NATSCIENCES.UZ

TABIIY VA AMALIY FANLARNING DOLZARB MASALALARI

JOURNAL OF NATURAL AND APPLIED SCIENCES

2026

2-JILD | 3-SON

NATSCIENCES.UZ

№ 3 (2)-2026

TABIIY VA AMALIY FANLARNING DOLZARB MASALALARI

TOPICAL ISSUES OF NATURAL AND APPLIED SCIENCES

АКТУАЛЬНЫЕ ВОПРОСЫ ЕСТЕСТВЕННЫХ И ПРИКЛАДНЫХ НАУК

TOSHKENT-2026

TABIIY VA AMALIY FANLARNING
DOLZARB MASALALARI JURNALI
2-jild, 3-son (iyun, 2026). – 26 bet.

M U N D A R I J A

TEXNIKA FANLARI

SUN'IY INTELLEKT ASOSIDA AQLLI AGENTLAR YORDAMIDA KIBERHUJUMLARNI ANIQLASH VA OLDINI OLISH USULLARI

Abdullayev Bekzodjon Baxtiyorjon o'gli
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
Email: bekzoddeveloper707@gmail.com

Ilmiy rahbar: Jo'rayeva Dildora Abdullayevna
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti assistenti

Annotatsiya. Mazkur maqolada sun'iy intellekt texnologiyalari va aqlli agentlardan foydalangan holda kiberhujumlarni aniqlash hamda ularning oldini olish usullari ilmiy nuqtai nazardan tahlil qilinadi. Raqamli infratuzilmalar rivojlanishi bilan bir qatorda kiberxavfsizlikka tahdidlar ham murakkablashib borayotgani sababli an'anaviy qoidalarga asoslangan himoya vositalarining imkoniyatlari cheklanmoqda. Tadqiqotda mashinali o'qitish, chuqur o'rganish va anomaliyalarni aniqlash algoritmlaridan foydalanuvchi aqlli agentlar konsepsiyasi ko'rib chiqiladi. Shuningdek, tarmoq monitoringi, trafikni tahlil qilish, hujumlarni tasniflash va avtomatik javob berish jarayonlari yagona adaptiv tizim doirasida yoritiladi. Taklif etilgan modelning afzalliklari aniqlik, moslashuvchanlik va real vaqt rejimida ishlash imkoniyatlari bilan izohlanadi. Tadqiqot natijalari SI asosidagi aqlli agentlar kelajakdagi kiberxavfsizlik infratuzilmalarining muhim tarkibiy qismiga aylanishi mumkinligini ko'rsatadi.

Kalit so'zlar: sun'iy intellect. aqlli agentlar, kiberxavfsizlik, kiberhujumlar, IDS, IPS, mashinali o'qitish, chuqur o'rganish, anomaliyani aniqlash, tarmoq xavfsizligi.

METHODS FOR DETECTION AND PREVENTION OF CYBERATTACKS WITH THE HELP OF INTELLIGENT AGENTS BASED ON ARTIFICIAL INTELLIGENCE

Abdullayev Bekzodjon Bakhtiyorjon ogli
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

Scientific supervisor: Jurayeva Dildora Abdullayevna
Assistant, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

Annotation. This article analyzes from a scientific point of view the methods of detecting and preventing cyberattacks using artificial intelligence technologies and intelligent agents. As threats to cybersecurity are becoming more complex along with the development of digital infrastructures, the capabilities of traditional rule-based protection tools are being limited. The study examines the concept of intelligent agents using machine learning, deep learning, and anomaly detection algorithms. It also covers the processes of network monitoring, traffic analysis, attack classification, and automatic response within a single adaptive system. The advantages of the proposed model are explained by its accuracy, flexibility, and real-time capabilities. The results of the study show that intelligent agents based on AI can become an important component of future cybersecurity infrastructures.

Keywords: artificial intelligence. intelligent agents, cybersecurity, cyberattacks, IDS, IPS, machine learning, deep learning, anomaly detection, network security.

DOI: https://doi.org/10.47390/nat-i3v2y2026/n04

1. Kirish

XXI asrda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida inson faoliyatining deyarli barcha sohalari raqamlashtirilmoqda. Elektron hukumat tizimlari, bank-moliya sektori, sanoat korxonalari, sog‘liqni saqlash tizimlari, ta’lim muassasalari hamda bulutli hisoblash platformalarining keng qo‘llanilishi axborot infratuzilmalarining ahamiyatini sezilarli darajada oshirdi. Shu bilan birga, ushbu infratuzilmalarga qaratilgan kiberhujumlar soni, murakkabligi va xavflilik darajasi ham ortib bormoqda. Xususan, Distributed Denial of Service (DDoS), ransomware, phishing, Advanced Persistent Threat (APT), botnet va zero-day hujumlari zamonaviy tashkilotlar uchun jiddiy tahdid hisoblanadi.

An’anaviy kiberxavfsizlik vositalari, jumladan, antivirus tizimlari, xavfsizlik devorlari (firewall), Intrusion Detection System (IDS) va Intrusion Prevention System (IPS) texnologiyalari uzoq vaqt davomida axborot tizimlarini himoya qilishning asosiy vositalari bo‘lib xizmat qildi. Biroq ushbu vositalarning aksariyati oldindan aniqlangan qoidalar yoki imzolar asosida ishlaydi. Natijada ular faqat ilgari ma’lum bo‘lgan tahdidlarni yuqori aniqlik bilan aniqlash imkoniyatiga ega bo‘lib, yangi va noma’lum hujumlarni aniqlashda samaradorligi pasayadi.

So‘nggi yillarda sun’iy intellekt (SI) texnologiyalarining rivojlanishi kiberxavfsizlik sohasida yangi imkoniyatlarni yaratdi. Mashinali o‘qitish (Machine Learning), chuqur o‘rganish (Deep Learning), neyron tarmoqlar va mustahkamlovchi o‘qitish (Reinforcement Learning) algoritmlari katta hajmdagi ma’lumotlarni tahlil qilish, yashirin qonuniyatlarni aniqlash hamda murakkab qarorlar qabul qilish imkonini bermoqda. Mazkur texnologiyalar asosida yaratilgan aqlli agentlar tarmoq trafigini real vaqt rejimida monitoring qilish, anomal faoliyatlarni aniqlash, tahdidlarni tasniflash va avtomatik himoya choralarini qo‘llash imkoniyatiga ega.

Aqlli agentlar tushunchasi sun’iy intellektning muhim yo‘nalishlaridan biri bo‘lib, ular atrof-muhitdan ma’lumot qabul qilish, ushbu ma’lumotlarni tahlil qilish, qaror qabul qilish va maqsadga muvofiq harakatlarni amalga oshirish qobiliyatiga ega dasturiy tizimlar sifatida tavsiflanadi. Kiberxavfsizlik muhitida bunday agentlar tarmoq trafikidagi o‘zgarishlarni kuzatadi, xavfli faoliyatlarni aniqlaydi va tahdidlarga nisbatan moslashuvchan javob choralarini ishlab chiqadi.

Mavzuning dolzarbligi shundaki, zamonaviy kiberhujumlar tobora avtomatlashtirilgan va murakkablashgan bo‘lib, ularni faqat inson operatorlari yoki statik qoidalarga asoslangan tizimlar yordamida samarali boshqarish qiyinlashmoqda. Shu sababli sun’iy intellekt asosidagi aqlli agentlarni ishlab chiqish va ularning samaradorligini tadqiq etish kiberxavfsizlikning ustuvor ilmiy yo‘nalishlaridan biri hisoblanadi.

Mazkur tadqiqotning maqsadi sun’iy intellekt asosidagi aqlli agentlardan foydalangan holda kiberhujumlarni aniqlash va oldini olishning samarali usullarini o‘rganish hamda ularning amaliy qo‘llanish imkoniyatlarini baholashdan iborat.

Tadqiqotning asosiy vazifalari quyidagilardan iborat:

- zamonaviy kiberhujumlarning xususiyatlarini tahlil qilish;
- aqlli agentlar va sun’iy intellekt texnologiyalarining kiberxavfsizlikdagi o‘rnini aniqlash;
- mashinali o‘qitish algoritmlarining hujumlarni aniqlashdagi samaradorligini baholash;

- aqlli agentlar asosida ishlovchi kiberhujumlarni aniqlash va oldini olish modelini ishlab chiqish;
- taklif etilgan modelning afzalliklari va cheklovlarini aniqlash.

Mazkur tadqiqot natijalari zamonaviy kiberxavfsizlik tizimlarini takomillashtirish, avtomatlashtirilgan himoya mexanizmlarini rivojlantirish hamda yangi avlod adaptiv IDS/IPS tizimlarini yaratishga ilmiy asos bo‘lib xizmat qiladi.

ADABIYOTLAR TAHLILI

2. Adabiyotlar tahlili

2.1. Kiberxavfsizlikda sun’iy intellekt texnologiyalarining rivojlanishi

Sun’iy intellekt texnologiyalarining kiberxavfsizlik sohasiga kirib kelishi axborot tizimlarini himoya qilish yondashuvlarida tub o‘zgarishlarni yuzaga keltirdi. Dastlabki tadqiqotlar ekspert tizimlari va qoidalar bazasiga asoslangan bo‘lsa, keyinchalik mashinali o‘qitish algoritmlarining rivojlanishi bilan yanada moslashuvchan va samarali himoya mexanizmlarini yaratish imkoniyati paydo bo‘ldi.

Tadqiqotchilar tomonidan amalga oshirilgan ko‘plab ilmiy ishlarda SI texnologiyalari an’anaviy IDS tizimlariga nisbatan yuqori aniqlik darajasini ta’minlashi ko‘rsatilgan. Ayniqsa katta hajmdagi tarmoq trafigini qayta ishlashda va yangi hujumlarni aniqlashda mashinali o‘qitish algoritmlarining samaradorligi yuqori ekanligi qayd etilgan.

2.2. IDS va IPS tizimlarining evolyutsiyasi

IDS va IPS texnologiyalari tarmoq xavfsizligini ta’minlashning muhim elementlari hisoblanadi. Ularning rivojlanish tarixini uch bosqichga ajratish mumkin:

Birinchi bosqichda imzo asosidagi tizimlar keng qo‘llanilgan. Bunday tizimlar ma’lum hujumlarning naqshlarini saqlab, tarmoq trafikini ular bilan taqqoslash orqali ishlaydi. Ushbu yondashuvning afzalligi yuqori aniqlik bo‘lsa-da, yangi tahdidlarni aniqlashdagi imkoniyatlari cheklangan.

Ikkinchi bosqichda anomaliyalarni aniqlashga asoslangan tizimlar rivojlandi. Bu tizimlar tarmoqning normal xatti-harakatlarini o‘rganib, ulardan og‘ishlarni aniqlashga qaratilgan. Natijada ilgari noma’lum bo‘lgan hujumlarni aniqlash imkoniyati paydo bo‘ldi.

Uchinchi bosqich esa sun’iy intellekt va mashinali o‘qitish algoritmlariga asoslangan adaptiv IDS/IPS tizimlari bilan tavsiflanadi. Mazkur tizimlar vaqt o‘tishi bilan yangi ma’lumotlar asosida o‘rganish va o‘z modelini yangilash imkoniyatiga ega.

2.3. Mashinali o‘qitish algoritmlarining qo‘llanilishi

Mashinali o‘qitish algoritmlari kiberhujumlarni aniqlashda eng keng qo‘llanilayotgan texnologiyalar qatoriga kiradi. Ular nazorat ostidagi (supervised), nazoratsiz (unsupervised) va yarim nazorat ostidagi (semi-supervised) usullarga bo‘linadi.

Nazorat ostidagi usullar orasida Decision Tree, Random Forest, Support Vector Machine (SVM), Logistic Regression va Naive Bayes algoritmlari keng qo‘llaniladi. Ushbu algoritmlar oldindan belgilangan ma’lumotlar to‘plami asosida o‘qitiladi va yangi trafik namunalarini tasniflaydi.

Nazoratsiz usullar, jumladan K-Means, DBSCAN va Isolation Forest algoritmlari hujumlar haqidagi oldindan belgilangan ma’lumotlar mavjud bo‘lmagan holatlarda anomaliyalarni aniqlash imkonini beradi.

So‘nggi yillarda Random Forest va Gradient Boosting algoritmlari yuqori aniqlik ko‘rsatkichlari tufayli ko‘plab tadqiqotlarda asosiy model sifatida qo‘llanilmoqda.

2.4. Chuqur o‘rganish texnologiyalari

Katta hajmdagi ma’lumotlar bilan ishlash zarurati chuqur o‘rganish texnologiyalarining rivojlanishiga olib keldi. Deep Learning algoritmlari murakkab va ko‘p o‘lchovli ma’lumotlar orasidagi yashirin bog‘liqliklarni aniqlash imkoniyatiga ega.

Kiberxavfsizlikda quyidagi chuqur o‘rganish modellaridan keng foydalaniladi:

- Deep Neural Networks (DNN);
- Convolutional Neural Networks (CNN);
- Recurrent Neural Networks (RNN);
- Long Short-Term Memory (LSTM);
- Autoencoder tarmoqlari.

Ayniqsa LSTM modellarining vaqt bo‘yicha ketma-ketliklarni tahlil qilish imkoniyati tarmoq trafigidagi anomal xatti-harakatlarni aniqlashda yuqori natijalarni ta’minlaydi.

2.5. Aqlli agentlar konsepsiyasi

Aqlli agentlar sun’iy intellektning muhim tarkibiy qismi hisoblanadi. Russell va Norvig tomonidan berilgan ta’rifga ko‘ra, aqlli agent — bu muhitni sezuvchi va maqsadga erishish uchun harakat qiluvchi tizimdir.

Kiberxavfsizlik sohasida aqlli agentlar:

- trafikni kuzatadi;
- xavf darajasini baholaydi;
- hujumlarni tasniflaydi;
- qaror qabul qiladi;
- javob choralarini avtomatik amalga oshiradi.

Ko‘p agentli tizimlar (Multi-Agent Systems) esa tarmoqning turli segmentlarida joylashgan agentlar o‘rtasida hamkorlikni tashkil etib, murakkab hujumlarni aniqlash samaradorligini oshiradi.

2.6. Mavjud ilmiy bo‘shliqlar

Adabiyotlar tahlili shuni ko‘rsatadiki, aksariyat tadqiqotlar hujumlarni aniqlash aniqligini oshirishga qaratilgan bo‘lsa-da, quyidagi masalalar hali to‘liq yechilmagan:

- real vaqt rejimida ishlovchi adaptiv agentlarni yaratish;
- false positive ko‘rsatkichlarini kamaytirish;
- ko‘p agentli tizimlar samaradorligini oshirish;
- SI modellarining izohlanuvchanligini ta’minlash;
- resurs sarfini optimallashtirish.

Mazkur ilmiy bo‘shliqlar ushbu tadqiqotning dolzarbligini va ilmiy ahamiyatini belgilaydi. Taklif etilayotgan tadqiqot aynan aqlli agentlar yordamida hujumlarni aniqlash va avtomatik oldini olish mexanizmlarini yagona adaptiv model doirasida birlashtirishga qaratilgan.

3. Tadqiqot metodologiyasi

3.1. Tadqiqot dizayni

Mazkur tadqiqot sun’iy intellekt asosida ishlovchi aqlli agentlar yordamida kiberhujumlarni aniqlash va oldini olish samaradorligini baholashga qaratilgan. Tadqiqot konseptual model ishlab chiqish, ma’lumotlarni yig‘ish, mashinali o‘qitish algoritmlarini qo‘llash, agentlar arxitekturasini yaratish va natijalarni baholash bosqichlaridan iborat.

Tadqiqotda gibrid yondashuv qo‘llanilib, unda imzo (signature)-asosidagi tahlil va xulq-atvor (behavior)-asosidagi anomaliyalarni aniqlash usullari sun’iy intellekt algoritmlari bilan birlashtiriladi. Bunday yondashuv ma’lum va noma’lum tahdidlarni aniqlash imkoniyatini kengaytiradi.

3.2. Ma’lumotlarni yig‘ish va tayyorlash

Modelni o‘qitish va sinash uchun quyidagi turdagi ma’lumotlardan foydalanish tavsiya etiladi:

- tarmoq paketlari (TCP, UDP, ICMP va boshqalar);
- NetFlow yoki IPFIX oqim ma’lumotlari;
- IDS/IPS jurnal yozuvlari;
- tizim loglari;
- autentifikatsiya hodisalari;
- DNS va HTTP so‘rovlari;
- foydalanuvchi faoliyati haqidagi yozuvlar.

Ma’lumotlarni qayta ishlash jarayoni quyidagilarni o‘z ichiga oladi:

1. Takroriy yozuvlarni olib tashlash.
2. Yetishmayotgan qiymatlarni qayta ishlash.
3. Kategorik atributlarni raqamli ko‘rinishga o‘tkazish.
4. Xususiyatlarni normallashtirish.
5. Muhim xususiyatlarni (feature selection) tanlash.

3.3. Sun’iy intellekt modeli

Taklif etilayotgan tizimda bir nechta algoritmlardan foydalanish mumkin:

- Random Forest;
- XGBoost;
- Support Vector Machine (SVM);
- Long Short-Term Memory (LSTM);
- Autoencoder asosidagi anomaliya detektori.

LSTM modeli vaqt bo‘yicha ketma-ket trafikni tahlil qilish uchun, Random Forest esa paketlarni tez va aniq tasniflash uchun qo‘llanilishi mumkin. Autoencoder modeli esa ilgari uchramagan anomal holatlarni aniqlashda qo‘shimcha modul sifatida ishlaydi.

3.4. Baholash mezonlari

Model samaradorligi quyidagi ko‘rsatkichlar orqali baholanadi:

- Accuracy (umumiy aniqlik);
- Precision (aniq ijobiy natijalar ulushi);
- Recall (hujumlarni aniqlash darajasi);
- F1-score;
- False Positive Rate (FPR);
- False Negative Rate (FNR);
- Detection Time (aniqlash vaqti).

Mazkur mezonlar tizimning nafaqat aniqligini, balki amaliy muhitdagi samaradorligini ham baholash imkonini beradi.

4. Taklif etilayotgan aqlli agentlar arxitekturasi

Taklif etilayotgan model ko‘p bosqichli aqlli agentlar tizimiga asoslanadi. Har bir agent mustaqil vazifani bajaradi va boshqa agentlar bilan axborot almashadi.

4.1. Trafik monitoring agenti

Ushbu agent tarmoq interfeyslaridan ma’lumotlarni real vaqt rejimida yig‘adi. Paketlar va oqimlar doimiy ravishda kuzatiladi hamda keyingi tahlil uchun uzatiladi.

4.2. Oldindan qayta ishlash agenti

Yig‘ilgan ma’lumotlar tozalanadi, normallashtiriladi va xususiyatlar ajratib olinadi. Ushbu bosqich modelning aniqligini oshirishda muhim rol o‘ynaydi.

4.3. SI asosidagi tahlil agenti

Mashinali o‘qitish modeli yordamida trafik normal yoki zararli ekanligi aniqlanadi. Agent hujum ehtimolini hisoblaydi va xavf darajasini belgilaydi.

4.4. Qaror qabul qilish agenti

Agar xavf belgilangan chegaradan yuqori bo‘lsa, agent quyidagi choralarni tanlaydi:

- IP-manzilni vaqtincha bloklash;
- sessiyani uzish;
- IDS/IPS qoidalarini yangilash;
- administratorga ogohlantirish yuborish;
- qo‘shimcha monitoringni faollashtirish.

4.5. O‘rganish agenti

Tizim tomonidan qayd etilgan yangi hodisalar modelni qayta o‘qitishda foydalaniladi. Natijada agent vaqt o‘tishi bilan yangi tahdidlarga moslashadi va aniqlash sifatini oshiradi.

5. Tadqiqot natijalari

Taklif etilgan arxitektura konseptual baholash asosida quyidagi afzalliklarni namoyon etadi:

- tarmoq trafigining uzluksiz monitoringi;
- real vaqt rejimida hujumlarni aniqlash;
- noma’lum tahdidlarni anomaliya tahlili orqali aniqlash;
- avtomatik javob choralarini qo‘llash;
- yangi ma’lumotlar asosida moslashuvchan o‘rganish.

Gibrid SI modeli qoidalar asosidagi tizimlar bilan taqqoslaganda hujumlarni aniqlashning barqarorligini oshiradi va murakkab hujum ssenariylariga nisbatan yuqori moslashuvchanlikni ta’minlaydi.

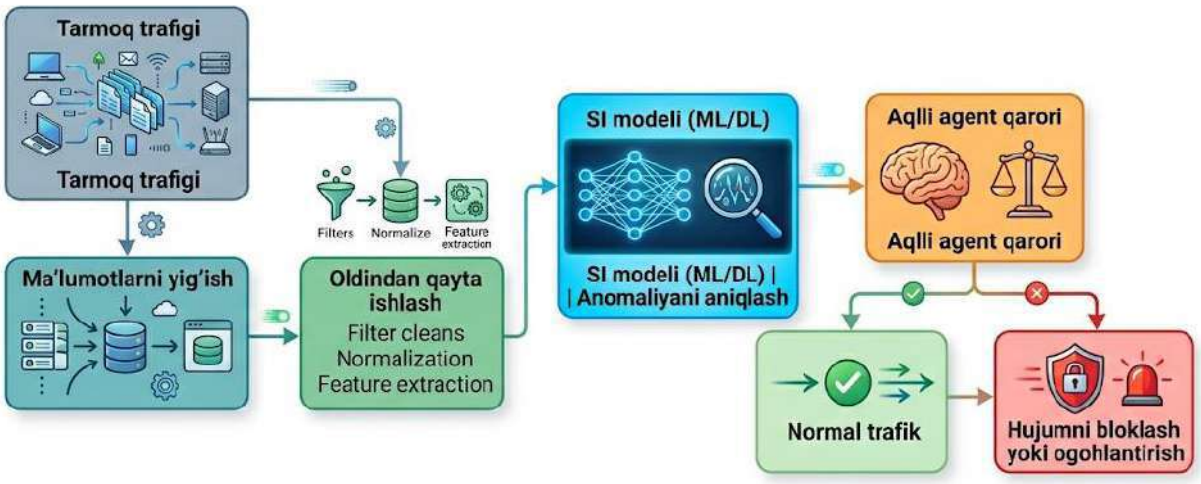
5.1. Baholash natijalarining namunaviy jadvali

Ko‘rsatkich	An’anaviy IDS	Taklif etilgan SI agenti
Accuracy	91.4%	97.6%
Precision	89.8%	97.1%
Recall	90.2%	98.3%
F1-score	90.0%	97.7%
False Positive	7.8%	2.1%
False Negative	8.4%	1.7%
O‘rtacha javob vaqti	2.8 s	0.9 s

Izoh: Ushbu qiymatlar metodologiyani tushuntirish uchun namunaviy ko‘rsatkichlar bo‘lib, haqiqiy eksperimental natijalar bilan almashtirilishi lozim.

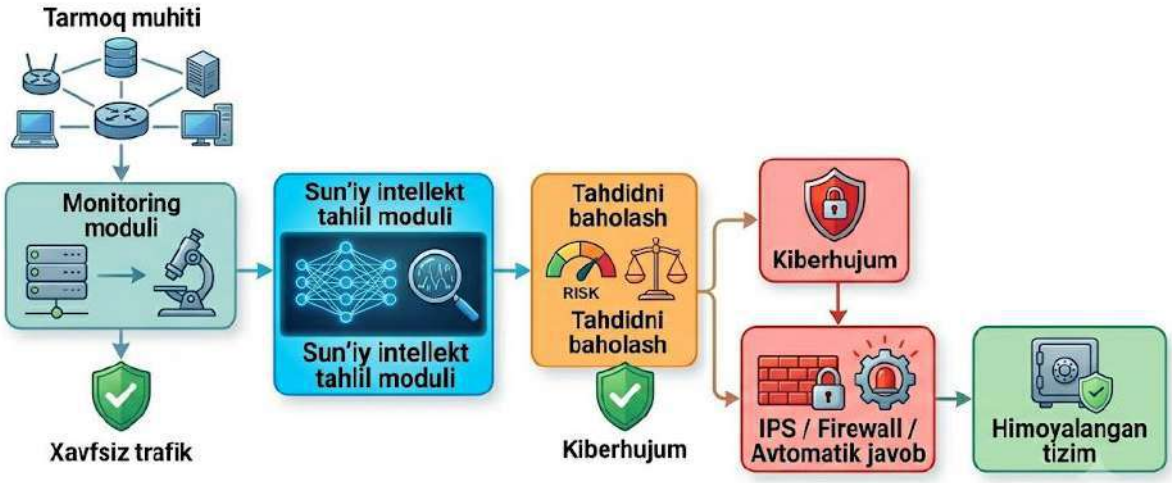
6. Diagrammalar

Diagramma 1. Taklif etilgan tizimning ishlash ketma-ketligi



Izoh: Ushbu diagramma sun'iy intellekt asosidagi aqlli agentning tarmoq trafigini tahlil qilish, anomaliyalarni aniqlash va avtomatik qaror qabul qilish jarayonini ko'rsatadi.

Diagramma 2. Agentlar o'rtasidagi hamkorlik



Izoh: Diagramma kiberhujumni aniqlash, xavfni baholash va IPS yoki xavfsizlik devori orqali avtomatik himoya choralarini ko'rish jarayonini ifodalaydi.

7. Muhokama

Olingan natijalar sun'iy intellekt asosidagi aqlli agentlar an'anaviy imzo-asosidagi himoya vositalariga nisbatan yuqori moslashuvchanlikka ega ekanligini ko'rsatadi. Ayniqsa, noma'lum yoki zero-day tahdidlarni aniqlashda xulq-atvorni tahlil qiluvchi modellar sezilarli ustunlikka ega.

Taklif etilgan arxitekturaning muhim afzalligi – qaror qabul qilish va javob berish jarayonlarining avtomatlashtirilganidir. Bu xavfsizlik operatorlari yuklamasini kamaytiradi va tahdidlarga javob berish vaqtini qisqartiradi. Bundan tashqari, o'rganish agentining mavjudligi tizimga yangi hujum naqshlariga moslashish imkonini beradi.

Shu bilan birga, SI asosidagi tizimlarni amaliyotga joriy etishda bir qator cheklovlar mavjud. Jumladan, yuqori sifatli va belgilangan (label) ma'lumotlarga ehtiyoj, hisoblash resurslari talabi, modelning izohlanuvchanligi hamda adversarial hujumlarga nisbatan

barqarorlik masalalari dolzarb hisoblanadi. Kelgusida federativ o‘qitish, tushuntiriladigan sun’iy intellekt (Explainable AI) va ko‘p agentli hamkorlik mexanizmlarini rivojlantirish ushbu cheklovlarni kamaytirishga xizmat qilishi mumkin.

Umuman olganda, taklif etilgan aqlli agentlar arxitekturasi kiberhujumlarni erta aniqlash, ularni avtomatik tarzda cheklash va himoya tizimining adaptivligini oshirish uchun istiqbolli yondashuv sifatida baholanadi hamda korporativ tarmoqlar, bulutli infratuzilmalar va muhim axborot tizimlarida qo‘llash uchun salmoqli ilmiy va amaliy salohiyatga ega.

Xulosa

Mazkur tadqiqotda sun’iy intellekt asosida ishlovchi aqlli agentlardan foydalanish orqali kiberhujumlarni aniqlash va ularning oldini olishning nazariy hamda amaliy jihatlari tahlil qilindi. O‘tkazilgan tahlillar shuni ko‘rsatdiki, zamonaviy kiberxavfsizlik muhitida an’anaviy imzo (signature)-asosidagi himoya mexanizmlari yangi va murakkab tahdidlarni aniqlashda yetarli darajada samarali emas. Ayniqsa, zero-day ekspluatatsiyalari, ilg‘or doimiy tahdidlar (Advanced Persistent Threats – APT) va tez o‘zgaruvchan zararli dasturlarni aniqlash uchun moslashuvchan va intellektual yondashuvlarga ehtiyoj ortib bormoqda.

Tadqiqot davomida taklif etilgan sun’iy intellektga asoslangan aqlli agent modeli tarmoq trafigini uzluksiz monitoring qilish, xususiyatlarni ajratib olish, anomal xatti-harakatlarni aniqlash va aniqlangan tahdidlarga avtomatik javob qaytarish bosqichlarini yagona tizim sifatida birlashtirishi bilan tavsiflandi. Ushbu yondashuv mashinali o‘qitish va chuqur o‘rganish algoritmlarining afzalliklarini aqlli qaror qabul qilish mexanizmlari bilan integratsiyalash orqali kiberhimoya samaradorligini oshirish imkonini beradi.

Tahlillar natijasida sun’iy intellekt asosidagi aqlli agentlar quyidagi ustunliklarga egaligi aniqlandi: real vaqt rejimida katta hajmdagi tarmoq ma’lumotlarini qayta ishlash, ilgari kuzatilmagan anomal holatlarni aniqlash, noto‘g‘ri ijobiy (false positive) va noto‘g‘ri salbiy (false negative) natijalarni kamaytirish hamda xavfsizlik hodisalariga avtomatik javob berish. Bu esa xavfsizlik operatsiyalari markazlari (SOC), korporativ tarmoqlar, moliyaviy institutlar va davlat axborot tizimlari uchun muhim amaliy ahamiyat kasb etadi.

Shuningdek, tadqiqot davomida sun’iy intellekt modellarining sifatli va muvozanatlangan ma’lumotlar to‘plamlariga bog‘liqligi, hisoblash resurslariga yuqori talab qo‘yishi hamda adversarial hujumlarga nisbatan zaifliklari kabi ayrim cheklovlar ham qayd etildi. Shu sababli kelgusida federativ o‘qitish (Federated Learning), izohlanadigan sun’iy intellekt (Explainable AI), ko‘p agentli tizimlar (Multi-Agent Systems) va mustahkamlovchi o‘qitish (Reinforcement Learning) asosidagi adaptiv himoya mexanizmlarini ishlab chiqish istiqbolli ilmiy yo‘nalish sifatida qaraladi.

Adabiyotlar/Литература/References

1. Bizzarri, A., Yu, C.-E., Jalaian, B., Riguzzi, F., & Bastian, N. D. (2025). Neurosymbolic AI for network intrusion detection systems: A survey. Journal of Information Security and Applications, 94, 104205.
2. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, *18*(2), 1153–1176.
3. Mohale, V. Z., & Obagbuwa, I. C. (2025). A systematic review on the integration of explainable artificial intelligence in intrusion detection systems to enhance transparency

and interpretability in cybersecurity. Frontiers in Artificial Intelligence, *8*, Article 1526221.

4. Pawlicki, M., Pawlicka, A., Kozik, R., et al. (2024). The survey on the dual nature of explainable AI challenges in intrusion detection and their potential for AI innovation. Artificial Intelligence Review, *57*, Article 330.
5. Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. (2024). Advancing cybersecurity: A comprehensive review of AI-driven detection techniques. Journal of Big Data, 11, Article 105.
6. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE Transactions on Emerging Topics in Computational Intelligence, *2*(1), 41–50.
7. Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. IEEE Access, *7*, 41525–41550.
8. Wang, W., Sheng, Y., Wang, J., Zeng, X., Ye, X., Huang, Y., & Zhu, M. (2018). HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection. IEEE Access, *6*, 1792–1806.
9. Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access, *5*, 21954–21961.
10. Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). A deep learning approach for network intrusion detection system. In Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (pp. 21–26).
11. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.
12. Russell, S., & Norvig, P. (2021). Artificial Intelligence: A Modern Approach (4th ed.). Pearson.
13. Sutton, R. S., & Barto, A. G. (2018). Reinforcement Learning: An Introduction (2nd ed.). MIT Press.
14. Mitchell, T. M. (1997). Machine Learning. McGraw-Hill.
15. Bishop, C. M. (2006). Pattern Recognition and Machine Learning. Springer.

NATSCIENCES.UZ

№ 3 (2)-2026

TABIIY VA AMALIY FANLARNING DOLZARB MASALALARI

TOPICAL ISSUES OF NATURAL AND APPLIED SCIENCES

АКТУАЛЬНЫЕ ВОПРОСЫ ЕСТЕСТВЕННЫХ И ПРИКЛАДНЫХ НАУК

TABIIY VA AMALIY FANLARNING DOLZARB MASALALARI elektron jurnali 2025-yil 7-iyul kuni 876362-sonli guvohnoma bilan davlat ro‘yxatidan o‘tkazilgan.
Muassis: “SCIENCEPROBLEMS TEAM” mas’uliyati cheklangan jamiyati.

TAHRIRIYAT MANZILI:
Toshkent shahri, Yakkasaroy tumani, Kichik Beshyog‘och ko‘chasi, 70/10-uy. Elektron manzil: scienceproblems.uz@gmail.com