XODJAYEVA Mavlyuda Sabirovna
O'zbekiston xalqaro islom akademiyasi,
Zamonaviy axborot-kommunikatsiya
texnologiyalari kafedrasi dotsenti,
texnika fanlari nomzodi,
m.xodjayeva@iiau.uz

SAIDMURODOV Shoxmurod
O'zbekiston xalqaro islom akademiyasi
magistranti
shoxmurodxon@gmail.com

KIBERXAVFSIZLIK MUAMMOLARNI BARTARAF ETISHDA SUN'IY INTELEKTNING O'RNI

РОЛЬ ИССКУСТВЕННОГО ИНТЕЛЛЕКТА В РЕШЕНИИПРОБЛЕМ КИБЕРБЕЗОПАСНОСТИ

THE ROLE OF ARTIFICIAL INTELLIGENCE IN SOLVING CYBER SECURITY PROBLEMS

Annotatsiya: *Maqolada parollardan foydalanish davriy almashtirilishga moyildigi, va bu parollar administratorlar tomonidan bir vaqtda boshqa tizimlarga kirish uchun ham ishlatilishi mumkinligi asoslab berilgan. Kiberxavfsizlik sohasida Sun 'iy intellect (SI) dan kiberhujum bilan bog'liq muammolarni hal qilish uchun qanday foydalanish mumkinligi Sun'iy intellect va Kiberxavfsizlikning o'zaro bog'liqliklari, Sun'iy intellect Operatsiyalari, Parol himoyasida SI algoritmlari Fishingni aniqlashda SI tizimlari, sun'iy intellektning keberxavfsizlik sohasida foydalanishning bir qancha usullari keltirilgan. Shuningdek, sun'iy intellekt xavflarni aniqlash, hodisaga javob berish yo'nalishi va zararli dasturlarning kiberhujumlarini ular sodir bo'lishidan oldin aniqlashda yordam berish masalalari ham ko'rilgan.*

Kalit so'zlar: *Sun'iy intelekt, kiberxavfsizlik, avtomatizatsiya, kiberhujumlar.*

Аннотация: *В статье рассматривается использование паролей, тенденции периодически меняющихся паролей и возможность использования пароли администраторами для одновременного доступа к другим системам. Уделяется внимание при использование искусственного интеллекта в кибербезопасности для решения проблем, кибератаки и взаимосвязь между ИИ и кибер безопасностью, Операции искусственного интеллекта, алгоритмы СИ в защите паролем, Системы СИ в обнаружении фишинга, представлены некоторые варианты использования ИИ в методах кибер безопасности. Также рассмотрены, как системы ИИ может помочь выявлять угрозы, направлять реагирование на инциденты и обнаруживать кибератаки вредоносных программ до того, как они произойдут.*

Ключевые слова: *Искусственный интеллект, кибербезопасность, авториязация, кибератаки*

Abstract: *This article looks at password usage, changing password trends, and the ability for administrators to use passwords to access other systems at the same time. Attention is paid to the use of artificial intelligence in cybersecurity for problem solving, cyberattacks and the relationship between AI and cybersecurity, AI operations, SI algorithms in password protection, SI systems in phishing detection, some options for using AI in cybersecurity methods are presented. It also looks at how AI systems can help identify threats, guide incident response, and detect malware cyberattacks before they happen.*

Key words: *artificial intelligence, cyber security, cyber attacks, automation*

Kalit so'zlar: *Sun'iy intelekt, kiberxavfsizlik, avtomatizatsiya, kiberhujumlar.*

KIRISH

Sun'iy intellektdan (SI) foydalanish nafaqat xizmatlarni taqdim etishda inqilob qildi, balki kiberxavfsizlikni ta'minlash imkoniyatlarini yana bir pog'ona yuqoriga ko'tarishga yordam berdi. Global miqyosda oladigan bo'lsak yirik kompaniyalarning 15 foizi AI texnologik innovatsiyalaridan foydalanayotganligi taxmin qilinmoqda [3]. Biroq, SI texnologiyalarini qabul qilish kompaniyalar uchun ham yaxshi, ham yomon ta'sir ko'rsatishi mumkin. Agar kompaniyalar qat'iy xavfsizlik choralarini qo'llamasa, xakerlar himoya uchun foydalanadigan texnologiyalardan foydalanish imkoniyatiga ega bo'lishlari mumkin. Shuning uchun faqat texnologiyaga asoslangan xavfsizlik yechimlaridan foydalanadigan tashkilotlarda, hech qachon bee'tibor bo'lmaslik talab qilinadi. Buning o'rniga, kompaniyalarni xavfsiz saqlash uchun AI xavfsizlik yechimlarini muntazam yangilab borish talab qilinadi [3].

Tez-tez kiberxavfsizlik xavfini baholashni o'tkazish AI tizimini yangilashning eng xavfsiz usullaridan biridir [3]. Agar tashkilot xodimi zararli dasturga duch kelsa yoki notanish pochta manzillaridan kelgan tushunarsiz xabarlarni ochsa, u foydalanayotgan ishchi kompyuter tashkilotning ichki local tarmog'iga ulangan bo'lsa, xodimning qilgan birgina xato harakati natijasida, kompyuterga tushgan birgina infektsiya boshqa kompyuterlarga ham tarqalishiga sabab bo'lishi mumkin [5]. Yuzaga kelgan havf-xatarlar natijasida, kiberxavfsizlik sohasi o'zining eng yuqori darajadagi muhimlik darajasiga ko'tariladi. Kiberhujum kiberjinoyatchining tarmoq yoki kompyuterga ruxsatsiz kirish, zarar etkazish yoki o'zgartirishga qaratilgan harakatlaridir [6]. Axborot tizimlariga bo'ladigan hujumlar, tizimlarning faoliyatiga zarar yetkazish maqsadida qasddan, tizimli va rejalashtirilgan bo'lishi mumkin [6]. Kiberxavflar to'liq bartaraf etildi deb xulosa qilish katta xato, chunki xakerlar aqlli va qat'iyatli bo'lib, har doim yangi tizimlraning mudofaasiga kirib borishning yangi usullarini izlaydilar. Shuning uchun ushbu maqolamizda AI kiberxavfsizlik muammolarini hal qilishda, xususan, kompyuter tarmog'iga mumkin bo'lgan hujumlarni to'xtatishda qanday ishlashi muhokama qilinadi. Viruslar va odamlarni chalg'itish uchun ishlatiladigan fishing xabarlariga qarshi kurashish usullari tadqiq qilinadi.

Maqsad: Ushbu maqola hal qiladigan asosiy muammo - kiberhujum bilan bog'liq muammolarni hal qilish uchun sun'iy intellektdan qanday foydalanish mumkinligini o'rganish. SI mashinalardagi o'zaro ta'sirning inson ishtirokiga bo'lgan ehtiyojni bartaraf qilishi mumkin bo'lsa-da, IT mutaxassislari o'zlarining kengayib borayotgan kompyuter tizimlariga ruxsat berish siyosatlarini qayta ko'rib chiqishlari kerak [8]. Axborot tizimlari boshqa tizimdan ma'lumotlarni olish uchun avtomatlashtirilgan so'rovni qabul qilsa ham, birinchi kompyuter so'rovni qat'iy autentifikatsiya qilish qobiliyatiga ega bo'lishi kerak. Korxonalarga axborot texnologiyalari xavfsizligini samarali himoya qilish vositalarini ishlab chiqish uchun afsuski, yillar, bir qancha yuqori darajadagi kiberhujumlar va tegishli hukumat qonunlari talab qilindi. Bugungi keng tarqalgan avtomatlashtirish davrida parollardan foydalanish bir qancha kamchiliklarga ega. Ular davriy almashtirilishga moyil, chunki bu parollar administratorlar tomonidan bir vaqtda boshqa tizimlarga kirish uchun ham ishlatilishi mumkin.

ASOSIY QISM

Kiberxavfsizlik landshafti:

Dunyoning texnologik darajasi kundan-kunga oshib bormoqda. Tashkilotlar texnologiyalardan foydalanishni o'z faoliyatining ko'p jihatlariga integratsiya qilmoqdalar. Bu biznes rivoji uchun juda ko'p afzalliklarga ega bo'lishi mumkin, ammo bu texnologiyalarga ko'p miqdorda qaramlik biznesingizni kiber jinoyatchilarning bemalol harakatlanishi uchun sezilarli darajada zaif qilib beradi [10]. Yangi texnologiyalarni qabul qilgandan keyin tashkilot xavfsizligini ta'minlash uchun kompaniyalar kiberxavfsizlik choralarini qo'llashlari kerak [10]. Bu tashkilotga tegishli ilovalar, tarmoqlar va texnologiyalarni kiberhujumlardan himoya qilishning keng qamrovli usullarini ishlab chiqishni nazarda tutadi. Kiberxavfsizlik landshafti tashkilotni kripto-jacking, ma'lumotlar sizib chiqishi, data fishing, to'lov dasturi va Internet of Things (IoT) tahdidlaridan himoya qilish choralarini o'z ichiga olishi kerak. Tashkilotda kiberxavfsizlikni so'nggi darajada rivojlangan SI texnologiyalari bilan ta'minlash uchun kompaniyalar yuqori malakaga ega IT mutahassislari va Axborot xavfsizligi xodimlarini yollashlari talab qilinadi.

SI va Kiberxavfsizlikning o'zaro bog'liqliklari

Sun'iy intellekt kompyuter tizimlarida qaror qabul qilishni belgilovchi asosiy omil hisoblanadi. Masalan, kompyuter tizimdagi shubhali faoliyatni aniqlashi va tegishli ruxsat berilmaguncha kirishni rad etishi mumkin. Ushbu sun'iy intellekt usullari Machine Learning (ML) dasturidan foydalanadi, unda IT mutaxassislari vaqt o'tishi bilan to'plangan ma'lumotlarga asoslangan algoritmlarni tuzadilar [11]. Algoritm shunday tuzilishi kerakki, u haqiqiy kirishda firibgarlikni aniqlash va ajrata olishi kerak. ML texnologiyasi hujumlar va anormalliklarni bashorat qilish imkoniyatini beradi va shu nuqtayi nazardan tashkilot xavfsizligini oshiradi [11]. Mumkin bo'lgan tahdidlarni oldindan aniqlashning aniqligi va tezligi kompaniyalar uchun bebaho hisoblanadi. Sun'iy intellekt va ML texnologiyalari kompaniyalar uchun millionlab dollarga tushishi mumkin bo'lgan kiberhujumlarning oldini olishga

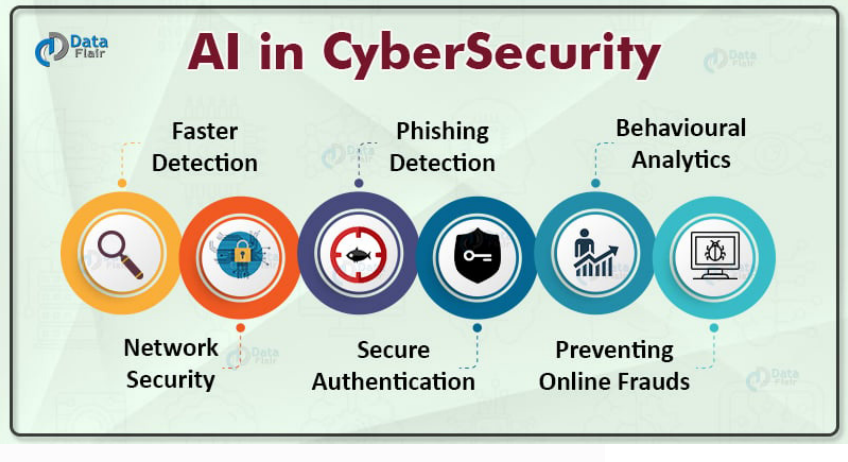
yordam beradi. Shunga qaramay, korxonalar xavfsizlik tizimlarini yangilashda davom etishlari kerak, chunki xakerlar texnologik taraqqiyotga mutanosib tarzda rivojlanmoqdalar.

SI Operatsiyalari

Sun'iy intellekt (AI) operatsiyalari tarmoqlardagi har qanday shubhali faoliyatni aniqlash va oldini olish uchun dasturlashtirilgan turli xil kompyuterlardan tashkil topgan tizimni o'z ichiga oladi [12]. Tizimlar inson aralashuvisiz xavflarni aniqlay oladigan shaklda dasturlashtirilgan bo'ladi. AI asosan mustaqil bo'lsa-da, kerak bo'lganda nazorat qilinadigan ko'rsatmalarni kiritish imkonini berishi kerak. Bu tashkilotga mumkin bo'lgan xavflarni tasniflash uchun muhimdir. Masalan, tizimga ransomware yoki turli viruslar kabi hujumlarni ularning xususiyatlariga qarab toifalarga ajratish buyruqi berilishi mumkin.

SI kiberxavfsizlikda

Kiberxavfsizlikka ta'sir ko'rsatayotgan yirik SI texnologik yutuqlari mavjud. Sun'iy intellekt (AI) endi oddiy atama emas; hozirda u turli sohalarda keng qo'llanilmoqda. Mijozlarni qo'llab-quvvatlash, sog'liqni saqlash va robototexnika - bu sun'iy intellekt taraqqiyotini tezlashtirgan ko'plab sohalardan faqat bir nechtasi [13]. Bundan tashqari, u kiberjinoyatchilikka qarshi davomli kurashga katta hissa qo'shmoqda. AI ning kiberxavfsizlikni yaxshilashga yordam beradigan bir necha usullari mavjud.



1-rasm. **Kiberxavfsizlik sohasida SI tizimlari**

AI ko'plab afzalliklarga ega va bir nechta sohalarda, jumladan kiberxavfsizlikda keng qo'llaniladi. Tez o'zgaruvchan kiberhujumlar va gadjetlarning tez ko'payishi bilan AI kiberjinoyatchilardan hushyor bo'lishga, tahdidlarni aniqlashni avtomatlashtirishga va standart dasturiy ta'minot va inson omili ishtirokida ishlatiladigan usullarga qaraganda samaraliroq javob berishga yordam beradi [14]. Quyida keberxavfsizlik sohasida SI tizimilardan foydalanishning bir qancha usullari keltirilgan:

Yangi tahdidlarni aniqlash:

AIdan kiberxavflar va potentsial zararli xatti-harakatlarni aniqlash uchun foydalanish mumkin. An'anaviy dasturiy ta'minot tizimlari har doim ham paydo bo'ladigan yangi viruslarning katta hajmini ushlab tura olmasligi sababli, bu sun'iy intellekt haqiqatan ham yordam berishi mumkin bo'lgan sohadir. Sun'iy intellekt algoritmlari zararli dasturlarni aniqlashi, dastur qoldirgan izlarni aniqlashi va hatto murakkab algoritmlar yordamida virus hujumining eng murakkab harakatlarini kompyuterga zarar etkazishdan oldin aniqlashi mumkin. Bundan tashqari, kiberjinoyatchilar ham zamon bilan o'zgarib bormoqda, shuning uchun ular orasida mashhur bo'lgan narsa doimiy ravishda o'zgarib turadi. Sun'iy intellektga asoslangan kiberxavfsizlik yechimlari nafaqat tizimlardan foydalanishda, balki tizimlarni nishonga olish uchun ishlatilishi mumkin bo'lgan narsaga asoslanib, asosiy ustuvor tanlovlarni yaxshiroq qilish uchun global va sanoatning yetakchi tahdidlari haqidagi eng yangi ma'lumotlarni taqdim etishi mumkin [14].

Buzilish xavfini bashorat qilish

Ushbu sun'iy intellekt echimlari tizimga kirishning turli darajalariga ega bo'lgan barcha ulanishlar, foydalanuvchilar va ilovalarning aniq va keng qamrovli hujjatlarini yaratishga yordam beradi. Bugungi kunda aktivlarni inventarizatsiya qilish va xavf-xatarga duchor bo'lishini hisobga olgan holda, sun'iy intellekt tizimlari kompaniyalar qanday va qayerda xavf ostida bo'lishini oldindan bilishlari mumkin, shunda ular resurslarni eng zaif hududlarga tayyorlashlari va taqsimlashlari mumkin. Sun'iy

intellektga asoslangan tahlildan olingan tavsiyali tushunchalar korporativ kiber barqarorlik va xavfsizlikni mustahkamlash uchun siyosat va tartiblarni ishlab chiqish va takomillashtirishga yordam beradi.

Tarmoqdagi so'nggi nuqta kompyuterlarini yaxshiroq himoya qilish

Masofadan ishlaydigan qurilmalar soni tez sur'atlar bilan o'sib bormoqda va AI ularning barchasini himoya qilishga yordam beradi. Albatta, antivirus va VPN yechimlari masofaviy viruslardan kiberhujumlarning oldini olishga yordam berishi mumkin, lekin ular ko'pincha imzolar asosida ishlaydi. Eng yangi xavf-xatarlardan xavfsiz qolish uchun imzo ta'riflari haqida xabardor bo'lish juda muhimdir. Antivirus dasturini yangilamaslik yoki dasturiy ta'minot provayderi tomonidan ma'lumot etishmasligi natijasida virus ta'riflari eskirgan bo'lsa, bu tashvish manbai bo'lishi mumkin. Natijada, agar zararli dastur hujumining yangi turi aniqlansa, imzo xavfsizligi undan himoyalana olmasligi mumkin [15].

Agar biror narsa bo'lsa, g'ayrioddiy ro'y bersa, AI professionalni ogohlantirishi yoki hatto ransomware hujumidan keyin tizimni xavfsiz holatga qaytarishi mumkin. Bu imzo o'zgarishlariga tayanish o'rniga proaktiv tahdidlarning oldini olishda yordam beradi [15].

Parol himoyasida SI algoritmlari

Parollar xavfsizlik taraflama har doim juda zaif nazorat ostidas bo'lgan soha desak mubo'aga bo'lmaydi. Ba'zida parollar bizning accountlarimiz va kiberjinoyatchilar o'rtasidagi yagona to'siq bo'lib qoladi. Ko'pchilik hollarda ko'pchiligimiz parollarimizga juda beparvo munosabatda bo'lamiz - ko'pincha hamma joyda bir xil paroldan foydalanamiz, yillar davomida bir xil parolga tayanamiz, va hokazo. Biometrik autentifikatsiya parollarning o'rnini bosuvchi vosita sifatida o'rganilgan bo'lsa-da, u noqulay va xakerlik hujumiga qarshi mumkin qadar zaifroqdir. Masalan, yuzni tanish tizimi yangi soch turmagi yoki shlyapa tufayli sizni aniqlay olmasa, foydalanish noqulay bo'lishi mumkin. Hujumchilar Facebook yoki Instagram kabi ijtimoiy media platformalaridagi profil rasmlaridan foydalanish orqali uni chetlab o'tishlari mumkin. Ishlab chiquvchilar AIdan biometrik autentifikatsiyani yaxshilash va ishonchli tizimga aylantirish uchun kamchiliklarini bartaraf etish uchun foydalanishni yo'lga qo'ydilar. Masalan, Apple kompaniyasi iPhone 11 va undan keying avlod smartfonlarida qo'llagan yuzni tanish texnologiyasidir. "Face ID" deb nomlangan tizim o'rnatilgan infraqizil sensorlar va neyron motorlar orqali foydalanuvchining yuz xususiyatlarini tahlil qilish orqali ishlaydi. Shaklni aniqlash orqali AI foydalanuvchi yuzining keng qamrovli tasvirini yaratadi. Apple kompaniyasining ta'kidlashicha, ushbu texnikadan foydalangan holda, AIni aldash va iPhone-ni boshqa yuzni aniqlash tizimi bilan ochish imkoniyati millionda birdir [16]. AI dasturiy ta'minoti dizayni turli yorug'lik holatlarida ham ishlashi mumkin va boshqa narsalar qatorida yangi soch turmagi, soqol o'sishi yoki shlyapa kiyish kabi o'zgarishlarga moslasha oladi.

Fishingni aniqlashda SI tizimlari

Fishing - bu kiberhujumning mashhur usuli bo'lib, unda kiberjinoyatchilar o'zlarining zararli dasturlarini fishing hujumi orqali tarqatishga harakat qilishadi. Fishing elektron pochta xabarlari juda keng tarqalgan; har 99 elektron pochtadan bittasi [16]. Yaxshiyamki, sun'iy intellekt (AI) fishing kiberhujumlarini aniqlash va oldini olishda katta rol o'ynash imkoniyatiga ega. Sun'iy intellekt 10 000 dan ortiq faol fishing saytlarini aniqlash va kuzatish, shuningdek, hodisalarga odamlardan ko'ra tezroq javob berish va tuzatishga qodir. Bundan tashqari, AI butun dunyo bo'ylab fishing tahdidlarini skanerlaydi va uning fishing harakatlari haqidagi bilimi geografik jihatdan cheklangan emas. AI soxta va haqiqiy veb-saytni tezda farqlash imkoniyatiga ega.

SI ning tarmoq xavfsizligi bilan bog'liq muammolarga tadbiqi

Tahdidlarning aqlli tizimlarga integratsiyasi aniqlash qobiliyatini yaxshilashga va hujumlar sonini kamaytirishga yordam beradi. Kiberxavfsizlikning ikkita muhim komponenti xavfsizlik siyosatini ishlab chiqish va muassasa tarmoq topologiyasini aniqlashdir [17,18]. Umuman olganda, ushbu vazifalarning har biri katta e'tibor talab qiladi. Biroq, biz sun'iy intellektdan ushbu protseduralarni tezlashtirish uchun foydalanishimiz mumkin, u tarmoq trafigini kuzatish va tushunish, shuningdek, ma'murlar va foydalanuvchilarga xavfsizlik qoidalarini taklif qilish orqali amalga oshiradi [18]. Bu nafaqat vaqtni, balki texnik o'sish va takomillashtirish sohalarida ishlatilishi mumkin bo'lgan katta miqdordagi ish va resurslarni ham tejaydi.

SI ning kiberxavfsizlik sohasidagi kamchiliklari

Yuqorida aytib o'tilganlar AIning kiberxavfsizlikni yaxshilash qobiliyatining faqat kichik bir qismini ifodalaydi. Biroq, bu sohada AIdan foydalanish sezilarli kamchiliklarga ega. AI tizimini yaratish va unga xizmat ko'rsatish uchun ko'proq mablag', ishchi kuchu va vaqt kerak bo'ladi. AI tizimlari katta miqdordagi ma'lumotlar va hodisalarsiz noto'g'ri noto'g'ri pozitivlarni taqdim etishi mumkin. Profissional hackerlar SIga ega bo'lishlari, uni o'zlarining maqsadlariga moslab yaratib olishlari mumkin. Asosiy tashvishlardan biri shundaki, kiberjinoyatchilar sun'iy intellektdan foydalangan holda juda katta miqyosda kiberoperatsiyalarni amalga oshirishlari mumkin [18]. Inson resurslarining etishmasligini to'ldirish va kiberxavfsizlik xarajatlarini kamaytirish uchun sun'iy intellektdan foydalanish ko'rib chiqilishi kerak bo'lgan yana bir muhim mavzudir. Bundan tashqari, sun'iy intellekt sohasidagi yutuqlar yangi turdagi kiber tahdidlarning paydo bo'lishiga yo'l ochishi mumkin. Sun'iy intellekt tizim zaifligidan insonga qaraganda tezroq va samaraliroq foydalanishi mumkin. Xakerlar AIdan jabrlanuvchi o'z tizimi yoki tarmog'iga putur etkazganini hech qachon sezmasligi mumkin bo'lgan hujumlarni tezda berkitish uchun foydalanishi mumkin.

Iqtisodiy foydalari

Sun'iy intellektning foydasini oldindan aytib bo'lmaydi, balki vaqt o'tishi bilan ortib borayotgan sur'atda aniqlanishi mumkin. 2030 yilga kelib, sun'iy intellektning iqtisodiyotga qo'shgan hissasi so'nggi 5 yildagiga qaraganda o'n yoki undan ko'proq baravar ko'payishi mumkin. Sun'iy intellektni joriy etish S-egri chizig'iga amal qilishi kutilmoqda, bu texnologiyalarni ishlab chiqish va qo'llash bilan bog'liq katta xarajatlar tufayli sust boshlanishi, keyin esa raqobatning uzoq muddatli ta'siri va ko'nikmalarni to'ldirishning yaxshilanishi tufayli tezlashishi mumkin. So'nggi bir necha yil davomida sun'iy intellekt (AI) texnologiyalari keng tarqalgan bo'lib, bizning ishlash, o'ynash va ulanish usullarini va dunyoning qolgan qismini o'zgartira oldi. IT va telekommunikatsiya sohasi, avtomobil sektori, tibbiyot, videoo'yinlar sanoati sun'iy intellektni joriy qilish bo'yicha eng etuk sanoat turlaridir. Turli sohalardagi 4500 dan ortiq siyosatchilarni o'rgangan yaqinda dunyo bo'ylab o'tkazilgan tadqiqotga ko'ra, yirik korxonalarning 45 foizi va kichik va o'rta korxonalarning 29 foizi sun'iy intellektni qabul qilganliklarini aytishgan. Xavfsizlik buzilishi yanada murakkablashsa-da, sun'iy intellekt (AI) kiberxavfsizlik biznesida muhimroq bo'ladi. Shunday qilib, global kiberxavfsizlik sanoati o'sha yilga kelib daromadni oshirishi kutilmoqda. Sun'iy intellektdan (AI) foydalanish xavf-xatarlardan xoli emas, chunki sun'iy intellektni qabul qilgan korxonalarning 60% dan ortig'i AI tomonidan yaratilgan kiberxavfsizlik tahdidlarini eng muhimi deb hisoblaydi [20]. Ko'pgina ekspertlarning fikricha, sun'iy intellekt (AI) va boshqa murakkab avtomatlashtirish turlari, masalan, robototexnika va sensorlar, umumiy maqsadli texnologiya (GPT) sifatida ko'rib chiqilishi mumkin, bu esa sezilarli innovatsiyalarni amalga oshirishga imkon beradi va natijada samaradorlikning oshishiga olib keladi.

XULOSA

Ushbu tadqiqotda sun'iy intellektning kiberxavfsizlik va kiberxavfsizlik tahdidlarini yumshatishga ta'siri baholandi. Tadqiqot natijalari shuni ko'rsatadiki, Kiberxavfsizlikda qo'llaniladigan SI texnikasi kuchli vositadir. SI ning o'rganish qobiliyati va oldingi ma'lumotlarga qarab tez xulosa chiqarish qobiliyati uning qanchalik darajada kuchli ekanini ifodalaydi. Sun'iy intellekt foydali bo'lsa-da, u zararli bo'lishi ham mumkin. Texnologiyani oqilona tanlash korxonalarga inqirozning oldini olishga imkon beradi. Sun'iy intellekt (AI) tezlik bilan tashkilotlarda axborot xavfsizligi sohasida qilinadigan ishlar samaradorligini oshirish uchun zarur vositaga aylanmoqda. Hech birimizga sir emaski, inson omili axborot tizimlarini bundan buyon korporativ darajadagi kiberhujumlardan yetarli darajada himoya qila olmaydi. Sun'iy intellekt xavfsizlik bo'yicha tashkilotning mudofaa qobiliyatini yaxshilash uchun foydalanishi mumkin bo'lgan juda zarur yechimni taklif qila olishi mumkin. Bundan tashqari, sun'iy intellekt xavflarni aniqlash, hodisaga javob berish yo'nalishi va zararli dasturlarning kiberhujumlarini ular sodir bo'lishidan oldin aniqlashda yordam berishi mumkin. Natijada, mumkin bo'lgan kamchiliklarga qaramay, sun'iy intellekt kiberxavfsizlikni rivojlantirishga yordam beradi va korxonalarga umumiy xavfsizlikni yanada mustahkamlashda yordam beradi.

FOYDALANILGAN ADABIYOTLAR RO'YHATI

1. D. Cole, "Artificial intelligence and personal identity", Synthese, vol. 88, no. 3, pp. 399-417, 1991. Available: 10.1007/bf00413555. [1]
2. M. Stefik, "Artificial intelligence applications for business management", Artificial Intelligence, vol. 28, no. 3, pp. 345-348, 1986. Available: 10.1016/0004-3702(86)90055-x. [2]
3. G. Babu, N. Anandakuma and D. Muralidhar, "Countermeasures Against DPA Attacks on FPGA Implementation of AES", Journal of Artificial Intelligence, vol. 5, no. 4, pp. 186-192, 2020. [3]
4. G. Qin, T. He and J. Chen, "Model of preventing URL attacks based on artificial immunity", Journal of Computer Applications, vol. 32, no. 5, pp. 1400-1403, 2019.
5. N. Lee, "Artificial Intelligence and Data Mining," Counterterrorism and Cybersecurity, pp. 323–341, 2021.
6. L. Shellberg, "A Cyber Chase in Cyber Space: How International Law Must Address the Threat of Cyber Attacks or Suffer the Consequences", SSRN Electronic Journal, 2022.
7. H. R. Nemati, Information security and ethics: concepts, methodologies, tools, and applications. Hershey Pa.: Information Science Reference, 2019.
8. T. Tagarev, "Intelligence, Crime and Cybersecurity", Information & Security: An International Journal, vol. 31, pp. 05-06, 2021.
9. R. Winkels, Eleventh International Conference on Artificial Intelligence and Law: proceedings: June 4-8, 2007, Stanford Law School, Stanford, California. Place of publication not identified: ACM, 2007.
10. D. Hutchison, M. Atiquzzaman, H.-H. Chen, T. Kanade, T.-hoon Kim, J. Kittler, J. M. Kleinberg, C. Lee, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. P. Rangan, J. H. Park, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M. Y. Vardi, G. Weikum, and S.-S. Yeo, Advances in Information Security and Assurance. Berlin, Heidelberg: Springer Berlin Heidelberg.
11. M. Zajko, "Canada's cyber security and the changing threat landscape", Critical Studies on Security, vol. 3, no. 2, pp. 147-161, 2019.
12. R. Winkels, Eleventh International Conference on Artificial Intelligence and Law: proceedings: June 4-8, 2007, Stanford Law School, Stanford, California. Place of publication not identified: ACM, 2007.
13. H. Bidgoli, Handbook of information security. Hoboken, NJ: John Wiley, 2006.
14. H. Zhuge, "Semantic linking through spaces for cyber-physical-socio intelligence: A methodology", Artificial Intelligence, vol. 175, no. 5-6, pp. 988-1019, 2021.
15. C. Blackwell and H. Zhu, Cyberpatterns: Unifying Design Patterns with Security and Attack Patterns, 2nd ed. Cham : Springer International Publishing, 2022.
16. A. R. Dengel, K. Berns, T. M. Breuel, F. Bomarius, and T. R. Roth-Berghofer, KI 2021: advances in artificial intelligence 41st Annual German Conference on AI, KI 2021, Kaiserslautern, Germany, September 23-26, 2021 ; proceedings. Berlin: Springer, 2021.