

Umarov Shuxratjon Azizjonovich¹, Abduqodirov Abdulhay Abdulaziz o'g'li²

¹*Muhammad al-Xorazmiy nomidagi TATU Farg'ona filiali Axborot xavfsizligi kafedrasi dotsenti, fizika-matematika fanlari bo'yicha falsafa doktori (PhD), sh.umarov81@mail.ru, +998913961130*

²*Muhammad al-Xorazmiy nomidagi TATU Farg'ona filiali talabasi,*

**BIOMETRIK IDENTIFIKATSIYALASH TIZIMLARINING
INTELLEKTUALLASHTIRISH USULLARI
МЕТОДЫ ИНТЕЛЛЕКТУАЛИЗАЦИИ СИСТЕМ БИОМЕТРИЧЕСКОЙ
ИДЕНТИФИКАЦИИ
METHODS FOR INTELLIGENTIZATION OF BIOMETRIC
IDENTIFICATION SYSTEMS**

Biometrik identifikatsiya usullari axborot xavfsizligi sohasida juda muhim ahamiyatga ega. Ushbu maqolada biometrik usullarning korxona va tashkilotlarning ma'lumotlar bazasi va axborot tizimlarini himoyalashdagi ahamiyati va ularning axborot xavfsizligiga o'z hissasi ko'rsatilgan. Biometrik identifikatsiya texnologiyalari shaxsiy xususiyatlarga asoslangan hisob-kitoblarni ishlab chiqishda qo'llaniladi. Bu texnologiyalar o'zgarmasa xususiyatlar, masalan, odamlarning qo'llab-quvvatlanish turi, chiroqlanish, to'g'ri qo'llanish shakli va boshqalar bilan ajralib turadi. Bunday xususiyatlardan foydalanib, biometrik identifikatsiya usullari shaxsiy identifikatsiya uchun ishlatiladi. Matematik modellari yordamida diskriminat yondashuv va biometrik texnologiyalar turlari tavsiflangan.

Tayanch so'zlar: axborot xavfsizligi, intellektual tizim, biometrika, yuz tasvir, ko'z gavhari, barmoq izlari, tanib olish, diskriminant yondashuv.

В данной статье подчеркнута важность биометрических методов идентификации в области информационной безопасности. Описана значимость использования биометрических методов для защиты баз данных и информационных систем корпораций и организаций. Биометрические

технологии идентификации опираются на уникальные личностные характеристики. Эти технологии используют неизменные характеристики, такие как тип отпечатка пальца, радужная оболочка глаза, форма лица и другие, для идентификации личности. С помощью математических моделей разрабатываются дискриминационные подходы и описываются различные типы биометрических технологий.

Ключевые слова: информационная безопасность, интеллектуальная система, биометрия, изображение лица, глазной камень, отпечатки пальцев, распознавание, дискриминантный подход.

This article highlights the importance of biometric identification methods in the field of information security. The importance of using biometric methods to protect databases and information systems of corporations and organizations is described. Biometric identification technologies rely on unique personal characteristics. These technologies use immutable characteristics such as fingerprint type, iris, face shape and others to identify an individual. Using mathematical models, discriminatory approaches are developed and various types of biometric technologies are described.

Keywords: information security, intelligent system, biometrics, facial image, eyestone, fingerprints, recognition, discriminant approach.

KIRISH

Axborot xavfsizligi sohasiga biometrika deganda shaxsning fiziologik va xulq-atvor xususiyatlaridan kelib chiqib, uning shaxsini avtomatik ravishda aniqlash va tasdiqlash usullarini ifodalovchi bilim sohasi tushuniladi.

Bugungi kunda biometrik usullar (vositalar) yordamida korxonalar ma'lumotlar, binolar va tizimlarni himoya qilishga harakat qilmoqdalar. Inson tanasining xususiyatlarini tan olish bozori haqiqiy "biometrik inqilob"ni boshdan kechirmoqda. BCC Research konsalting kompaniyasi tadqiqotiga ko'ra, 2015 yildan 2024 yilgacha bo'lgan davrda global biometrik bozorning o'rtacha yillik o'sish sur'ati 32,7% bo'lishi mumkin. 2024 yilga kelib biometrik bozor 56,7 milliard dollargacha o'sadi (taqqoslash uchun 2014 yilda global biometrik bozor hajmi taxminan 14,9 milliard dollarni tashkil etgan).

O'tgan asrning 90-yillarida biometrik tizimlar asosan harbiy sirlarni va ayniqsa muhim tijorat ma'lumotlarini himoya qilish uchun ishlatilgan. Hozirgi kunda aeroportlar, yirik savdo markazlari, ko'plab kompaniyalarning ofislari biometrik kirish tizimlari bilan jihozlangan. Talabning ortishi ushbu sohadagi tadqiqotlarni rivojlantirdi, bu esa o'z navbatida yangi qurilmalar va yangi texnologiyalarning paydo bo'lishiga olib keldi. Biometrik mahsulotlar bozoridagi yetakchilar - Identix, Digital Persona, Precise Biometrics, Visionics, Ethentica, BioScript, Secugen, AcSys Biometrics bilan bir qatorda biometrik sohaga ixtisoslashgan kuchli korporatsiyalar paydo bo'ldi:- Sony, Panasonic, LG, Compaq va boshqalar.

ADABIYOTLAR

Axborot xavfsizligini ta'minlashning intellektual usullari va ularning Matematik asoslarini tahlil qilish orqali shifrlash algoritmlarini ishlab chiqish masalalari U.Gawande, Y.Golhar, A. K.Jain, P.Flynn, J. L.Wayman, D.Maltoni, D.Maio, V. I. Vasilev, V. L.Sirlov, A.A.Moldovyan, V.M.Fomichev, P.F.Xasanov, M.M.Aripov, M.M.Karimov, A.V.Kabulov, D.E.Akbarov, R.Adaxanov va boshqalarning ilmiy ishlarida ko'rib chiqilgan. Hozirda O'zbekiston Respublikasida axborot-kommunikatsiya tarmoqlari texnika va texnologiyalarining

jadal rivojlanib borishi natijasida axborot xavfsizligini ta'minlashning intellektual usullarining milliy algoritmlarini, modellarini ishlab chiqish ustuvor masala va vazifalardan bo'lib qolmoqda.

TADQIQOT METODOLOGIYASI

Odatda, biometrik texnologiyalarni tasniflashda ishlatiladigan biometrik xususiyatlar turiga qarab biometrik tizimlarning ikki guruhi ajratiladi.

Birinchi guruh biometrik tizimlar inson tomonidan tug'ilganda mavjud bo'lgan va vaqt o'tishi bilan deyarli o'zgarmaydigan statik biometrik xususiyatlardan foydalanadi. Bularga quyidagilar kiradi:

- barmoq izlari;
- ko'z gavhari;
- yuz tasviri;
- qo'l geometriyasi;
- barmoqlarni tuzilishi;
- DNK va boshqalar.

Ikkinchi guruh biometrik tizimlar vaqt o'tishi bilan o'zgarib turadigan va har bir shaxsning quyidagi individual xususiyatlarini aks ettiruvchi identifikatsiya qilish uchun dinamik biometrik xususiyatlardan foydalanadi:

- qo'lda yozilgan yozuv (imzo);
- ovoz;
- klaviaturada ishlash uslubi va boshqalar.

Ushbu xususiyatlarning har biri o'zining afzalliklari va kamchiliklariga ega. Statik biometrik xususiyatlardan foydalanishning afzalligi – ularning shaxsning psixofizik holatidan nisbiy mustaqilligi, tanib olish algoritmlari uchun kam xarajatlar va ko'plab odamlarning biometrik identifikatsiyalashni tashkil qilish imkoniyatidir. Amalda eng keng tarqalgani birinchi guruhdagi xususiyatlarning dastlabki uchtasi ekanligi bejiz emas (barmoq izlari, ko'z gavhari va yuz geometriyasining xususiyatlari bilan tanib olish). Statik biometrikaning kamchiliklari - foydalaniladigan biometrik xususiyatlarning statik qat'iyligi, ularni

soxtalashtirish (almashtirish) mumkinligi va maxsus o'qish uskunalariga bo'lgan talab zurligidir.

Birinchi guruh usullaridan farqli o'laroq, dinamik biometrik usullar ko'proq o'zgaruvchanlikni ta'minlaydi (masalan, imzo yoki parolni o'zgartirish har doim oson), ular kompyuter yordamida dasturiy ta'minotda orqali osonlik bilan amalga oshiriladi. Ushbu holatlar foydalanuvchilarga masofaviy kirish vaqtida autentifikatsiya/identifikatsiya qilish uchun dinamik biometrikni afzalroq qiladi. Dinamik usullarning asosiy kamchiligi biometrik tizimning ishlashiga shaxsning psixofizik holatining (charchoq, qo'rquv, dori vositalariga ta'sir qilish) ta'siridir.

Turli tadqiqotlar shuni ko'rsatadiki, bugungi kunda biometrik echimlarning taxminan yarmi barmoq izini aniqlash tizimlaridir. Taxminlarga ko'ra, aholi ushbu usulini oson qabul qiladi: barmoq izlari tez va qulay tarzda skanerdan o'tkaziladi va tekshirish ko'p vaqt va xarajatlarni talab qilmaydi. Biometrik yechimlarning qolgan yarmi asosan yuz, ovoz va go'z gavharini tanib olish texnologiyalari tashkil qiladi. Bu texnologiyalar moliya sektorida, savdoda, yangi pasport tizimlarida, chegara nazorati punktlarida keng qo'llanib kelinmoqda.

TAHLIL VA NATIJALAR

Aynan yuzning raqamli tasviri bugungi kunda barcha mamlakatlarda yangi avlod pasport va viza hujjatlari (biometrik pasportlar) uchun tan olingan, unga yana ikkita parametr - barmoq izlari va ko'z gavhari tasviri qo'shimcha hisoblanadi. Har bir davlat ularni biometrik pasportlarga o'z xohishiga ko'ra kiritishi mumkin. Uch o'lchamli (3D) yuz tasviri eng yangi biometrik texnologiyadir (ishlab chiqaruvchi A4 Vision). Biometrik pasportga atigi 5 KB hajmdagi uch o'lchamli fotosurat yozilishi mumkin, bu shaxsiy identifikatsiyaning aniqligini oshiradi va hujjatni avtomatik tekshirish ishonchliligini oshiradi. Mutaxassislarining ta'kidlashicha, uch o'lchamli yuz tasvirni tanib olish darajasi 90% dan ortiq, ikki o'lchovli tasvir uchun esa bu ko'rsatkich kamdan-kam hollarda 50% dan oshadi.

Har qanday biometrik tizimning ishlashi quyidagi harakatlar zanjiriga asoslanadi (1-rasm):

1) yozib olish - foydalanuvchining biometrik ma'lumotlari skaner yordamida o'qiladi;

2) tanlash - taqdim etilgan biometrik ma'lumotlardan (axborot xususiyatlari vektori yoki qisqa identifikatsiya kodi shaklida, uzunligi 1000 bitgacha bo'lgan) noyob ma'lumotlar olinadi, bu ma'lum bir shaxsning biometrik "tasvirini" aks ettiradi;

3) taqqoslash - taqdim etilgan biometrik tasvir tizim ma'lumotlar bazasida saqlanadigan bir yoki bir nechta standartlar (shablonlar) bilan taqqoslanadi;

5) qaror qabul qilish - tizim biometrik tasvirlar mos keladimi yoki yo'qligini hal qiladi va identifikatsiya qilish protsedurasining tugashi, uni takrorlash yoki uni amalga oshirish shartlarini o'zgartirish to'g'risida qaror qabul qiladi.

Biometrik ma'lumotlarni ajratish va taqqoslash bosqichida biometrik shablonlardan foydalaniladi. Biometrik shablonlar odatda yopiq, ikkilik formatdagi, kodlangan (siqilgan) shaklda tegishli biometrik tasvirlar haqidagi ma'lumotlarni o'z ichiga olgan ma'lumotlar to'plami bo'ladi. Biometrik shablonlar uchun CBEFF (Common Biometric Exchange File Format) xalqaro standart mavjud bo'lib, u biometrik ma'lumotlarni taqdim etishning yagona formatini taqdim qiladi, bunda esa bugungi kunda apparat va dasturiy ta'minot ishlab chiqaruvchilari tomonidan qo'llaniladigan biometrik formatlardan kelib chiqib taklif qiladi.

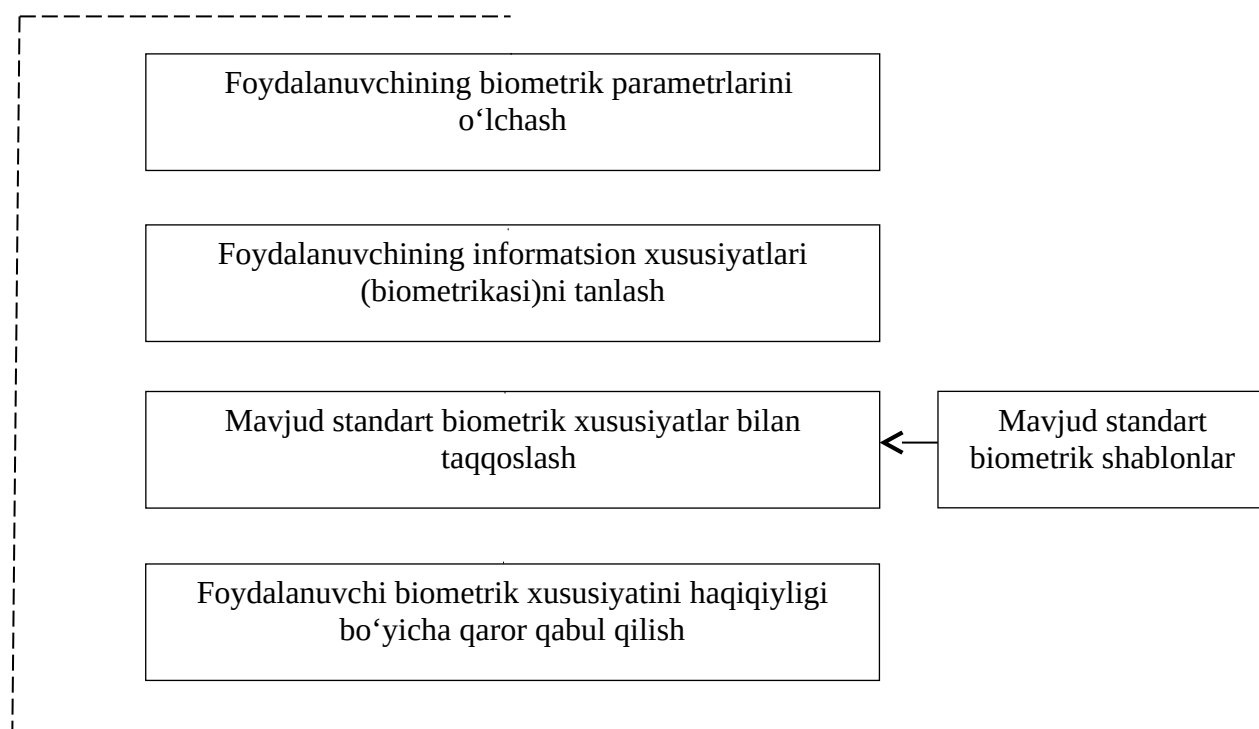
Biometrik tizimning ikkita ish rejimi mavjud (1-rasm):

- tekshirish ("birini biriga solishtirish");
- identifikatsiya qilish (birini ko'p bilan solishtirish").

Tekshirish rejimida foydalanuvchi tizimga o'zining biometrik ma'lumotlarini taqdim etadi va shu bilan "kimligini" bildiradi. Bu holda tizimning vazifasi olingan ma'lumotlarning "to'g'riligini" tekshirishdir, ya'ni olingan biometrik ma'lumotlarning deklaratsiya qilingan jismoniy shaxsning ilgari qayd etilgan shabloniga (standartiga) muvofiqligini tekshirish.

Identifikatsiya rejimida ham foydalanuvchi tizimga o'zining biometrik ma'lumotlarini taqdim etadi, ammo bunda tizimning vazifasi o'zgaradi:

foydalanuvchi unga ma'lum bo'lgan shaxslar soniga tegishli yoki tegishli emasligini aniqlashi kerak kerak. Agar bazada mavjud bo'lsa, u kim? Bunday holda, biometrik ma'lumotlar tizimga "ma'lum" bo'lgan barcha foydalanuvchilarning oldindan yozib olingan shablonlari ma'lumotlar bazasi bilan taqqoslanadi.



1-rasm. Biometrik identifikatsiya jarayoni.

Ko'rinib turibdiki, real foydalanish sharoitida biometrik tizimlar bir qator muammolarga duch keladi, masalan, shaxsiy tan olinishining yuqori ishonchliligini ta'minlash zaruriyati. Ushbu muammoni hal qilish quyidagicha:

a) biometrik identifikatsiya/tekshirish protsedurasining o'zi ehtimollik xususiyatiga ega, chunki olingan biometrik ma'lumotlarning o'zi ko'plab omillari ta'sir qiladi, natijada "o'zinikini tan olmaslik" va "o'zinikini tan olish" ehtimoli paydo bo'ladi.

b) biometrik tizim qasddan aldash va biometrik skanerlash ob'ektini almashtirishlardan himoyalangan bo'lishi kerak;

v) qabul qilingan biometrik ma'lumotlarning xavfsizligi masalasi ayniqsa dolzarb bo'lib qolmoqda, bunda nafaqat biometrik ma'lumotlarni buzish ehtimoli, balki har qanday ta'sirlar nazarda tutiladi. Masalan, shaxs sog'ligi nuqtai nazaridan

ko'z gavharini yoki ko'z tomirlarini o'zgarishi, qo'lning sinishi yoki barmoq izining shilinishi va shu kabilar.

Turli xil biometrik texnologiyalarning (yuz tasviri - ikki o'lchovli (2D) va uch o'lchovli (3D), barmoq izi va ko'z gavhari bo'yicha) samaradorligi qiyosiy baholandi (1-jadval).

1. O'lchash mumkinligi. Biometrik xususiyat osongina o'lchanadigan bo'lishi kerak. O'lchash imkoniyatini FER (*Failure to Enroll*) qiymati bilan aniqlash mumkin. FER - ro'yxatdan o'ta olmagan va o'rtacha tanib olish vaqti (*Recognition Time*). Tanib olish vaqti tizimning ishlash rejimiga qarab tekshirish vaqti yoki identifikatsiya vaqtini bildiradi. FER jismoniy shaxslarda zarur biometrik ma'lumotlarga ega bo'lmagan holatlarni o'z ichiga oladi, lekin asosan ma'lum bir sababga ko'ra bir shaxs uchun ma'lumotlarni o'lchash qiyin bo'lgan holatlar mavjud. Masalan, ko'z gavharini tanib olish yuqori aniqlikdagi tasvirni talab qiladi, bu esa skanerlash moslamasiga nisbatan ko'zni aniq joylashtirish talab qiladi, o'z navbatida bu yerda joylashtirish bilan bog'liq qiyinchilik yuzaga keladi. Barmoq izlari bo'yicha odamlarning ba'zi guruhlari, ya'ni qo'l mehnati bajaradigan ishchilar, teri nuqsonlari bo'lgan va kekxa odamlar uchun ham tanib olish qiyin bajariladi. Yuz tasvirini aniqlash usullari kontaktsiz va shuning uchun yuqori darajada o'lchanadigan biometrik xususiyatga ega hisoblanadi.

2. Atrof muhitga qarshilik. Biometrik texnologiya atrof-muhit o'zgarishlariga bardoshli bo'lishi kerak. Turli texnologiyalarning ishlashi atrof-muhit sharoitlariga bog'liq va bu sharoitlar o'zgarganda o'zgarib qolishi mumkin. Masalan, barmoq izlari skanerlari tezda ifloslanadi, bunda ish sifati pasayadi, skanerni tez-tez tozalab turish zarur bo'ladi. Ikki o'lchovli yuzni tanib olish uchun tashqi yoritish tizim muhim ahamiyatga ega.

3. Soxtalashtirishga qarshilik. Biometrik tizim turli xil soxtalashtirishga (ruxsatsiz kirish) bardoshli bo'lishi kerak. Ikki o'lchovli yuz tasviriga asoslangan tanib olish tizimini "tanish" bo'lganlar orasidan "to'g'ri" shaxsning fotosuratini taqdim etish orqali osongina aldash mumkin. Boshqa shaxsning ko'zining tasvirini

o'g'irlash, albatta, yuzning fotosuratini o'g'irlashdan ko'ra qiyinroqdir, lekin agar kontakt linzalari almashtirish orqali buni amalga oshirilish mumkin.

Barmoq izini soxtalashtirishda qandaydir sirtida qolgan shaxsning barmoq izlarini olish, ularni raqamlashtirish va olingan tasvirni kompyuterda qayta ishlab "soxta" barmoq yoki qoplama yaratish mumkin. Masalan, yaponiyalik Tsutomu Matsumoto Yokogama universiteti laboratoriyasida autentifikatsiya tizimini aldash uchun soxta barmoq izlarini yaratish qanchalik oson ekanligini ko'rsatib bergan.

Soxtalashtirish juda qiyin bo'lgan texnologiya bu uch o'lchovli yuz tasviriga asoslangan tanib olish tizimidir. Bunday tizimni aldash uchun yuz tasvirning geometriyasini barcha tafsilotlarini ifodalaydigan niqobni ishlab chiqarish kerak bo'ladi.

4. Tanib olishning aniqligi. Biometrik tizimning aniqliligini baholash uchun quyidagi ko'rsatkichlar qo'llaniladi::

-*FAR (False Acceptance Rate)* – tizimda mavjud bo'lmagan foydalanuvchiga ruxsat bermaslikning ehtimoli;

-*FRR (False Rejection Rate)* - tizim sub'ektni tanimasa va shunga mos ravishda uni "begona" deb tan olish va kirishni rad etish ehtimoli.

Statistik nazariyada FRR va FAR qiymatlari odatda mos ravishda 1 va 2 turdagi xatolar deb ataladi.

Amaliyotda, biometrik tizimlar turli darajadagi "hushyorlik" ga sozlanishi mumkin. Ya'ni FARni aniqligini kamayishi tizimning sezgirligining pasayishiga va FRRning ishlamay qolishi tan olmaslik ehtimolining oshishiga olib keladi. Zamonaviy tizimlarda FAR qiymatlari kichik foizlarda, FRR qiymatlari bir necha foizlarda (2 ... 5%) hisoblanadi.

Tadqiqotlar shuni ko'rsatadiki, tizim aniqligining ko'rsatkichlari ishlab chiqaruvchi va sinov usullariga qarab juda farq qiladi, ammo 1-jadvalda keltirilgan Tanish texnologiyalarining uchtasi – 3D yuz tasviri, barmoq izi va ko'z gavhari muhim ahamiyatga va aniqlikka ega. Boshqa tomondan, shuni ta'kidlash kerakki, ikki o'lchovli yuz tasviri vizual taqqoslash uchun eng qulaydir.

Biometrik texnologiyalar xarakteristikasi

Kriteriy Texnologiya	O'lchash mumkinligi	Atrof- muhitga qarshilik	Soxtalashtirishg a qarshilik	Tanib olishning aniqligi
Yuz tasviri:				
2D-tasvir	Y	P	P	P
3D-tasvir	Y	Y	A	Y
Barmoq izi	P	P	P	Y
Ko'z gavhari	P	Y	P	Y
P-past darajada, Y-yaxshi darajada, A-yuqori darajada				

Shuni ham yodda tutingki, identifikatsiya rejimida biometrik tizimdan foydalanilganda tanib olish aniqligi tekshirish rejimiga nisbatan yomonlashib boradi. Shunday qilib, masalan, agar FRR 1,3% bo'lsa, tekshirish rejimida eng yaxshi barmoq skaneri FARni 0,001% ga teng bo'ladi, ma'lumotlar bazasi bilan solishtirishda identifikatsiya rejimida FAR 0,1% bo'lib qoladi. Bu esa ko'p ilovalar uchun mumkin emas.

XULOSA

Oxirgi qoida uchun kriteriylardan foydalanishda xavflarni hisobga olish kerak:

- *Baes kriteriysi - qaror qabul qilish strategiyasi minimal o'rtacha xavfni ta'minlaydigan tarzda tanlanadigan qoida;*
- *minimax kriteriysi - o'rtacha xavfning mumkin bo'lgan maksimal qiymatini minimallashtiradigan mezon;*
- *Neyman-Pirson kriteriysi - tanib olish xatolarini minimallashtirishga asoslangan.*

Qaror qoidasining sifati ko'p jihatdan $F_i(V)$ dagi haqiqiy va taqsimot parametrlari o'rtasidagi muvofiqlik darajasiga bog'liq. Statistik ma'lumotlar mavjud bo'lmaganda (yoki kichik bo'lganda) taqsimot parametrlarini baholash va

qarorlar qabul qilish muammosi mutaxassislar tomonidan tayinlangan "sub'ektiv ehtimolliklar" yordamida va lingvistik o'zgaruvchilar nazariyasi yordamida hal qilinishi mumkin.

Shaxsiy identifikatsiyalash biometrik usullarining umumiy kamchiliklari:

- tanshi olish sifati ko'p jihatdan o'lchangan biometrik ma'lumotlarning sifatiga bog'liq;
- tizim sifat ko'rsatkichlarida sezilarli o'zgarishlar mavjud, chunki mavjud biometrik tizimlar mavhum foydalanuvchiga qaratilgan;
- noaniqlik omillari ta'sirida xatolarning yuqori foizi, tan olish aniqligi ko'rsatkichlarining tizim foydalanuvchilari soniga bog'liqligi;
- ko'p faktorli biometrik identifikatsiyadan foydalanishda tanib olish algoritmlari murakkablashishi;
- foydalanuvchini biometrik identifikatsiyalash vositalarini baholash va sertifikatlashtirish masalalari to'liq hal etilmagan.

Ushbu kamchiliklar, "o'zini o'zi o'rganish" orqali biometrik ma'lumotlar bazasida foydalanuvchiga moslashtirish mexanizmlaridan foydalanadigan neyron tarmoq biometrik identifikatsiya tizimlarini qurishda sezilarli darajada bartaraf etiladi.

FOYDALANILGAN ADABIYOTLAR

1. Gawande, U., & Golhar, Y. (2018). Biometric security system: a rigorous review of unimodal and multimodal biometrics techniques. *International Journal of Biometrics*, 10(2), 142-175.
2. Jain, A. K., Flynn, P., & Ross, A. A. (Eds.). (2007). *Handbook of biometrics*. Springer Science & Business Media.
3. Umarov, S., & Abduqodirov, A. (2024). NOANIQ EKSTRAKTORLARGA ASOSLANGAN BIOMETRIK IDENTIFIKATSIYA TIZIMLARI TAHLILI. *Research and implementation*, 2(5), 150-156.

4. Wayman, J. L., Jain, A. K., Maltoni, D., & Maio, D. (Eds.). (2005). Biometric systems: Technology, design and performance evaluation. Springer Science & Business Media.
5. Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). Handbook of fingerprint recognition (Vol. 2). London: springer.
6. Васильев, В. И. (2013). Интеллектуальные системы защиты информации.
7. Цирлов, В. Л. (2008). Основы информационной безопасности автоматизированных систем. М.: Феникс, 173.
8. Мухториддинов, М., Акбаров, Н., & Умаров, Ш. (2023, October). MACHINE LEARNING FOR NETWORK SECURITY AND ANOMALY DETECTION. In Conference on Digital Innovation:" Modern Problems and Solutions".
9. Azizjonovich, U. S., & Abdulhay, A. (2024). AXBOROT XAVFSIZLIGI TIZIMLARINI INTELLEKTUALLASHTIRISH MASALALARI. Al-Farg'oniy avlodlari, 1(1), 4-10.
10. Тожиматов, Д. (2022). Актуальность обеспечения кибербезопасности с помощью искусственного интеллекта. Противодействие правонарушениям в сфере цифровых технологий и вопросы организационно-правового обеспечения информационной безопасности, 1(01), 304-306.
11. Умаров, Ш. (2023, November). ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБУЧЕНИИ КИБЕРБЕЗОПАСНОСТИ: АВТОМАТИЗАЦИЯ И АНАЛИЗ УГРОЗ. In Conference on Digital Innovation:" Modern Problems and Solutions".
12. Otaboyeva, M. (2023). BIOMETRIK IDENTIFIKATSIYALASH TIZIMLARINING TAHLILI. Академические исследования в современной науке, 2(17), 159-164.
13. Umarov, Sh. (2024). Axborot xavfsizligining intellektual tizimlarini qurish asoslari. Buxoro davlat universiteti ilmiy axboroti, 2, 9-16.

14. Adaxanov, R. (2022, August). BIOMETRIK BARMOQ IZI ORQALI AXBOROTLAR XAVFSIZLIGI. In INTERNATIONAL CONFERENCES (Vol. 1, No. 5, pp. 64-68).
15. Zoxirovich, X. M. (2024). BIOMETRIK AUTENTIFIKATSIYA VA IDENTIFIKATSIYA TIZIMLARINI ISHLAB CHIQISH HAMDA BIOMETRIK IDENTIFIKATSIYA MEZONLARI. Ta'lim innovatsiyasi va integratsiyasi, 17(4), 161-167.