

Етичні та безпекові аспекти використання ШІ

Використання штучного інтелекту в робочому середовищі вимагає розуміння критичних аспектів безпеки та відповідальності. Навіть просте завантаження документа може мати серйозні наслідки для працівника та організації.

КОЖИНА Алла - голова ГО «Інститут громадських стратегій», доктор наук з державного управління, професор, тренер з цифрової грамотності, ШІ та кібергігієни



Правило "Червоної папки": Що ніколи не можна вантажити в ШІ



Категорично заборонено передавати:

- **Персональні дані бенефіціарів** – імена, паспортні дані, адреси, контакти
- **Автентифікаційні дані** – паролі, токени доступу, ключі шифрування
- **Непублічні фінансові звіти** – звітність, бюджети, прогнози
- **Внутрішні документи** – стратегії, договори, протоколи зустрічей
- **Клієнтські бази даних** – контактна інформація, історія взаємодії

❏ **⚠ Важливо:** Передача таких даних сторонньому сервісу – пряме порушення політики інформаційної безпеки, режиму конфіденційності та умов NDA.

Юридичні наслідки передачі конфіденційних даних

Дисциплінарна відповідальність

Від офіційної догани до розірвання трудового договору за порушення внутрішніх політик компанії

Матеріальна відповідальність

Відшкодування збитків, заподіяних компанії внаслідок витоку інформації

Кримінальна відповідальність

За розголошення комерційної таємниці – якщо інформація офіційно має такий статус

Чи є це розголошенням комерційної таємниці?

Так, якщо одночасно виконуються три умови: інформація офіційно визнана комерційною таємницею компанії, працівник знав або мав знати про її конфіденційний статус, та передача відбулася без попереднього дозволу керівництва. Важливо розуміти: наявність чи відсутність умислу впливає на ступінь відповідальності, але не звільняє від неї повністю.



Має значення, який саме AI-сервіс ви використовуєте



Публічні AI-сервіси

Приклади: безкоштовна версія ChatGPT, Claude, Gemini

Ризик: Високий – дані можуть зберігатися та використовуватися для навчання моделі. Історія запитів може бути доступна іншим користувачам через витоки.

Рекомендація: Не використовувати для робочих завдань із конфіденційною інформацією



Корпоративні AI-рішення

Приклади: ChatGPT Team/Enterprise, Microsoft Copilot для бізнесу, Google Workspace AI

Захист: Політики нерозголошення, дані не використовуються для навчання моделі, додаткове шифрування

Важливо: Навіть у цьому випадку працівник зобов'язаний дотримуватися внутрішніх правил компанії та не передавати дані без дозволу

Що робити, якщо ви вже передали конфіденційні дані?



Негайно повідомте керівництво

Зверніться до безпосереднього керівника або служби інформаційної безпеки. Це буде розцінено як добросовісна поведінка та може пом'якшити наслідки.



Вивчіть внутрішні політики

Детально ознайомтеся з політиками компанії щодо використання AI-інструментів та обробки конфіденційної інформації.



Зверніться до підтримки AI-сервісу

Надішліть запит на видалення конкретного чату або даних. Збережіть підтвердження звернення – це документує вашу спробу мінімізувати ризики.



Застосовуйте анонімізацію надалі

У майбутньому завжди видаляйте або замінюйте імена, цифри, назви клієнтів та іншу ідентифікуючу інформацію перед аналізом.

Галюцинації ШІ та авторське право: критичні ризики

● Чому штучний інтелект "бреше"

ШІ-моделі генерують контент на основі ймовірностей, а не фактів. Це призводить до "галюцинацій" – впевнено сформульованої, але неправдивої інформації.

Як перевіряти:

- Завжди верифікуйте факти через незалежні джерела
- Перевіряйте посилання та цитати – ШІ часто їх вигадує
- Критично оцінюйте статистичні дані та цифри
- Використовуйте cross-check кількома AI-моделями

© Кому належить контент, створений ШІ

Питання авторського права на AI-контент залишається юридично неврегульованим у більшості країн.

Ключові моменти:

- ШІ може непередбачувано генерувати фрагменти захищеного контенту
- Компанія може нести відповідальність за плагіат
- Завжди перевіряйте унікальність згенерованого тексту
- Документуйте процес створення контенту



Практичне завдання: Анонімізація даних

Вихідний текст

Грантова заявка для Іванченка Петра,
паспорт ME123456, проживає в м. Харків,
вул. Сумська 1, телефон +38050123456,
email: ivanchenko@example.com
Сума гранту: 250,000 грн

Анонімізований варіант

Грантова заявка для [Бенефіціар 1],
паспорт [ДОКУМЕНТ-001], проживає в
[Місто А], вул. [Вулиця Х] [Номер],
телефон [ТЕЛЕФОН-1],
email: [EMAIL-1]
Сума гранту: [СУМА-1] грн

Мікро-завдання на 1 хвилину

Інструмент: Notepad / Word (локально, без підключення до інтернету)

Завдання: Переписати будь-який робочий документ так, щоб його можна було безпечно відправити в AI-сервіс. Замініть всі ідентифікуючі дані на умовні позначення: імена → [Особа 1], [Особа 2]; міста → [Локація А]; номери → [ID-001]; суми → [ЗНАЧЕННЯ-Х].

