KIBERXAVFSIZLIK VA SUN'IY INTELLEKT: ZAMONAVIY TAHDIDLAR VA INTELLEKTUAL HIMOYA TIZIMLARI

Xoliqnazarov Rashidjon
Qo’chqorov Muhammadyahyo
Ergashov Shohbozbek
Farg’ona davlat texnika universiteti
https://doi.org/10.5281/zenodo.20393811

ANNOTATSIYA

Ushbu ilmiy maqolada kiberxavfsizlik sohasida sun'iy intellekt (SI) texnologiyalarining o'rni va ahamiyati keng ko'lamda tahlil qilingan. Maqolada kibertahdidlarning zamonaviy ko'rinishlari, mashinaviy o'qitish (Machine Learning), chuqur o'qitish (Deep Learning) va neyron tarmoqlar (Neural Networks) asosida qurilgan himoya tizimlari, shuningdek, SI yordamida kiberhujumlarni aniqlash va oldini olish usullari batafsil yoritilgan. Tadqiqot davomida real hayotdagi misollar va statistik ma'lumotlarga tayanilgan holda, O'zbekiston va jahon miqyosida kiberxavfsizlik sohasidagi hozirgi holat hamda kelajakdagi rivojlanish yo'nalishlari muhokama qilingan. Maqola natijasida sun'iy intellektning kiberxavfsizlikka qo'shadigan salmoqli hissasi aniqlangan va ushbu texnologiyalarni joriy etishning strategik zarurligi asoslangan.

Kalit so'zlar: *kiberxavfsizlik, sun'iy intellekt, mashinaviy o'qitish, chuqur o'qitish, neyron tarmoqlar, kiberhujumlar, anomaliyani aniqlash, tahdid razvedkasi, zararli dasturlar, ma'lumotlar himoyasi.*

1. KIRISH

Bugungi kunda raqamli texnologiyalar jadal sur'atlar bilan rivojlanib, jamiyatning barcha sohalari — tibbiyot, moliya, ta'lim, davlat boshqaruvi va savdo-sotiqni qamrab olmoqda. Internet foydalanuvchilarining soni har yili o'sib borayotgani, bulutli hisoblash (cloud computing) va narsalar interneti (IoT) kabi yangi texnologiyalarning keng joriy etilishi axborot maydonini kengaytirmoqda. Biroq bu jarayon bir vaqtning o'zida yangi xavf va tahdidlarni ham yuzaga keltirmoqda.

Kiberxavfsizlik — axborot tizimlari, tarmoqlar va ma'lumotlarni ruxsatsiz kirish, buzilish, o'g'irlash yoki yo'q qilishdan himoya qilish sohasidir. Cybersecurity Ventures tadqiqot kompaniyasining ma'lumotlariga ko'ra, 2025-yilga kelib kiberjinoatchilik dunyo iqtisodiyotiga yiliga 10,5 trillion AQSh dollari miqdorida zarar yetkazishi kutilmoqda. Bu ko'rsatkich 2015-yildagi 3 trillion dollarlik zarardan uch baravar ko'p demakdir. Bunday sharoitda an'anaviy himoya usullari yetarli bo'lmay qolmoqda va yangi yechimlar izlash zarurati paydo bo'lmoqda.

Aynan shu nuqtada sun'iy intellekt texnologiyalari kiberxavfsizlik sohasiga inqilobiy o'zgarishlar olib kirmoqda. Sun'iy intellekt asosidagi tizimlar sekundiga millionlab ma'lumotlarni qayta ishlab, g'ayritabiiy faoliyatni darhol aniqlay oladi va xavfsizlik mutaxassislarining ko'zidan chetda qolgan tahdidlarni ham topishi mumkin. Shunday bo'lsa-da, bir tanganing ikki tomoni bo'lgani kabi, xuddi shu SI texnologiyalaridan kiberjinoyatchilar ham o'z maqsadlari uchun foydalanayotgani haqiqat.

Ushbu maqolaning asosiy maqsadi kiberxavfsizlik va sun'iy intellektning kesishish nuqtalarini chuqur tahlil qilish, SI texnologiyalarining himoya sohasiga qo'shadigan hissasini baholash hamda ularga xos xavf-xatarlarni ko'rsatishdan iborat. Tadqiqotda tavsifiy va taqqosiy tahlil metodlaridan foydalanilgan bo'lib, xalqaro ilmiy nashrlar, sanoat hisobotlari va hujjatlashtirilgan real voqealar asos sifatida qo'llanilgan.

2. ASOSIY QISM: KIBERXAVFSIZLIKNING ZAMONAVIY MANZARASI

Axborot xavfsizligi sohasida so'nggi o'n yil ichida kuzatilgan eng katta o'zgarish — hujumlarning murakkablashuvi va avtomatlashuvidir. Agar ilgari kiberhujumlar asosan tarmoqdagi zaif nuqtalarni qo'lda topib, ulardan individual foydalanishga asoslangan bo'lsa, hozirda zamonaviy tahdidlar bir butun ekotizimga aylangan.

IBM Security X-Force 2024 Tahdid Razvedkasi Indeksiga ko'ra, kiberhujumlarning 71 foizi moliyaviy manfaat maqsadida amalga oshirilmoqda. Hujumlarning 67 foizida zararli dasturlar (malware) ishlatilgan bo'lsa, 26 foizida fishing (phishing) usulidan foydalanilgan. Fishing hujumlari ayni paytda kiberjinoyatchilikning eng keng tarqalgan usuli sifatida saqlanib qolmoqda, chunki inson omili — charchoq, e'tiborsizlik va ishonuvchanlik — texnik himoya usullarini chetlab o'tish imkonini beradi.

Zamonaviy kiberxavfsizlik sohasi quyidagi asosiy tahdid turlari bilan kurashadi: to'lov dasturlari (ransomware) — tizimni blokirovka qilib to'lov talab qiluvchi zararli dasturlar; APT (Advanced Persistent Threat) — maqsadli va uzoq muddatli hujumlar; DDoS (Distributed Denial of Service) — tarmoqni yuklamalar bilan to'xtatib qo'yish; nol kunlik ekspluatatsiyalar (zero-day exploits) — hali noma'lum zaifliklardan foydalanish; va ichki tahdidlar (insider threats) — tashkilot ichidagi shaxslar tomonidan sodir etiladigan zararlar.

Verizon 2024 Data Breach Investigations Report ma'lumotlariga ko'ra, barcha ma'lumotlar buzilishlarining 74 foizida inson omili ishtirok etgan. Bu ko'rsatkich texnik himoya qanchalik kuchli bo'lmasin, foydalanuvchilarni o'qitish va xabardorlikni oshirish ham xuddi shunday muhim ekanligini ko'rsatadi. Biroq texnik jihatdan qaraganda, tarmoqlardagi anomaliyalarni qo'lda aniqlash endi imkonsizga aylangan — bitta yirik kompaniya tarmoqida kuniga milliardlab ma'lumot paketlari harakatlanadi.

3. SUN'IY INTELLEKTNING KIBERXAVFSIZLIKDAGI QO'LLANILISHI

Sun'iy intellekt — mashinalarning insoniy fikrlash jarayonlarini taqlid qilishi, ya'ni o'rganish, muammolarni hal qilish va qaror qabul qilish qobiliyatini qamrab oluvchi keng tushunchadir. Kiberxavfsizlik kontekstida SI quyidagi asosiy yo'nalishlarda qo'llanilmoqda:

3.1. Tahdidlarni Avtomatik Aniqlash va Oldini Olish

An'anaviy antivirus dasturlari imzolarga (signatures) asoslangan bo'lib, faqat allaqachon ma'lum bo'lgan zararli dasturlarni aniqlay oladi. SI asosidagi tizimlar esa xatti-harakatlarni tahlil qilish (behavioral analysis) orqali yangi, hali ko'rilmagan tahdidlarni ham topishi mumkin. Masalan, Darktrace kompaniyasi tomonidan ishlab chiqilgan Immune System platformasi tarmoqdagi barcha qurilmalar va foydalanuvchilar uchun me'yoriy xatti-harakat namunasini o'rganadi. Ushbu me'yordan og'ish kuzatilganda tizim avtomatik ravishda ogohlantirib, zaruriy hollarda faoliyatni to'xtatib qo'yadi.

3.2. Foydalanuvchi Identifikatsiyasi va Kirishni Boshqarish

Zamonaviy SI tizimlari foydalanuvchining xatti-harakatini o'rganadi: u odatda qachon, qayerdan, qaysi qurilmadan tizimga kirishi, qanday fayllarga murojaat qilishi va tezligining qanday bo'lishini hisobga oladi. UEBA (User and Entity Behavior Analytics) deb ataluvchi bu yondashuv odatdan tashqari holatlarni, masalan, ish vaqtidan tashqari ma'lumot yuklab olishni yoki g'ayriodatiy geografik joydan kirishni darhol aniqlab beradi. Microsoft tomonidan qo'llaniladigan Azure Active Directory Identity Protection ana shunday SI imkoniyatlarini amalga oshiruvchi tizimga misol bo'la oladi.

3.3. Zararli Dasturlarni Tahlil Qilish

SI asosidagi xavfsizlik tizimlari zararli dasturlarni aniqlashda oldindan belgilangan qoidalar o'rniga neyron tarmoqlarga tayanadi. CrowdStrike Falcon kabi platformalar yangi zararli dastur namunalarini millisekundlar ichida tahlil qilib, ularni mavjud zararli dastur oilalari bilan taqqoslaydi va xavf darajasini baholaydi. 2023-yil Mandiant hisobotiga ko'ra, neyron tarmoqlarga asoslangan tizimlar zararli dasturlarni aniqlashda an'anaviy usullarga qaraganda 40-60 foiz yuqori aniqlik ko'rsatishi kuzatilgan.

4. AI YORDAMIDA KIBERHUJUMLARNI ANIQLASH USULLARI

Kiberhujumlarni aniqlashda sun'iy intellektning qo'llanilishi bir necha texnik yondashuv orqali amalga oshiriladi. Ularning har biri turli turdagi tahdidlarni topishda o'ziga xos kuchli tomonlarga ega.

4.1. Anomaliyani Aniqlash (Anomaly Detection)

Bu usulda mashinaviy o'qitish modeli tizimning odatdagi ishlash ko'rsatkichlarini o'rganadi va statistik jihatdan me'yordan sezilarli darajada farq qiluvchi holatlarni belgilaydi. Masalan, tarmoq trafigining kunlik o'rtacha ko'rsatkichi har kuni kuzatiladi. Agar bir tunda ma'lumot uzatish hajmi to'satdan bir necha baravar oshsa, bu ma'lumot o'g'irlash (data exfiltration) jarayonining belgisi bo'lishi mumkin. Isolation Forest, DBSCAN va Autoencoder neyron tarmoqlari anomaliyalarni aniqlashda keng qo'llaniladigan algoritmlar hisoblanadi.

4.2. Tasniflovchi Modellar (Classification Models)

Tarmoq paketlari, jurnal fayllari (log files) yoki fayl metama'lumotlarini tahlil qilib, ularni 'normal' yoki 'xavfli' sifatida tasniflash uchun nazorat ostidagi o'qitish (supervised learning) algoritmlari ishlatiladi. Random Forest, Support Vector Machine (SVM) va Gradient Boosting kabi algoritmlar katta hajmdagi ma'lumotlarni qayta ishlab, kiberhujumlarni real vaqt rejimida identifikatsiya qilish uchun keng qo'llanilmoqda. CICIDS-2017 va NSL-KDD kabi standart kiberxavfsizlik ma'lumotlar to'plamlarida ushbu modellar 97-99 foizga yaqin aniqlikka erishganligi kuzatilgan.

4.3. Natural Language Processing (NLP) Asosidagi Fishing Aniqlanishi

NLP — sun'iy intellektning insoniy tilni tushunish va tahlil qilish sohasidir. Kiberxavfsizlikda NLP modellar fishing elektron xatlarini aniqlashda qo'llaniladi. Model xat matnini tahlil qilib, shoshilinch til, soxta havolalar, grammatik xatolar va noodatiy jo'natuvchi manzillar kabi belgilarni aniqlaydi. Google tomonidan Gmail xizmatida qo'llaniladigan fishing aniqlash tizimi NLP asosida ishlaydi va kuniga 100 million dan ortiq fishing urinishini bloklashini e'lon qilgan.

4.4. To'lov Dasturlarini Aniqlash

Ransomware hujumlarida zararli dastur qisqa vaqt ichida ko'plab fayllarni shifrlashga harakat qiladi. SI tizimlari fayl tizimidagi bunday g'ayriodatiy faoliyatni — ko'p sonli fayllarni tez-tez o'qish va qayta yozish jarayonini — millisoniyalar ichida aniqlash imkoniga ega. Microsoft Defender for Endpoint ushbu usulni qo'llab, 2022-yilda WannaCry va Petya kabi to'lov dasturlarining yangi avlodlarini fayl tizimiga ziyon yetkazilmasidan oldin to'xtatishga muvaffaq bo'lganligi hujjatda ko'rsatilgan.

5. SUN'IY INTELLEKTNING KIBERXAVFSIZLIKDAGI AFZALLIKLARI

Sun'iy intellektni kiberxavfsizlik sohasida qo'llashning bir qator muhim afzalliklari mavjud bo'lib, ular an'anaviy usullarga nisbatan sezilarli ustunliklarni ta'minlaydi.

Birinchidan, tezlik va miqyos. Insonlar sekundiga bir nechta hodisani ko'rib chiqa olsa, SI tizimlari sekundiga millionlab tarmoq paketlarini va jurnal yozuvlarini tahlil qila oladi. Katta tashkilotlarda kuniga 500 gigabaytdan ortiq jurnal ma'lumoti yig'iladi — buni qo'lda tekshirib chiqish mutlaqo imkonsiz.

Ikkinchidan, uzluksiz ishlash qobiliyati. SI tizimlari charchamas, uyquga ketmas va hissiyotga berilmas. Ular tungi soatlarda, dam olish kunlarida va bayram kunlarida ham bir xil samaradorlik bilan ishlaydi. Statistik ma'lumotlarga ko'ra, kiberhujumlarning 60 foizdan ortig'i ish vaqtidan tashqarida — odamlar tizimni kuzatmayotgan vaqtda sodir bo'ladi.

Uchinchidan, noma'lum tahdidlarni aniqlash. Imzolarga asoslangan an'anaviy tizimlar faqat avval ro'yxatga olingan tahdidlarni topishi mumkin. Nol kunlik hujumlarga (zero-day attacks) qarshi esa bu tizimlar ojiz. SI modellari xatti-harakat namunalarini o'rganish orqali imzosi yo'q yangi tahdidlarni ham aniqlash imkoniga ega.

To'rtinchidan, avtomatlashtirilgan javob chorasi. SOAR (Security Orchestration, Automation and Response) platformalari SI bilan birgalikda ishlab, tahdid aniqlanganidan so'ng avtomatik ravishda izolyatsiya, bloklash va xabarnoma yuborish kabi choralarni amalga oshiradi. Bu inson xatosini kamaytiradi va tahdidga javob vaqtini soatlardan daqiqalarga tushiradi.

6. AI BILAN BOG'LIQ XAV VA MUAMMOLAR

Afzalliklari bilan birga, sun'iy intellektni kiberxavfsizlikda qo'llash bir qator muhim xavf va muammolarni ham o'z ichiga oladi. Ushbu muammolarni to'g'ri tushunish va ularga tayyor bo'lish zarur.

6.1. SI Asosidagi Kiberhujumlar

Mudofaa uchun ishlatiladigan xuddi shu SI texnologiyalarini kiberjinoyatchilar ham o'z maqsadlari uchun qo'llashmoqda. Deepfake texnologiyasi yordamida soxta video va audio materiallar yaratib, ijtimoiy muhandislik hujumlarida ishlatilmoqda. 2019-yilda Buyuk Britaniyada bir energetika kompaniyasining rahbari CFO unvonli shaxsning AI tomonidan sintetik qilingan ovozini haqiqiy deb qabul qilib, 243 000 dollar fraudulent o'tkazmaga ruxsat bergan holat kiberxavfsizlik tarixiga kirgan.

6.2. Noto'g'ri Ijobiy Natijalar (False Positives)

SI tizimlari ba'zan oddiy faoliyatni xavfli deb belgilashi mumkin. Bu false positive deb ataladi. Natijada xavfsizlik guruhi haqiqiy tahdidlarga e'tibor qaratishi o'rniga, o'nlab yolg'on signallarni ko'rib chiqishga vaqt va resurs sarflashga majbur bo'ladi. 2023-yil ISACA tadqiqotiga ko'ra, xavfsizlik mutaxassislarining 67 foizi false positive muammosi ularning ish samaradorligiga salbiy ta'sir qilayotganini ta'kidlagan.

6.3. Ma'lumotlarni Zaharlash (Data Poisoning)

Mashinaviy o'qitish modellari sifati o'quv ma'lumotlariga bevosita bog'liq. Agar tajovuzkor o'quv ma'lumotlarini manipulyatsiya qilishga muvaffaq bo'lsa, model noto'g'ri o'rganishi va tahdidlarni o'tkazib yuborishi mumkin. Bu adversarial machine learning yoki data poisoning hujumi deb ataladi. Misol uchun, tajovuzkor tarmoq trafigiga asta-sekin zararli namunalar kiritib, modelni bu namunalarni normal deb qabul qilishga o'rgatishi mumkin.

6.4. Maxfiylik va Etik Muammolar

SI asosidagi kuzatuv tizimlari foydalanuvchilarning xatti-harakatlari haqida juda katta hajmdagi ma'lumot to'playdi. Bu GDPR (General Data Protection Regulation) va boshqa ma'lumotlarni himoya qilish qonunlari bilan ziddiyat keltirib chiqarishi mumkin. Bundan tashqari, ba'zi algoritmlar tanlab olingan guruhlarni nohaq belgilashi — algoritmik tarafkashlik (algorithmic bias) — muammosi ham kiberxavfsizlik tizimlarida jiddiy etik muammo hisoblanadi.

7. KIBERXAVFSIZLIKDA MASHINAVIY O'QITISH TEXNOLOGIYALARI

Kiberxavfsizlik tizimlari ishlayotgan asosiy texnologiyalarni to'liq tushunish uchun mashinaviy o'qitish paradigmalarini alohida ko'rib chiqish zarur.

7.1. Mashinaviy O'qitish (Machine Learning)

Machine Learning — kompyuter tizimlarining aniq dasturlashtirilmasdan, ma'lumotlardan o'rganish qobiliyatidir. Kiberxavfsizlikda ML uch asosiy shaklda qo'llaniladi: nazorat ostidagi o'qitish (supervised learning) — belgilangan ma'lumotlardan o'rganish; nazorat ostidagi bo'lmagan o'qitish (unsupervised learning) — ma'lumotlardagi yashirin naqshlarni topish; va mustahkamlash orqali o'qitish (reinforcement learning) — tajriba asosida optimal qarorlar qabul qilishni o'rganish. Kiberxavfsizlikda eng ko'p qo'llaniladigan ML algoritmlari: Decision Trees, Random Forest, k-Nearest Neighbors va Naive Bayes hisoblanadi.

7.2. Chuqur O'qitish (Deep Learning)

Deep Learning — insonning biologik neyron tarmog'idan ilhomlangan ko'p qavatli sun'iy neyron tarmoqlari yordamida amalga oshiriladigan mashinaviy o'qitish turi. Chuqur o'qitish tizimlari ko'rinishdagi, ovozli va matnli ma'lumotlardan yuqori darajadagi abstrakt belgilarni (features) o'z-o'zidan ajrata olishi bilan ajralib turadi. Kiberxavfsizlikda chuqur o'qitish ayniqsa tarmoq trafigini tahlil qilishda va murakkab APT hujumlarini aniqlashda katta yutuqlar bermoqda. Konvolyutsion neyron tarmoqlar (CNN) ikkilik dastur fayllarini vizual tahlil qilishda, rekurrent neyron tarmoqlar (RNN/LSTM) esa vaqt qatoriga asoslangan tarmoq trafigini tahlil qilishda qo'llanilmoqda.

7.3. Neyron Tarmoqlar (Neural Networks)

Neyron tarmoq — ko'plab oddiy hisoblash elementlaridan (neylonlar) tashkil topgan, ular o'rtasida og'irlikka ega aloqalar mavjud bo'lgan matematik model. Kirish qavati (input layer), yashirin qavatlar (hidden layers) va chiqish qavati (output layer) dan iborat bu tuzilma juda murakkab naqshlarni ham aniqlash qobiliyatiga ega. Generative Adversarial Networks (GAN) — ikki raqobatchi neyron tarmog'idan iborat arxitektura — kiberxavfsizlikda ham hujum, ham mudofaa maqsadida tadqiq etilmoqda. GAN asosida zararli trafik namunalarini sun'iy yaratish orqali modellarni yanada barqaror o'qitish imkoni paydo bo'lmoqda.

8. ZAMONAVIY MISOLLAR VA REAL HAYOTDAGI QO'LLANISHLAR

Nazariy bilimlarni to'liq tushunish uchun real hayotda kuzatilgan misollarni ko'rib chiqish muhim ahamiyat kasb etadi.

8.1. SolarWinds Hujumi (2020) va SI Saboqlari

2020-yildagi SolarWinds kiberhujumi zamonaviy kiberjangning eng murakkab misollaridan biri hisoblanadi. Tajovuzkorlar SolarWinds Orion dasturiy ta'minotining yangilanish mexanizmiga zararli kod kiritib, 18 000 dan ortiq tashkilotga, shu jumladan AQSh hukumati idoralariga ham kirish imkoniga ega bo'ldi. Hujum 9 oyga yaqin aniqlanmay qoldi. Keyingi tahlillar shuni ko'rsatdiki, an'anaviy tarmoq kuzatuv tizimlari bu hujumni aniqlay olmadi. Biroq Microsoft's Defender ATP kabi SI asosidagi tizimlar muhit ichidagi g'ayriodatiy harakatlarni kuzatib, izlarni erta bosqichda topish imkonini berdi. Bu voqea tarmoq xavfsizligida AI ning nafaqat tashqi, balki ichki tahdidlarni ham aniqlashdagi rolini yanada muhimroq qildi.

8.2. Google DeepMind va Kiberxavfsizlik

Google o'z infratuzilmasini himoya qilish uchun chuqur o'qitish modellarini qo'llamoqda. Chronicle Security Operations platformasi Google Cloud'da ishlaydi va sekundiga petabaytlab ma'lumotni tahlil qilib, tahdidlarni real vaqtda aniqlash imkonini beradi. 2022-yilgi ommaviy ma'lumotlarga ko'ra, Google'ning SI asosidagi xavfsizlik tizimi kuniga 1 trilliondan ortiq xavfsizlik hodisasini qayta ishlaydi.

8.3. Tibbiyot Sohasidagi Kiberxavfsizlik

2021-yilda Florida shtatidagi Oldsmar shahrining suv tozalash stantsiyasiga kiberhujum urinishi amalga oshirildi. Tajovuzkor tizimga kirib, natriy gidroksid miqdorini 111 barobar

oshirishga harakat qildi. Operatordan biri g'ayriodatiy faoliyatni ko'rib, o'z vaqtida to'xtatdi. Agar tizimda SI asosidagi anomaliya aniqlash qurilgan bo'lganda edi, bu urinish operatorning ko'ziga chalingunga qadar to'xtatilgan bo'lar edi. Bu misoldan keyin ko'plab kommunal xizmatlar SI asosidagi OT/ICS xavfsizlik tizimlarini joriy etishga kirishdi.

9. O'ZBEKISTON VA JAHONDA AI HAMDA KIBERXAVFSIZLIK RIVOJI

Global miqyosda kiberxavfsizlik sanoatining hajmi 2023-yilda 188 milliard AQSh dollarini tashkil etgan bo'lsa, 2030-yilga kelib bu ko'rsatkich 500 milliard dollardan oshishi kutilmoqda (MarketsandMarkets, 2024). Eng faol investorlar qatorida AQSh, Xitoy, Buyuk Britaniya va Isroil turadi.

O'zbekiston Respublikasida ham kiberxavfsizlik sohasiga e'tibor yildan yilga oshib bormoqda. 2021-yil avgustda Axborot xavfsizligi sohasidagi davlat siyosati to'g'risidagi qonun qabul qilingan bo'lib, u davlat organlari va tanqidiy infratuzilma ob'ektlarida axborot xavfsizligini ta'minlashga doir talablarni belgilaydi. O'zbekiston Respublikasi Prezidentining 2022-yil 2-iyuldagi Farmoni bilan «Sun'iy intellekt texnologiyalarini rivojlantirish va ularni joriy etish chora-tadbirlari to'g'risida»gi Farmon qabul qilingan bo'lib, unda kiberxavfsizlik sohasida ham SI dan foydalanishni kengaytirish borasida ko'rsatmalar mavjud.

Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi huzuridagi Kiberxavfsizlik markazi (CERT-UZ) respublika miqyosida kibertahdidlar monitoringini olib bormoqda. 2023-yil ma'lumotlariga ko'ra, O'zbekiston tarmog'iga yo'naltirilgan kiberhujumlar soni 2022-yilga nisbatan 35 foizga oshgan. Bu holat rivojlangan kiberxavfsizlik infratuzilmasini, xususan SI asosidagi mudofaa tizimlarini shakllantirish zarurligini ko'rsatadi.

O'zbekistonda INHA University, Turin Polytechnic University in Tashkent, Webster University Toshkent va Toshkent Axborot Texnologiyalari Universiteti (TATU) kabi oliy o'quv yurtlarida kiberxavfsizlik bo'yicha ixtisoslashgan dasturlar taklif etilmoqda. IT-Park rezidentlari qatorida kiberxavfsizlik yo'nalishidagi startaplar ham paydo bo'lmoqda va sohadagi kadrlar tayyorlash masalasi davlat miqyosida kun tartibiga qo'yilgan.

10. KELAJAK ISTIQBOLLARI

Sun'iy intellekt va kiberxavfsizlik sohasining kelajagi ko'plab va'da beruvchi, ayni vaqtda e'tiborni tortadigan tendensiyalar bilan bog'liq.

10.1. Kvant Hisoblash va Post-Kvant Kriptografiya

Kvant kompyuterlarining paydo bo'lishi bugungi kriptografik tizimlarni — RSA va AES — daqiqalar ichida buzish imkonini berishi mumkin. NIST (AQSh Milliy Standartlar va Texnologiyalar Instituti) 2024-yilda kvantga chidamli kriptografiya standartlarini rasmiy tasdiqladi. Kelajakda SI tizimlari yangi kriptografik standartlarning joriy etilishini nazorat qilish va kvant hujumlarining dastlabki belgilarini aniqlashda muhim rol o'ynaydi.

10.2. Autonomous Security Operations Center (SOC)

Mustaqil xavfsizlik operatsiyalari markazi (Autonomous SOC) kelajakda tahdidlarni aniqlash, tahlil qilish va bartaraf etishni deyarli to'liq avtomatik bajarishi rejalashtirilmoqda. Gartner prognoziga ko'ra, 2027-yilga kelib yirik tashkilotlarning 40 foizi SOC operatsiyalarining 60 foizini sun'iy intellektga topshirgan bo'ladi.

10.3. Large Language Models (LLM) va Kiberxavfsizlik

GPT-4 va shunga o'xshash katta til modellarining kiberxavfsizlikka ta'siri ikki tomonlama. Bir tomondan, Security Copilot (Microsoft) va Google Security AI Workbench kabi platformalar xavfsizlik mutaxassislarining samaradorligini oshirmoqda. Boshqa tomondan, LLMlar yordamida yanada ishonchli fishing elektron xatlari, soxta kontentlar va zararli kod yozish ham

osonlashmoqda. Bu doimiy ta'sir — offensiv va defensiv SI — kelajakda ham davom etishi muqarrar.

11. XULOSA

Ushbu tadqiqot natijalariga asoslanib, bir qator muhim xulosalar qilish mumkin. Birinchidan, sun'iy intellekt kiberxavfsizlik sohasida inqilobiy o'zgarish keltirmoqda va bu jarayon kelgusi yillarda yanada jadallashadi. Mashinaviy o'qitish, chuqur o'qitish va neyron tarmoqlar asosidagi tizimlar an'anaviy usullar yetarli bo'lmagan joylarda — noma'lum tahdidlarni aniqlash, katta hajmdagi ma'lumotlarni real vaqtda qayta ishlash, tongdan-tongga uzluksiz monitoring — hal qiluvchi rol o'ynamoqda.

Ikkinchidan, SI ikki tomonlama qurol ekanligi unutilmasligi lozim. Kiberjinoyatchilar ham xuddi shu texnologiyalardan foydalanayotgani kiberxavfsizlik sohasini doimiy rivojlanishga majbur etmoqda. Tahdid manzarasi o'zgargani sari mudofaa tizimlari ham yangilanib boraverishi shart.

Uchinchidan, O'zbekiston uchun kiberxavfsizlik va SI sohasini rivojlantirish davlat va xususiy sektor hamkorligi asosida amalga oshirilishi zarur. Malakali kadrlar tayyorlash, ilmiy-tadqiqot infratuzilmasini kengaytirish va xalqaro tajriba almashish bu yo'ldagi asosiy ustuvorliklar bo'lib qolishi kerak.

To'rtinchidan, SI tizimlarining o'zi ham xavfsiz ishlab chiqilishi shart. Model ro'yxatga olish, skriptlar auditlash, ma'lumotlar sifatini ta'minlash va adversarial hujumlarga qarshi mustahkamlik kabi choralar zamonaviy MLSecOps amaliyotining asosi bo'lib qolmoqda. Kelajakda insonlar bilan SI o'rtasidagi to'g'ri muvozanat — insonning nazorat vazifasini saqlab qolgan holda SI samaradorligidan to'liq foydalanish — kiberxavfsizlikning eng asosiy tamoyiliga aylanadi.

Adabiyotlar, References, Литературы:

1.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. https://doi.org/10.1109/COMST.2015.2494502

2. Cybersecurity Ventures. (2023). Cybercrime To Cost The World 8 Trillion Annually In 2023. Cybercrime Magazine. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016

3. Darktrace. (2023). AI Cybersecurity Annual Threat Report 2023. Darktrace Ltd. https://www.darktrace.com/resources

4. Gartner Research. (2024). Top Trends in Cybersecurity 2024. Gartner Inc.

5. IBM Security. (2024). X-Force Threat Intelligence Index 2024. IBM Corporation.

6. Kirat, D., Vigna, G., & Kruegel, C. (2014). BareCloud: Bare-metal Analysis-based Evasive Malware Detection. USENIX Security Symposium, 287–301.

7. Mandiant. (2023). M-Trends 2023 Special Report. Mandiant Inc. https://www.mandiant.com/m-trends

8. NIST. (2024). Post-Quantum Cryptography Standards. National Institute of Standards and Technology. https://csrc.nist.gov/projects/post-quantum-cryptography

9. O'zbekiston Respublikasi Prezidentining 2022-yil 2-iyuldagi PF-128-son Farmoni. Sun'iy intellekt texnologiyalarini rivojlantirish va ularni joriy etish chora-tadbirlari to'g'risida. lex.uz

10. Sommer, R., & Paxson, V. (2010). Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. IEEE Symposium on Security and Privacy, 305–316.

11. Verizon. (2024). 2024 Data Breach Investigations Report. Verizon Communications Inc. https://www.verizon.com/business/resources/reports/dbir
12. Xin, Y., Kong, L., Liu, Z., et al. (2018). Machine Learning and Deep Learning Methods for Cybersecurity. IEEE Access, 6, 35365–35381. https://doi.org/10.1109/ACCESS.2018.2836950
13. CERT-UZ. (2023). O'zbekiston Respublikasi kompyuter hodisalariga javob berish milliy guruhi hisoboti. cert.uz