Asian Journal of Technology and Applied Sciences
ISSN: 2301-xxxx (online) | IF: 10.01 | Vol: 1, issue 1
Available: http://asiansciencejournal.org

THE ROLE AND APPLICATION OF MODERN CYBER ATTACK DETECTION SYSTEMS

SAODAT RAKHMATOVA AMRAKULOVNA
Scientific supervisor: Associate Professor of the Department of Languages Samarkand branch of Tashkent University of Information Technologies Samarkand, Uzbekistan
gmail: saodatraxmatova67@gmail.com
ABDUMALIKOVA MEKHRANGIZ AKBAROVNA
Samarkand Branch of Tashkent University of Information Technologies
Student of group KI25-01
mehrangizabdumalikova006@gmail.com

Abstract: In the current era of rapidly evolving digital technologies, ensuring the security of information systems and networks has become one of the most pressing issues. The increasing number and complexity of cyber attacks intensify the need for their timely detection and mitigation. This article analyzes the role, operating principles, and practical application aspects of modern cyber attack detection systems. Furthermore, approaches aimed at improving the efficiency of attack detection systems, real-time monitoring capabilities, and their significance in early-stage threat detection are highlighted. Research results indicate that the effective use of these systems serves as a vital factor in ensuring information security.

Keywords: cybersecurity, cyber attack, intrusion detection systems, network security, threat detection, real-time monitoring.

Introduction. What is the relevance of modern cyber attacks? The current stage of human development is characterized by the rapid penetration and deep rooting of digital technologies in all spheres of social life. Today, the continuous operation of public administration, economy, finance, healthcare, and education systems has become directly dependent on the stability of information and communication technologies and global networks. However, such high development of digitalization processes brings not only wide opportunities but also serious cyber threats. Modern cyber attacks are becoming more complex every year, and their execution methods and scales are exceeding the capabilities of traditional protection systems. This has made the issue of ensuring the confidentiality, integrity, and availability of data in the global information space a priority for national security.

Currently, the methods employed by cybercriminals range from simple viral programs to complex multi-stage targeted attacks. In particular, cyber-sabotage aimed at critical infrastructure objects is assessed as a risk that could lead to catastrophic consequences for society. It should be particularly noted that cyber attacks cause not only technical system failures but also significant financial losses and reputational damage resulting from the leakage of confidential information. Under such conditions, relying solely on passive methods of protecting information systems does not yield the expected results. Therefore, applying proactive approaches in ensuring information security, specifically detecting cyber attacks at their initial stages, is of urgent importance.

Methods. In this research, complex scientific approaches were utilized to study the role and effectiveness of modern cyber attack detection systems. During the research process, theoretical and practical methods were applied in harmony, which allowed for a comprehensive and deep analysis of the topic. First, scientific literature on cybersecurity,

network security, and intrusion detection systems was studied based on theoretical analysis. International standards, scientific articles, and the works of leading experts were analyzed to clarify the theoretical foundations and development trends of cyber attack detection systems.

Furthermore, open-source intrusion detection systems were compared using comparative analysis. Their operating mechanisms, efficiency, speed, and application possibilities were studied, and the advantages and disadvantages of each system were identified. During the practical analysis, the operating principles of these systems in a real network environment were examined.

Processes of network traffic monitoring, event logging, and threat detection were studied, and their real-time effectiveness was evaluated. In addition, the general architecture of cyber attack detection systems was conceptually developed based on a modeling approach. Through this model, the operating principles of signature-based and anomaly-based detection mechanisms were explained. Using a systematic approach, the role of intrusion detection systems in the information security infrastructure was analyzed comprehensively. Their integration with other security tools and their significance in the overall protection system were revealed.

Results. At the same time, the role of artificial intelligence and machine learning methods in cyber attack detection was evaluated based on the analysis of modern technologies. This approach was explained by its ability to expand the possibilities for detecting unknown threats. Cyber attack detection systems are an integral part of modern information security architecture. These systems allow for the detection of suspicious activities and rapid response by constantly monitoring network traffic and system events. Today, great attention is paid to the integration of advanced technologies such as artificial intelligence, machine learning, and big data analysis to increase the efficiency of such systems. This, in turn, opens the way for real-time detection of even previously unknown new types of threats (Zero-day attacks). Within the framework of this article, the theoretical foundations, classification, and practical application effectiveness of modern cyber attack detection systems are deeply analyzed. Furthermore, scientific and practical recommendations on the role of these systems in ensuring network security and prospective directions for their improvement are developed. This research is intended to be a foundation for creating modern mechanisms for reliably protecting information systems from various external and internal threats.

What are the practical aspects of cyber attack detection? In the field of information security, there are not only paid and complex programs for detecting cyber attacks but also open-source systems developed by experts worldwide. Such systems are very convenient for small and medium-sized business representatives as well as specialists studying this field. They provide extensive opportunities for analyzing network traffic, detecting suspicious activities in real-time, and logging security events. Among these open-source systems, one of the most famous is Snort. It is known for its rule-based operating mechanism and has a very large user community. With its help, it is possible to perform deep analysis of network data and detect various types of attacks, such as buffer overflows or stealth port scanning.

Discussion. Another modern system is Suricata, which stands out for its multi-threaded processing capability. This allows Suricata to work effectively even in very high-speed networks and inspect large volumes of data without delays. Additionally, the Zeek system is highly valued among specialists. It is not limited to just detecting attacks but also creates a detailed archive of all events in the network. This archive later serves as a crucial source for understanding and analyzing how a cyber attack occurred. Such systems are often

used in conjunction with data visualization tools called the ELK stack, which allows security specialists to observe the network situation through convenient graphs and tables. However, one must not forget that there are specific difficulties in using these systems. Open-source systems usually do not have a graphical interface, and their correct configuration requires a high level of knowledge and experience from administrators. Also, the need for constant updates and manual entry of new attack rules may arise. Nevertheless, their flexibility and being absolutely free prompt many large companies to use these open tools as a foundation for creating their personal security systems.

In conclusion, it can be said that cyber attack detection systems are an integral part of protecting any organization's digital infrastructure in the modern world. Through them, not only are existing risks detected, but a solid foundation is created to prevent future attacks. Currently, as information technology has deeply penetrated all aspects of our lives, the issue of cybersecurity is gaining more importance than ever. Cyber attacks are becoming more complex day by day, and their scale and degree of damage are increasing. In such conditions, traditional protection methods are becoming insufficient. For this reason, cyber attack detection systems have become an integral part of modern information security. These systems constantly monitor network traffic and system activity and serve to detect suspicious actions at an early stage.

The main task of modern cyber attack detection systems is not only to stop known types of attacks but also to predict new, as-yet-unknown threats. Artificial intelligence and machine learning algorithms are of great help in this regard. With the help of these technologies, the system can distinguish a normal state from an anomalous one. For example, any activity that differs sharply from the user's usual behavior is evaluated by the system as a risk and the security service is immediately notified. This plays a decisive role in preventing data leakage and ensuring system stability.

The application of these systems covers a wide range from government organizations to large financial institutions and private enterprises. Particularly in the banking sector, their role in ensuring the security of transactions is invaluable. Also, with the development of cloud technologies and the Internet of Things, new approaches are required to combat cyber attacks. Modern detection systems are distinguished by their ability to conduct real-time analysis and respond quickly to attacks. In conclusion, building walls alone is not enough to ensure cybersecurity; using smart systems that meticulously analyze every movement within the network is an urgent requirement of today. The development of modern cyber attack detection systems is directly linked to new directions such as cloud technologies and the Internet of Things. Nowadays, as a large part of data is stored on cloud servers, protection systems are also operating in adaptation to this environment. Such systems ensure the security not only of local networks but also of users connecting from different points of the world. Especially in an era where the remote working system has become widespread, cyber attack detection technologies have gained the ability to control the behavior of each device individually.

Next-generation systems are not limited to just detecting an attack but also have the capability to respond to it automatically. In this process, the system can disconnect a suspicious user from the network or restrict the movement of malicious packets. This happens within fractions of a second without human intervention and prevents major potential damages. Also, information gathered through the systems is processed through big data analysis, allowing for the prediction of new strategies of cybercriminals in advance. At the same time, the use of intelligent agents in modern cyber attack detection systems is of significant importance. These agents move independently across the network, searching for

vulnerable points and providing recommendations on closing them. This signifies a transition from passive protection to active protection. In the future, such systems are expected to provide an even higher level of protection by harmonizing with quantum computing technologies. This applies to information at any level. Conclusion. Modern cyber attack detection systems are one of the most important pillars of ensuring information security in today's digital world. As technologies evolve, cyber attacks are also becoming more complex, and traditional protection methods often fall short in preventing such risks.

For this reason, cyber attack detection systems protect data that is vital for organizations by monitoring network traffic in real-time and immediately noticing suspicious actions. The primary role of these systems is not only to stop ongoing attacks but also to predict potential future threats and prepare against them. Modern systems, using artificial intelligence and machine learning algorithms, analyze unusual changes in the network and allow for the detection of previously unknown attack types. This creates a convenient opportunity for security specialists to identify vulnerable points in the system in advance and eliminate them.

Conclusion

In terms of practical application, these systems are being widely implemented in government institutions, the banking and finance sector, and large industrial enterprises. Along with ensuring the continuous operation of information systems, they prevent confidential information from falling into the wrong hands. Every suspicious signal detected during the monitoring process is deeply analyzed by the system, and based on these analyses, firewalls are further strengthened. In conclusion, cyber attack detection systems are an integral part of a modern cybersecurity strategy. They reliably protect digital infrastructures from external and internal threats, contributing greatly to the stable development of society and the creation of a secure environment in cyberspace. The effective operation of these systems raises the management of information flows to a new level and serves to preserve data integrity even in any complex situation.

LIST OF USED LITERATURE

1. National Institute of Standards and Technology (NIST). Guide to Intrusion Detection and Prevention Systems (IDPS). Special Publication 800-94.
2. International Organization for Standardization / International Electrotechnical Commission. ISO/IEC 27001: Information Security Management Systems, 2022.
3. European Union Agency for Cybersecurity. Threat Landscape Report, 2023.
4. SANS Institute. Intrusion Detection and Network Security Monitoring, 2021.
5. William Stallings. Network Security Essentials: Applications and Standards. Pearson.
6. Behrouz A. Forouzan. Data Communications and Networking. McGraw-Hill.