європейська комісія наголошує, що використовувати технології штучного інтелекту для цілей віддаленої біометричної ідентифікації можливо лише за умови, якщо таке використання

є обґрунтованим належним чином, пропорційним, підлягає відповідним гарантіям та становить значний суспільний інтерес (наприклад, якщо це критично необхідно для розшуку зниклої дитини, для запобігання конкретної та неминучої терористичної загрози або для виявлення та притягнення до відповідальності винного чи підозрюваного у серйозному кримінальному злочині). Подібне використання підлягає дозволу судового чи іншого незалежного органу та відповідних обмежень у часі, географічному охопленні та пошукових базах даних.

Беручи до уваги, що на різних етапах життєвого циклу штучного інтелекту, зокрема у процесі розробки, виготовлення, реалізації, користування та ін., залучено декілька груп зацікавлених осіб виникає необхідність у визначенні певного кола осіб, яким адресовані юридичні вимоги щодо використання технологій штучного інтелекту з високим ризиком. До таких осіб відносяться розробники, виробники, дистриб'ютори чи імпортери, постачальники послуг, фахівці та користувачі. Зважаючи на це, Європейська Комісія виділяє декілька проблемних питань, які потребують подальшого вирішення.

По-перше, необхідно передбачити розподіл зобов'язань між залученими суб'єктами господарювання. На думку Комісії, нормативно-правова база, визнаючи зобов'язання певного суб'єкта (ів), повинна орієнтуватися на наявність у них належних можливостей для подолання будь-яких потенційних ризиків. Наприклад, розробники штучного інтелекту, маючи відповідні ресурси, спроможні запобігти ризикам, які виникають на етапі розробки певної технології, проте їхні можливості щодо здійснення контролю за ризиками на етапі виробництва та використання технології штучного інтелекту обмежені. Таким чином, на етапі розробки технології штучного інтелекту відповідне зобов'язання за спричинення ризиків буде нести розробник. На етапі виробництва відповідно до ст. 1 Директиви Ради 85/374/ЄЕС "Про наближення законів, постанов та адміністративних положень держав-членів щодо відповідальності за неякісну продукцію" «виробник є відповідальним за збитки завдані недоліками його продукції» [10]. Згідно зі ст. 3 зазначеного документа терміном «виробник» визначено «виробника кінцевого продукту, будь-якої сировини чи будь-яких комплектуючих, а також будь-яку особу, що, позначаючи продукцію своїм ім'ям, товарним знаком чи іншою відмінною ознакою, заявляє про себе як виробника» [10]. Національне законодавство держав-учасниць Європейського Союзу також може передбачати окремі види стягнень за дефектну продукцію.

По-друге, потребує чіткого визначення питання щодо географічного охоплення законодавчого втручання. На думку Комісії, надзвичайно важливо, щоб юридичні вимоги застосовувалися до відповідних суб'єктів господарювання, які виробляють продукцію або надають послуги з використанням штучного інтелекту, на території Європейського Союзу, незалежно від того, чи зареєстровані вони в ЄС чи ні.

Передбачається, що за контроль щодо дотримання обов'язкових правових вимог відповідатимуть національні регулятори країн-членів Європейського Союзу. Крім цього, планується створення Європейської ради з питань штучного інтелекту (European Artificial Intelligence Board), яка пізніше представить більш детальні стандарти з розробки й експлуатації технологій штучного інтелекту та сприятиме їх впровадженню. На додаток пропонуються зацікавленим особам сформувати добровільні етичні кодекси поведінки щодо штучного інтелекту без високого ризику, а також відповідні для них нормативні вимоги з метою сприяння запровадженню та поширенню зазначених інновацій.

Запровадження єдиної європейської структури управління в галузі штучного інтелекту на основі співпраці національних компетентних органів дозволить уникнути фрагментації щодо визначення відповідальності та посилити й модернізувати наявний дослідницький і промисловий потенціал держав-членів Європейського Союзу.

Висновки. Оскільки штучний інтелект – це технології, що надзвичайно швидко розвиваються, встановлення та дотримання правових вимог до них, зокрема до «високоризикованих» технологій, сприятиме введенню в експлуатацію та потраплянню на ринок товарів і послуг лише безпечному та надійному штучному інтелекту. Необхідною умовою реалізації цього, є забезпечення протягом всього життєвого циклу штучного інтелекту постійного управління якістю та ризиками з боку всіх провайдерів. Запропоновані вимоги дозволять: своєчасно виключити та усунути потенційні ризики, створені штучним інтелектом; сформувати перелік програм/застосунків із високим ризиком; визначити конкретні зобов'язання для користувачів та провайдерів програм/застосунків штучного інтелекту з високим ризиком; сформувати структуру управління в галузі штучного інтелекту на європейському та національному рівнях.

Література

1. Ринок технологій штучного інтелекту цього року виросте до $156,5 млрд. URL: https://mind.ua/news/20214273-rinok-tehnologij-shtuchnogo-intelektu-cogo-roku-viroste-do-1565-mlrd (дата звернення: 21.02.2022).
2. Великанова М.М. Штучний інтелект: правові проблеми та ризики. *Вісник* Національної академії правових наук України. Харків, 2020. №4. С. 185-198. Doi: 10.37635/jnalsu.27(4).2020.185-198.
3. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017IP0051 (дата звернення: 03.03.2022).
4. White Paper on Artificial Intelligence A European approach to excellence and trust. URL: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (дата звернення: 17.03.2022).
5. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. URL: https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng (дата звернення: 13.05.2022).
6. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/reg/2018/1725/oj (дата звернення: 13.05.2022).
7. Article 4 GDPR. Definitions. URL: https://gdpr-text.com/uk/read/article-4/ (дата звернення: 13.05.2022).
8. Article 9 GDPR. Processing of special categories of personal data. URL: https://gdpr-text.com/uk/read/article-9/ (дата звернення: 13.05.2022).
9. Хартія основних прав Європейського Союзу: Міжнародний документ від 07.12.2000. URL: https://zakon.rada.gov.ua/laws/show/994_524#Text.
10. Директива Ради 85/374/ЄЕС "Про наближення законів, постанов та адміністративних положень держав-членів щодо відповідальності за неякісну продукцію": Міжнародний документ від 25.07.1985 № 85/374/ЄЕС. URL: https://zakon.rada.gov.ua/laws/show/994_348#Text.

References

1. Rynok tekhnolohiy shtuchnoho intelektu ts'oho roku vyroste do $156,5 mlrd. Retrieved from https://mind.ua/news/20214273-rinok-tehnologij-shtuchnogo-intelektu-cogo-roku-viroste-do-1565-mlrd [in Ukrainian]. (2022, February, 21).
2. Velykanova, M. (2020). Artificial intelligence: legal problems and risks. Journal of the National Academy of Legal Sciences of Ukraine, Vol. 27, No. 4, 185-198. [in English].
3. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017IP0051 [in English]. (2022, March, 03).
4. White Paper on Artificial Intelligence A European approach to excellence and trust. Retrieved from https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf [in English]. (2022, March, 17).
5. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. Retrieved from https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng [in English]. (2022, May, 13).
6. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance). Retrieved from https://eur-lex.europa.eu/eli/reg/2018/1725/oj [in English]. (2022, May, 13).
7. Article 4 GDPR. Definitions. Retrieved from https://gdpr-text.com/uk/read/article-4/ [in English]. (2022, May, 13).
8. Article 9 GDPR. Processing of special categories of personal data. Retrieved from https://gdpr-text.com/uk/read/article-9/ [in English]. (2022, May, 13).

9. Khartiya osnovnykh prav Yevropeys'koho Soyuzu (2000). *The official website of the Verkhovna Rada of Ukraine* [The official website of the Verkhovna Rada of Ukraine]. Retrieved from https://zakon.rada.gov.ua/laws/show/994_524#Text. [in Russian].
10. Dyrektyva Rady 85/374/YeES "Pro nablyzhennya zakoniv, postanov ta administratyvnykh polozhen' derzhav-chleniv shchodo vidpovidal'nosti za neyakisnu produktsiyu" (1985). *The official website of the Verkhovna Rada of Ukraine* [The official website of the Verkhovna Rada of Ukraine]. Retrieved from https://zakon.rada.gov.ua/laws/show/994_348#Text. [in Ukrainian].