УДК 004.49

М.В. Головань[1], к.т.н. В.О. Гнатюк[1,2]
([1]Національний авіаційний університет, [2]Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації, Україна)

Інтеграція месенджерів з ШІ у діяльність авіаційного підприємства для підвищення рівня кібербезпеки

Використання віртуальних помічників є актуальним і перспективним напрямком підвищення рівня кібербезпеки та ефективного реагування на потенційні кіберзагрози у сучасних авіаційних підприємствах. З огляду на це, метою даної роботи є організаційно-технічне забезпечення кібербезпеки за допомогою віртуального помічника, який може значно підвищити рівень безпеки в організаціях та знизити ризики кібератак.

Використання віртуальних помічників є актуальним і перспективним напрямком підвищення рівня кібербезпеки та ефективного реагування на потенційні кіберзагрози у сучасних авіаційних підприємствах [1-10].

Опис функціоналу месенджерів з ШІ включає базові можливості, а також може бути доопрацьований. Серед основних можливостей варто виділити:

1. Повідомлення про кіберзагрози (бот може надсилати повідомлення про останні кіберзагрози та інформувати користувачів про нові види атак або вразливості, що виявлені).

2. Навчання користувачів (бот може надавати короткі інструкції або поради з кібербезпеки, допомагаючи користувачам уникати загроз і захищати свої дані).

3. Моніторинг систем КБ (бот може підключатися до систем моніторингу кібербезпеки та надсилати повідомлення про будь-які аномалії або підозрілі активності). Це можуть бути системи виявлення кіберінцидентів (SIEM - Security Information and Event Management), які допомагають виявляти та відстежувати підозрілі активності в комп'ютерних системах та мережах. Ось кілька з них: Splunk: Splunk - це платформа SIEM, яка забезпечує централізований збір, індексацію та аналіз журналів подій з різних джерел, що дозволяє виявляти кіберзагрози та використовувати розумні аналітичні можливості для виявлення аномалій. IBM QRadar: QRadar від IBM - це інша платформа SIEM, яка надає розширені засоби виявлення загроз, включаючи аналіз потоків даних, кореляцію подій та виявлення вразливостей. ArcSight: ArcSight від Micro Focus - це ще одна популярна платформа SIEM, яка дозволяє аналізувати та реагувати на кіберінциденти в реальному часі, а також вести журнал інцидентів та здійснювати аудит безпеки. Elastic Security: Elastic Security (раніше відомий як Elastic SIEM) - це відкрита та розширювана платформа SIEM, яка базується на відомій системі Elasticsearch та надає інтегрований набір інструментів для виявлення та відстеження кіберінцидентів. LogRhythm: LogRhythm - це інша популярна платформа SIEM, яка забезпечує комплексний аналіз журналів подій, виявлення аномалій та автоматизовану реакцію на кіберзагрози.

Ці системи надають широкий спектр функціональності для виявлення, аналізу та реагування на кіберінциденти, що дозволяє організаціям підтримувати високий рівень кібербезпеки.

Узагальнюючи, інтеграція телеграм-бота до систем виявлення кіберінцидентів може полегшити та покращити процеси моніторингу та реагування на кіберзагрози, забезпечуючи більш ефективну та оперативну роботу з безпекою.

4. Запитання та відповіді (бот може відповідати на питання користувачів про кібербезпеку та надавати поради щодо захисту особистої інформації та пристроїв).

5. Повідомлення про підозрілі активності (користувачі можуть надсилати боту звіти про будь-які підозрілі активності або атаки, і бот може надати відповідні рекомендації щодо подальших кроків).

Зважаючи на можливості сучасних месенджерів з ШІ запропоновано схему розробки месенджерів з ШІ для автоматизації організаційно-технічного забезпечення КБ в авіаційному підприємстві зображена на рис. 1.

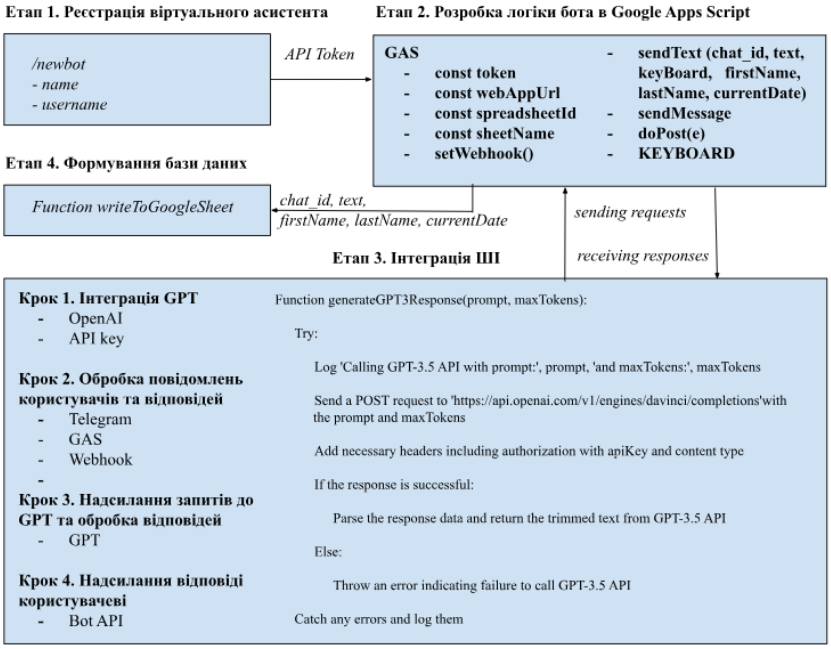

Рис. 1. Схема розробки месенджерів з ШІ для автоматизації організаційно-технічного забезпечення КБ в авіаційному підприємстві

Таким чином, розроблене рішення для автоматизації організаційно-технічного забезпечення КБ в авіаційному підприємстві. Основні можливості включають: повідомлення про кіберзагрози, навчання користувачів,

моніторинг систем КБ, відповіді на запити користувачів щодо КБ, повідомлення про підозрілі активності тощо.

Це загальні особливості розробленого рішення, яке поєднує в собі ефективну комунікацію з користувачами через месенджер, розширення можливостей генерації відповідей за допомогою ШІ, та ефективне управління та аналіз даних через GAS.

Список літератури

1. Al-Riyami, S., & Al-Hinai, S. (2020). A Framework for Automating Cybersecurity Tasks Using Telegram Bots. In International Conference on Cyber Security and Protection of Digital Services (pp. 187-197). Springer, Cham.
2. Gupta, B., & Singhal, A. (2020). Cybersecurity Awareness Enhancement through Telegram Bot. In Emerging Technologies in Computing and Communication (pp. 43-52). Springer, Singapore.
3. Al-Safi, A., & Al-Hinai, S. (2021). A Framework for Responding to Cyber Incidents Using Telegram Bots. In International Conference on Cyber Security and Protection of Digital Services (pp. 235-246). Springer, Cham.
4. A.S. Al-Hammadi, S.A. Al-Jarrah, A.A. Al-Saffar, A.H. Al-Hammadi. "Cybersecurity Awareness Enhancement Using Telegram Chatbot". 2020 IEEE 10th International Conference on Information and Communication Systems (ICICS), 2020, pp. 188-193.
5. S.R. Chinnaswamy, A.V. Vasudevan. "A Survey of Chatbots for Cybersecurity Education". 2020 International Conference on Emerging Trends in Information Technology and Engineering (ICETITE), 2020, pp. 1-6.
6. M.A. Al-Hussein, A.A. Al-Saffar, A.H. Al-Hammadi. "A Framework for Cybersecurity Incident Response Using Telegram Chatbots". 2021 2nd International Conference on Computer Science and Artificial Intelligence (CSAI), 2021, pp. 1-6.
7. Гнатюк В.О., Бондаренко І.О., Каплун І.С. Використання систем обміну миттєвими повідомленнями для автоматизації надання консультативних послуг. Реєстрація, зберігання і обробка даних. Т 23. № 4. 2021. С. 58-67.
8. Гнатюк В.О., Батрак О.Г., Яроцький С.В. Автоматизована система реєстрації місцезнаходження працівника // Проблеми інформатизації та управління: Збірник наукових праць: Випуск 2 (74). К.: НАУ, 2023. С.14-20.
9. Гнатюк В.О., Батрак О.Г., Скуратівський А.А., Кудренко С.О. Метод оптимізації роботи системи масового обслуговування з використанням віртуального асистента на базі штучного інтелекту // Проблеми інформатизації та управління: Збірник наукових праць: Випуск 3 (75). К.: НАУ, 2023. С.21 -28.
10. Shead, Sam. Why everyone is talking about the A.I. text generator released by an Elon Musk-backed lab. CNBC. https://ramaonhealthcare.com/why-everyone-is-talking-about-the-a-i-text-generator-released-by-an-elon-musk-backed-lab/.