5-SHO‘BA: TA’LIMDA ERGONOMIKA VA SUN’IY INTELLEKT: ISHLAB CHIQARISH VA TA’LIM INTEGRATSIYASI

MA'LUMOTLAR XAVFSIZLIGINI TA'MINLASHDA SUN’IY INTELLEKTDAN FOYDALANISH.

Nigmatov X.

T.f.d.,prof.

Annotatsiya. Axborot xavfsizligini ta'minlash sohasida sun'iy intellektdan foydalanishning mumkin bo‘lgan usullarining qisqacha tahlili keltirilgan. Ma'lumotlarga ruxsatsiz kirishni oldini olish, shuningdek, axborot xavfsizligini buzish oqibatlarini kamaytirish uchun sun’iy intellektdan foydalanishning afzalliklari va uning samarali bo‘lishligi uchun takliflar berilgan.

Kalit so‘zlar: Kiberxavfsizlik, axborot xavfsizligi, sun'iy intellekt, raqamli texnologiya.

Kirish

Hammaga ma’lum, bugungi kunda dunyo bo‘yicha rivojlanayotgan davlatlarda zamonaviy axborot kommunikatsiya texnologiyalari asosida faoliyat olib borilmoqda. Raqamlashtirish jarayonlari iqtisodiyotning barcha jabxalarida qo‘llanishi natijasida katta moliyaviy yutuqlarga erishilmoqda.

Bugungi kunda har bir axborot o‘z qiymatiga ega bo‘lib, ularning bahosi olinayotgan, saqsalanayotgan, uzatilayotgan yoki qabul qilinayotgan axborotlarning butunligiga, o‘zgartirilmaganligiga, xatosiz berilganligiga va talab qilingan vaqtda yetkazib berilganligiga bog‘liq bo‘lib qolayapti. Bu shartlarning bajarilmaganligi axborotlardan foydalanuvchilarga juda katta ma’naviy, siyosiy, axloqiy va eng asosiysi iqtisodiy zarar keltirishi barchaga ma’lum.

Asosiy qism.

Albatta xozirgi raqamlashtirish davrda barcha korxonalar, tashkilotlar, vazirliklar, muassasalar, aktsiyadorlik kompaniyalar, assosatsiyalar, mas’uliyati cheklangan jamiyat va firmalar o‘zlarining faoliyati yuzasidan barcha ma’lumotlarni kompyuterlarga joylashtirib, ulardan kerak paytda foydalanib kelinmoqda, lekin ushbu ma’lumotlarni himoyalash masalalari ko‘p joylarda hisobga olinmay qolayapti /1,2/.

Axborot xavfsizligi tobora ko‘proq joriy etilayotgan va foydalaniladigan kompyuter tizimlarini hisobga olgan holda zamonaviy dunyoda muhim o‘rin tutadi. Har bir inson, xoh shaxs, xoh kompaniya bo‘lsin, o‘z ma'lumotlarini o‘g'irlash, o‘chirish yoki o‘zgartirish xavfini kamaytirishga xarakat qiladi. Shu jumladan, avtomatlashtirilgan tizimda kiberxavfsizlik muhim rol o‘ynaydi.

Bugun dunyo bo‘ylab axborot xavfsizligi bilan birgalikda “kiberxavfsizlik” tushunchasi keng qo‘llanilib, uning ahamiyati borgan sari to‘liqroq e’tirof etilmoqda. **Kiberxavfsizlik** – bu kibermakonning barcha tashkil etuvchilari (ya’ni texnik qurilmalar va foydalanuvchilar)ni har qanday tahdidlar va kutilmagan ta’sirlardan himoyalanganlik holati hisoblanadi.

Bugungi kunga kelib, kiberhujumlar soni tez va barqaror o‘sishda davom etmoqda, hujumlarning o‘zi tobora takomillashib bormoqda va bunday kiberhujumlarning maqsadi odatda maxfiy ma'lumotlarga kirish, uni o‘zgartirish yoki yo‘q qilish, foydalanuvchilardan pul undirish, biznes va moliyaviy markazlar, davlat tashkilotlari faoliyati uchun mas'ul bo‘lgan hisoblash tizimlarining ishlashini buzishga qaratilgan bo‘lib qolmoqda.

Kiberxavfsizlik sohasida ilg'or texnologiyalarni joriy etish hujumlarni batafsil aniqlash va ularni kiberxavfsizlik bo‘yicha mutaxassislarga qaraganda tezroq hal qilish uchun sun'iy intellektdan foydalanishga to‘g’ri kelmoqda /3/.

Sun'iy intellekt (SI) - bu tahdidlarni aniqlay oladigan va ularni bartaraf etish va oldini olish uchun avtomatik ravishda zarur choralarni ko‘radigan texnologiya deb hisoblasa bo‘ladi. Sun'iy intellektga asoslangan vositalarga quyidagilar kiradi:

1. Biometrik autentifikatsiyani qo‘llash. Hozirgi kunda raqamli parol tizimlari o‘zini oqlamay qoldi. Shuning uchun oxirgi vaqtda insonning fiziologik parametrlari va xarakteristikalarini, xulqining xususiyatlarini o‘lchash orqali foydalanuvchini ishonchli autentifikatsiyalashga imkon beruvchi biometrik autentifikatsiyalash tizimini yaratish keng tarqala boshlandi.

Biometrik autentifikatsiyalash usullari an’anaviy usullarga nisbatan quyidagi afzalliklarga ega:

- biometrik alomatlarning noyobligi tufayli autentifikatsiyalashning ishonchlilik darajasining yuqoriligi;
- biometrik alomatlarning sog‘lom shaxsdan ajratib bo‘lmasligi;
- biometrik alomatlarni soxtalashtirishning qiyinligi.

Foydalanuvchini autentifikatsiyalashda biometrik algoritmlarni faol ishlatish koefitsientini mutaxassislar hozrcha quyidagicha aniqladilar:

- barmoq izlari (52 %);
- qo‘l panjasining geometrik shakli (10%);
- yuzning shakli va o‘lchamlari (11,4%);
- ovoz xususiyatlari (4,1%);
- ko‘z yoyi va to‘r pardasining naqshi (7,3%);
- insonni imzosi bo‘yicha (2,4%).

Ushbu ishlatish koefitsienti bugungi kunda ishlab chiqilgan texnikaviy vositalarga bog’liq bo‘lganligi uchun o‘zgarishi nazarda tutilmoqda.

Iste’molchi nuqtai nazaridan biometrik autenfikatsiyalash tizimi quyidagi ikkita parametr orqali xarakterlanadi:

- xatolik inkorlar koeffitsiyenti FRR (false-reject rate);
- xatolik tasdiqlar koeffitsiyenti FAR (false-alarm rate).

Mukammal biometrik tizimda ikkala xatolikning parametlari nulga teng bo‘lishi shart. Afsuski, biometrik tizim ideal emas, shu sababli nimanidur qurbon qilishga to‘g‘ri keladi. Odatda tizimli parametrlar shunday sozlanadiki, mos xatolik inkorlar koeffitsiyentini aniqlovchi xatolik tasdiqlarning istalgan koeffitsiyentiga

erishiladi. Ushbu jarayonlardagi barcha ma’lumotlar bilimlar bazasiga joylashgan bo‘ladi.

Biometrik tizimlarning aksariyati identifikatsiyalash parametri sifatida barmoq izlaridan foydalanadi yani autentifikatsiyaning daktiloskopik tizimi hisoblanadi. Bunday tizimlar sodda, qulay va texnik qurilmaning arzon bo‘lganligi uchun uning keng tarqalishiga asosiy sabab bo‘ldi. Xozirgi paytda barcha davlatlarda insonning shahsiy xujjatlariga (pasportlarga) barmoq izlari kiritilganligi va juda katta ma’lumotlar ombori yaratilganligi hisoblanadi.

Qo‘l panjasi shaklini o‘quvchi qurilmalar barmoqlar uzunligini, qo‘l panja qalinligi va yuzasini o‘lchash orqali qo‘l panjasining hajmiy tasvirini yaratadi. Qo‘l panjasini skanerlovchi qurilmalar narxining yuqoriligi va o‘lchamlarining kattaligi sababli tarmoq muhitida kamdan-kam ishlatilsada. Ularning aniqligi yuqori va inkor koeffitsiyenti ya’ni inkor etilgan qonuniy foydalanuvchilar foizi ancha kichik bo‘ladi.

Yuz tuzilishini skanerlash texnologiyasi boshqa biometrik texnologiyalar yaroqsiz bo‘lgan ilovalar uchun to‘g‘ri keladi. Bu holda shaxsni identifikatsiyalash va verifikatsiyalash uchun ko‘z, burun va lab xususiyatlari ishlatiladi. Yuz tuzilishini aniqlovchi qurilmalarni ishlab chiqaruvchilar foydalanuvchini identifikatsiyalashda hususiy matematik algoritmlardan foydalanadilar.

Ovoz bo‘yicha autentifikatsiyalash tizimlari har bir odamga noyob bo‘lgan balandligi, modulyatsiyasi va tovush chastotasi kabi ovoz xususiyatlariga asoslanadi. Ovozni aniqlash nutqni aniqlashdan farqlanadi. Chunki nutqni aniqlovchi texnologiya abonent so‘zini izoxlasa, ovozni aniqlash texnologiyasi so‘zlovchining shaxsini tasdiqlaydi.

Ko‘z yoyi to‘r pardasining shakli bo‘yicha autentifikatsiyalash tizimlarni ikkita sinfga ajratish mumkin:

- ko‘z yoyi rasmidan foydalanish;
- ko‘z to‘r pardasi qon tomirlari rasmidan foydalanish.

Odam ko‘z pardasi autentifikatsiya uchun noyob ob'yekt hisoblanadi. Ko‘z tubi qon tomirlarining rasmi hatto egizaklarda ham farqlanadi.

Identifikatsiyalashning bu vositalaridan xavfsizlikning yuqori darajasi talab etilganida (masalan harbiy va mudofaa ob'yektlarining rejimli zonalarida) foydalaniladi.

2. Tahdidlarni aniqlashni tezlashtirish. An'anaviy kiberxavfsizlik tizimlari bir vaqtning o‘zida turli xil zararli dasturlarni qayta ishlashga qodir emas. Bundan tashqari, nafaqat kiberxavfsizlik paneli, balki xakerlar ham standartni ko‘tarishdi. Kengaytirilgan tahdidlarni tezda aniqlash uchun bunday muammolarni hal qila oladigan ilg'or xavfsizlik vositalaridan foydalanish kerak. Kompaniyalar doimiy ravishda yangilanib turadigan ilg'or algoritmlar va kodlar yordamida naqshni aniqlash orqali tahdidni osongina aniqlay oladigan SI tomonidan boshqariladigan tizimlarni joriy qilmoqdalar. Sun’iy intellekt xavfsizlik tizimini o‘rganish bilan birgalikda saytni chetlab o‘tish yo‘lini, zararli dasturlarning mikro xatti-harakatlarini va qaror qabul qilishga yordam beradigan har qanday zararli harakatlarni tahlil qilishda samarali hisoblanadi.

3. Hujumlarga tezkor javob berish. Agar tizim tahdidlarga qarshi kurasha olmasa va tizimga ozgina zarar etkazmasdan oldin ularni oldini olishga qodir bo‘lmasa, real vaqt rejimida tahdidlarni aniqlash mantiqiy bo‘lmay qoladi. Xakerlar jamoasi tizimga turli nuqtalardan hujum qilganda, SI darhol nuqtalarni bog'laydi va avtomatik ravishda hujumning oldini olish rejalarini taklif qiladi. SI hujumlarni aniqlash va yo‘q qilish uchun osonroq va tezroq yondashuv bo‘lgan aqlli tahlillardan foydalanadi.

4. Dinamik autentifikatsiya muhitini yaratish. Ma'lumotlar tarmoqlarda ham ushlanishi mumkin. Bu tizimlarga masofadan kirish huquqiga ega bo‘lgan xodimlar uchun tashvishli holat, ya'ni an'anaviy autentifikatsiya modellari endi xavfsiz emas bo‘lib qoldi. Bu erda ham SI yordamga keladi. SI tizimlari ko‘p faktorli autentifikatsiyadan foydalangan holda joylashuv yoki tarmoqqa muvofiq kirish imtiyozlarini o‘zgartiradigan global real vaqtda autentifikatsiya muhitini yaratadi. Bunga ma'lumotlarni yig'ish va ma'lumotlarga masofadan kirishda ilova, qurilma va tarmoqdagi foydalanuvchi xatti-harakatlarini tahlil qilish kiradi.

5. Inson ishtirokini kamaytirish. Hech qanday mashina odamlarning

ijodkorligi, tasavurlari va fikrlash qobiliyatidan oshib keta olmaydi. Ammo muhandislar tomonidan qabul qilingan qarorlar, shuningdek, to‘g'ri ma'lumotlar to‘plami, fikrlar va hozirgi tendentsiyalar bilan qo‘llab-quvvatlanadi. Muhim ma'lumotlarni o‘rganish va ulardan foydalanish ko‘p vaqt talab etadi va yuqori xavfli muammoni hal qilish bir zumda imkonsiz bo‘lib qoladi. Kompaniyalar SI texnologiyasidan foydalanadigan xavfsiz dasturni yaratganda, xavfsizlik xodimlari inson aralashuvisiz xavfsizlik tahdidlarini aniqlash va oldini olishni avtomatlashtirish orqali amalga oshirishadi. Bashoratli tahlilga qo‘shimcha ravishda foydalanuvchi xatti-harakatlarini doimiy tahlil qilish tizimlarni bir qator hujumlardan himoya qilish uchun muhandisning aralashuvini kamaytiradi.

Biroq, sun'iy intellekt tizimlari odamlar tomonidan o‘qitiladi va boshqariladi va ba'zi joylarda inson muhandislariga bo‘lgan ehtiyoj majburiydir, chunki ular mashinalar aniqlay olmaydigan anomaliyalardan tashqariga chiqishga va taxmin qilingan hujumning haqiqiyligini tasdiqlashga qodir hisoblanadilar.

Sun'iy intellekt iterativ va dinamik tizim hisoblanadi. Bunday tizim tahlil qiladigan, tajribadan "o‘rganadigan" juda ko‘p ma'lumotlar bilan qanday ishlashni biladi va o‘zi uchun kelajakda birini boshqasidan ajrata oladigan belgilarni ishlab chiqadi va shu bilan tobora rivojlanib boradi va avtonom bo‘ladi (ya'ni operatorning aralashuvini talab qilmaydi). Ma'lumotlarni tahlil qilish, o‘z navbatida, ixtisoslashgan tizimlar va dasturiy ta'minot orqali ulardagi ma'lumotlar haqida xulosa chiqarish uchun katta ma'lumotlar massivlarini o‘rganadigan statik jarayon deb hisoblash mumkin.

Bugungi kunda SI **uchta** rivojlanish darajasiga ega:

1. **Yordamchi vosita sifatida -** bugungi kunda keng tarqalgan, inson qarorlarini yaxshilaydi va optimallashtiradi, ishni tezroq va yaxshiroq bajarishga yordam beradi.
2. **Kengaytirilgan vosita** - yuqorida aytilganlarning barchasiga qo‘shimcha ravishda, muayyan sharoitlar uchun eng yaxshi echimlarni topishga qodir, odamga o‘zi bajara olmaydigan muammolarni hal qilishga yordam beradi.
3. **Avtonom qurulma** - kelajak uchun ishlab chiqilgan, mustaqil qaror qabul

qilishni oʻz ichiga oladigan texnikaviy – dasturiy vosita. Bunga oʻziyurar transport vositalari misol boʻla oladi.

SI ma'lum darajada inson aql-idrokiga ega: mavzu sohasi boʻyicha bilimlar zaxirasi, yangi bilimlarni olish mexanizmlari va ushbu bilimlardan foydalanish mexanizmlaridan tashkil topgan boʻladi. Ular ehtiyotkorlik bilan tanlangan ma'lumotlar massivlari orqali aql-idrokka asoslangan holda muammolarni hal qilishadi va qaror qabul qilishadi. Neyron tarmoqlar kompyuterga kuzatuv ma'lumotlaridan oʻrganish imkonini beruvchi dasturlash modelidan foydalanadi.

Bugungi kunda doimiy ravishda rivojlanib borayotgan kiberhujumlarni oʻrganish va sun'iy intellekt an'anaviy dasturiy yondashuvlarga qaraganda samaraliroq javob berishi orqali tahdidlarni aniqlash qobiliyatini avtomatlashtirishga yordam beradi.

Yuqorida keltirilganlar bilan birga, kiberxavfsizlik bir qator noyob muammolarni ham keltirib chiqaradi:

- hujum maydonining kengligi;
- yuzlab hujum vektorlarining sonini koʻpligi;
- malakali xavfsizlik boʻyicha mutaxassislarining tanqisligi va boshqalar.

Oʻz-oʻzini oʻrganadigan sun'iy intellektga asoslangan kiberxavfsizlikni boshqarish tizimi quyidagi ushbu muammolarning koʻpini hal qilishga qodir:

Yangi tahdidlarni aniqlash - kiberhujumlarga operativ javob berish hisoblanadi. Hujumlarning yangi turlari, xatti-harakatlar va vositalar mutaxassislarni chalkashtirib yuborishi mumkin, natijada ular yanada sekinroq javob berishadi. Bularni oʻrganishga asoslangan SI dagi dastur hujumni aniqlashga yordam beradi, yangi tahdidning umumiy xususiyatlarini ochib beradi.

Samaradorlikni nazorat qilish - xavfsizlikning mustahkam holatini saqlab qolish uchun ishlatilgan turli xil xavfsizlik vositalari va xavfsizlik jarayonlarining ta'sirini tushunish muhimdir. SI yaratilgan dasturingizning qaerda kuchli tomonlari borligini va kamchiliklari qaerda ekanligini koʻrsatib beradi.

Buzilish xavfini bashorat qilish - sun'iy intellektga asoslangan tizimlar zaif joylar uchun resurslar va vositalarni taqsimlashni rejalashtirish uchun qanday va

qayerda buzilishi mumkinligini taxmin qilishi mumkin. SI tahlilidan olingan natijalar bo‘yicha g'oyalar kiber barqarorlikni eng samarali oshirish uchun boshqaruv va jarayonlarni sozlash va yaxshilashga yordam beradi.

Xulosa.

Sun'iy intellekt (SI) zamonaviy kiberxavfsizlikning ajralmas qismiga aylandi. Texnologiyaning rivojlanishi bilan SI tahdidlarni aniqlash, kiberhujumlardan himoya qilish va qaror qabul qilishda keng qo‘llanila boshlandi. Kiberxavfsizlikda SI dan foydalanishning asosiy sabablaridan biri bu katta hajmdagi ma'lumotlarni tezda tahlil qilish qobiliyati hisoblanadi. SI tarmoqni doimiy ravishda kuzatishi va kiberhujumni ko‘rsatishi mumkin bo‘lgan g'ayritabiiy xatti-harakatlarni aniqlashi mumkin. Bundan tashqari, SI tahdidlarga avtomatik ravishda javob berishi mumkin, bu xakerlarning kirishini bloklaydi va ma'lumotlar buzilishining oldini oladi.

Biroq, barcha afzalliklarga qaramay, kiberxavfsizlikda SI dan foydalanish ham o‘zining kamchiliklari va xavflariga ega. Xakerlar himoya tizimlarini chetlab o‘tish va yanada murakkab kiberhujumlarni yaratish uchun sun'iy intellektdan foydalanishlari mumkin. Kiberxavfsizlikda sun'iy intellektdan foydalanishning xatarlari va kamchiliklarini hisobga olish va undan foydalanish xavfsizligi va to‘g’ri xarakatini ta'minlash choralarini ham ko‘rish kerak.

Kiberxavfsizlikda SI dan foydalanish samarali va xavfsiz bo‘lishi uchun quyidagi muhim fikrlarni hisobga olish kerak:

Birinchidan, SI ma'lumotlari va algoritmlarini kiberhujumlar va xakerlardan himoya qilish kerak. Xakerlar SI ni tizimga kiritish va himoya tizimlarini chetlab o‘tish va uning ishlashini o‘zgartirish uchun zararli algoritmlardan foydalanishlari mumkin. Shuning uchun sun'iy intellektga asoslangan tizimlar uchun himoya choralarini kuchaytirish va zaifliklarni muntazam tekshirib turish kerak.

Ikkinchidan, sun'iy intellektni har xil turdagi kiberhujumlar va tahdidlarga o‘rgatish va dolzarb ma'lumotlardan foydalanish kerak. SI yangi tahdid turlarini samarali aniqlay olmaydi, agar u ularga o‘rgatilmagan bo‘lsa. Shu sababli, yangi

tahdid turlarini aniqlay olishi uchun kiber tahdidlar haqidagi dolzarb ma'lumotlardan foydalanish va sun'iy intellekt bo‘yicha muntazam treninglar o‘tkazib turish lozim.

Uchinchidan, kiberxavfsizlikda sun'iy intellektdan foydalanish bilan bog'liq axloqiy va huquqiy masalalarni hisobga olish kerak. Masalan, sun'iy intellektga asoslangan qarorlar qabul qilish inson shaxsiy huquqlarini buzilishiga olib kelishi mumkin. Shuning uchun kiberxavfsizlikda sun'iy intellektdan foydalanishni tartibga soluvchi axloqiy va huquqiy standartlarni ishlab chiqish kerak.

Va nihoyat, kiberxavfsizlikda sun'iy intellektdan foydalanish inson omilini to‘liq almashtira olmasligini hisobga olish kerak. SI tahdidlarni aniqlash va ularga javob berish jarayonlarini avtomatlashtirishga yordam berishi mumkin, ammo xavfsizlik to‘g'risida yakuniy qaror qabul qilish hali ham inson ishtirokini talab qiladi. Shuning uchun sun'iy intellektni odamga yordam beradigan va uning o‘rnini bosmaydigan vosita sifatida ishlatish kerak.

Sun'iy intellekt texnologiyalari kiberhujumlarni yuqori tezlikda aniqlash, xavfsizlik hodisalariga maqbul javobni tanlash, hodisalarning dolzarbligi va oqibatlarini avtomatik ravishda baholash va Real vaqtda mutanosib javobni ishlab chiqish imkonini beradigan ancha yuqori samaradorlik echimlarini yaratish imkoniyatini beradi.

Umuman olganda, kiberxavfsizlikda SI dan foydalanish kiber tahdidlarga qarshi kurashishda muhim va samarali vositadir. Biroq, sun'iy intellektdan foydalanishning xatarlari va kamchiliklarini hisobga olish va undan foydalanish xavfsizligini ta'minlash choralarini ko‘rish lozim bo‘ladi.

Foydalangan adabiyotlar ro‘yxati

1. Chipiga A. F. Avtomatlashtirilgan tizimlarning axborot xavfsizligi. M.: Helios ARV, 2010 yil. 336 c.

2. Efimova L. L., Kocherga S. A. Axborot xavfsizligi. Rossiya va xorijiy tajriba: monografiya. M.: Birlik, 2015 Yil. 239 c.

3. Nigmatov H., Tursunbayev B.X. “Zamonaviy axborot-kommunikatsiya texnologiyalari asosida intellektual tizimlar yaratish”. O‘quv qo‘llanma. “Fan va

texnologiyalar” bosmaxonasi.Toshkent sh. 2020 y.

РАЗРАБОТКА СИСТЕМЫ УПРАВЛЕНИЯ ДВИЖЕНИЕМ АВТОНОМНОГО РОБОТА – ПЕШЕХОДА

Халдаров Хикматулла Ахматович
к.т.н., доцент Xikmatilla_dosent@mail.ru +998983053828
кафедра «Информационные технологии»
Ташкентский государственный педагогический университет имени Низами

Аннотация: данная исследовательская работа посвящена разработку и создания системы управления пешеходами с помощью искусственного интеллекта – робота, в переходах улиц города.

Ключевые слова и направление: разработка, создание, искусственный интеллект, управление, система, робот, переход, пешеход, улица, город.

Abstract: in this article, the development of a project in controlling the movement of a pedestrian robot, in general, at street crossings of the city using an intelligent system is presented.

Keywords and directions: algorithm, intelligent system, robot, system, control, traffic, motor transport, pedestrian, intersection.

Целью данной исследовательской работы является, разработка проекта системы управления пешеходами интеллектуальной системы (СУП ИС), т.е. – робота, в переходах улиц города [12-13].

В настоящее время, «цифрирование» разных не выполнимых функций, дает возможность осуществления ее с помощью разработки, создания и внедрение ее в народное хозяйство. Потому что, еще очень много встречаются «непрерывные», т.е. аналоговые данные, которых необходимо преобразовывать в цифру, а особенно они необходимы в разработке и создании разных интеллектуальных систем.