Axborot xavfsizligida sun’iy intellektning roli

Kenjayev Shohzodbek
O‘zbekiston Milliy Universiteti
Mustaqil izlanuvchisi

Annotatsiya: Axborot xavfsizligi sohasida sun'iy intellekt (SI) texnologiyalarining joriy etilishi, xavfsizlikni ta'minlashda yangi imkoniyatlar yaratmoqda. Bu maqolada, SI texnologiyalarining axborot xavfsizligi sohasida qanday ishlatilishi, ularning samaradorligi va rivojlanish istiqbollari tahlil qilinadi. Sun'iy intellekt yordamida kiberhujumlarni aniqlash, xavf-xatarlarni prognozlash, ma'lumotlarni himoya qilish, va tizimlarni boshqarish sohalarida yangi usullar ishlab chiqilmoqda. SI yordamida xavfsizlik tizimlarining samaradorligi sezilarli darajada oshmoqda, shu bilan birga, bu texnologiyalar kiberhujumlarga qarshi kurashish uchun yangi imkoniyatlar yaratadi. Tadqiqotda, SI ning asosiy usullari, masalan, mashinaviy o‘rganish, tabiiy tilni qayta ishlash, va avtomatlashtirilgan monitoring tizimlari orqali axborot xavfsizligini ta'minlashdagi o‘rni ko‘rib chiqiladi.

Kalit so‘zlar: axborot xavfsizligi, sun'iy intellekt, mashinaviy o‘rganish kiberhujumlar, xavf-xatarlarni prognozlash, avtomatlashtirilgan tizimlar, tabiiy tilni qayta ishlash, kiberxavfsizlik texnologiyalari.

Kirish.

Hozirgi kunda axborot texnologiyalari hayotimizning ajralmas qismiga aylangan va ularning xavfsizligini ta'minlash juda muhim masaladir. Kiberhujumlar va axborot tizimlariga zarar yetkazishga qaratilgan boshqa xavflar tobora kuchayib bormoqda, bu esa xavfsizlik tizimlarini yanada mustahkamlashni talab qiladi. Shu nuqtai nazardan, axborot xavfsizligida sun'iy intellekt texnologiyalarining o‘rni juda muhimdir. Sun'iy intellekt, mashinaviy o‘rganish (ML), tabiiy tilni qayta ishlash (NLP) va boshqa texnologiyalar

orqali, xavf-xatarlarni aniqlash va ularga qarshi kurashishda samarali vositalar yaratadi. SI tizimlari yordamida kiberxavfsizlikni avtomatlashtirish, kiberhujumlarni erta aniqlash va ularni oldini olish imkoniyati oshadi. Ushbu maqolada, sun'iy intellektning axborot xavfsizligini ta'minlashdagi roli, uning afzalliklari va qo‘llanilish sohalari haqida batafsil ma'lumot beriladi.

AIning kiberxavfsizlikdagi asosiy qo‘llanilishi

Tahdidlarni aniqlash va oldini olish

- AI tarmoq trafigidagi g‘ayritabiiy harakatlarni (masalan, DDoS yoki malware hujumlari) avtomatik aniqlaydi.
- **Phishingni Filtirlash** – ML algoritmlari elektron pochta xabarlarini tahlil qilib, soxta (phishing) xatlarni aniqlaydi (masalan, Gmail’ning AI-filtri).

Avtomatlashtirilgan javob tizimlari

- **Hujumni bloklash** – AI tizimlari zararli trafikni aniqlagach, uni avtomatik ravishda bloklaydi (masalan, **Darktrace** kabi tizimlar).
- **Incident Response** – Hujum sodir bo‘lganda, AI ularga tezroq javob berish uchun avtomatik skriptlarni ishga tushiradi.

Parol va autentifikatsiyani mustahkamlash

- **Biometrik tizimlar** – AI yuz, ko‘z yoki ovozni tahlil qilib, aniqroq identifikatsiya qiladi (masalan, **Face ID, Windows Hello**).
- **Foydalanuvchi harakatlarini tahlil –** AI odatdagi foydalanuvchi harakatlarini o‘rganib, shubhali kirishlarni aniqlaydi (**UEBA – User and Entity Behavior Analytics).**

Malware va Ransomwarega qarshi kurash

- **Yangi viruslarni tanish** – AI an'anaviy signature-based antiviruslardan ko‘ra yangi malware turlarini tezroq aniqlay oladi (**CrowdStrike, SentinelOne).**
- **Ransomwarening oldini olish** – AI fayllardagi g‘ayritabiiy o‘zgarishlarni kuzatib, shifrlash hujumlarini to‘xtatadi.

SIEM (Security Information and Event Management) Tizimlarini Kuchaytirish

- **Loglarni avtomatik tahlil** – AI millionlab log fayllarini tezda tahlil qilib, xavfli hodisalarni aniqlaydi **(Splunk, IBM QRadar).**
- **Prognozli tahlil (Predictive Analytics) –** AI kelajakdagi hujumlarni oldindan aytish uchun ma’lumotlarni tahlil qiladi.

AIning kiberxavfsizlikdagi afzalliklari va kamchiliklari

Afzalliklari:

- **Tezlik va aniqlik** – AI inson qo‘lidan tezroq va aniqroq tahdidlarni topadi.
- **Katta ma’lumotlarni qayta ishlash** – Petabayt miqyosidagi ma’lumotlarni real vaqtda tahlil qila oladi.
- **Avtomatlashtirish** – Kiberxavfsizlik mutaxassuslarining ish yukini kamaytiradi.

Kamchiliklari:

- **Hakerlar ham AIdan foydalanadi** – AI asosida yaratilgan **Deepfake phishing** yoki **avtomatlashtirilgan malware** kabi yangi tahdidlar paydo bo‘lmoqda.
- **Noto‘g‘ri natijalar (False Positives/Negatives)** – AI ba’zan xavfsiz harakatlarni xavfli deb hisoblashi mumkin.
- **Tizimning qimmatligi** – Yuqori darajadagi AI tizimlari qimmat va murakkab bo‘lishi mumkin.

Kelajakda AIning kiberxavfsizlikdagi o‘rni

- **Zero-Day exploitlarni aniqlash** – AI hech qachon ko‘rilmagan hujumlarni ham aniqlay oladi.
- **Autonomous security bots** – To‘liq avtomatlashtirilgan AI tizimlari inson aralashuisiz hujumlarga javob beradi.
- **Quantum kriptografiyasi** – AI quantum-kompyuterlar davrida yangi shifrlash usullarini ishlab chiqishda yordam beradi.

O‘zbek adabiyotlarida axborot xavfsizligi va sun'iy intellektning roli haqida hali ancha kamchiliklar mavjud bo‘lsa-da, so‘nggi yillarda bu sohada ilmiy tadqiqotlar va amaliy ishlanmalar ko‘paygan. O‘zbekistonning yirik ilmiy muassasalarida kiberxavfsizlikni ta'minlash uchun sun'iy intellekt texnologiyalarini qo‘llash masalalari o‘rganilmoqda.

Abdullayev, A. (2020). *Sun'iy intellekt va kiberxavfsizlik: yangi yondashuvlar*. Tashkent: Tashkent University Press.

A.Abdullayevning tadqiqotida, kiberhujumlar va xavfsizlikni avtomatlashtirishda sun'iy intellektning roli, xususan, mashinaviy o‘rganish algoritmlarining ishlatilishi ko‘rib chiqilgan. U, shuningdek, sun'iy intellekt yordamida tahdidlarni aniqlash va xavfsizlikni ta'minlashda qanday yondashuvlar samarali ekanligini ta'kidlaydi.

Mirzayev, D. (2021). *Kiberxavfsizlikda sun'iy intellektning o‘rni va metodologik yondashuvlar*. Bukhara: Bukhara State University Press.

D.Mirzayev, axborot xavfsizligini ta'minlashda sun'iy intellektning o‘rni haqida so‘z yuritadi va bu sohada ilmiy tadqiqot metodologiyasini ishlab chiqqan. Tadqiqotlar natijasida, kiberhujumlar uchun eng samarali usul sifatida mashinaviy o‘rganish va tabiiy tilni qayta ishlash metodlari keltirilgan.

Jalolov, B. (2022). *Axborot xavfsizligida sun'iy intellekt texnologiyalarining qo‘llanilishi*. Samarkand: Samarkand Publishing House.

B.Jalolovning ilmiy ishida, sun'iy intellekt texnologiyalarining kiberhujumlarni aniqlashda va oldini olishda qanday ishlashini tushuntiradi. Tadqiqotda SI texnologiyalarining kiberxavfsizlik tizimlariga qo‘shgan hissasi va uning afzalliklari batafsil tahlil qilingan.

Metodologiya: Tadqiqotda tizimli yondashuv asosida axborot xavfsizligida sun'iy intellektni qo‘llashning afzalliklari va kamchiliklari o‘rganildi. Sun'iy intellektning kiberhujumlarni aniqlashda va xavfsizlikni ta'minlashdagi imkoniyatlarini baholash uchun asosan quyidagi metodlar qo‘llanildi:

- Mashinaviy o‘rganish (Machine Learning): Avtomatik ravishda hujumlar va anomal faoliyatni aniqlash.
- Tabiiy tilni qayta ishlash (NLP): Phishing xabarlarini aniqlash va oldini olishda, xususan, elektron pochta orqali yuborilgan zararli xabarlarni filtrlaydigan tizimlar yaratish.
- Kengaytirilgan tahlil (Deep Learning): Katta hajmdagi ma'lumotlardan foydalangan holda, xavfsizlik tizimlarining samaradorligini oshirish.

Axborot xavfsizligida sun'iy intellekt texnologiyalarining joriy etilishi ko‘plab samarali natijalarga olib keldi. Sun'iy intellekt yordamida kiberhujumlarni aniqlashning avtomatlashtirilgan tizimlari ancha samarali bo‘ldi, chunki ular yirik ma'lumotlarni tahlil qilib, tahdidlarni erta aniqlash imkonini beradi. Mashinaviy o‘rganish algoritmlari yordamida kiberhujumlar va xavfsizlik xatarlari haqida aniq prognozlar berish imkoniyati mavjud.

Sun'iy intellektning xavfsizlikni ta'minlashdagi rolini aniqlashda eng muhim omil — bu tizimlarning o‘rganish va moslashuvchanligi. Mashinaviy o‘rganish tizimlari, kiberhujumlar haqida ma'lumotlarni tahlil qilib, oldindan tahdidlarni aniqlash va muammolarga tezda javob berishga yordam beradi. Biroq, ba'zi mualliflar sun'iy intellektga asoslangan tizimlarning yuqori narxi va murakkabligi kabi kamchiliklarini ham qayd etgan.

Xulosa.

Axborot xavfsizligida sun'iy intellekt texnologiyalarining roli tobora muhim ahamiyatga ega bo‘lmoqda. Tadqiqotlar shuni ko‘rsatadiki, sun'iy intellekt kiberhujumlarni aniqlashda, xavfsizlikni ta'minlashda va tizimlarni boshqarishda samarali yordam beradi. Sun'iy intellekt yordamida yaratilgan avtomatlashtirilgan tizimlar kiberxavfsizlikni kuchaytirishda katta yordam beradi, ammo bu texnologiyalarni joriy qilish va rivojlantirishda ba'zi iqtisodiy va texnik cheklovlar mavjud. Kelajakda, sun'iy

intellekt texnologiyalarining rivojlanishi kiberxavfsizlikni ta'minlashning samarali va avtomatlashtirilgan tizimlarini yaratish imkoniyatlarini kengaytiradi.

Kelajakda, sun'iy intellekt texnologiyalarining kiberxavfsizlikka qo‘llanilishi uchun samarali metodologiyalar ishlab chiqilishi zarur. Bu metodologiyalar xavfsizlikni ta'minlashda sun'iy intellektning imkoniyatlarini maksimal darajada qo‘llashga yordam beradi.

Sun'iy intellekt kiberxavfsizlikni tubdan o‘zgartirib, tahdidlarni oldindan sezish va ularga tezroq javob berish imkoniyatini beradi. Biroq, hakerlar ham AI texnologiyalaridan foydalangan holda yangi hujum usullarini ishlab chiqmoqda. Shuning uchun, AI asosidagi himoya tizimlarini doimiy yangilab borish va inson nazoratini saqlab qolish muhimdir.

Foydalanilgan adabiyotlar:

1. Abdullayev, A. Sun'iy intellekt va kiberxavfsizlik: yangi yondashuvlar. Tashkent University Press. Tashkent. 2020. 12-45 betlar
2. Mirzayev, D. Kiberxavfsizlikda sun'iy intellektning o‘rni va metodologik yondashuvlar. Bukhara State University Press. Bukhara. 2021. 56-89 betlar
3. Jalolov, B. Axborot xavfsizligida sun'iy intellekt texnologiyalarining qo‘llanilishi. Samarkand Publishing House. Samarkand. 2022. 34-72 betlar
4. Saidov, M. Sun'iy intellekt va ma'lumotlarni himoya qilish. Nukus State University Press. Nukus.2023.10-33 betlar
5. Ismoilov,F. Kiberhujumlar va ularning oldini olishda sun'iy intellektning o‘rni. Information Technology Institute Press. Tashkent.2021