Kibertəhlükəsizlik və Süni İntellekt

Fazil Aşumov
Hərbi İdarəetmə İnstitutu, Bakı, Azərbaycan
fazil.ashumov@mmu.edu.az

***Xülasə*— Məqalədə süni intellektin kibertəhlükəsizlik sahəsində rolu və tətbiq imkanları təhlil olunur. Müasir dövrdə kibertəhdidlərin mürəkkəbləşməsi və sürətlə artması ənənəvi təhlükəsizlik metodlarının effektivliyini azaldır. Bu baxımdan süni intellekt texnologiyaları real-vaxtda təhlükələrin aşkarlanması, hücumların proqnozlaşdırılması və avtomatlaşdırılmış müdafiə mexanizmlərinin qurulmasında mühüm rol oynayır. Məqalədə maşın təlimi, dərin təlim və davranış analizi kimi yanaşmaların kibertəhlükəsizlikdə tətbiqi araşdırılır. Eyni zamanda, süni intellektin istifadəsi ilə bağlı risklər və etik problemlər də nəzərdən keçirilir.**

Açar sözlər*— *süni intellekt; kibertəhlükəsizlik; maşın öyrənilməsi; ekspert sistemləri; idarəetmə informasiya sistemləri; avtonom sistemlər; kibermüdafiə.

I. GİRİŞ

XXI əsr informasiya və kommunikasiya texnologiyalarının sürətli inkişafı ilə xarakterizə olunur. Rəqəmsallaşma prosesi dövlət idarəçiliyindən tutmuş iqtisadiyyat, müdafiə, səhiyyə və təhsil sahələrinə qədər bütün sistemləri əhatə edir [1, 2]. Bu transformasiya informasiya mübadiləsini sürətləndirməklə yanaşı, eyni zamanda yeni təhlükəsizlik problemləri də yaratmaqdadır. Xüsusilə kiberməkanın genişlənməsi ilə kiberhücumların miqyası, mürəkkəbliyi və təsir gücü əhəmiyyətli dərəcədə artmışdır.

Müasir dövrdə kibertəhlükələr artıq lokal xarakter daşımır, qlobal təhlükə səviyyəsinə yüksəlmişdir [3]. Dövlət qurumları, hərbi strukturlar və kritik infrastruktur obyektləri (enerji sistemləri, bank sektoru, nəqliyyat şəbəkələri və s.) kiberhücumların əsas hədəflərinə çevrilmişdir. Bu hücumlar yalnız məlumatların oğurlanması ilə məhdudlaşmır, eyni zamanda iqtisadi itkilərə, sosial sabitliyin pozulmasına və milli təhlükəsizliyə ciddi təhdidlər yaradır.

Bu baxımdan süni intellekt texnologiyalarının kibertəhlükəsizlik sahəsində tətbiqi xüsusi aktuallıq kəsb edir və kibertəhdidlərə qarşı mübarizədə yeni imkanlar yaradır.

II. KİBERTƏHLÜKƏSİZLİK

Kibertəhlükə – informasiya sistemlərinə, kompüter şəbəkələrinə və ya rəqəmsal resurslara qarşı yönəlmiş, onların məxfiliyini, bütövlüyünü və əlçatanlığını poza bilən təhlükə və ya hücumdur.

Kibertəhlükəsizlik kompüterlərin, serverlərin, mobil qurğuların, elektron sistemlərin, şəbəkələrin və məlumatların ziyankar hücumlardan qorunması təcrübəsidir. İnformasiya texnologiyaları təhlükəsizliyi və ya elektron məlumat təhlükəsizliyi kimi də tanınır və bir neçə ümumi kateqoriyaya bölünə bilir:

Şəbəkə təhlükəsizliyi - kompüter şəbəkəsinin təcavüzkarların və ya təsadüfi ziyankar proqramların müdaxilələrindən mühafizə edilməsidir.

Proqram təhlükəsizliyi - proqram təminatının və qurğuların təhlükələrdən mühafizə edilməsidir. Təhlükəyə məruz qalmış proqram qorunması nəzərdə tutulmuş məlumat bazasına daxil olmağa imkan verə bilər. Təhlükəsizliyin təmin olunması layihələndirmə mərhələsindən başlayır və proqram və ya qurğu istifadəyə verilməzdən əvvəl nəzərə alınmalıdır.

İnformasiya təhlükəsizliyi - həm saxlanılan, həm də göndərilən məlumatların bütövlüyünü və məxfiliyini qoruyur.

Kibertəhlükəsizlik, şəbəkələri, qurğuları, proqramları və məlumatları hücumlardan və ya icazəsiz girişlərdən qorumaq üçün nəzərdə tutulmuş inkişaf edən alətlər dəstindən, risklərin idarə olunması yanaşmalarından, texnologiyalardan, təlimlərdən və qabaqcıl təcrübələrdən ibarətdir.

İlk milli kibertəhlükəsizlik strategiyaları 2000-ci illərdə meydana çıxmışdır. Kibertəhlükəsizliyi milli strateji məsələ kimi qəbul edən ilk ölkə ABŞ olmuşdu. 2003-cü ildə "Kiberfəzanın təhlükəsizliyi üzrə Milli Strategiya" qəbul edilib. Bu strategiya 11 sentyabr 2001-ci il terror hücumlarından sonra qəbul edilmiş "Milli Təhlükəsizlik üzrə Milli Strategiya"nın tərkib hissəsidir.

Kiberhücum – kompüter və internet sahəsində ixtisaslaşmış şəxslərin (hakerlərin) dövlət, qeyri-dövlət təşkilatlarının və şəxslərin kompüter sistemləri vasitəsi ilə onlara zərər vurma əməliyyatıdır. Kiberhücumlar haker adlanan şəxs və ya bir qrup şəxslər tərəfindən həyata keçirilir.

Haker termini əvvəllər yüksək ixtisaslı proqramçılar üçün işlədilsə də, hazırda əsasən kompüter sistemlərinin təhlükəsizlik boşluqlarından istifadə edərək icazəsiz giriş həyata keçirən şəxsləri ifadə etmək üçün istifadə olunur.

Hakerlər xüsusi kompüterlərdən başqa böyük şəbəkələrə də hücum edirlər. Sistemə giriş əldə etməklə, konfidensial məlumatları ələ keçirir və ya ziyanverici proqramlar yerləşdirirlər. Bu gün kiber təhdidlər dünyada ən aktual problemlərdən birinə çevrilib.

Hücumlar adətən istifadəçilərin xüsusi saxlanan, emal edilən və mübadilə edilən məlumatlarının və ya məlumat daşıyıcılarının məhv edilməsinə (pozulmasına, dəyişdirilməsinə) yönəlir.

Kibertəhdidlər icazəsiz olaraq serverlərin təhlükəsizliyini

DOI: 10.25045/forensic.gov.2026.83

pozan və onlardan məlumat əldə edən hakerlər tərəfindən yerinə yetirilir. Hakerlər kompüter sistemlərinin və proqram təminatının iş prinsiplərini dərindən bilən yüksək ixtisaslı mütəxəssislərdir.

Kiber hücumun aşağıdakı növləri mövcuddur:

- Kibercasusluq – kompüter və informasiya texnologiyaları şəbəkələrindən rəqəmsal formada emal olunan məxvi məlumatların oğurlanaraq ələ keçirilməsidir.
- Kibermüharibə – informasiya və informasiya sistemlərinə internet üzərindən edilən hücumlardır. Onun əsas məqsədi rəsmi veb-sayt və şəbəkələrinin işini iflic etmək, sistemləri, müasir silahları, servisləri, bankları, nəqliyyat və s. xidmət sahələrini yararsız vəziyyətə salmaqdır.
- Haktivizm – internet saytları və kompüter şəbəkələrinin işini pozmaq fəaliyyətidir. Haktivistlər bu üsulu tətbiq edərək siyasi və ya ictimai müraciətlərini bəyan edir.
- Kibercinayət – cinayətin bir növüdür və kompüter vasitəsilə həyata keçirilir. Bu cinayət müxtəlif kiberhücum vasitələri və alətlərinin yardımı ilə icra oluna bilər.

III. SÜNİ İNTELLEKTİN YARANMASI VƏ İNKİŞAFI

Əsrimiz informasiya texnologiyalarının sürətli inkişafı ilə səciyyələnir. Bu inkişafın ən mühüm istiqamətlərindən biri süni intellekt və onun müxtəlif informasiya sistemlərinə inteqrasiyasıdır [4]. Müasir dövrdə məlumatların toplanması, emalı və təhlili insanların deyil, alqoritmlərin idarə etdiyi çoxşaxəli bir prosesə çevrilib. Bu vəziyyət informasiya sistemlərinin yalnız məlumat bazaları və hesablama vasitələri kimi deyil, həm də "ağıllı" qərar qəbuletmə mexanizmləri kimi formalaşmasına şərait yaradır [5, 6].

Süni intellekt anlayışı informatikanın, riyaziyyatın, mühəndisliyin və aidiyyatı elmlərin sintezindən yaranmışdır [7]. Onun əsas məqsədi insan beyninin idrak funksiyalarını texnoloji səviyyədə təqlid etmək, yəni maşınlara öyrənmək, düşünmək, qərar vermək və problem həll etmək qabiliyyəti aşılamaqdır. Bu məqsədlə yaradılan alqoritmlər və modellər informasiya sistemlərinin effektivliyini artırır, məlumat axınlarının idarə olunmasını optimallaşdırır və müxtəlif qurumların müəyyən qərar qəbuletmə mexanizmlərini avtomatlaşdırır.

İnformasiya sistemləri və süni intellekt bir-birini tamamlayan iki əsas texnoloji sahədir. Əgər informasiya sistemləri məlumatları toplayır və saxlayırsa, süni intellekt həmin məlumatları analiz edərək nəticə çıxarmağa, proqnozlar verməyə və səmərəli qərarlar qəbul etməyə imkan yaradır [8, 9]. Bu baxımdan süni intellektin informasiya sistemlərinə inteqrasiyası müasir iqtisadiyyatın, dövlət idarəçiliyinin, sosial münasibətlərin və hərbi məsələlərin həllinin yenidən formalaşmasında həlledici rol oynayır.

Süni intellekt anlayışı ilk dəfə 1956-cı ildə ABŞ-ın Dartmut Kollecində keçirilən konfransda rəsmi elmi termin kimi istifadə olunmuşdur [10]. Bu konfrans süni intellekt elminin başlanğıcı hesab edilir. Tədqiqatçılar Con Makkarti, Marvin Minski, Herbert Saymon və Alan Nyuell kimi alimlər insan düşüncəsini alqoritmik şəkildə modelləşdirməyə çalışırdılar.

Süni intellektin yaranması və inkişafı dörd dövrü əhatə edir:

1. Erkən dövr (1950–1970-ci illər) – bu mərhələdə əsas məqsəd insan beyninin düşünmə modelini kompüter proqramlarında təqlid etmək idi. Alan Tyurinqin "Maşınlar düşünə bilərmi?" adlı sualı və onun təklif etdiyi Tyurinq testi süni intellekt nəzəriyyəsinin əsasını qoydu. İlk "ağıllı" proqramlardan biri ELIZA idi (1966-cı il). O, sadə dialoqları simulyasiya edirdi.

2. Ekspert sistemləri dövrü (1970–1990-cı illər) - bu mərhələdə süni intellekt əsasən ekspert sistemləri formasında inkişaf etdi. Bu sistemlər müəyyən bir sahədə (məsələn, tibb, mühəndislik, maliyyə, eləcə də hərbi) mütəxəssislərin biliklərini bazaya daxil edərək qərarlar qəbul edirdilər. MYCIN (1975) adlı tibbi ekspert sistemi bakterial infeksiyaları, daha sonra yaradılan belə yönəmli sistemlər insanlarda yaranan xəstəlikləri diaqnozlaşdırmaq üçün istifadə olunurdu. Lakin, qeyd etmək də lazımdır ki, belə sistemlərin son nəticələri aidiyyatı mütəxəssislər tərəfindən mütləq şəkildə yoxlanılırdı və ümumi nəticə əldə edilirdi.

3. Neyron şəbəkələr və sistem öyrənilməsi dövrü (1990–2010-cu illər) - kompüterlərin hesablama gücünün artması nəticəsində neyron şəbəkələr, genetik alqoritmlər və sistem öyrənilməsi sahələri sürətlə inkişaf etdi. Bu dövrdə süni intellekt sistemləri böyük məlumat bazaları ilə işləməyə başladı.

4. Müasir dövr (2010–bu gün) - bu mərhələ dərin öyrənmə (Deep Learning) texnologiyalarının və bulud hesablama infrastrukturunun inkişafı ilə səciyyələnir. Google, OpenAI, Meta və digər nəhəng şirkətlər tərəfindən yaradılan sistemlər - ChatGPT, AlphaGo, Bard, Copilot və s. - yüksək keyfiyyətlə mətn, səs, şəkil və video emalı bacarığına malikdirlər.

Süni intellekt artıq yalnız bir elmi sahəsi deyil, həm də iqtisadi, sosial və etik təsirləri olan qlobal texnoloji inqilabın əsas qüvvəsidir [5, 6].

IV. SÜNİ İNTELLEKTİN KİBERTƏHLÜKƏSİZLİYƏ İNTEQRASİYASI

İnformasiya sistemlərinə kibertəhdidlərin müasir xüsusiyyətlərindən biri onların yüksək dərəcədə avtomatlaşdırılmış və adaptiv olmasıdır. Hücumlar getdikcə daha çox süni intellekt və avtomatlaşdırılmış alqoritmlər vasitəsilə həyata keçirilir [11]. Bu isə ənənəvi təhlükəsizlik yanaşmalarının – xüsusilə imza (signature-based) və qayda əsaslı sistemlərin – effektivliyini əhəmiyyətli dərəcədə azaldır. Belə sistemlər yalnız əvvəlcədən məlum olan təhdidləri aşkar edə bilir və yeni, daha mürəkkəb hücumlara qarşı zəif qalır.

Bu kontekstdə süni intellektin kibertəhlükəsizlik sistemlərində tətbiqi xüsusi əhəmiyyət kəsb edir. Süni intellekt böyük həcmli məlumatları analiz etmək, gizli qanunauyğunluqları aşkar etmək və anomaliyaları müəyyən etmək qabiliyyətinə malikdir. Bu xüsusiyyətlər ona real-vaxt rejimində qərarvermə və proqnozlaşdırma imkanı verir. Nəticədə kibertəhlükəsizlik sistemləri daha çevik, adaptiv və effektiv hala gəlir.

Bununla yanaşı, süni intellektin tətbiqi yalnız müdafiə məqsədləri ilə məhdudlaşmır [12]. Kibercinayətkarlar da süni

intellekt texnologiyalarından istifadə edərək daha mürəkkəb və gizli hücumlar həyata keçirirlər. Bu isə kiberməkanda "texnoloji yarış" fenomenini yaradır və təhlükəsizlik strategiyalarının daim yenilənməsini tələb edir.

Ənənəvi kibertəhlükəsizlik sistemləri çox vaxt yalnız əvvəlcədən proqramlaşdırılmış qaydalarla (alqoritmlə) işləyir və dəyişkən şəraitə uyğunlaşmaqda çətinlik çəkir. Lakin süni intellektin tətbiqi bu məhdudiyyətləri aradan qaldırır. Məsələn, maşın öyrənməsi alqoritmləri vasitəsilə sistemlər dinamik olaraq yeni məlumatlardan nəticə çıxara və öz fəaliyyətini təkmilləşdirə bilir [13].

Bu gün süni intellekt sistemləri kibertəhlükəsizlik sahəsində mühüm rol oynayır və misal olaraq göstərilənləri yerinə yetirə bilir:

- Anomaliya aşkarlama sistemləri şəbəkə trafiki və istifadəçi davranışlarını analiz edərək qeyri-normal fəaliyyətləri müəyyənləşdirir.
- Proqnozlaşdırıcı modellər potensial təhlükələri əvvəlcədən qiymətləndirərək müdafiə mexanizmlərini aktivləşdirir.
- Real-vaxt rejimində təhlükəli fəaliyyətləri üzə çıxarır və təhlil edir.
- Real-vaxt rejimində kiberhücumları aşkar edir və qarşısını alır.

Ümumilikdə süni intellektin kibertəhlükəsizlikdə tətbiqi mühafizə olunan sistemdə trafik monitorinqinə, məlumatların qorunmasına, anomaliyaların aşkarlanmasına, ünsiyyətlərin analizinə, antivirus sistemlərinin fəaliyyətinə, real-vaxtda müdafiənin pozulmasının və sistemə olan hücumların qarşısının alınmasına, məlumatları analiz etməyə, riskləri qiymətləndirməyə, avtomatik qərar verməyə imkan yaradır.

Süni intellektin kibertəhlükəsizlik sistemlərinə inteqrasiyası aşağıdakı üstünlükləri təmin edir:

- Əsas proseslərin intellektual avtomatlaşdırılması;
- Əldə olunan böyük həcmli məlumatların sürətli və dəqiq təhlili;
- Qərar qəbuletmədə insan faktorunun azaldılması;
- İstifadəçi davranışına uyğun adaptiv sistemlərin formalaşdırılması.

Bu baxımdan, süni intellekt kibertəhlükəsizlik sistemlərini passiv müdafiə platformasından aktiv intellektual qərar mexanizminə çevirir [14, 15].

Bununla belə, süni intellektin təhlükəsizlik sistemlərinə tətbiqi ilə bağlı müəyyən risklər də mövcuddur. Məsələn, alqoritmlərin yanlış öyrədilməsi və ya məlumatların manipulyasiyası saxta nəticələrə səbəb ola bilər. Bu səbəbdən etik və hüquqi tənzimləmə mexanizmləri xüsusi əhəmiyyət kəsb edir [8, 9].

NƏTİCƏ

Aparılan təhlillər göstərir ki, süni intellekt kibertəhlükəsizlik sahəsində keyfiyyətcə yeni mərhələnin formalaşmasına səbəb olmuşdur. Müasir kibertəhdidlərin mürəkkəbliyi və dinamikliyi ənənəvi təhlükəsizlik sistemlərinin imkanlarını məhdudlaşdırdığı halda, süni intellekt texnologiyaları bu boşluğu doldurараq daha effektiv və adaptiv müdafiə mexanizmləri təqdim edir.

Lakin süni intellektin tətbiqi ilə yanaşı yeni risklər də meydana çıxır. Adversarial hücumlar və süni intellekt əsaslı kiberhücumlar bu sahənin əsas problemləri sırasındadır. Bu risklər süni intellekt sistemlərinin etibarlılığını və təhlükəsizliyini təmin etmək üçün əlavə tədbirlərin görülməsini zəruri edir.

Eyni zamanda etik və hüquqi məsələlər də xüsusi əhəmiyyət kəsb edir. Məlumatların məxfiliyi, şəxsi məlumatların qorunması və süni intellektin qərarvermə prosesində şəffaflığın təmin edilməsi müasir dövrdə aktual problemlərdən biridir. Bu baxımdan süni intellektin tətbiqi yalnız texnoloji deyil, həm də hüquqi və etik çərçivədə tənzimlənməlidir.

Gələcək perspektivlər baxımından süni intellektin kibertəhlükəsizlik sahəsində rolu daha da artacağı gözlənilir. Xüsusilə avtonom təhlükəsizlik sistemlərinin yaradılması və süni intellekt əsaslı təhlükəsizlik əməliyyat mərkəzlərinin inkişafı bu sahənin əsas istiqamətləri kimi qiymətləndirilir.

Nəticə etibarilə, süni intellekt kibertəhlükəsizlik strategiyalarının ayrılmaz tərkib hissəsinə çevrilmişdir. Onun effektiv tətbiqi kibertəhdidlərə qarşı mübarizədə mühüm üstünlüklər yaratsa da, bu texnologiyanın yaratdığı risklər də nəzərə alınmalı və kompleks yanaşma tətbiq olunmalıdır. Bu baxımdan süni intellektin inkişafı və tətbiqi balanslaşdırılmış, təhlükəsiz və davamlı şəkildə həyata keçirilməlidir.

ƏDƏBİYYAT

[1] Azərbaycan Respublikası, Rəqəmsal transformasiya konsepsiyası 2022–2026, Bakı, Azərbaycan, 2022.

[2] Azərbaycan Respublikası, Şəxsi məlumatlar haqqında Qanun, Bakı, Azərbaycan, 2010.

[3] S. Russell and P. Norvig, Artificial Intelligence: A Modern Approach, 4th ed. Upper Saddle River, NJ, USA: Pearson, 2021.

[4] A. Turing, "Computing machinery and intelligence," Mind, vol. 59, no. 236, pp. 433–460, Oct. 1950.

[5] B. Marr, Artificial Intelligence in Practice. Hoboken, NJ, USA: Wiley, 2020.

[6] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.

[7] J. Kaplan, Artificial Intelligence: What Everyone Needs to Know. Oxford, UK: Oxford University Press, 2016.

[8] European Commission, "Proposal for a Regulation on Artificial Intelligence (AI Act)," Brussels, Belgium, Tech. Rep., 2021.

[9] UNESCO, "Recommendation on the ethics of artificial intelligence," Paris, France, Tech. Rep., 2021.

[10] N. Nilsson, Artificial Intelligence: A New Synthesis. San Francisco, CA, USA: Morgan Kaufmann, 1998.

[11] NIST, "Cybersecurity Framework (CSF)," National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep. NIST CR 1-110, 2023.

[12] Gartner, "Artificial intelligence security trends report," Gartner Inc., Stamford, CT, USA, Tech. Rep., pp. 1–85, 2024.

[13] McKinsey & Company, "The state of AI in cybersecurity," McKinsey Global Institute, New York, NY, USA, Tech. Rep., pp. 1–70, 2023.

[14] Cisco, "Cybersecurity threat trends report," Cisco Systems, San Jose, CA, USA, Tech. Rep., pp. 1–95, 2024.

[15] MIT Technology Review, "AI and cybersecurity research papers," MIT, Cambridge, MA, USA, Tech. Review

Cybersecurity and Artificial Intelligence

Fazil Ashumov
Military Administration Institute, Baku, Azerbaijan
fazil.ashumov@mmu.edu.az

Abstract – The article analyses the role and application possibilities of artificial intelligence in the field of cybersecurity. In the modern era, the increasing complexity and rapid growth of cyber threats reduce the effectiveness of traditional security methods. From this perspective, artificial intelligence technologies play an important role in the real-time detection of threats, prediction of attacks, and establishment of automated defence mechanisms. The article examines the application of approaches such as machine learning, deep learning, and behavioural analysis in cybersecurity. At the same time, risks and ethical issues related to the use of artificial intelligence are also considered.

Keywords – artificial intelligence; cybersecurity; machine learning; expert systems; management information systems; autonomous systems; cyber defence.