

РОЗРОБКА НАВЧАЛЬНОЇ СИСТЕМИ ДЛЯ ЗБОРУ ПЕРСОНАЛЬНИХ ДАНИХ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ ТА СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

DEVELOPMENT OF A TRAINING SYSTEM FOR COLLECTING PERSONAL DATA USING AI AND SOCIAL ENGINEERING

Сучасні конфлікти, зокрема війна між Україною та Росією, демонструють, що кіберпростір стає одним із ключових фронтів. Збір персональних даних через соціальну інженерію та їх використання для інформаційних атак став важливим інструментом агресора. Розробка навчальних систем із використанням штучного інтелекту допоможе не лише дослідити ці методи, але й підготувати фахівців для протидії таким загрозам [1].

Штучний інтелект пропонує нові інструменти для збору та аналізу персональних даних, але водночас створює виклики, пов'язані з етикою та конфіденційністю. Навчальні системи, що симулюють сценарії соціальної інженерії, дозволяють зрозуміти поведінкові моделі та розробити механізми захисту. Це особливо актуально для країн, які перебувають у зоні геополітичної нестабільності, як Україна [2].

Актуальність теми зумовлена масштабним використанням соціальної інженерії для маніпуляції громадською думкою, збору конфіденційної інформації та проведення інформаційних операцій. В умовах війни, такі дії можуть мати катастрофічні наслідки для безпеки держави. Навчальні системи на основі штучного інтелекту допоможуть моделювати реальні загрози, формувати критичне мислення та вдосконалювати розуміння стосовно цього. Україна вже кілька років стикається з інформаційними атаками, що є частиною гібридної війни з Росією. Розуміння механізмів збору даних допоможе протистояти таким загрозам [3].

Основна робота зосереджена на створенні телеграм-бота, який імітує один із можливих методів збору інформації для соціальної інженерії. Telegram є популярним месенджером в Україні, що робить його ефективним середовищем для моделювання потенційних загроз і навчання користувачів реагувати на них. Цей бот демонструє вразливість до фішингових атак і навчає користувачів розпізнавати загрози. За допомогою цього бота, також можна продемонструвати анонімний збір персональних даних користувачів.

Сучасний світ дедалі більше залежить від цифрових технологій, що робить суспільство вразливим до атак, які використовують персональні дані. Тому запропонована модель демонстрації загрози має високий потенціал для вивчення цієї теми та в подальшому використанні методів захисту на основі запропонованого навчального бота.

Література

1. Roles and Implications of AI in the Russian-Ukrainian Conflict URL: Warfare <https://www.cnas.org/publications/commentary/roles-and-implications-of-ai-in-the-russian-ukrainian-conflict>.
2. RAND Corporation URL: <https://www.rand.org/pubs/commentary/2022/11/ukraines-lessons-for-the-future-of-hybrid-warfare.html>.
3. Oxford Academic. URL: <https://academic.oup.com/book/56111/chapter-abstract/442747673?redirectedFrom=fulltext&login=false>.