O‘ZBEKISTONDA AXBOROT HAVFSIZLIGINI MA’NAVIY VA HUQUQIY ASOSLARI

Shamsiddinov G‘iyosjon Husniddin o‘g‘li
Shahrisabz davlat pedagogika instituti “Informatika va uni o‘qitish metodikasi” kafedrasi o‘qituvchisi
Raxmatova Gulandom Baxrom qizi
Shahrisabz davlat pedagogik instituti “Matematika va informatika” yo‘nalishi 1-bosqich talabasi
https://doi.org/10.5281/zenodo.10974243

Annotatsiya: Davlatning axborot xavfsizligini ta’minlash muammosi milliy xavfsizlikni ta’minlashning asosiy va ajralmas qismi bo‘lib, axborot himoyasi esa davlatning birlamchi prioritet masalalariga aylanmoqda. Hozirgi kunda xavfsizlikning bir qancha yo‘nalishlarini qayd etish mumkin. Axborotning muhimlik darajasi qadim zamonlardan ma’lum. Shuning uchun ham qadimda axborotni himoyalash uchun turli xil usullar qo‘llanilgan. Zamonaviy axborot-kommunikatsiyalar texnologiyalarining yutuqlari himoya uslublarining bir qator zaruriy instrumental vositalarini yaratish imkonini berdi. Axborotni himoyalovchi instrumental vositalar deganda dasturlash, dasturiy-apparatli va apparatli vositalar tushuniladi.

Tayanch so‘zlar: Axborot, axborot xavfsizligi, maxfiylik, yaxlitlik, autentifikatsiya, axborotning hayotiy davri, axborotni himoyalashning dasturiy-matematik elementi.

Аннотация: Проблема обеспечения информационной безопасности государства является основной и неотъемлемой частью обеспечения национальной безопасности, а защита информации становится главным приоритетом государства. В настоящее время можно отметить несколько направлений безопасности. Важность информации известна с давних времен. Именно поэтому в древности для защиты информации использовались разные методы. Развитие современных информационно-коммуникационных технологий позволило создать ряд необходимых инструментальных средств защиты. Инструментальные средства защиты информации – это программные, программные и аппаратные средства.

Ключевые слова: Информация, информационная безопасность, конфиденциальность, целостность, аутентификация, жизненный цикл информации, программно-математический элемент защиты информации.

Annotation: The problem of ensuring the state's information security is the main and integral part of ensuring national security, and information protection is becoming the primary priority of the state. Currently, several

directions of security can be noted. The importance of information has been known since ancient times. That is why different methods were used to protect information in ancient times. Advances in modern information and communication technologies have made it possible to create a number of necessary instrumental means of protection. Instrumental means of information protection means programming, software and hardware.

Key words: Information, information security, confidentiality, integrity, authentication, life cycle of information, software-mathematical element of information protection.

Mamlakatimiz milliy iqtisodining hech bir tarmog‘i samarali va mo‘tadil tashkil qilingan axborot infratuzilmasisiz faoliyat ko‘rsatishi mumkin emas. Hozirgi kunda milliy axborot resurslari har bir davlatning iqtisodiy va harbiy salohiyatini tashkil qiluvchi omillaridan biri bo‘lib xizmat qilmoqda. Ushbu resursdan samarali foydalanish mamlakat xavfsizligini va demokratik axborotlashgan jamiyatni muvaffaqiyatli shakllantirishni ta'minlaydi. Bunday jamiyatda axborot almashuvi tezligi yuksaladi, axborotni yig‘ish, saqlash, qayta ishlash va ulardan foydalanish bo‘yicha ilg‘or axborot-kommunikatsiyalarni qo‘llash kengayadi. Turli xildagi axborot xududiy joylashishidan qatiy nazar bizning kundalik hayotimizga internet xalqaro kompyuter tarmog‘i orqali kirib keldi. Axborotlashgan jamiyat ushbu kompyuter tarmog‘i orqali tezlik bilan shakllanib bormoqda. Axborot dunyosiga sayohat qilishda davlat chegaralari degan tushuncha yo‘qolib bormoqda. Jahon kompyuter tarmog‘i davlat boshqaruvini tubdan o‘zgartirmoqda, ya'ni davlat axborotning tarqalishi mexanizmini boshqara olmay qolmoqda. Shuning uchun ham mavjud axborotga noqonuniy kirish, ulardan foyddlanish va yo‘qotish kabi muammolar dolzarb bo‘lib qoldi. Bularning bari shaxs, jamiyat va davlatning axborot xavfsizligi darajasining pasayishiga olib kelmoqda.

Davlatning axborot xavfsizligini ta’minlash muammosi milliy xavfsizlikni ta’minlashning asosiy va ajralmas qismi bo‘lib, axborot himoyasi esa davlatning birlamchi prioritet masalalariga aylanmoqda. Hozirgi kunda xavfsizlikning bir qancha yo‘nalishlarini qayd etish mumkin. Axborotning muhimlik darajasi qadim zamonlardan ma’lum. Shuning uchun ham qadimda axborotni himoyalash uchun turli xil usullar qo‘llanilgan. Ulardan biri - sirli yozuvdir. Undagi xabarni xabar yuborilgan manzil egasidan boshqa shaxs o‘qiy olmagan. Asrlar davomida bu san’at-sirli yozuv jamiyatning yuqori tabaqalari, davlatning elchixona rezidentsiyalari va razvedka missiyalaridan tashqariga chiqmagan. Faqat bir necha o‘n yil oldin hamma narsa tubdan o‘zgardi, ya'ni axborot o‘z

qiymatiga ega bo‘ldi va keng tarqaladigan mahsulotga aylandi. Uni endilikda ishlab chiqaradilar, saqlaydilar, uzatishadi, sotadilar va sotib oladilar. Bulardan tashqari uni o‘g‘irlaydilar, buzib talqin etadilar va soxtalashtiradilar. Shunday qilib, axborotni himoyalash zaruriyati tug‘iladi. Axborotni qayta ishlash sanoatining paydo bo‘lishi axborotni himoyalash sanoatining paydo bo‘lishiga olib keladi. Avtomatlashtirilgan axborot tizimlarida axborot o‘zining hayotiy davriga ega bo‘ladi. Bu davr uni yaratish, undan foydalanish va kerak bo‘lmaganda yo‘qotishdan iboratdir . Axborot hayotiy davrining har bir bosqichida ularning himoyalanganlik darajasi turlicha baholanadi.

Axborotning hayotiy davri maxfiy va qimmatbaho axborotga ruxsatsiz kirishdan himoyalash eng muhim vazifalardan biri sanaladi. Kompyuter egalari va foydalanuvchilarning mulkiy huquqlarini himoyalash-bu ishlab chiqarilayotgan axborotni jiddiy iqtisodiy va boshqa moddiy hamda nomoddiy zararlar keltirishi mumkin bo‘lgan turli kirishlar va o‘g‘irlashlardan himoyalashdir. Axborot xavfsizligi deb ma'lumotlarni yo‘qotish va o‘zgartirishga yunaltirilgan tabiiy yoki sun'iy xossali tasodifiy va qasddan ta'sirlardan har qanday tashuvchilarda axborotning himoyalanganligiga aytiladi.

Ilgarigi xavf faqatgina konfidentsial (maxfiy) xabarlar va hujjatlarni o‘g‘irlash yoki nusxa olishdan iborat bo‘lsa, hozirgi paytdagi xavf esa kompyuter ma’lumotlari to‘plami, elektron ma'lumotlar, elektron massivlardan ularning egasidan ruxsat olmasdan foydalanishdir.Bulardan tashqari, bu harakatlardan moddiy foyda olishga intilish ham rivojlandi.

Axborotning himoyasi deb boshqarish va ishlab chiqarish faoliyatining axborot xavfsizligini ta’minlovchi va tashkilot axborot zaxiralarining yaxlitliligi, ishonchliligi, foydalanish osonligi va maxfiyligini ta’minlovchi qatiy reglamentlangan dinamik texnologik jarayonga aytiladi.

Axborotning egasiga, foydalanuvchisiga va boshqa shaxsga zarar yetkazmoqchi bo‘lgan nohuquqiy muomaladan har qanday hujjatlashtirilgan, ya'ni identifikatsiya qilish imkonini beruvchi rekvizitlari qo‘yilgan holda moddiy jismda qayd etilgan axborot himoyalanishi kerak.

Axborot xavfsizligi nuqtai nazaridan axborotni quyidagicha turkumlash mumkin:

•**maxfiylik**-aniq bir axborotga faqat tegishli shaxslar doirasigina kirishi mumkinligi, ya'ni foydalanilishi qonuniy xujjatlarga muvofiq cheklab qo‘yilib, hujjatlashtirilganligi kafolati. Bu bandning buzilishi o‘g‘irlik yoki axborotni oshkor qilish, deyiladi;

•**konfidentsiallik**-ishonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;

•**yaxlitlik**-axborot boshlang‘ich ko‘rinishda ekanligi, ya'ni uni saqlash va uzatishda ruxsat etilmagan o‘zgarishlar qilinmaganligi kafolati. Bu bandning buzilishi axborotni soxtalashtirish deyiladi;

•**autentifikatsiya**-axborot zaxirasi egasi deb e'lon qilingan shaxs haqiqatan ham axborotning egasi ekanligiga beriladigan kafolat. Bu bandning buzilishi xabar muallnfini soxtalashtirish deyiladi;

•**apellyatsiya qilishlik**-yetarlicha murakkab kategoriya, lekin elektron biznesda keng ko‘llaniladi. Kerak bo‘lganda xabarning muallifi kimligini isbotlash mumkinligi kafolati.

Yuqoridagidek, axborot tizimiga nisbatan quyidagacha tasnifni keltirish mumkin:

Ishonchlilik-tizim me’yoriy va g‘ayri tabiiy hollarda rejalashtiriganidek o‘zini tutishlik kafolati;

aniqlilik- hamma buyruqlarni aniq va to‘liq bajarish kafolati;

tizimga kirishni nazorat qilish-turli shaxs guruhlari axborot manbalariga har xil kirishga egaligi va bunday kirishga cheklashlar doim bajarilishlik kafolati; **nazorat qilinishi**-istalgan paytda dastur majmuasining xohlagan qismini to‘liq tekshirish mumkinligi kafolati;

identifikatsiyalashni nazorat qilish-hozir tizimga ulangan mijoz aniq o‘zini kim deb atagan bo‘lsa, aniq o‘sha ekanligining kafolati;

qasddan buzilishlarga to‘sqinlik-oldindan kelishilgan me’yorlar chegarasida qasddan xato kiritilgan ma'lumotlarga nisbatan tizimning oldindan kelishilgan holda o‘zini tutishi.

Axborotni himoyalashning maqsadlari quyidagilardan iborat:

- Axborotning kelishuvsiz chiqib ketishi, o‘g‘irlanishi, yo‘qotilishi, o‘zgartirilishi, soxtalashtirilishlarning oldini olish;
- shaxs, jamiyat, davlat xavfsizliligiga bo‘lgan xavf-xatarning oldini olish;
- axborotni yo‘q qilish, o‘zgartirish, soxtalashtirish, nusxa ko‘chirish, to‘siqlash bo‘yicha ruxsat etilmagan harakatlarning oldini olish;
- xujjatlashtirilgan axborotning miqdori sifatida huquqiy tartibini ta'minlovchi, axborot zaxirasi va axborot tizimiga har qanday noqonuniy aralashuvlarning ko‘rinishlarining oldini olish;
- axborot tizimida mavjud bo‘lgan shaxsiy ma'lumotlarning shaxsiy maxfiyligini va konfidentsialligini saqlovchi fuqarolarning konstitutsion xuquqlarini himoyalash;
- davlat sirini, qonunchilikka mos hujjatlashtirilgan axborotning konfidentsialligini saqlash;

- axborot tizimlari, texnologiyalari va ularni ta'minlovchi vositalarni yaratish, ishlab chiqish va qo‘llashda sub'ektlarning huquqlarini ta'minlash.

Ilmiy va amaliy tekshirishlar natijalarini umumlashtirish natijasida axborotga nisbatan xavf-xatarlarni quyidagicha tasniflash mumkin.

Xavfsizlik siyosatining eng asosiy vazifalaridan biri himoya tizimida potentsial xavfli joylarni qidirib topish va ularni bartaraf etish hisoblanadi.

Tekshirishlar shuni ko‘rsatadiki, tarmoqdagi eng katta xavflar - bu ruxsatsiz kirishga mo‘ljallangan maxsus dasturlar, kompyuter viruslari va dasturning ichiga joylashtirilgan maxsus kodlar bo‘lib, ular kompyuter tarmoqlarining barcha ob'ektlari uchun katta xavf tug‘diradi.

Zamonaviy axborot-kommunikatsiyalar texnologiyalarining yutuqlari himoya uslublarining bir qator zaruriy instrumental vositalarini yaratish imkonini berdi. Axborotni himoyalovchi instrumental vositalar deganda dasturlash, dasturiy-apparatli va apparatli vositalar tushuniladi. Ularning funktsional to‘ldirilishi xavfsizlik xizmatlari oldiga qo‘yilgan axborotlarni himoyalash masalalarini yechishda samaralidir. Hozirgi kunda tarmoq xavfsizligini nazorat qilish texnik vositalarining juda keng spektri ishlab chiqarilgan.

Axborotni himoyalash tizimlari Axborot-kommunikatsiya texnologiyalarining ommaviy ravishda qog‘ozsiz avtomatlashtirilgan asosda boshqarilishi sababli axborot xavfsizligini ta'minlash murakkablashib va muhimlashib bormoqda. Shuning uchun ham avtomatlashtirilgan axborot tizimlarida axborotni himoyalashning yangi zamonaviy texnologiyasi paydo bo‘lmoqda, DataQuest kompaniyasining ma'lumotiga ko‘ra, 1996-2000 yillarda axborot himoyasi vositalarining sotuvdagi hajmi 13 mlrd. AQSh dollariga teng bo‘lgan.

Axborotning zaif tomonlarini kamaytiruvchi va axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yuqolishiga to‘sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul va choralarning kompleksi - axborotni himoyalash tizimi deyiladi.

Axborot egalari hamda vakolatli davlat organlari shaxsan axborotning qimmatliligi, uning yo‘qotilishidan keladigan zarar va himoyalash mexanizmining narxidan kelib chiqqan holda axborotni himoyalashning zaruriy darajasi hamda tizimning turini, himoyalash usullar va vositalarini aniqlashlari zarur. Axborotning qimmatliligi va talab qilinadigan himoyaning ishonchliligi bir-biri bilan bevosita bog‘liq.

Himoyalash tizimi uzluksiz, rejali, markazlashtirilgan, maqsadli, aniq, ishonchli, kompleksli, oson mukammallashtiriladigan va ko‘rinishi tez o‘zgartiriladigan bo‘lishi kerak. U odatda barcha ekstremal sharoitlarda samarali bo‘lishi zarur.

Axborot hajmi kichik bo‘lgan tashkilotlarda axborotni himoyalashda oddiy usullarni qo‘llash maqsadga muvofiq va samaralidir. Masalan, o‘qiladigan qimmatbaho qog‘ozlarni va elektron hujjatlarni alohida guruhlarga ajratish va niqoblash, ushbu hujjatlar bilan ishlaydigan xodimni tayinlash va o‘rgatish, binoni qo‘riqlashni tashkil etish, xizmatchilarga qimmatli axborotni tarqatmaslik majburiyatini yuklash, tashqaridan keluvchilar ustidan nazorat qilish, kompyuterni himoyalashning eng oddiy usullarini qo‘llash va hokazo. Odatda, himoyalashning eng oddiy usullarini qo‘llash sezilarli samara beradi.

Murakkab tarkibli, ko‘p sonli avtomatlashtirilgan axborot tizimi va axborot hajmi katta bo‘lgan tashkilotdarda axborotni himoyalash uchun himoyalashning majmuali tizimi tashkil qilinadi. Lekin ushbu usul hamda himoyalashning oddiy usullari xizmatchilarning ishiga haddan tashqari xalaqit bermasligi kerak.

Himoya tizimining komplekslilig‌iga unda huquqiy, tashkiliy, muhandis-texnik va dasturiy-matematik elementlarning mavjudligi bilan erishiladi. Elementlar nisbati va ularning mazmuni tashkilotlarning axborotni himoyalash tizimining o‘ziga xosligini va uning takrorlanmasligini hamda buzish qiyinligini ta'minlaydi. Aniq tizimni ko‘p turli elementlardan iborat, deb tasavvur qilish mumkin. Tizim elementlarining mazmuni nafaqat uning o‘ziga xosligini, balki axborotning qimmatliligini va tizimning qiymatini hisobga olgan holda belgilangan himoya darajasini aniqlaydi.

Axborotni xuquqiy himoyalash elementi himoyalash choralarining haqli ekanligi ma'nosida tashkilot va davlatlarning o‘zaro munosabatlarini yuridik mustahkamlash hamda personalning tashkilot qimmatli axborotini himoyalash tartibiga rioya qilishi va ushbu tartibning buzilishida javobgarligi tasavvur qilinadi.

Himoyalash texnologiyasi personalni tashkilotning qimmatli axborotini himoyalash qoidalariga rioya kilishga undovchi boshqarish va cheklash xarakteriga ega bo‘lgan chora-tadbirlarni o‘z ichiga oladi.

Tashkiliy himoyalash elementi boshqa barcha elementlarni yagona tizimga bog‘lovchi omil bo‘lib hisoblanadi. Ko‘pchilik mutaxassislarning fikricha, axborotni himoyalash tizimlari tarkibida tashkiliy himoyalash 50-60 % ni tashkil qiladi. Bu hol ko‘p omillarga bog‘liq, jumladan, axborotni tashkiliy himoyalashning asosiy tomoni amalda himoyalashning printsipi va usullarini bajaruvchi personalni tanlash, joylashtirish va o‘rgatish hisoblanadiAxborotni himoyalashning tashkiliy chora-tadbirlari tashkilot xavfsizligi xizmatining me'yoriy uslubiy hujjatlarida o‘z aksini topadi. Shu munosabat bilan ko‘p

hollarla yuqorida ko‘rilgan tizim elementlarining yagona nomi - axborotni tashkiliy-huquqiy himoyalash elementini ishlatadilar.

Axborotni texnik himoyalash elementi-texnik vositalar kompleksi yordamida hudud, bino va qurilmalarni qo‘riqlashni tashkil qilish hamda texnik tekshirish vositalariga qarshi sust va faol kurash uchun mo‘ljallangan. Texnik himoyalash vositalarining narxi baland bo‘lsada, axborot tizimini himoyalashda bu element muxim ahamiyatga ega.

Axborotni himoyalashning dasturiy-matematik elementi kompyuter, lokal tarmoq va turli axborot tizimlarida qayta ishlanadigan va saqlanadigan qimmatli axborotni himoyalash uchun mo‘ljallangan.

Kompyuter tizimi (tarmog‘i)ga ziyon yetkazishi mumkin bo‘lgan sharoit, harakat va jarayonlar kompyuter tizimi (tarmog‘i) uchun xavf-xatarlar, deb hisoblanadi.

Avtomatlashtarilgan axborot tizimlariga tasodifiy ta'sir ko‘rsatish sabablari tarkibiga quyidagilar kiradi Avtomatlashtirilgan axborot tizimlariga tasodifiy ta’sir ko‘rsatish sabablari Ma’lumki, kompyuter tizim (tarmog‘)ining asosiy komponentlari-texnik vositalar, dasturiy-matematik ta’minot va ma’lumotlardir. Nazariy tomondan bu komponentlarga nisbatan to‘rt turdagi xavflar mavjud, ya’ni uzilish, tutib qolish, o‘zgartirish va soxtalahtirish.

Uzilish - tashqi harakatlar (ishlar, jarayonlar)ni bajarish uchun hozirgi ishlarni vaqtincha markaziy protsessor qurilmasi yordamida to‘xtatish, ularni bajargandan so‘ng protsessor oldingi holatga qaytadi va to‘xtatib qo‘yilgan ishni davom ettiradi. Har bir uzilish tartib raqamiga ega, unga asosan markaziy protsessor qurilmasi qayta ishlash uchun qism-dasturni qidirib topadi. Protsessorlar ikki turdagi uzilishlar bilan ishlashni vujudga keltirishi mumkin: dasturiy va texnik. Biror qurilma favqulodda xizmat ko‘rsatilishiga muhtoj bo‘lsa, unda texnik uzilish paydo bo‘ladi. Odatda bunday uzilish markaziy protsessor uchun kutilmagan hodisadir. Dasturiy uzilishlar asosiy dasturlar ichida protsessorning maxsus buyruqliari yordamida bajariladi. Dasturiy uzilishda dastur o‘z-o‘zini vaqtincha to‘xtatib, uzilishga taalluqli jarayonni bajaradi.

Tutib olish - bu jarayon oqibatida g‘arazli shaxslar dasturiy vositalar va axborotning turli magnitli tashuvchilariga kirishni yo‘lga qo‘yadi. Dastur va ma'lumotlardan noqonuniy nusxa olish, kompyuter tarmoqlari aloqa kanallaridan ruxsatsiz o‘qishlar va hokazo harakatlar tutib olish jarayonlariga misol bo‘la oladi.

O‘zgartirish - ushbu jarayon yovuz niyatli shaxs nafaqat kompyuter tizimi komponentlariga (ma'lumotlar to‘plamlari, dasturlar, texnik elementlari)

kirishni yo‘lga qo‘yadi, balki ular tarkibini (ko‘rinishini) o‘zgartiradi. Masalan, o‘zgartirish sifatida g‘arazli shaxsning ma'lumotlar to‘plamidagi ma'lumotlarni o‘zgartirishi, yoki umuman kompyuter tizimi fayllarini o‘zgartirishi, yoki qandaydir qo‘shimcha noqonuniy qayta ishlashni amalga oshirish maqsadida foydalanilayotgan dasturning kodini o‘zgartirishi tushuniladi.

Soxtalashtirish - bu jarayon yordamida g‘arazli shaxslar tizimda hisobga olinmagan vaziyatlarni o‘rganib, undagi kamchiliklarni aniqlab, keyinchalik o‘ziga kerakli harakatlarni bajarish maqsadida tizimga qandaydir soxta jarayonni yoki tizim va boshqa foydalanuvchilarga soxta yozuvlarni yuboradi.

Axborot hafvsizligini ta’minlashda biometrik usullardan foydalanish

Hozirgi vaqtga kelib, kompyuter-kommunikatsiya texnologiyalari kundan-kunga tez rivojlanib bormoqda. Shu sababli ham kompyuter texnologiyalari kirib bormagan sohaning o‘zi qolmadi, desak xato bo‘lmaydi. Ayniqsa ta'lim, bank, moliya tizimlarida ushbu zamonaviy texnologiyalarni qo‘llash yuqori samara bermoqda. Shu bilan birga axborot havfsizligiga bo‘lgan tahdid ham tobora kuchayib borayotgani hech kimga sir emas. Demak, hozirgi davrning eng dolzarb muammolardan biri axborot havfsizligini ta'minlashdan iborat.

Hozirga qadar tizimga ruxsatsiz kirishni taqiqlashning eng keng tarqalgan usuli sifatida «parol» qo‘yish printsipi hisoblanib kelmoqda. Chunki ushbu usul juda sodda, foydalanish uchun qulay va kam harajat talab etadi. Lekin, hozirga kelib «parol» tizimi to‘laqonli o‘zini oqlay olmayapti. Ya’ni ushbu usulning bir qator kamchiliklari ko‘zga tashlanib qoldi.

Birinchidan, ko‘pchilik foydalanuvchilar sodda va tez esga tushadigan parollarni qo‘llaydilar. Masalan, foydalanuvchi o‘z shaxsiga oid sanalar, nomlardan kelib chiqqan holda parol qo‘yadilar. Bunday parollarni buzish esa, foydalanuvchi bilan tanish bo‘lgan ixtiyoriy shaxs uchun unchalik qiyinchilik tug‘dirmaydi.

Ikkinchidan, foydalanuvchi parolni kiritishi jarayonida, kuzatish orqali ham kiritilayotgan belgilarni ilg‘ab olish mumkin.

Uchinchidan, agar foydalanuvchi parol qo‘yishda murakkab, uzundan-uzoq belgilardan foydalanadigan bo‘lsa, uning o‘zi ham ushbu parolni esidan chiqarib qo‘yishi extimoldan holi emas.

Va nihoyat, hozirda ixtiyoriy parollarni buzuvchi dasturlarning mavjudligi ko‘zga tashlanib qoldi.

Yuqoridagi kamchiliklardan kelib chiqqan holda aytish mumkinki, axborotni himoyalashning parolli printsipidan foydalanish to‘la samara bermayapti. Shu sababli ham hozirda axborotlardan ruxsatsiz foydalanishni cheklashning

biometrik usullarini qo‘llash dunyo bo‘yicha ommaviylashib bormoqda va ushbu yo‘nalish biometriya nomi bilan yuritilmoqda.

Biometriya - bu insonning o‘zgarmaydigan biologik belgilariga asosan aynan o‘xshashlikka tekshirishdir (identifikatsiya). Hozirda biometrik tizimlar eng ishonchli himoya vositasi hisoblanadi va turli xil maxfiy ob'ektlarda, muhim tijorat axborotlarini himoyalashda samarali qo‘llanilmoqda.

Hozirda biometrik texnologiyalar insonning quyidagi o‘zgarmas biologik belgilariga asoslangan: barmoqning papillyar chiziqlari, qo‘l kaftining tuzilishi, ko‘zning kamalak qobig‘i chiziqlari, ovoz parametrlari, yuz tuzilishi, yuz termogrammasi (qon tomirlarining joylashishi), yozish formasi va usuli, genetik kodi fragmentlari. Insonning ushbu biologik belgilaridan foydalanish turli xil aniqliklarga erishishga imkon beradi. Biz ushbu maqolada hozirda keng qo‘llanilayotgan barmoq izlari va qo‘l kaftining tuzilishi bo‘yicha insonni tanish masalalariga to‘xtalib o‘tishni lozim topdik.

Barmoq izlari buyicha insonni idetifikatsiyalash hozirda eng keng tarqalgan usul bo‘lib, axborotni himoyalash biometrik tizimlarida keng qo‘llanilmoqda. Bu usul o‘tgan asrlarda ham keng qo‘llanilganligi xech kimga yangilik emas. Hozirgi kunga kelib barmoq izlari bo‘yicha identifikatsiyalashning uchta asosiy texnologiyasi mavjud. Ularning birinchisi ko‘pchilikka ma'lum optik skanerlardan foydalanishdir. Ushbu qurilmadan foydalanish printsipi odatiy skanerdan foydalanish bilan bir xil. Bu yerda asosiy ishni ichki nur manbai, bir nechta prizma va linzalar amalga oshiradi. Optik skanerlarni qo‘llashning e'tiborli tomoni uning arzonligidir. Lekin, kamchilik tomonlari bir muncha ko‘p. Ushbu qurilmalar tez ishdan chiquvchi hisoblanadi. Shu sababli foydalanuvchidan avaylab ishlatish talab etiladi. Ushbu qurilmaga tushgan chang, turli xil chiziqlar shaxsni aniqlashda xatolikka olib keladi, ya'ni foydalanuvchining tizimga kirishiga to‘sqinlik qiladi. Bundan tashqari, optik skanerda tasviri olingan barmoq izi foydalanuvchi terisining holatiga bog‘liq. Ya'ni, foydalanuvchi terisining yog‘liligi yoki quruqligi shaxsni aniqlashga xalaqit beradi.

Barmoq izlari bo‘yicha identifikatsiyalashning ikkinchi texnologiyasi elektron skanerlarni qo‘llashdir. Ushbu qurilmadan foydalanish uchun foydalanuvchi 90 ming kondensator plastinkalaridan tashkil topgan, kremniy moddasi bilan qoplangan mahsus plastinkaga barmog‘ini qo‘yadi. Bunda o‘ziga xos kondensator hosil qilinadi. Kondensator ichidagi elektr maydon potentsiali plastinkalar orasidagi masofaga bog‘liq. Ushbu maydon kartasi barmoqning

papillyar chizmasini takrorlaydi. Elektron maydon hisoblanadi, olingan ma'lumotlar esa, katta aniqlikka ega sakkiz bitli rastrli tasvirga aylantiriladi.

Ushbu texnologiyaning e'tiborli tomoni shundaki, foydalanuvchi terisining har qanday holatida ham barmoq izi tasviri yuqori aniqlikda hosil qilinadi. Ushbu tizim foydalanuvchi barmog‘i kirlangan taqdirda ham tasvirni aniq oladi. Bundan tashqari qurilma hajmining kichikligi sababli, ushbu qurilmani hamma joyda ishlatish mumkin. Ushbu qurilmaning kamchilik tomonlari sifatida quyidagilarni keltirish mumkin: 90 ming kondensatorli plastinkani ishlab chiqarish ko‘p harajat talab etadi, skanerning asosi bo‘lgan kremniy kristali germetik (zich yopiladigan) qobiqni talab etadi. Bu esa, qurilmani ishlatishda turli xil cheklanishlarni yuzaga keltiradi. Nihoyat, kuchli elektromagnit nurlanishi vujudga kelganda elektron sensor ishlamaydi.

Barmoq izi buyicha identifikatsiyalashning uchinchi texnologiyasi Who Vision Sustems kompaniyasi tomonidan ishlab chiqarilgan Tactile Sense skanerlaridir. Ushbu skanerlarda maxsus polimer material ishlatilgan bo‘lib, terining bo‘rtib chiqqan chiziqlari va botiqlari orasida hosil bo‘lgan elektr maydonni sezish orqali tasvir hosil qilinadi. Umuman olganda ushbu skanerlarning ishlash printsipi elektron skanerlar ishlash printsipi bilan deyarli bir xil. Fakat ushbu qurilmalarning quyidagi afzalliklarini sanab o‘tishimiz mumkin: qurilmani ishlab chikarish bir necha yuz barobar kam harajat talab etadi, qurilma avvalgi qurilmadan mustahkam va foydalanishda hech qanday cheklanishlar yuzaga kelmaydi.

Insonining qo‘l kafti tuzilishiga ko‘ra identifikatsiyalashning ikki xil usuli mavjud. Birinchi usulda qo‘l kaftining tuzilishidan foydalaniladi. Buning uchun maxsus qurilmalar ishlab chiqarilgan bo‘lib, ushbu qurilma kamera va bir nechta yorituvchi diodlardan tashkil topgan. Ushbu qurilmaning vazifasi qo‘l kaftining uch o‘lchovli tasvirini hosil qilishdan iborat. Keyinchalik ushbu hosil qilingan tasvir ma'lumotlar bazasiga kiritilgan tasvir bilan solishtiriladi. Ushbu qurilma yordamida identifikatsiyalash yuqori aniqlikda amalga oshiriladi. Lekin kaft tasvirini oluvchi skaner o‘ta nozik ishlangan bo‘lib, ushbu qurilmadan foydalanish noqulayliklar tug‘diradi.

Qo‘l kafti tuzilishiga ko‘ra identifikatsiyalashning ikkinchi texnologiyasi esa, kaftning termogrammasini aniqlashga asoslangan. Qo‘l kaftida juda ko‘p qon tomirlari mavjud bo‘lib, ushbu qon tomirlari har bir insonda, hattoki egizaklarda ham turlicha joylashadi. Ushbu qon tomirlarining joylashish tasvirini olish uchun maxsus infraqizil nurli fotokameradan foydalaniladi. Ushbu hosil bo‘lgan tasvir kaft termogrammasi deb ataladi. Ushbu usulning ishonchliligi juda ham

yuqori. Bu usulning vujudga kelganiga ko‘p vaqt bo‘lmaganligi sababli hali keng tarqalib ulgurmagan.

Keltirib o‘tilgan barcha biometrik usullar axborotni himoya qilishda keng qo‘llanilmoqda. Ushbu himoya tizimining ishonchliligi shundaki, tizimda foydalanilayotgan insonning biologik belgilari hech qachon o‘zgarmaydi, biron-bir jaroxat yetgan taqdirda ham qayta tiklanadi.

Yuqorida biz insonning biologik belgilariga asosan shaxsni tanish maqsadida barmoq izi va qo‘l kaftining tasvirini hosil qilish texnologiyalari bilan tanishib chiqdik. Endigi masala hosil qilingan tasvirni ma'lumotlar bazasida saqlanayotgan tasvir bilan taqqoslash va shaxsni aniqlash algoritmi bilan bog‘liq. Biz ushbu masalada hosil qilingan barmoq izidan foydalangan holda shaxsni aniqlash algoritmini keltirib o‘tishga harakat qilamiz.

Yuqorida ta'kidlaganimizdek, birinchi navbatda ixtiyoriy qurilma orqali barmoq izi tasviri hosil qilinadi. Qolgan bosqichlarni quyidagi ketma-ketlik orqali bayon qilishga harakat qilamiz:

1. Tasvirga boshlang‘ich ishlov berish – bunda hosil qilingan tasvir Binar tasvirga o‘tkaziladi, ya'ni, tasvirdagi faqat barmoq izining chiziqlari olib qolinadi va tasvirning markazi (og‘irlik markazi) aniqlanadi;
2. Tasvirdagi o‘ziga xos belgilarni aniqlash – bunda tasvirning markazidan turli xil radiusli bir nechta aylanalar chiziladi (aylanalar qanchalik ko‘p bo‘lsa, aniqlik shunchalik ortadi). Natijada aylanalar hosil qilingan tasvir chiziqlarining bir nechta nuqtalarida kesishadi. Ushbu kesishish nuqtalari shartli ravishda A1, A2, ..., An (birinchi aylana), B1, B2, ..., Bm (ikkinchi aylana), C1, C2, ..., Ck (uchinchi aylana) harflari yordamida belgilanadi. Har bir aylanadagi kesishish nuqtalarini birlashtirish orqali A1A2...An, B1B2...Bm, C1C2...Ck ko‘pburchaklar hosil qilinadi. Ushbu hosil qilingan ko‘pburchaklar perimetrlari (P1, P2, P3) hisoblanadi.

Olingan tasvirni ma'lumotlar bazasida saqlanayotgan tasvir bilan solishtirish – bunda yuqoridagi bosqichda olingan natijalar: R1, R2, R3 radiusli aylanalardagi kesishishlar soni n, m, k; aylanalarda hosil qilingan ko‘pburchaklar perimetri P1, P2, P3 lar ma'lumotlar bazasida saqlanayotgan ushbu kattaliklar bilan taqqoslanadi. Ushbu kattaliklar o‘zaro mos tushsagina shaxs tasdiqlanadi. Ushbu keltirilgan shaxsni tanish algoritmi ustida respublikamizdagi bir nechta olimlar guruhi ish olib bormoqdalar va ushbu sohada ijobiy natijalarga erishilmoqda.

Foydalanilgan adabiyotlar:

1. Shamsiddinov, G‘iyosjon, and Temurbek Zarifov. "GLOBAL TARMOQ QURISHDA TARMOQ QURILMALARIDAN FOYDALANISH VA TARMOQ

TOPOLOGIYALARINING O'RNI." Science and innovation in the education system 3.5 (2024): 50-60.
2. Shamsiddinov, G'iyosjon, Jasmina Murodulloyeva, and Umida Nurmaxmatova. "YASHIL IQTISODIYOT VA YO 'NALISHLARI BO 'YICHA TA'LIM DASTURLARINI RIVOJLANTIRISH MEXANIZMLARI." Models and methods in modern science 3.5 (2024): 44-49.
3. Shamsiddinov, G'iyosjon, Umida Nurmaxmatova, and Durdona Turayeva. "INFORMATIKA VA RAQAMLI TEXNOLOGIYALARNING TA'LIM JARAYONIDAGI O'RNI." Science and innovation in the education system 3.4 (2024): 102-105.
4. Shamsiddinov, G'iyosjon, Umida Nurmaxmatova, and Durdona Turayeva. "INFORMATIKA VA RAQAMLI TEXNOLOGIYALARNING TA'LIM JARAYONIDAGI O'RNI." Science and innovation in the education system 3.4 (2024): 102-105.
5. Shamsiddinov, G'iyosjon, Jasmina Murodulloyeva, and Durdona Turayeva. "GLOBAL IQLIM O 'ZGARISHI SHAROITIDA EKOLOGIK BARQARORLIKNI SAQLASHNING ZAMONAVIY, INNOVATSION USULLARI." Инновационные исследования в современном мире: теория и практика 3.3 (2024): 103-106.
6. SHAMSIDDINOV G'IYOSJON HUSNIDDIN O'G'LI. Chiziqli dasturlash nazariyasi usullari. Buxoro davlat pedagogika instituti FIZIKA, MATEMATIKA VA INFORMATION TEXNOLOGIYALARNING INNAVATSIOAN RIVOJLANISHDAGI O'RNI" Respublika ilmiy-nazariy anjumani. 2023/12/22. Ст 59-63
7. SHAMSIDDINOV G'IYOSJON HUSNIDDIN O'G'LI. ЧИСЛЕННОЕ РЕШЕНИЕ СТАЦИОНАРНОЙ ЗАДАЧИ ОПТИМАЛЬНОГО РАЗМЕЩЕНИЯ ИСТОЧНИКОВ ТЕПЛА В СТЕРЖНЕ. Qo'qoqn davlat pedagogika instituti "Zamonaviy fan va ta'lim-tarbiya: muammo va yechimlari" mavzusidagi respublika ilmiy-amaliy anjuman materiallari". 2022/11/25. Ст-81-83
8. SHAMSIDDINOV G'IYOSJON HUSNIDDIN O'G'LI. СТЕРЖЕНДА ИССИҚЛИК МАНБАЛАРИНИ ОПТИМАЛ ЖОЙЛАШТИРИШНИНГ СТАЦИОНАР МАСАЛАСИНИ СОНЛИ ЕЧИШ. O'zbekiston Milliy Universiteti "O'zbekiston Milliy universiteti talabalar va ilmiy-tadqiqotchilarining ilmiy konferensiyasi". 2022/3/24. Ст 86-87
9. Kodirov A. Raxmatov Sh. TA'LIM JARAYONIDA BULUTLI TEXNOLOGIYALARDAN FOYDALANISHNING SAMARADORLIGI. "PEDAGOGS" international research journal. Ст 157-161
10. Berdiyeva, Gulnoza. "O'ZBEKISTON ELEKTRON SAVDO TIZIMIDA MUAMMOLAR VA TAKLIFLAR." Science and innovation in the education system 3.5 (2024): 16-22.

11. Berdiyeva, Gulnoza, and Raimbek Muzaffarov. "ELEKTRON TIJORATNING AN'ANAVIY SAVDO TURLARI BILAN XARAKTERLI XUSUSIYATLARI." Инновационные исследования в современном мире: теория и практика 3.4 (2024): 14-18.
12. Berdiyeva, Gulnoza. "RAQAMLI IQTISODIYOTNING MAQSAD VA VAZIFALARI VA UNING O'ZBEKISTONDA RIVOJLANISHI." Педагогика и психология в современном мире: теоретические и практические исследования 3.4 (2024): 11-14.
13. Jo'rayeva, Feruza. "TA'LIM JARAYONIDA AQL XARITALARIDAN FOYDALANISH VA ULARNING AHAMIYATI." Молодые ученые 2.9 (2024): 159-166.
14. Jo'rayeva, Feruza, and Shahrizoda Pardayeva. "KOMPYUTER O 'YINLARI-MANQURTLIK VOSITASI." Current approaches and new research in modern sciences 3.4 (2024): 12-18.
15. Jo'rayeva, Feruza, and Gulhayo Hamdamova. "MEDIA SAVODXONLIK TUSHUNCHASI VA UNING JAMIYATIMIZ HAYOTIDAGI AHAMIYATI." Педагогика и психология в современном мире: теоретические и практические исследования 3.3 (2024): 31-35.
16. Berdiyeva, Gulnoza, and Avazbek Narzulloyev. "VIRTUAL REALLIKDA TA'LIM RESURSLARI VA VIRTUAL TA'LIM." Наука и технология в современном мире 3.4 (2024): 13-20.
17. Berdiyeva, Gulnoza, and Avazbek Narzulloyev. "VIRTUAL BORLIQ VA UNING TURLI SOHALARDA QO 'LLANILISHI." Solution of social problems in management and economy 3.4 (2024): 18-23. Berdiyeva, G. "INFORMATIKA VA AXBOROT TEXNOLOGIYALARI FANINI OQITISHDA MASOFAVIY TALIM TEXNOLOGIYALARINING AHAMIYATI." Экономика и социум 12-1 (91) (2021): 146-150.
18. Berdiyeva, Gulnoza. "INFORMATIKA VA AXBOROT TEXNOLOGIYALARI FANINI OQITISHDA MASOFAVIY TALIM TEXNOLOGIYALARINING AHAMIYATI Gulnoza Berdiyeva, Qarshi davlat universitetining Pedagogika instituti oqituvchisi."