УДК 004.8:342.7:004.056
DOI https://doi.org/10.32782/2524-0374/2024-8/59

ПРОБЛЕМИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ПІД ЧАС ОБРОБЛЕННЯ ПЕРСОНАЛЬНИХ ДАНИХ ТА НАПРЯМИ ЇХ ВИРІШЕННЯ

PROBLEMS OF USING ARTIFICIAL INTELLIGENCE DURING PROCESSING OF PERSONAL DATA AND WAYS TO SOLVE THEM

Машталяр О.М., аспірант кафедри інформаційних технологій та кібербезпеки
Навчально-науковий інститут № 1 Національної академії внутрішніх справ

Стаття присвячена дослідженню проблем використання штучного інтелекту (ШІ) та його впливу на обробку (зберігання, використання, захисту) персональних даних в Україні. Особлива увага приділяється правовим аспектам, зокрема необхідності гармонізації українського законодавства з європейськими стандартами, такими як Загальний регламент про захист даних (GDPR). Також розглядаються технічні рішення для підвищення рівня захисту даних, такі як шифрування, анонімізація даних та системи виявлення витоків. Аналізуються етичні питання та способи забезпечення справедливості та прозорості алгоритмів ШІ. Використання ШІ дозволяє автоматизувати процеси виявлення та реагування на загрози, підвищувати ефективність шифрування та анонімізації даних, а також забезпечувати відповідність нормативним вимогам. Проте разом із перевагами використання ШІ існують і проблеми, такі як ризики конфіденційності, упередженість алгоритмів і складність їх перевірки. Однією з ключових проблем використання ШІ є забезпечення належного рівня захисту персональних даних під час їх обробки. Це включає питання зберігання, використання та захисту даних від несанкціонованого доступу та витоків. Сучасне нормативно-правове забезпечення України часто не враховує специфіку ШІ, що створює правові прогалини та ускладнює ефективне регулювання цієї сфери. Крім того, технологічні аспекти, такі як забезпечення прозорості та етичності алгоритмів ШІ, також потребують уваги для запобігання дискримінації прав користувачів. Ця стаття має на меті дослідити основні проблеми використання ШІ під час обробки персональних даних в Україні, а також запропонувати можливі шляхи їх вирішення, враховуючи досвід певних країн у цій сфері. Також, основна проблема полягає в тому, що існуючі правові та регуляторні рамки не встигають за швидким технологічним розвитком ШІ, що призводить до недостатнього захисту персональних даних та порушень прав користувачів. Багато країн, включаючи Україну, мають законодавство щодо захисту персональних даних, яке було розроблене до широкого впровадження технологій ШІ. Це означає, що багато аспектів використання ШІ залишаються нерегульованими або недостатньо регульованими. В даній статті розглядаються як переваги, так і недоліки використання ШІ для захисту персональних даних, а також окреслюються деякі шляхи вдосконалення правових та технологічних підходів до захисту даних в умовах швидкого розвитку ШІ в Україні.

Ключові слова: штучний інтелект, законодавство України, персональні дані, захист даних, обробка даних, інформація, кібербезпека, технології ШІ.

The article is devoted to the study of the problems of using artificial intelligence (AI) and its impact on the processing (storage, use, protection) of personal data in Ukraine. Particular attention is paid to legal aspects, in particular, the need to harmonise Ukrainian legislation with European standards, such as the General Data Protection Regulation (GDPR). Technical solutions to improve data protection, such as encryption, data anonymisation and leak detection systems, are also considered. Ethical issues and ways to ensure the fairness and transparency of AI algorithms are analysed. The use of AI allows automating threat detection and response, increasing the effectiveness of data encryption and anonymisation, and ensuring compliance with regulatory requirements. However, along with the benefits of using AI, there are also challenges, such as privacy risks, algorithm bias, and the complexity of their verification. One of the key challenges of using AI is ensuring an adequate level of protection of personal data during its processing. This includes the storage, use and protection of data from unauthorised access and leakage. Ukraine's current regulatory framework often does not take into account the specifics of AI, which creates legal gaps and complicates effective regulation of this area. In addition, technological aspects, such as ensuring transparency and ethics of AI algorithms, also require attention to prevent discrimination of user rights. This article aims to explore the main problems of using AI in personal data processing in Ukraine, as well as to propose possible ways to solve them, taking into account the experience of certain countries in this area. Also, the main problem is that the existing legal and regulatory frameworks do not keep pace with the rapid technological development of AI, which leads to insufficient protection of personal data and violations of users' rights. Many countries, including Ukraine, have personal data protection legislation that was developed before the widespread adoption of AI technologies, meaning that many aspects of AI use remain unregulated or under-regulated. This article discusses both the advantages and disadvantages of using AI to protect personal data, and outlines some ways to improve legal and technological approaches to data protection in the context of the rapid development of AI in Ukraine.

Key words: artificial intelligence, Ukrainian legislation, personal data, data protection, data processing, information, cybersecurity, AI technologies.

Вступ. Штучний інтелект (ШІ) швидко стає невід'ємною частиною нашого життя, зокрема у сфері обробки персональних даних. Використання технологій ШІ відкриває нові можливості для аналізу значних обсягів інформації, прогнозування тенденцій та прийняття рішень. Однак, поряд із перевагами, виникають численні проблеми використання ШІ, пов'язані з конфіденційністю, безпекою та правовою охороною персональних даних. В Україні ці виклики стають особливо актуальними в умовах швидкого технологічного розвитку та необхідності адаптації національного законодавства до міжнародних стандартів [11, с. 12].

Однією з ключових проблем використання ШІ є забезпечення належного рівня захисту персональних даних під час їх обробки. Це включає питання зберігання, використання та захисту даних від несанкціонованого доступу та витоків цих даних. Сьогодні чинне нормативно-правове забезпечення України часто не враховує специфіку ШІ, що створює правові прогалини та ускладнює ефективне регулювання цієї сфери. Крім того, технологічні аспекти, такі як забезпечення прозорості та етичності алгоритмів ШІ[1], також потребують уваги для запобігання дискримінації прав користувачів.

Ця стаття має на меті дослідити основні проблеми використання ШІ під час обробки персональних даних в Україні, а також запропонувати можливі шляхи їх вирішення враховуючи досвід певних країн в цій сфері. Особлива увага приділяється правовим аспектам, зокрема необхідності гармонізації українського законодавства з європейськими стандартами, такими як Загальний регламент про захист даних (GDPR). Також розглядаються технічні рішення для підвищення рівня захисту даних, такі як шифрування, анонімізація даних[2] та системи виявлення

[1] Етичність алгоритмів ШІ – це концепція, що охоплює набір принципів та практик, які забезпечують відповідність алгоритмів штучного інтелекту етичним стандартам та соціальним нормам.

[2] Анонімізація даних – це процес перетворення персональних даних таким чином, щоб ідентифікація конкретного індивіда стала неможливою.

витоків. Аналізуються етичні питання та способи забезпечення справедливості та прозорості алгоритмів ШІ.

Проблематикою використання ШІ в обробці персональних даних порушували у своїх працях Кузьменко О. В., Смірнов І., Шевченко А. Є., Кудін С. В., Радутний О. Е., Бєлова М. В., Бєлов Д. М. та інші як вітчизняні так і іноземні науковці.

Постановка проблеми. Штучний інтелект (ШІ) стає все більш важливою частиною сучасних технологій, що викликає значні зміни у способах обробки та захисту персональних даних. Незважаючи на величезний потенціал, який ШІ має для покращення ефективності та безпеки обробки даних, його застосування також породжує низку серйозних проблем та викликів.

Основна проблема полягає в тому, що існуючі правові та регуляторні рамки не встигають за швидким технологічним розвитком ШІ, що призводить до недостатнього захисту персональних даних та порушень прав користувачів. Багато країн, включаючи Україну, мають законодавство щодо захисту персональних даних, яке було розроблене до широкого впровадження технологій ШІ. Це означає, що багато аспектів використання ШІ залишаються нерегульованими або недостатньо регульованими.

Використання ШІ для обробки персональних даних викликає такі основні проблеми:

1. Конфіденційність та безпека даних: Моделі ШІ потребують великих обсягів даних для навчання, що підвищує ризик витоку даних та їх зловживання. Це особливо актуально в умовах, коли дані можуть бути використані для тренування алгоритмів без належного контролю та захисту.

2. Упередженість та дискримінація: Алгоритми ШІ можуть відображати упередження, що містяться в тренувальних даних, що може призводити до дискримінації певних груп користувачів. Це вимагає розробки методів для виявлення та усунення упередженостей, а також забезпечення прозорості та справедливості алгоритмів.

3. Правові колізії: Наявні правові норми часто не враховують специфіку ШІ, що може призводити до правових колізій. Наприклад, Закон України «Про захист персональних даних» не повністю охоплює всі аспекти використання ШІ, що створює прогалини в правовому регулюванні.

4. Відповідність міжнародним стандартам: Для забезпечення належного рівня захисту даних Україна потребує гармонізації свого законодавства з міжнародними стандартами, такими як Загальний регламент про захист даних (GDPR). Це дозволить забезпечити високий рівень захисту персональних даних та уникнути правових колізій у міжнародних відносинах.

5. Етичні аспекти: Використання ШІ викликає значні етичні питання, пов'язані з конфіденційністю, безпекою та правами користувачів. Важливо розробити етичні керівництва та стандарти для використання ШІ, щоб забезпечити дотримання етичних норм та захист прав користувачів.

Таким чином, для ефективного та безпечного використання ШІ в обробці персональних даних необхідно розробити комплексну правову та етичну базу. Це включає оновлення існуючих законодавчих актів, впровадження нових стандартів захисту даних, розробку етичних керівництв, а також забезпечення прозорості та підзвітності алгоритмів ШІ. Вирішення цих проблем є критично важливим для забезпечення довіри користувачів до технологій ШІ та забезпечення їх прав на конфіденційність та безпеку персональних даних.

Метою статті є дослідження основних проблем, пов'язаних з використанням штучного інтелекту (ШІ) під час обробки персональних даних в Україні, а також розробка ефективних рекомендацій та стратегій для вирішення цих проблем. Особлива увага приділяється аналізу аспектів конфіденційності, безпеки, упередженості алгоритмів та правового регулювання, зокрема, гармонізації національного законодавства з міжнародними стандартами, такими як Загальний регламент про захист даних (GDPR).

Актуальність теми дослідження. Використання штучного інтелекту (ШІ) під час обробки персональних даних в Україні обумовлена низкою факторів, які свідчать про важливість і своєчасність розгляду цієї проблематики.

Виклад основного матеріалу. Відповідно до абз. 3 Загальної частини Концепції розвитку штучного інтелекту в Україні, схваленої розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р, під штучним інтелектом розуміють «Штучний інтелект – організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань» [5, с. 12].

Використання ШІ для обробки персональних даних надає значні переваги, проте також супроводжується низкою проблем, які потребують вирішення.

Однією з найбільших загроз при використанні ШІ для обробки персональних даних є ризик витоку інформації. Це може статися через недостатню захищеність систем або через атаки з боку зловмисників. Наприклад, у випадках несанкціонованого доступу до баз даних, що містять персональні дані, інформація може бути викрадена і використана для шахрайства, шантажу або інших незаконних цілей. На сьогоднішній день зафіксовані випадки витоку персональних даних, пов'язані з використанням штучного інтелекту, але жоден з них не став широко відомим або не привернув значної уваги громадськості. Тим не менш, можна виділити деякі приклади, де були порушені принципи захисту персональних даних у контексті застосування ШІ: Cambridge Analytica: У 2018 році було виявлено випадок, коли штучний інтелект використовували для збору та обробки персональних даних мільйонів користувачів Facebook. Компанія Cambridge Analytica, яка спеціалізувалася на аналізі даних для політичних кампаній, отримала доступ до персональних даних без належної згоди користувачів, порушивши принципи конфіденційності та приватності [1, с. 11].

ШІ-системи, які використовуються для аналізу великих обсягів даних, можуть випадково розпізнати або виявити особисту інформацію, яка була призначена для анонімізації. Це може статися через недостатню точність алгоритмів анонімізації або через зворотнє аналізування даних, що дозволяє відновити первинну інформацію. Технологія розпізнавання обличчя: Використання технології розпізнавання обличчя (Facial Recognition) також може становити загрозу для приватності осіб. Наприклад, були випадки, коли системи розпізнавання обличчя застосовувалися без дозволу користувачів, збираючи їхні персональні дані без належної інформованості та контролю [1, с. 11].

Використання ШІ для обробки персональних даних також піднімає питання отримання згоди від користувачів. У багатьох випадках користувачі не розуміють, яким чином їхні дані будуть використовуватися, або не мають можливості контролювати процес їх обробки. Це може призвести до порушення права на приватність і створити негативні наслідки для користувачів [4, с. 12].

ШІ-системи можуть мати вразливості, які можуть бути використані зловмисниками для компрометації системи або викрадення даних. Наприклад, атаки типу «обману машинного навчання» (adversarial attacks) можуть змусити ШІ-систему приймати неправильні рішення або розкрити конфіденційну інформацію. Такі атаки можуть бути складними для виявлення і попередження. Алгоритми машинного навчання можуть бути вразливими до атак,

якщо вони не були належним чином захищені. Зловмисники можуть використовувати вразливості в алгоритмах для отримання доступу до даних або для маніпуляції результатами аналізу. Це може мати серйозні наслідки для конфіденційності і безпеки даних.

Застосування ШІ для обробки персональних даних також підвищує ризик кіберзагроз, таких як фішинг, шкідливе програмне забезпечення та атаки на мережу. ШІ-системи можуть стати мішенню для зловмисників, які прагнуть отримати доступ до конфіденційної інформації або викликати збої в роботі системи. Це вимагає додаткових заходів безпеки для захисту систем і даних [6, с. 12].

Також однією з основних етичних проблем є непрозорість алгоритмів ШІ, які використовуються для обробки персональних даних. Користувачі часто не знають, як їхні дані обробляються і які алгоритми використовуються для прийняття рішень. Це може призвести до недовіри до ШІ-систем і порушення прав користувачів на прозорість і контроль над своїми даними. В свою чергу алгоритми ШІ можуть мати вбудовані упередження, які можуть призвести до дискримінації окремих груп користувачів. Це може статися через неправильне навчання алгоритмів на необ'єктивних даних або через використання некоректних методів аналізу. Такі проблеми можуть мати серйозні соціальні і правові наслідки.

Використання ШІ для обробки персональних даних також піднімає питання щодо згоди користувачів і відповідальності за можливі зловживання. Користувачі повинні мати право контролювати, як їхні дані використовуються, і отримувати чітку інформацію про цілі і методи обробки. В одночас враховуючи теперішню війну України з Росією та необхідності збору та обробки великою кількості додаткової інформації, включаючи геномну інформацію про людину, технології ШІ та персональні дані, які ними обробляються на території України є напрочуд вразливими [7, с. 12].

Основні шляхи вирішення даної проблеми: Одним із ефективних шляхів вирішення проблем є впровадження нових технологій захисту даних, таких як диференціальна конфіденційність, гомоморфне шифрування та блокчейн. Ці технології дозволяють захистити дані під час їх обробки та зберігання. Диференціальна приватність забезпечує анонімність даних, додаючи випадковий шум до інформації, що обробляється, що ускладнює ідентифікацію індивідуальних записів [8, с. 12]. Гомоморфне шифрування дозволяє виконувати обчислення над зашифрованими даними, не розшифровуючи їх, що забезпечує високий рівень безпеки [9, с. 12]. Блокчейн-технологія забезпечує прозорість і незмінність записів, що робить неможливим несанкціоноване змінення даних.

Важливим кроком є розробка правових та етичних стандартів, які регулюватимуть використання ШІ. Це включає встановлення чітких правил щодо обробки персональних даних та відповідальності за їх порушення. Міжнародне співробітництво є необхідним для створення узгоджених стандартів і забезпечення їх дотримання. Крім того, необхідно розробити етичні кодекси для розробників і користувачів ШІ, які враховують права і інтереси всіх зацікавлених сторін [10, с. 12].

Підвищення обізнаності та освіти серед користувачів та розробників ШІ також є важливим аспектом. Це дозволить зменшити ризики, пов'язані з неправомірним використанням ШІ та підвищити рівень захисту персональних даних. Важливо, щоб користувачі розуміли, як їхні дані обробляються і які ризики можуть виникнути. Для цього можна проводити інформаційні кампанії, тренінги та освітні програми, які сприятимуть підвищенню обізнаності про питання конфіденційності та безпеки даних.

Висновок. Штучний інтелект (ШІ) має величезний потенціал у сфері захисту та охорони персональних даних, завдяки своїм можливостям автоматизації, аналізу великих обсягів інформації та виявлення загроз у режимі реального часу. ШІ може значно покращити виявлення та реагування на кіберзагрози, дозволяючи організаціям швидше та ефективніше захищати дані користувачів. Використання машинного навчання для аналізу аномалій та виявлення підозрілої активності дозволяє вчасно виявляти потенційні атаки та запобігати витокам даних. Крім того, ШІ може автоматизувати процеси шифрування та анонімізації даних, підвищуючи їх безпеку.

Серед переваг використання ШІ для захисту персональних даних можна виділити наступні:

1. Автоматизація безпекових процесів: ШІ дозволяє автоматизувати виявлення загроз і реагування на них, що зменшує навантаження на людські ресурси та покращує швидкість реакції.
2. Покращене виявлення аномалій: Алгоритми машинного навчання здатні аналізувати великі обсяги даних і виявляти аномалії, які можуть свідчити про кіберзагрози.
3. Підвищення ефективності шифрування та анонімізації: ШІ може допомагати у розробці та впровадженні більш ефективних методів захисту даних.
4. Автоматизація дотримання нормативних вимог: ШІ може автоматично забезпечувати відповідність даних вимогам нормативних актів, таких як GDPR.

Однак, використання ШІ для захисту персональних даних не позбавлене недоліків та ризиків:

1. Конфіденційність даних: Для навчання моделей ШІ необхідний доступ до великих обсягів даних, що може підвищувати ризик витоків і зловживань.
2. Упередженість алгоритмів: Моделі ШІ можуть містити упередження, які виникають через недосконаліть даних, що може призвести до дискримінації та несправедливого ставлення до користувачів.
3. Складність та прозорість: Алгоритми ШІ часто є складними та непрозорими, що ускладнює їх перевірку та валідацію.
4. Правові та етичні виклики: Відсутність чітких регуляторних рамок може створити правові та етичні проблеми у використанні ШІ для захисту даних.

Таким чином, для ефективного та безпечного використання ШІ у сфері захисту персональних даних необхідно розробити комплексний підхід, який включає вдосконалення законодавства, впровадження новітніх технологічних рішень та забезпечення етичних стандартів. Гармонізація українського законодавства з міжнародними стандартами, такими як GDPR, є критично важливою для забезпечення високого рівня захисту даних. Лише так можна досягти балансу між інноваціями та захистом прав користувачів, забезпечуючи безпечне та етичне використання ШІ у всіх сферах життя.

ЛІТЕРАТУРА

1. World Intellectual Property Organization (WIPO) – Artificial Intelligence and Intellectual Property Policy Considerations. URL: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf (Last accessed: 22.07.2024).
2. Про інформацію: Закон України від 2 жовтня 1992 р. № 2658. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 22.07.2024).
3. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 р. № 80/94. URL: https://zakon.rada.gov.ua/laws/card/80/94-%D0%B2%D1%80 (дата звернення: 23.07.2024).
4. Про захист персональних даних: Закон України від 1 червня 2010 р. № 2297. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 23.07.2024).
5. Про схвалення Концепції розвитку штучного інтелект в Україні: Розпорядження Кабінету Міністрів України від 02.12.20 р. № 1556. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення: 24.07.2024).
6. Конвенція про кіберзлочинність / *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 24.07.2024).
7. Про державну реєстрацію геномної інформації людини: Закон України від 9 липня 2022 р. № 2391. URL: https://zakon.rada.gov.ua/laws/show/2391-IX#Text (дата звернення: 25.07.2024).
8. «Диференційна приватність» як спосіб припинити гонитву за особистими даними користувачів Cybercalm : веб-сайт. URL: https://cybercalm.org/novyny/dyferentsijna-pryvatnist-yak-sposib-prypynyty-gonytvu-za-osobystymy-danymy-korystuvachiv/ (дата звернення: 25.07.2024).
9. Що таке гомоморфне шифрування? Keyfactor : веб-сайт. URL: https://www.keyfactor.com/blog/what-is-homomorphic-encryption/ (дата звернення: 26.07.2024).
10. Ірина Кудрянь, Етичні аспекти використання штучного інтелекту в маркетингу Theantmedia : веб-сайт URL: https://www.theantmedia.com/post/etichni-aspekti-vikoristannya-shtuchnogo-intelektu-v-marketingu (дата звернення: 26.07.2024).
11. Гуртова, К. М. (2024). Теорія і практика адаптації законодавства України до законодавства ЄС. *Київський часопис права*. 2024. Вип. 4. С. 162–168.