УДК 004.056:342.9
Олена Сміх, Руслан Козак, к.т.н., доцент
Тернопільський національний технічний університет імені Івана Пулюя

АНАЛІЗ МОЖЛИВОСТЕЙ ПЛАТФОРМ GAI ДЛЯ ГЕНЕРУВАННЯ ВИМОГ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Olena Smikh, Ruslan Kozak Ph.D., Assoc. Prof.

ANALYSIS OF THE CAPABILITIES OF GAI PLATFORMS FOR GENERATING INFORMATION SECURITY REQUIREMENTS

Інтеграція генеративного штучного інтелекту (ГШІ) (Generative Artificial Intelligence, GAI) у процес розробки програмного забезпечення привносить не лише інновації, але й дає можливість революціонізувати визначення та формулювання вимог безпеки.

Перший у світі проект регламенту щодо застосування ШІ було запропоновано у ЄС у червні 2023 року, який отримав назву EU Artificial Intelligence Act (AIA) [1]. Проект регламенту розподіляє ШІ на три різні категорії залежно від ризику, що його ШІ може становити для людей: неприйнятний ризик, високий ризик і обмежений ризик.

Відповідность моделей GAI до EU AIA було проаналізовано в [2]. Зокрема, двадцять дві вимоги акту були прокласифіковані, і з них було обрано 12 вимог, які розділені між 4 різними категоріями. Понад 90% серед доступних GAI платформ базуються на популярних моделях [3], зокрема, на GPT 3.5.

У дослідженні для з'ясування типів, особливостей та ризиків застосування ГШІ проаналізовано такі GAI платформи: ChatGPT, Bard, Claude, AI21 Studio, BLOOM. Методику проведення порівняльного аналізу згідно критеріїв, запропонованих в [2], та структуру результатів дослідження представлено у вигляді наступних таблиць:

№	Платформа	Готовність до застовування	Дата оновлення наборів даних	Відповідність до EU Artificial Intelligence Act (AIA)				Загальна оцінка
				Data	Compute	Model	Deployment	

Платформа	ChatGPT	Bard	Claude	AI21 Studio	BLOOM
Загальна оцінка	29	32	10	11	39

Оцінки для кожної із 4 категорій щодо відповідності до AIA були визначені на основі результатів аналізу GAI платформ. З метою вибору платформи GAI для генерації вимог інформаційної безпеки до програмного забезпечення, аналіз здійснено не лише на основі технічних характеристик платформ, але й з врахуванням ризиків, етичних аспектів та вимог правового регулювання.

Література

1. Regulating generative AI. Towards Data Science. [Електронний ресурс]/ Sweenor, D – 4 серпня 2023 – Режим доступу до ресурсу: https://towardsdatascience.com/regulating-generative-ai-e8b22525d71a

2. EU AI Act. [Електронний ресурс]/ Center for Responsible AI at Stanford University – 15 червня 2023 – Режим доступу до ресурсу: https://crfm.stanford.edu/2023/06/15/eu-ai-act.html

3. Announcing AI21 Studio and Jurassic-1. [Електронний ресурс]/ AI21 Labs – 7 червня 2023 – Режим доступу до ресурсу: https://www.ai21.com/blog/announcing-ai21-studio-and-jurassic-1