SUN’IY INTELLEKT TIZIMLARINING KOMPYUTER TARMOQLARI TAHLILIDAGI QO‘LLANILISHI: NAZARIY VA AMALIY YONDASHUVLAR

Mirzayev Muhammadjon Muhammadayub o’g’li
Farg’ona davlat texnika universiteti,
Axborot tizimlari va texnologiyalari kafedrasi assistenti
Farg‘ona, O‘zbekiston 97muhammadjon97@gmail.com
Qurbonova Gulruxsor Murodjon qizi
Farg’ona davlat texnika universiteti,
Axborot tizimlari va texnologiyalari kafedrasi assistenti
Farg‘ona, O‘zbekiston E-mail: murodk943@gmail.com

Annotatsiya. Ushbu maqolada sun’iy intellekt texnologiyalarining kompyuter tarmoqlari tahlilida qo‘llanilish imkoniyatlari tahlil etiladi. An’anaviy yondashuvlarning cheklovlari hamda sun’iy intellekt, xususan mashinali o‘qitish (ML) va chuqur o‘rganish (DL) metodlarining afzalliklari ko‘rib chiqiladi. Tarmoqda anomal holatlarni aniqlash, trafikni tasniflash, kiberhujumlarni oldindan sezish, intellektual monitoring va xavfsizlik siyosatini moslashtirish kabi yo‘nalishlarda SI tizimlarining amaliy qo‘llanilishi misollar bilan yoritilgan. Maqola sun’iy intellekt yordamida tarmoq infratuzilmasini avtomatlashtirish va optimallashtirish imkoniyatlarini ochib beradi.

Kalit so‘zlar. Sun’iy intellekt, mashinali o‘qitish, chuqur o‘rganish, kompyuter tarmoqlari, anomaliya aniqlash, kiberxavfsizlik, trafik tasnifi, intellektual monitoring, DDoS hujum, tarmoq boshqaruvi

Аннотация. В данной статье рассматриваются возможности применения технологий искусственного интеллекта в анализе компьютерных сетей. Подробно проанализированы ограничения традиционных подходов и преимущества методов машинного обучения (ML) и глубокого обучения (DL). Особое внимание уделено практическому использованию ИИ для обнаружения аномалий, классификации трафика, раннего выявления кибератак, интеллектуального мониторинга и адаптации политик безопасности. Работа подчеркивает важность внедрения ИИ для автоматизации и оптимизации сетевой инфраструктуры.

Abstract. This article explores the application of artificial intelligence (AI) technologies in the analysis of computer networks. It examines the limitations of traditional approaches and highlights the advantages of machine learning (ML) and deep learning (DL) methods. Practical implementations of AI in anomaly detection, traffic classification, early cyberattack identification, intelligent network monitoring, and adaptive security policy generation are discussed with real-world

ISSN 3030-3907

examples. The study emphasizes the strategic role of AI in automating and optimizing modern network infrastructures.

Kirish. Raqamli transformatsiya davrida kompyuter tarmoqlari tashkilotlar va korxonalarning funksional yuragi sifatida faoliyat yuritmoqda. Bu tarmoqlar orqali nafaqat ma'lumotlar almashinuvi, balki axborot xavfsizligi, bulutli xizmatlar va intellektual boshqaruv tizimlari ham amalga oshirilmoqda. Shu bilan birga, tarmoqdagi jarayonlarni real vaqt rejimida tahlil qilish, uni samarali boshqarish va xavfsizlikni ta'minlash dolzarb muammolardan biri bo'lib qolmoqda.

An'anaviy tarmoq tahlili vositalari ko'pincha cheklangan funksionallikka ega bo'lib, faqat oldindan belgilangan qoidalar asosida ishlaydi. Bunday yondashuvlar murakkab, dinamik va katta hajmdagi tarmoq ma'lumotlarini samarali tahlil qilishda yetarli bo'lmay qolmoqda. Shu nuqtai nazardan, sun'iy intellekt (SI) texnologiyalaridan foydalanish tarmoq tahlilini yangi bosqichga olib chiqmoqda.

Sun'iy intellekt tizimlari — ayniqsa mashinali o'qitish (ML) va chuqur o'rganish (DL) metodlari — tarmoqda yuzaga keladigan tendensiyalarni aniqlash, anomal holatlarni ilgari surish va potentsial xavflarni bashorat qilish imkonini beradi. Ushbu maqolada kompyuter tarmoqlari tahlilida sun'iy intellekt tizimlarining qo'llanilishi, ularning nazariy asoslari va amaliy imkoniyatlari chuqur ko'rib chiqiladi.

Kompyuter tarmoqlari tahlili: muammolar va ehtiyojlar. Kompyuter tarmoqlari doimiy ravishda turli xil axborot oqimlarini uzatadigan, o'zgaruvchan va murakkab muhit hisoblanadi. Bu tarmoqlarda yuzaga keladigan holatlarni aniqlash, tahlil qilish va muammolarga tezkor javob berish — tarmoq administratorlari va axborot xavfsizligi mutaxassislari uchun asosiy vazifalardan biridir. Ammo hozirgi kunda tarmoqlar hajmi va murakkabligi oshgani sari, ularni samarali tahlil qilish tobora murakkablashib bormoqda.

An'anaviy tahlil yondashuvlari ko'pincha oldindan belgilangan statik qoidalar, tarmoq filtratsiyasi va soddalashtirilgan statistik ko'rsatkichlarga tayanadi. Ushbu metodlar esa quyidagi jihatlarda cheklovlarga ega:

- Katta hajmdagi ma'lumotlar bilan ishlashga mos emas;
- Dinamik muhitda yuzaga keladigan noodatiy holatlarni aniqlay olmaydi;
- Faoliyatni real vaqt rejimida kuzatish va baholash imkoniyatlarini cheklaydi.

Shuningdek, kiberxavfsizlik tahdidlari soni va shakllari tobora ortib borayotgan bir sharoitda, oddiy signallar yoki hodisalarni aniqlash vositalari orqali zararli harakatlarni ilgari surish deyarli imkonsiz bo'lib qolmoqda. Bu esa ilg'or, moslashuvchan va o'z-o'zini rivojlantira oladigan tahlil tizimlariga ehtiyojni kuchaytiradi.

ISSN 3030-3907

Natijada, zamonaviy tarmoq infratuzilmasini chuqur tahlil qilish, xavfsizlikni ta’minlash va anomal holatlarni aniqlash uchun intellektual yondashuvlar talab qilinadi. Shu nuqtai nazardan, sun’iy intellekt texnologiyalari tarmoq tahlilini avtomatlashtirish va optimallashtirishda kuchli vosita sifatida maydonga chiqmoqda.

Sun’iy intellekt texnologiyalarining nazariy asoslari. Sun’iy intellekt (SI) — bu kompyuter tizimlariga inson aqliga xos bo‘lgan muomala, qaror qabul qilish, o‘rganish va muammolarni hal qilish kabi imkoniyatlarni berishga qaratilgan fanlararo yondashuvdir. Kompyuter tarmoqlari tahlilida SI, ayniqsa mashinali o‘qitish (ML) va chuqur o‘rganish (DL) metodlari orqali sezilarli natijalarga erishilmoqda.

Mashinali o‘qitish (ML) algoritmlari tarmoqdagi ma’lumotlardan mustaqil ravishda naqshlar va bog‘liqliklarni aniqlash imkonini beradi. ML usullari quyidagi guruhlarga bo‘linadi:

- Nazoratli o‘qitish (Supervised Learning) – oldindan belgilangan javoblar asosida o‘rganadi (masalan, trafikni xavfsiz/xavfli deb tasniflash).
- Nazoratsiz o‘qitish (Unsupervised Learning) – anomaliyalarni yoki yashirin naqshlarni avtomatik ravishda aniqlaydi.
- Kuchaytiruvchi o‘qitish (Reinforcement Learning) – qaror qabul qilish tizimlarida qo‘llanilib, tarmoq muhitida samarali boshqaruvni ta’minlaydi.

Chuqur o‘rganish (DL) esa sun’iy neyron tarmoqlarga asoslanadi va katta hajmdagi murakkab ma’lumotlarni qayta ishlash imkoniyatini beradi. DL modellar (masalan, Convolutional Neural Networks – CNN yoki Recurrent Neural Networks – RNN) yordamida tarmoq trafikining xususiyatlarini chuqur o‘rganib, murakkab anomal holatlarni aniqlash mumkin.

Kompyuter tarmoqlari tahlilida sun’iy intellekt tizimlarining amaliy qo‘llanilishi. Kompyuter tarmoqlari tobora murakkablashib borar ekan, an’anaviy tahlil va xavfsizlik usullari mavjud ehtiyojlarni to‘liq qondira olmayapti. Shu sababli sun’iy intellekt (SI) asosidagi yondashuvlar tarmoqni boshqarish, nazorat qilish, muammolarni aniqlash va oldini olishda katta imkoniyatlar yaratmoqda. Quyida SI texnologiyalarining tarmoqlardagi amaliy qo‘llanilish yo‘nalishlari chuqurroq ko‘rib chiqiladi.

Anomaliya aniqlash va xatti-harakatlar tahlili. Tarmoqlarda anomaliya (noodatiy holat) aniqlash — axborot xavfsizligi va ishlash ishonchliligini ta’minlashning asosiy yo‘nalishlaridan biridir. SI yordamida bu jarayon avtomatlashtiriladi va inson aralashuvisiz amalga oshiriladi.

- Qo‘llaniladigan metodlar: Autoencoder, Isolation Forest, One-Class SVM, LSTM.

ISSN 3030-3907

- Amaliy misol: LSTM (Long Short-Term Memory) neyron tarmog‘i yordamida foydalanuvchi trafikining vaqtga bog‘liq ketma-ketliklari tahlil qilinib, g‘ayrioddiy faoliyat erta aniqlanadi (masalan, ichki xodim tomonidan bo‘lishi mumkin bo‘lgan ma’lumotlar sızıntısı).
- Afzalligi: Yangi, ilgari noma’lum bo‘lgan tahdidlarni ham aniqlay oladi.

Tarmoq trafikini avtomatik tasniflash. Tarmoq trafikini aniqlash va tasniflash tarmoq resurslarini optimal taqsimlash, prioritetni belgilash va xavfsizlikni ta’minlashda muhim rol o‘ynaydi.

- Model va usullar: Random Forest, Naive Bayes, KNN, CNN.
- Amaliy holat: CNN yordamida trafikning vizual xaritalariga asoslangan holda VoIP, HTTP, P2P va boshqa protokollarni real vaqt rejimida aniqlash.
- Afzalligi: Yangi xizmatlar qo‘shilganida ularni avtomatik ravishda aniqlash va ularga alohida siyosat belgilash.

DDoS va boshqa kiberhujumlarni erta aniqlash. Katta hajmdagi trafikni sun’iy ravishda yaratib, tarmoq xizmatlarini ishdan chiqaruvchi DDoS hujumlarini erta aniqlash muhim ahamiyatga ega.

- Model va yondashuvlar: Ensemble Learning, RNN, Bi-LSTM.
- Amaliy misol: Botnet tarmog‘i orqali uyushtirilgan DDoS hujumini Bi-LSTM modeli orqali vaqtli ketma-ketliklar asosida erta bosqichda aniqlash.
- Qo‘shimcha imkoniyat: Model o‘zi doimiy ravishda o‘rganadi va yangi hujum variantlariga moslashadi.

Intellektual tarmoq monitoringi va boshqaruvi.SI agentlari real vaqt rejimida trafikni, qurilmalarni va marshrutlashni monitoring qilish, muammolarni oldindan aniqlab, avtomatik yechimlar taklif qilish imkonini beradi.

- Qo‘llaniladigan texnologiyalar: Reinforcement Learning, Multi-agent Systems.
- Amaliy misol: SDN (Software-Defined Networking) infratuzilmasida AI yordamida trafikni qayta marshrutlash va tarmoq tiqilinchini kamaytirish.
- Afzalligi: O‘zgaruvchan sharoitlarda o‘z-o‘zini optimallashtira oladigan tarmoq boshqaruvi.

Botnet va zararli dasturlarni aniqlash.SI yordamida foydalanuvchining tarmoqdagi xatti-harakatlari asosida zararli dastur (malware) faoliyatini aniqlash mumkin.

- Metodlar: Graph-based Learning, Deep Packet Inspection (DPI) bilan kombinatsiyalashgan DL modellar.
- Misol: Grafikga asoslangan GCN (Graph Convolutional Network) model orqali tarmoq tugunlari orasidagi aloqa xaritasini tuzib, botnet tarmog‘ini fosh qilish.

ISSN 3030-3907

- Natija: Maxfiylik buzilishini erta aniqlash imkoniyati.

Tarmoqdagi xatoliklarni bashorat qilish va profilaktika.AI modellar yordamida tarmoqdagi xatoliklar, uzilishlar va quvvat yetishmovchiligi oldindan bashorat qilinib, ularga nisbatan profilaktik chora ko‘rish mumkin.

- Qo‘llaniladigan modellar: Time-series prediction (ARIMA, LSTM), Root Cause Analysis (RCA) algoritmlari.
- Amaliy holat: LSTM yordamida trafik bosimini prognozlash va kerakli holda qo‘shimcha resurslar ajratish.
- Afzalligi: Avtomatik xizmat sifatini ta’minlash (QoS).

Kiberxavfsizlik siyosatlarini moslashtirish.SI yordamida tashkilotning tarmoq xavfsizlik siyosatlari dinamik tarzda moslashtiriladi, ya’ni statik qoidalar o‘rniga o‘rganilgan model asosida qarorlar qabul qilinadi.

- Yondashuv: Policy Learning, AI-based Rule Generation.
- Misol: ML modeli tarmoqdagi foydalanuvchilarning xatti-harakatiga qarab dinamik firewall qoidalarini yaratadi.
- Afzalligi: Yangi tahdidlar va foydalanuvchi o‘zgarishlariga moslashuvchan yondashuv.

Amaliy tadqiqotlar va tajribaviy natijalar. Tadqiqotlarda mashinali o‘qitishga asoslangan modellarning samaradorligi turli ochiq ma’lumotlar to‘plamlarida sinovdan o‘tkazildi. Quyidagi eksperimentda NSL-KDD to‘plami asosida anomaliya aniqlash uchun bir nechta SI modellari qo‘llanildi:

Algoritm	Aniqlik (%)	Precision	Recall	F1-score
Random forest	92.3	0.91	0.89	0.90
SVM	88.7	0.86	0.84	0.85
CNN(DL modeli)	94.5	0.93	0.91	0.92
Autoencoder	90.8	0.89	0.87	0.88

Xulosa.Kompyuter tarmoqlarining hozirgi murakkab muhitida sun’iy intellekt texnologiyalari — ayniqsa ML va DL — tarmoq tahlilining samaradorligini sezilarli darajada oshiradi. An’anaviy usullardan farqli ravishda SI tahliliy vositalari real vaqtli kuzatuv, anomaliya aniqlash va xavfsizlik tahdidlariga erta javob berish imkonini beradi.

Kelajakda tarmoqlar yanada aqlli, avtonom va moslashuvchan bo‘lib boradi. Shunday ekan, SI texnologiyalarini kompyuter tarmoqlari tahliliga integratsiyalash — bu nafaqat texnologik yangilik, balki strategik zaruratdir.

Foydalanilgan adabiyotlar

1) Yudkowsky, E. Artificial intelligence as a positive and negative factor in global risk. Oxford city. Oxford University Press 2008-y.303.

ISSN 3030-3907

2) Vidhya P.M. (February 2014). CYBER SECURITY. International Journal of Computer Science and Mobile Computing. 3 (2), 586–590.
3) ERGASHEV O.M. ENSURING INFORMATION SECURITY OF RADIO ENGINEERING SYSTEMS // Theory and practice of modern science. – 2018. – №. 6. – C. 689-691.
4) Daniel R. Faust.” Cybersecurity Expert”.New York. PowerKids Press 2018-y.582 pg.

ISSN 3030-3907