**NIGMATOV Hikmatulla**
*O‘zbekiston xalqaro islom akademiyasi Zamonaviy axborot-kommunikatsiya texnologiyalari kafedrasi professori, texnika fanlari doktori, professor*

**RAXMANOV Qurbon Sodikovich**
*O‘zbekiston xalqaro islom akademiyasi Zamonaviy axborot-kommunikatsiya texnologiyalari kafedrasi mudiri, texnika fanlari nomzodi, dotsent*

**XODJAYEVA Mavluda Sobirovna**
*O‘zbekiston xalqaro islom akademiyasi Zamonaviy axborot-kommunikatsiya texnologiyalari kafedrasi dotsenti, texnika fanlari nomzodi, dotsent*

# AXBOROTLARNI HIMOYALASHDA SUN’IY INTELLEKTDAN FOYDALANISH

# ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЗАЩИТЕ ИНФОРМАЦИИ

# USE OF ARTIFICIAL INTELLIGENCE IN INFORMATION PROTECTION

***Annotatsiya***. *Ushbu maqolada 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 qanday texnologiyalardan foydalanishligi hamda axborotlarni himoya qilishda inson tajribasini va tushunchasini saqlash juda muhim, chunki inson faktori, tezlik va tajribaga asoslangan vazifalarni bajarishda katta ahamiyatga egaligi to‘g‘risida ma’lumotlar berilgan.*

***Kalit so‘zlar:*** *kiberxavfsizlik, axborot xavfsizligi, sun’iy intellekt, raqamlashtirish, ruxsatsiz kirish, shaxsiy ma’lumotlar xavfsizligi, axborotlarni butunligini ta’minlash.*

***Аннотация***. *В данной статье представлен краткий анализ возможных способов использования искусственного интеллекта в сфере информационной безопасности. Для предотвращения несанкционированного доступа к информации, а также для снижения последствий нарушений информационной безопасности важно сохранять человеческий опыт и понимание того, какие технологии используются, а также защищать информацию, поскольку огромное значение имеет человеческий фактор, скорость и компетентность при выполнении задач на основе опыта, предоставленной информации.*

***Ключевые слова:*** *кибербезопасность, информационная безопасность, искусственный интеллект, цифровизация, несанкционированный доступ, безопасность персональных данных, целостность информации.*

***Annotation***. *This article provides a brief analysis of possible ways to use artificial intelligence in the field of information security. To prevent unauthorized access to information, as well as to reduce the consequences of information security breaches, it is important to maintain human experience and understanding of what technologies are used and to protect information, because the human factor, speed and expertise are of great importance in performing tasks based on experience given information.*

***Keywords:*** *cyber security, information security, artificial intelligence, digitization, unauthorized access, personal data security, information integrity.*

***Annotation***. *This article provides a brief analysis of possible ways to use artificial intelligence in the field of information security. To prevent unauthorized access to information, as well as to reduce the consequences of information security breaches, it is important to maintain human experience and understanding of what technologies are used and to protect information, because the human factor, speed and expertise are of great importance in performing tasks based on experience given information.*

***Keywords:*** *cyber security, information security, artificial intelligence, digitization, unauthorized access, personal data security, information integrity.*

## KIRISH

Bugungi kunda dunyo bo‘yicha rivojlanayotgan davlatlarda zamonaviy axborot-kommunikatsiya texnologiyalari asosida faoliyat olib borilmoqda. Raqamlashtirish jarayonlari iqtisodiyotning barcha jabhalarida qo‘llanishi natijasida katta moliyaviy yutuqlarga erishilmoqda.

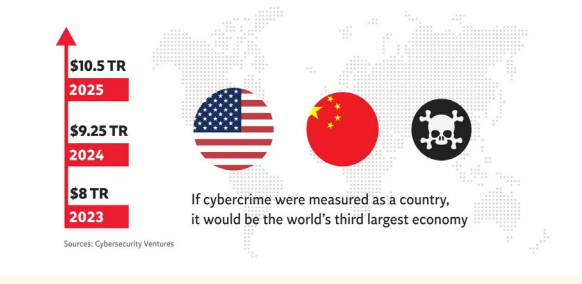
Har bir axborot o‘z qiymatiga ega bo‘lib, ularning bahosi olinayotgan, saqsalanayotgan, uzatilayotgan yoki qabul qilinayotgan axborotlarning butunligiga, o‘zgartirilmaganligiga, xatosiz berilganligiga va talab qilingan vaqtda yetkazib berilganligiga bog‘liq bo‘ladi. Bu


ISSN 2181-9572

shartlarning bajarilmaganligi axborotlardan foydalanuvchilarga juda katta ma'naviy, siyosiy, axloqiy va eng asosiysi iqtisodiy zarar keltirishi barchaga ma'lum.

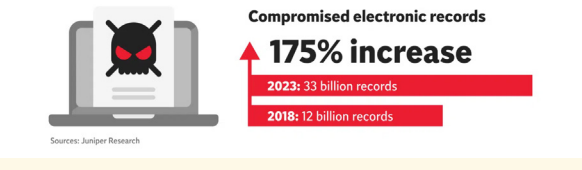
## ASOSIY QISM

Statistik ma'lumotlarga ko'ra, Cybersecurity Ventures bosh muharriri Stiv Morgan fikricha[1]: Agar kiberjinoyatchilikni bir mamlakat sifatida o'lchanganida, u dunyoda AQSh va Xitoydan keyin uchinchi yirik iqtisodiyot bo'lar edi.




1-rasm. Kiberjinoyatchilikni iqtisodiyotdagi o'rni.

Yana shuni alohida ta'kidlash kerakki, 2023 yilga 33 milliard elektron yozuv o'g'irlangan, bu esa 2021-yilga nisbatan 175% ga o'sgan[2].




**2-rasm. Elektron yozuvlarni o'g'irlanish statistikasi**

Demak, ko'rishimiz mumkinki, biror bir jarayonni avtomatlashtiruvchi tizim ishlab chiqishda ularni axborot xavfsizligiga alohida e'tibor qaratish lozim. Albatta, barcha korxonalar, tashkilotlar, vazirliklar, muassasalar, aktsiyadorlik kompaniyalar, assosatsiyalar, mas'uliyati cheklangan jamiyat va firmalar o'zlarining faoliyatida axborot tizimlaridan foydalanib kelmoqda, ulardan kerak paytda foydalanib kelinmoqda, lekin ushbu ma'lumotlarni himoyalash masalalari ko'p ham e'tibir berilmayapdi.

Axborot xavfsizligi tobora ko'proq joriy etilayotgan va foydalaniladigan axborot tizimlarini hisobga olgan holda 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. Bunda, albatta kiberxavfsizlik muhim rol o'ynaydi.

Kiberxavfsizlik - kibermakonning barcha tashkil etuvchilari (ya'ni texnik qurilmalar va foydalanuvchilar)ni har qanday tahdidlar va kutilmagan ta'sirlardan himoyalanganlik holati hisoblanadi [1].

Bugungi kunga kelib, kiberhujumlar soni tez va barqaror o'sishda davom etmoqda, hujumlarning o'zi tobora takomillashib bormoqda va hozirda aqlli uy qurilmalarini o'z ichiga olgan potentsial maqsadlar tobora ortib bormoqda va hujumlarning zarari tobora ko'payib bormoqda. 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 buzishdir. Antivirusga qarshi kurashning «klassik» vositalari endi bunday umumiy hujumlarni yengishga qodir emas. Bunda bizga sun'iy intellektga asoslangan yechimlar yordamga keladi.

Kiberxavfsizlik sohasida ilg'or texnologiyalarni joriy etish hujumlarni batafsil aniqlash va ularni kiberxavfsizlik bo'yicha mutaxassislarga qaraganda tezroq hal qilish imkonini beruish albatta vaqt talab etadi. Sun'iy intellekt bunday texnologiya sifatida harakat qilishi mumkin. Sun'iy intellekt (SI) - bu boshqa narsalar qatori tahdidlarni aniqlay oladigan va ularni bartaraf etish va oldini olish uchun avtomatik ravishda zarur choralarni ko'radigan texnologiya hisoblanadi. Sun'iy intellektga asoslangan vositalar turli xil kiberxavfsizlik ehtiyojlariga javob beradi [2-6].

**1. Biometrik autentifikatsiya.** Parollar buzilishi mumkin, bu foydalanuvchi, korxona yoki davlat organining muhim ma'lumotlarini buzadi. Bu yerda sun'iy intellektga asoslangan autentifikatsiya, barmoq izlari va kaftlarni skanerlashdan qat'iy nazar, ancha xavfsizroq va tizim ularni ishonchli skanerlashi mumkin.

Oxirgi vaqtda insonning fiziologik parametrlari va xarakteristikalarini, xulqining xususiyatlarini o'lchash orqali foydalanuvchini ishlonchli autentifikatsiyalashga imkon beruvchi biometrik autentifikatsiyalash keng tarqalmoqda.

[1] https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

[2] https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

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 koeffitsientini mutaxassislar quyidagicha aniqladilar [7]:

– 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%).

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

– xatolik inkorlao koeffitsiyenti FRR (false-reject rate);

– xatolik tasdiqlar koeffitsiyenti FAR (false-alarm rate).

Xatolik inkor tizim qonuniy foydalanuvchi shaxsini tasdiqlamaganda paydo bo'ladi (odatda FRR qiymati taxminan 100 dan birni tashkil etar ekan). Xatolik tasdiq tizim noqonuniy foydalanuvchi shaxsini tasdiqlaganida paydo bo'ladi (odatda FAP qiymati taxminan 10000 dan birni tashkil etadi). Bu ikkala koeffitsiyent bir - biri bilan bog'liq va xatolik inkor koeffitsiyentining har biriga ma'lum xatolik tasdiq koeffitsiyenti mos keladi.

Mukammal biometrik tizimda ikkala xatolikning parametlari nolga 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, ya'ni autentifikatsiyaning daktiloskopik tizimi hisoblanadi. Bunday tizimlar sodda va qulay, autentifikatsiyalashning yuqori ishonchliligiga ega. Bunday tizimlarning keng tarqalishiga asosiy sabab barmoq izlari bo'yicha katta ma'lumotlar ba'zasining mavjudligidir. Ya'ni hozirgi paytda barcha davlatlarda insonning shaxsiy hujjatlariga (pasportlarga) barmoq izlari kiritilganligidir.

Autentifikatsiyalashda skanerlangan barmoq izi ma'lumotlar (bilimlar) bazasidagi «pasportlar» bilan taqqoslanadi.

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, ular qat'iy xavfsizlik rejimiga va shiddatli trafikka ega bo'lgan hisoblash muhiti uchun qulay hisoblanadi. Ularning aniqligi yuqori va inkor koeffitsiyenti ya'ni inkor etilgan qonuniy foydalanuvchilar foizi kichik bo'ladi.

Bunday tizimlar ko'p ishlatiladi, chunki aksariyat zamonaviy kompyuterlar video va audeo vositalariga ega. Bu sinf tizimlari telekommunikatsiya tarmoqlarida masofadagi foydalanuvchi sub'yektni identifikatsiyalash uchun ishlatiladi. 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 xususiy 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 izohlasa, 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.


ISSN 2181-9572

**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 tasvirni aniqlash orqali tahdidni osongina aniqlay oladigan, SI tomonidan boshqariladigan tizimlarni joriy qilmoqda. SI mashinali o'qitish 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**. Agar tizim tahdidlarga qarshi kurasha olmasa va tizimga ozgina zarar yetkazmasdan 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. Bu yerda 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 SIdan 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, SI odamlar tomonidan o'qitiladi va boshqariladi hamda ba'zi joylarda inson muhandislariga bo'lgan ehtiyoj zarur, chunki ular mashinalar aniqlay olmaydigan chiziqlardan tashqariga chiqishga va taxmin qilingan hujumning haqiqiyligini tasdiqlashga qodir hisoblanadilar.

SI haqiqatan ham xavfsizlik darajasini sezilarli darajada oshirishi mumkinmi? SI va Machine Learning axborot xavfsizligi sohasida muhim texnologiyaga aylandi, chunki ular millionlab hodisalarni tezda tahlil qilish va «nol kunlik zaifliklar» dan foydalanadigan zararli dasturlardan tortib, fishing hujumiga yoki zararli kodni yuklashga olib kelishi mumkin bo'lgan xavfli xatti – harakatlarni aniqlashgacha bo'lgan turli xil tahdidlarni aniqlashga qodir. SI modellari hozirda hujumlarning yangi turlarini taniy olish uchun juda katta miqdordagi haqiqiy ma'lumotlar va simulyatsiyalardan o'rganadilar.

SI iterativ va dinamik tizimdir. 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). 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 jarayondir.

Bugungi kunda SI **uchta** rivojlanish darajasiga ega [8]:

**1. Yordamchi razvedka** - bugungi kunda keng tarqalgan, inson qarorlarini yaxshilaydi va optimallashtiradi, ishni tezroq va yaxshiroq bajarishga yordam beradi.

**2. Kengaytirilgan razvedka** - yuqorida aytilganlarning barchasiga qo'shimcha ravishda, muayyan sharoitlar uchun eng yaxshi yechimlarni topishga qodir, odamga o'zi bajara olmaydigan muammolarni hal qilishga yordam beradi.

**3. Avtonom razvedka** - kelajak uchun ishlab chiqilgan, mashinalar tomonidan mustaqil qaror qabul qilishni o'z ichiga oladi. Bunga o'ziyurar transport vositalari misol bo'la oladi.

SI ma’lum darajada inson aql-idrokiga ega: mavzu sohasi bo‘yicha bilimlar zaxirasi, yangi bilimlarni olish mexanizmlari va ushbu bilimlardan foydalanish mexanizmlaridan tashkil topgan. Machine Learning, ekspert tizimlari, neyron tarmoqlari — bularning barchasi zamonaviy SI texnologiyalarida qo‘llanilgan. Machine Learning kompyuter tizimlariga aniq dasturlashtirilgan emas, balki ma’lumotlardan foydalangan holda “o‘rganish” (masalan, unumdorlikni asta-sekin oshirish) imkoniyatini berish uchun statistik usullardan foydalanadi.

**Ekspert tizimlari** - bu ixtisoslashgan sohalardagi muammolarni hal qilish uchun mo‘ljallangan dasturlar. Inson mutaxassislarining fikrlashiga taqlid qilib, 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 o‘rganish imkonini beruvchi dasturlash modelidan foydalanadi. Neyron tarmog‘ida har bir tugun o‘z kirishiga bajarilgan operatsiyaga nisbatan qanchalik to‘g‘ri yoki noto‘g‘ri ekanligini ifodalovchi qiymat beradi. Keyin yakuniy natija bunday qiymatlarning yig‘indisi bilan aniqlanadi.

Bugungi kunda doimiy ravishda rivojlanib borayotgan kiberhujumlarni o‘rganish 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 vektorlari sonini ko‘pligi;
– malakali xavfsizlik bo‘yicha mutaxassislarning tanqisligi va boshqalar.

O‘z-o‘zini o‘rganadigan SIga asoslangan kiberxavfsizlikni boshqarish tizimi ushbu muammolarning ko‘pini hal qilishga qodir. Ushbu tizimni barcha axborot tizimlaridan ma’lumotlarni uzluksiz va mustaqil ravishda to‘plashni to‘g‘ri o‘rgatish uchun texnologiyalar mavjud, keyin bu ma’lumotlar tahlil qilinadi va hujumga tegishli millionlab va milliardlab signallar o‘rtasidagi tasvirlarning o‘zaro bog‘liqligini amalga oshirish uchun ishlatiladi. Natijada, axborot xavfsizligining turli toifalarida bajarishga olib keladi:

**Yangi tahdidlarni aniqlash** - kiberhujumlarga javob berish vaqtiga ta’sir qiluvchi omil hisoblanadi. Javob berishning kechikishi, hatto ma’lum turdagi tahdidlar bilan ham sodir bo‘ladi. Hujumlarning yangi turlari, xatti-harakatlar va vositalar mutaxassislarni chalkashtirib yuborishi mumkin, natijada ular yanada sekinroq javob beriadi. Bularni o‘rganishga asoslangan 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 muhim. SI yaratilgan dasturingizning qayerda kuchli tomonlari borligini va kamchiliklari qayerda ekanligini ko‘rsatib beradi.

**Buzilish xavfini bashorat qilish** - SIga 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

SI zamonaviy kiberxavfsizlikning ajralmas qismiga aylanib bormoqda. Texnologiyaklarning rivojlanishi bilan SI tahdidlarni aniqlash, kiberhujumlardan himoya qilish va qaror qabul qilishda keng qo‘llanila boshlandi. Kiberxavfsizlikda SIdan 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.

Kiberxavfsizlikda SIdan foydalanishning yana bir muhim jihati uning tajribadan o‘rganish qobiliyatidir. SI algoritmlarini yaxshilash va kelajakda tahdidlarni aniqroq aniqlashni ta’minlash uchun oldingi kiberhujumlar ma’lumotlaridan foydalanishi mumkin. 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 SIdan foydalanishlari mumkin.


ISSN 2181-9572

Bundan tashqari, xavfsizlik qarorlarini qabul qilish uchun SIdan foydalanish bilan bog‘liq axloqiy savollar paydo bo‘lishi mumkin. Umuman olganda, SI kiberxavfsizlikda muhim rol o‘ynaydi va hozirda kiber tahdidlarga qarshi kurashish uchun zarur vosita bo‘lib hisoblanadi. Biroq, kiberxavfsizlikda SIdan 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 quyidagilarni hisobga olish kerak.

**Birinchidan,** SI ma’lumotlari va algoritmlarini kiberhujumlar va xakerlardan himoya qilish. Xakerlar SIni tizimga kiritish va himoya tizimlarini chetlab o‘tish va uning ishlashini o‘zgartirish uchun zararli algoritmlardan foydalanishlari mumkin. Shuning uchun, SIga asoslangan tizimlar uchun himoya choralarini kuchaytirish va zaifliklarni muntazam tekshirib turish zarur.

**Ikkinchidan**, SIni 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 SI bo‘yicha muntazam treninglar o‘tkazib turish kerak.

**Uchinchidan,** kiberxavfsizlikda SIdan foydalanish bilan bog‘liq axloqiy va huquqiy masalalarni hisobga olish kerak. Masalan, SIga asoslangan qarorlar qabul qilish inson shaxsiy huquqlarini buzilishiga olib kelishi mumkin. Shuning uchun, kiberxavfsizlikda SIdan foydalanishni tartibga soluvchi axloqiy va huquqiy standartlarni ishlab chiqish kerak.

**Va nihoyat,** kiberxavfsizlikda SIdan 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, SIni odamga yordam beradigan va uning o‘rnini bosmaydigan vosita sifatida ishlatish kerak.

SI 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 yechimlarini yaratish imkoniyatini beradi.

Axborotlar himoyalashda SI foydalanish, tarmoq himoyalashini yangilash, xavfsizlikni oshirish va xavfsizlik hodisalariga tez javob berishda yordam beradi. Shuningdek, axborotlarni himoya qilishda inson tajribasini va tushunchasini saqlash juda muhim, chunki inson faktori, tezlik va tajribaga asoslangan vazifalarni bajarishda katta ahamiyatga ega.

Umuman olganda, kiberxavfsizlikda SI dan foydalanish kibertahdidlarga qarshi kurashishda muhim va samarali vosita hisoblanadi. Biroq, SIdan foydalanishning xatarlari va kamchiliklarini hisobga olish va undan foydalanish xavfsizligini ta’minlash choralarini ko‘rish lozim.

## FOYDALANGAN ADABIYOTLAR RO‘YXATI


1. Корнеев В.В., Гарев А.Ф. и др. Базы данных. Интеллектуальная обработка информации. – М.: Нолидж, 2000. – 352 с.
2. Chipiga A. F. Avtomatlashtirilgan tizimlarning axborot xavfsizligi. – M.: Helios ARV, 2010. – 336 c.
3. Nigmatov H., Tursunbayev B.X. Zamonaviy axborot-kommunikatsiya texnologiyalari asosida intellektual tizimlar yaratish. O‘quv qo‘llanma. – Toshkent: Fan va texnologiyalar, 2020. – 264 b.
4. Нигматов Х., Умаров У.А., Турсунбаев Т.Б. A New Methodology for Evaluating the Efficiency of Complex Machine Mechanisms. International scientific and technical conference // Digital technologies: problems and solutions of practical implementation in the spheres. April 27-28, 2023. – P. 381-386.
5. Нигматов Х. Применение интеллектуальных систем для мониторинга работы вычислительных комплексов // Zamonaviy informatikaning dolzarb muammolari: o‘tmish tajribasi va istiqbollari: Respublika ilmiy-amaliy konferensiya. Toshkent, 29.05.2023.
6. Нигматов Х., Турсунбаев Т.Б. Анализ различных интеллектуальных систем мониторинга за работой вычислительных комплексов // “Axborot xavfsizligi sohasida raqamlashtirish muammolari va istiqbollari”. Respublika ilmiy-amaliy anjumani materiallari to’plami. Toshkent, 2022-yil 20-may.
7. Маркофф Д. Homo Roboticus? Люди и машины в поисках взаимопонимания / Джон Маркофф ; Пер. с англ. — М.: Альпина нон-фикшн, 2016. — 406 с.
8. Казанцев Т. Chat GPT и Революция Искусственного Интеллекта. 2022. – 141 с.
9. https://cybersecurityventures.com - Cybercrime Magazine portali.