In summary, Docker facilitates the easy deployment of applications into containers, ensuring their isolation and portability. Docker Swarm extends these capabilities by enabling the management of container clusters.

REFERENCES

1. Biggs J., Salanov J. Building Intelligent Cloud Applications: Develop Scalable Models Using Serverless Architectures with Azure 1st Edition. O'Reilly Media, 2019. 154 p.
2. Load Balancing in Cloud Computing, 2016. URL: https://www.researchgate.net/publication/297667.
3. Miell I. Docker in Practice, Second Edition / I. Miell, A. Hobson Sayers., 2018. – 425 c

V. Sarancha, O. Verba, A. Kutovyi

ARTIFICIAL INTELLIGENCE (AI) IN CYBERSECURITY: KEY ASPECTS AND CHALLENGES

Artificial intelligence (AI) has revolutionized the cybersecurity industry by providing advanced threat detection and prevention. This technology can help security teams counter threats more effectively by providing real-time analysis of potential threats and vulnerabilities. By detecting and eliminating security threats before they can cause damage, AI can significantly improve the overall security of an organization.

Artificial intelligence is becoming an essential tool in the fight against cyber threats, including phishing, fraud, and data theft [3]. The potential for severe losses from cybercrime has led to an increasing focus on the use of AI to protect corporate networks and data [1]. By analyzing large amounts of data, AI can detect even the slightest signs of a cyber threat and take preventive measures [3].

However, as the role of AI in cybersecurity grows, new problems arise. For example, many AI systems operate as black boxes, making the decision-making process opaque. This makes it difficult to understand what decisions are being made and why. There is also a risk of malicious attacks when attackers exploit vulnerabilities in the systems [2]. To overcome these problems, it is necessary to develop and improve the use of AI in cybersecurity actively: it is important to ensure accountability of decisions and data confidentiality in artificial intelligence systems.

In addition, the development of joint AI systems and the intersection of AI and quantum computing may be a promising area for further development of cyber-security [2].

As cybersecurity threats are constantly growing, information protection requires not only a reactive, but also a proactive approach. Modern technologies are able to detect and prevent cyber threats at an early stage and ensure reliable protection of networks and data.

The next step in the development of cybersecurity might be to increase interaction between industry, academia, and government to develop and implement new technologies and defense strategies jointly. Cooperation in this area can provide a more effective response to threats and increase resilience to cyber attacks.

Another important aspect is to train users and raise their awareness of cybersecurity. The responsibility for network and data security lies not only with information security professionals, but also with all users. Awareness and understanding of risks can significantly reduce cybersecurity threats.

Therefore, the development and use of AI in cybersecurity requires continuous improvement of technologies and methods, as well as cooperation between organizations and institutions in various industries. Continued research and innovation in this area are important to improve the effectiveness of protection against cyber threats and ensure the security of the digital space.

REFERENCES

1. Роль штучного інтелекту в кібербезпеці // Probesto Blog [Electronic resource]. – Access mode: https://www.probesto.com/ua/роль-штучного-інтелекту-в-кібербезпе/ (date of access: 08.03.2024).
2. Роль штучного інтелекту в кібербезпеці: передбачення та запобігання атакам // European Business Association [Electronic resource]. – Access mode: https://eba.com.ua/rol-shtuchnogo-intelektu-v-kiberbezpetsi-peredbachennya-ta-zapobigannya-atakam/ (date of access: 08.03.2024).
3. Shutenko V. AI in Cyber Security: Top 6 Use Cases/ *Victoria Schutenko*. – Electronic resource. – Access mode: https://www.techmagic.co/blog/ai-in-cybersecurity/ (date of access: 08.03.2024).