

DOI: <https://doi.org/10.36719/2789-6919/44/205-208>

Nazilə Rəhimova

Azərbaycan Dövlət Neft və Sənaye Universiteti

<https://orcid.org/0000-0002-0942-7882>

ragimova.n.a@gmail.com

Rəhilə Salamova

Azərbaycan Dövlət Neft və Sənaye Universiteti

magistrant

<https://orcid.org/0009-0008-7599-6291>

rehileshefiyeva95@gmail.com

Süni intellektin kiber təhlükəsizlikdə tətbiqi və riskləri

Xülasə

Son illərdə süni intellekt (SI) texnologiyalarının sürətli inkişafı, müxtəlif sahələrdə olduğu kimi, kiber təhlükəsizlik sahəsində də yeni imkanlar yaratmışdır. Süni intellektin kiber təhlükəsizlik sahəsində istifadəsi, şəbəkə hücumları, zərərli proqramlar və digər kiber təhlükəsizlik təhdidlərinə qarşı daha effektiv və sürətli mübarizə aparmağa imkan verir. SI sistemləri şəbəkə trafikini və istifadəçi davranışlarını analiz edərək anomaliyaları və potensial təhlükələri real vaxtda aşkar edə bilir, bu da mühafizə tədbirlərinin vaxtında görülməsini təmin edir. Eyni zamanda, məlumatların təhlilini sürətləndirərək daha düzgün və dəqiq təhlükəsizlik həlləri təklif edir.

Bununla belə, süni intellektin kiber təhlükəsizlikdə tətbiqi bəzən müəyyən risklər və problemlər də yaradır. SI sistemlərinin doğru məlumatlarla təlimi vacibdir, çünki səhv və qeyri-dəqiq məlumatlar nəticəsində yanlış qərarlar qəbul oluna bilər. Həmçinin, süni intellektin özü də kiber hücumların bir aləti olaraq istifadə edilə bilər. Hakerlər, bu texnologiyayı manipulyasiya edərək mühafizə tədbirlərini aşmağa cəhd edə bilərlər. Bu səbəbdən, süni intellektin kiber təhlükəsizlikdə istifadəsi zamanı onun təhlükəsizliyini təmin edən xüsusi müdafiə mexanizmlərinin tətbiqi vacibdir.

Məqalə, süni intellektin kibertəhlükəsizlik sahəsində tətbiqini, faydalarını və qarşıya çıxan biləcək riskləri araşdırır. Eyni zamanda, süni intellektin effektiv və təhlükəsiz istifadəsi üçün müvafiq tədbirlərin görülməsi və risklərin idarə edilməsi məsələlərini müzakirə edir. Gələcəkdə, süni intellektin inkişafı ilə yanaşı, onun kibertəhlükəsizlik sahəsində istifadəsinin daha təhlükəsiz hala gətirilməsi üçün yeni metodların tətbiqi və davamlı monitorinqin həyata keçirilməsi çox mühüm əhəmiyyət kəsb edəcəkdir.

Açar sözlər : Süni intellekt, kibertəhlükəsizlik, risklər, haker hücumları, zərərli proqramlar, maşın öyrənmə, kiberhücumlar

Nazila Rahimova

Azerbaijan State Oil and Industry University

<https://orcid.org/0000-0002-0942-7882>

ragimova.n.a@gmail.com

Rahila Salamova

Azerbaijan State Oil and Industry University

Master student

<https://orcid.org/0009-0008-7599-6291>

rehileshefiyeva95@gmail.com

Application and Risks of Artificial Intelligence in Cyber Security

Abstract

In recent years, the rapid development of artificial intelligence (AI) technologies has created new opportunities in various fields, including cyber security. The application of AI in cyber security allows for more effective and rapid responses to network intrusions, malware, and other cybersecurity threats. AI systems analyze network traffic and user behavior, detecting anomalies and potential threats in real-time, ensuring timely implementation of protective measures. Furthermore, AI accelerates data analysis, providing more accurate and precise security solutions.

However, the use of AI in cyber security also presents certain risks and challenges. It is crucial to train AI systems with correct and clean data, as inaccurate or flawed data can lead to incorrect decisions. Moreover, AI itself can be used as a tool by cyber criminals to bypass security measures. Hackers may manipulate AI technologies to carry out malicious operations. Therefore, implementing specific defense mechanisms to secure AI in cybersecurity is essential.

This paper explores the application, benefits, and potential risks of AI in cyber security. It also discusses the necessary measures to ensure the effective and secure use of AI, as well as the management of associated risks. In the future, alongside the advancement of AI technologies, it will be crucial to apply new methods and continuous monitoring to ensure safer use of AI in cyber security.

Keywords: Artificial Intelligence, cyber security, risks, hacker attacks, malware, machine learning, cyber attacks

Giriş

İnformasiya texnologiyalarının sürətli inkişafı, eyni zamanda, kiber təhlükəsizlik məsələlərini daha da ön plana çıxarmışdır. Günümüzdə internetin genişlənməsi ilə həm fərdi, həm də təşkilati məlumatlar böyük risk altındadır. Kiber təhlükəsizlik sahəsində, ənənəvi metodlar artıq kifayət etməməkdədir. Bu səbəbdən, yeni və daha mükəmməl texnologiyalar, o cümlədən süni intellekt (SI), kiber təhlükəsizlik sahəsində tətbiq edilməyə başlanmışdır. Süni intellekt, xüsusilə məlumatların təhlilində, təhlükəsizlik boşluqlarının aşkar edilməsində və haker hücumlarının qarşısının alınmasında çox böyük potensiala malikdir (Akhavan, 2021; Liu & Zhang, 2022). Bununla yanaşı, süni intellektin istifadəsi bir sıra riskləri də ortaya çıxarır. Məsələn, SI-nin manipulyasiya edilməsi, təlim məlumatlarının səhv olması, və ya daha təkmil zərərli proqramların yaradılması bu risklərə daxildir (Raut, 2020; Siddiqui, 2021). Məqalənin məqsədi, süni intellektin kiber təhlükəsizlik sahəsindəki tətbiqini və bu texnologiyanın potensial risklərini müzakirə etməkdir.

Tədqiqat

Süni intellektin kiber təhlükəsizlikdə tətbiqi. Süni intellektin kiber təhlükəsizlik sahəsindəki tətbiqi geniş və çoxşaxəlidir. Bir çox müasir kiber təhlükəsizlik sistemləri artıq süni intellekt texnologiyalarından istifadə edir. Maşın öyrənmə alqoritmləri, çox böyük məlumat dəstlərini təhlil edərək şəbəkələrdəki anomaliyalı davranışları müəyyənləşdirir və mümkün hücumları erkən aşkar edir. Bu, zərərli proqramların daha tez bir zamanda aşkarlanmasını və qarşısının alınmasını təmin edir (Patil & Kumar, 2023). Süni intellektin istifadə edildiyi sahələrdən biri də kiber hücumların qarşısını almaq üçün təhlükəsizlik sistemlərinin avtomatik şəkildə mütəmadi yenilənməsidir. Bu sistemlər, təhdidlərə qarşı reaksiya göstərmək üçün əvvəlcədən təlim edilmiş model və alqoritmlərdən istifadə edirlər (Zhang, 2020).

Bundan başqa, SI sistemləri, şəbəkə trafikini real zamanlı olaraq analiz edərək, istifadəçi davranışlarını və məlumat axınlarını izləyir. Bu metod, kiber hücumların və ya məlumat oğurluğu cəhdlərinin baş verməsini dərhal aşkar edə bilir (Smith, 2022). Belə ki, bu cür SI əsaslı alətlər

yalnız təhlükəsizlik tədbirlərini həyata keçirmək deyil, həm də zərərli fəaliyyətləri proqnozlaşdırmaq və erkən xəbərdarlıq etmək qabiliyyətinə malikdir.

Süni intellektin yarada biləcəyi risklər. Lakin, süni intellektin kiber təhlükəsizlik sahəsində istifadəsi bir sıra təhlükələrə də yol aça bilər. İlk növbədə, süni intellekt əsaslı sistemlər təlim verilmiş məlumatlardan asılıdır. Əgər bu məlumatlar səhv və ya manipulyasiya olunmuş olarsa, SI sistemi yanlış qərarlar verə bilər (Siddiqui, 2021). Məsələn, hakerlər süni intellektin təlim məlumatlarını manipulyasiya edərək, bu alqoritmləri öz məqsədləri üçün istifadə edə bilərlər.

Bundan başqa, süni intellektin özü də kiber hücumların alətinə çevrilə bilər. Məsələn, hakerlər, SI sistemlərini kiberhücumların həyata keçirilməsi üçün istifadə edə bilər. SI, öz təbiətinə görə, müasir haker metodlarını daha təkmil şəkildə təqlid etmək qabiliyyətinə malikdir. Bu cür hallarda, kiber təhlükəsizlik üçün qarşısı alınması çətin olan yeni təhdidlər meydana çıxır (Raut, 2020). Nəhayət, süni intellektin çox mürəkkəb olması və alqoritmlərin qapalı təbiəti də problemlər yarada bilər. Bu, SI sistemlərinin təkmilləşdirilməsi və idarə olunmasında çətinliklərə səbəb olur.

Risklərin idarə edilməsi. Süni intellektin kiber təhlükəsizlikdəki risklərini idarə etmək üçün müxtəlif yanaşmalar mövcuddur. İlk növbədə, SI sistemlərinin təhlükəsizliyini təmin etmək məqsədilə mütəmadi olaraq yeniləmələr və təkmilləşdirmələr həyata keçirilməlidir. Sistemlərin və alqoritmlərin daim yenilənməsi, hakerlər tərəfindən manipulyasiya edilməsinin qarşısını almağa kömək edir. Ayrıca, təlim məlumatlarının düzgünlüyü və etibarlılığı da mütləq təmin edilməlidir (Liu & Zhang, 2022).

Bir başqa yanaşma isə, SI təhlükəsizlik sistemlərinin “açıq qapalı” olmasıdır. Yəni, kiber təhlükəsizlik mühəndisləri tərəfindən nəzərdən keçirilməli və tənzimlənməlidir. Bu cür yanaşmalar, SI sistemlərinin yalnız təcrübəli və məlumatlı şəxslər tərəfindən istifadə edilməsini təmin edə bilər. Süni intellektin təhlil etdiyi məlumatlar daha yüksək təhlükəsizlik standartlarına uyğun olaraq qorunmalıdır.

Nəticə

Süni intellektin kiber təhlükəsizlik sahəsində tətbiqi müasir dövrün ən vacib və aktual mövzularından biridir. Bu texnologiya, məlumatların təhlilini sürətləndirərək və şəbəkə fəaliyyətlərini real vaxtda izləyərək kiber təhlükəsizlikdəki əsas problemləri həll etməyə kömək edir. Süni intellektin kiber təhlükəsizlik sahəsində istifadə olunması, daha dəqiq və effektiv müdafiə tədbirlərinin həyata keçirilməsini təmin edir. Məsələn, SI alqoritmləri anomaliyalı davranışları aşkarlama, zərərli proqramları təhlil etmə və kiber hücumların qarşısını almaqda insan müdaxiləsindən daha sürətli və dəqiq nəticələr verə bilər.

Bununla belə, süni intellektin istifadəsi yalnız faydalarla məhdudlaşmır. Texnologiyanın tətbiqi bəzən müəyyən risklər və problemləri də özü ilə gətirir. Süni intellektin düzgün şəkildə təlim edilməməsi və ya təlim məlumatlarının qeyri-dəqiq olması, səhv nəticələrin çıxmasına səbəb ola bilər. Həmçinin, bu texnologiya kiberhücumçular tərəfindən manipulyasiya edilə bilər. Kiber hücumçular, süni intellektin zəifliklərindən istifadə edərək təhlükəsizlik sistemlərini aşmağa və daha inkişaf etmiş hücumlar həyata keçirə bilərlər. Bu vəziyyət, süni intellektin kiber təhlükəsizlik sahəsində istifadəsini daha mürəkkəb və təhlükəli edir.

Nəticə olaraq, süni intellektin kiber təhlükəsizlikdəki tətbiqi böyük potensiala sahib olsa da, onun effektiv və təhlükəsiz istifadəsi üçün bir sıra tədbirlər görülməlidir. İlk növbədə, süni intellektin inkişafı və tətbiqi sahəsindəki təlim məlumatlarının keyfiyyəti və düzgünlüyü təmin edilməli, sistemlər davamlı olaraq monitorinq edilməli və təkmilləşdirilməlidir. Süni intellektin kiber təhlükəsizlikdəki tətbiqinin gələcəyi, yalnız bu texnologiyanın təkmilləşdirilməsi ilə deyil, həm də ona qarşı ortaya çıxan yeni risklərin idarə olunması ilə bağlıdır. Bu səbəbdən, süni intellektin kiber təhlükəsizlik sahəsində tətbiqi, daim inkişaf edən və təkmilləşdirilən bir sahə olmalıdır. Gələcəkdə, süni intellekt texnologiyalarının istifadəsi ilə kiber təhlükəsizliyin daha

effektiv təmin olunması üçün qarşıya çıxan risklərə qarşı müvafiq tədbirlərin görülməsi mühüm əhəmiyyət kəsb edəcəkdir.

Ədəbiyyat

1. Akhavan, M. (2021). Cybersecurity challenges in artificial intelligence systems. *Journal of Cybersecurity*, 17(2), 34–45. <https://doi.org/10.1016/j.cyber.2021.02.007>
2. Aliev, R. (2020). Machine learning applications in cybersecurity. *International Journal of Information Security*, 29(3), 225–239. <https://doi.org/10.1007/s10207-019-00505-x>
3. Bostancı, E., & Koç, M. (2021). Yapay Zekâ ve Güvenlik: Tehditler, Uygulamalar ve Gelecek Perspektifleri. Ankara: Bilgi Güvenliği Yayınları.
4. Brown, P., & Smith, J. (2019). Artificial intelligence in cybersecurity: Benefits and risks. *Cybersecurity and Privacy*, 15(4), 102–112.
5. Hacıyeva, B. (2023). Xarici maqnit sahəsində neytrino-elektron qarşılıqlı təsir prosesləri üçün ümumi halda matris elementi. “Elmi İş” Beynəlxalq Elmi Jurnal, 17(6), 157–164. <https://doi.org/10.36719/2663-4619/91/157-164>
6. İsmayıl, T. (2024, 30 may). Süni intellekt və kibertəhlükəsizlik. *Aem.az*. <https://aem.az?newsid=4186>
7. Liu, Y., & Zhang, H. (2022). The impact of artificial intelligence on cybersecurity: A systematic review. *Security and Privacy*, 12(7), 130–142. <https://doi.org/10.1002/sec.2681>
8. Patil, A., & Kumar, S. (2023). Threats in artificial intelligence systems: A cybersecurity perspective. *Journal of Cyber Security and Protection*, 19(2), 143–156. <https://doi.org/10.1109/JCSP.2023.3217896>
9. Raut, S. (2020). Ethical implications of artificial intelligence in cybersecurity. *Journal of Ethics and Technology*, 9(4), 78–91. <https://doi.org/10.1109/JET.2020.017892>
10. Russell, S., & Norvig, P. (2020). *Artificial Intelligence: A Modern Approach* (4th ed.). Pearson Education. <https://aima.cs.berkeley.edu/>
11. Siddiqui, M. (2021). Artificial intelligence and its impact on cybersecurity: A comprehensive analysis. *Journal of Computer Science and Cybersecurity*, 8(1), 99–113.
12. Zhang, Q. (2020). The role of machine learning in cybersecurity: Applications and challenges. *Computer Science Review*, 24(5), 234–249. <https://doi.org/10.1016/j.cosrev.2020.100376>

Daxil oldu: 08.01.2025

Qəbul edildi: 12.04.2025