PARADIGMA, No.1, 2025, səh.125-128
https://doi.org/10.30546/30015.2025.1.054

SÜNİ İNTELLEKTİN KİBERHÜCUMLARA QARŞI MÜDAFİƏSİNİN EFFEKTLİYİ

C.K. Kazımov, E.N. Qəhrəmanov
Azərbaycan Universiteti, Ceyhun Hacıbəyli, 71, Bakı, Azərbaycan
e-mail: javanshir.kazimov@au.edu.az
e-mail: emil.gahramanov@student.au.edu.az

Xülasə. Məqalədə süni intellektin kibertəhlükəsizlik sahəsində tətbiq imkanları və kiberhücumlara qarşı effektivliyi təhlil olunur. Sürətlə artan rəqəmsal təhdidlər qarşısında ənənəvi təhlükəsizlik sistemlərinin məhdudluqları nəzərə alınaraq, süni intellekt əsaslı yanaşmaların potensialı araşdırılır. Maşın öyrənməsi və dərin öyrənmə texnologiyaları vasitəsilə anomaliyanın aşkarlanması, davranış təhlili və avtomatlaşdırılmış müdafiə mexanizmləri süni intellektin bu sahədəki əsas funksiyalarından hesab olunur. Nəticədə, süni intellektin kibertəhlükəsizlik sistemlərinin gələcəyində əvəzsiz rola malik olduğu qənaətinə gəlinir.

Açar sözlər: Süni intellekt, kibertəhlükəsizlik, maşın öyrənməsi, davranış təhlili, avtomatlaşdırılmış müdafiə.

Süni intellektin kibertəhlükəsizlikdə rolu nədir?

Rəqəmsal texnologiyaların sürətlə inkişaf etdiyi dövrdə kibertəhlükəsizlik məsələləri ön plana çıxır. Hər keçən gün daha mürəkkəb və aqressiv xarakter daşıyan kiberhücumlar fərdi və korporativ sistemlərə ciddi təhlükə yaradır. Bu çərçivədə süni intellekt (Sİ) kibertəhlükəsizlik sahəsində inqilabi dəyişikliklər yaradır. Sİ, maşın öyrənməsi və "big data" (iri-həcmli verilənlərin) analizi vasitəsilə kiberhücumları daha effektiv şəkildə aşkar edərək onların qarşısını almağa kömək edir.

Kibertəhlükəsizlikdə aktual problemlər

Müasir dövrdə kibertəhlükəsizlik sahəsində mövcud olan əsas problemlər informasiya texnologiyalarının sürətli inkişafı və kiberhücumçuların adaptasiya qabiliyyəti ilə əlaqəlidir. Aşağıda kibertəhlükəsizliyin qarşılaşdığı ən aktual problemlər ətraflı şəkildə təsvir edilir:

- Kiberhücumların artması və geniş miqyaslılığı
- Ənənəvi kibertəhlükəsizlik sistemlərinin qeyri-kafiliyi
- İnsana aid xətalar və təhlükəsizlik maarifçiliyinin çatışmazlığı
- Kibertəhlükəsizlik mütəxəssislərinin çatışmazlığı
- Məlumatların mühafizəsi və məxfiliyin təmini
- Süni intellektin kiberhücumçular tərəfindən istifadəsi

Kiberhücumların sayı və mürəkkəbliyi sürətlə artır və ənənəvi kibertəhlükəsizlik yanaşmaları bu hücumların qarşısını almaqda kifayət qədər effektiv olmur. Fişinq hücumları və DDoS hücumları getdikcə daha da inkişaf edir. İnsan amili də təhlükəsizlikdə əsas zəif nöqtələrdən biridir. İşçilərin təhlükəsizlik biliklərinin kifayət qədər olmaması kiberhücumların uğurlu olmasına şərait yaradır. Bundan əlavə, ixtisaslı kibertəhlükəsizlik mütəxəssislərinin

çatışmazlığı təşkilatların yeni texnologiyalara uyğunlaşmasını çətinləşdirir. Məlumat məxfiliyinin qorunması da kritik problemlərdən biridir. Süni intellektin müdafiə sahəsində istifadə olunmasına baxmayaraq, onun kibercinayətkarlar tərəfindən də tətbiqi təhlükəsizlik məsələlərini daha da mürəkkəbləşdirir.

Süni intellekt vasitəsi ilə kiberhücumların aşkarlanması və qarşısının alması

Süni intellekt kibertəhlükəsizlik sahəsində inqilabi dəyişikliklərə səbəb olmuş texnologiyalardan biridir. Müasir süni intellekt sistemləri böyük verilənlərin sürətli analizini, maşın öyrənməsi və "deep learning" modelləri vasitəsilə kiberhücumları aşkar etmək və qarşısını almaq üçün geniş imkanlar yaradır. Ənənəvi təhlükəsizlik sistemləri yalnız məlum hücum nümunələrinə əsaslanaraq işləyir. Lakin, süni intellekt fərqli bir yanaşma tətbiq edir. O, davranış təhlili apararaq, sistemlərdə anormal fəaliyyəti aşkar edir və əvvəlcədən müəyyən edilməmiş kiberhücumları belə müəyyən edə bilir. Bu özəllik sayəsində süni intellekt yeni yaranan və inkişaf edən kiberhücum texnikalarına qarşı daha dayanıqlı olur.

Süni intellekt kibertəhlükəsizlikdə əsasən dörd mərhələdə tətbiq edilir: aşkarlama, analiz, hücumun qarşısının alınması və cavab tədbirləri olaraq dörd mərhələdə tətbiq edilir. Aşkarlama mərhələsində süni intellekt müxtəlif mənbələrdən daxil olan verilənləri təhlil edərək anormal fəaliyyətləri müəyyənləşdirir. Maşın öyrənməsi metodları vasitəsilə normal və anormal fəaliyyətlər arasındakı fərqlər sistem tərəfindən daha aydın şəkildə ayırd edilə bilir. Bu, kiberhücumların ilkin mərhələdə aşkarlanmasını təmin edərək, onların təsirini minimuma endirməyə imkan yaradır.

Süni intellektin kibertəhlükəsizlikdə ən mühüm funksiyalarından biri də avtomatlaşdırılmış müdafiə mexanizmlərini təmin etməsidir. Ənənəvi təhlükəsizlik sistemləri hücumları aşkar etdikdə, çox vaxt insan müdaxiləsinə ehtiyac duyulur. Lakin süni intellekt real vaxt rejimində qərarlar qəbul edərək müstəqil şəkildə kiberhücumlara müdaxilə edə və zərərverici fəaliyyətləri dayandıra bilir. Bu isə təşkilatların təhlükəsizlik səviyyəsini yüksəldir və mümkün yarana biləcək riskləri azaldır. Süni intellekt kiberhücumlara qarşı qabaqlayıcı tədbirlər görərək, təhlükəsizlik meyarlarını davamlı olaraq təkmilləşdirir. Sİ, kiberhücumların tarixçəsini və məzmununu analiz edərək, gələcəkdə baş verə biləcək hücumları proqnozlaşdıra bilir və yarana biləcək yeni hücuma qarşı strategiyalar formalaşdırır.

Süni intellekt sistemləri hələ də müsbət və mənfi nəticələr çıxarmaqla bağlı problemlər yaşayır. Bəzi hallarda, adi və zərərsiz fəaliyyətləri təhlükə kimi qəbul edə bilər, yaxud əksinə, real kiberhücumları nəzərdən qaçıra bilər. Bundan əlavə, süni intellektin kibercinayətkarlar tərəfindən manipulyasiya olunması riski də mövcuddur. Əgər hücumçular sistemə məqsədyönlü şəkildə yanlış və yanıltıcı məlumatlar ötürsələr, süni intellektin qərar qəbuletmə mexanizmi zəifləyə bilər, nəticədə onun təhlükəsizlik səviyyəsi aşağı düşər və müdafiə mexanizmləri effektivliyini itirər.

Süni intellektin bu sahədə üstünlükləri və çatışmazlıqları

Süni intellektin kibertəhlükəsizlik sahəsində nümayiş etdirdiyi üstünlüklərin əsasını onun məlumat analizi və təhlil prosesində göstərdiyi yüksək sürət və dəqiqlik təşkil edir. Bu texnologiya, geniş və strukturlaşmamış məlumat dəstlərini real vaxtda işləyərək, ən incə fərqlilikləri belə aşkar edə bilir. Bunun nəticəsində, normal fəaliyyət və anomaliyalar arasındakı incə xəttləri dəqiq müəyyən etmək mümkündür.

Süni intellektin öyrənmə qabiliyyəti, mövcud təhlükəsizlik sistemlərini davamlı təkmilləşdirməyə və yeni yaranan kiberhücum nümunələrini öncədən tanımağa imkan verir. Bu dinamik adaptasiya prosesi, təşkilatların qabaqlayıcı müdafiə strategiyalarını gücləndirir və risklərin vaxtında aradan qaldırılmasına şərait yaradır.

Bununla belə, süni intellektin tətbiqi müəyyən çatışmazlıqları da özündə ehtiva edir. Əsas problemlərdən biri, sistemin effektivliyinin böyük həcmdə məlumatın keyfiyyəti və etibarlılığına bağlı olmasıdır; yanlış və ya natamam məlumat daxil olduqda, nəticə etibarsız qərarlara gətirib çıxara bilər. Bundan əlavə, kibercinayətkarlar süni intellekt modellərini manipulyasiya edərək müdafiə mexanizmlərini yanıltmaq üçün yeni strategiyalar inkişaf etdirə bilirlər, bu isə texnologiyanın davamlı səmərəliliyini təhdid edir.

Beləliklə, süni intellektin kibertəhlükəsizlikdə rolu həm böyük potensial, həm də müəyyən riskləri özündə birləşdirir; onun inkişafı və tətbiqi, etibarlı məlumatların toplanması, düzgün şəkildə toplanmış məlumatların analizi və davamlı təkmilləşdirmələr ilə birgə aparıldığı halda, gələcəkdə daha güclü və çevik müdafiə sistemlərinin qurulmasına zəmin yarada bilər. Aşağıda Sİ kibertəhlükəsizlik sahəsində olan ümumi üstünlükləri və çatışmazlıqları göstərilmişdir

Üstünlüklər

- Sürətli və effektiv analiz – Sİ qısa müddətdə böyük həcmdə məlumatı analiz edərək qərarlar qəbul edir.
- Öyrənmə qabiliyyəti – Süni intellekt yeni hücum texnikalarına uyğunlaşaraq inkişaf edə bilir.
- Resursların optimallaşdırılması – Kibertəhlükəsizlik üzrə mütəxəssislərin iş yükünü azaldır.

Çatışmazlıqlar:

- Yanlış pozitivlər və neqativlər – Sİ bəzi hallarda adi fəaliyyətləri təhlükə kimi tanıya və ya real hücumu gözardı edə bilər.
- Kiberhücumçular tərəfindən manipulyasiya olunma riski – Süni intellekt sistemləri xüsusi hücumlarla manipulyasiya edilə bilər.
- Məlumat məxfiliyinin pozulması – Böyük verilənlərin toplanması və analizi məxfi informasiyanın sızmasına səbəb ola bilər.

Nəticə. Süni intellektin kibertəhlükəsizlik sahəsində tətbiqi, müasir texnologiyaların gətirdiyi təhdidlərə qarşı verimli və dinamik müdafiə mexanizmlərinin qurulmasında inqilabi rol oynayır. Bu texnologiyanın inteqrasiyası, ənənəvi yanaşmaların əhatə dairəsini

genişləndirərək, kiberhücumların ilkin mərhələlərində aşkarlanması və zərərin minimuma endirilməsi üçün yeni imkanlar təqdim edir.

Süni intellektin kibertəhlükəsizlikdə rolu günbəgün artır və bu sahədə yeni texnologiyaların tətbiqi ilə daha da güclənir. Onun real vaxt rejimində təhlil aparması, avtomatik qərarlar qəbul etməsi və anomaliyalara çevik reaksiya verməsi, kibertəhlükəsizlik sahəsində effektivliyi artıran əsas amillərdəndir. Süni intellektin tətbiqi ilə təşkilatlar kiberhücumların qarşısını daha effektiv şəkildə ala bilir və təhlükəsizlik səviyyəsini yüksəldə bilirlər. Bu texnologiyanın gələcəkdə daha da inkişaf edərək kibertəhlükəsizlik sistemlərində mərkəzi rol oynayacağı şübhəsizdir.

Gələcəkdə süni intellekt texnologiyalarının davamlı inkişafı, həm avtomatlaşdırılmış təhlükəsizlik sistemlərinin, həm də insan-mühəndis əməkdaşlığının yeni səviyyəyə qaldırılmasını təmin edəcəkdir. İnnovativ modellərin tətbiqi, etik və hüquqi çərçivələrin gücləndirilməsi ilə birləşərək, kibertəhlükəsizlik sahəsində daha güclü və çevik müdafiə mexanizmlərinin qurulmasına şərait yaradacaq. Nəticə etibarilə, süni intellektin kibertəhlükəsizlikdəki rolu, müasir rəqəmsal mühitin təhlükəsizlik ehtiyaclarını qarşılamaq üçün əvəzolunmaz bir vasitə kimi ön plana çıxır və bu istiqamətdə atılan addımlar gələcəkdə daha etibarlı və səmərəli sistemlərin yaranmasına təkan verəcəkdir.

Ədəbiyyat

1. Benaich, I., Hogarth, N. (2023). Artificial Intelligence and Cybersecurity: Advances and Innovations. Routledge.
2. Priyadarshini, I., Sharma, R. (2023). Artificial Intelligence and Cybersecurity: Advances and Innovations. Routledge.
3. Саймон, В. (2021). Искусственный интеллект: современные подходы и методы. Санкт-Петербург: Бомбора.

EFFECTIVENESS OF ARTIFICIAL INTELLIGENCE IN DEFENDING AGAINST CYBER-ATTACKS

C.K. Kazimov, E.N. Gahramanov
Azerbaijan University, Ceyhun Hajibeyli, 71, Baku, Azerbaijan

Abstract. This paper explores the application of artificial intelligence in cybersecurity and its effectiveness in mitigating cyber-attacks. With the rapid rise of digital threats, traditional security systems are often insufficient, necessitating the integration of more intelligent solutions. AI technologies, particularly machine learning and deep learning, enable anomaly detection, behavioral analysis and real-time automated defense. Ultimately, the study concludes that artificial intelligence will play a central and indispensable role in the evolution of robust cybersecurity infrastructures.

Keywords: Artificial intelligence, cybersecurity, machine learning, behavioral analysis, automated defense.