ETHIOPIAN INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

eISSN: 2349-5715 pISSN: 2349-5707

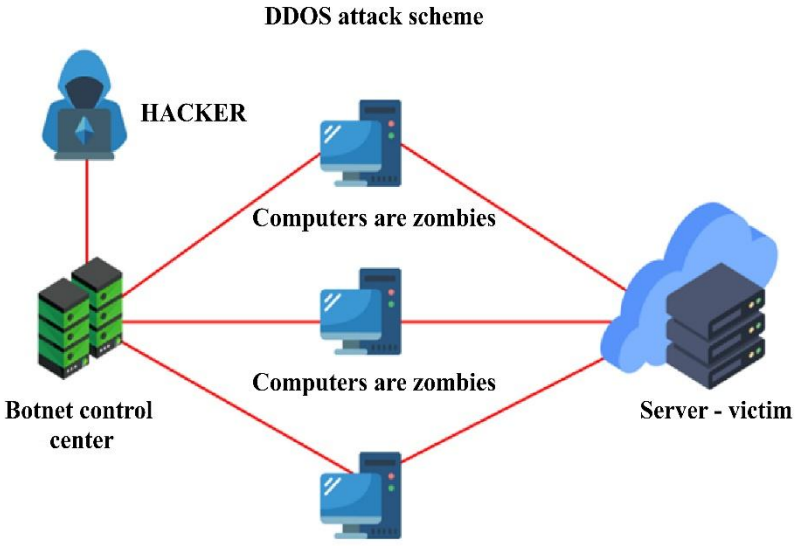
Volume: 11, Issue 12, December-2024 SJIF 2019: 4.702 2020: 4.737 2021: 5.071 2022: 4.919 2023: 6.980 2024: 7,662

Aliev Avazbek Ulugbek Ugli
Teacher at the Digital Technologies and Information Security of the Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan
Dzhamatov Mustafa Khatamovich
Teacher at the Digital Technologies and Information Security of the Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan

CYBERSECURITY IN ARTIFICIAL INTELLIGENCE

Abstract: In this article, we consider the relationship between artificial intelligence systems and cybersecurity. In modern interpretation, artificial intelligence systems are machine learning systems, sometimes this is further narrowed to artificial neural networks. The penetration of machine learning into various areas of broader applications If we talk about all information technologies, it is natural that there should be intersections with cybersecurity.
Key words: artificial intelligence, machine learning, cybersecurity.

Other known sources of cyber threats include malware (computer viruses), DDoS attacks aimed at disrupting the operation of important components of a service's infrastructure, or phishing attacks aimed at deceiving users into providing confidential information, for example, by sending emails to victims. Moreover, cyber attacks are becoming more complex and sophisticated every year. This is due not only to the development of traditional attack methods, but also to the introduction of new technologies into various areas of human life. Therefore, sometimes it turns out that cyber security services do not have time to cope with all the threats.



How AI tracks cyber threats

Artificial intelligence has become one of the most important technologies, the emergence of which has already changed and will further change many areas of human activity. Models obtained using machine learning have proven to be capable of solving many non-trivial problems that cannot be solved using a sequence of strictly defined instructions. Due to the fact that the model observes a significant amount of data during training, or, as they say, "precedents", it is able to make generalizations and identify complex relationships between various features of the input data.

Thus, cybersecurity specialists train several models on a large set of data, each of which is capable of solving its own narrow task, for example, filtering spam emails, analyzing network traffic or user

eISSN: 2349-5715 pISSN: 2349-5707

Volume: 11, Issue 12, December-2024 SJIF 2019: 4.702 2020: 4.737 2021: 5.071 2022: 4.919 2023: 6.980 2024: 7,662

behavior. And all this is based on complex relationships that the model has learned from historical data.

Artificial intelligence is actively being implemented by cybersecurity specialists for the automated detection of major threats, such as spoofing, phishing, and others. With the help of machine learning, it was possible to achieve a significant reduction in the number of false positives of such systems, while maintaining the highest level of detection. This has been very beneficial due to the increase in the amount of data used and the complexity of the attack scheme.

Another example of using AI in cybersecurity is behavioral analysis, that is, the analysis of various information about a user or employee, such as their geographic location, the time of execution of some action, device identifiers and many others, to identify anomalies in their behavior and block suspicious actions.

An important advantage of using AI in cybersecurity is its ability to predict attacks before they are fully implemented, which will help to strengthen security measures in time. Another advantage is the reduction of the human factor - artificial intelligence is not subject to various psychological influences or fatigue.

If we talk about regular security, then video surveillance using AI is being implemented quite widely. Such systems are capable of detecting multiple objects on video in real time, recognizing faces and warning security services about illegal actions.

Importance of Cybersecurity in Artificial Intelligence.

For organizations trying to succeed online today, artificial intelligence is the best cybersecurity option. To function effectively and protect their organizations from cyberattacks, security professionals need the help of advanced technologies such as intelligent machines and artificial intelligence [1].

Cybersecurity experts are actively implementing artificial intelligence to automatically detect major threats such as spoofing, phishing, etc. With the help of machine learning, the number of false positives for such systems can be significantly reduced while maintaining the highest detection rate. This provides great benefits due to the increased amount of data used and the complexity of the attack scheme.

The Importance of Cybersecurity in the Modern World.

Cybersecurity is the protection of computers, networks, software applications, critical systems, and data from potential digital threats. Organizations are responsible for maintaining data security to maintain customer trust and comply with regulatory requirements. They implement cybersecurity measures and use specialized tools to protect sensitive data from unauthorized access and prevent disruptions to business operations caused by unwanted network activity. Organizations ensure cybersecurity by optimizing digital protection methods for employees, processes, and technology.

Cybersecurity is a growing field that deals with the protection of computer networks and personal data. The job of a cybersecurity specialist is to ensure that businesses, governments, and individuals are protected from hackers, viruses, and other threats to their digital security.

It is difficult to overstate the importance of cybersecurity in the modern world. It is important because cybersecurity measures are designed to protect confidential data, personal health information, intellectual property, government and industry information systems—everything that is stored and operated using information technology—from being stolen and subsequently used for malicious purposes.

Common Cyber Threats and Vulnerabilities.

eISSN: 2349-5715 pISSN: 2349-5707

Volume: 11, Issue 12, December-2024 SJIF 2019: 4.702 2020: 4.737 2021: 5.071 2022: 4.919 2023: 6.980 2024: 7,662

No matter how many security measures a company takes against the growing number of cybercrimes, vulnerability to invisible threats remains. Therefore, companies must have a security incident response plan in place in the event of an attack. Such planning will allow management to limit the damage from a security breach and effectively remediate the situation.

Since cybersecurity attacks are constantly evolving, no security measure can be 100% foolproof. This is why cyber resilience, which entails improved precautions to mitigate the effects of cyber attacks, comes in handy. After all, even in adverse conditions such as a compromised cyber attack, you still need to resume business operations by doing everything possible to limit the damage and create value. In addition, you will be in a better position to know how best to counter a cyber attack in the future.

Cyber attacks evolve as technology advances. Attackers use new tools and invent new strategies to gain unauthorized access to systems. Organizations are adopting and improving cybersecurity measures to keep up with new and evolving technologies and digital attack tools.

Best practices for protecting your digital assets.

Most importantly, cloud computing will protect your company's data with automated backups and world-class security measures. Cloud application developers are large companies that conduct extensive research and investment in ensuring the security of their products for your company to use.

Data security protects data in motion and at rest with reliable storage and secure data transfer. Developers use security measures such as encryption and isolated backups to ensure operational resiliency against potential data security breaches. In some cases, developers use the AWS Nitro system to ensure storage privacy and restrict operator access.

BIBLIOGRAPHY:

1. ИИ компьютеры переопределил в https://www.technologyreview.com/2021/10/22/1037179/ai-reinventing-computers/
2. Applications for artificial intelligence in Department of Defense cyber missions https://blogs.microsoft.com/on-the-issues/2022/05/03/artificial- intelligence-department-of-defense-cyber-missions/
3. Information Security Analysts https://www.bls.gov/ooh/computer-and- information-technology/information-security-analysts.htm
4. Cybersecurity Workforce Study https://www.isc2.org/News-and- Events/Press-Room/Posts/2021/10/26/ISC2-Cybersecurity-Workforce- Study-Sheds-New-Light-on-Global-Talent-Demand
5. Kouliaridis, Vasileios, and Georgios Kambourakis. "A comprehensive survey on machine learning techniques for android malware detection." Information 12.5 (2021): 185.
6. AV-Test Institute https://www.av-test.org/en/statistics/malware/
7. ML malware detection for https://scholar.google.com/scholar?q=ml+for+malware+detection&hl=e n&as_sdt=0,5
8. Yuan, Zhenlong, et al. "Droid-sec: deep learning in android malware detection." Proceedings of the 2014 ACM conference on SIGCOMM. 2014.