УДК: 34:[004.8+004.383.8]
DOI https://doi.org/10.24144/2307-3322.2025.90.3.19

ДОСТУП ДО ДАНИХ ТА КОНФІДЕНЦІЙНІСТЬ В КОНТЕКСТІ ШТУЧНОГО ІНТЕЛЕКТУ

Бочкова І.І.,
кандидат юридичних наук,
старший викладач кафедри патентознавства
та основ правозастосовної діяльності
Харківського національного університету
міського господарства імені О.М. Бекетова
ORCID: 0000-0003-0522-2908
e-mail: inga.bochkova@gmail.com

Врублевська-Місюна К.М.,
кандидат юридичних наук,
доцент кафедри патентознавства
та основ правозастосовної діяльності
Харківського національного університету
міського господарства імені О.М. Бекетова
ORCID: 0000-0002-6973-3945
e-mail: vkatrin21@gmail.com

Бочкова І.І., Врублевська-Місюна К.М. Доступ до даних та конфіденційність в аспекті штучного інтелекту.

У сучасну епоху стрімкого розвитку технологій штучний інтелект (далі – ШІ) стає важливим інструментом, що трансформує численні сфери суспільного життя — від медицини й освіти до економіки й державного управління. Утім, разом із безпрецедентними можливостями ШІ виникають суттєві виклики, серед яких питання доступу до даних та забезпечення конфіденційності набувають особливої актуальності. ШІ залежить від великих обсягів даних для навчання, функціонування та вдосконалення, однак використання персональної інформації часто породжує ризики порушення приватності та зловживань.

Для розроблення правових механізмів попередження таких ризиків та мінімізації негативного впливу вважаємо важливим дослідити ключові аспекти доступу до даних і забезпечення конфіденційності в контексті застосування ШІ. З цією метою в статті аналізуються особливості правового режиму штучного інтелекту, розроблені і рекомендовані світовою та українською практикою технічні й організаційні інструменти та етичні підходи до балансування між ефективністю алгоритмів ШІ і захистом прав людини. Особлива увага надається дослідженню питання відповідності сучасних технологій вимогам законодавства про захист персональних даних, зокрема Загальному регламенту захисту даних (GDPR), а також вивчаються приклади конфліктів інтересів між потребою вільного обміну інформацією і дотриманням конфіденційності.

Проведене дослідження спрямоване на визначення викликів та перспектив регулювання доступу до даних у сфері ШІ, а також на розробку рекомендацій для забезпечення безпечного і прозорого використання цих технологій. Стаття містить огляд нормотворчої діяльності Уповноваженого Верховної Ради України з прав людини як наглядового органу за дотриманням розпорядниками інформації вимог законодавства щодо захисту персональних даних.

Також дослідження розкриває деякі практичні аспекти щодо застосування законодавчих вимог при поводженні з персональними даними: застосування проєктованої приватності, порядок ведення Реєстру обробки персональних даних, особливості впровадження ризико-орієнтованого підходу в компаніях, що є володільцями чи розпорядниками персональних даних.

Ключові слова: інформація, персональні дані, проєктована приватність, обмеження доступу до інформації, реєстр обробки персональних даних.

Bochkova I.I., Vrublevska-Misiuna K.M. Data access and confidentiality in the context of artificial intelligence.

In this era of rapid technological development, artificial intelligence (AI) is becoming an important tool that is transforming numerous areas of public life, from medicine and education to economics and public administration. However, along with the unprecedented opportunities offered by AI, significant challenges arise, among which issues of data access and confidentiality are particularly relevant. AI depends on large amounts of data for training, functioning, and improvement, but the use of personal information often poses risks of privacy violations and abuse.

In order to develop legal mechanisms to prevent such risks and minimize negative impacts, we believe it is important to examine key aspects of data access and privacy in the context of AI application. To this end, the article analyzes the peculiarities of the legal regime of artificial intelligence, technical and organizational tools developed and recommended by global and Ukrainian practice, and ethical approaches to balancing the effectiveness of AI algorithms and the protection of human rights. Particular attention is paid to researching the issue of compliance of modern technologies with the requirements of personal data protection legislation, in particular the General Data Protection Regulation (GDPR), as well as studying examples of conflicts of interest between the need for free exchange of information and compliance with confidentiality.

Thus, the study aims to identify the challenges and prospects for regulating access to data in the field of AI, as well as to develop recommendations for ensuring the safe and transparent use of these technologies. The article provides an overview of the regulatory activities of the Ukrainian Parliament Commissioner for Human Rights as the supervisory body for compliance by information managers with the requirements of personal data protection legislation.

The study also reveals some practical aspects of the application of legislative requirements when handling personal data: the application of privacy by design, the procedure for maintaining the Record of Processing Activities, and the specifics of implementing a risk-based approach in companies that are owners or controllers of personal data.

Key words: information, personal data, privacy by design, restrictions on access to information, Record of Processing Activities.

Постановка проблеми. Шлях законодавчого закріплення правового режиму ШІ в українському законодавстві тільки розпочався. Україна у жовтні 2019 року приєдналася до Рекомендацій Організації економічного співробітництва і розвитку з питань штучного інтелекту (OECD/LEGAL/0449). Після цього Розпорядженням КМУ від 02.12.2020 № 1556-р. була схвалена Концепція розвитку штучного інтелекту в Україні, яка окреслила основні аспекти, що стосуються ШІ, зокрема і закріпила дефініцію. [1] Чи не єдиним офіційним вираженням позиції національного законодавця щодо правового режиму ШІ стала норма статті 33 ЗУ «Про авторське право та суміжні права» від 01.12.2022 № 2811-IX, щодо прав особливого роду (sui generis) на неоригінальні об'єкти, згенеровані комп'ютерною програмою. [2] Робота з визначення режиму ШІ триває на підзаконному рівні в консультативних та рекомендаційних актах міністерств та відомств. Так, нещодавно, було оприлюднено Білу книгу штучного інтелекту (Мінцифри, червень 2024) [3], Рекомендації щодо відповідального використання ШІ: питання права інтелектуальної власності (Міністерство економіки, листопад 2024) [4], Права людини в епоху штучного інтелекту: виклики та правове регулювання (2024, Міністерство цифрової трансформації України при взаємодії з Офісом Омбудсмана) [5].

Отже наразі акценти в розробках правової регламентації використання ШІ зміщуються на такі два аспекти – захист прав інтелектуальної власності і захист прав суб'єктів персональних даних. В цьому дослідженні зупинимось більш детально на використанні ШІ в контексті захисту персональних даних людини.

Стан опрацювання проблематики. У контексті цифрової трансформації та впровадження ШІ в різні сфери життя наукова спільнота України все активніше досліджує питання правового регулювання, етики, захисту персональних даних та інформаційної безпеки. Зазначені питання розглядаються в працях М.В. Бєлової, Д.М. Бєлова, О.А. Дзюбенка, І.О. Кальченко, Т.В. Кучерявенка, В.П. Пєтухової, А.І. Савченка та інших. Однак аналізу практичних аспектів запровадження визначених законодавством організаційних і технічних заходів в діяльність компаній, що використовують ШІ під час обробки даних, детальної уваги не приділялось, що дає можливість провести дослідження в цьому напрямі.

Мета статті полягає у виробленні підходу для практичного втілення організаційних і технічних заходів в діяльність компаній, що використовують ШІ для обробки конфіденційної інформації та персональних даних, заснованого на аналізі правових актів нормативного і рекомендаційного характеру органів державної влади та міжнародних організацій.

Виклад основного матеріалу. Поняття даних не є правовим – це категорія, що використовується в математичних, статистичних, інформаційних галузях знань. Так, найпоширеніший підхід до розуміння даних в навчальних виданнях з інформатики зводиться до того, що дані – це деякі знаки або сигнали, які можуть бути передані, оброблені і зафіксовані на певному носії. [6, с. 3] Сукупність даних, що несуть в собі певний зміст можемо розглядати як інформацію. З точки зору законодавства, під інформацією розуміємо будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді; (ст.1 Закону України «Про інформацію»). Основним напрямом державної політики в сфері інформації є забезпечення доступу кожного до інформації. [7]

Підхід законодавця до розуміння доступу викладено у ЗУ «Про доступ до публічної інформації». З аналізу статті 10 цього закону вбачається, що під доступом розуміється будь-яка дія зацікавленого суб'єкта, пов'язана з правом 1) знати у період збирання інформації, але до початку її використання, які відомості та з якою метою збираються, як, ким і з якою метою вони використовуються, передаються чи поширюються, крім випадків, встановлених законом; 2) доступу до інформації, яка збирається та зберігається; 3) вимагати виправлення неточної, неповної, застарілої інформації, знищення інформації, збирання, використання чи зберігання якої здійснюється з порушенням вимог закону; 4) на ознайомлення за рішенням суду з інформацією про інших осіб, якщо це необхідно для реалізації та захисту прав та законних інтересів; 5) на відшкодування шкоди у разі розкриття інформації з порушенням вимог, визначених законом. [8]

Особливого аспекту поняття доступу набуває в залежності від виду інформації, відповідно і обсяг обмежень у наданні доступу до інформації буде змінюватися в залежності від її виду, мети, однак, в будь якому разі, забезпечення впровадження і дотримання таких обмежень, перш за все, має ґрунтуватися на організаційних і технічних засадах умов розміщення/оприлюднення інформації, і, вже в другу чергу, – на покладенні обов'язку на користувачів використовувати таку інформацію відповідно до обмежень. Саме в такому ракурсі варто розглядати особливості використання інформації ШІ, який не наділений розумом і усвідомленням наслідків своєї діяльності, але який, через розширені технічні характеристики (швидкість обробки, обсяг інформації, яким він оперує), використовує інформацію різних видів. Такі обмеження передусім мають стосуватися володільців (особа, яка визначає мету обробки персональних даних, встановлює склад та процедури їх обробки) чи розпорядників (особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця) інформації. Так, відповідно до Закону України «Про захист персональних даних» встановлено, що обсяг інформації про особу, що збирається, зберігається і використовується розпорядниками інформації, має бути максимально обмеженим і використовуватися лише з метою та у спосіб, визначений законом. Розпорядники інформації, які володіють інформацією про особу, зобов'язані: 1) надавати її безперешкодно і безкоштовно на вимогу осіб, яких вона стосується, крім випадків, передбачених законом; 2) використовувати її лише з метою та у спосіб, визначений законом; 3) вживати заходів щодо унеможливлення несанкціонованого доступу до неї інших осіб; 4) виправляти неточну та застарілу інформацію про особу самостійно або на вимогу осіб, яких вона стосується. При цьому регламентуються часові обмеження зберігання інформації, визначені метою збору та передбачається право на оскарження відмови в доступі до інформації про особу, приховування, незаконне збирання, використання, зберігання чи поширення інформації. [9]

Таким чином, в контексті доступу передбачається, що особа, чиї персональні дані обробляються, має право звернутися до володільців чи розпорядників інформації з відповідним запитом в межах обов'язків розпорядників. У зв'язку з цим і, керуючись вимогами п.1 ст. 30 (GDPR) *«Кожний контролер і, за необхідності, представник контролера повинні вести запис опрацювання даних, що належать до його сфери відповідальності.»*, постає питання про використання першого елементу механізму забезпечення правомірного використання персональних даних, пов'язаних з наданням доступу до даних і попередженням порушень з боку інших осіб, це обов'язок вести Реєстр обробки персональних даних. [10]

Record of Processing Activities (RoPA), або реєстр обробки персональних даних – це таблиця, яка містить інформацію про обробку всіх ПД, що відбуваються в компанії, інформацію про особу та контактні дані контролера та, за необхідності, об'єднаного контролера, представника контролера та співробітника з питань захисту даних; цілі обробки; опис категорій суб'єктів даних і категорій персональних даних; категорії одержувачів, яким персональні дані були або будуть розкриті, в тому числі одержувачі в третіх країнах або міжнародні організації; за необхідності, передавання персональних даних третій країні або міжнародній організації, в тому числі, ідентифікацію такої третьої країни чи міжнародної організації; за можливості, – передбачені часові обмеження для стирання різних категорій даних; за можливості, – загальний опис технічних і організаційних заходів безпеки. В Регламенті передбачено, що зазначений Реєстр можна не вести, якщо: на підприємствах з кількістю працівників, меншою за 250 осіб, за винятком, якщо здійснюване опрацювання може призвести до виникнення ризику для прав і свобод суб'єктів даних, призначене для окремого випадку, або якщо опрацювання передбачає спеціальні категорії даних (чутливі дані)), або персональні дані про судимості і кримінальні злочини. [10]

Отже, другий елемент механізму охоплює обов'язок володільців/розпорядників даних застосовувати ризико-орієнтований підхід, який полягає в тому, що за наявності певних обставин розпорядник має оцінювати ризики шляхом складання відповідного акту про оцінку ризиків від певної операції. Перелік високоризикованих процесів може встанавлюватися країною, тому треба звертатися до офіційної інформації наглядових органів.

У ст. 9 Закону України «Про захист персональних даних» передбачено обов'язок володільця персональних даних повідомляти Уповноваженого ВРУ з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, упродовж тридцяти робочих днів з дня початку такої обробки. Види обробки таких «ризикових» персональних даних та категорії суб'єктів, на яких поширюється вимога щодо повідомлення, визначаються Уповноваженим, який і є тим самим наглядовим органом в розумінні GDPR, до обов'язків якого в порядку ст. 22 ЗУ «Про захист персональних даних» належить контроль за додержанням законодавства про захист персональних даних. [9]

Відповідно Уповноважений є особою, яка, крім іншого є нормотворчим суб'єктом в сфері захисту персональних даних. Так, 8 грудня 2014 року Уповноваженим було видано Роз'яснення основних положень Порядку повідомлення Уповноваженого щодо визначення обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних (джерело) (далі – Порядок), відповідно до якого основним критерієм ризиковості є категорії персональних даних, що обробляються. До таких категорій персональних даних віднесено відомості про расове, етнічне та національне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та або організаціях, професійних спілках, релігійних організаціях чи в громадських організаціях світоглядної спрямованості, стан здоров'я, статеве життя, біометричні дані, генетичні дані, місцеперебування та або шляхи пересування особи, факт притягнення до адміністративної чи кримінальної відповідальності, застосування щодо особи заходів в рамках досудового розслідування та заходів, передбачених Законом України «Про оперативно-розшукову діяльність», вчинення щодо особи тих чи інших видів насильства. При цьому Уповноваженим надається роз'яснення, що «ризиковою» є інформація, передбачена вище, а також персональні дані про осіб, що належать до категорій, передбачених вище, наприклад, персональні дані особи, що притягається до кримінальної відповідальності, будуть «ризиковими». [11]

Зазначеним Порядком визначено особливості здійснення повідомлення Уповноваженого і розкрито зміст такого повідомлення. Особливої уваги, з нашої точки зору, для мети цього дослідження становить інформація про загальний опис технічних та організаційних заходів, що вживаються володільцем з метою забезпечення захисту персональних даних, які належать до категорій «ризиковості». Серед запропонованих заходів захисту один вид заходів стосується фізичної організації роботи з персональними даними (обладнання приміщення, створення і зберігання картотек, надання допусків певних категоріям працівників тощо), а інший – кіберзаходам, які, на нашу думку, набувають окремого змісту з огляду на можливості ШІ. В Порядку Уповноважений пропонує звернути увагу на те, чи приєднані комп'ютери, на яких здійснюється обробка персональних даних, до мережі та чи встановлено антивірусне та інше програмне забезпечення. На наш погляд ці вимоги мають набути більш широкого і глибокого наповнення. Вбачається, що загрози вільного використання комп'ютерними програмами на базі ШІ персональних даних криється саме в

ігноруванні або недостатньому розробленні зазначених технічних і організаційних заходів. Так, програми з ШІ отримують інформацію з мережі. Першою, на нашу думку, технічно-організаційною умовою з недопущення отримання програмою таких даних, є не завантаження їх в сервіси, до яких технічно можуть отримати доступ сторонній суб'єкт чи комп'ютерна програма (наприклад спільні хмарні сервіси, внутрішня пам'ять комп'ютера, під'єднаного до мережі). В цьому випадку краще зберігати інформацію виключно на сторонніх носіях і обробляти її на пристрої, не під'єднаному до мережі.

Таким чином третім елементом механізму забезпечення захисту прав суб'єктів персональних даних в контексті використання ШІ є застосування технічних та організаційних заходів. Ведучи мову про організаційні і технічні заходи треба звернути увагу на концепцію проєктованої приватності (або «приватності за задумом»), зміст якої полягає в розумінні і реалізації завчасного вбудовування механізмів, пов'язаних з реалізацією процедур безпеки персональних даних, до робочих процесів (сайтів, процедур збирання даних, створення картотек, створення комп'ютерних програм тощо). Термін «проєктована приватність» був впроваджений канадською фахівчинею в сфері захисту даних Енн Кавукян і полягає у необхідності консультування з фахівцями у сфері приватності на початкових етапах розроблення проєкту, а також інформування всіх спеціалістів проєкту про необхідність захисту персональних даних і надання їм мінімальних знань щодо поняття песрональних даних, мети та принципів їх обробки, прав суб'єктів персональних даних на їх виправлення, доступу до них, їх знищення тощо. [12] В контексті штучного інтелекту розробники програм, що використовують ШІ, повинні працювати в тісному взаємозв'язку з фахівцями в сфері безпеки даних на кожному етапі розробки програми, щоб вчасно інтегрувати механізми цензури. На момент видання роботи Ен Кавукян законодавчого закріплення вимоги проєктованої приватності не існувало, однак вже у 2018 році в Європі з'являється GDPR у ст. 25 якого передбачено обов'язок контролера у момент визначення засобів для опрацювання персональних даних вжити необхідних технічних і організаційних умов для реалізації принципу мінімізації даних, забезпечення захисту прав і свобод суб'єктів даних, а також для того, щоб за замовчуванням забезпечити опрацювання даних тільки для заявлених цілей. Тобто міститься вимога прогнозування можливих ризиків під час опрацювання даних осіб. Прогнозування ризиків знаходить своє втілення у стратегічному підході, що охоплює три основні етапи: 1) розуміння можливих порушень приватності; 2) оцінка ризиків таких порушень – прогнозування порушень з метою їх недопущення; 3) використання стратегій і тактик з недопущення порушені і мінімізації їх наслідків.

Для розкриття першого етапу має бути розроблена певна класифікація можливих порушень приватності, яка має охоплювати і порушення, які можливі через використання штучного інтелекту. За основу розробки такої класифікації можна взяти відому таксономію приватності Деніела Дж. Соула, який виділяє чотири прояви порушень приватності: ті, що допускаються під час збирання інформації (безпідставне стеження за поведінкою особи (зокрема – машинне навчання щодо розпізнавання обличь, знятих на камерах відеоспостереження у публічних місцях), примусове отримання інформації (наприклад, в якості виконання приписів органів влади, виконання наказу роботодавця працівником та інші прояви юридичної нерівності статусів осіб)), ті, що допускаються під час її оброблення (агрегація – об'єднання різних наборів даних для створення докладного профілю, ідентифікація – зіставлення даних для встановлення особи, другорядне використання – використання даних у цілях, для яких вони не збиралися, неправильне використання – зловживання або неналежне використання інформації, невірна атрибуція – поширення неправдивих або помилкових даних); ті, що допускаються під час поширення інформації (розкриття – публікація приватної інформації, експлуатація – використання особистої інформації для вигоди інших, порушення конфіденційності – злом або розголошення даних, які очікувалися залишитися конфіденційними) та ті, що передбачають втручання в приватне життя (нав'язливий інтерес до особистих справ людини). [13] Насправді, кожне з цих порушень, виділених Соулом, набуває більшої ймовірності допущення через використання ШІ. Можливості комп'ютерних програм генерувати відео, на якому людина вимовляє згенерований текст, в одному результаті містить прояви майже всіх запропонованих порушень, якщо усі вихідні дані (голос, зображення людини, її рухи, тло відео тощо) – отримані без добровільної поінформованої згоди суб'єкта даних, наприклад, запозичено з соціальної мережі.

На другому етапі передбачається обов'язок розпорядників розробити локальний акт – загальну модель оцінки ризиків, якою варто передбачити: коло осіб у ризику (партнери, співробітники, ко-

ристувачі), коло суб'єктів, що несуть загрозу (розпорядники, володільці, їх партнери-особи, яким передають інформацію), коло відносин між суб'єктами осіб у групі ризиків з суб'єктами погроз (щоб виключити можливість примусової передачі даних за наявності дисбалансу влади у відносинах між суб'єктом даних та розпорядником), фактори оцінки ризиків. До факторів оцінки ризиків у GDPR віднесено два – вірогідність та серйозність. На підставі цих факторів процеси, пов'язані з обробкою даних поділяють на певні види, які і вимагають застосування певних додаткових превентивних заходів, або є критерієм заборони здійснення певних процесів, наприклад, використання відповідної програми з ШІ. Відповідно до Регламенту обов'язковість проведення оцінки ризиків передбачена у випадках: 1) систематичного масштабного оцінювання персональних аспектів людини, яке ґрунтується на автоматизованій обробці; 2) масштабної обробки чутливих даних або даних про суд чи злочини; 3) систематичного та масштабного моніторингу публічних місць. На нашу думку, за умов стрімкого поширення використання ШІ, до цього переліку треба віднести і четвертий випадок – використання програм з вбудованим ШІ для аналізу персональних даних. У цих випадках має бути застосований ризико-орієнтований підхід.

В акті Уповноваженого «Права людини в епоху штучного інтелекту» зазначена класифікація, що передбачає поділ систем, що працюють зі ШІ, на чотири види: системи ШІ з мінімальним ризиком або неризикові (ШІ використовується як інструмент для виконання рутинних завдань, результати процесів не впливають на права осіб, допомагають пришвидшити підготовчі дії); системи ШІ з обмеженим ризиком (суб'єкти, що приймають рішення, використовують ШІ, але контролюють свої запити і в будь-який момент можуть відмовитись від результатів запиту і прийняти рішення самостійно); системи ШІ з високим ступенем ризику (певний процес повністю здійснюється комп'ютерною програмою на основі ШІ – відбувається автоматизоване прийняття рішення, що безпосередньо впливає на права суб'єктів даних. В цьому випадку системи ШІ повинні відповідати обов'язковим вимогам й пройти процедури оцінювання відповідності, а на постачальників і користувачів цих систем покладаються чіткі зобов'язання); заборонені системи ШІ (технології, які можуть становити загрозу для людини або суспільства загалом: переслідування, маніпулювання, введення пропаганди, або застосування їх проти вразливих соціальних груп). [5,с. 15]

З точки зору тлумачення положень GDPR важливо мати хоч якусь модель ризиків, яка не буде суб'єктивна, а буде об'єктизована в певну формулу. Маючі формулу володільці/розпорядники даних зможуть порахувати реальні затрати для вжиття превентивних заходів або для усунення порушень.

На третьому етапі має відбутися вбудовування стратегій до діяльності володільців/розпорядників персональних даних. Ці стратегії можуть стосуватися як організації процесу обробки так і її технічної сторони: шифрування даних, таким чином, щоб у випадку використання даних сторонніми особами чи програмами, зокрема і ШІ, дані були просто інформацією, яка не стосується якоїсь конкретної людини (людина не ідентифікована, а отже це не персональні дані). Способи шифрування можуть передбачати: симетричне та асиметричне шифрування, гібридні криптографічні методи, шифрування на рівні диска, файлів, в базах даних, гешування, End-to-End Encryption (E2EE), технології безпечного зберігання ключів, обмеження доступу тощо

Щодо організаційних заходів, то мова йде зокрема й про примусове обмеження технічних можливостей комп'ютерних програм, впровадження цензури на пошук конкретного виду інформації або виконання певного завдання за запитом користувача. На наш погляд, оскільки ШІ працює на підставі машинного навчання, що передбачає надання програмі великого обсягу інформації з відкритих джерел у ЗМІ, навчання відбувається за завданням особи, що навчає. Таким чином, однією з можливих пропозицій буде заборона, або тимчасова заборона, навчати програми для аналізу ПД (розпізнавання облич, голосу, маніпуляції з паспортними даними чи іншою інформацією про особу). Так з аналізу політики приватності OpenAI, який створив Chat GPT виходить, що розробники ChatGPT (OpenAI) впровадили різні заходи для забезпечення відповідності вимогам захисту персональних даних, які стосуються дотримання вимог: мінімізації збору даних (OpenAI не збирає більше інформації, ніж необхідно для роботи моделі, зокрема під час взаємодії з користувачами не збираються чутливі персональні дані), анонімізації даних (зібрані дані підлягають анонімізації та агрегації, щоб запобігти можливості ідентифікації конкретних осіб), безпеки даних (дані користувачів захищені шифруванням під час передачі та зберігання), політики конфіденційності (в доступі користувачів перебуває детальна політика конфіденційності, що розкриває всі аспекти обробки персональних даних), видалення даних (користувачі мають право на запит про видалення своїх даних, що відповідає вимогам GDPR і аналогічних нормативних актів (тестування та

аудит (Системи ChatGPT підлягають регулярному тестуванню на відповідність вимогам захисту даних та безпеки), навчання моделі (для тренування моделей використовуються великі набори даних із публічно доступних джерел, проте OpenAI запобігає інтеграції персональних даних, якщо вони ідентифікуються в таких джерелах). [14]

Висновки: Підбиваючи підсумки дослідження питання конфіденційності в контексті штучного інтелекту зазначимо, що основні вимоги до поводження і захисту прав суб'єктів персональних даних, викладені в українському і європейському законодавстві, залишаються визначальними під час користування комп'ютерними програмами на базі штучного інтелекту. ШІ з огляду на свої безпрецедентні можливості щодо обсягу даних, якими він здатний оперувати, і швидкості обробки, ставить під загрозу можливість забезпечення безпеки даних після їх поширення чи вільного оприлюднення. Через це важливо особливо ретельно дотримуватись вимог механізму забезпечення правомірного використання персональних даних, що полягає в поєднанні запровадження ризико-орієнтованого підходу до аналізу процесів, що розпочинаються, прогнозованої приватності та використанні науково-обумовлених максимально ефективних технічних та організаційних заходів під час обробки персональних даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Концепція розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. / Верховна Рада України. URL : https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення 11.06.2025).
2. Про авторське право і суміжні права: Закон України від 01.12.2022 № 2811-IX / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2811-20#n855 (дата звернення 11.06.2025).
3. Біла книга з регулювання штучного інтелекту в Україні: бачення Мінцифри. Версія для консультацій, 2024 р / Міністерство цифрової трансформації України. URL: https://thedigital.gov.ua/storage/uploads/files/page/community/docs/%D0%A0%D0%B5%D0%B3%D1%83%D0%BB%D1%8E%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F%20%D0%A8%D0%86.pdf (дата звернення 11.06.2025).
4. Рекомендації щодо відповідального використання ШІ: питання права інтелектуальної власності. Управління інтелектуальної власності та інновацій. / Міністерство економіки України, листопад 2024 р. URL: https://me.gov.ua/Documents/Detail?lang=uk-UA&id=bd21c45a-a984-456e-b523-c03aa942dcb9&title=RekomendatsiiSchodoVidpovidalnogoVikoristanniaShi-PitanniaPravaIntelektualnoiVlasnosti (дата звернення 10.06.2025).
5. Права людини в епоху штучного інтелекту: виклики та правове регулювання. Міністерство цифрової трансформації України при взаємодії з Офісом Омбудсмана. Київ, 2024 р. URL: https://ombudsman.gov.ua/storage/app/media/uploaded-filesA3_compressed.pdf (дата звернення 11.06.2025).
6. Семйон І.В., Чупов С.В., Брила А.Ю., Апшай Н.І. Основи інформатики. Методичні матеріали з організації самостійної роботи для студентів математичного факультету з дисципліни "програмування" / Державний вищий навчальний заклад "Ужгородський національний університет": Ужгород, 2010. 41. URL: chttps://dspace.uzhnu.edu.ua/jspui/bitstream/lib/2994/1/%D0%9E%D1%81%D0%BD%D0%BE%D0%B2%D0%B8%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B8.pdf (дата звернення 10.06.2025).
7. Про інформацію: Закон України від 02.10.1992 № 2657-XII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення 10.06.2025).
8. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення 11.12.2024)
9. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2297-17#n170 (дата звернення 10.06.2025).
10. Загальний Регламент Європейського Парламенту і Ради ЄС 2016/679 «Про захист даних» від 27.04.2016 р. URL: kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf (дата звернення 10.06.2025).

11. Роз'яснення основних положень Порядку повідомлення Уповноваженого щодо визначення обробки персональних даних, яка становить особливий ризик для прав і свобод: Роз'яснення Уповноваженого ВР з прав людини від 08.01.2014 / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/n0003715-14#Text (дата звернення 05.06.2025).
12. Конфіденційність за задумом у законодавстві, політиці та практиці. Біла книга для регуляторів, осіб, які приймають рішення, та політиків. Ен Кавукян. Онтаріо, Канада, 2011 р. URL: https://web.archive.org/web/20181123150913/ http://www.ontla.on.ca/library/repository/mon/25008/312239.pdf (дата звернення 05.06.2025)
13. Daniel J. Solove A Taxonomy of Privacy. Penn Carey Law Journals. University of Pennsylvania/ Vol. 154 (2005-2006). Iss. 3 (2006) https://scholarship.law.upenn.edu/penn_law_review/vol154/iss3/1/ (дата звернення 05.06.2025).
14. Політика конфіденційності Open AI. Open AI. URL: https://openai.com/policies/privacy-policy/ (дата звернення 05.06.2025)