SUN‘IY INTELLEKT ASOSIDAGI KIBERXAVFSIZLIK: ZAMONAVIY YECHIMLAR VA MUAMMOLAR

Islomova Ozoda Zokirjon qizi
Axborot texnologiyalari va menejment universiteti
Filologiya va tillarni o‘qitish (ingliz) yo‘nalishi talabasi

Annotatsiya: Ushbu maqolada sun‘iy intellekt (SI) texnologiyalarining kiberxavf-sizlik sohasidagi o‘rni, zamonaviy yechimlari va uchraydigan muammolar tahlil qilinadi. Sun’iy intellekt asosida ishlovchi tizimlar kiberhujumlarni oldindan aniqlash, ularga javob qaytarish va xavfsizlikni mustahkamlashda samarali vosita bo‘lib xizmat qilmoqda. Xususan, sun’iy intellekt algoritmlari zararli dasturlarni aniqlash, firibgarlikdan himoya qilish, anomal faollikni kuzatish va Avtomatlash-tirilgan xavfsizlik choralarini qo‘llashda keng qo‘llanmoqda. Shu bilan birga, ushbu texnologiyalarning rivojlanishi bilan bir qator muammolar ham yuzaga kelmoqda. Jumladan, sun’iy intellekt asosida ishlovchi kiberxavfsizlik tizimlarining buzilish ehtimoli, noto‘g‘ri tahlil natijalari, maxfiylik va ma’lumotlar xavfsizligiga oid masalalar dolzarb hisoblanadi. Shuningdek, tajovuzkorlar ham sun’iy intellektdan foydalanib, yanada rivojlangan hujum usullarini ishlab chiqayotganligi sababli, kiberxavfsizlik tizimlarini doimiy ravishda yangilab borish talab etiladi. Maqolada zamonaviy sun‘iy intellekt texnologiyalari yordamida kiberxavfsizlikni mustahkamlash usullari va bu boradagi muammolarni bartaraf etish bo‘yicha ilmiy-amaliy yondashuvlar muhokama qilinadi.

Kalit so’zlar: kiberxavfsizlik, axborot xavfsizligi, ma’lumotlarni himoya qilish, inson omili, kiberjinoyatchilik, kiber etika, anomal faollik, Adversarial hujumlar

KIRISH

Bugungi kunda raqamli texnologiyalarning jadal rivojlanishi kiberxavfsizlik masalalarini dolzarb muammolardan biriga aylantirdi. Internet va axborot tizimlarining keng qo‘llanilishi natijasida kiberhujumlar soni ortib, ularning murakkabligi ham oshib bormoqda. Shu bois, zamonaviy texnologiyalar yordamida samarali himoya mexanizmlarini yaratish muhim ahamiyat kasb etmoqda.

XXI asr – axborot texnologiyalari asri. Qariyb chorak asr bo‘lganiga qaramasdan, dasturlash, axborotni uzatish, ma’lumotlar tahlili, axborot xavfsizligi, kiberxavfsizlik hamda sun’iy intellekt texnologiyalari sohasida o‘zgarishlar yaqqol sezilmoqda.

O‘zbekiston Respublikasi Prezidenti Shavkat Miromonovich Mirziyoyev aholiga ko‘rsatilayotgan xizmatlarni raqamlashtirishga alohida e’tibor qaratdilar. Buning natijasida 2024-yilda https://my.gov.uz/oz yagona interaktiv davlat xizmatlari portali orqali 684 ta onlayn xizmat joriy qilindi.

Axborot texnologiyalari rivojlanib borgani sari kiberjinoyatlar salmog‘i ham o‘sib bormoqda. 2024-yil may oyida O‘zbekistonning “.uz” domeni veb-saytlariga 6,6 milliondan ortiq kiberhujumlar amalga oshirildi. Bu esa internet yoki ijtimoiy tarmoqlar orqali sodir etilayotgan turli huquqbuzarlik va jinoyatlarga qarshi kurashishning samarali mexanizmlarini taqozo etadi.

O‘zbekiston Respublikasi Prezidentining 2023-yil 30-noyabrdagi “Raqamli mahsulotlar (xizmatlar) iste’molchilari huquqlarini himoya qilish va raqamli texnologiyalar vositasida sodir etiladigan huquqbuzarliklarga qarshi kurashishni kuchaytirish choralari to‘g‘risida”gi PQ-381-sonli Qaroriga asosan, soha mutaxassislari kiberjinoyatchilikka qarshi kurashishda o‘z malakalarini oshirib borishi yo‘lga qo‘yildi.

O‘zbekiston Respublikasi Ichki ishlar vazirligida kiberxavfsizlikni ta’minlash, kiberjinoyatlarning oldini olish, aniqlash va fosh etish Axborot texnologiyalari aloqa va axborotni himoyalash boshqarmasi, Tezkor qidiruv departamenti Kiberxavfsizlik markazi hamda Ekspert kriminalistika bosh markazining Raqamli axborot-qidiruv tizimlari markazi mas’ul xodimlari tomonidan amalga oshirib kelinmoqda.

Ushbu maqolada sun’iy intellekt asosidagi kiberxavfsizlik yechimlari, ularning afzalliklari hamda duch kelinayotgan asosiy muammolar tahlil qilinadi. Zamonaviy texnologiyalar va ularning rivojlanish istiqbollari haqida fikr yuritiladi.

ADABIYOTLAR TAHLILI

Sun’iy intellekt (SI) asosidagi kiberxavfsizlik bo‘yicha tadqiqotlar so‘nggi yillarda katta e’tiborga sazovor bo‘lib, ushbu yo‘nalishda ko‘plab ilmiy maqolalar, monografiyalar va xalqaro hisobotlar chop etilgan. Quyida ushbu sohadagi asosiy adabiyotlar tahlil qilinadi.

O‘zbekiston Respublikasining 2022-yil 15-apreldagi “Kiberxavfsizlik to‘g‘risida”O‘RQ764-sonli Qonunida “kiberxavfsizlik – kibermakonda shaxs, jamiyat va davlat manfaatlarining tashqi va ichki tahdidlardan himoyalanganlik holati” deb ta’rif berilgan.

Mishra (2021) o‘z tadqiqotida anomal faollikni aniqlash uchun sun’iy intellekt asosidagi monitoring tizimlarini tahlil qilgan. Ularning fikriga ko‘ra, chuqur o‘rganish usullari (Deep Learning) tarmoq trafigidagi noodatiy harakatlarni aniqlashda yuqori samaradorlikka ega.

Sun’iy intellektning kiberxavfsizlikda samarali qo‘llanilishiga qaramay, bu texnologiya kiberjinoyatchilar tomonidan ham ekspluatatsiya qilinishi mumkin. Huang (2020) tadqiqotida tajovuzkorlar sun’iy intellektdan foydalanib, murakkab kiberhujumlarni amalga oshirishi mumkinligi ta’kidlangan. Masalan, “DeepFake” texnologiyalari ijtimoiy muhitda firibgarlikning yangi shakllarini yaratmoqda.

Shuningdek, Barreno (2021) adversarial hujumlar orqali sun’iy intellekt modellarini aldash imkoniyatlarini o‘rganib chiqishgan. Ushbu tadqiqotda sun’iy

intellekt asosidagi kiberxavfsizlik tizimlarining zaif tomonlari va ularni mustahkamlash yo‘llari taklif qilingan.

Adabiyotlar tahlili shuni ko‘rsatadiki, sun’iy intellekt kiberxavfsizlik tizimlarini rivojlantirishda katta imkoniyatlar taqdim etmoqda. Biroq, sun’iy intellekt asosidagi xavfsizlik tizimlarining zaif tomonlari va tajovuzkorlarning ushbu texnologiyadan foydalanish ehtimoli ham muhim muammolardan biridir. Shu sababli, sun’iy intellekt asosida kiberxavfsizlikni yanada rivojlantirish uchun texnologik takomillashtirish va xavfsizlik choralari doimiy ravishda yangilanib borishi lozim.

METODOLOGIYA

Ushbu tadqiqotda sun’iy intellekt asosidagi kiberxavfsizlik yechimlari va ularning samaradorligini baholash uchun quyidagi metodologik yondashuvlar qo‘llaniladi:

Nazariy tahlil – SI va kiberxavfsizlik bo‘yicha ilmiy maqolalar, tadqiqot ishlari va xalqaro standartlar o‘rganiladi. Shuningdek, zamonaviy tahdidlar va ularni bartaraf etish usullari bo‘yicha tahliliy sharh tayyorlanadi.

Mavjud yechimlarni tahlil qilish – kiberxavfsizlik sohasida qo‘llanilayotgan sun’iy intellekt algoritmlari, jumladan, mashinani o‘rganish (ML) va chuqur o‘rganish (DL) modellarining ishlash tamoyillari o‘rganiladi. Anomal faollikni aniqlash, zararli dasturlarni oldindan bashorat qilish va avtomatlashtirilgan himoya tizimlari tahlil qilinadi.

Baholash – SI asosidagi texnologiyalarni rivojlantirish uchun takliflar ishlab chiqiladi.

Ushbu metodologiya sun’iy intellekt asosidagi kiberxavfsizlik tizimlarining samaradorligini ilmiy va amaliy jihatdan o‘rganish, mavjud muammolarni aniqlash hamda kelajakda yanada rivojlantirish yo‘llarini belgilashga yordam beradi.

MUHOKAMA VA NATIJALAR

Kiberxavfsizlik sohasida sun’iy intellekt asosidagi yechimlar zamonaviy tahdidlarga qarshi kurashda muhim rol o‘ynaydi. Quyida sun’iy intellekt asosidagi kiberxavfsizlik yechimlarining ba’zi asosiy jihatlari va ularning qo‘llanilishi haqida ma’lumot keltirilgan:

1. Anomaliyalarni aniqlash (Anomaly Detection)

Sun’iy intellekt yordamida tarmoq trafigi, foydalanuvchi harakatlari yoki tizimlar o‘rtasidagi o‘zaro aloqalardagi g‘ayritabiiy faoliyatni aniqlash mumkin. Machine Learning (ML) modellari odatdagi faoliyatni o‘rganib, undan chetga chiqadigan harakatlarni avtomatik ravishda aniqlaydi.

Masalan: DDoS hujumlari, firibgarlik (fraud) harakatlari yoki ma’lumotlarni o‘g‘irlashga urinishlar.

2. Xavfni bashorat qilish (Threat Prediction)

Sun’iy intellect tizimlari katta hajmdagi ma’lumotlarni tahlil qilib, potensial xavflarni oldindan bashorat qilish imkoniyatiga ega. Behavioral Analytics yordamida

foydalanuvchilarning odatiy harakatlari o‘rganilib, ularning xatti-harakatlaridagi o‘zgarishlar asosida xavf baholanadi.

Masalan: Foydalanuvchi hisobiga noqonuniy kirishga urinishlar yoki zararli dasturlarning tarqalishi.

3. Zararli dasturlarni aniqlash (Malware Detection)

Sun’iy intellect zararli dasturlarni aniq va tezda aniqlash uchun ishlatiladi. Deep Learning modellari yordamida yangi va noma’lum zararli dasturlar ham aniqlanishi mumkin [4].

Masalan: Ransomware, viruslar, trojanlar va boshqa zararli dasturlar.

4. Foydalanuvchi autentifikatsiyasi (User Authentication)

Biometrik ma’lumotlar (masalan, barmoq izi, yuzni tanib olish) va sun’iy intellect yordamida foydalanuvchilarning haqiqiyligi tekshiriladi. Behavioral Biometrics yordamida foydalanuvchilarning klaviaturadagi urish tezligi, sichqonchani boshqarish uslubi kabi xususiyatlari asosida autentifikatsiya amalga oshiriladi [5].

Masalan: Parolni buzishga urinishlar yoki noqonuniy kirishlar.

5. Xavfsizlikni avtomatlashtirish (Security Automation)

Sun’iy intellekt tizimlari xavfsizlik hodisalarini avtomatik ravishda boshqarish va ularga javob berish imkoniyatini beradi. SOAR (Security Orchestration, Automation, and Response) platformalari yordamida xavfsizlik hodisalari tezda hal qilinadi.

Masalan: Xavfsizlik buzilishlarini avtomatik ravishda to‘sib qo‘yish yoki zararli faoliyatni bloklash.

6. Ma’lumotlarni shifrlash va himoya qilish (Data Encryption and Protection)

Sun’iy intellekt yordamida ma’lumotlarni shifrlash va ularni himoya qilish jarayonlari avtomatlashtiriladi. Homomorphic Encryption kabi texnologiyalar yordamida ma’lumotlar shifrlangan holda ham tahlil qilinishi mumkin.

Masalan: Ma’lumotlarni o‘g‘irlashga qarshi himoya.

7. Xavfsizlikni doimiy ravishda yangilash (Continuous Security Monitoring)

Sun’iy intellekt tizimlari tarmoq va tizimlarni doimiy ravishda monitoring qilib, xavflarni real vaqt rejimida aniqlaydi. SIEM (Security Information and Event Management) tizimlari yordamida xavfsizlik hodisalari yig‘ilib, tahlil qilinadi.

Masalan: Tarmoqda sodir bo‘layotgan g‘ayritabiiy faoliyatni aniqlash.

8. Phishing va ijtimoiy muhandislikka qarshi kurash (Anti-Phishing and Social Engineering)

Sun’iy intellekt yordamida phishing elektron pochta xatlari va ijtimoiy muhandislik hujumlarini aniqlash va oldini olish mumkin. Natural Language Processing (NLP) yordamida xatlarning mazmuni tahlil qilinadi va zararli bo‘lishi mumkin bo‘lgan xabarlar bloklanadi.

Masalan: Phishing xatlari yoki soxta veb-saytlarga yo‘naltirishga urinishlar.

9. IoT qurilmalarini himoya qilish (IoT Security)

Sun’iy intellekt Internet of Things (IoT) qurilmalarini himoya qilish uchun ishlatiladi. IoT qurilmalarining xavfsizligini ta’minlash uchun ularning faoliyati doimiy ravishda monitoring qilinadi.

Masalan: IoT qurilmalariga hujumlarni aniqlash va bloklash. Sun’iy intellekt asosidagi kiberxavfsizlik yechimlari zamonaviy tahdidlarga qarshi kurashda muhim rol o‘ynaydi.

Sun’iy intellekt tizimlari yordamida xavflarni oldindan bashorat qilish, zararli faoliyatni aniqlash va xavfsizlikni avtomatlashtirish kabi imkoniyatlar yaratiladi. Biroq, sun’iy intellekt tizimlarining o‘zi ham xavfsizligini ta’minlash va ularni doimiy ravishda yangilab turish muhimdir.

Kiberxavfsizlik sohasida sun’iy intellekt asosidagi yechimlar tobora keng qo‘llanilmoqda. Biroq, bu texnologiyalar o‘ziga xos muammolar va qiyinchiliklarni ham keltirib chiqaradi. Quyida sun’iy intellekt asosidagi kiberxavfsizlikdagi ba’zi muammolar keltirilgan:

1. Sun’iy intellekt tizimlarining zaif tomonlari

Hujumlar uchun mo‘ljallangan hujumlar (Adversarial Attacks): Sun’iy intellekt modellari, ayniqsa, tasvirni tanib olish yoki matnni tahlil qilish kabi vazifalarda, kichik va ataylab yaratilgan o‘zgartirishlar (masalan, piksellar yoki belgilardagi o‘zgarishlar) tufayli noto‘g‘ri natijalar berishi mumkin. Bu xavfsizlik tizimlarini osongina aldash imkonini beradi.

Modelning buzilishi (Model Poisoning): Agar hujumchi sun’iy intellekt modelini o‘qitish jarayoniga kirib borsa, u noto‘g‘ri ma’lumotlar kiritib, modelni buzishi mumkin. Bu esa modelni noto‘g‘ri qarorlar qabul qilishiga olib keladi.

2. Ma’lumotlar xavfsizligi va maxfiylik muammolari

Ma’lumotlar sizishi: sun’iy intellekt tizimlari ko‘pincha katta hajmdagi ma’lumotlarni qayta ishlaydi. Agar bu ma’lumotlar noto‘g‘ri himoyalansa, shaxsiy yoki maxfiy ma’lumotlar sizib ketishi mumkin.

Ma’lumotlar manipulyatsiyasi: sun’iy intellekt modellari noto‘g‘ri yoki manipulyatsiya qilingan ma’lumotlar asosida qaror qabul qilsa, bu jiddiy xavflarga olib kelishi mumkin.

3. Sun’iy intellekt asosidagi hujumlarning murakkabligi

Avtomatlashtirilgan hujumlar: Sun’iy intellekt yordamida hujumlar avtomatlashtirilishi va tezroq amalga oshirilishi mumkin. Bu esa an’anaviy himoya usullarini samarasiz qiladi.

Adaptiv hujumlar: sun’iy intellekt tizimlari hujumlarni dinamik ravishda moslashtirib, himoya tizimlarini chetlab o‘tishi mumkin.

4. Himoya tizimlarining qiyinligi

Sun’iy intellekt tizimlarini himoya qilish: sun’iy intellekt asosidagi

kiberxavfsizlik tizimlarini o‘zlari ham hujumlarga uchrashi mumkin. Shuning uchun ularni qanday himoya qilish murakkab masaladir.

Soxta ijobiy natijalar (False Positives): sun’iy intellekt tizimlari ba’zan xavfsiz hodisalarni xavfli deb baholashi mumkin, bu esa tizimning ishonchliligini pasaytiradi.

5. Qonuniy va axloqiy muammolar

Mas’uliyat muammosi: Agar sun’iy intellekt tizimi noto‘g‘ri qaror qabul qilsa va zarar yetkazsa, mas’ul kim bo‘lishi aniq emas. Bu qonuniy jihatdan murakkab masaladir.

Avtonom qurollar va hujumlar: sun’iy intellekt asosidagi avtonom qurollar yoki hujumlar insoniyat uchun jiddiy xavf tug‘dirishi mumkin. Bu axloqiy jihatdan ham qabul qilinishi qiyin.

6. Sun’iy intellekt tizimlarini tushunish qiyinligi

Qora quti muammosi: Ko‘pgina sun’iy intellekt modellari, ayniqsa, chuqur o‘rganish (deep learning) modellari, qanday qaror qabul qilganini tushunish qiyin. Bu esa ularni ishonchli va tushunarli qilishni qiyinlashtiradi.

Tekshirish va audit qilish qiyinligi: sun’iy intellekt tizimlarining ichki ishlashini tekshirish va ularni audit qilish an’anaviy dasturiy ta’minotga qaraganda ancha murakkab.

7. Sun’iy intellekt tizimlaridan noto‘g‘ri foydalanish

Soxta ma’lumotlar yaratish (Deepfakes): sun’iy intellekt yordamida soxta videolar, audiolar yoki matnlar yaratish mumkin. Bu esa noto‘g‘ri ma’lumotlar tarqalishiga olib keladi.

Spam va firibgarlik: sun’iy intellekt tizimlari spamlarni yoki firibgarlik xabarlarini yanada murakkabroq qilishi mumkin, bu esa odamlarni aldashni osonlashtiradi.

Sun’iy intellekt asosidagi kiberxavfsizlik yechimlari katta imkoniyatlar va afzalliklarga ega bo‘lsa-da, ular bilan bog‘liq muammolar ham jiddiy. Bu muammolarni hal qilish uchun texnologik, qonuniy va axloqiy jihatdan yondashuvlar kerak. Sun’iy intellekt tizimlarini yanada ishonchli, xavfsiz va tushunarli qilish bo‘yicha ishlar olib borilmoqda, ammo bu yo‘lda hali ko‘p qiyinchiliklar mavjud.

Kiberxavfsizlik muammolarini hal qilish yondashuvlardan biri bu – texnologik yondashuvlarda shifrlash va autentifikatsiya: Shaxsiy va tijorat ma’lumotlarini xavfsiz saqlash uchun shifrlash algoritmlaridan foydalanish. Masalan, Advanced Encryption Standard (AES) va Rivest-Shamir-Adleman (RSA) algoritmlari ma’lumotlarning xavfsizligini ta’minlash uchun ishlatiladi.

XULOSA VA TAKLIFLAR

Sun’iy intellekt texnologiyalarining kiberxavfsizlik sohasida qo‘llash bo‘yicha takliflar:

- birinchidan, sun’iy intellekt asosida ishlovchi xavfsizlik tizimlarini doimiy

ravishda takomillashtirish – sun’iy intellekt algoritmlarining aniqlik darajasini oshirish va noto‘g‘ri tahlillarni kamaytirish maqsadida mashinaviy o‘rganish modellarini yanada rivojlantirish zarur;

- ikkinchidan, Adversarial hujumlarga qarshi choralar ishlab chiqish – kiberjinoyatchilarning sun’iy intellekt texnologiyalaridan foydalangan holda amalga oshirayotgan hujumlariga qarshi yangi yondashuvlar ishlab chiqish talab etiladi. Shu jumladan, adversarial training usullarini qo‘llash muhim ahamiyat kasb etadi;

- uchinchidan, sun’iy intellekt asosida ishlovchi xavfsizlik tizimlarini inson nazorati bilan uyg‘unlashtirish – sun’iy intellekt avtomatlashtirilgan tahlil vositasi sifatida samarali bo‘lsa-da, kiberxavfsizlik bo‘yicha mutaxassislarning nazorati va qaror qabul qilish jarayonlari bilan integratsiya qilinishi kerak;

- to‘rtinchidan, ma’lumotlar maxfiyligi va etik muammolarni hisobga olish– sun’iy intellekt tizimlari foydalanuvchi ma’lumotlari bilan ishlashi sababli, ma’lumotlar maxfiyligini ta’minlash uchun shaffoflik va xalqaro xavfsizlik standartlariga rioya qilish zarur;

- beshinchidan, sun’iy intellekt asosida ishlovchi kiberxavfsizlik texnologiyalarini tarmoq infratuzilmasiga keng joriy etish – davlat tashkilotlari, xususiy sektor va ilmiy markazlar sun’iy intellekt asosida kiberxavfsizlik tizimlarini kengroq joriy etish hamda ularni xavfsizlik choralariga mos ravishda optimallashtirishga e’tibor qaratishlari lozim;

- oltinchidan, mutaxassislarni tayyorlash va malakasini oshirish – kiberxavfsizlik va sun’iy intellekt bo‘yicha mutaxassislar tayyorlash va ularning bilimlarini yangilab borish muhim ahamiyatga ega. Universitetlar, tadqiqot markazlari va IT kompaniyalar ushbu yo‘nalishda hamkorlikni kuchaytirishi zarur.

Sun’iy intellekt asosidagi kiberxavfsizlik yechimlari axborot xavfsizligini ta’minlashda yangi imkoniyatlar yaratmoqda, biroq ushbu texnologiyalar bilan bog‘liq muammolarni hal qilish uchun doimiy tadqiqotlar va innovatsion yondashuvlar talab etiladi. Kelajakda sun’iy intellekt asosidagi xavfsizlik tizimlarini yanada rivojlantirish va ularning ishonchliligini oshirish uchun ilmiy-amaliy tadqiqotlarni kengaytirish muhim ahamiyat kasb etadi.

References:

1. ISO 15408. Axborot texnologiyalari — Xavfsizlik texnikasi – IT xavfsizligini baholash mezonlari. — Geneve: ISO / IEC Mualliflik huquqi idorasi, 2019. - 44 s;

2. ISO 17799. Axborot xavfsizligini boshqarish bo'yicha amaliyot kodeksi. - Geneve: ISO / IEC Mualliflik huquqi idorasi, 2000 yil. - 25 s;

3. ISO 19791. Operatsion tizimlarni xavfsizlikni baholash. - Geneve: ISO / IEC Mualliflik huquqi idorasi, 2019. - 165 s;

4. NIST maxsus nashri 800-26. Axborot texnologiyalari tizimlari uchun xavfsizlik o'z-o'zini baholash bo'yicha qo'llanma [Elektron resurs]: O'zbekiston Respublikasi

Standartlar va texnologiyalar instituti tavsiyalari. - Vashington: AQSh hukumati bosmaxonasi, 2021- yil; Ma'lumot sanasi: 05.06.2019;

5. NIST maxsus nashri 800-30. Axborot texnologiyalari tizimlari uchun risklarni boshqarish bo‘yicha yo'riqnoma [Elektron resurs]: O'zbekiston Respublikasi Standartlar va texnologiyalar instituti tavsiyalari. - Vashington: AQSh hukumati bosmaxonasi, 2021- yil. - [55] s. - URL: Ma'lumot sanasi: 15.09.2019.

6. https://cyberleninka.ru/article/n/kiber-xavfsizlik-muammolari-va-uni-ta-minlashusullari