

# Organizational and technical support of cyber security using a virtual assistant

Viktor Gnatyuk<sup>1,2,\*</sup>, Oleh Batrak<sup>1,†</sup>, Roman Hamretskyi<sup>1,†</sup> and Mykhailo Golovan<sup>1,†</sup>

<sup>1</sup> National Aviation University, Liubomyra Huzara Ave. 1, Kyiv, 03058, Ukraine

<sup>2</sup> State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, Maksym Zalizniak Str., 3/6, Kyiv, 03142, Ukraine

## Abstract

In today's digital world, where cyberattacks are becoming increasingly complex and widespread, the importance of effective organizational and technical support for cybersecurity is growing. In this context, the use of virtual assistants is a relevant and promising approach for enhancing cybersecurity levels and effectively responding to potential cyber threats. Considering this, the purpose of this work is to provide organizational and technical support for cybersecurity using a virtual assistant, which can significantly increase security levels in organizations and reduce the risks of cyberattacks. The work has developed a solution for organizational and technical support of cybersecurity using a virtual assistant. Key capabilities include cyber threat reporting, user training, monitoring of cybersecurity systems, responding to user inquiries about cybersecurity, reporting suspicious activity, and more.

## Keywords

cyber security, virtual assistant, telegram bot, artificial intelligence, google apps script

## 1. Introduction

In today's digital world, where cybersecurity (CS) threats are becoming increasingly complex and widespread, the importance of effective organizational and technical CS support is growing. In this context, the use of virtual assistants (VAs) (e.g., Telegram Bot) is a relevant and promising approach for enhancing security levels and effectively responding to potential threats [1, 2]. Key aspects that highlight the relevance of this approach include:

- Threat notifications: VAs can provide timely alerts about new threats and vulnerabilities, enabling quick responses and appropriate measures to prevent or eliminate them.
- User training: VAs can serve as a tool for training staff on internet security, identifying suspicious situations, and timely response, thereby improving the organization's overall CS.
- Security system monitoring: VAs can automatically monitor security systems and provide reports on their status, detected anomalies, and potential threats, aiding in prompt responses to potential incidents.
- Automated response mechanisms: VAs can utilize automated means to respond to threats, such as blocking suspicious IP addresses, disabling compromised accounts, etc., which reduces response time and risks for the organization.
- Q&A: VAs can serve as a convenient channel for users to ask questions about CS and receive timely answers and recommendations on information protection.


---

*CH&CMiGIN'24: Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, January 24–27, 2024, Kyiv, Ukraine*

\* Corresponding author.

† These authors contributed equally.

✉ viktor.hnatiuk@npp.nau.edu.ua (V. Gnatyuk); oled.batrak@npp.nau.edu.ua (O. Batrak); hamretskyi@gmail.com (R. Hamretskyi); 2199038@stud.kai.edu.ua (M. Golovan)

 0000-0002-4916-7149 (V. Gnatyuk); 0000-0002-7983-8118 (O. Batrak); 0000-0001-5514-9783 (R. Hamretskyi); 0009-0002-4146-5210 (M. Golovan)



© 2025 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

- Suspicious activity notifications: VAs can analyze user and system activities, identify suspicious behavior patterns, and provide alerts about possible threats, helping to prevent serious security breaches.

Given the above, the aim of this work is to provide organizational and technical CS support using VAs, which can significantly enhance security levels in organizations and reduce the risk of cyberattacks.

## 2. Analysis of modern scientific research

The review of contemporary scientific literature on the use of VAs for organizational and technical CS support allows identifying the following features: in works [3, 4], VAs are used for task automation; scientific papers [5, 6] describe the use of VAs (Telegram Bot) for enhancing user awareness; in works [7, 8], VAs are used for responding to cyber incidents. Based on the analysis results, it is worth noting that the use of VAs for organizational and technical CS support is a relevant scientific and technical task that enables task automation, improves user awareness, and automates the response to cyber incidents. Therefore, further development of this topic is extremely important.

However, besides the advantages of using VAs, there are several disadvantages, including:

- Vulnerability to cyberattacks: VAs can be compromised by hackers, leading to the theft of confidential data, the spread of malware, and disruption of VA operations.
- Ineffectiveness: VAs may not always effectively identify cyber threats, such as phishing attacks, fraud, and sophisticated cyberattacks.
- Functional limitations: VAs cannot perform complex CS tasks, such as cyber incident investigation, data analysis, and CS policy development and implementation.
- Need for human oversight: VAs require human oversight for setup and configuration, information updates, and problem resolution.
- Risk of abuse: VAs can be used for spreading misinformation, conducting cyberattacks, and committing fraud.
- Imperfections of language models: The language models used in VAs can misinterpret user requests, provide inaccurate or incomplete information, and generate texts that do not match the context.
- Platform dependency: VAs depend on the platform they operate on (Telegram), which can lead to operational failures, API changes, and platform shutdowns.
- Need for user training: Users need to be trained on how to properly use VAs, understand VA limitations, and recognize fraud.
- Privacy issues: VAs collect user data, which can lead to data misuse, loss of privacy, and unauthorized data access.
- High cost: The development and implementation of VAs can be costly, time-consuming, and complex.

Therefore, the use of VAs for organizational and technical CS support must take into account their advantages and disadvantages.

## 3. Automation of organizational and technical cybersecurity support using VAs

The description of VA functionality includes basic features and can also be further developed. Among the main features are:

1. **Cyber Threat Notifications:** The bot can send notifications about the latest cyber threats and inform users about new types of attacks or vulnerabilities that have been identified.
2. **User Training:** The bot can provide short instructions or tips on cybersecurity, helping users avoid threats and protect their data.
3. **CS System Monitoring:** The bot can connect to cybersecurity monitoring systems and send notifications about any anomalies or suspicious activities. These can be cybersecurity incident detection systems (SIEM - Security Information and Event Management) that help detect and track suspicious activities in computer systems and networks. Here are some examples:
  - **Splunk:** Splunk is a SIEM platform that provides centralized collection, indexing, and analysis of event logs from various sources, allowing the detection of cyber threats and utilizing intelligent analytics to identify anomalies.
  - **IBM QRadar:** IBM's QRadar is another SIEM platform that offers advanced threat detection tools, including data flow analysis, event correlation, and vulnerability detection.
  - **ArcSight:** ArcSight from Micro Focus is another popular SIEM platform that enables real-time analysis and response to cyber incidents, as well as incident logging and security auditing.
  - **Elastic Security:** Elastic Security (formerly known as Elastic SIEM) is an open and extensible SIEM platform based on the well-known Elasticsearch system, providing an integrated set of tools for detecting and tracking cyber incidents.
  - **LogRhythm:** LogRhythm is another popular SIEM platform that provides comprehensive event log analysis, anomaly detection, and automated response to cyber threats.

These systems offer a wide range of functionalities for detecting, analyzing, and responding to cyber incidents, enabling organizations to maintain a high level of cybersecurity. Connecting a Telegram bot to incident detection systems can be appropriate and useful, as it improves communication and interaction with security personnel and other stakeholders.

Here are some advantages of this approach: rapid notification and response (the Telegram bot can send notifications about detected cyber incidents or suspicious activities in real-time, allowing prompt responses to threats and taking necessary security measures), convenient access to information (security personnel can use the Telegram bot to access information about the system's security status, event logs, and analytical data from anywhere with internet access), personnel training (the Telegram bot can provide short training materials and cybersecurity instructions, enhancing the awareness and competence of personnel in cybersecurity), interactive interaction (personnel can use the Telegram bot to communicate with the incident detection system, request additional information, or perform actions to ensure effective analysis and response to incidents), mobility and flexibility (the Telegram bot can be used from any device that supports the Telegram messenger, allowing security personnel to stay informed about the security status even outside the office or in mobile conditions).

4. **Q&A:** The bot can answer user questions about cybersecurity and provide advice on protecting personal information and devices.
5. **Suspicious Activity Notifications:** Users can send reports of any suspicious activities or attacks to the bot, and the bot can provide appropriate recommendations for further actions.

In summary, integrating a Telegram bot into incident detection systems can ease and improve the processes of monitoring and responding to cyber threats, ensuring more effective and timely security operations.

## 4. Development of VA

To develop a VA for automating organizational and technical cybersecurity support, it is necessary to choose tools, a platform, and perform the following stages.

### 4.1. Stage 1. Registration of VA

This stage involves registering a Telegram bot and obtaining the necessary access and keys for interacting with the Telegram API. To register a VA, it is necessary to choose a platform. Based on the research in works [9–11], we will choose the Telegram instant messaging system as an example.

### 4.2. Stage 2. Development of bot logic in Google Apps Script

At this stage, the logic of the bot is developed using Google Apps Script (GAS), which will allow processing user messages, interacting with external services, and sending responses to users. When developing a Telegram bot, we will use Google Apps Script (GAS), which is a scripting platform developed by Google for creating lightweight web applications on the Google Workspace platform (Figure 1). GAS projects run on Google's server-side infrastructure. According to GAS, it "provides easy ways to automate tasks across Google products and third-party services." GAS is also a tool for writing extensions for Google Docs, Sheets, and Slides.

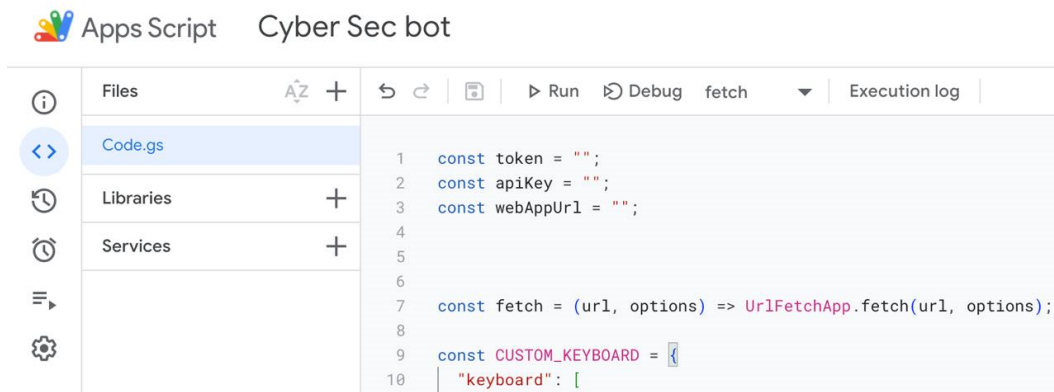


Figure 1: GAS platform.

On the GAS platform, create a new project where we define variables such as token (the Telegram bot token used to communicate with the Telegram API), webAppUrl (the URL of the web application used as a webhook (Figure 2) for receiving incoming messages from Telegram; a webhook is a method of augmenting or extending the functionality of a webpage or web application with custom callbacks), and apiKey (for connecting AI). Additional variables can be created as needed, for example, spreadsheetId (the identifier of the Google Sheet where data will be stored), sheetName (the name of the sheet in the Google Sheet where Telegram chat messages will be logged), etc.

When developing the Telegram bot, we use the following functions:

- setWebhook(): Sets the webhook for the Telegram bot using the Telegram API.
- sendText(chat\_id, text, keyBoard, firstName, lastName, currentDate): Sends a text message to the user using the sendMessage method of the Telegram API. The function parameters include:
  - chat\_id: Chat identifier,
  - text: Message text,
  - keyBoard: Keyboard to display,
  - firstName: User's first name,
  - lastName: User's last name,
  - currentDate: Current date/time.

- doPost(e): This function handles incoming HTTP requests sent by the web application, receives data about the incoming message from Telegram, parses it, and logs the necessary data into a Google Sheet.
- KEYBOARD\_1, KEYBOARD\_2: Objects representing keyboards (Figure 3) for display in the Telegram chat, containing rows and buttons that can be clicked to interact with the bot.

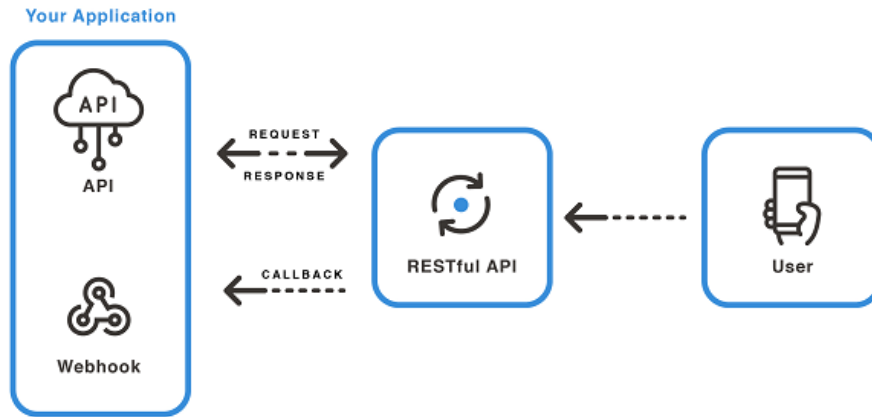


Figure 2: Webhook method.

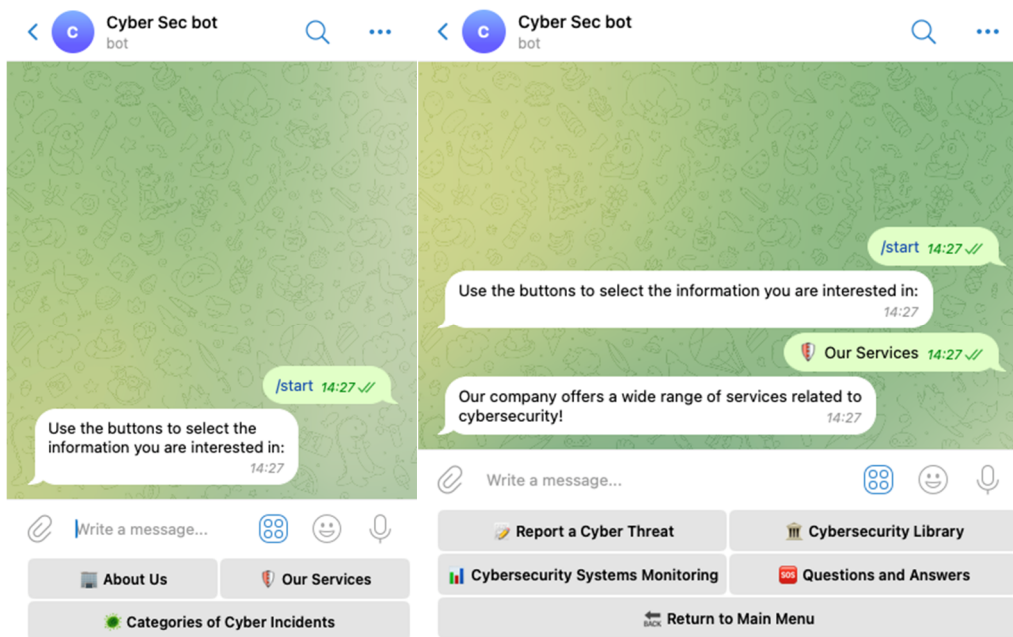


Figure 3: Cyber security bot keyboards.

### 4.3. Stage 3. Integration of artificial intelligence into a Cyber security bot

At this stage, we integrate artificial intelligence, specifically GPT, to enhance the functionality of the bot. For user assistance, we use GPT-3 (Generative Pre-trained Transformer 3), which is an autoregressive language model that uses deep learning to generate human-like text (Figure 4). By drawing from a large text dataset, Chat GPT uses this dataset to learn about language, grammar, structure, and the meaning of words and sentences. This enables it to understand the context and intent of user queries and generate appropriate responses. It is the third-generation language prediction model in the GPT-n series, created by OpenAI, an AI research lab in San Francisco [12]. It is also possible to perform pre-training of the AI based on documentation provided to Chat GPT.

To use GPT to assist users in the Telegram bot and connect it to GAS, several steps need to be taken:

1. Step 1. Integration of GPT. Obtain access to the service that provides GPT, such as OpenAI GPT-3, and obtain an API key. Use the key in GAS to interact with GPT by sending requests and receiving responses.
2. Step 2. Processing user messages and responses. After receiving a message from the user through Telegram webhooks, process the message by extracting the necessary information.
3. Step 3. Sending requests to GPT and processing responses. Create a request to GPT, including the user's message text or other necessary information. Receive the response from GPT and process it for further use.
4. Step 4. Sending a response to the user. Develop the logic that will send the processed response to the user in Telegram via the Bot API.

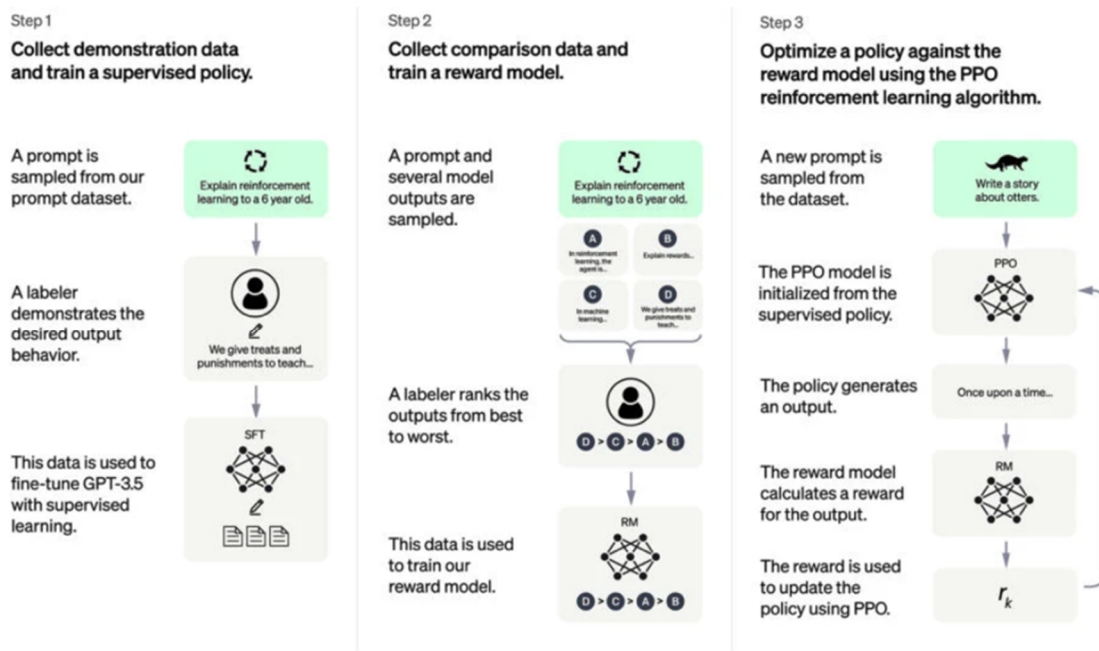


Figure 4: Chat GPT training model.

#### 4.4. Stage 4. Database formation

To form the database, data will be recorded in Google Sheets (writeToGoogleSheet) using the `writeToGoogleSheet` function, which is responsible for recording user data and their requests to Google Sheets.

Development scheme of AI-based VA for automating organizational and technical cybersecurity support (Figure 5).

General pseudocode of the software interacting with users through the Telegram bot, using GAS to process messages, OpenAI GPT-3 to generate responses, and Google Sheets to store user chats.

Listing 1: Google Apps Script pseudocode

```
const token = "TOKEN";
const apiKey = 'OPENAI_API_KEY';
const webAppUrl = "GOOGLE_APPS_SCRIPT_WEB_APP_URL";

function setWebhook() {
  // Call the Telegram API to set the webhook to the URL of our web app
}

async function generateGPT3Response(prompt, maxTokens) {
```



```

// Call the OpenAI GPT-3 API using the provided prompt and token count
// Receive and return the generated response
}

function sendText(chat_id, text, keyBoard) {
  // Call the Telegram API to send a message with the provided text and keyboard
}

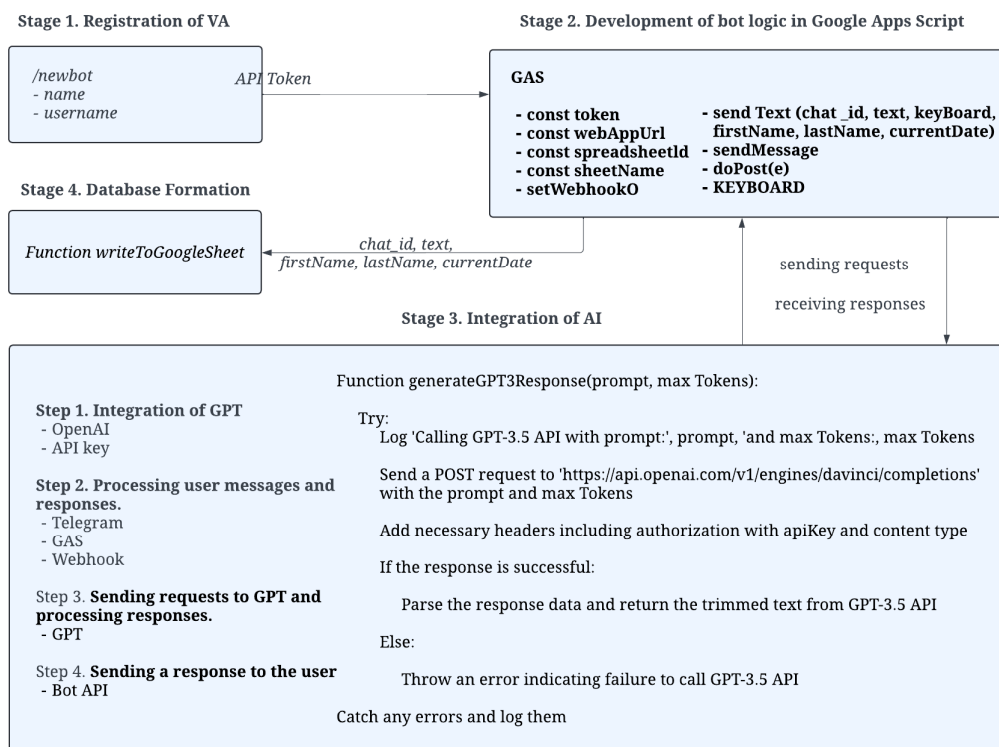
function writeToGoogleSheet(chat_id, text) {
  // Access the Google Sheet
  // Log the chat with the user and the message in the Google Sheet
}

function doPost(e) {
  // Receive the message from the user
  // Process the received message and generate a response
  // Send the generated response to the user
  // Log the chat with the user and the message in the Google Sheet
}

setWebhook();

```

This is the general logic of the program code that allows the bot to interact with the user via Telegram, call the GPT-3.5 API to generate responses, and log information about users and their queries in Google Sheets (Figure 5).



**Figure 5:** AI-based virtual assistant development scheme for automating organizational and technical cybersecurity support.

## 5. Conclusions

Thus, the developed solution for organizational and technical cybersecurity support using a VA includes the following main features: notifications about cyber threats, user training, CS system monitoring, responses to user queries regarding CS, notifications about suspicious activities, and more.

These are the general features of the developed solution, which combines effective communication with users through the VA, enhanced response generation capabilities using AI, and efficient data management and analysis through GAS.

## Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

## References

- [1] A. Zaporozhets, V. Babak, V. Isaienko, K. Babikova, Analysis of the air pollution monitoring system in Ukraine, *Studies in Systems, Decision and Control* 298 (2020) 85–110. doi: 10.1007/978-3-030-48583-2\_6.
- [2] Y. Averyanova, et al., UAS cyber security hazards analysis and approach to qualitative assessment, In: S. Shukla, A. Unal, J. Varghese Kureethara, D.K. Mishra, D.S. Han (Eds.), *Data science and security*, volume 290 of *Lecture Notes in Networks and Systems*, Springer, Singapore, 2021, pp. 258–265. doi: 10.1007/978-981-16-4486-3\_28.
- [3] S. Al-Riyami, S. Al-Hinai, A framework for automating cybersecurity tasks using telegram bots, in: *Proceedings of International Conference on Cyber Security and Protection of Digital Services*, Springer, Cham, 2020, pp. 187–197.
- [4] A. S. Al-Hammadi, S. A. Al-Jarrah, A. A. Al-Saffar, A. H. Al-Hammadi, Cybersecurity awareness enhancement using telegram chatbot, in: *Proceedings of IEEE 10th International Conference on Information and Communication Systems (ICICS)*, 2020, pp. 188–193.
- [5] B. Gupta, A. Singhal, Cybersecurity awareness enhancement through telegram bot, in: *Proceedings of Emerging Technologies in Computing and Communication*, Springer, Singapore, 2020, pp. 43–52.
- [6] S. R. Chinnaswamy, A. V. Vasudevan, A survey of chatbots for cybersecurity education, in: *Proceedings of International Conference on Emerging Trends in Information Technology and Engineering (ICETITE)*, 2020, pp. 1–6.
- [7] A. Al-Safi, S. Al-Hinai, A framework for responding to cyber incidents using telegram bots, in: *Proceedings of International Conference on Cyber Security and Protection of Digital Services*, Springer, Cham, 2021, pp. 235–246.
- [8] M. A. Al-Hussein, A. A. Al-Saffar, A. H. Al-Hammadi, A framework for cybersecurity incident response using telegram chatbots, in: *Proceedings of 2nd International Conference on Computer Science and Artificial Intelligence (CSAI)*, 2021, pp. 1–6.
- [9] V. O. Hnatyuk, I. O. Bondarenko, I. S. Kaplun, Using instant messaging systems for automating the provision of advisory services, *Registration, Storage and Data Processing* 23 (2021) 58–67.
- [10] V.O. Hnatyuk, O.H. Batrak, S.V. Yarotskyi, Automated Employee Location Registration System, *Problems of Informatization and Management* 2(74) (2023) 14–20.
- [11] V. O. Hnatyuk, O. H. Batrak, A. A. Skurativskyi, S. O. Kudrenko, Method for optimizing the operation of a mass service system using a virtual assistant based on artificial intelligence, *Problems of Informatization and Management* 3(75) (2023) 21–28.
- [12] S. Shead, Why everyone is talking about the A.I. text generator released by an Elon Musk-backed lab, *CNBC*, 2023. URL: <https://ramaonhealthcare.com/why-everyone-is-talking-about-the-a-i-text-generator-released-by-an-elon-musk-backed-lab>.