American Academic Scientific Research Journal for Engineering, Technology, and Sciences
ISSN (Print) 2313-4410, ISSN (Online) 2313-4402
https://asrjetsjournal.org/index.php/American_Scientific_Journal/index

Using AI Assistants to Enhance Information Security Efficiency

Sergei Beliachkov*

Head of Department, Platform Cybersecurity Center, JSC Sberbank-Technologies, Moscow, Russia
Email: belyaserg@gmail.com

Abstract

This article explores the potential of deploying virtual AI assistants to strengthen information security in light of the rapid evolution of digital technologies and the growing complexity of cyber threats. The study addresses the organizational aspects of implementing AI-based solutions—including threat notifications, user training, monitoring, and analytics—and the technical integration of such assistants with existing information security systems. This includes practical steps such as registering Telegram bots, leveraging Google Apps Script, and integrating with the OpenAI API. Special attention is given to challenges and limitations, such as technical vulnerabilities, false positives, ethical and legal considerations, and functional constraints in complex scenarios. The methodology is grounded in a review of findings from related studies. Results indicate that the integration of innovative AI-driven solutions holds strong potential for advancing the field of information security. Future research should focus on improving Explainable AI algorithms, enhancing the protection of transmitted data, and developing a regulatory framework to support such systems' safe and ethical use. The insights presented in this article will be of particular interest to cybersecurity professionals, researchers, and systems architects focused on the development and deployment of AI-powered approaches for improving threat detection and mitigation mechanisms in information security.

Keywords: information security; AI assistant; artificial intelligence; cybersecurity; technical integration; organizational aspects; Explainable AI; Telegram bot; Google Apps Script; OpenAI.

1. Introduction

In the context of rapidly advancing digital technologies and the increasing sophistication of cyberattacks, the issue of enhancing information security (hereafter, IS) is more pressing than ever. Currently, 5.78 billion people—equivalent to 70.5% of the global population—use mobile phones.

Received: 4/20/2025
Accepted: 6/1/2025
Published: 7/14/2025

---

* Corresponding author.

Over the past 12 months alone, the number of unique subscribers grew by 112 million (a 2.0% year-over-year increase), with smartphones now accounting for nearly 87% of all mobile devices. Simultaneously, as of early 2025, the Internet reaches 5.56 billion users (67.9% of the global population), reflecting an annual increase of 136 million (+2.5%). However, 2.63 billion people remain offline. According to the latest report from Kepios, more than 5.24 billion people (63.9%) now use social media, with the user base growing by 206 million in the past year alone (+4.1%). This scale of connectivity demands that organizations implement high-precision analytics platforms and automated response systems to rapidly detect and mitigate cyber threats across global network infrastructures [12].

One promising direction is the deployment of artificial intelligence (AI)-based assistants, which can not only automatically alert users to suspicious activity but also support incident response operations. These systems help reduce the time required to identify and resolve security incidents, enhancing the overall resilience of cybersecurity infrastructures [1, 2].

Research on the use of AI assistants in cybersecurity reveals a multifaceted approach to integrating artificial intelligence into threat detection and response, as illustrated in a range of contemporary publications. One area of development involves interactive agents—including chatbots—designed to raise user awareness and enable rapid incident handling. For instance, Gnatyuk V. and his colleagues [2] propose both organizational and technical frameworks for implementing virtual assistants that improve cybersecurity processes within corporate environments. Similarly, studies by Al-Hammadi A. S., Al-Jarrah S. A., Al-Saffar A. A., Al-Hammadi A. H. [4], and Al-Safi A., Al-Hinai S. [5] explore the use of Telegram messenger bots to increase cyber threat awareness and establish responsive incident management workflows. These efforts showcase how AI technologies can be embedded into everyday user interactions, effectively reducing the influence of human error in threat assessment and mitigation.

Another vital direction involves using AI for risk analysis, threat evaluation, and anomaly detection. The work of Binhammad M. and his colleagues [1] focuses on digital identity protection, offering a methodology aimed at preventing identity spoofing and unauthorized access. Averyanova Y. and his colleagues [3] provide a structured approach to threat analysis within unmanned aerial systems, emphasizing the importance of holistic vulnerability assessment. Khinvasara T., Ness S., and Tzenios N. [7] examine risk management in the context of medical devices, where precise risk assessment is critical to patient safety, while Abdelkhalek M., Ravikumar G., and Govindarasu M. [10] demonstrate the use of machine learning to detect anomalies in smart grid communications, marking a shift from conventional methods toward more adaptive and dynamic threat detection systems.

Several studies highlight the synergistic potential of artificial intelligence when combined with other emerging technologies. The work of Ness S., Shepherd N. J., and Xuan T. R. [6] explores the integration of AI and robotics in the development of comprehensive automated cybersecurity systems, where enhanced robotic capabilities enable rapid threat response. In a related line of inquiry, Xuan T. R. and Ness S. [8] examine the fusion of blockchain technologies with AI, paving the way for decentralized digital security systems and increased trust in information infrastructures.

Another area of growing interest is the impact of generative AI and the development of new tools for analyzing and forecasting cyber threats. Gupta M. and his colleagues [9] discuss the evolution of generative models from general-purpose systems like ChatGPT to specialized applications such as ThreatGPT, which are designed not only to analyze but also to anticipate emerging threats, potentially generating novel attack vectors. Li Z. and his colleagues [11] propose constructing domain-specific knowledge graphs based on cyber threat intelligence reports, offering a structured and in-depth framework for analyzing the technical dimensions of cyber threats.

It is also worth noting that the statistical data referenced in this section is drawn from source [12], with details available via the DataReportal website.

The literature review reveals inconsistencies in approaches to AI adoption within cybersecurity. On one hand, there is a growing interest in deploying intelligent chatbots and virtual assistants to enhance user responsiveness and awareness. On the other hand, there is a rising demand for high-quality risk assessment and anomaly detection—areas where traditional methods increasingly give way to adaptive AI systems. Moreover, current discussions emphasize the integration of AI with blockchain and robotics, reflecting an interdisciplinary search for optimal solutions. However, there is no consensus on the efficacy or applicability of these integrations across different economic sectors. Issues related to the scalability of such systems and their integration into existing infrastructures remain underexplored, as do the ethical and legal implications of AI deployment in critical sectors, highlighting the need for further study and theoretical elaboration.

This study aims to analyze the potential of AI assistants to improve the organizational and technical support of information security systems.

The novelty of the research lies in its comprehensive approach, combining organizational and technical aspects of information security through the implementation of virtual AI assistants—a subject that has not yet been thoroughly examined. The study proposes a methodological framework for integrating these assistants into cybersecurity monitoring systems, with an emphasis on current demands for speed and precision in threat response.

The central hypothesis is that integrating AI assistants into corporate information security infrastructures—provided they are correctly configured and regularly updated—can significantly reduce detection and response times for cyber threats while alleviating the workload of security personnel. This hypothesis will be tested through a comparative analysis of system performance with and without AI assistant support during simulated cyber incidents.

The methodology is based on a review and analysis of findings from prior research in this field.

2. Organizational Aspects of Using AI Assistants in Information Security

The use of AI assistants in information security (IS) represents a comprehensive organizational and technical solution aimed at enhancing both the speed of threat detection and the overall resilience of corporate information systems. Studies by Binhammad M. and his colleagues [1] and Gnatyuk V. and his colleagues [2]

show that virtual assistants, such as Telegram bots, can be integrated into existing monitoring and alerting systems, while also supporting user training and operational analytics. As such, the deployment of AI assistants is emerging as a key area in the modernization of IS practices within contemporary enterprises.

One of the primary functions of an AI assistant is to automate and integrate information flows between threat detection systems and end users. Virtual assistants can perform the following key tasks:

- Threat notification. AI assistants can automatically distribute alerts about new vulnerabilities, detected incidents, and suspicious activity. This reduces response times and helps minimize the impact of attacks [2].
- Training and awareness. Assistants can provide concise guidelines and security tips, as well as conduct interactive training sessions to improve employee awareness of IS best practices [1].
- Interactive support and feedback. AI assistants can process user inquiries, respond to security-related questions, and offer recommendations, facilitating faster resolution of incidents and improving communication within the organization.
- Monitoring and reporting. When integrated with SIEM systems (such as Splunk, IBM QRadar, and ArcSight), AI assistants can analyze data from servers, network devices, and log systems, identify anomalies, and generate actionable reports for IS leadership [2, 9].

The implementation of AI assistants in a corporate environment provides several distinct advantages:

- Reduced response time. Automated alerts enable faster mitigation of incidents, reducing potential damage and financial losses [8, 10].
- Improved training and communication. Ongoing user engagement and real-time recommendations help lower the risk of human error and promote more cohesive collaboration within IS teams.
- Seamless integration with existing infrastructure. AI assistants can be incorporated into current monitoring ecosystems, ensuring smooth interaction between different components of the security architecture and contributing to more systemic IS management [2, 4].
- Lower operational load. Automating routine tasks—such as data collection, preliminary analysis, and alert generation—frees up security personnel to focus on advanced analytics and strategic planning.

For instance, Gnatyuk V. and his colleagues [2] describe a Telegram-based virtual assistant integrated with Google Apps Script and OpenAI, which proved effective in promptly notifying employees about suspicious incidents and automating the collection and analysis of SIEM data. Meanwhile, Binhammad M. and his colleagues [1] emphasize the importance of AI in improving anomaly detection accuracy and maintaining infrastructure resilience. Together, these cases demonstrate how AI assistants contribute not only to technical improvements but also to organizational refinement in cybersecurity operations.

To summarize the functional scope of AI assistants in organizational IS support, Table 1 outlines their core capabilities.

Table 1: The main functional capabilities of AI assistants in the information security system *(based on data from [2])*

Functional Capability	**Description**	**Benefits**
Threat Notification	Automated delivery of alerts regarding new threats, anomalies, and vulnerabilities	Faster response time; timely incident containment
Security Training	Providing protection guidelines and user education through interactive sessions	Increased awareness; reduced risk from human error
Interactive Support	Processing user queries and offering recommendations on security policies	Faster incident resolution; improved internal communication
SIEM Integration and Monitoring	Connecting to log and analytics systems (e.g., Splunk, IBM QRadar) for anomaly detection	Monitoring automation; early threat detection
Suspicious Activity Reporting	Gathering and analyzing suspicious behavior data for executive decision-making	Enhanced analytical capacity; proactive risk identification

The organizational implementation of AI assistants in information security shows strong potential for improving response speed, optimizing training and monitoring processes, and integrating seamlessly with existing defense infrastructures. These virtual tools support the creation of a unified information ecosystem, where user interactions and system monitoring are automated and enhanced by modern analytics. However, successful deployment requires more than technical capability—it also demands cultural change, heightened employee awareness of cybersecurity practices, and continuous quality control of AI assistant performance.

In conclusion, the integration of AI assistants into IS management contributes to strengthening organizational resilience by reducing incident response times, improving communication workflows, and optimizing decision-making. Case studies and current research in international literature point to the need for further refinement and standardization of methodologies for implementing such tools in enterprise environments.

3. Technical Integration of AI Assistants into Information Security Systems

Modern information security systems demand not only effective organizational support but also robust technical integration of automated threat monitoring tools. AI assistants—implemented via messenger bots and server-side scripts—enable the unification of monitoring, alerting, and analytical capabilities into a single platform, significantly improving the response time to cyber incidents [4]. The technical integration of such solutions involves several sequential stages, including assistant registration, message handling logic development, integration of AI-driven response generation, and the creation of a database to store interaction logs.

A fundamental element of this integration process is selecting the appropriate platform for developing and hosting the AI assistant. Message handling functions typically include:

- setWebhook(): sets the webhook for receiving requests from Telegram.
- sendText(): sends text messages to users via the Telegram API.
- doPost(): handles incoming HTTP requests from users and logs the data into Google Sheets [2, 5].

The next step is the integration of artificial intelligence. By obtaining an API key to access OpenAI GPT (or an equivalent model), the assistant sends requests to generate IS-related responses. This enables the AI assistant to engage in user dialogues, answering questions and providing context-specific recommendations [1, 6]. A key architectural element is the creation of a database to log bot interactions, which allows for activity monitoring and evaluation of the assistant's performance.

The development of an integrated AI assistant solution generally includes the following stages:

Stage 1. Registration and initial setup: register the bot with Telegram, obtain an access token, and configure the webhook. This step establishes the basic infrastructure for communication between the bot and the user [2, 9].

Stage 2. Message processing logic: using Google Apps Script, server-side logic is implemented to receive messages (doPost()), generate responses using AI APIs (generateGPT3Response()), and return messages to users via sendText(). This provides the foundation for automating IS monitoring processes [2, 6].

Stage 3. AI integration: connect to the OpenAI platform (or equivalent) via API key. The assistant sends user messages for processing and receives generated responses, which are then adapted to information security scenarios [1, 5]. This enables not only automatic response generation but also the dynamic learning of the system based on real-time data.

Stage 4. Database and analytics: a mechanism is established for logging incoming messages and AI responses in Google Sheets. This supports statistical analysis of requests and incidents. The collected data is used for iterative improvement of the assistant's accuracy in threat detection [7, 8].

The core steps of technical integration are summarized in Table 2, which outlines their functions, advantages, and associated challenges.

Table 2: The main stages of the technical integration of AI assistants into information security systems *(based on data from [2, 9, 11])*

Stage	Description	Key Functions / Components	Advantages
Registration and Setup	Creating the bot account, obtaining the token, and configuring the webhook	setWebhook(), Telegram API token	Fast initial integration; minimal setup costs
Message Handling Logic	Developing server-side logic with Google Apps Script to receive, process, and send messages	doPost(), sendText(), Apps Script functions	Automated communications; real-time data handling
AI Integration	Connecting to an AI platform (e.g., OpenAI GPT) to generate user-specific IS responses	generateGPT3Response(), GPT API integration	Relevant, automated answers; capacity for continuous learning
Database and Analytics	Logging interactions in Google Sheets for ongoing analysis and model optimization	writeToGoogleSheet(), database tools	Data-driven improvement; better threat identification and reporting over time

In summary, the technical integration of AI assistants into information security systems is a complex, multi-stage process involving bot registration, message logic development, AI model integration, and data structuring. When combined with sound organizational measures, this approach enables the automation of threat detection and response, thereby enhancing the overall security posture of information systems.

Despite challenges such as ensuring secure connections and dependency on external services, the benefits of these technologies are well-documented in recent research. As AI-driven assistants continue to evolve, their implementation offers a promising path toward more intelligent, adaptive, and responsive cybersecurity solutions.

4. Challenges, Limitations, and Development Prospects

Recent research on the use of AI assistants in information security reveals considerable potential for improving the speed and accuracy of threat detection and response. However, the integration of such technologies comes with a range of challenges and limitations that must be addressed in the development and deployment of

comprehensive protection systems for corporate IT infrastructures.

Like any software module, AI assistants may themselves become targets of cyberattacks. Vulnerabilities at the integration level—such as insecure APIs or intercepted network traffic—pose a serious threat to the integrity and confidentiality of data [2]. Furthermore, reliance on third-party services like OpenAI GPT or the Telegram API increases the risk of disruptions due to changes in policy or technical support.

The use of AI assistants in security also raises concerns about data privacy, user rights, and algorithmic transparency. The lack of Explainable AI (XAI) mechanisms complicates system auditing, which may hinder broader adoption in corporate environments [1]. At the same time, collecting and analyzing user data requires strict compliance with data protection laws and regulatory standards.

Certain high-complexity tasks in cybersecurity—such as analyzing causal chains in advanced cyber incidents or developing strategies to counter persistent threats (APT)—often demand expert intervention. Despite advances in AI, current AI assistants have limited capabilities when it comes to deep analytical reasoning and adapting to novel attack vectors.

In light of these issues, future research and development efforts are focusing on enhancing the quality and reliability of AI assistants in the cybersecurity domain. Promising directions include:

- Development of Explainable AI (XAI) techniques. The introduction of transparent algorithms will help build user trust and simplify auditing processes, enabling real-time model evaluation and correction.
- Integration with emerging technologies. Combining AI assistants with quantum computing, blockchain, and distributed storage systems may provide an added layer of security and improve infrastructure scalability. These approaches are viewed as potential solutions for reducing dependency on individual services and increasing system resilience.
- Improved adaptability and self-learning. Hybrid models that blend machine learning with expert systems can boost the precision of anomaly detection, reduce false positives, and enable more effective responses to evolving threats.
- Creation of a regulatory framework. To support the stable integration of AI assistants, it is essential to develop standards and guidelines governing data privacy, algorithmic transparency, and quality assurance in data collection [2, 4].

Table 3 summarizes the primary challenges, limitations, and future development prospects for AI assistants in information security.

Table 3: Main challenges, limitations, and prospects for the development of AI assistants in information security *(based on data from [1, 2, 4])*

Category	**Challenge / Limitation Description**	**Impact on IS Systems**	**Development Prospects**
Technical Vulnerability	Risk of system compromise via API flaws or insecure network interactions	Potential data leaks; system integrity compromise	Encryption, two-factor authentication, and regular security audits
False Positives	Errors in threat evaluation leading to incorrect alerts or missed real threats	Increased analyst workload; reduced trust in the system	Feedback-driven learning; advanced deep learning models with adaptive mechanisms
Ethical and Legal Issues	Lack of algorithmic transparency; concerns over data privacy and auditing complexity	Barriers to adoption; risks of non-compliance, and rights violations	Implementation of XAI methods; creation of data protection standards and legal norms
Functional Limitations	Difficulty adapting to new attack types; dependence on expert input in complex cases	Restricted system autonomy; reliance on human expertise	Hybrid AI–expert systems; development of predictive and self-learning capabilities

A systematic review reveals that despite the strong potential of AI assistants to enhance cybersecurity operations, their effectiveness remains constrained by several technical, organizational, and ethical issues. Core challenges include technology vulnerabilities, misidentification of threats, and limited algorithmic transparency. Future development should focus on addressing these constraints through Explainable AI, stronger data protection mechanisms, and hybrid learning models that combine machine intelligence with expert knowledge. Continued research should aim at building systems resilient to adaptive threats, refining self-learning algorithms, and establishing regulatory mechanisms that ensure the ethical and secure deployment of AI assistants in enterprise environments. Such an interdisciplinary approach is essential for shaping the next generation of information security systems—capable of responding dynamically to the complex threats of the digital era.

5. Conclusion

The analysis of organizational and technical aspects of virtual assistant integration has shown that automating processes such as alerting, training, and monitoring not only streamlines the work of information security professionals but also significantly reduces response times to threats. Nonetheless, the adoption of these technologies entails several challenges—ranging from technical vulnerabilities and false positives to legal complexities and a lack of algorithmic transparency. The identified research gap and the outlined development trajectories—including the implementation of Explainable AI, integration with quantum computing and

blockchain technologies, and the creation of unified regulatory standards—underscore the need for continued exploration in this area. This study confirms the hypothesis that a comprehensive approach to integrating AI assistants into corporate information security systems contributes to faster incident response, more effective threat analysis, and an overall improvement in data protection. The findings provide a foundation for the development of more advanced and efficient cybersecurity solutions and represent a step toward building the next generation of secure information infrastructures.

References

[1]. Binhammad M. et al. The Role of AI in Cyber Security: Safeguarding Digital Identity //Journal of Information Security. – 2024. – Vol.2 (15). – pp. 245-278.

[2]. Gnatyuk V. et al. Organizational and technical support of cyber security using a virtual assistant. – 2025. – pp.1-8.

[3]. Averyanova Y. et al. UAS Cyber Security Hazards Analysis and Approach to Qualitative Assessment //Data Science and Security: Proceedings of IDSCS 2021. – Springer Singapore, 2021. – pp. 258-265.

[4]. Al-Hammadi A. S., Al-Jarrah S. A., Al-Saffar A. A., Al-Hammadi A. H. Cybersecurity Awareness Enhancement Using Telegram Chatbot // Proceedings of IEEE 10th International Conference on Information and Communication Systems (ICICS). - 2020. - pp.188–193.

[5]. Al-Safi A., Al-Hinai S. A framework for responding to cyber incidents using telegram bots, in: Proceedings of International Conference on Cyber Security and Protection of Digital Services, Springer. - 2021. - pp. 235–246.

[6]. Ness S., Shepherd N. J., Xuan T. R. Synergy Between AI and Robotics: A Comprehensive Integration //Asian Journal of Research in Computer Science. – 2023. – Vol. 4 (16). – pp. 80-94.

[7]. Khinvasara T., Ness S., Tzenios N. Risk Management in Medical Device Industry //J. Eng. Res. Rep. – 2023. – Vol. 8 (25). – pp. 130-140.

[8]. Xuan T. R., Ness S. Integration of Blockchain and AI: Exploring Application in the Digital Business //Journal of Engineering Research and Reports. – 2023. – Vol. 8 (25). –pp. 20-39.

[9]. Gupta M. et al. From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy //IEEE Access. – 2023. – Vol. 11. – pp. 80218-80245.

[10]. Abdelkhalek M., Ravikumar G., Govindarasu M. ML-Based Anomaly Detection System for DER Communication in Smart Grid //2022 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). – IEEE. - 2022. – pp. 1-5.

[11]. Li Z. et al. AttacKG: Constructing Technique Knowledge Graph from Cyber Threat Intelligence Reports //European Symposium on Research in Computer Security. – Cham: Springer International Publishing, - 2022. – pp. 589-609.

[12]. Digital 2025: Global Overview Report. [Electronic resource] Access mode: https://datareportal.com/reports/digital-2025-global-overview-report (date of request: 04/14/2025).