ЕТИКА ТА ЗАХИСТ ДАНИХ В ШТУЧНОМУ ІНТЕЛЕКТІ

Макушенко Т.В., кандидат технічних наук, доцент,
ПЗВО «Харківський технологічний університет
«ШАГ», м. Харків, Україна
ORCID ID: https://orcid.org/0000-0001-7124-9610
Десятниченко О.В., кандидат технічних наук,
ПЗВО «Харківський технологічний університет
«ШАГ», м. Харків, Україна
ORCID ID: https://orcid.org/0009-0001-2768-5578
Горшков О.М.,
ПЗВО «Харківський технологічний університет
«ШАГ», м. Харків, Україна

Швидкий прогрес у сфері штучного інтелекту (ШІ) у останні десятиліття змінив ландшафт інформаційних технологій та суттєво вплинув на різні аспекти нашого життя. З великими обіцянками щодо автоматизації процесів, оптимізації прийняття рішень та розв'язання складних проблем, ШІ стає драйвером інновацій у різних галузях, починаючи від медицини та фінансів і закінчуючи автономними транспортними засобами та роботами. Підтримуємо думку Погореленко А.К. «Штучний інтелект – це те, що кардинально змінило світ» [1].

Проте разом зі зростанням потужності ШІ постають і серйозні етичні та правові питання, зокрема стосовно збору, обробки та використання великих обсягів персональних даних [2]. Ці питання стають набагато актуальнішими в контексті необмеженого доступу до великої кількості інформації, що може бути використана для здійснення впливу, порушення приватності та навіть шкоди індивідам.

У багатьох країнах по всьому світу прийнято законодавство, спрямоване на захист приватності та регулювання використання даних, включаючи дані, що використовуються у штучному інтелекті. Наприклад, в Європейському Союзі набув чинності Загальний регламент з захисту даних (GDPR), який встановлює правила щодо збору, обробки та використання особистих даних і застосовується до будь-яких організацій, які працюють з даними європейських громадян. Деякі країни також мають свої власні законодавчі акти, що регулюють сферу захисту даних, такі як Закон про захист особистих даних в США.

Однак, хоча існують певні стандарти і законодавчі акти, вони часто не враховують повністю специфічні вимоги та виклики, що виникають у зв'язку з використанням штучного інтелекту. Наприклад, питання, пов'язані з прозорістю алгоритмів, відповідальністю за рішення, прийняті штучним інтелектом, та етичними аспектами використання даних, залишаються не повністю вирішеними у багатьох законодавчих актах.

Таким чином, етика та захист даних в ШІ стають важливими аспектами розвитку технологій, які вимагають серйозного обговорення та розробки адекватних стратегій реагування. У цьому есе ми дослідимо ключові етичні проблеми, пов'язані з збором та використанням даних у системах ШІ, а також розглянемо можливі підходи до їх вирішення та захисту приватності користувачів.

Сучасний світ переживає епоху швидкого розвитку технологій, особливо у сфері штучного інтелекту (ШІ), який відіграє значну роль у багатьох аспектах нашого життя. Проте, разом із зростанням можливостей ШІ, постають етичні питання, пов'язані зі збором, обробкою та використанням даних у цих системах.

По-перше, прозорість у зборі та використанні даних є ключовою для забезпечення довіри користувачів. ШІ може збирати великі обсяги даних про користувачів без їх повідомлення, що порушує принцип прозорості. Користувачі мають право знати, які дані збираються, як вони обробляються та за якими цілями використовуються.

Друге етичне питання стосується згоди на обробку даних. Вимагається забезпечення згоди користувачів на збір та використання їхніх персональних даних, особливо в чутливих сферах, таких як медицина чи фінанси. Недостатня чіткість у процесі отримання згоди може призвести до порушення приватності та викликати недовіру до систем ШІ.

Третє етичне питання включає використання алгоритмів зі збереженням конфіденційності. Багато систем ШІ використовують алгоритми машинного навчання, які можуть бути вразливі до атак на конфіденційність даних. Забезпечення конфіденційності даних через алгоритмічні методи стає ключовою проблемою в епоху масового збору і обробки інформації.

Узагальнюючи, етичні питання, пов'язані зі збором, обробкою та використанням даних у системах ШІ, вимагають пристосування та розвитку етичних норм і правил у цій галузі. Це включає в себе забезпечення прозорості, чіткої згоди на обробку даних та розробку алгоритмів, які забезпечують конфіденційність інформації. Відповідно до цих принципів, ми можемо зберегти баланс між розвитком технологій та забезпеченням прав та приватності користувачів у цифровій ері.

Загрози для приватності та безпеки даних у зв'язку з розвитком ШІ наступні:

1. Злам систем безпеки. Розвиток ШІ може призвести до зростання кількості та складності атак на системи безпеки. Штучний інтелект може бути використаний для автоматизації атак, злому паролів, а також для виявлення вразливостей у системах безпеки.

2. Недостатня захищеність алгоритмів ШІ. Багато систем ШІ використовуються на основі алгоритмів машинного навчання, які можуть бути вразливі до атак, таких як атаки з введенням даних, злам моделей тощо.

3. Порушення приватності через використання даних. Зі збільшенням обсягу та різноманітності даних, що збираються системами ШІ, існує загроза порушення приватності користувачів. Використання цих даних без належної згоди чи без заходів захисту може призвести до витоку особистої інформації та порушення приватності.

Тож, такі ситуації вимагають не простого розуміння наявності проблеми, а безпосереднього застосування практичних заходів та інструментів, зокрема криптографію, анонімізацію даних, контроль доступу та постійний моніторинг та аудит.

Література:

1. Погореленко А.К. Штучний інтелект: сутність, аналіз застосування, перспективи розвитку. *Науковий вісник Херсонського державного університету*. 2018. Вип. 32. С. 22-27.

2. Парасюк Є.О., Джалілова В.Р. Доцільність визнання суб'єктами права роботів, штучного інтелекту та штучно інтелектуальних роботів. *Журнал Науковий огляд*. 2019. № 4(57). URL: https://www.naukajournal.org/index.php/naukajournal/article/view/1821/1871