UDC 004.8(075)

METHODS OF TREATMENT OF COMPUTER DATA WITH THE USE OFARTIFICIAL INTELLIGENCE

D. İslamova
Mingachevir State University, Azerbaijan

Keywords: artificial intelligence, security threats, cyber attacks, web attacks, authentication.

Today, automated control systems for complex technological industries and industries are being developed in accordance with the legislative and regulato- ry framework to ensure cyber security (information security). The solution of these issues is in the focus of the management and control of companies of large enterprises, educational and scientific institutions, developers of software andhardware systems and information security systems.

The application of artificial intelligence technology in the field of cybersecurity allows you to detect attacks in detail and solve them faster than cybersecuri- ty experts. Artificial intelligence is a technology that can detect threats compared to other methods and automatically take the necessary measures to eliminate and prevent them. The following tools based on artificial intelligence meet various cybersecurity requirements:

1 Biometric authentication;
2 Timely and rapid detection of danger;
3 Quick response to attacks;
4 Creating a dynamic authentication environment;
5 Decreased human participation.

Biometric authentication - Authentication based on artificial intelligence through fingerprint and palm scan can provide secure access to the system and re- fusals. When biometric logins are associated with passwords, the likelihood of user data being compromised is significantly reduced.

Timely and rapid threat detection - conventional security systems cannot handle different types of malware at the same time. Companies use artificial intel- ligence-controlled systems that can easily detect threats through sample recogni- tion using advanced algorithms and constantly updated codes. Along with ma- chine learning, artificial intelligence is effective in analyzing the path of scanning, the micro-behavior of malware, and any malicious activity that helps you make more decisions.

Quick response to attacks - Simple detection of threats in real time does not make sense if the system is unable to deal with threats and prevent them before causing minor damage to the system. When the security team attacks the sys- tem from different points and immediately connects the points, it automatically of- fers plans to prevent the attack. SI uses intelligent analytics, which is an easier and faster approach to addressing these types of threats. For example, when the SI finds a malicious file in the system, it automatically isolates that file from the sys- tem.

Creating a dynamic authentication environment - data can also be stolen on networks. This is a concern for employees who remotely access the systems, meaning that traditional authentication models are no longer secure. This is where artificial intelligence comes in handy right now. Artificial intelligence systems use multi-factor authentication to create a dynamic authentication environment for access privileges by space or network. This includes data collection and analysis of user behavior across software, devices, and networks while remotely retrieving information.

Decreased human participation - No machine can exceed the creative potential, imagination and ability to think people. However, the decisions made by engineers are also supported by the correct views of data, opinions and current trends. Learning and using meaningful information takes a lot of time, and solving a high-risk problem is not immediately possible. When companies create a se- cure program that uses SI technology, security personnel will be deployed through automation to detect and prevent security threats without human intervention.

Thus, this method reduces engineering interference to protect information systems from a number of attacks, and at the same time increases the system's re- sistance to threats.

An overview of the state of information protection on a computer with the use of artificial intelligence allows us to draw the following conclusions:

– Artificial intelligence is resistant to modern information threats;

– It reduces the time of identification of problems and response to incidents in the information security of the activity areas, as well as the costs of personnel management.

– Operators quickly and efficiently determine the effectiveness of detection of unknown threats, as well as the analysis and detection of malicious activity in endpoints and applications.

– The proposed scheme will ensure user satisfaction and quick response to system threats.

Thus, AI systems are trained and operated by humans, and in some places human engineers are needed because they can go beyond anomalies that they can- not detect and confirm that a suspicious machine attack is real.

References

1. Tripathi, Keyur and Mubarak, Usama, Protecting Privacy in the Era of Artifi- cial Intelligence (March 24, 2020). Available at SSRN: https://ssrn.com/abstract=3560047 or http://dx.doi.org/10.2139/ssrn.35600 47

2. Hasanli X.F. Analysis of information security breaches in corporate offices. News of Azerbaijan Higher Technical Schools ISSN 1609-1620 Volume 22, No. 5(2020), 62-66.

3. Kassem AK., Arkoub SA., Daya B., Chauvet P. "A Survey of Methods for the Construction of an Intrusion Detection System", Artificial Intelligence and Ap- plied Mathematics in Engineering Problems. ICAIAME 2019. Lecture Notes on Data Engineering and Communications Technologies. Springer, Cham, pp. 211- 225, 2019, Volume 43.