Süni İntellekt Əsaslı Kibertəhlükəsizlik Mexanizmləri və Milli Kibersuverenlik

Rəşad Rəsulzadə
Dövlət Təhlükəsizliyi Xidmətinin Heydər Əliyev adına Akademiyası, Bakı, Azərbaycan
rashad.rasulzada@gmail.com

***Xülasə*— Müasir rəqəmsal transformasiya şəraitində artan və mürəkkəbləşən kiberhücumlar dövlətlərin milli təhlükəsizliyinə ciddi təhdid yaradır və kiberməkanı suverenliyin strateji komponentinə çevirir. Məqalədə süni intellekt əsaslı kibertəhlükəsizlik mexanizmlərinin dövlət səviyyəsində tətbiq imkanları və milli informasiya infrastrukturunun qorunmasında rolu təhlil edilir. Maşın və dərin öyrənmə alqoritmlərinin anomaliyaların aşkarlanması, təhlükələrin erkən müəyyənləşdirilməsi və proqnozlaşdırılmasındakı effektivliyi araşdırılır. Bununla yanaşı, yerli məlumat bazalarının məhdudluğu, xarici texnoloji asılılıq və modellərin izah edilə bilənliyi kimi elmi-praktiki problemlər sistemli şəkildə qiymətləndirilir. Tədqiqat çərçivəsində milli kibersuverenliyin gücləndirilməsi üçün institusional və texnoloji yanaşmalar üzrə tövsiyələr irəli sürülür.**

Açar sözlər— süni intellekt; kibertəhlükəsizlik arxitekturası; maşın öyrənmə; təhlükəsizlik; kibersuvenerlik.

I. GİRİŞ

XXI əsrdə dövlətlərin gücü yalnız hərbi və iqtisadi göstəricilərlə deyil, həm də rəqəmsal infrastruktura nəzarət imkanları ilə ölçülür. Elektron hökumət sistemləri, maliyyə infrastrukturu, enerji şəbəkələri və telekommunikasiya sistemləri informasiya texnologiyalarına əsaslanır. Azərbaycan Respublikasında rəqəmsal transformasiya dövlət strategiyasının prioritet istiqamətlərindən biri kimi müəyyən edilmişdir.

Lakin rəqəmsallaşma paralel olaraq hücum səthini genişləndirir. Müasir hücumlar avtomatlaşdırılmış botnet şəbəkələri, süni intellektlə gücləndirilmiş phishing kampaniyaları və sıfır-gün zəifliklərı vasitəsilə həyata keçirilir. Klassik imza əsaslı sistemlər yalnız əvvəlcədən məlum hücumları aşkar edə bilir və naməlum təhlükələrə qarşı effektiv deyil [1].

Tədqiqat işində [1] göstərilir ki, maşın öyrənməsi metodlarının tətbiqi ənənəvi qapalı təhlükəsizlik modelindən kənara çıxmağı tələb edir. Tədqiqat işində [2] isə intrusion detection sistemlərində maşın öyrənməsi metodlarının effektivliyi geniş şəkildə təhlil olunmuşdur.

Bu baxımdan süni intellekt əsaslı müdafiə mexanizmləri milli kibersuverenliyin təmin olunmasında strateji alət kimi çıxış edir.

A. Suverenlik Konsepsiyasının Transformasiyası

Ənənəvi suverenlik anlayışı ərazi, sərhəd və fiziki resurslara nəzarət üzərində qurulmuşdur. Lakin rəqəmsal mühitdə sərhədlər virtual xarakter daşıyır. Tədqiqat işində [3] internet idarəçiliyinin müasir dövrdə dövlət hakimiyyətinin yeni forması olduğu qeyd olunur.

Kibersuverenlik aşağıdakı elementləri əhatə edir:

- İnformasiya axınlarına nəzarət
- Rəqəmsal infrastruktura milli nəzarət
- Texnoloji müstəqillik
- Milli məlumat təhlükəsizliyi siyasəti

B. Azərbaycan Respublikasında İnformasiya Təhlükəsizliyi Strategiyası

Azərbaycan Respublikasında rəqəmsal hökumət modelinin inkişafı çərçivəsində informasiya təhlükəsizliyi prioritet istiqamət kimi müəyyən edilmişdir. Dövlət qurumlarının rəqəmsal transformasiyası milli kibertəhlükəsizlik sisteminin gücləndirilməsini tələb edir.

Milli CERT strukturları, dövlət məlumat mərkəzləri və kritik infrastrukturun qorunması mexanizmləri kibersuverenliyin institusional əsasını təşkil edir.

III. SÜNİ İNTELLEKT TEXNOLOGİYALARININ TEXNİKİ ƏSASLARI

A. Maşın Öyrənməsi Modelləri

Nəzarətli öyrənmə metodları (Random Forest, SVM, Gradient Boosting) şəbəkə trafikinin təsnifatı üçün istifadə olunur [2]. Bu modellər etiketlənmiş məlumatlar əsasında hücum və normal trafik arasında fərqi öyrənir.

Nəzarətsiz öyrənmə metodları isə klasterləşdirmə və anomaliya aşkarlanması üçün tətbiq edilir. Bu yanaşma xüsusilə naməlum hücumların aşkarlanmasında əhəmiyyətlidir [4].

B. Dərin Öyrənmə Arxitekturaları

Konvolyusion neyron şəbəkələri (CNN) trafik nümunələrinin xüsusiyyətlərini çıxarmaq üçün istifadə olunur. Rekurrent neyron şəbəkələri (RNN və LSTM) isə zaman asılılığı olan hücumların aşkarlanmasında effektivdir [5].

C. Böyük Verilənlər və Real Vaxt Analitika

Milli SOC mərkəzlərində saniyədə milyonlarla hadisə qeydə alınır. Bu məlumatların real vaxt rejimində emalı üçün paylanmış hesablama infrastrukturu tələb olunur.

DOI: 10.25045/cyber.gov.2026.34

IV. Süni İntellekt Əsaslı Təhlükəsizlik Arxitekturası

A. SIEM və SOAR Sistemləri

SIEM sistemləri təhlükəsizlik hadisələrini mərkəzləşdirilmiş şəkildə toplayır və analiz edir. Süni intellekt bu sistemlərə inteqrasiya edilərək anomaliya aşkarlanmasını avtomatlaşdırır.

SOAR sistemləri isə aşkarlanan insidentlərə avtomatik cavab mexanizmləri tətbiq edir.

B. Davranış Əsaslı Təhlükəsizlik

İstifadəçi və qurğu davranışının modelləşdirilməsi daxili təhdidlərin aşkarlanmasında effektivdir. Bu yanaşma insider risklərin qarşısının alınmasında mühüm rol oynayır.

C. Adversarial Risklər

Goodfellow və digərləri göstərmişdir ki, süni intellekt modelləri xüsusi manipulyasiya edilmiş giriş məlumatları ilə yanıla bilər [6]. Bu isə əlavə qoruma mexanizmlərinin tətbiqini tələb edir.

V. Kritik İnfrastrukturun Süni İntellekt Əsaslı Müdafiəsi

A. Enerji İnfrastrukturunun Qorunması

Enerji sistemləri dövlətin strateji təhlükəsizlik komponentlərindən biridir. Elektrik paylayıcı şəbəkələr, SCADA sistemləri və sənaye nəzarət mexanizmləri kiberhücumlara qarşı həssasdır. Ənənəvi təhlükəsizlik sistemləri sənaye protokollarının spesifik xüsusiyyətlərini nəzərə almaqda çətinlik çəkir.

Süni intellekt əsaslı davranış modelləri sənaye şəbəkələrində normal əməliyyat parametrlərini öyrənərək qeyri-adi dəyişiklikləri müəyyən edə bilər. Bu yanaşma xüsusilə enerji ötürülməsi zamanı manipulyasiya cəhdlərinin erkən aşkarlanmasında effektivdir.

B. Maliyyə Sistemlərinin Müdafiəsi

Bank və ödəniş infrastrukturu milli iqtisadi sabitliyin əsasını təşkil edir. Süni intellekt əsaslı fraud detection sistemləri tranzaksiya davranışını analiz edərək şübhəli əməliyyatları müəyyən edir. Maşın öyrənməsi modelləri real vaxt rejimində risk skoru hesablayaraq potensial təhlükələri bloklaya bilir [2].

C. Telekommunikasiya Şəbəkələri

Telekommunikasiya infrastrukturu dövlət idarəçiliyinin fasiləsizliyini təmin edir. DDoS hücumları və siqnal manipulyasiyası hallarında süni intellekt əsaslı trafik analiz sistemləri hücum nümunələrini erkən mərhələdə aşkar edə bilər [4].

VI. Azərbaycan Respublikasında Süni İntellekt Əsaslı Milli Təhlükəsizlik Modeli

A. Konseptual Arxitektura

Azərbaycan kontekstində süni intellekt əsaslı kibertəhlükəsizlik modeli aşağıdakı təbəqələrdən ibarət ola bilər:

1) Məlumat Toplama Təbəqəsi (loglar, trafik, endpoint məlumatları)
2) Məlumat Emalı və Normalizasiya
3) Süni İntellekt Analitik Modulu
4) Risk Qiymətləndirmə Sistemi
5) Avtomatik Cavab Mexanizmi (SOAR)

Bu struktur milli SOC mərkəzlərində tətbiq oluna bilər.

B. Milli Datasetlərin Formalaşdırılması

Effektiv model qurmaq üçün yerli trafik və insident məlumatlarının toplanması vacibdir. Dövlət qurumları arasında təhlükəsizlik məlumatlarının anonimləşdirilmiş paylaşımı modelin dəqiqliyini artırar.

C. Kadr Potensialının İnkişafı

Süni intellekt və kibertəhlükəsizlik sahəsində mütəxəssislərin hazırlanması milli kibersuverenliyin əsas şərtlərindən biridir. Universitetlər və dövlət qurumları arasında əməkdaşlıq mexanizmləri gücləndirilməlidir.

VII. Elmi-Praktiki Problemlərin Geniş Təhlili

A. Modelin Etibarlılığı və Overfitting Problemi

Maşın öyrənməsi modelləri bəzən yalnız təlim verilənlər bazasına uyğunlaşır və real mühitdə zəif nəticə göstərə bilər. Bu problem overfitting kimi tanınır və təhlükəsizlik sistemlərində yanlış pozitivlərin artmasına səbəb ola bilər [2].

B. Adversarial Hücumların Təhlükəsi

Goodfellow və digərləri göstərmişdir ki, xüsusi manipulyasiya edilmiş giriş məlumatları modelin qərar mexanizmini dəyişə bilər [6]. Milli təhlükəsizlik sistemlərində bu risk xüsusi diqqət tələb edir.

C. İzah Oluna Bilənlik və Hüquqi Məsuliyyət

Dərin öyrənmə modelləri “qara qutu” xarakteri daşıyır. Dövlət qərarvermə sistemlərində şəffaflıq vacib olduğundan izah edilə bilən süni intellekt yanaşmaları tətbiq olunmalıdır [7].

D. Texnoloji Asılılıq Problemi

Xarici platformalara həddindən artıq asılılıq milli təhlükəsizlik riskləri yarada bilər. Yerli alqoritmlərin və proqram təminatının hazırlanması strateji əhəmiyyət daşıyır.

VIII. Risk Modelləşdirilməsi və Strateji Ssenarilər

A. Kiber Müharibə Ssenariləri

Müasir dövrdə kiberhücumlar dövlətlərarası qarşıdurmanın yeni forması kimi çıxış edir. Kritik infrastruktura qarşı koordinasiyalı hücumlar iqtisadi və sosial sabitliyi poza bilər.

B. Hibrid Təhdidlər

Kiberhücumlar informasiya müharibəsi və dezinformasiya kampaniyaları ilə birlikdə həyata keçirilə bilər. Süni intellekt əsaslı media monitorinq sistemləri saxta məlumatların aşkarlanmasında istifadə oluna bilər.

C. Risk İndikatorlarının Formalaşdırılması

Risk indikatorları aşağıdakı parametrlərə əsaslana bilər:

- Hücum tezliyi;
- Hücum mənbəyi;
- Zərər səviyyəsi;
- Sistem zəiflik indeksi.

Süni intellekt bu indikatorları dinamik şəkildə yeniləyərək real vaxt risk xəritəsi formalaşdıra bilər.

IX. Strateji Tövsiyələr və Milli Yol Xəritəsi

1) Milli Süni İntellekt Təhlükəsizlik Platformasının yaradılması
2) Dövlət qurumları üçün vahid təhlükəsizlik məlumat paylaşım sistemi
3) Yerli kibertəhlükəsizlik laboratoriyalarının yaradılması
4) Akademik-tətbiqi tədqiqat mərkəzlərinin formalaşdırılması
5) Süni intellekt modellərinin təhlükəsizlik audit mexanizmi
6) Milli məlumat lokallaşdırma siyasətinin gücləndirilməsi

Nəticə

Süni intellekt əsaslı kibertəhlükəsizlik mexanizmləri milli kibersuverenliyin təmin olunmasında strateji rol oynayır. Azərbaycan Respublikasında rəqəmsal transformasiya prosesinin sürətlənməsi bu texnologiyaların tətbiqini zəruri edir. Yerli texnoloji həllərin hazırlanması, milli datasetlərin formalaşdırılması və kadr potensialının gücləndirilməsi uzunmüddətli rəqəmsal müstəqilliyin əsasını təşkil edir. Süni intellektin təhlükəsizlik arxitekturasına inteqrasiyası yalnız texniki məsələ deyil, eyni zamanda strateji və institusional yanaşma tələb edir. Kompleks və sistemli tətbiq modeli milli təhlükəsizlik sisteminin dayanıqlılığını artıraraq Azərbaycan Respublikasının rəqəmsal suverenliyini möhkəmləndirə bilər.

ƏDƏBİYYAT

[1] R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," Proc. IEEE Symposium on Security and Privacy, 2010.

[2] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016.

[3] L. DeNardis, The Global War for Internet Governance. Yale University Press, 2014.

[4] P. Garcia-Teodoro et al., "Anomaly-Based Network Intrusion Detection," Computers & Security, 2009.

[5] J. Saxe and K. Berlin, "Deep Neural Network Based Malware Detection," IEEE, 2015.

[6] I. Goodfellow et al., "Explaining and Harnessing Adversarial Examples," ICLR, 2015.

[7] A. Adadi and M. Berrada, "Explainable Artificial Intelligence," IEEE Access, 2018.

Artificial Intelligence-Based Cybersecurity Mechanisms and National Cyber Sovereignty

Rashad Rasulzada

The Academy of the State Security Service of the Republic of Azerbaijan named after Heydar Aliyev, Baku, Azerbaijan

Abstract— In the context of modern digital transformation, growing and increasingly complex cyber-attacks pose a serious threat to states' national security and turn cyberspace into a strategic component of sovereignty. The article analyses the potential for the application of artificial intelligence-based cybersecurity mechanisms at the state level and their role in protecting the national information infrastructure. The effectiveness of machine and deep learning algorithms in anomaly detection, threat identification, and forecasting is examined. Furthermore, scientific and practical challenges such as the limitations of local databases, external technological dependence, and the explainability of models are systematically assessed. The research offers recommendations on institutional and technological approaches to strengthen national cyber sovereignty.

Keywords— artificial intelligence; cybersecurity architecture; machine learning; security; cyber sovereignty.