***Модуль:* Захист персональних даних**

Практична вправа:
«Перевірка факту компрометації персональних даних»

Навчальна мета заняття: пересвідчитись у відсутності або наявності витоку власних автентифікаційних даних.

Час проведення: 1 год. *Місце проведення:* комп'ютерний клас.

Устаткування:
персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі Інтернет, обліковий запис в системі генеративного штучного інтелекту, веб-браузер, ChatALL (https://github.com/sunner/ChatALL).

Порядок проведення заняття

Увійти в обліковий запис Google. З використанням ресурсу https://takeout.google.com замовити відомості про персональні дані, прив'язані до облікового запису, які зберігає Google. Оцінити отримані результати.

За адресами https://haveibeenpwned.com, https://monitor.firefox.com перевірити наявність власних поштових облікових записів у витоках даних. Повторити попереднє завдання з використанням ресурсу leakpeek.com.

У випадку виявлення облікових записів у витоках терміново змінити паролі на відповідних ресурсах та, за можливості, налаштувати двофакторну автентифікацію.

Авторизуватись на сайті ChatGPT chat.openai.com. Спробувати змінити роль машини в системі штучного інтелекту (flowgpt.com).

Спробувати згенерувати запит для пошуку своїх персональних даних в мережі Інтернет. Наприклад: «Напиши якісний Google dork для пошуку моїх персональних даних в мережі Інтернет. Мене звати ...».

Спробувати згенерувати запит щодо назв ресурсів, які містять витоки даних. Наприклад: «Напиши перелік онлайн-ресурсів для пошуку витоків даних. Залиш у переліку ті, які відображають за запитом електронною поштою паролі, що були втрачені».

Відпрацювати попередні завдання з використанням програми ChatALL (https://github.com/sunner/ChatALL) та perplexity perplexity.ai.

Сконструювати власний запит в контексті захисту персональних даних.