“KIBRXAVSIZLIK VA SI: XAKKERLARGA QARSHI AQLLI HIMOYA TIZIMLARI”

***Muallif**:Qarshi davlat universiteti professori :*

Sharopova Muhabbat Arapovna

Saydullayeva Gulsevar Alisher qizi

Tuychiyeva Setorabonu Nodir qizi

Annotatsiya: *Ushbu maqolada kiberxavfsizlikni ta’minlashda sun’iy intellekt (SI) texnologiyalarining o‘rni va ahamiyati yoritilgan. Zamonaviy xakerlik hujumlarining murakkablashishi fonida an’anaviy himoya tizimlarining kamchiliklari va SI yordamida yaratilgan "aqlli" himoya mexanizmlarining afzalliklari tahlil qilingan. Shuningdek, mashinali o‘rganish (Machine Learning) va neyron tarmoqlarining kiberhujumlarni oldindan aniqlashdagi samaradorligi ko‘rib chiqilgan.*

Kalit so‘zlar: *Kiberxavfsizlik, Sun’iy intellekt, Mashinali o‘rganish, Xakerlik hujumlari, Kiber-tahdidlar, Neyron tarmoqlari, Ma’lumotlar himoyasi.*

Kirish

Bugungi raqamli transformatsiya davrida axborot xavfsizligi har qanday davlat va xususiy tashkilotning ustuvor vazifasiga aylandi. Kiberjinoyatchilar har kuni o‘rtacha 2,200 dan ortiq hujumlarni amalga oshirmoqdalar. An'anaviy antivirus va devor (firewall) tizimlari faqat ma'lum bo‘lgan tahdidlarga (signature-based) javob bera oladi, ammo "nol kunlik" (Zero-day) hujumlari va murakkab adaptiv viruslar oldida ojiz qolmoqda. Kiberxavfsizlik sohasiga sun'iy intellektning integratsiya qilinishi nafaqat ehtiyoj, balki zaruriyatga aylandi. SI tizimlari katta hajmdagi ma'lumotlarni real vaqt rejimida tahlil qilib, inson ko‘zi ilg‘amaydigan anomal holatlarni aniqlash imkonini beradi. Zamonaviy axborot jamiyatida kiberxavfsizlik endi shunchaki texnik tushuncha emas, balki milliy xavfsizlik va iqtisodiy barqarorlikning asosiy ustuniga aylandi. So‘nggi yillarda

kiberhujumlarning tabiati tubdan o‘zgardi: oddiy viruslardan tortib, davlat miqyosidagi **APT (Advanced Persistent Threats)** — murakkab va davomiy tahdidlargacha bo‘lgan spektr kengaydi.An’anaviy xavfsizlik tizimlari "qora ro‘yxat" (blacklist) va signaturalarga tayanadi. Ammo, har kuni dunyoda **350,000 dan ortiq** yangi zararli dasturlar yaratilayotgan bir paytda, inson omili va statik qoidalar yetarli emas. Bu yerda Sun'iy Intellekt (SI) "raqamli immun tizimi" rolini o‘ynaydi. SI nafaqat ma'lum bo‘lgan viruslarni to‘xtatadi, balki tizimdagi noodatiy tebranishlarni tahlil qilib, hali fanga ma'lum bo‘lmagan hujumlarni ham "sezish" qobiliyatiga ega. Maqolaning ushbu qismida biz SIning kiber-mudofaadagi strategik o‘rnini fundamental tahlil qilamiz. Zamonaviy kiberfazoda xavfsizlik tushunchasi statik himoya devorlaridan dinamik va o‘zi o‘rganuvchi tizimlarga o‘tish bosqichini boshidan kechirmoqda. Sun’iy intellektning kiberxavfsizlikka integratsiyasi insoniyatni ma’lumotlar oqimini shunchaki kuzatishdan, ularni chuqur tahlil qilish va intellektual darajada bashorat qilish bosqichiga olib chiqdi. Mazkur jarayonning fundamental asosi mashinali o‘rganish algoritmlariga tayanadi. Xususan, neyron tarmoqlari inson miyasining neyronlari kabi axborotni qatlamlararo qayta ishlab, tarmoqdagi har bir paketning xavfsizlik darajasini aniqlaydi. Bu jarayonda nazorat ostidagi va nazoratsiz o‘rganish usullari birgalikda qo‘llanilib, tizimga nafaqat ma’lum bo‘lgan tahdidlarni, balki hali fanga noma’lum bo‘lgan, murakkab algoritmik o‘zgarishlarga ega zararli kodlarni ham aniqlash imkonini beradi.Aqlli himoya tizimlarining eng muhim xususiyatlaridan biri bu anomaliyalarni aniqlash qobiliyatidir. An’anaviy tizimlar qat’iy qoidalar asosida ishlasa, sun’iy intellektga asoslangan platformalar tizimning "sog‘lom" holatini o‘rganadi va har qanday og‘ishni xavf sifatida baholaydi. Masalan, ma’lumotlar bazasiga kirish huquqiga ega bo‘lgan foydalanuvchining noodatiy vaqtlarda yoki kutilmagan geografik nuqtalardan ulanishi aqlli tizimlar tomonidan darhol shubhali harakat sifatida qayd etiladi. Bu yerda xatti-harakatlar tahlili (Behavioral Analytics) markaziy o‘rinni egallaydi. Tizim foydalanuvchining klaviaturada yozish tezligi, ko‘p ishlatadigan buyruqlari va tarmoqdagi harakatlanish trayektoriyasini doimiy ravishda kuzatib boradi. Agar ushbu ko‘rsatkichlarda keskin o‘zgarish kuzatilsa, sun’iy intellekt buni

akkauntning xakerlar tomonidan egallab olingani sifatida talqin qiladi va avtomatik tarzda kirishni cheklaydi.Kiberhujumlarning murakkablashishi fonida sun’iy intellektning bashoratli tahlil imkoniyatlari alohida ahamiyat kasb etadi. Bashoratli modellashtirish o‘tmishdagi yuz minglab kiberhujumlar tarixini tahlil qilib, kelajakda xakerlar qaysi zaif nuqtalardan foydalanishi mumkinligini aniqlaydi. Bu jarayonda katta ma’lumotlar (Big Data) tahlili hal qiluvchi rol o‘ynaydi. Tizim soniyasiga millionlab log-fayllarni skanerlab, ular orasidagi mantiqiy bog‘liqlikni qidiradi. Xakerlar ko‘pincha tizimga kirishdan oldin "razvedka" ishlarini olib borishadi, bu esa tarmoqda juda kichik, deyarli sezilmas izlar qoldiradi. Inson tahlilchisi bu kichik detallarni umumiy shovqin ichidan ajratib ololmasligi mumkin, biroq sun’iy intellekt ushbu signallarni birlashtirib, bo‘lajak yirik hujumning proektsiyasini yaratadi.

Shuningdek, sun’iy intellekt zararli dasturlarni klassifikatsiya qilishda inqilobiy o‘zgarish yasadi. Bugungi kunda polimorfik viruslar, ya’ni o‘z kodini har bir yangi qurilmaga o‘tganda o‘zgartiradigan dasturlar an’anaviy antiviruslarni osongina aldab o‘tadi. Sun’iy intellekt esa kodning tashqi ko‘rinishiga emas, balki uning funksional semantikasiga, ya’ni nima ish bajarishiga e’tibor qaratadi. Agar dastur tizim xotirasida o‘zini yashirishga yoki muhim fayllarni shifrlashga urinsa, uning kodi qanchalik o‘zgartirilgan bo‘lmasin, aqlli tizim uni zararli deb topadi. Bu jarayon "sandbox" deb ataladigan izolyatsiya qilingan muhitda amalga oshirilib, tizimning asosiy qismiga zarar yetishi oldi olinadi.

Biroq, aqlli himoya tizimlarini yaratishda "adversarial machine learning" deb ataladigan yangi tahdid turi bilan ham hisoblashish lozim. Xakerlar ham o‘z navbatida sun’iy intellekt modellarini aldash uchun maxsus algoritmlar ishlab chiqmoqdalar. Ular mudofaa tizimining o‘rganish algoritmlariga "zaharli ma’lumotlar" (data poisoning) kiritish orqali tizimning hushyorligini pasaytirishga urinishadi. Bu kiber-olamda qurollanish poygasining yangi bosqichini boshlab berdi. Himoya tizimlari endi nafaqat tashqi hujumlardan himoyalanishi, balki o‘zining ichki qaror qabul qilish mexanizmlarini manipulyatsiyadan saqlashi ham talab etiladi. Shu sababli, "mustahkam sun’iy intellekt" (Robust AI) tushunchasi ilmiy

doiralarda keng muhokama qilinmoqda, bu esa modelning har qanday noto‘g‘ri kiritilgan ma’lumotlarga qaramay, to‘g‘ri xulosaga kela olish qobiliyatini anglatadi.

Aqlli tizimlarning yana bir strategik afzalligi bu hodisalarga avtomatik javob qaytarish tezligidir. Kiberhujum sodir bo‘lganda, har bir soniya hal qiluvchi ahamiyatga ega. Inson omili ishtirok etgan tizimlarda xavfni aniqlash va unga chora ko‘rish soatlar yoki kunlarni talab qilishi mumkin. Sun’iy intellektga asoslangan SOAR (Security Orchestration, Automation and Response) platformalari esa hujumni millisoniyalar ichida bloklaydi, zararlangan tarmoq segmentini boshqalaridan ajratadi va tizimni avtomatik ravishda xavfsiz holatga qaytaradi. Bu esa kiber-insidentlar natijasida ko‘riladigan iqtisodiy zararni keskin kamaytiradi.

Xulosa

Xulosa qilib aytganda, sun'iy intellekt kiberxavfsizlikning ajralmas qismiga aylandi. U xakerlarga qarshi dinamik va adaptiv himoya tizimini yaratishga imkon beradi. Biroq, SI faqat texnik vositadir; uning samaradorligi inson mutaxassislar tomonidan qanday boshqarilishi va o‘qitilishiga bog‘liq. Kelajakda kiber-himoya tizimlari to‘liq avtonom shaklga o‘tishi kutilmoqda, bu esa kiberjinoyatchilik xavfini minimal darajaga tushirish imkonini beradi.

FOYDALANILGAN ADABIYOTLAR

1. Bhardwaj, A., & Gupta, S. C. (2023). *Artificial Intelligence in Cybersecurity: Challenges and Innovations.* Springer.

2. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning.* MIT Press.

3. O‘zbekiston Respublikasi Prezidentining 2022-yil 15-iyundagi "Kiberxavfsizlik sohasida kadrlarni tayyorlash tizimini takomillashtirish chora-tadbirlari to‘g‘risida"gi PQ-284-son qarori.

4. National Institute of Standards and Technology (NIST). (2024). *Cybersecurity Framework 2.0.*