TARMOQDA SUN'IY INTELLEKT YORDAMIDA KIBER TAHDIDLARNI REAL VAQTDA ANIQLASH.

***Ibragimov SH.M.*[1] *Abdumajidova M.SH.*[2]**

[1]*FarDU dotsenti, shavkat19702008@gmail.com*

[2]*FarDU talabasi, muxlisa100404@gmail.com*

Annotatsiya: Ushbu maqolada sun'iy intellekt yordamida tarmoqdagi kiber tahdidlarni real vaqt rejimida aniqlash usullari ilmiy va amaliy jihatdan tahlil qilinadi. Zamonaviy kiberxavfsizlik tizimlarida mashinaviy o'qitish, neyron tarmoqlar va avtomatlashtirilgan monitoring texnologiyalarining qo'llanilishi o'rganilgan. Shuningdek, real vaqt rejimida ishlovchi xavfsizlik tizimlarining samaradorligi, afzalliklari va mavjud muammolari yoritilgan.

Kalit so'zlar: sun'iy intellekt, kiberxavfsizlik, tarmoq xavfsizligi, mashinaviy o'qitish, real vaqt monitoringi, IDS, IPS, neyron tarmoqlar, kiber tahdid, avtomatlashtirilgan himoya.

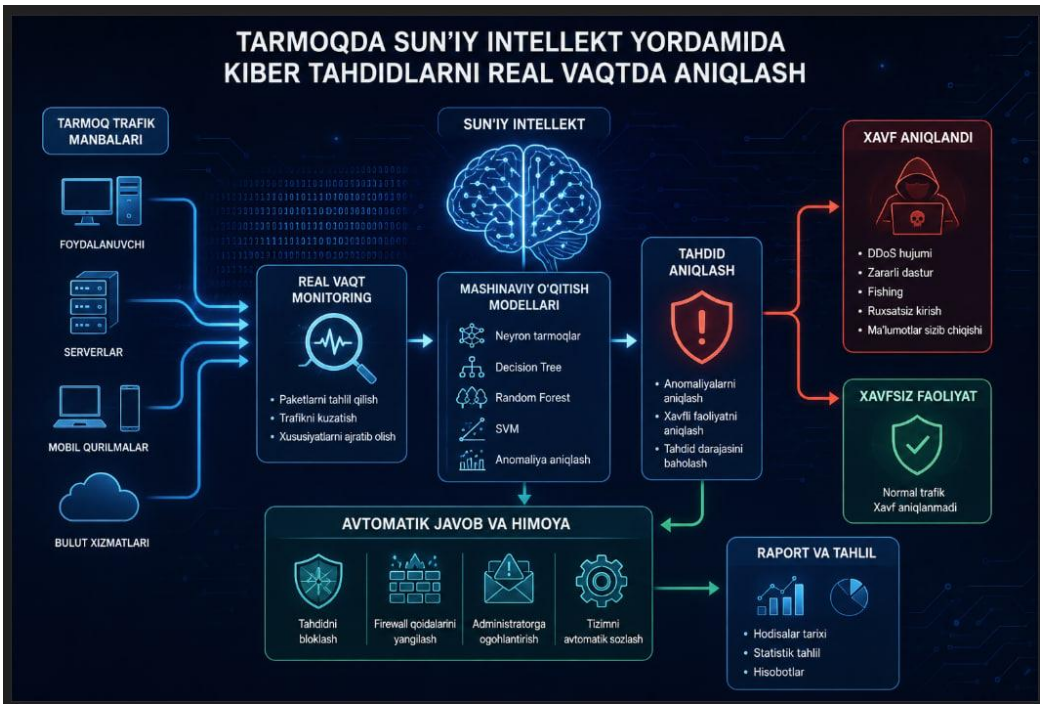
KIRISH

XXI asrda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida internet tarmoqlari va raqamli infratuzilmalardan foydalanish keskin ortdi. Davlat tashkilotlari, bank tizimlari, ta'lim muassasalari va yirik korxonalar o'z faoliyatini global tarmoqlarsiz tasavvur qila olmaydi. Shu bilan birga, kiberjinoyatchilik va tarmoq hujumlari soni ham ortib bormoqda. Zamonaviy kiber tahdidlar orasida DDoS hujumlari, fishing, ransomware, zararli dasturlar va ma'lumotlar o'g'irlanishi kabi xavfli holatlar mavjud bo'lib, ular axborot xavfsizligiga jiddiy zarar yetkazadi.

An'anaviy xavfsizlik tizimlari asosan oldindan belgilangan qoidalar asosida ishlaydi. Bunday tizimlar yangi va murakkab hujumlarni aniqlashda yetarli samaradorlikni ko'rsatmaydi. Shu sababli sun'iy intellekt texnologiyalaridan

foydalanish zamonaviy kiberxavfsizlikning muhim yo‘nalishiga aylandi. Sun’iy intellekt katta hajmdagi ma’lumotlarni tezkor tahlil qilish, anomal holatlarni aniqlash va tahdidlarni avtomatik ravishda bashorat qilish imkonini beradi.

So‘nggi yillarda mashinaviy o‘qitish va neyron tarmoqlar asosidagi xavfsizlik tizimlari real vaqt rejimida ishlovchi himoya vositalari sifatida keng qo‘llanilmoqda. Ayniqsa, katta hajmdagi tarmoq trafikini tahlil qilish va xavfli faoliyatni qisqa vaqt ichida aniqlash zamonaviy kiberxavfsizlikning asosiy talablaridan biri hisoblanadi. Shu sababli sun’iy intellekt asosidagi xavfsizlik tizimlarini o‘rganish muhim ilmiy va amaliy ahamiyatga ega.



ADABIYOTLAR TAHLILI VA USULLAR

Sun’iy intellekt yordamida kiber tahdidlarni aniqlash texnologiyalari so‘nggi yillarda ilmiy tadqiqotlarning muhim yo‘nalishiga aylandi. Ilmiy manbalarda mashinaviy o‘qitish algoritmlarining tarmoq xavfsizligini ta’minlashdagi samaradorligi keng yoritilgan. Tadqiqotlar shuni ko‘rsatadiki, sun’iy intellekt asosidagi tizimlar an’anaviy xavfsizlik vositalariga nisbatan yuqori aniqlik va tezkorlikka ega.

Mashinaviy o‘qitish algoritmlari yordamida tarmoqdagi normal va zararli trafikni farqlash mumkin. Decision Tree, Random Forest va Support Vector Machine kabi algoritmlar kiber tahdidlarni aniqlashda samarali hisoblanadi.

Sun’iy intellekt algoritmlarining kiber tahdidlarni aniqlashdagi samaradorligi 1-jadval

Algoritm nomi	**Ishlash tezligi**	**Aniqlik darajasi**	**Afzalliklari**	**Kamchiliklari**
Decision Tree	Yuqori	O‘rtacha	Oddiy va tez ishlaydi	Murakkab tahdidlarni aniqlash qiyin
Random Forest	Yuqori	Yuqori	Aniqlik darajasi yuqori	Hisoblash resursi ko‘proq talab etadi
Support Vector Machine (SVM)	O‘rtacha	Yuqori	Kichik xatolik bilan ishlaydi	Katta ma’lumotlarda sekin ishlaydi
Sun’iy neyron tarmoqlar	O‘rtacha	Juda yuqori	Murakkab tahdidlarni aniqlaydi	Katta ma’lumot va GPU talab qiladi
Deep Learning	Pastroq	Juda yuqori	Yangi tahdidlarni aniqlaydi	O‘qitish jarayoni murakkab

1-jadvaldan ko‘rinib turibdiki, sun’iy intellekt algoritmlari orasida neyron tarmoqlar va Deep Learning texnologiyalari murakkab kiber tahdidlarni aniqlashda yuqori samaradorlikka ega. Shu bilan birga, ular katta hajmdagi hisoblash resurslarini talab qiladi.

Ayniqsa, chuqur o‘rganish texnologiyalari va sun’iy neyron tarmoqlar murakkab hujumlarni aniqlash imkoniyatini kengaytirmoqda.

IDS va IPS tizimlari ham zamonaviy kiberxavfsizlikning muhim komponentlari hisoblanadi. IDS tizimi tarmoqdagi shubhali faoliyatni aniqlasa, IPS tizimi tahdidni avtomatik ravishda bloklaydi. Sun'iy intellekt asosidagi IDS va IPS tizimlari real vaqt rejimida ishlash imkoniyati bilan ajralib turadi.

Tadqiqot davomida nazariy tahlil, qiyosiy tahlil va tizimli yondashuv usullaridan foydalanildi. Turli xil sun'iy intellekt algoritmlarining ishlash prinsiplari o'rganildi hamda ularning samaradorligi tahlil qilindi. Shuningdek, real vaqt monitoring tizimlarining afzalliklari va kamchiliklari qiyosiy baholandi.

MUHOKAMA

Sun'iy intellekt asosidagi xavfsizlik tizimlari zamonaviy tarmoq infratuzilmasining muhim tarkibiy qismiga aylanmoqda. Ushbu texnologiyalar katta hajmdagi ma'lumotlarni qisqa vaqt ichida qayta ishlash imkonini beradi. Bu esa kiber tahdidlarni real vaqt rejimida aniqlash samaradorligini oshiradi.

Mashinaviy o'qitish algoritmlarining asosiy afzalligi yangi va noma'lum tahdidlarni aniqlash imkoniyatidir. An'anaviy xavfsizlik tizimlari faqat oldindan ma'lum bo'lgan hujumlarni aniqlasa, sun'iy intellekt tizimlari anomal faoliyatni tahlil qilish orqali yangi turdagi tahdidlarni ham aniqlashi mumkin. Ayniqsa, neyron tarmoqlar murakkab hujumlarni aniqlashda yuqori natija ko'rsatadi.

Biroq sun'iy intellekt texnologiyalarining ayrim cheklovlari ham mavjud. Tizimlarni samarali ishlatish uchun katta hajmdagi sifatli ma'lumotlar talab etiladi. Bundan tashqari, ayrim hollarda noto'g'ri ijobiy natijalar kuzatilishi mumkin. Bu oddiy foydalanuvchi faoliyatining ham tahdid sifatida qabul qilinishiga olib keladi.

Real vaqt monitoring tizimlarining samaradorligi tarmoq infratuzilmasining to'g'ri tashkil etilishiga ham bog'liq. Agar xavfsizlik siyosati noto'g'ri sozlansa, tizim samaradorligi pasayadi. Shu sababli sun'iy intellekt asosidagi xavfsizlik tizimlarini joriy etishda malakali mutaxassislar ishtiroki muhim ahamiyatga ega.

Zamonaviy tadqiqotlar shuni ko'rsatadiki, sun'iy intellekt, avtomatlashtirilgan monitoring va bulutli texnologiyalar integratsiyasi

kiberxavfsizlik tizimlarini yanada samarali qiladi. Kelajakda sun’iy intellekt asosidagi xavfsizlik platformalari global tarmoq infratuzilmalarining asosiy himoya vositalaridan biriga aylanishi kutilmoqda.

NATIJALAR

Tadqiqot davomida sun’iy intellekt yordamida kiber tahdidlarni real vaqt rejimida aniqlash texnologiyalari tahlil qilindi va bir qator muhim natijalar olindi.

Birinchidan, sun’iy intellekt asosidagi tizimlar an’anaviy xavfsizlik vositalariga nisbatan yuqori tezkorlik va aniqlikni ta’minlashi aniqlandi. Tarmoq trafikini avtomatik tahlil qilish orqali tahdidlarni qisqa vaqt ichida aniqlash imkoniyati mavjud.

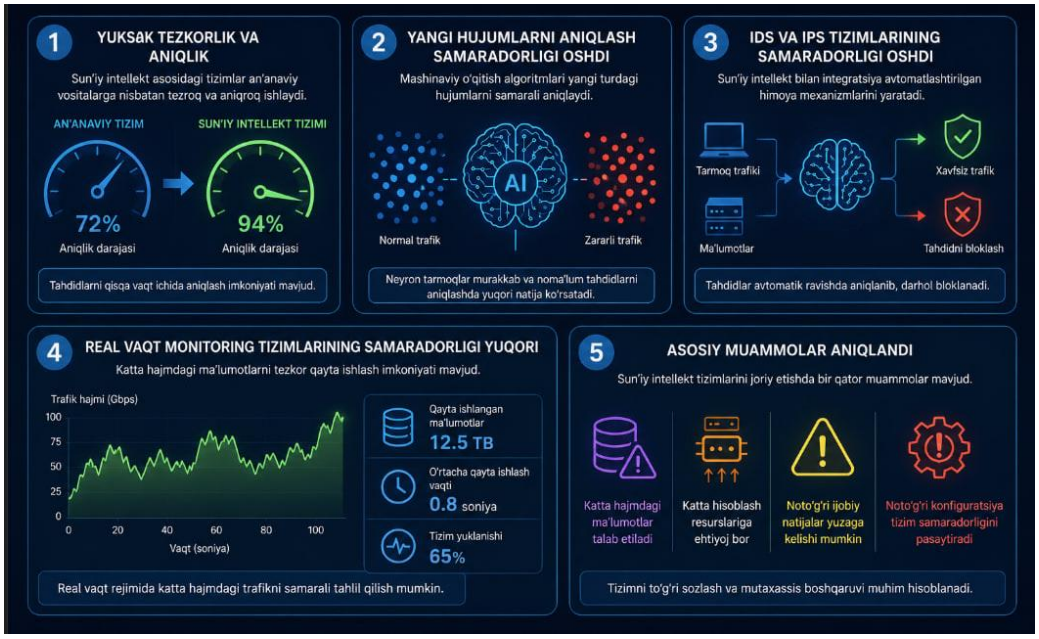
Ikkinchidan, mashinaviy o‘qitish algoritmlarining qo‘llanilishi yangi turdagi hujumlarni aniqlash samaradorligini oshirishi isbotlandi. Ayniqsa, neyron tarmoqlar va chuqur o‘rganish texnologiyalari murakkab tahdidlarni aniqlashda samarali hisoblanadi.

Uchinchidan, IDS va IPS tizimlarining sun’iy intellekt bilan integratsiyasi avtomatlashtirilgan himoya mexanizmlarini yaratish imkonini berishi aniqlandi. Bu esa tarmoq xavfsizligini sezilarli darajada oshiradi.

To‘rtinchidan, real vaqt monitoring tizimlari katta hajmdagi ma’lumotlarni qayta ishlash imkoniyati bilan ajralib turishi qayd etildi. Biroq bunday tizimlar katta hisoblash resurslarini talab qilishi ham aniqlandi.

Beshinchidan, sun’iy intellekt asosidagi xavfsizlik tizimlarini joriy etishda noto‘g‘ri konfiguratsiya va noto‘g‘ri ijobiy natijalar asosiy muammolardan biri ekanligi belgilandi.

Umuman olganda, tadqiqot natijalari sun’iy intellekt texnologiyalarining zamonaviy kiberxavfsizlik tizimlarida muhim o‘rin tutishini tasdiqladi.



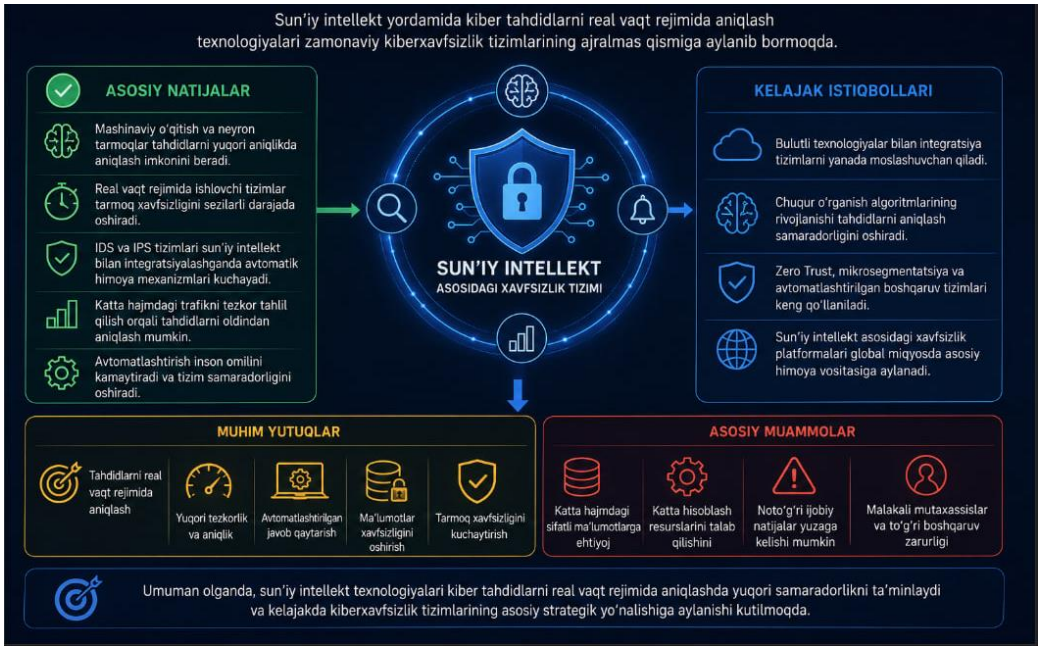
XULOSA

Ushbu tadqiqotda sun’iy intellekt yordamida tarmoqdagi kiber tahdidlarni real vaqt rejimida aniqlash texnologiyalari kompleks ravishda o‘rganildi. Olib borilgan tahlillar natijasida sun’iy intellekt zamonaviy kiberxavfsizlik tizimlarining ajralmas qismiga aylanib borayotgani aniqlandi.

Tadqiqot natijalari shuni ko‘rsatdiki, mashinaviy o‘qitish, neyron tarmoqlar va avtomatlashtirilgan monitoring tizimlari kiber tahdidlarni aniqlashda yuqori samaradorlikni ta’minlaydi. Ayniqsa, real vaqt rejimida ishlovchi xavfsizlik tizimlari tarmoq xavfsizligini oshirishda muhim rol o‘ynaydi.

Shu bilan birga, sun’iy intellekt tizimlarini joriy etishda katta hajmdagi ma’lumotlar, hisoblash resurslari va professional boshqaruv talab qilinishi aniqlandi. Noto‘g‘ri konfiguratsiya va xavfsizlik zaifliklari tizim samaradorligiga salbiy ta’sir ko‘rsatishi mumkin.

Kelajakda sun’iy intellekt asosidagi xavfsizlik tizimlari yanada rivojlanib, avtomatlashtirilgan va aqlli himoya platformalariga aylanishi kutilmoqda. Shu sababli sun’iy intellekt texnologiyalarini chuqur o‘rganish va amaliyotga samarali joriy etish muhim ilmiy va amaliy vazifalardan biri hisoblanadi.



FOYDALANILGAN ADABIYOTLAR

1. Stallings W. Network Security Essentials. Pearson Education, 2020.
2. Behrouz A. Forouzan. Data Communications and Networking. McGraw-Hill, 2019.
3. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. Pearson, 2021.
4. Goodfellow I., Bengio Y., Courville A. Deep Learning. MIT Press, 2018.
5. Bishop C. Pattern Recognition and Machine Learning. Springer, 2017.
6. William Stallings. Cryptography and Network Security. Pearson, 2020.
7. NIST Cybersecurity Framework. National Institute of Standards and Technology, 2021.
8. Jo‘rayev R.X. Axborot xavfsizligi asoslari. Toshkent, 2022.
9. Ahmedov B.A. Kiberxavfsizlik va tarmoq himoyasi. Toshkent, 2023.
10. Cisco Systems. Network Security and AI Technologies Documentation, 2022.