ISSN: 2181-3906 2025

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 4 / ISSUE 5 / UIF:8.2 / MODERNSCIENCE.UZ

AI VA MACHINE LEARNING ASOSIDAGI TARMOQLARARO EKRANLAR: KIBERXAVFSIZLIKDA YANGI AVLOD YONDASHUVI

Ergashev Azizbek Xakimjon o'g'li
University of Management and Future Technologies
Kommunikatsiya va Raqamli Texnologiyalar kafedrasi Magistranti.

https://doi.org/10.5281/zenodo.15406051

Annotatsiya. *Ushbu maqolada sun'iy intellekt (AI) va mashinaviy o'rganish (Machine Learning, ML) texnologiyalariga asoslangan tarmoqlararo ekranlar (firewall)ning kiberxavfsizlikdagi o'rni va ahamiyati ko'rib chiqiladi. Maqolada an'anaviy tarmoqlararo ekranlar bilan solishtirilganda AI va ML asosidagi tizimlarning afzalliklari, real vaqt rejimida tahdidlarni aniqlash, moslashuvchanlik va oldindan ogohlantirish imkoniyatlari yoritiladi. Yangi avlod tarmoq himoya vositalarining arxitekturasi, ishlash prinsiplari hamda amaliy qo'llanilish holatlari tahlil qilinadi.*

Kalit so'zlar: *sun'iy intellekt, mashinaviy o'rganish, kiberxavfsizlik, tarmoqlararo ekran, aqlli xavfsizlik tizimi, tahdidlarni aniqlash.*

МЕЖСЕТЕВЫЕ ЭКРАНЫ НА ОСНОВЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И МАШИННОГО ОБУЧЕНИЯ: ПОДХОД НОВОГО ПОКОЛЕНИЯ К КИБЕРБЕЗОПАСНОСТИ

Аннотация. *В данной статье рассматривается применение технологий искусственного интеллекта (ИИ) и машинного обучения (МО) в современных межсетевых экранах нового поколения. Представлены преимущества ИИ-основных решений по сравнению с традиционными системами, такие как способность выявлять угрозы в реальном времени, адаптивность и возможность предиктивного анализа. Также анализируется архитектура, принципы работы и практическое применение интеллектуальных систем безопасности в корпоративных, государственных и облачных инфраструктурах.*

Ключевые слова: *искусственный интеллект, машинное обучение, кибербезопасность, межсетевой экран, интеллектуальная защита, анализ угроз.*

AI AND MACHINE LEARNING-BASED CROSS-NETWORK SCREENS: A NEXT-GENERATION APPROACH TO CYBERSECURITY

Abstract. *This article explores the implementation of Artificial Intelligence (AI) and Machine Learning (ML) technologies in next-generation firewalls. It highlights the advantages of AI-powered solutions over traditional systems, such as real-time threat detection, adaptability, and predictive capabilities. The article also examines the architecture, operational principles, and real-world applications of intelligent security systems in enterprise, government, and cloud infrastructures.*

Keywords: *artificial intelligence, machine learning, cybersecurity, firewall, intelligent protection, threat detection.*

Kirish

Raqamli transformatsiya jarayonida barcha sohalar internet va axborot texnologiyalariga tobora ko'proq tayanmoqda.

Shu bilan birga, kiberxavfsizlik masalalari ham dolzarb ahamiyat kasb etmoqda.

Tarmoqlararo ekranlar (firewalls) – bu tarmoqni ichki va tashqi tahdidlardan himoya qiluvchi muhim vositalardan biridir. Ammo an'anaviy tarmoqlararo ekranlar zamonaviy tahdidlar, xususan murakkab, o'zgaruvchan va avtomatlashtirilgan kiberhujumlarga qarshi yetarlicha samarali bo'la olmayapti. Shu sababli, yangi avlod tarmoqlararo ekranlar, xususan sun'iy intellekt (AI) va mashinaviy o'rganish (ML) asosidagi echimlar jadal rivojlanmoqda.

An'anaviy tarmoqlararo ekranlarning chegaralari

Tarmoqlararo ekranlar (firewall) axborot xavfsizligi sohasida uzoq yillardan beri asosiy himoya vositasi sifatida xizmat qilib kelmoqda. Ularning asosiy vazifasi — tarmoq ichiga yoki tarmoqdan tashqariga chiqayotgan trafikni tahlil qilish va xavfsizlik siyosatlari asosida ruxsat berish yoki rad etishdan iborat. Ammo zamonaviy kiberxavflar murakkablashgan sayin, quyidagi kamchiliklar an'anaviy tarmoqlararo ekranlarda yaqqol namoyon bo'lmoqda:

- **Statik qoida asosidagi ishlash**: Qo'llanilayotgan siyosatlar o'zgarmas, bu esa dinamik tahdidlarga moslasha olmaydi.
- **Shifrlangan trafikni tahlil qilmaslik**: HTTPS orqali amalga oshirilayotgan tahdidlar ko'pincha e'tibordan chetda qoladi.
- **Zamonaviy tahdidlar – APT, AI-dastakli viruslar, 0-day ekspluatlar – aniqlanmaydi**.
- **Qo'lda sozlash zaruriyati**: Katta tarmoqlarda siyosatlarni doimiy ravishda yangilab borish resurs va vaqt talab qiladi.

Shu sababli tarmoq xavfsizligini ta'minlashda ilg'or yondashuvlar – xususan **AI va ML texnologiyalari asosida qurilgan tizimlar** zarurati keskin oshmoqda.

AI va ML asosidagi tarmoqlararo ekranlarning texnologik afzalliklari

AI va ML yordamida qurilgan tarmoqlararo ekranlar (Intelligent Firewalls) an'anaviy uslublarga nisbatan bir qancha ustunliklarga ega:

1 Real vaqtli tahdidlarni aniqlash

AI asosidagi tizimlar doimiy ravishda trafikni o'rganib, o'zgarishlarni aniqlaydi. Bu orqali tahdidlar yuzaga kelishidan avval ularni aniqlash va bloklash imkoni paydo bo'ladi.

2 Anomaliya asosida tahlil qilish

AI nafaqat belgilangan siyosatlarni, balki har bir paket yoki foydalanuvchi harakatlaridagi odatiy bo'lmagan xatti-harakatlarni (anomalies) aniqlaydi. Misol: tarmoqda birdan ortiq joydan bir xil IP orqali kirish urinishlari.

3 Doimiy o'rganish (self-learning)

Mashinaviy o'rganish modellari yangi trafik naqshlari (patterns)ni aniqlab, o'zini avtomatik tarzda yangilaydi. Bu xususiyat tahdidlarning o'zgaruvchan tabiatiga moslashishga yordam beradi.

4 Kontekstual tahlil

AI model foydalanuvchi lokatsiyasi, qurilma turi, soat zonasi, odatiy ish soati va boshqa faktorlarga asoslangan holda tahdid ehtimolini hisoblaydi.

5 Xatolik darajasining pasayishi

AI va ML asosida qurilgan ekranlar noto'g'ri ijobiy va salbiy aniqlash holatlarini kamaytiradi. Bu esa tarmoq ma'murlarining ishini osonlashtiradi.

Texnik arxitektura va ishlash mexanizmi

AI asosida ishlovchi tarmoqlararo ekranlar odatda quyidagi modullardan tashkil topadi:

Modul nomi	Funktsiyasi
Trafik monitoring moduli	Tarmoq orqali o‘tadigan barcha trafikni yig‘adi va qayd qiladi.
Xatti-harakatni aniqlovchi modul (Behavioral Analysis)	Har bir foydalanuvchi yoki qurilmaning odatiy harakatini o‘rganadi.
Mashinaviy o‘rganish modeli (ML Engine)	To‘plangan trafik asosida modelni o‘rgatadi va tahdidlarni aniqlashga moslashtiradi.
Qaror qabul qilish moduli (Decision Layer)	Aniqlangan harakatga qarab ruxsat berish, bloklash yoki ogohlantirish harakatlarini bajaradi.
Ma’lumotlar bazasi va loglash	Har bir tahdid haqida to‘liq log yuritadi, analiz uchun imkoniyat yaratadi.

Bu tizimlar nafaqat signaturalar asosida, balki **kontekstual va xulqiy ma’lumotlar** asosida qaror chiqaradi – bu esa ularni ancha aqlli qiladi.

Amaliy qo‘llanilish holatlari

1 Korporativ infratuzilmalarda

Katta kompaniyalarda AI asosidagi tarmoqlararo ekranlar DLP (Data Loss Prevention) va SIEM tizimlari bilan birga ishlaydi. Masalan, **Palo Alto Networks Cortex XDR** korporativ tarmoqlarda ko‘plab tahdidlarni real vaqt rejimida aniqlaydi.

2 Bulutli muhitda

AWS, Azure va GCP kabi platformalarda AI asosidagi ekranlar (masalan, **Fortinet FortiAI**) foydalanuvchining virtual mashinalarini himoya qiladi, container-based muhitlarni nazorat ostiga oladi.

3 Milliy xavfsizlik tizimlarida

Davlat muassasalari AI asosidagi tarmoqlararo ekranlarni strategik tarmoqlarni himoya qilishda ishlatadi. Bu orqali 0-day va APT (Advanced Persistent Threats) hujumlar oldi olinadi.

Tahdidlar va muammolar

AI asosidagi tizimlar mukammal bo‘lsa-da, ba’zi kamchiliklarga ega:

- **Model o‘rgatishdagi noto‘g‘ri ma’lumotlar** noto‘g‘ri tahdid aniqlashga olib keladi.
- **AI tizimlarining aldanishi (Adversarial Attacks)**: kiberjinoyatchilar AI’ni chalg‘itish uchun manipulyatsiyalangan trafik yuborishi mumkin.
- **Hisoblash resurslari talabi**: chuqur neyron tarmoqlari katta hisoblash quvvatini talab qiladi.
- **Yurisdiksiya va maxfiylik**: ma’lumotlarni AI orqali doimiy monitoring qilish foydalanuvchi maxfiyligi bilan bog‘liq muammolarni keltirib chiqaradi.

Kelajak tendensiyalari

- **Explainable AI (XAI)**: qaror chiqarish jarayonlarini izohlash imkoniyati.
- **Federated Learning**: ma’lumotlarni markazlashtirmasdan, har bir tugunda o‘rganish.

- **AI-integratsiyalashgan SIEM**: hodisalarni kuzatish va bashorat qilishni yanada samarali qilish.
- **5G tarmoqlarda AI-Firewall**: past kechikishli xavfsizlik mexanizmlari.

Xulosa

Bugungi kunda raqamli dunyo tobora murakkablashib borar ekan, kiberxavfsizlik sohasi ham an’anaviy yondashuvlardan voz kechib, sun’iy intellekt va mashinaviy o‘rganish texnologiyalariga tayanmoqda. Ayniqsa, AI va ML asosidagi tarmoqlararo ekranlar – yangi avlod xavfsizlik tizimlari sifatida shakllanib bormoqda. Ushbu tizimlar nafaqat oddiy trafikni tahlil qiladi, balki foydalanuvchining xatti-harakatlarini, muhitdagi o‘zgarishlarni, kontekstual ma’lumotlarni chuqur o‘rganadi va real vaqt rejimida tahdidlarni aniqlab, ularga qarshi choralar ko‘radi.

Tahlillar shuni ko‘rsatmoqdaki, AI integratsiyalashgan xavfsizlik tizimlari an’anaviy signatura va qoidalar asosida ishlovchi ekranlardan sezilarli darajada samaraliroqdir. Ular murakkab va ilg‘or tahdidlar, ayniqsa 0-day ekspluatlar, APT (Advanced Persistent Threats) hujumlari va shifrlangan trafik orqali beriladigan zararli ta’sirlarni aniqlashda o‘zini oqlamoqda.

Shu bilan birga, bu texnologiyalarni amaliyotga joriy etish uchun muayyan muammolar mavjud: modellarni to‘g‘ri o‘rgatish, sun’iy intellektga nisbatan ishonchni ta’minlash, maxfiylik muammolari, hisoblash resurslari bilan bog‘liq cheklovlar va AI’ni aldatishga qaratilgan hujumlar (adversarial attacks). Ammo bu muammolar texnologik taraqqiyot orqali hal etilishi mumkin.

Kelajakda kiberxavfsizlik sohasida **“aqlli xavfsizlik”** konsepsiyasi keng tarqaladi. Har bir tarmoq elementi — foydalanuvchi qurilmasidan tortib, server va bulutli infrastrukturagacha — AI orqali boshqariladi, o‘rganiladi va himoya qilinadi. AI asosidagi tarmoqlararo ekranlar esa bu infratuzilmada markaziy rol o‘ynaydi.

Shunday qilib, **AI va ML texnologiyalariga asoslangan tarmoqlararo ekranlar — nafaqat zamonaviy tahdidlar bilan samarali kurashish vositasi, balki kelajakdagi kiberxavfsizlik me’zonlarini belgilovchi ustuvor yo‘nalishdir**. Texnik oliygohlar, ilmiy muassasalar va IT kompaniyalar bu sohada izlanishlar olib borib, ushbu texnologiyalarni milliy va korporativ infratuzilmalarga keng joriy etish yo‘lida faol harakat qilishlari lozim.

REFERENCES

1. Sommer, R., & Paxson, V. (2010). **Outside the Closed World: On Using Machine Learning for Network Intrusion Detection**. *IEEE Symposium on Security and Privacy.*
2. Kim, G., Lee, S., & Kim, S. (2014). **A novel hybrid intrusion detection method integrating anomaly detection with misuse detection**. *Expert Systems with Applications, 41*(4).
3. Sculley, D., et al. (2015). **Machine Learning: The High-Interest Credit Card of Technical Debt**. *NIPS.*
4. Fortinet (2023). **FortiAI: Artificial Intelligence for Cybersecurity** – Whitepaper.
5. Darktrace (2024). **Enterprise Immune System: AI for Cyber Defense** – Technical Overview.

6. Palo Alto Networks (2024). **Cortex XDR and the Role of ML in Threat Detection** – Product Documentation.
7. Moustafa, N., & Slay, J. (2015). **UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems**. *Military Communications and Information Systems Conference.*