DOI: https://doi.org/10.36719/2789-6919/57/217-221

Ayxan Məmmədli
Azərbaycan Dövlət İqtisad Universiteti
magistrant
https://orcid.org/0009-0008-8043-1519
aykhanmammadli0@gmail.com

Kiber təhlükəsizlikdə süni intellektin tətbiqi və onun effektivliyinin təhlili

Xülasə

Müasir informasiya cəmiyyətində rəqəmsal texnologiyaların sürətli inkişafı ilə paralel olaraq kiber təhlükələrin miqyası və mürəkkəbliyi əhəmiyyətli dərəcədə artmışdır. Ənənəvi kiber təhlükəsizlik sistemləri əsasən əvvəlcədən müəyyən edilmiş qaydalar və imza əsaslı yanaşmalar üzərində qurulduğundan, yeni və dinamik hücumlara qarşı effektiv müdafiə təmin etməkdə çətinlik çəkir. Bu səbəbdən süni intellekt texnologiyalarının kiber təhlükəsizlik sahəsində tətbiqi son illərdə xüsusi aktuallıq qazanmışdır.

Bu məqalədə süni intellektin kiber təhlükəsizlik sahəsində tətbiqi imkanları, istifadə olunan əsas metodlar və onların effektivliyi təhlil edilir. Xüsusilə maşın öyrənməsi və dərin öyrənmə modellərinin hücumların aşkarlanması, anomaliyaların müəyyən edilməsi və təhlükələrin proqnozlaşdırılması sahəsində rolu araşdırılır. Tədqiqat nəticəsində müəyyən edilir ki, süni intellekt əsaslı yanaşmalar ənənəvi metodlarla müqayisədə daha yüksək dəqiqlik və adaptivlik təmin edir.

Bununla yanaşı, süni intellekt sistemlərinin tətbiqi ilə bağlı bəzi məhdudiyyətlər və risklər, o cümlədən yanlış pozitiv nəticələr, məlumat keyfiyyətindən asılılıq və adversarial hücumlar da nəzərdən keçirilir. Məqalənin nəticəsi olaraq, süni intellektin kiber təhlükəsizlik sahəsində perspektivli və effektiv bir alət olduğu, lakin onun optimal istifadəsi üçün kompleks yanaşmanın vacibliyi vurğulanır.

Açar sözlər: *süni intellekt, kiber təhlükəsizlik, maşın öyrənməsi, hücum aşkarlanması, anomaliya analizi, dərin öyrənmə*

Aykhan Mammadli
Azerbaijan State University of Economics
Master's student
https://orcid.org/0009-0008-8043-1519
aykhanmammadli0@gmail.com

Application of Artificial Intelligence in Cybersecurity and Analysis of its Effectiveness

Abstract

In the modern information society, the rapid development of digital technologies has significantly increased the scale and complexity of cyber threats. Traditional cybersecurity systems, which are primarily based on predefined rules and signature-based approaches, often struggle to effectively detect and prevent new and evolving attacks. Therefore, the application of artificial intelligence (AI) in cybersecurity has gained significant importance in recent years.

This article analyzes the application of AI in cybersecurity, focusing on key methods and their effectiveness. In particular, the role of machine learning and deep learning models in threat detection, anomaly identification, and predictive analysis is examined. The study reveals that AI-based approaches provide higher accuracy and adaptability compared to traditional methods.

However, several limitations and risks associated with AI systems are also discussed, including false positives, dependency on data quality, and adversarial attacks.

The findings highlight that while AI is a powerful and promising tool in cybersecurity, its effective implementation requires a comprehensive and balanced approach.

Keywords: *artificial intelligence, cybersecurity, machine learning, intrusion detection, anomaly detection, deep learning*

Giriş

Müasir dövrdə rəqəmsal texnologiyaların sürətli inkişafı kiber təhlükəsizlik məsələlərini qlobal səviyyədə aktual problemlərdən birinə çevirmişdir. İnternet, bulud texnologiyaları və IoT sistemlərinin geniş yayılması informasiya mühitinin həm həcmini, həm də mürəkkəbliyini artırmış, nəticədə kiber hücumların sayı və müxtəlifliyi əhəmiyyətli dərəcədə artmışdır. Xüsusilə fidyə proqramları, fişinq hücumları və məlumat sızmaları həm təşkilatlar, həm də fərdi istifadəçilər üçün ciddi risk yaradır (ENISA, 2022; Microsoft, 2022).

Ənənəvi təhlükəsizlik sistemləri əsasən imza və qayda əsaslı yanaşmalara əsaslanır və yalnız məlum hücumları aşkar etməkdə effektivdir. Lakin müasir hücumların dinamik xarakter daşıması bu sistemlərin effektivliyini azaldır və daha çevik texnologiyalara ehtiyac yaradır.

Bu baxımdan süni intellekt kiber təhlükəsizlik sahəsində mühüm rol oynayır. AI sistemləri böyük həcmli məlumatları analiz edərək anomaliyaları müəyyən edə, hücumları proqnozlaşdıra və real vaxt rejimində təhlükələri aşkar edə bilir (Sarker, 2021).

Bu məqalənin məqsədi süni intellektin kiber təhlükəsizlik sahəsində tətbiq imkanlarını təhlil etmək və onun üstünlükləri ilə məhdudiyyətlərini qiymətləndirməkdir.

Tədqiqat

Süni intellekt və kiber təhlükəsizlik anlayışı. Süni intellekt kompüter sistemlərinin öyrənmə, analiz və qərarvermə kimi funksiyaları yerinə yetirməsini təmin edən texnologiyalar toplusudur. Onun əsas istiqamətləri olan maşın öyrənməsi və dərin öyrənmə böyük həcmli məlumatların emalı və nümunələrin müəyyən edilməsi üçün geniş istifadə olunur.

Kiber təhlükəsizlik sahəsində süni intellekt sistemləri şəbəkə trafiki və istifadəçi davranışlarını analiz edərək normal və qeyri-normal fəaliyyətləri müəyyən edə bilir. Ənənəvi yanaşmalardan fərqli olaraq, bu sistemlər yalnız məlum hücumlarla məhdudlaşmır və yeni təhlükələrin aşkarlanmasına imkan yaradır.

Dərin öyrənmə modelləri mürəkkəb məlumat strukturlarını analiz edərək daha yüksək dəqiqlik təmin edir və kompleks hücum nümunələrinin müəyyən edilməsində istifadə olunur (Russell və Norvig, 2021; McAfee Labs, 2021).

Beləliklə, süni intellekt kiber təhlükəsizlikdə daha çevik və adaptiv yanaşma təqdim edərək müasir təhlükələrə qarşı effektiv müdafiə imkanı yaradır.

AI əsaslı hücum aşkarlama sistemləri. Kiber təhlükəsizlik sistemlərində hücumların vaxtında aşkarlanması mühüm əhəmiyyət daşıyır. Ənənəvi intrusion detection və prevention sistemləri əsasən imza əsaslı işlədiyindən yalnız məlum hücumları müəyyən edə bilir və yeni təhlükələrə qarşı məhdud effektivlik göstərir.

Süni intellekt əsaslı sistemlər isə normal və anormal davranışları analiz edərək bu yanaşmanı daha da inkişaf etdirir. Bu sistemlər böyük həcmli məlumatları emal edərək əvvəllər məlum olmayan, xüsusilə *zero-day* tipli hücumları aşkar edə bilir.

Anomaliya əsaslı yanaşma sistemin normal fəaliyyətini öyrənərək ondan kənara çıxan halları təhlükə kimi qiymətləndirir və dinamik mühitlərdə daha effektiv hesab olunur. Dərin öyrənmə modelləri isə mürəkkəb hücum nümunələrinin müəyyən edilməsində yüksək dəqiqlik təmin edir.

Süni intellekt sistemlərinin əsas üstünlüklərindən biri real vaxt rejimində işləməsidir. Bu isə hücumların erkən mərhələdə aşkarlanmasına və qarşısının alınmasına imkan yaradır. Bununla yanaşı, sistemlərin effektivliyi istifadə olunan məlumatların keyfiyyətindən asılıdır və bəzi hallarda yanlış nəticələr yarana bilər (Buczak və Guven, 2016; Goodfellow və b., 2016).

Cədvəl 1.
Ənənəvi və süni intellekt əsaslı təhlükəsizlik sistemlərinin müqayisəsi

Xüsusiyyət	Ənənəvi sistemlər	Süni intellekt əsaslı sistemlər
Aşkarlama üsulu	İmza və qayda əsaslı	Anomaliya və öyrənmə əsaslı
Yeni hücumlara uyğunlaşma	Məhdud	Yüksək
Real vaxt analizi	Məhdud	Effektiv
Dəqiqlik	Orta	Yüksək
Adaptivlik	Zəif	Güclü
Avtomatlaşdırma	Az	Yüksək

Cədvəldən göründüyü kimi, süni intellekt əsaslı sistemlər daha yüksək adaptivlik və effektivlik təmin edir.

Süni intellektin kiber təhlükəsizlikdə tətbiq sahələri. Süni intellekt texnologiyaları kiber təhlükəsizlik sahəsində müxtəlif istiqamətlərdə tətbiq olunur və müasir təhlükə mühitində sistemlərin daha çevik və effektiv fəaliyyət göstərməsinə imkan yaradır.

Əsas tətbiq sahələrindən biri zərərli proqramların (*malware*) aşkarlanmasıdır. Süni intellekt modelləri proqramların davranışını analiz edərək yeni və dəyişkən təhlükələri müəyyən edə bilir və bu, xüsusilə mürəkkəb *malware* növlərinə qarşı effektiv müdafiə təmin edir.

Fişinq hücumlarının aşkarlanması da AI-nin geniş istifadə olunduğu sahələrdəndir. Süni intellekt sistemləri e-poçt məzmunu və URL strukturlarını analiz edərək şübhəli fəaliyyətləri müəyyən edir və bu hücumların qarşısının alınmasına kömək edir.

Bundan əlavə, süni intellekt şəbəkə trafikinin monitorinqində istifadə olunur. Sistemlər böyük həcmli məlumatları real vaxt rejimində analiz edərək normal davranışdan kənara çıxan halları müəyyən edir və potensial təhlükələri erkən mərhələdə aşkar etməyə imkan yaradır (Shaukat və b., 2020; Bishop, 2006; Sommer & Paxson, 2010).

Süni intellekt əsaslı kiber təhlükəsizlik sistemlərinin üstünlükləri. Süni intellekt əsaslı kiber təhlükəsizlik sistemləri ənənəvi yanaşmalarla müqayisədə bir sıra mühüm üstünlüklərə malikdir. Bu üstünlüklər əsasən sistemlərin adaptivliyi, sürətli işləməsi və böyük həcmli məlumatları emal etmə qabiliyyəti ilə bağlıdır.

Əsas üstünlüklərdən biri adaptivlikdir. AI modelləri yeni məlumatlar əsasında öyrənərək dəyişən hücum növlərinə uyğunlaşa bilir. Bu xüsusiyyət dinamik kiber mühitdə onların effektivliyini artırır.

Digər mühüm üstünlük real vaxt rejimində analiz imkanlarıdır. Süni intellekt sistemləri böyük həcmdə məlumatları sürətlə emal edərək təhlükələri operativ şəkildə müəyyən edə bilir. Bu isə hücumların erkən mərhələdə qarşısının alınmasına kömək edir.

Bundan əlavə, AI sistemləri böyük verilənlərlə işləmək qabiliyyətinə malikdir. Müxtəlif mənbələrdən toplanan məlumatlar analiz edilərək gizli nümunələr və əlaqələr aşkar edilir ki, bu da daha dəqiq nəticələr əldə etməyə imkan verir.

Süni intellect, həmçinin, təhlükəsizlik proseslərinin avtomatlaşdırılmasını təmin edir. Bu, insan müdaxiləsini azaldır və sistemlərin daha effektiv işləməsinə şərait yaradır.

Araşdırmalar göstərir ki, süni intellekt texnologiyalarının tətbiqi təhlükəsizlik sistemlərinin ümumi effektivliyini artırır və aşkarlama dəqiqliyini yüksəldir (IBM Security, 2025; NIST, 2018).

Süni intellekt əsaslı kiber təhlükəsizlik sistemlərinin problemləri və riskləri. Süni intellekt texnologiyaları kiber təhlükəsizlik sahəsində mühüm üstünlüklər təqdim etsə də, onların tətbiqi müəyyən problemlər və risklərlə də müşayiət olunur. Bu problemlərin nəzərə alınmaması sistemlərin effektivliyinə mənfi təsir göstərə bilər.

Əsas çətinliklərdən biri yanlış pozitiv və yanlış neqativ nəticələrin yaranmasıdır. Süni intellekt modelləri bəzən normal fəaliyyəti təhlükə kimi qiymətləndirə və ya əksinə, real hücumları müəyyən edə bilməyə bilər. Bu isə sistemin etibarlılığını azalda bilər.

Digər mühüm məsələ modellərin məlumatlardan asılılığıdır. Təlim üçün istifadə olunan məlumatlar qeyri-dəqiq və ya balanssız olduqda modelin nəticələri də düzgün olmaya bilər. Bu isə qərarların keyfiyyətinə birbaşa təsir edir.

Süni intellekt sistemləri, həmçinin, adversarial hücumlara qarşı həssas ola bilər. Bu tip hücumlar zamanı modellər manipulyasiya edilərək yanlış nəticələr verməyə məcbur edilir.

Bundan əlavə, bu texnologiyaların tətbiqi yüksək hesablama resursları tələb edir və bəzi hallarda izaholunma problemi yaradır. Xüsusilə mürəkkəb modellərdə qərarların necə qəbul edildiyini izah etmək çətin olur.

Bu səbəbdən süni intellekt sistemlərinin effektiv istifadəsi üçün mövcud risklərin nəzərə alınması və onların düzgün idarə olunması vacibdir (Sarker, 2021; Kaspersky, 2024).

Nəticə

Müasir dövrdə kiber təhlükələrin artması təhlükəsizlik sistemlərinin daha çevik və effektiv olmasını tələb edir. Ənənəvi yanaşmalar müəyyən hallarda faydalı olsa da, onların məhdudiyyətləri müasir hücumlara qarşı tam müdafiə təmin etmir. Bu baxımdan süni intellekt texnologiyalarının tətbiqi kiber təhlükəsizlik sahəsində mühüm əhəmiyyət kəsb edir.

Bununla yanaşı, süni intellekt təhlükəsizlik proseslərinin avtomatlaşdırılmasına şərait yaradır və sistemlərin daha operativ işləməsini təmin edir. Bu isə həm vaxt itkisinin qarşısını alır, həm də ümumi təhlükəsizlik səviyyəsini artırır.

Lakin bu texnologiyanın tətbiqi ilə bağlı bəzi problemlər də mövcuddur. Məlumat keyfiyyətindən asılılıq, yanlış nəticələr və modellərin izah olunması ilə bağlı çətinliklər nəzərə alınmalıdır. Bu səbəbdən süni intellektin tətbiqi kompleks yanaşma tələb edir.

Nəticə olaraq, süni intellekt kiber təhlükəsizlik sahəsində effektiv və perspektivli bir vasitədir. Onun düzgün tətbiqi daha etibarlı və çevik təhlükəsizlik sistemlərinin qurulmasına imkan yaradır.

Ədəbiyyat

1. Bishop, C. M. (2006). *Pattern Recognition and Machine Learning*. Springer.
2. Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials*, *18*(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502
3. ENISA. (2022). *ENISA threat landscape 2022*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
4. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.
5. IBM Security. (2025). *Cost of a Data Breach Report 2025*. https://www.ibm.com/reports/data-breach
6. Kaspersky. (2024). *Kaspersky Incident Response Report 2023*. https://securelist.com/kaspersky-incident-response-report-2023/
7. McAfee Labs. (2021). *McAfee Labs Threats Report, April 2021*.
8. Microsoft. (2022). *Microsoft Digital Defense Report 2022*. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/microsoft-digital-defense-report-2022.pdf?culture=en-us&country=us
9. NIST. (2018). *Framework for improving critical infrastructure cybersecurity*. https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf
10. Russell, S., & Norvig, P. (2021). *Artificial Intelligence: A Modern Approach*. Pearson.
11. Sarker, I.H., Furhad, M.H. & Nowrozy, R. (2021). AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. *SN Computer Science*, *2*, 173. https://doi.org/10.1007/s42979-021-00557-0

12. Shaukat, K., Alam, T. M., Hameed, I. A., et al. (2020). A Survey on Machine Learning Techniques for Cyber Security in the Last Decade. *IEEE Access*, *8*, 222310–222331. https://ieeexplore.ieee.org/document/9277523
13. Sommer, R., & Paxson, V. (2010). Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. *IEEE Symposium on Security and Privacy*, 305–316. https://doi.org/10.1109/SP.2010.25

Daxil oldu: 04.01.2026
Qəbul edildi: 14.04.2026