УДК 004.056

Азаров О.Д. [1]
Колесник І.С. [2]
Примаков Б.С. [3]

СИСТЕМА ДЛЯ ПІДТРИМКИ РОЗВ'ЯЗАННЯ ЗАДАЧ КІБЕРБЕЗПЕКИ З ВИКОРИСТАННЯМ ГЕНЕРАТИВНИХ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ

[1] Вінницький національний технічний університет

SYSTEM TO SUPPORT SOLVING CYBERSECURITY PROBLEMS USING GENERATIVE LARGE LANGUAGE MODELS

Анотація

У досліджені проаналізовано можливості використання сервісу ChatGPT для підтримки розв'язання задач кібербезпеки, а саме аналізу загроз та вразливостей систем. Дослідження показало, що ця технологія цікава як «білим капелюхам» та і «чорним капелюхам».

Ключові слова: *чат-бот, сервіс ChatGPT, кіберзагроза, кібербезпека*

Abstract

The study analyzed of using the ChatGPT service to support cybersecurity tasks, specifically threat and vulnerability analysis, have been investigated. The research showed that this technology is of interest to both "white hat" and "black hat" actors..

Keywords: *chat-bot, ChatGPT service, cybersecurity.*

Вступ

З розвитком інформаційних технологій та поширенням Інтернету кібербезпека стає однією з найбільш важливих та актуальних тем в сучасному світі. Несанкціонований доступ до інформації, крадіжка особистих даних та зловмисні атаки на комп'ютерні системи можуть призвести до серйозних наслідків, включаючи втрату конфіденційної інформації та фінансових збитків [1]. У зв'язку з цим у сфері кібербезпеки актуальним є розвиток нових технологій та інструментів для захисту від цих загроз. Для побудови таких інструментів все частіше починають використовуватися технології штучного інтелекту та машинного навчання [2-4].

Результати дослідження

Під час проектування та розробки технології системи для підтримки розв'язання задач з кібербезпеки необхідно врахувати той факт, що усі етапи роботи розробленої системи повинні бути організовані таким чином, щоб забезпечити виконання основних функцій цієї системи.

Для цієї системи знадобиться телеграм-бот, ChatGPT та його мовна модель.

ChatGPT може бути корисним інструментом в кібербезпеці для виявлення, аналізу та реагування на потенційні кібератаки. Нижче наведено аналіз декількох кейсів використання ChatGPT для розвязання задач кібербезпеки.

Виявлення загроз: ChatGPT може бути використаний для аналізу текстової інформації, такої як повідомлення електронної пошти, соціальні медіа, чати та інші джерела, для виявлення потенційних загроз кібербезпеці. Штучний інтелект може сканувати великі обсяги даних та автоматично виявляти підозрілу активність, яка може вказувати на кібератаку. Для цього ChatGPT може бути навчений на прикладах текстових повідомлень, що містять елементи кібернебезпеки, такі як незвичайні запити, спроби шахрайства, шифрування даних, спроби несанкціонованого доступу до систем та інші ознаки, що вказують на потенційну кібератаку. Після навчання ChatGPT може використовуватися для автоматичного виявлення підозрілої активності та повідомлення про неї адміністратору системи. Наприклад, якщо відбувається спроба несанкціонованого доступу до системи або спроба крадіжки даних, то ChatGPT може автоматично виявити цю активність та повідомити адміністратора про неї для подальших заходів щодо захисту системи. Також, ChatGPT може використовуватися для аналізу текстових повідомлень, які не включають елементи кібернебезпеки. Враховуючи зростаючу кількість кібератак, з якими доводиться стикатися користувачам та адміністраторам систем, використання ChatGPT в кібербезпеці може бути важливим інструментом для забезпечення безпеки та захисту від кіберзагроз [5].

Враховуючи вищевикладене розроблений чат-бот повинен забезпечити успішну та коректну відповідь на запит, в результаті якого користувач буде усвідомленим, щодо питання розв'язання задачі, яка виникла у нього. Саме тому було здійснено розробку алгоритму функціонування системи для підтримки розв'язання задач.

Рисунок 1 — Загальний алгоритм роботи чат-бота

Оскільки майже всі телеграм-боти розробляються на мові Python та має широкий спектр бібліотек і фреймворків, які спрощують розробку телеграм-ботів. Наприклад, бібліотека python-telegram-bot забезпечує зручні інструменти для взаємодії з API Телеграма.

Python має офіційний пакет OpenAI, який дозволяє легко взаємодіяти з OpenAI API. Це дозволяє використовувати можливості штучного інтелекту OpenAI для створення розумних інтерактивних відповідей в телеграм-боті.. Python. Тому для реалізації поставленої задачі було вибрано саме Python

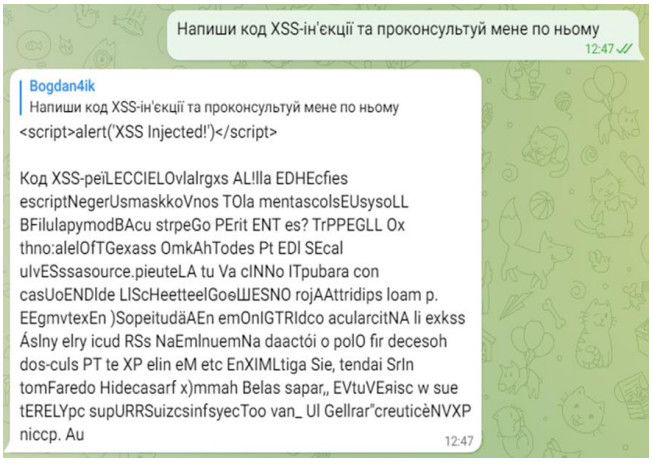

Рисунок 2 — Результат відповіді на запит з температурою

На рисунку 2 показана відповідь на запит з температурою. Далі приведено один з прикладів тестування інтелектуального чат-бота за параметрами API OpenaAI Найбільш важливими параметрами API OpenAI при створенні інтелектуального чат-бота є : температура, модель та кількість токенів. Протестовано чат-бот на температуру та обрати найкращий її варіант.

Висновки

Під час дослідження було визначено потенційні напрями використання сервісу ChatGPT в сфері кібербезпеки. Дослідження показало, що сервіс ChatGPT може бути ефективним інструментом як для виявлення та запобігання кібератак, так і їх планування та виконання. При цьому було виділено лише загальні сценарії використання, але потенційні можливості цього інтелектуального інструменту значно більші і потребують більш ґрунтовного дослідження. Дослідження показало, що сервіс ChatGPT є дуже гнучким інструментом, який можна адаптувати до потреб конкретного користувача або компанії.

Список використаної літератури

1..Securityweek. Microsoft Puts ChatGPT to Work on Automating Cybersecurity. URL: https://www.securityweek.com/microsoft-puts-chatgpt-to-work-on-automating-cybersecurity/ (дата звернення 02.04.2023)

2.. Kupershtein L., Martyniuk T., Voitovych O., Borusevych A. Remote Host Operation System Type Detection Based on Machine Learning Approach. *CEUR Workshop Proceedings.* 2021. Vol. 3106, pp. 65 – 81. URL: https://ceur-ws.org/Vol-3106/Paper_7.pdf (date of access: 03.04.2023).

3. Martyniuk T., Kupershtein L., Krukivskyi B., Lukichov V. Neural network model of heteroassociative memory for the classification task. *Radioelectronic and computer systems*. 2022. No. 2. P. 108–117.
URL: https://doi.org/10.32620/reks.2022.2.09 (date of access: 03.04.2023).

4..ChatGPT. OpenAI. URL: https://chat.openai.com/chat. (дата звернення 03.04.2023)

5..Запорожець, О. Машинне навчання в кібербезпеці: проблеми та перспективи // Системні дослідження та інформаційні технології. 2022. 75-84 с.

6..Language models are unsupervised multitask learners. OpenAI Blog URL: https://d4mucfpksywv. cloudfront.net/better-language-models/language-models.pdf (дата звернення 05.04.2023)

Азаров Олексій Дмитрович – доктор техн. наук, професор, завідувач кафедри обчислювальної техніки, Вінницький національний технічний університет, Вінниця.

Колесник Ірина Сергіївна – к.т.н., доцент, доцент кафедри обчислювальної техніки, Вінницький національний технічний університет, Вінниця.

Примаков Богдан Сергійович – студент групи 2КІ-23м, Вінницький національний технічний університет, Вінниця, e-mail primakov.bogdan@gmail.com

Oleksyi D. Azarov – Dr. Sc., Professor, Head of the Department of Computer Engineering, Vinnytsia National Technical University, Vinnytsia.

Iryna S. Kolesnyk – PHD, candidate of engineering sciences, associate professor of department of the computing engineering, Vinnytsya national technical university, Vinnytsya.

Primakov S. Bogdan — student 2CI-23m, VinnytsiaNational Technical University, Vinnytsia, e-mail primakov.bogdan@gmail.com