Серія «Технічні науки»
Випуск 1(109) 2025 р.

УДК 004.42 https://doi.org/10.31713/vt1202516

Бачишина Л. Д., к.е.н., доцент, Касперська А. О., студентка (Національний університет водного господарства та природокористування, м. Рівне, l.d.bachyshyna@nuwm.edu.ua, kasperska_ak20@nuwm.edu.ua)

ВПЛИВ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ НА БЕЗПЕКУ ТА КОНФІДЕНЦІЙНІСТЬ ІНФОРМАЦІЇ

У статті детально описані методи захисту інформації, розглянуто принципи цифрового захисту, що є актуальними у часи стрімкого розвитку технологій штучного інтелекту. Під час дослідження було розглянуто основні типи порушень кібербезпеки, з якими існує ймовірність зіткнутися в мережі. Не є секретом, що штучний інтелект з кожним днем проникає в найрізноманітніші аспекти життя людини і є корисним інструментом, який допоможе автоматизувати існуючі процеси, ухвалювати нові рішення, аналізувати та прогнозувати сценарії дій. Більш широке використання означає збільшення обсягу зібраних даних, що несе ризики та небезпеки, пов'язані з безпекою та конфіденційністю.

Попри те, що штучний інтелект багато в чому спростив діяльність людини, його використання не скасовує необхідності дотримання правил цифрової безпеки. Заключна частина роботи містить профілактичні заходи, які допоможуть уберегти особисту інформацію від витоку та знизити ризики кібератак.

Ключові слова: **штучний інтелект; кібербезпека; кіберзахист; безпека інформації; автентифікація користувача; цифрова грамотність**.

Вступ. Разом зі зростанням популярності штучного інтелекту і його інтеграції у діяльність людини з'явилися нові ризики несанкціонованого доступу до особистих даних користувача [1; 8]. Актуальність теми зумовлена розвитком штучного інтелекту та збору даних, які є основою функціонування цієї системи. Порушення цілісності даних може призвести до серйозних наслідків, в тому числі перехоплення персональної інформації, яка може бути використана у злочинних цілях. Крім того, штучний інтелект також може використовуватися для масового збору даних про користувачів.

Мета статті. Аналіз проблем конфіденційності та безпеки інформації у часи штучного інтелекту, а також формулювання

рекомендацій щодо їх запобігання або вирішення, у разі виникнення.

Для досягнення поставленої мети необхідно вирішити такі завдання:

- дослідити закономірності впливу штучного інтелекту на конфіденційність користувача в мережі;
- провести аналіз інцидентів, пов'язаних із витоком інформації і порушенням безпеки даних;
- розробити рекомендації що стосуються підвищення рівня безпеки та конфіденційності даних.

Перераховані вище завдання необхідно розглядати безпосередньо в контексті штучного інтелекту. Для їх вирішення необхідно використовувати методи порівняльного аналізу, аналізу наукової літератури, а також методи статистичного аналізу. Результати дослідження можуть стати корисними експертам з інформаційної безпеки та розробникам систем штучного інтелекту.

Аналіз випадків витоку даних користувачів, пов'язаних з ШІ

Необхідно враховувати інциденти фактичного витоку даних під час використання технологій штучного інтелекту. Аналіз таких випадків допоможе виявити вразливі місця та вжити необхідних заходів щодо покращення безпеки та конфіденційності даних.

Таблиця

Інциденти з витоком даних із залученням штучного інтелекту

№	Де відбувся витік даних	Опис події
1	Microsoft	За даними компанії Wiz, близько 38 ТБ даних, які включали резервну копію декількох комп'ютерів, а також ключі шифрування паролів і потоки Microsoft Teams, було випадково завантажено в репозиторій Microsoft AI GitHub. Цей випадок підкреслює важливість впровадження суворого контролю доступу та навчання персоналу
2	Facebook	Дослідники виявили, що Cambridge Analytica неналежним чином використовувала дані мільйонів користувачів Facebook. Цей випадок підкреслив важливість моніторингу та контролю роботи ШІ, що має змогу використовувати, аналізувати та поширювати особисту інформацію без згоди користувача

продовження таблиці

3	Capital One	Хакер отримав доступ до особистих даних близько 106 мільйонів банківських клієнтів. Цей випадок продемонстрував важливість захисту інфраструктури, яка використовується для роботи зі штучним інтелектом

Ця таблиця ілюструє деякі з основних випадків витоків даних із залученням штучного інтелекту, показуючи різні способи, якими вразливості, пов'язані зі штучним інтелектом, можуть призвести до серйозних інцидентів безпеки.

Проблема конфіденційності даних у рішеннях із залученням ШІ

Виклики, пов'язані зі сферою штучного інтелекту, надзвичайно значущі, а можливі ризики дуже високі. У центрі уваги – питання безпеки системи та надійності даних. Розглянемо основні ризики обробки інформації за допомогою систем ШІ.

Величезні потоки інформації. Важливо зазначити, що штучний інтелект значно впливає на конфіденційність користувача, оскільки системам ШІ необхідна значна кількість даних, щоб вчитися, адаптуватися та надавати точні результати [2]. Ці дані можуть варіюватися від основної демографічної інформації до більш конфіденційних деталей, таких як фінансові дані, медичні записи або особисті вподобання. Однак збір таких обширних персональних даних потенційно може призвести до небажаного витоку. Наприклад, без належних заходів безпеки доступ до особистої інформації можуть отримати неавторизовані особи чи організації, що призведе до порушення конфіденційності.

Чорний ящик. Моделі на базі ШІ часто є «чорними ящиками», тобто важко зрозуміти, як саме вони ухвалюють рішення [3]. Відсутність прозорості, очевидно викликає занепокоєння щодо конфіденційності використаної інформації, оскільки користувачі можуть не знати, які дані збирає ШІ, як вони застосовуються, або як щодо них приймаються рішення.

Автоматизоване ухвалення рішень. Штучний інтелект може приймати автоматизовані рішення на основі даних, що прискорює процеси та підвищує ефективність. Однак це також може обмежити особистий вибір і контроль над власними даними.

Ціль кібератак. Оскільки системи ШІ збирають і зберігають великі обсяги даних, вони є потенційними цілями для кібератак.

Якщо подібне програмне рішення застосувати до проєкту з великою базою користувачів без впровадження необхідних заходів безпеки, то особиста інформація багатьох людей може бути розкрита, що призведе до серйозних порушень конфіденційності.

Забезпечення безпеки та конфіденційності даних

Розробники можуть застосовувати різні заходи для забезпечення безпеки та конфіденційності даних. За допомогою правильних стратегій захисту можливо використовувати потужність систем ШІ, зберігаючи при цьому конфіденційність.

Розробка та впровадження чіткої політики конфіденційності є першочерговим кроком на шляху до цілісності даних. Така політика має чітко визначати, яка інформація збирається, як вона використовується та як вона захищена. Це дозволяє встановити прозорі процедури обробки даних і забезпечує дотримання прав користувачів. Регулярні тренінги з безпеки даних для працівників необхідні, щоб підвищити їхню обізнаність щодо важливості захисту даних. Співробітники повинні розуміти, як запобігати витокам інформації та ефективно реагувати на потенційні загрози.

Розробка плану реагування системи на інциденти порушення безпеки включає процедури сповіщення та відновлення. Це дозволяє швидко реагувати на інциденти та мінімізувати їх наслідки. Проведення регулярних перевірок та оцінок безпеки допомагає виявити та усунути вразливі місця [4]. Це сприяє підтримці високого рівня безпеки даних і дозволяє своєчасно оновлювати захисні заходи.

Обмеження доступу до даних на основі попередньо встановлених ролей співробітників в організації допомагає мінімізувати ризики. Це означає, що кожен працівник має доступ лише до інформації, необхідної для виконання своїх обов'язків, що зменшує ймовірність несанкціонованого доступу. Забезпечення фізичної безпеки приміщень, де зберігаються дані, є критично важливим [6]. Це включає контроль доступу, відеоспостереження та інші заходи, спрямовані на запобігання несанкціонованому проникненню.

Застосування надійного шифрування для захисту даних під час зберігання та передачі забезпечує додатковий рівень безпеки, захищаючи дані від кібератак і витоків. Регулярне створення резервних копій даних необхідно для забезпечення їх відновлення у разі втрати або пошкодження. Це допомагає уникнути втрат даних і забезпечує їх доступність у критичних ситуаціях.

Стратегія, що полягає в анонімізації та псевдонімізації даних може допомогти вирішити проблему конфіденційності під час роботи зі ШІ. Це методи, які використовуються для захисту індивідуальних даних шляхом видалення або заміни ідентифікаційної інформації (PII) штучними ідентифікаторами. Це схоже на маскування кожної частини даних, що ускладнює пов'язування даних із особою, від якої вони надійшли.

Впровадження політики керування пристроєм, в тому числі шифрування, віддалене видалення даних і блокування в разі втрати або крадіжки, забезпечує додатковий захист даних на мобільних пристроях та інших носіях.

Дотримання всіх відповідних законів і норм щодо конфіденційності є обов'язковим. Це стосується таких нормативних актів, як Загальний регламент захисту даних (GDPR) у Європейському Союзі. Відповідність законодавству гарантує, що наші рішення штучного інтелекту працюють у межах, встановлених суспільством [8].

Усі ці заходи допомагають мінімізувати ризики, пов'язані з безпекою даних, і забезпечити їх конфіденційність відповідно до етичних стандартів і законодавства.

Висновки

Захист конфіденційності даних і запобігання дискримінації при використанні штучного інтелекту є ключовими аспектами, які вимагають не тільки суворого дотримання правил і норм, але й впровадження відповідних механізмів контролю. Прозорість і підзвітність у процесах штучного інтелекту також відіграють ключову роль.

Користувачі повинні мати розуміння того, як використовуються їхні дані, а рішення, прийняті на основі штучного інтелекту, повинні бути перевіреними. Щоб відповідати вимогам захисту даних, необхідна відповідність законодавству, наприклад Загальному регламенту захисту даних (GDPR).

Постійне навчання співробітників і адаптація політики захисту даних до мінливого середовища є невід'ємними елементами забезпечення безпеки. Технічні та організаційні заходи, такі як шифрування даних і керування доступом, є важливими для ефективного захисту інформації. Готовність до змін законодавства та технологій важлива для оперативного реагування на нові загрози та вимоги.

Одним із основних напрямків є удосконалення криптографічних методів, що включає розробку нових і вдосконалення існуючих технологій для забезпечення більш надійного захисту даних. Ще одним важливим напрямком є розширення додатків технології блокчейн, яка може підвищити прозорість і надійність зберігання даних шляхом створення децентралізованих і захищених від втручання систем запису даних.

Важливим кроком є мінімізація потоку даних, що полягає у зборі лише необхідної інформації. Шифрування даних під час зберігання та передачі разом із регулярними аудитами та моніторингом систем допоможе запобігти несанкціонованому доступу та виявити потенційні вразливості.

Слід також розглянути інтеграцію принципів «захист даних за проєктом» і «захист даних за замовчуванням» на ранніх стадіях розробки системи та продукту. Співпраця з експертами з безпеки, забезпечення технічної підтримки та регулярне оновлення програмного забезпечення також відіграють вирішальну роль у забезпеченні безпеки даних.

Комплексний підхід до використання штучного інтелекту, що включає технічні, етичні, правові та освітні аспекти, необхідний для забезпечення справедливого та відповідального використання технологій і захисту даних на всіх рівнях.

Застосування цих рекомендацій допоможе організаціям створити більш надійну систему захисту даних і використовувати штучний інтелект більш відповідально та безпечно.

1. Security Challenges and Solutions in AI-Enabled Systems. URL: https://www.propulsiontechjournal.com/ (accessed: 15.07.2024). **2.** Ethical Considerations in AI Data Privacy. Int J Artif Intell Ethics. URL: https://www.researchgate.net/ (accessed: 15.07.2024). **3.** AI Solutions and Privacy: Overcoming Common Challenges & Committing to Responsible AI URL: https://www.itmagination.com/ (accessed: 15.07.2024). **4.** Privacy-Preserving Techniques for Data Sharing in AI Applications. URL: https://ieeexplore.ieee.org/ (accessed: 15.07.2024). **5.** Securing Data in AI Systems: Challenges and Solutions. URL: https://ieeexplore.ieee.org/ (accessed: 15.07.2024). **6.** Emerging Challenges and Opportunities in AI Data Privacy and Security. URL: https://www.researchgate.net/ (accessed: 15.07.2024). **7.** Privacy and Security Challenges in the Era of Artificial Intelligence. URL: https://www.researchgate.net/ (accessed: 15.07.2024). **8.** Advances in Cryptography for Data Privacy in AI Systems. https://ieeexplore.ieee.org/ (accessed: 15.07.2024).

REFERENCES:

1. Security Challenges and Solutions in AI-Enabled Systems. URL: https://www.propulsiontechjournal.com/ (accessed: 15.07.2024). **2.** Ethical Considerations in AI Data Privacy. Int J Artif Intell Ethics. URL: https://www.researchgate.net/ (accessed: 15.07.2024). **3.** AI Solutions and Privacy: Overcoming Common Challenges & Committing to Responsible AI URL: https://www.itmagination.com/ (accessed: 15.07.2024). **4.** Privacy-Preserving Techniques for Data Sharing in AI Applications. URL: https://ieeexplore.ieee.org/ (accessed: 15.07.2024). **5.** Securing Data in AI Systems: Challenges and Solutions. URL: https://ieeexplore.ieee.org/ (accessed: 15.07.2024). **6.** Emerging Challenges and Opportunities in AI Data Privacy and Security. URL: https://www.researchgate.net/ (accessed: 15.07.2024). **7.** Privacy and Security Challenges in the Era of Artificial Intelligence. URL: https://www.researchgate.net/ (accessed: 15.07.2024). **8.** Advances in Cryptography for Data Privacy in AI Systems. https://ieeexplore.ieee.org/ (accessed: 15.07.2024).

Bachyshyna L. D., Candidate of Economics (Ph.D.), Associate Professor, Kasperska A. O., Senior Student (National University of Water and Environmental Engineering, Rivne, l.d.bachyshyna@nuwm.edu.ua ; kasperska_ak20@nuwm.edu.ua)

INFLUENCE OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES ON INFORMATION SECURITY AND CONFIDENTIALITY

The article describes in detail the methods of information protection and considers the principles of digital protection that are relevant in the times of rapid development of artificial intelligence technologies. The research examined the main types of cybersecurity breaches that are likely to be encountered on the network. It's no secret that artificial intelligence is penetrating various aspects of human life every day and is a useful tool that can help automate existing processes, make new decisions, analyze and predict action scenarios. Wider use means an increase in the amount of data collected, which, in turn, carries risks and dangers related to security and privacy.

Although artificial intelligence has simplified human activity in many ways, its use does not eliminate the need to comply with digital security rules. The final part of the publication contains preventive

measures that will help protect personal information from leakage and reduce the risks of cyberattacks.

***Keywords*: artificial intelligence; cybersecurity; cyber protection; information security; user authentication; digital literacy.**