Додаток

**Рекомендації**

**для громадян щодо безпечного використання онлайн-сервісів зі штучним інтелектом**

Штучний інтелект (ШІ) – потужний інструмент, що відкриває нові можливості для навчання, роботи та творчості. Як і будь-яка інша технологія, він вимагає відповідального та обережного підходу. Щоб захистити вашу особисту та конфіденційну інформацію, дотримуйтесь цих правил:

**1.⁠ ⁠Ніколи не вводьте конфіденційні дані**

Це найголовніше правило. Не надавайте чат-ботам жодної чутливої інформації. До такої інформації належить:

▪️персональні дані: ПІБ, дата народження, ідентифікаційний код (РНОКПП), паспортні дані, адреса проживання;

▪️фінансова інформація: номери банківських карток, паролі до інтернет-банкінгу, дані про рахунки;

▪️медичні дані: діагнози, результати аналізів, історія хвороби;

▪️облікові дані: логіни, паролі, секретні запитання від будь-яких сервісів;

▪️корпоративна таємниця: службові документи, дані про клієнтів, фінансові звіти компанії, внутрішня документація.

Пам'ятайте: вся введена інформація зберігається на серверах компанії-розробника та може бути використана для тренування моделі.

**2.⁠ ⁠Усвідомлюйте ризики функції «Поділитися» (Share)**

Функція створення посилання на діалог робить вашу розмову публічною. Не використовуйте цю функцію для обміну чутливою інформацією. Розглядайте таке посилання як публікацію в інтернеті – її може побачити будь-хто.

Якщо ви ділитеся посиланням, переконайтеся, що в діалозі немає жодних даних, які могли б скомпрометувати вас чи інших людей.

**3.⁠ ⁠Перевіряйте налаштування приватності.**

Сучасні ШІ-сервіси (наприклад, ChatGPT) дозволяють керувати своєю приватністю. Зайдіть у налаштування та перевірте такі опції:

▪️історія чатів (Chat History): Ви можете вимкнути збереження історії діалогів. У такому разі ваші розмови не будуть зберігатися та використовуватися для навчання моделі;

▪️використання даних для тренування: Деякі сервіси надають можливість заборонити використання ваших даних для вдосконалення ШІ.

**4.⁠ ⁠Використовуйте анонімізацію даних**

Якщо вам потрібно обговорити з ШІ певну ситуацію, що стосується реальних даних, замініть їх на вигадані або узагальнені.

Неправильно: «Проаналізуй фінансовий звіт ТОВ «Мрія» за кодом ЄДРПОУ 12345678».

Правильно: «Проаналізуй фінансовий звіт уявної компанії з такими показниками: дохід – X, витрати – Y. Які можна зробити висновки?»

**5.⁠ ⁠Уникайте використання ШІ для роботи з документами, що мають гриф обмеження доступу**

Категорично заборонено завантажувати або вставляти в чат-боти службові, таємні чи будь-які інші документи з обмеженим доступом. Це створює пряму загрозу національній та корпоративній безпеці.

**6.⁠ ⁠Будьте обережні з розширеннями для браузерів.**

Існує багато сторонніх плагінів, які нібито розширюють можливості ШІ-сервісів. Встановлюйте розширення лише з офіційних магазинів (Chrome Web Store, Firefox Add-ons) та від перевірених розробників. Ненадійні плагіни можуть перехоплювати всі дані, які ви вводите.

**ІНФОРМАЦІЙНИЙ ЛИСТ**

Шановні колеги!

Останнім часом у медіапросторі з’явилася інформація про індексацію пошуковими системами, зокрема Google, розмов користувачів із популярними сервісами на основі штучного інтелекту, такими як ChatGPT та Grok. Важливо розуміти, що йдеться не про злам систем чи витік даних у прямому сенсі, а про наслідки використання функції «Поділитися» (Share).

Коли користувач створює публічне посилання на свою розмову, цей діалог стає доступним для будь-кого, хто має це посилання. Якщо таке посилання публікується на відкритих ресурсах (форумах, соціальних мережах, блогах), пошукові роботи можуть його знайти та проіндексувати.

У зв'язку з цим та загальним зростанням популярності ШІ-інструментів, Держспецзв'язку надав громадянам рекомендації щодо безпечного використання таких сервісів (додаються).

Начальник служби

захисту інформації Наталія САВІНОВА

**Кібербезпека в епоху ШІ: як захистити свої дані при використанні онлайн-чатботів**

[Новини](https://cip.gov.ua/ua/filter?tagId=49651)19.08.2025 09:00