УДК 342.7:004.8
DOI https://doi.org/10.24144/2307-3322.2024.85.3.7

# ШТУЧНИЙ ІНТЕЛЕКТ ТА ПЕРСОНАЛЬНІ ДАНІ: ЗАХИСТ ПРИВАТНОСТІ В ЦИФРОВОМУ СЕРЕДОВИЩІ[1]

**Остіян Є.З.,**
*студентка 4 курсу юридичного факультету*
*ДВНЗ «Ужгородський національний університет»*
*ORCID: 0009-0007-4166-7177*
*e-mail: evgost0112@gmail.com*

**Остіян Є.З. Штучний інтелект та персональні дані: захист приватності в цифровому середовищі.**

Стаття робить акцент на актуальних ризиках, пов'язаних з використанням штучним інтелектом (ШІ) персональних даних (ПД), зокрема у контексті порушення права на конфіденційність та приватність фізичних осіб. Було виявлено та опрацьовано конкретні сфери обробки штучним інтелектом даних, а також те, як сучасні тенденції та загрози для захисту даних такої обробки впливають на розвиток стійкої й ефективної нормативно-правової бази з регулювання подібних технологій.

Через аналіз шляху до цифрової трансформації України та конкретних випадків порушень захисту права на конфіденційність за допомоги штучного інтелекту у світі, несанкціонованого доступу до них та відсутності достатньої превентивної діяльності, спрямованої на захист інформації, встановлено негативний вплив на інформаційну безпеку та економічну стабільність. Попри це на онлайн-платформах виділено тенденцію щодо позначення контенту, створеного за допомоги штучного інтелекту.

Приділено увагу заглибленню у юридичну природу штучного інтелекту, до якого через комплексність даних, які він використовує, має застосовуватися міжгалузевий підхід правових механізмів та технологічних і правових інструментів регулювання. Окрім цього, штучний інтелект визначається як каталізатор для оновлення багатьох правових режимів, зокрема в полі інформаційної безпеки, захисту персональних даних і конфіденційності особи.

З огляду на це, розглянуто основні недоліки національного законодавства про захист ПД, проаналізовано національну стратегію з регулювання штучного інтелекту та запропоновано шляхи вирішення ключових проблем в даних полях. Окремим пунктом було зауважено на законопроєктах про захист персональних даних в Україні і на тому, як вони враховують європейські стандарти із захисту даних в умовах розвитку штучного інтелекту. Також для порівняння наведено стратегії розвитку штучного інтелекту через призму міжнародного досвіду, опрацьовано європейське законодавство про захист даних (Загальний регламент про захист даних) та Акт ЄС про ШІ з метою виявлення основних моментів їх взаємозв'язку.

**Ключові слова:** штучний інтелект, GDPR, персональні дані, криза згоди, соціальні мережі, економіка даних.

**Ostiian Y.Z. Artificial intelligence and personal data: privacy protection in the digital environment.**

This paper focuses on the current risks associated with the use of artificial intelligence (AI) in processing personal data (PD), particularly about individuals' privacy and confidentiality rights. The paper identifies and examines specific areas of artificial intelligence data processing and discusses how modern trends and threats to data protection impact the development of a robust regulatory framework for managing such technologies.

[1] Науковий керівник: Пішта Вадим Іванович, доцент кафедри адміністративного, фінансового та інформаційного права ДВНЗ «Ужгородський національний університет», доктор філософії.

The analysis of Ukraine's digital transformation journey and specific cases of privacy rights violations through artificial intelligence globally has highlighted unauthorized access to data and insufficient preventive measures for information protection. These issues have been found to harm information security and economic stability. Despite this, there has been a notable trend on online platforms to label content created with the assistance of artificial intelligence.

The paper delves into the legal nature of artificial intelligence and the need for an interdisciplinary approach involving both legal mechanisms and technological tools due to the complexity of the data it uses. Furthermore, artificial intelligence is shown to play a crucial role in updating legal regimes, particularly in information security, personal data protection, and individual privacy.

Given this, the main shortcomings of the national legislation on the protection of PD have been considered. The national strategy for regulating artificial intelligence has been analyzed, and ways of solving key problems in these fields have been proposed. A separate point was noted in the draft laws on protecting personal data in Ukraine and how they align with European data protection standards in the context of developing artificial intelligence. Also, for comparison, strategies for developing artificial intelligence through the prism of international experience are presented, and European legislation on data protection (General Data Protection Regulation) and the EU Act on AI are processed to identify the main points of their relationship**.**

**Key words**. Artificial intelligence, GDPR, personal data, crisis of consent, social networks, data economy.

**Актуальність теми дослідження.** Згідно з Постановою КМУ від 30 квітня 2024 № 476 «Про затвердження переліку пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 31 грудня року, наступного після припинення або скасування воєнного стану в Україні року» системи штучного інтелекту, глибоке навчання, великі дані (big data) та нейроподібні мережі є актуальними до опрацювання зокрема у правовій доктрині, оскільки штучний інтелект в епоху цифровізації людства створює нові виклики для безпеки в кіберпросторі, одні з яких створюють загрозу витоків великих наборів персональних даних, зловживання ними та несанкціонованого доступу до них.

У доповіді Уповноваженого за 2023 рік резюмується, що законодавство про захист персональних даних потребує оновлення у зв'язку зі стрімким технологічним розвитком і використанням технологій штучного інтелекту. Застосування цих сучасних технологій у різних сферах створює необхідність у чіткому правовому регулюванні для забезпечення захисту прав і свобод людини, що в сукупності робить тему актуальною для досліджень у юридичній науці.

**Аналіз останніх досліджень та публікацій.** Використання персональних даних штучним інтелектом та можливих правових наслідків, пов'язаних з такою обробкою, досліджувалося такими вітчизняними вченими, як Пунда О.О., Арзянцева Д.А., Резворович К.Р., Береда М.В., Базалицький В.І., Бєлова М.В., Бєлов Д.М. Зокрема питання про правосуб'єктність ШІ підіймалося у працях наступних науковців: Каткова Т.Г., Зозуляк О.І., Жорнокуй Ю.М., Щербина Б.С., Ткаченко В.В.

Суттєву увагу науковою спільнотою приділено використанню ШІ в медицині, так як персональні дані обробляються в даній галузі за допомоги цього інноваційного продукту у великій кількості та з різною метою, що веде до актуалізації захисту приватності пацієнтів та/або користувачів технології. Також у сферах біоінформатики та медицини проведено деякі дослідження для вирішення юридичних та етичних проблем шляхом анонімізації даних за допомоги шифрування, деідентифікації записів, які складаються з персональних даних (псевдонімізація). Певною мірою ці рішення обмежували витік даних, але з іншого боку погано працювали під час завдань аналізу та дослідження.

**Мета статті** полягає у визначенні правових проблем та ризиків використання штучного інтелекту у процесі обробки персональних даних та наданні пропозицій щодо шляхів покращення законодавства на основі міжнародного досвіду.

**Виклад основного матеріалу.** Штучний інтелект в епоху цифровізації людства широко впроваджується всюди: від побуду, користувацького досвіду в мережі Інтернет й електронної комерції до забезпечення правопорядку, правосуддя, оборонної сфери та навіть дипломатії. Новації створюють нові можливості та виклики для безпеки в кіберпросторі, одні з яких можуть спровокувати дезінформацію, підрив довіри до уряду з боку суспільства та перетворення людей на «прозорих

громадян», а великі обсяги їхніх персональних даних підштовхнути до незаконного використання, де інформація у відкритому потоці економіки даних використовується без її дозволу та, більше того, проти неї. Система ШІ вчиться на даних, використовує дані та заснована на даних. Це алгоритм, і дані різного характеру є основою його функціонування.

Саме тому завдяки доступності великих наборів даних з інтернету система досягла суттєвого прогресу в навчанні [1, с. 174]. Однак нові дослідження показують, що зростає так звана «криза згоди» у веб-доменах, які вжили заходів для запобігання збирання штучним інтелектом даних, які ті зберігають, і натомість можуть вимагати плату за доступ до них [2].

«Криза згоди» як сучасна проблематика отримання *ефективної* та *реальної* згоди на обробку персональних даних досліджувалася широким колом науковців з різних перспектив, зокрема технологій і права. Наприклад, у праці «The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection» явище описується як неприйняття суб'єктом даних усвідомленого та обґрунтованого рішення через перенавантаження згоди та інформації, коли той стикається із відповідним запитом на згоду обробки його даних [3, с. 179], але в дослідженні про заборону використання даних для навчання ШІ під назвою «Consent in Crisis: The Rapid Decline of the AI Data Commons» визначення інтерпретується здебільшого у площині того, що на колись відкриті дані в мережі тепер покладені певні обмеження. Слід виділити, що несанкціонований доступ до відкритих даних в мережі може спричинити різні правові наслідки для обох сторін. Нижче наведені деякі приклади:

1. The New York Times у 2023 році подала позов до суду на OpenAI та Microsoft за порушення авторських прав: компанії без дозволу використовували статті новин для навчання ШІ [2];
2. У тому ж році подавався колективний позов до Google, який порушував права на конфіденційність та власність, збираючи персональні дані та матеріали, захищені авторським правом, для навчання мовної моделі Gemini [4];
3. Випадок у 2018 році, коли компанія Cambridge Analytica отримала несанкціонований доступ до персональних даних користувачів соцмережі Facebook для аналізу даних в рамках політичної кампанії, що порушувало основний принцип конфіденційності [5, с. 19].

Узагальнюючи приклади, можна підвести до того, що початково наявні дані в мережі були відкритими для перегляду, однак ШІ несанкціоновано використовував ці дані для конкретних цілей, при цьому нехтуючи принципом транспарентності системи. Правова практика у контексті використання даних відповідними системами ШІ в такому випадку зосереджуватиметься у наступних аспектах: право власності на дані, їхня безпека, відповідальність за прозорість системи та регулювання обробки збору даних.

У юридичній науці ШІ виступає каталізатором для переосмислення багатьох правових режимів, адже дана технологія може входити одночасно до декількох галузевих юридичних конструкцій через специфіку різноманіття даних, які вона збирає.

Урядом України поставлена мета створити цифрову державу, де штучний інтелект – важлива частина цього завдання. Навесні 2024 року Міністерство закордонних справ України представило першу у світі цифрову дипломатку, створену нейромережею на основі реальної людини [6]. Існує чітка вірогідність ризиків, пов'язаних з цифровими аватарами, наприклад, широке поняття кризи згоди, яке теж відноситься до необхідності надання однозначно закріпленої згоди людини на обробку її зображення (біометричних даних), а також можливість створення цифрової підробки аватара та поширення дезінформації серед суспільства. Саме тому уряд передбачає загрози і закріплює за аватаром QR-код. З іншого боку, в такому випадку повинна впроваджуватися обізнаність серед населення щодо перевірки ШІ-технологій, які використовує влада.

Інший український інноваційний продукт на базі ШІ – приклад біометричної ідентифікації через сервіс, який за системи стеження за очима веб-камери ідентифікує, аналізує та записує процес читання [7]. Ай-трекінг як технологія аналізу поведінки людини, що лежить в основі програми, може створювати окремі ризики для приватності даних, які система використовує.

Генерування фейкових зображень/відео/аудіо є «реверсом» полегшення роботи уряду на відміну від прикладу впровадження ШІ в українську дипломатію. Навесні 2023 року у мережі з'явилося реалістичне зображення вибуху у Пентагоні, що тимчасово спричинило коливання американського ринку [8].

Виборча кампанія США 2024 року також перебуває під тиском поширення дезінформації про кандидатів. Хоча у Штатах існує «Закон про захист виборців від оманливого ШІ», який надає

політикам право захисту від порушення з боку штучно згенерованого неправдивого контенту в судовому порядку та забороняє підрив виборів за допомоги інструментів ШІ, експерти вказують на поширену світову тенденцію правового регулювання не встигати за розвитком технологій [9].

Вищеописані інциденти мають безпосередній негативний вплив на інформаційну безпеку та економічну стабільність через розповсюдження дезінформації, підриву довіри до влади і сприяння шахрайству різного виду, зменшення інвестицій через ризики та втраті конкурентоспроможності компаній та секторів економіки.

У той же час за словами Міністерства цифрової трансформації України видалення фейків у судовому порядку є неефективним та застарілим через можливість повторення подібних інцидентів в майбутньому, власне, через ту саму динамічність технології [10, с. 16]. Натомість технологічні заходи, які зараз є доволі поширені в мережі, лежать у позначенні контенту, який створений за допомоги ШІ. Наприклад, такі соцмережі, як Facebook та Instagram надають можливість відмітити відповідний контент позначкою. Якщо цього не буде зроблено, система розпізнавання ШІ може автоматично виявити і позначити вміст публікації відміткою, що слугує превенцією поширення дезінформації.

Повертаючись до правових механізмів та заходів, слід виділити попередження подібних інцидентів за допомоги спеціального маркування систем ШІ, сертифікація та їх поділ за рівнями ризику. У цих рамках на сьогодні взірцем слугує Акт ЄС про ШІ. Основний підхід до регулювання згідно з Актом лежить у 4 рівнях класифікації ризиків, згідно з якими певний вид технології може бути: а) заборонений (неприйнятний ризик); б) суворо обмежений (високий ризик); в) підданий правилам (обмежений ризик); г) допущений до використання без спеціальних вимог (мінімальний ризик) [11].

Відтак, наразі виникає необхідність врегулювати ШІ таким чином, щоб в основі забезпечення розвитку технології стояла перш за все гнучкість, етика, прозорість та безпека. Безпека перш за все конфіденційності фізичних осіб. Персональні дані як важливий інструмент роботи ШІ й об'єкт особливої правової охорони першочергово згадувалися як в міжнародних, так і національних рекомендаціях, білих книгах, концепціях тощо, які покликані створити підґрунтя для формування надійної регуляції ШІ.

У 2021 році ЮНЕСКО представило Рекомендацію щодо етики штучного інтелекту. Перший глобальний стандарт у сфері встановлює рекомендації за одинадцятьма сферами стратегічної дії, одна з яких політика даних, і саме цей сектор містить вимоги щодо захисту конфіденційності у системі ШІ. Одні з таких вимог є прозорість; гарантії конфіденційності; належний рівень захисту; підзвітність; можливість видалення ПД; узгодженість із законодавством про захист даних; *ефективний незалежний нагляд* [12, с. 29].

Україна як держава-член прийняла цю Рекомендацію і поступово впроваджує її через Дорожню карту з регулювання ШІ, яка має підготувати компанії та громадян до майбутнього закону-аналога Акту ЄС про ШІ через наступні позазаконодавчі заходи: регуляторна пісочниця як контрольований простір для компаній-розробників ШІ створити безпечний продукт; оцінка ризиків, добровільне маркування систем ШІ, Біла книга, кодекси поведінки тощо. Можливі труднощі, які можуть виникнути при їхньому впровадженні, обумовлюються недостатнім фінансуванням, людським та організаційним ресурсом, що пов'язано в основному з воєнним конфліктом, а також динамічністю суспільних відносин, які постає необхідність врегулювати у сфері ШІ [10, с. 16].

Такий досвід можна зустріти і на міжнародній арені, наприклад, Дорожня карта штучного інтелекту для Африки. Обидві концепції різняться, щонайбільше, метою: Україна направлена на євроінтеграційний шлях та ставить в пріоритет оборонну сферу, а Африка націлена на викорінення голоду та зменшення бідності через підвищення соціально-економічного розвитку за допомоги ШІ. Усе це дозволяє робити висновок про значення технології не тільки в полі окремого користувацького досвіду, але й у вирішенні національних та глобальних питань.

Наразі захист персональних даних з розвитком ШІ-технологій аналогічно фіксується в документах юридично-зобов'язуючого статусу.

За теоретичним підходом до визначення ШІ було взято за приклад законодавче його закріплення в Європейському Союзі, де законодавець у статті 3 Акту ЄС про ШІ розпочинає формування понятійного апарату наступним чином: «Система штучного інтелекту» означає машинну систему, яка розроблена для роботи з різними рівнями автономності та може проявляти адаптивність після розгортання, і яка, для явних або *неявних* цілей, робить висновок на основі вхідних даних, які

вона отримує, як генерувати результати, такі як прогнози, вміст, рекомендації або рішення, які можуть впливати на фізичне або віртуальне середовище» [11].

Із огляду на широкий обсяг поняття ШІ, закріплення його законодавчо як «система» видається вдалим дефініюванням. Можна припустити, що «неявні» цілі стосуються предмету дослідження через проблематику «чорних скриньок» в ШІ, тобто непрозорості роботи системи (можливі порушення принципу транспарентності), а також необхідності наявності *законної мети* для обробки персональних даних.

Остання вимога обґрунтована низкою європейських та національних нормативно-правових документів в полі захисту персональних даних, які негласно регламентують обробку ПД штучним інтелектом. Одні з таких: ЗУ «Про захист персональних даних»; Загальний регламент про захист даних (далі – GDPR); Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних; Директива ЄС про захист персональних даних при обробці компетентними органами.

Важливо уточнити, що Акт ЄС про ШІ «не має на меті впливати на застосування чинного законодавства Союзу, що регулює обробку персональних даних» [11], а навпаки враховує їх і вказує на взаємозв'язок документів.

Доцільним є звернути увагу на місце ШІ у відповідних регуляторних актах із захисту конфіденційності даних особи. Дані можуть входити до одночасно декількох правових режимів захисту [13, с. 72]. Відповідно, така ситуація може створювати правову невизначеність у контексті ШІ.

Таке твердження аргументується тим, що ШІ є новою, важко врегульованою сферою, яка постійне змінюється і поєднує різні аспекти технологій і права, а тому є винятковою. Відповідно, до ШІ повинен застосовуватися міжгалузевий підхід (комбінація елементів права через комплексний характер наборів даних). Як наслідок, до нього має застосовуватися більш гнучке право.

Позиція Кабінету Міністрів України з цього приводу однозначна. У рамках Дорожньої карти з регулювання ШІ влітку 2024 року Міністерством цифрової трансформації України (далі – Мінцифри) було презентовано вищеназвану Білу книгу, в якій вказано, що окремий об'єкт суспільних відносин, до якого ШІ має відношення, має охоплюватися своїм галузевим законодавством [10, с. 11]. Насамкінець, автори Токарєва К.С. та Савліва Н.О. у статті «Особливості правового регулювання штучного інтелекту в Україні» теж наголошують на тому, що реформування законодавства згідно з вимогами цифрової епохи повинно бути комплексним [14, с. 151].

Якщо Урядом України пропонується регуляція ШІ шляхом застосування того чи іншого сектору права, то йдеться перш за все удосконалення наявного законодавства, а не створення нового, тим більше у його тимчасову відсутність чинні норми ЗУ «Про захист персональних даних» заслуговують окремої уваги і є особливо актуалізовані. Комітетом з питань цифрової трансформації до Проєкту оновленого Закону про захист персональних даних № 8153 від 25 жовтня 2022 року внесено рекомендації щодо включення таких операцій з ПД, як псевдонімізація, профілювання та знеособлення: ці методи роботи ШІ з ПД є необхідними в умовах його розвитку. Також Комісією рекомендується уточнення критеріїв порядку доступу *третіх осіб* до ПД [19].

Водночас А.П. Колесніков та О.М. Карапетян вказують на те, що в контексті обробки персональних даних ШІ виступатиме як «третя *сторона*», тому варто доповнити коригування законодавства саме таким чином [15].

Таке зауваження є доречним з огляду на те, що на сьогодні в силу характеру слабкого ШІ його не можна вважати суб'єктом права, до якого входить «третя *особа*» в розумінні статті 4 Закону, а ще ШІ в площині обробки ПД є радше алгоритмічним інструментом, хоч це і є мінливим ствердженням і залежить від цілей напрямку, в якому ШІ обробляє дані. Наприклад, роль ШІ у обробці великого обсягу ПД для досягнення цілей маркетингу відрізняється від ролі у навчанні своєї ж системи даними, які той збирає. Незважаючи на те що в обох випадках ШІ використовує ПД, *мета* (навчання для покращення моделі і персоналізація для таргетингу), *методи* (переважна анонімізація даних для навчання і не завжди деідентифіковані дані для реклами) та *контекст*, зокрема законодавчий, різняться.

Що стосується ширших прогалин наведеного Закону, можна проаналізувати недоліки через призму частини 1 статті 51 GDPR, а саме положення про створення одного чи кількох публічних незалежних наглядових органів, які мають здійснювати нагляд за дотриманням Регламенту про захист даних [16]. До того ж схожа вимога Рекомендації ЮНЕСКО була продекламована вище. Частково функції наглядового органу згідно з частини 1 статті 22 ЗУ «Про захист персональних

даних» покладені на Уповноваженого з прав людини. Проблема в тому, що фактично повноцінним наглядовим органом його вважати не можна, а це є важливим пунктом для реалізації надійного цифрового простору за стратегією Мінцифри.

Проєктом закону про захист персональних даних № 8153 від 25 жовтня 2022 року вносяться корективи до законодавчого розуміння контролюючого органу, що узгоджується із GDPR і є істотним компонентом захисту фізичних осіб у зв'язку з опрацюванням їхніх персональних даних. Наразі цей законопроєкт знаходиться у активній розробці, однак на противагу цьому слід відокремити існуючий з кінця 2021 року проєкт закону про Національну комісію з питань захисту персональних даних та доступу до публічної інформації. Висновком Комітету з питань інтеграції України до Європейського Союзу підтверджено, що останній проєкт потребує суттєвого доопрацювання, зокрема, з метою врахування деяких положень GDPR (разом з тим в світлі приділення особливої уваги опрацюванню персональних даних, спрямованому на дітей) [17].

Було виявлено відсутність будь-якої роботи щодо проєкту після повномасштабного вторгнення рф, тому, з огляду на вищенаведене, необхідно підкреслити про необхідність продовження правотворчої діяльності в цьому напрямку після прийняття нового ЗУ «Про захист персональних даних».

Пункт (b) частини 1 статті 57 GDPR як одне із завдань наглядового органу підкреслює важливість приділення уваги обробці даних, які стосуються дітей. Наприклад, у 2023 році наглядовий орган Італії заборонив використання чат-боту ChatGPT на своїй території через виявлення порушень у тому, що розробники не мали правових підстав для зберігання та збору персональних даних користувачів для навчання алгоритмів, а також незахищеності дітей від шкідливої інформації [18]. Пізніше компанія усунула проблеми і її було відновлено з розширеною прозорістю та правами для європейських користувачів. Зокрема, кожна особа в Євросоюзі може мати право заперечення на використання його персональних даних й у випадку навчання системи (стаття 21 GDPR).

Компанія Meta (Instagram, Facebook тощо) відповідно до оновленої політики конфіденційності влітку 2024 року також надає можливість заперечити щодо використання персональних даних у тренуванні ШІ. Функція працює щонайменше у країнах Євросоюзу згідно з вимогами GDPR.

**Висновки.** Таким чином, оскільки через комплексність даних, які ШІ обробляє, він може підпадати під декілька правових режимів одночасно і через це виникає правова невизначеність. Впровадження ШІ в різні сфери суспільного життя потребує гнучкого регулювання та адаптації існуючих норм для забезпечення належного рівня захисту персональних даних та безпеки. Дослідження показує, що потрібно більше уваги приділяти захисту прав людини, ніж швидкому розвитку технологій. Оскільки правове регулювання відстає від темпів розвитку ШІ-технологій, виникає проблема з приватністю даних. Саме тому етика, прозорість і безпека повинні бути на першому місці в забезпеченні прав людини. При цьому надмірне регулювання може завдавати шкоду як розвитку ШІ, так і захисту приватності, тому у цьому питанні необхідно досягнути балансу завдяки створенню спільних міжнародних стандартів та принципів.

В умовах створення підходів до розуміння системи ШІ та його впливу на захист персональних даних українському законодавцю варто дотримуватися євроінтеграційного шляху і надалі працювати над створенням закону-аналога Акту ЄС про ШІ, аби м'яке право, яке носить підготовчий та рекомендаційний характер трансформувалося у юридично-зобов'язуючі норми, які сповна забезпечуватимуть захист персональних даних. Зокрема, додатковою перспективою у цьому напрямку для України є підписання першої у світі Рамкової конвенції Ради Європи «Про штучний інтелект і права людини, демократію та верховенство права».

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:**

1. Юридичні інновації та стартапи: підручник. Київ: за заг. ред. Пряміцина В., 2024. 290 с.
2. Roose K. The Data That Powers A.I. Is Disappearing Fast. *The New York Times*. 2024. URL: https://www.nytimes.com/2024/07/19/technology/ai-data-restrictions.html (дата звернення: 17.08.2024).
3. Schermer B. W., Custers B., van der Hof S. The crisis of consent: how stronger legal protection may lead to weaker consent in data protection. *Ethics and information technology*. Vol. 16. 2014. P. 171–182.

4. На Google подали позов до суду через неправомірний збір даних для навчання ШІ. *Останній бастіон*. 2023. URL: https://bastion.tv/na-google-podali-pozov-do-sudu-cherez-nepravomirnij-zbir-danih-dlya-navchannya-shi_n56168 (дата звернення: 17.08.2024).
5. Бєлова М.В., Бєлов Д.М. Виклики та загрози захисту персональних даних у роботі за штучним інтелектом. *Науковий вісник Ужгородського національного університету*. № 79. 2023. С. 17–22.
6. МЗС України призначило цифрову особу для інформування щодо консульських питань. *Міністерство закордонних справ України*. 2024. URL: https://mfa.gov.ua/news/mzs-ukrayini-priznachilo-cifrovu-osobu-dlya-informuvannya-shchodo-konsulskih-pitan (дата звернення: 17.08.2024).
7. Українці створили сервіс, що дозволяє зрозуміти, дочитують чи тексти. *Електронна Україна*. 2019. URL: https://eukraine.org.ua/ua/news/ukrayinci-stvorili-servis-shcho-dozvolyaye-zrozumiti-dochituyut-chi-teksti (дата звернення: 17.08.2024).
8. Комиза Р. Вибух Пентагону та обвал ринку. Як штучний інтелект змусив увесь світ здригнутися. *Фокус*. 2023. URL: https://focus.ua/uk/opinions/ 568270-vibuh-pentagonu-ta-obval-rinku-yak-shtuchniy-intelekt-zmusiv-uves-svit-zdrignutisya (дата звернення: 17.08.2024).
9. Бєдовська О. Штучний інтелект і президентські вибори США: хто кого? *Ukrinform.ua.* 2024. URL: https://www.ukrinform.ua/amp/rubric-world/3858936-stucnij-intelekt-i-prezidentski-vibori-ssa-hto-kogo.html (дата звернення: 17.08.2024).
10. Регулювання штучного інтелекту в Україні: Мінцифри презентує Білу книгу. *Урядовий портал*. 2024. 30 с. URL: https://www.kmu.gov.ua/ news/rehuliuvannia-shtuchnoho-intelektu-v-ukraini-mintsyfry-prezentuie-bilu-knyhu (дата звернення: 17.08.2024).
11. 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). URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (дата звернення: 17.08.2024).
12. UNESCO Recommendation on the Ethics of Artificial Intelligence. 43 с. URL: https://unesdoc.unesco.org/ark:/48223/pf0000381137 (дата звернення: 17.08.2024).
13. Дубняк М.В. Економіка даних: правовий та етичний аспект. *Інформація і право*. 2023. № 3 (46). С. 64–74.
14. Токарєва К.С., Савліва Н.О. Особливості правового регулювання штучного інтелекту в Україні. *Юридичний вісник*. 2021. № 3 (60). С. 148–153.
15. Колесніков А.П., Карапетян О.М. Штучний інтелект: переваги та загрози використання. *Ефективна економіка*. 2023. № 8. С. 1–13.
16. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ ЄС (Загальний регламент про захист даних). *Відомості Верховної Ради України*. 2016. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 17.08.2024).
17. Проект Закону про Національну комісію з питань захисту персональних даних та доступу до публічної інформації № 6177 від 18.10.2021. *Відомості Верховної Ради України*. URL: https://itd.rada.gov.ua/billInfo/Bills/CardByRn?regNum=6177&conv=9 (дата звернення: 17.08.2024).
18. Italy lifts ban on ChatGPT after data privacy improvements. *Deutsche Welle*. 2024. URL: https://www.dw.com/en/ai-italy-lifts-ban-on-chatgpt-after-data-privacy-improvements/a-65469742 (дата звернення: 17.08.2024).
19. Проект Закону про захист персональних даних № 8153 від 25 жовтня 2022 року. *Відомості Верховної Ради України*. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/40707 (дата звернення: 17.08.2024).