

**TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI**  
**HUZURIDAGI ILMIY DARAJALAR BERUVCHI**  
**DSc.13/30.12.2019.T.07.02 RAQAMLI ILMIY KENGASH**

---

**TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI**

**YULDASHEVA NAFISA SALIMOVNA**

**AXBOROT TIZIMLARI FOYDALANUVCHILARINING OVOZI**  
**BO‘YICHA BIOMETRIK AUTENTIFIKATSIYALASH MODEL I VA**  
**ALGORITMLARI**

**05.01.05 – Axborotlarni himoyalash usullari va tizimlari.**  
**Axborot xavfsizligi**

**TEXNIKA FANLARI BO‘YICHA FALSAFA DOKTORI (PhD) DISSERTATSIYASI**  
**AVTOREFERATI**

**Toshkent-2024**

**Texnika fanlari bo‘yicha falsafa doktori (PhD) dissertatsiyasi avtoreferati  
mundarijasi**

**Оглавление автореферата диссертации доктора философии (PhD)  
по техническим наукам**

**Contents of dissertation abstract of the doctor of philosophy (PhD)  
on technical sciences**

**Yuldasheva Nafisa Salimovna**

Ахборот тизимлари фойдаланувчиларининг ovozi bo‘yicha biometrik  
autentifikatsiyalash modeli va algoritmlari ..... 3

**Юлдашева Нафиса Салимовна**

Модель и алгоритмы голосовой биометрической аутентификации  
пользователей информационных систем..... 21

**Yuldasheva Nafisa Salimovna**

Model and algorithms of biometric authentication based on the voices of  
information systems users ..... 41

**E‘lon qilingan ishlar ro‘yxati**

Список опубликованных работ  
List of published works..... 45

**TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI**  
**HUZURIDAGI ILMIY DARAJALAR BERUVCHI**  
**DSc.13/30.12.2019.T.07.02 RAQAMLI ILMIY KENGASH**

---

**TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI**

**YULDASHEVA NAFISA SALIMOVNA**

**AXBOROT TIZIMLARI FOYDALANUVCHILARINING OVOZI**  
**BO‘YICHA BIOMETRIK AUTENTIFIKATSIYALASH MODELI VA**  
**ALGORITMLARI**

**05.01.05 – Axborotlarni himoyalash usullari va tizimlari.**  
**Axborot xavfsizligi**

**TEXNIKA FANLARI BO‘YICHA FALSAFA DOKTORI (PhD) DISSERTATSIYASI**  
**AVTOREFERATI**

**Toshkent-2024**

**Texnika fanlari doktori (DSc) dissertatsiyasi mavzusi O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligi huzuridagi Oliy attestatsiya komissiyasida B2023.4.PhD/T4177 raqam bilan ro‘yxatga olingan.**

Dissertatsiya Toshkent axborot texnologiyalari universitetida bajarilgan.

Dissertatsiya avtoreferati uch tilda (o‘zbek, rus, ingliz (rezyume)) Ilmiy kengash veb-sahifasida ([www.tuit.uz](http://www.tuit.uz)) va «Ziyonet» Axborot ta’lim portalida ([www.ziyonet.uz](http://www.ziyonet.uz)) joylashtirilgan.

**Ilmiy rahbar:**

**Tashev Komil Axmatovich**

texnika fanlari nomzodi, dotsent

**Rasmiy opponentlar:**

**Kerimov Kamil Fikratovich**

texnika fanlari doktori, professor

**Yusupov Bahodir Karamatovich**

texnika fanlari bo‘yicha falsafa doktori (PhD), dotsent

**Yetakchi tashkilot:**

**“UNICON.UZ - Fan-texnika va marketing tadqiqotlari markazi” MChJ**

Dissertatsiya himoyasi Toshkent axborot texnologiyalari universiteti huzuridagi DSc.13/30.12.2019.T.07.02 Ilmiy kengashning 2024-yil « 16 » noyabr soat 10<sup>00</sup> daqi majlisida bo‘lib o‘tadi. (Manzil: 100084, Toshkent shahri, Amir Temur ko‘chasi, 108-uy. Tel.: (99871) 238-64-43, e-mail: [info@tuit.uz](mailto:info@tuit.uz)).

Dissertatsiya bilan Toshkent axborot texnologiyalari universiteti Axborot-resurs markazida tanishish mumkin (\_\_\_ raqam bilan ro‘yxatga olingan.). (Manzil: 100084, Toshkent shahri, Amir Temur ko‘chasi, 108-uy. Tel.: (99871) 238-64-70)

Dissertatsiya avtoreferati 2024-yil « 4 » noyabrda tarqatildi.  
(2024-yil « \_\_\_ » noyabr daqi 16 raqamli reyestr bayonnomasi)

**B.Sh. Maxkamov**

Ilmiy darajalar beruvchi ilmiy kengash raisi, iqtisodiyot fanlari doktori, professor

**M.S. Saitkamolov**

Ilmiy darajalar beruvchi ilmiy kengash ilmiy kotibi, iqtisodiyot fanlari doktori, dotsent

**B.F. Abduraximov**

Ilmiy darajalar beruvchi ilmiy kengash qoshidagi ilmiy seminar raisi o‘rinbosari, fizika-matematika fanlari doktori, professor

## **KIRISH (falsafa doktori (PhD) dissertatsiyasining annotatsiyasi)**

**Dissertatsiya mavzusining dolzarbligi va zarurati.** Hozirda biometrik texnologiyalariga asoslangan xavfsizlikni ta'minlashga yo'naltirilgan ilovalarni ishlab chiqishga katta e'tibor qaratilmoqda. Ushbu yo'nalishda axborot tizimlari foydalanuvchilarining nutq signallarini ishlash va tanib olishga asoslangan usul, algoritm va ilovalarni ishlab chiqish muhim masalalardan biri bo'lib qolmoqda. Xususan, GITNEX ma'lumotiga ko'ra "2025-yilda biometrik tizimlarni sotishdan tushadigan daromad butun dunyo bo'ylab taxminan 15,1 milliard dollarni tashkil etishi taxmin qilinmoqda<sup>1</sup>". Bu esa biometrik parametrlarga asoslangan, xususan, foydalanuvchilarni nutqiga asoslangan autentifikatsiya tizimlarini tadqiq etishni taqozo etadi. Hozirda AQSH, Xitoy, Angliya, Rossiya Federatsiyasi, Germaniya, Hindiston, Janubiy Koreya kabi davlatlarda axborot tizimlari foydalanuvchilarini nutq asosida identifikatsiyalash tizimlari asoslarini tashkil etuvchi nutq signallarini ishlash hamda nutq asosida shaxsni identifikatsiyalash yo'nalishlarining nazariy va amaliy masalalarini yechishga katta e'tibor qaratilmoqda.

Jahonda nutq signallariga ishlov berish, nutq signali belgilarini shakllantirish, nutq va uning asosida shaxsni identifikatsiyalash usul va algoritmlarini takomillashtirish, ishlab chiqish hamda hisoblashning tezkor algoritmlarini yaratishga yo'naltirilgan keng qamrovli ilmiy ishlar olib borilmoqda. Bu borada, jumladan, nutq signallariga dastlabki ishlov berish, nutq joylashgan sohani aniqlash hamda nutqni xarakterlovchi informativ belgilarni ajratish, shaxsni identifikatsiyalash usul va algoritmlarini ishlab chiqish, takomillashtirish hamda nutq modellari va identifikatsiyalashning avtomatlashtirish tizimlarini yaratish bo'yicha ilmiy tadqiqotlar olib borilmoqda. Mamlakatimizda ham nutq signallariga raqamli ishlov berish va tahlil qilishga asoslangan shaxsni biometrik identifikatsiyalashning intellektual tizimlarini ishlab chiqish va joriy etishga alohida e'tibor qaratilmoqda.

Respublikamizda davlat va bank xizmatlaridan foydalanish jarayonida shaxsni identifikatsiyalash tizimini takomillashtirishga qaratilgan keng qamrovli chora-tadbirlar amalga oshirilmoqda. O'zbekiston Respublikasi Prezidentining 2022-yil 20-apreldagi PF-113-son farmonida keltirilgan "Davlat xizmatlari ko'rsatish tizimini modernizatsiya qilish va jadal rivojlantirishning 2022 - 2026-yillarga mo'ljallangan milliy strategiyasi"ning ustuvor yo'nalishlarida "bank-moliya va davlat xizmatlarini ko'rsatish sohasida yagona identifikatsiya tizimini joriy etish", "davlat, bank, ijtimoiy xizmatlarni ko'rsatish va boshqa ma'muriy tartib-taomillardan o'tishda shaxsni identifikatsiya qilishning muqobil usullarini joriy etish" kabi vazifalar belgilab berilgan. Mazkur vazifalarni amalga oshirishda nutq signallariga ishlov berish va tahlil qilishning yondashuvi, modeli, usul va algoritmlarini, shaxsni nutqi asosida tanib olish va nutq signallarini, optimal belgilar majmuasini inobatga olgan holda, takomillashtirish, shuningdek, axborot tizimlaridan ruxsatsiz foydalanishni cheklash, foydalanuvchilarni nazorat qilish

---

<sup>1</sup> <https://gitnux.org/biometric-statistics/#:~:text=As%20of%202019%2C%2087%25%20of,increase%20in%20biometric%20data%20breaches.>

hamda boshqarish tizimlarida qo‘llash muhim biri hisoblanadi.

Ushbu dissertatsiya tadqiqoti O‘zbekiston Respublikasi Prezidentining 2018-yil 19-fevraldagi “Axborot texnologiyalari va kommunikatsiya sohasini yanada takomillashtirish chora-tadbirlari to‘g‘risida”gi PF-5349-son, 2020-yil 5-oktyabrdagi “Raqamli O‘zbekiston- 2030 strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida”gi PF-6079 Farmonlari, 2023-yil 31-maydagi “O‘zbekiston Respublikasining muhim axborot infratuzilmasi obyektlari kiberxavfsizligini ta‘minlash tizimini takomillashtirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi PQ-167-sonli qarori hamda mazkur faoliyatga tegishli boshqa me‘yoriy-huquqiy hujjatlarda belgilangan vazifalarni amalga oshirishga ushbu dissertatsiya tadqiqoti muayyan darajada xizmat qiladi.

**Tadqiqotning respublika fan va texnologiyalari rivojlanishining ustuvor yo‘nalishlariga mosligi.** Mazkur tadqiqot respublika fan va texnologiyalar rivojlanishining IV. “Axborotlashtirish va axborot kommunikatsiya texnologiyalarini rivojlantirish” ustuvor yo‘nalishiga mos ravishda bajarilgan.

**Muammoning o‘rganilganlik darajasi.** Shaxsni biometrik identifikatsiyalash, nutq signallariga raqamli ishlov berish va tanib olish model, usul va algoritmlarini takomillashtirish hamda ishlab chiqish va ularni amaliyotga joriy etish bo‘yicha xorijiy olimlardan<sup>2</sup> L.R. Rabiner, H. Beigi, D.A. Reynolds, P. Nguyen, J.D. Markel, A.H. Grey, J.R. Vacca, J. Chirillo, Y. Liu, Y. Xian, X. Chen, T. Fu, A.A. Lanne, B.M. Lobanov, A.B. Agranovskiy, D.A. Lednov, A. Kozlov, O. Kudashev va boshqalarning ilmiy ishlari diqqatga sazovor.

Respublikamizda axborot xavfsizligini ta‘minlash, axborot tizimi foydalanuvchilarini identifikatsiyalashning nazariy asoslarini rivojlantirishga<sup>3</sup> S.K.Ganiyev, M.M.Karimov, D.T.Muxamediyeva, M.M.Musayev, N.S.Mamatov, Z.T.Xudoykulov, Sh.Z.Islomov va boshqalar o‘zlarining hissalarini qo‘shib kelmoqdalar.

Hozirgi kunda nutq signallariga ishlov berish va tahlil qilish asosida shaxsni biometrik identifikatsiyalash ilovalari, shuningdek, nutq bilan bog‘liq bo‘lgan

---

<sup>2</sup> L.R. Rabiner and R.W. Schafer “Introduction to Digital Speech Processing”; H. Beigi “Fundamentals of Speaker Recognition”; D.A Reynolds, T.F. Quatieri, R.B. Dunn “Speaker verification using adapted Gaussian mixture models”; Ch.Ch. Chiu, T.N. Sainath, Y. Wu, R. Prabhavalkar, P. Nguyen, Z. Chen, A. Kannan, R.J Weiss, K. Rao, E. Gonina, N. Jaitly, B.Li, J. Chorowski, M. Bacchiani “State-of-the-art speech recognition with sequence-to-sequence models”; J.D. Markel, A.H. Gray “Linear Prediction of Speech”; J.R. Vacca “Computer Forensics : Computer Crime Scene Investigation”; J. Chirillo, S. Blaul “Implementing Biometric Security”; K. Chen, D. Zhang, L. Yao, B. Guo, Z. Yu, Y. Liu “Deep learning for sensor-based human activity recognition: Overview, challenges, and opportunities”; Y.Xian, Y. Pu, Z. Gan, L. Lu, A. Thompson “Adaptive DCTNet for audio signal classification”; D. Yu, X. Chen, L. Deng “Factorized Deep Neural Networks for Adaptive Speech Recognition”; Y.Liu, Y. Qian, N. Chen, T. Fu, Y. Zhang, K. Yu “Deep feature for text-dependent speaker verification”; A.A. Lanne, T.V. Merkucheva “Filters with Double Symmetry”; B. Lobanov, L. Tsirulnik, D. Zhadinets, E. Karnevskaia “Language-and speaker specific implementation of intonation contours in multilingual TTS synthesis”; A.B. Agranovskiy, D.A. Lednov “Teoreticheskie aspekti algoritmov obrabotki i klassifikatsii rechevix signalov”; G. Lavrentyeva, S. Novoselov, E. Malykh, A. Kozlov, O. Kudashev, V. Shchemelinin “Audio replay attack detection with deep learning frameworks”

<sup>3</sup> S.K. Ganiyev, Z.T.Khudoykulov “Biometric cryptosystems: Open issues and challenges”; M.M. Karimov; Z.T.Khudoykulov; Sh.Z.Islomov “Biometric Cryptosystem Security Threats”; D.T. Muxamediyeva, N.A. Niyozmatova, R.A. Sobirov, B.N. Samijonov, E.K. Khamidov “Approaches to Solving Problems of Markov Modeling Training in Speech Recognition”; M. Musaev, S. Mussakhojayeva, I. Khujayorov, Y. Khassanov, M. Ochilov, H.A. Varol “USC: An open-source Uzbek speech corpus and initial speech recognition experiments”; N. Mamatov, N. Niyozmatova, A. Samijonov “Software for preprocessing voice signals”;

axborot xavfsizligi texnologiyalari jadal rivojlanmoqda. Ushbu yo‘nalish bo‘yicha o‘tkazilgan tadqiqotlar axborot tizimlarini himoyalashning biometrik texnologiyalari istiqbolli texnologiyalaridan biri ekanligini ko‘rsatdi. Jumladan, shaxsni nutqi asosida identifikatsiyalash ilovalari foydalanuvchi uchun eng qulay identifikatsiyalash usuli bo‘lib, yuqori aniqlikdagi identifikatsiyalashni ta‘minlaydi va xarajatlarni keskin kamaytiradi. Hozirgi kunda shaxsni nutqi asosida identifikatsiyalashni ko‘plab usul va algoritmlari ishlab chiqilganligiga qaramay, ideal bo‘lmagan sharoitlardagi nutq signallari asosida identifikatsiyalashni amalga oshirish, real vaqt rejimi talablariga javob beruvchi usul va algoritmlarni takomillashtirish yoki ishlab chiqish muammosi yetarli darajada o‘rganilmagan.

**Dissertatsiya tadqiqotining dissertatsiya bajarilgan oliy ta‘lim muassasasining ilmiy-tadqiqot ishlari rejalari bilan bog‘liqligi.** Dissertatsiya tadqiqoti Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti ilmiy-tadqiqot ishlari rejasining BV-Atex-2018 (240+147) “Yuz tasvirlarini oqimli qayta ishlash asosida shaxsni identifikatsiya qilish algoritmlari va dasturiy ta‘minotini ishlab chiqish” hamda Raqamli texnologiyalar va sun‘iy intellektni rivojlantirish ilmiy-tadqiqot instituti ilmiy-tadqiqot ishlari rejasining IL-33,41-2105981 “Nutq signallarini qayta ishlash asosida shaxsni tanib olish algoritmlari va dasturiy mahsulotini yaratish” (2021-2023) mavzularidagi loyihalar doirasida bajarilgan.

**Tadqiqotning maqsadi** nutq signallariga dastlabki ishlov berish va tahlil qilish asosida axborot tizimlari foydalanuvchilarini biometrik identifikatsiyalashning tezkor usul, algoritmlari va dasturiy majmuasini ishlab chiqishdan iborat.

**Tadqiqotning vazifalari:**

ovozga asoslangan tizimlar uchun tahdid modelini ishlab chiqish va tahdidlarning risk darajasini hisoblash;

matnga bog‘liq hamda bog‘liq bo‘lmagan ovoz asosidagi autentifikatsiya usullarini takomillashtirish;

axborot tizimlarida foydalanuvchilarning nutq signallariga dastlabki ishlov berish algoritmini takomillashtirish;

foydalanuvchilarni autentifikatsiyalashda nutq signali belgilarini ajratib olish algoritmini ishlab chiqish;

shaxsni nutqi asosida identifikatsiyalashning chuqur neyron tarmoqli modelini ishlab chiqish;

nutq signallari asosida axborot tizimlari foydalanuvchilarini biometrik identifikatsiyalashning dasturiy majmuasini yaratish.

**Tadqiqotning ob‘yekt**i sifatida axborot tizimlari foydalanuvchilarini biometrik identifikatsiyalash jarayoni olingan.

**Tadqiqotning predmetini** shaxsni nutqi asosida biometrik identifikatsiyalashning model, usul va algoritmlari tashkil etadi.

**Tadqiqotning usullari.** Tadqiqotlarni olib borish jarayonida tizimli tahlil, diskret matematika, ehtimollar nazariyasi va matematik statistika, signallarga raqamli ishlov berish, timsollarni tanib olish va mashinali o‘qitish usullaridan foydalanilgan.

**Tadqiqotning ilmiy yangiligi** quyidagilardan iborat:

tahdidlarni tahlil qilish STRIDE metodologiyasi yordamida ovozga asoslangan tizimlar uchun tahdid modeli ishlab chiqilgan va DREAD modeli asosida tahdidlarning risk darajalari hisoblangan;

ovoz ma'lumotlarga dastlabki ishlov berish, belgilarni ajratish va chuqur neyron tarmoqqa asoslangan matnga bog'liq hamda bog'liq bo'lmagan ovoz asosidagi autentifikatsiya usullari takomillashtirilgan;

nutq signalini raqamli shaklga o'zgartirish, ovozdagi harakatsiz sohalarni olib tashlash va filtrlashga asoslangan nutq signallariga dastlabki ishlov berish algoritmi takomillashtirilgan;

mel-chastotali kepsstral koeffitsiyentlar usuliga asoslangan nutq signali belgilarini ajratish algoritmi va ovoz modelini hosil qilishda shaxsni nutqi asosida identifikatsiyalashning chuqur neyron tarmoqli modeli ishlab chiqilgan;

ovozli ma'lumotlarga asoslangan identifikatsiya tizimining har bir algoritmlarini alohida modul sifatida ifodalashga asoslangan axborot tizimlari foydalanuvchilarini biometrik identifikatsiyalashning dasturiy majmuasi yaratilgan.

**Tadqiqotning amaliy natijalari** quyidagilardan iborat:

axborot tizimlariga, kirish-chiqishni nazorat qilish va boshqarish hamda kompyuter tarmoqlarida foydalanuvchilarni identifikatsiyalash tizimini yaratish uchun nutq asosida biometrik identifikatsiyalashning algoritmik ta'minoti ishlab chiqilgan;

nutq signallariga dastlabki ishlov berish algoritmlari, belgilar vektorini shakllantirish algoritmlari va chuqur neyron tarmoq asosida shaxsning ovoz modelini qurish algoritmi hamda identifikatsiyalash muammolarini yechishga mo'ljallangan dasturiy majmua ishlab chiqilgan.

**Tadqiqot natijalarining ishonchliligi** tizim asosini tashkil etuvchi usul va algoritmlarni ishlab chiqishda nutq signallarini ishlash va identifikatsiyalash matematik apparatining to'g'ri qo'llanilganligi, o'tkazilgan tajribaviy va amaliy tadqiqotlarning ijobiy natijalari, hamda ishlab chiqilgan dasturiy majmuani mutasaddi tashkilotlar tomonidan amaliyotga joriy etilganligi bilan izohlanadi.

**Tadqiqot natijalarining ilmiy va amaliy ahamiyati.** Tadqiqot natijalarining ilmiy ahamiyati nutq signallariga raqamli ishlov berish asosida shaxsni nutqi asosida biometrik identifikatsiyalash texnologiyalarining nazariy asoslarini rivojlanishiga ishlab chiqilgan algoritmlarning hissa qo'shishi bilan izohlanadi.

Tadqiqot natijalarining amaliy ahamiyati ishlab chiqilgan dasturiy majmua axborot tizimlarida kirish-chiqishni nazorat qilish va boshqarish tizimlari foydalanuvchilarini identifikatsiyalash muammolarini hal etishda qo'llanilishi bilan izohlanadi.

**Tadqiqot natijalarining joriy qilinishi.** Nutq signallariga raqamli ishlov berish va identifikatsiyalashning mavjud hamda taklif etilgan yondashuv, model, usul va algoritmlari asosida yaratilgan dasturiy majmua asosida:

dissertatsiya ishining ilmiy va nazariy ma'lumotlaridan, shuningdek, shaxsni identifikatsiyalash uchun kod kitoblarini yaratish algoritmi hamda ikki omilli autentifikatsiyalash masalasini yechish uchun so'zlar ketma –ketligini hosil qilish

algoritmi asosida ishlab chiqilgan dasturiy vosita O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligi huzuridagi Bilim va malakalarni baholash agentligining amaliy faoliyatida tatbiq etilgan (BMBA 2024-yil 2-yanvardagi dalolatnomasi; O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligining 2024-yil 19-martdagi 33-8/1867-son ma’lumotnomasi) Mazkur dasturiy majmuani qo‘llash natijasida xodimning ishchi stansiyadan foydalanishning xavfsizlik darajasini ikki barobarga oshirish imkonini bergan;

so‘zlovchini identifikatsiyalash uchun kod kitoblarini yaratish algoritmi hamda ikki omilli autentifikatsiyalash masalasini yechish uchun so‘zlar ketma –ketligini hosil qilish algoritmi asosida ishlab chiqilgan dasturiy vosita Aksiyadorlik tijorat “ALOQABANK” ning amaliy faoliyatida tatbiq etilgan (AT “ALOQABANK” 2024-yil 30-yanvardagi dalolatnomasi; O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligining 2024-yil 19-martdagi 33-8/1867-son ma’lumotnomasi). Erishilgan ilmiy natijalar asosida ishlab chiqilgan dasturiy vosita tashkilotda xodimlarning kirish –chiqishini nazorat qilishga sarflanadigan vaqtni o‘rtacha 15% qisqartirish imkonini bergan;

dissertatsiyada olingan ilmiy natijalar asosida ishlab chiqilgan dasturiy vosita “SERVERCONF” mas’uliyati cheklangan jamiyatning amaliy faoliyatida tatbiq etilgan (“SERVERCONF” MChJ 2024-yil 15-yanvardagi dalolatnomasi; O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligining 2024-yil 19-martdagi 33-8/1867-son ma’lumotnomasi). Dissertatsiyaning ilmiy natijalar asosida ishlab chiqilgan dasturiy vosita tashkilotda qo‘llash natijasi maxsus xonalarning xavfsizlik darajasini oshirish imkonini bergan.

foydalanuvchini nutq ma’lumotlariga asosan identifikatsiya qilish tizimi “Kiberxavfsizlik markazi” davlat unitar korxonasining lokal tarmog‘iga tatbiq etilgan (“Kiberxavfsizlik markazi” DUK 2024-yil 12-fevraldagi dalolatnomasi; O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligining 2024-yil 19-martdagi 33-8/1867-son ma’lumotnomasi). Ishlab chiqilgan dasturiy vosita, axborot tizimlari, kirish-chiqishni nazorat qilish va boshqarish hamda kompyuter tarmoqlarida foydalanuvchilarni kirish-chiqishni nazorat qilishga sarflanadigan vaqtni o‘rtacha 15% ga qisqartirishga imkon bergan.

**Tadqiqot natijalarining aprobatsiyasi.** Mazkur tadqiqot natijalari 2 ta xalqaro va 4 ta respublika ilmiy-amaliy anjumanlarida ma’ruza qilingan va muhokamadan o‘tkazilgan.

**Tadqiqot natijalarining e’lon qilinganligi.** Dissertatsiyaning mavzusi bo‘yicha jami 20 ta ilmiy ish chop etilgan, jumladan, O‘zbekiston Respublikasi Oliy attestatsiya komissiyasining dissertatsiyalarning asosiy ilmiy natijalarini chop etish tavsiya etilgan ilmiy nashrlarida 5 ta xorijiy va 6 ta respublika jurnallarida nashr etilgan hamda EHM uchun yaratilgan 3 ta dasturiy vositalarni qayd etish guvohnomalari olingan.

**Dissertatsiyaning tuzilishi va hajmi.** Dissertatsiya kirish, to‘rtta bob, xulosa, foydalanilgan adabiyotlar ro‘yxati va ilovalardan iborat. Dissertatsiyaning hajmi 99 sahifani tashkil etadi.

## DISSERTATSIYANING ASOSIY MAZMUNI

**Kirish** qismida dissertatsiya mavzusining dolzarbligi va zaruriyati asoslangan, tadqiqotning O‘zbekiston Respublikasi fan va texnologiyalari rivojining ustuvor yo‘nalishlariga mosligi ko‘rsatilgan, maqsad va vazifalar shakllantirilgan, tadqiqot obyekti va predmeti aniqlangan, tadqiqotning ilmiy yangiligi va amaliy natijalari ko‘rsatib o‘tilgan, olingan natijalarning ishonchliligi asoslangan, ularning nazariy va amaliy ahamiyati ochib berilgan, tadqiqot natijalarining amaliyotga tatbiq etilishi, nashr etilgan ishlar va dissertatsiya tuzilishi bo‘yicha ma‘lumotlar keltirilgan.

Dissertatsiyaning **“Biometrik parametrlar asosida shaxsni tanib olish texnologiyalari”** deb nomlangan birinchi bobida biometrik parametrlar asosida shaxsni tanib olish texnologiyalari tahlil qilingan. Shuningdek, shaxsni ovozi asosida identifikatsiyalashga qaratilgan tahdidlar hamda shaxsni nutq asosida identifikatsiyalash texnologiyasining qo‘llanilish sohalari va muammolari o‘rganilgan.

*Birinchi paragrafda* biometrik parametrlar asosida shaxsni tanib olish texnologiyalari tahlili keltirilgan. Biometrik identifikatsiyalash usullari odatda ikki guruhga ajratiladi: fiziologik va xulq-atvor. Fiziologik identifikatsiyalash usullari barmoq yoki kaft izlari, ko‘z qorachig‘i yoki rangdor parda, 2 o‘lchovli va 3 o‘lchovli yuz tasvirlari va boshqalar kabi xususiyatlardan foydalanishdan iborat bo‘lsa, xulq-atvorga asoslangan parametrlarga inson ovozi, klaviaturada yozish uslubi, harakat tarzi kabilarni kiritish mumkin.

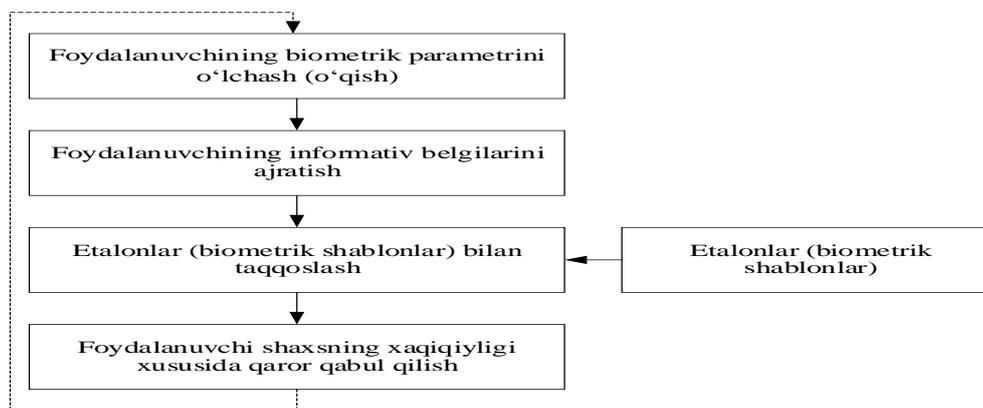
Har qanday biometrik tizim ishlashi asosida quyidagi harakatlar zanjiri yotadi (1-rasm):

– *yozish* - foydalanuvchining biometrik malumotlari skaner yordamida o‘qiladi;

– *ajratish* - taqdim etilgan biometrik malumotlardan noyob axborot tanlab olinadi va bu axborot muayyan shaxsning biometrik “obrazi” hisoblanadi;

– *taqqoslash* - taqdim etilgan biometrik obrazni tizim ma‘lumotlar bazasida saqlanuvchi bitta yoki ko‘p sonli etalonlar (shablonlar) bilan taqqoslash amalga oshiriladi;

– *qaror qabul qilish* - tizim biometrik obrazlar mosligini yoki mos emasligini hal etib identifikatsiya protsedurasining tuganlanganligi, uni takrorlash yoki o‘tkazish shartlarini o‘zgartirish xususida qaror qabul qiladi.



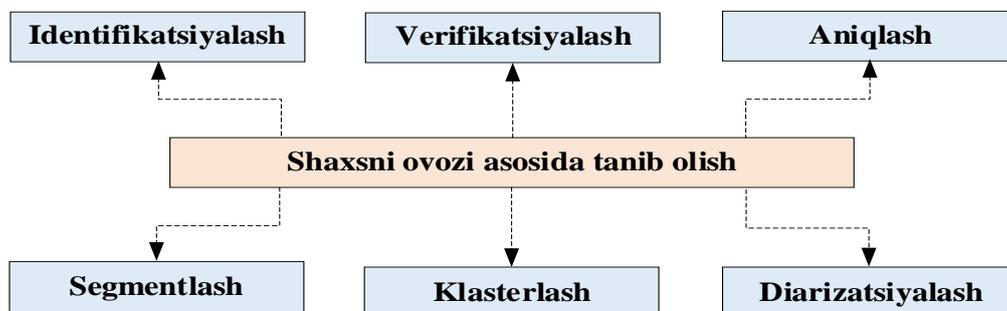
**1 -rasm. Biometrik identifikatsiya protsedurasi**

*Ikkinchi paragrafda* shaxsni ovozi asosida identifikatsiyalash tizimlariga qaratilgan tahdidlar tahlili amalga oshirilgan. Amalda ovozga asoslangan identifikatsiyalash tizimlarida ko‘plab tahdidlar, xususan, ovozni qalbakilashtirish, ovozni ko‘chirib qayta foydalanish, tizimni aldash, xizmat ko‘rsatishdan voz kechishga undash kabilar keng uchraydi. Shu sababli, keyingi bobda ishlab chiqiladigan ovozga asoslangan identifikatsiyalash tizimi uchun tahdid modelini ishlab chiqish, ularda mavjud risk darajalarini aniqlash masalasi bilan batafsil tanishib chiqiladi.

*Uchunchi paragrafda* shaxsni nutq asosida identifikatsiyalash texnologiyasining qo‘llanilish sohalari va ulardagi muammolar tahlil qilingan. Ovozga asoslangan xavfsizlik ilovalari asosan moliyaviy, firibgarlikni passiv nazoratlash, kriminalistika muammolarini yechish, tashkilotlarda kirishni nazoratlash, audio va video kontentlarni indekslash, videokuzatuv masalalarida qo‘llanilishi aniqlandi. Bundan tashqari ushbu tizimlarda jummalarning qisqaligi, ovoz fonidan shovqinning mavjud bo‘lishi, ularning real vaqt tizimida ishlashi bilan bog‘liq ko‘plab muammolar kuzatilishi tahlillar natijasida aniqlandi.

Dissertatsiyaning **“Shaxsni ovozi asosida biometrik identifikatsiyalashning zamonaviy holati”** deb nomlangan ikkinchi bobida shaxsni ovozi asosida identifikatsiyalash tizimining asosiy masalalari va ovoz asosidagi ilovalar uchun tahdid modeli keltirilgan hamda matnga bog‘liq va bog‘liq bo‘lmagan ovoz asosidagi autentifikatsiya usullari taklif qilingan.

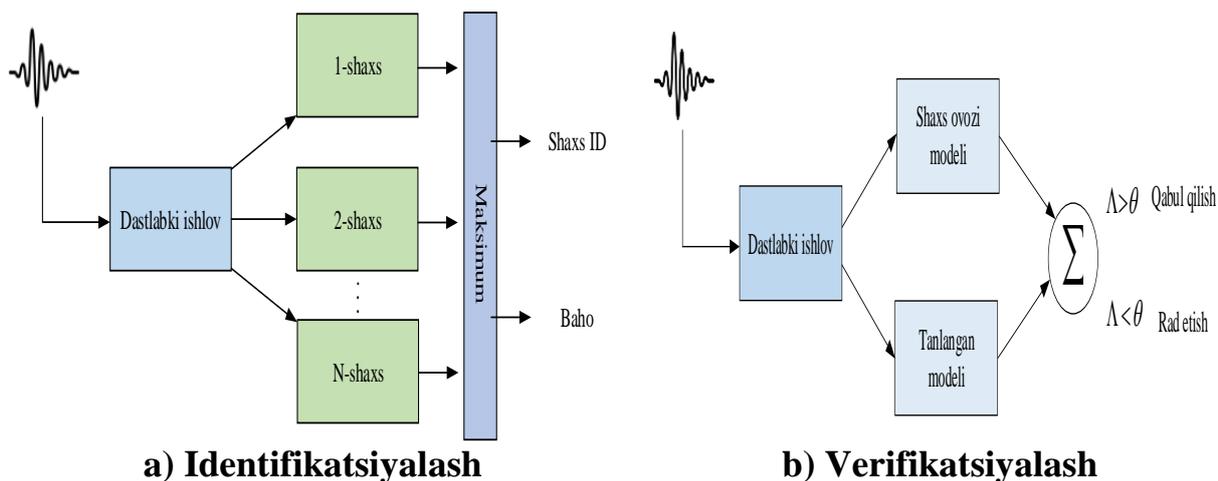
*Birinchi paragrafda* shaxsni ovozi asosida identifikatsiyalash tizimining asosiy masalalari tahlil qilingan. Umumiy holda shaxsni tanib olishda ko‘plab masalalar yechilib, ularning muhimlari 2-rasmda keltirilgan.



**2-rasm. Shaxsni ovozi asosida identifikatsiyalash tizimi qamrab olgan masalalar**

Ushbu masalalardan amalda keng qo‘llaniladigani shaxsni ovozi asosida identifikatsiyalash bo‘lib, u noma‘lum shaxsni ovozi bo‘yicha oldindan aniqlangan shaxslar to‘plamidagi ma‘lum bir shaxsga bog‘lash bilan shug‘ullanadi. Shaxsni ovozi asosida verifikatsiyalash (autentifikatsiyalash) rejimi ikki toifali (binar) tasniflash vazifasiga mos keladi, bunda testlash namunasi to‘plami bir xil shaxslarga tegishlimi yoki yo‘qmi degan savol qiziqtiradi.

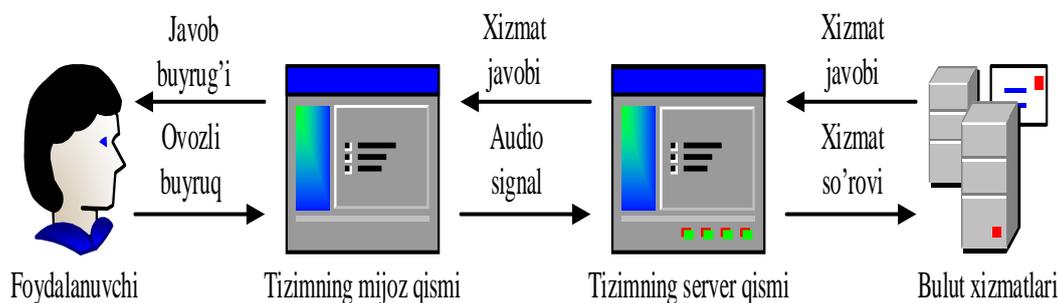
Shaxsni identifikatsiyalash va verifikatsiyalash tizimlarining asosiy tuzilmalari mos ravishda 3- (a) va (b) rasmlarda keltirilgan, bu ikki tizimda ham nutq signaliga birinchi navbatda shaxs haqida ma‘lumot beruvchi xususiyatlarni tanlash uchun, ishlov beriladi.



**3-rasm. Identifikatsiyalash va verifikatsiyalash tizimlarining tuzilishi**

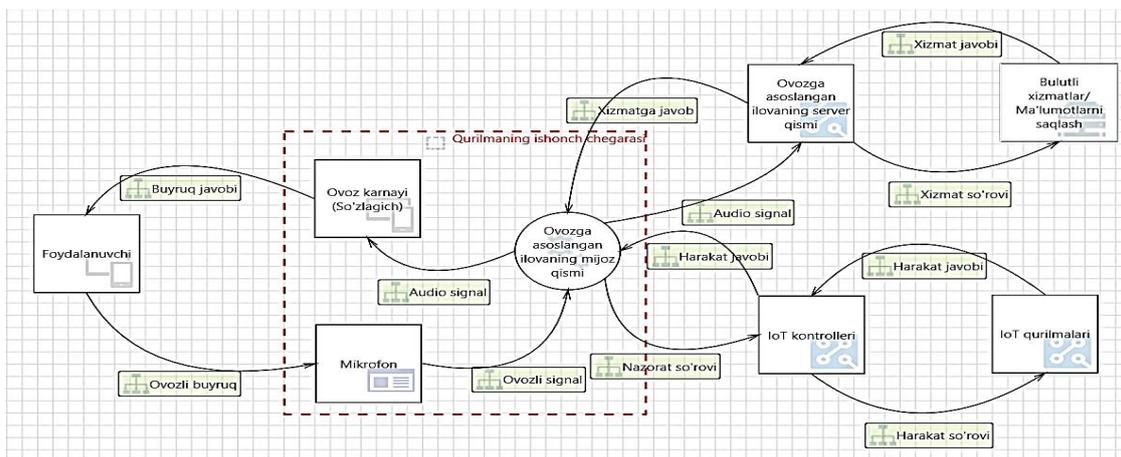
*Ikkinchi paragrafda ovozga asoslangan ilovalar uchun amalga oshirishda bo‘lishi mumkin bo‘lgan tahdidlar va risklarning tahlili bilan tanishib chiqiladi. Xususan, STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of privileges) metodologiyasi bo‘yicha tahdidlarni tasniflash, DREAD (Damage Potential, Reproducibility, Exploitability, Affected Users, Discoverability) modeli bo‘yicha tahdid risklarini baholash va ularga qarshi himoya choralalarini ko‘rish masalalari ko‘rib chiqiladi.*

Umumiy holda, ovozga asoslangan ilovalarni 4-rasmdagi kabi tasvirlash mumkin. Unga ko‘ra dastlab, foydalanuvchi tomonidan aytilgan buyruq (signal) foydalanuvchi tomonidagi tizimning mijoz qismiga kiritiladi. Ushbu qismtizim qabul qilingan ovoz buyrug‘ini audio signalga aylantirib, ishlash uchun tizimning server qismiga junatadi. Kiritilgan ma‘lumotga asosan server mos javobni hosil qiladi va uni mijozga qaytarishi yoki biror ruxsatni nazoratlash tizimidagi amalni (masalan, ruxsat berish) bajarishi mumkin. Bulutli xizmat mazkur arxitekturada tanlovga ko‘ra amalga oshirilib, ma‘lumotni saqlash yoki biror xizmatni amalga oshirishi mumkin bo‘ladi.



**4-rasm. Ovozga asoslangan ilovalar arxitekturasi**

Tahdidni modellashtirishda dastlabki qadamlardan biri-avtomatlashtirilgan tizimlar yordamida mavjud tahdidlarni aniqlash. Ushbu vazifani bajarishda Microsoft Threat Modeling Tool v.7.3.31026.3 vositasidan foydalanildi. Umumiy holda ovozga asoslangan ilovalar uchun DFD (Data Flow Diagram) ko‘rinish 5-rasmda keltirilgan.



**5-rasm. Ovozga asoslangan ilovalar uchun DFD. Qizil rangli to'rtburchak ovozga asoslangan tizim qurilmasini ifodalaydi.**

Bunda dastlab foydalanuvchi tomonidan aytilgan buyruq mikrofon orqali tizimning mizoj qismiga audio signal sifatida yetkaziladi. Ilovaning mijoz qismi muhim ahamiyat kasb etib, ma'lumotni tizimning server qismiga va undan olingan javob asosida IoT kontrolleriga yuboradi. Bundan tashqari, amalga oshirilgan hakaratlar bo'yicha ovozi karnay orqali foydalanuvchi xabar yetkazadi. O'z navbatida ilovaning server tomoni o'z faoliyatini yuritishda bulutli xizmatlardan yoki ma'lumotlarni saqlash tizimlaridan foydalanishi mumkin. IoT kontrolleri esa bir necha IoT qurilmalarini boshqarish orqali biror xavfsizlik harakatini (masalan, eshikni ochish) amalga oshirishi mumkin.

**1-jadval**

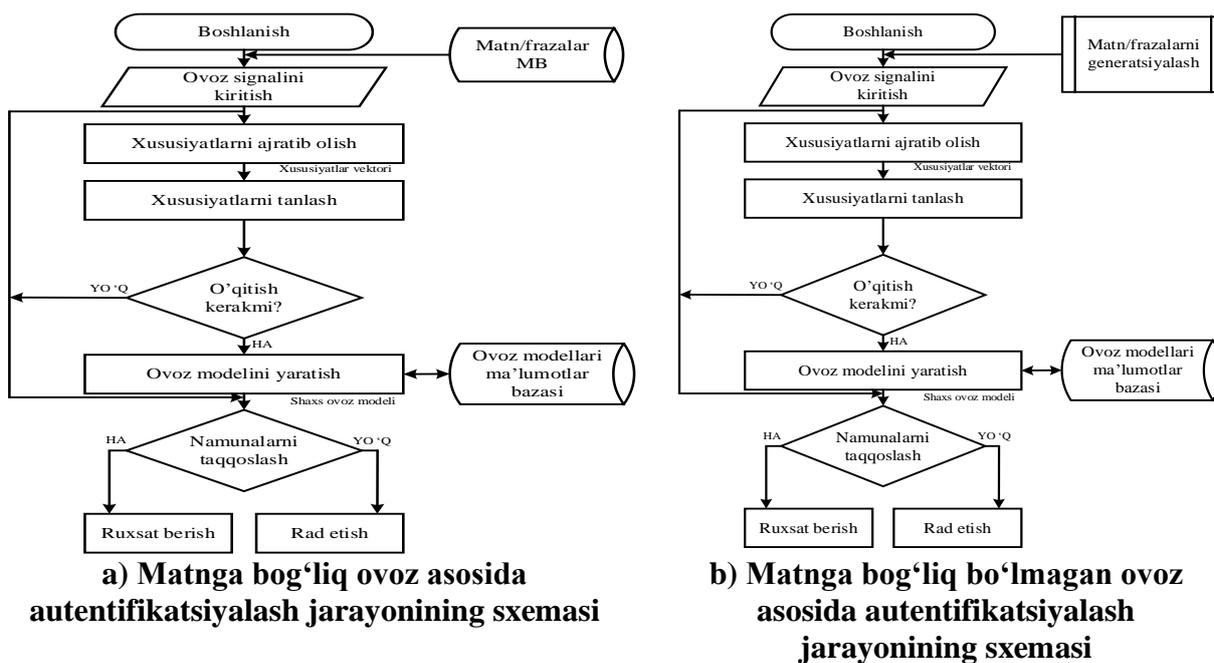
**Ovozga asoslangan tizimdagi tahdidlar va ularning risk tahlili**

| Ma'lumot oqimi                         | Tahdid                                  | D         | R         | E         | A         | D         | Umumiy (D+R+E+A+D)/5 |
|--|---|-----------|-----------|-----------|-----------|-----------|----------------------|
| Audio signal (M→C)                     | Soxtalashtirish                         | 0         | 0         | 10        | 5         | 0         | 3                    |
| Ovozli buyruq (foydalanuvchi→mikrofon) | <b>Soxtalashtirish</b>                  | <b>10</b> | <b>10</b> | <b>10</b> | <b>10</b> | <b>10</b> | <b>10</b>            |
|  | O'zgartirish                            | 10        | 0         | 0         | 10        | 0         | 4                    |
|  | Xizmat ko'rsatishdan voz kechish        | 0         | 10        | 0         | 10        | 0         | 4                    |
| Xizmat javobi (S→M)                    | <b>O'zgartirish</b>                     | <b>10</b> | <b>10</b> | <b>10</b> | <b>10</b> | <b>5</b>  | <b>9</b>             |
|  | Axborotni oshkor bo'lishi               | 10        | 10        | 10        | 10        | 0         | 8                    |
|  | Xizmat ko'rsatishdan voz kechish        | 0         | 10        | 5         | 10        | 10        | 7                    |
| Nazorat so'rovi                        | Imtiyozlarni ortishi                    | 10        | 10        | 0         | 10        | 0         | 6                    |
|  | Soxtalashtirish                         | 10        | 10        | 5         | 10        | 0         | 7                    |
|  | <b>O'zgartirish</b>                     | <b>10</b> | <b>10</b> | <b>5</b>  | <b>10</b> | <b>10</b> | <b>9</b>             |
| Harakat javobi                         | Soxtalashtirish                         | 0         | 10        | 5         | 10        | 10        | 7                    |
|  | O'zgartirish                            | 0         | 10        | 0         | 10        | 10        | 6                    |
|  | Axborotni oshkor bo'lishi               | 10        | 10        | 5         | 5         | 0         | 6                    |
|  | <b>Xizmat ko'rsatishdan voz kechish</b> | <b>10</b> | <b>10</b> | <b>10</b> | <b>10</b> | <b>10</b> | <b>10</b>            |
|  | Imtiyozlarni ortishi                    | 10        | 0         | 0         | 0         | 0         | 2                    |
| Buyruq javobi                          | Axborotni oshkor bo'lishi               | 0         | 10        | 10        | 10        | 0         | 6                    |

Microsoft Threat Modeling Tool v.7.3.31026.3 vositasi yordamida olingan tahlil natijalari va tahdidlarning risk darajalari 1-jadvalda keltirilgan. DREAD modelidan foydalanib, quyidagi tarzda tavsiflangan besh toifaning har biriga tegishli tahdidning jiddiyligini raqamli qiymatlar (0 (quyi, qiyin), 5 (oʻrta) va 10 (yuqori, oson)) bilan aniqlash mumkin. Yakuniy reytingni hisoblashda tahdidning noravshan darajasi va uning sonli qiymatlari quyidagi tartibda belgilandi: yuqori (8-10), oʻrta (4-7) va quyi (0-3).

1-jadvalga, koʻra 2 ta quyi risk darajasiga, 10 ta oʻrta risk darajasiga va 4 ta yuqori risk darajasiga ega tahdidlar mavjud. Masalan, mikrofonga nisbatan soxtalashtirish tahdidiga koʻra autentifikatsiya mexanizmi mavjud boʻlmaganida, haqiqiy foydalanuvchini soxtalashtirish yoki ovozni obroʻsizlantirish imkoniyati mavjudligi sababli, qonuniy foydalanuvchilarning imtiyoziga ega boʻlishi mumkin. Shuning uchun,  $D = 10$  ga teng. Ushbu tahdidni amalga oshirish uchun qimmat boʻlmagan jihozlar talab etilgani bois,  $E = 10$  ga teng boʻlsa, hujumni amalga oshirish osonligi sababli,  $R = 10$  ga teng boʻladi. Aksariyat tizimlarda xavfsizlik masalasiga eʼtibor berilmaganligi, tizimning ovozni haqiqiyligini aniqlashning imkoni yoʻqligi sababli  $D = 10$  ga teng boʻladi. Va nihoyat, bu turdagi tahdidlar foydalanuvchiga jiddiy taʼsir qilgani bois  $A = 10$  ga teng boʻladi. Ushbu tahdid uchun umumiy risk darajasi 10 ga teng boʻladi.

*Uchinchi paragrafda* matnga bogʻliq va matnga bogʻliq boʻlmagan holda ovoz asosida autentifikatsiyalash usullarini ishlab chiqish masalasi koʻrib oʻtilgan. Soʻzlovchining modeli (odatda belgilar taqsimoti qiymati) – ovoz asosida autentifikatsiya tizimida qayd etilgan inson xarakteristikasi. Nutqni kiritish xiliga bogʻliq holda aniqlash tizimini ikki turga ajratish mumkin: matnga bogʻliq va matnga bogliq boʻlmagan tizimlar. Nutqni aniqlashning matnga bogʻliq tizimida foydalanuvchi oldindan maʼlum matn/iboralarni talaffuz qilish lozim. Ogʻzaki matn/iboralarni oldindan bilishda yaxshi aniqlik darajasiga erishiladi, ammo niyati buzuvchi tizim xavfsizligini buzish uchun haqiqiy foydalanuvchi matnini yozib olishi va keyinchalik tadqiqlashi mumkin.



**a) Matnga bogʻliq ovoz asosida autentifikatsiyalash jarayonining sxemasi**

**b) Matnga bogʻliq boʻlmagan ovoz asosida autentifikatsiyalash jarayonining sxemasi**

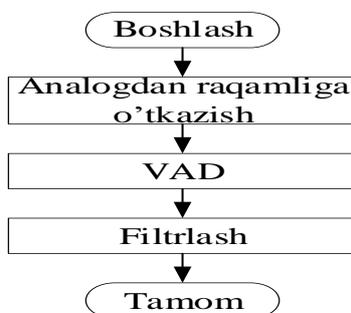
**6-rasm. Matnga bogʻliq hamda bogʻliq boʻlmagan ovoz asosida autentifikatsiyalash sxemalari**

Nutqni aniqlashning matnga bog‘liq bo‘lmagan tizimda foydalanuvchidan oldindan ma’lum matn/iboralar kutilmaydi. Foydalanuvchi tasodif tanlangan matn/iboralarni talaffuz etishi mumkin. Aniqlashning matnga bog‘liq bo‘lmagan tizimi ishlatishda moslanuvchan, ammo, matnga bog‘liq tizimga qaraganda aniqligi past. Matnga bog‘liq tizimga o‘xshab matnga bog‘liq bo‘lmagan tizim ham qayta tiklash hujumidan zarar ko‘radi.

Ushbu ikki holatda autentifikatsiyalash jarayonining blok sxemalari 6(a) va 6(b)-rasmlarda keltirilgan.

Dissertatsiyaning “**Nutq signallariga ishlov berish hamda nutq asosida shaxsni tanib olish usul va algoritmlari**” deb nomlangan uchinchi bobida nutq signali va unga dastlabki ishlov berish va nutq signali belgilarini ajratish algoritmlari keltirilgan hamda chuqur neyron tarmog‘iga asoslangan shaxsni ovozi asosida identifikatsiyalash modeli taklif qilingan.

*Birinchi paragrafda* nutq signaliga dastlabki ishlov berish algoritmi taklif etilgan (7-rasm). Ushbu algoritm u 3 ta bosqichdan iborat: analog shakldagi signalni raqamli shaklga o‘tkazish, VAD va filtrlash.



**7-rasm. Dastlabki ishlov berish algoritmi**

Dastlabki ishlov berish signal belgilarini ajratib olish bosqichiga tayyorlash uchun amalga oshiriladi. Signalga ichki organlar, tana yoki qo‘l harakatlari va h.k. sabab bo‘lgan shovqin ta’sir qilishi mumkin. Dastlabki ishlov berish quyidagi bosqichlarda amalga oshiriladi:

1) Past chastotalar filtrida keraksiz yuqori chastotali shovqin olib tashlanadi, ya’ni, 300 Gs chastotali elliptik past o‘tish filtri qo‘llaniladi.

2) Shovqinni olib tashlashda ma’lum bir chegaradan yuqori qiymatlar portlash shovqinini minimallashtirish uchun chegaralar bilan tenglashtiriladi.

3) Amplitudani normallashtirishda barcha signallar  $[-1,1]$  oralig‘iga keltiriladi.

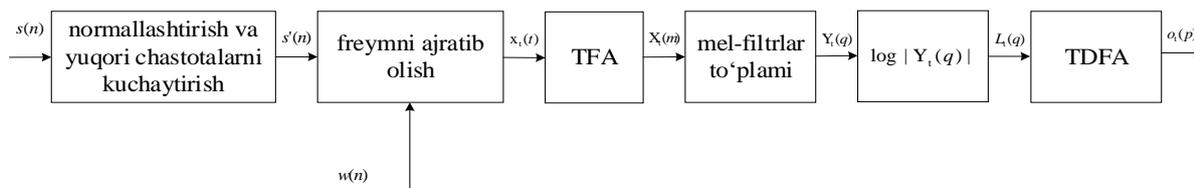
Analog shakldan raqamli shaklga o‘tkazish. Analog shakldagi signallarni raqamli shaklga keltirishda quyidagi uchta jarayonni ko‘rsatish mumkin: diskretlash, kvantlash va kodlash.

VAD. Ovozli aloqada signalda nutq ma’lumotlari joylashgan oraliq nutq faol sohasi deb ataladi. Fon shovqinini mavjudligi yoki mavjud emasligidan qat’iy nazar, nutq ma’lumotlarini o‘z ichiga olmaydigan oraliq to‘xtash joylari deb ataladi. Adabiyotlarda nutq faolligi vaqt chegaralarini aniqlash algoritmi VAD (Voice Activity Detection) deb ataladi. VAD algoritmi signalni ikkita faollik A (activity) va S (silence) to‘xtash segmentga ajratish imkonini beradi.

Filtrlash. Nutq signalini oldindan qayta ishlashning navbatdagi bosqichi

tovushning odamlarga eshitilmaydigan qismlarini kamaytirish uchun chastotalar sohasida filtrlashdan iborat. Buning uchun amplitudali xususiyatlarga ega yuqori o'tkazuvchan filtri (22-tartibli 2-turdagi Chebyshev filtri)dan foydalanilgan. Mazkur holda filtr parametrlari optimallashtirish jarayoni orqali tanlandi.

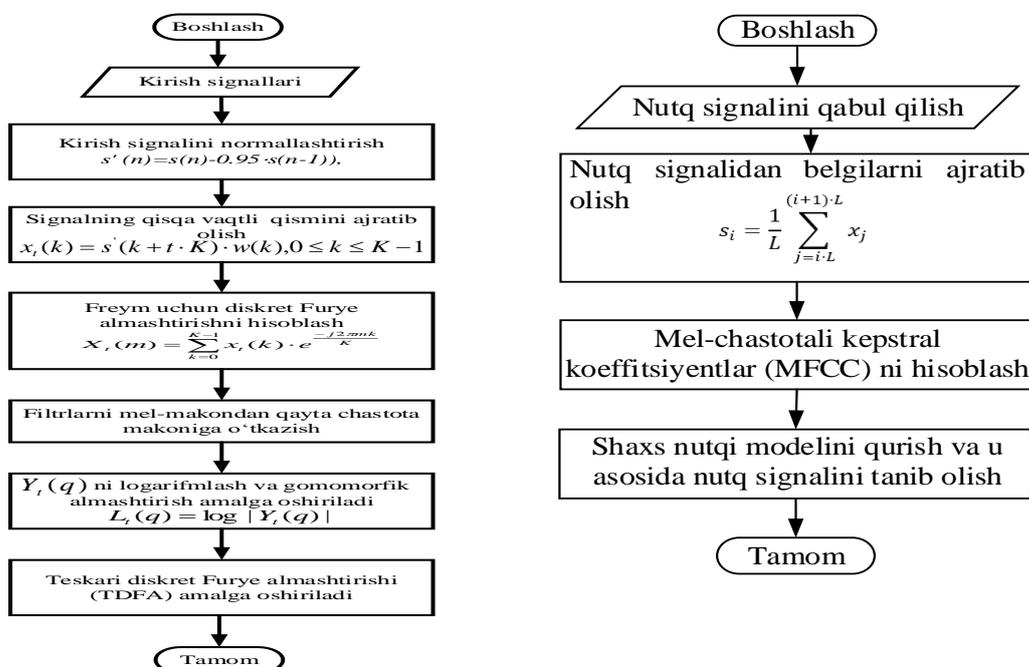
Ikkinchi paragrafda nutq signali belgilarini ajratish algoritmlarini ishlab chiqish masalasi ko'rib o'tilgan. Tanib olish tizimlari samaradorligi ajratib olingan belgilarga bevosita bog'liq. Dastlabki belgilar majmui qanchalik aniq shakllantirilsa, tanib olish ham shunchalik aniq bo'ladi. Nutq signalining shunday belgilarini ajratib olish kerakki, ular yordamida tilning turli fonemalarini ajratib olish mumkin bo'lsin.



**8-rasm. Mel- chastotali keprstral ko'effitsiyentlarini aniqlash bosqichlari**

Mazkur masalani yechishda bugungi kunda belgilarni ajratib olishning eng mashhur usuli – mel chastotali keprstral ko'effitsiyentlarini topish usulidan foydalanildi. Mel-chastotali keprstral ko'effitsiyentlarini aniqlash bir necha bosqichda amalga oshiriladi (8-rasm):

Yuqorida keltirilgan algoritmlarning qiyosiy tahlili 2-jadvalda keltirilgan. Bunda 100 ta shaxs (74 ta erkak kishi va 26 ta ayol kishi) nutqlaridan foydalanildi. Xar bir shaxs uchun 10 ta nutq fayli mavjud shundan 5 tasi o'qitish uchun va qolgan 5 tasi test uchun ishlatildi. Har bir fayl davomiyligi 2-5 sekund.



**a) Nutq signali belgilari vektorini shakllantirish algoritmi**

**b) Tizim ishlash uchun sarflanadigan vaqtni kamaytirishga imkon beruvchi algoritmi**

**9-rasm. Nutq signali belgilari vektorini shakllantirish va ajratib olish algoritmlari**

Nutq signali belgilari vektorini shakllantirish algoritmi 9(a)-rasmda keltirilgan (*A1 algoritm*). 9(b)-rasmda tizim ishlashi uchun sarflanadigan vaqtni kamaytirishga imkon beruvchi algoritm taklif etiladi (*A2 algoritm*).

2-jadval

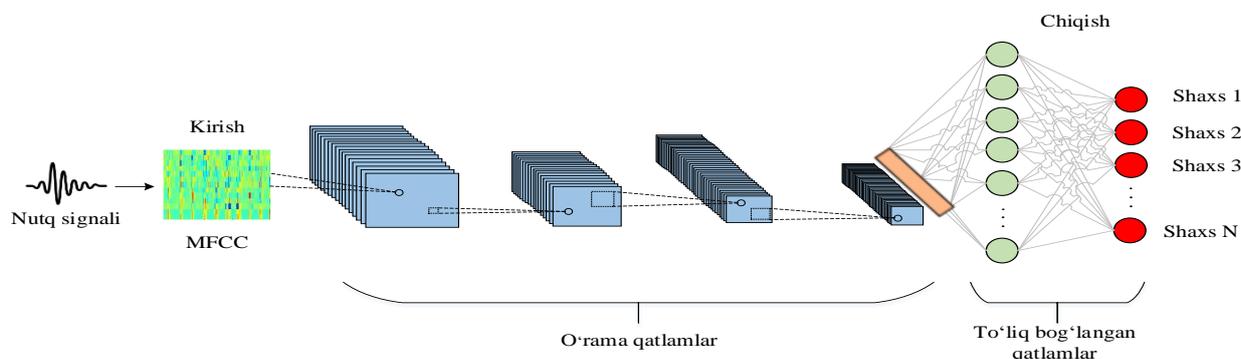
Algoritmning qiyosiy tahlili

| Ko'rsatkichlar<br>Algoritm | Ma'lumotlar hajmi (MB) | Natija (%) | O'qitish uchun sarflangan vaqt (sek.) | Tanib olishga sarflangan vaqt (sek.) |
|----------------------------|------------------------|------------|---------------------------------------|--------------------------------------|
| Asosiy (A1)                | 285,3                  | 99,6       | 45,3                                  | 69,3                                 |
| Taklif etilayotgan (A2)    | 31,5                   | 98,4       | 6,7                                   | 13,1                                 |

Jadvaldan ko'rinib turibdiki, tizim ishlashi uchun sarflanadigan vaqtning kamayishiga asosan belgilar sonining kamaytirish hisobiga erishilgan.

*Uchinchi paragrafda* chuqur neyron tarmog'iga asoslangan shaxsni ovozi asosida identifikatsiyalash modelini ishlab chiqish masalasi bilan tanishib chiqiladi.

Ushbu ishda shaxsni ovozi asosida uni modelini yaratish uchun chuqur neyron tarmog'idan foydalanildi. Chuqur neyron tarmoq o'ramli neyron tarmoqlari CNN ga asoslangan bo'lib, unda d-vektorli yondashuvdan foydalanildi. Qatlamlar va sig'imlarning o'zgaruvchanligiga qaramasdan, barcha tizimlar bir xil muhim elementlarni, ya'ni kadr darajasida ishlaydigan qismni (convolution), birlashtirish (polling), modellarni giperfazodagi joylashuvini hisoblash uchun to'liq bog'langan (fully connected) qatlamli segment darajasidagi qismlarni o'z ichiga oladi. Birlashtirish qatlamining asosiy g'oyasi o'rtacha (average polling) yoki o'rtacha standart og'ish (statistical polling) ni hisoblash orqali barcha kirish freymlari bo'yicha ma'lumotni jamlashdan iborat. O'ramli chuqur neyron tarmoq arxitekturasi 10-rasmda keltirilgan.

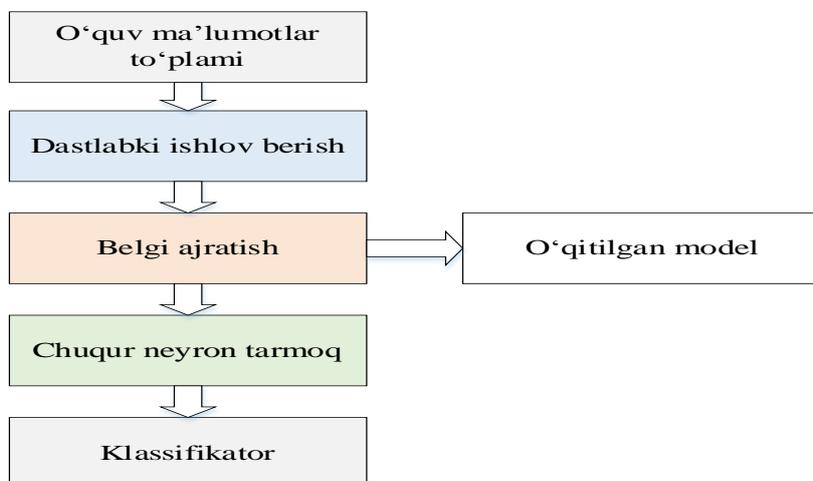


10-rasm. O'ramli chuqur neyron tarmoq arxitekturasi

Chuqur neyron tarmoq asosida shaxsni ovozi asosida tanib olish modelining tashqi shovqinlarga bardoshlilikini oshirish maqsadida nutq signalini ishlashda ma'lumotlar augmentatsiyasidan foydalanildi.

Tajribalar uchun ikki turdagi belgilar to'plamini ajratish funksiyalaridan foydalanilgan: mel-masshtablangan filtr banklar (*A3 algoritm*) va mel-chastotali kepsstral koefitsiyentlar (*A4 algoritm*). Ma'lumotlarni qayta ishlashdan oldin 4 soniyadan qisqaroq audio segmentlar o'qitish ma'lumotlar to'plamidan chiqarib tashlandi. O'qitish va testlash ma'lumotlar to'plamidagi har bir jumla uchun bir xil qayta ishlash konveyeri qo'llanilgan.

Tajribalarning birinchi qismida har bir kadr uchun A3 algoritmi asosida 60 ta mel-masshtablangan filtr banklari va ikkinchi qismida esa har bir kadr uchun A4 algoritmi asosida 20 ta mel-chastotali keprstral koeffitsiyentlar olingan. Chuqur neyron tarmoqni o‘qitish asosida shaxsni identifikatsiyalash modeli 11-rasmda keltirilgan.



**11-rasm. Chuqur neyron tarmog‘ini o‘qitish asosida shaxsni identifikatsiyalash modeli**

Chuqur neyron tarmoqni o‘qitish uchun tajribaviy tadqiqotlar Python dasturlash tilida olib borildi. Har bir model GeForce GTX 1080 grafik protsessorida 100 ta epoxada o‘qitildi. Chuqur neyron tarmoqni o‘qitish natijalari 3-jadvalda keltirilgan.

**3-jadval**

**Chuqur neyron tarmoqni o‘qitish natijalari**

| Diskretlash | Belgi shakllantirish | Aniqlik (%) | Xatolik (Loss) |
|-------------|----------------------|-------------|----------------|
| A1          | A3                   | 94,74       | 0,302          |
| A2          | A3                   | 95,78       | 0,292          |
| A1          | A4                   | 92,62       | 0,351          |
| A2          | A4                   | 93,95       | 0,321          |

Jadvaldan ko‘rinib turibdiki chuqur neyron tarmoqni o‘qitishda taklif etilgan A2, A3 algoritmlari va chuqur neyron tarmoq modelidan foydalanganda 95,78% aniqlik va 0,292 xatolik, A2, A4 algoritmlari va chuqur neyron tarmoq modelidan foydalanganda 93,95% aniqlik va 0,321 xatolik bilan eng yaxshi natijaga erishildi

Dissertatsiyaning “**Dasturiy ta‘minot va uning amaliy masalalarda qo‘llanilishi**” deb nomlangan to‘rtinchi bobida nutq signallari asosida axborot tizimlari foydalanuvchilarini biometrik identifikatsiyalash dasturiy majmuasi ishlab chiqilgan hamda dasturiy majmua modullari batafsil yoritilgan. Shuningdek, dasturiy majmua ustida tajriba tadqiqotlari va uni amaliyotga tatbiq etish natijalari keltirilgan.

*Birinchi paragrafda* nutq signallari asosida axborot tizimlari foydalanuvchilarini biometrik identifikatsiyalash dasturiy majmuasini yaratish masalasi va uning tavsifi keltirilgan. Ro‘yxatdan o‘tkazilgan shaxslar ma‘lumotlarini saqlash uchun dasturiy majmuada ma‘lumotlar bazasi yaratilgan,

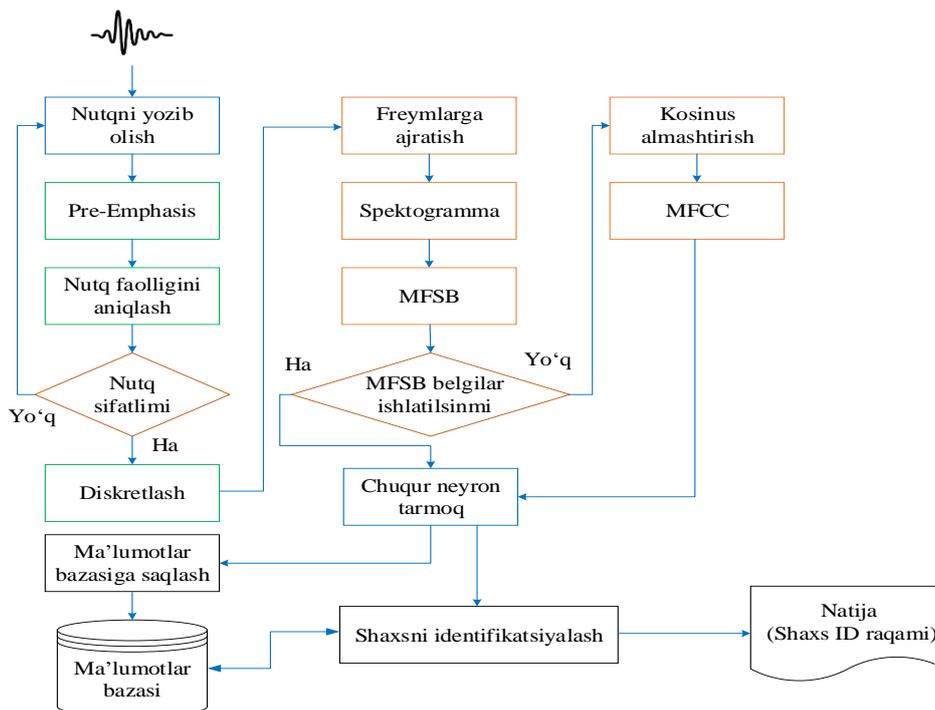
buning uchun SQLite ma'lumotlar bazasini boshqarish tizimidan va chuqur neyron tarmoqlari bilan ishlash uchun PyTorch kutubxonasidan foydalanilgan.

Modullik prinsipi asosida ishlab chiqilgan shaxsni nutqi asosida biometrik identifikatsiyalash / autentifikatsiyalash dasturiy majmuaning umumlashtirilgan sxemasi 12-rasmda keltirilgan.

*Ikkinchi paragrafda* dasturiy majmuaning modullari bayon etilgan.

Ishlab chiqilgan dasturiy majmua normallashtirish, shovqindan tozalash, silliqlash, Mel-masshtablangan filtr banklar, Delta-delta kabi modullardan iborat.

*Uchinchi paragrafda* dasturiy majmua ustida tajriba tadqiqotlari va uni amaliyotga tatbiq etish natijalari keltirilgan.



**12-rasm. Shaxsni ovozi asosida identifikatsiyalash dasturiy majmuasining umumlashtirilgan sxemasi**

Dissertatsiya ishi doirasida ishlab chiqilgan ovoz signallari asosida identifikatsiya/ autentifikatsiyalash dasturiy majmuasining mamlakatimiz iqtisodiyot sohalariga tatbiq etildi va olingan natijalar 4-jadvalda aks ettirilgan.

**4-jadval**

**Tanib olish ko'rsatkichlari**

| <b>Xususiyatlar</b>  | <b>Shaxslar soni</b> | <b>O'rganiluvchi ovozi signallar soni. Bitta shaxs/jami</b> | <b>Yolg'ondan rad etish xatoligi, %</b> | <b>Aniqligi, %</b> |
|--|----------------------|---|---|--------------------|
| <b>Ovozli signallar bazasi</b>                             |                      |   |   |                    |
| Davlat test markazining ovozli signallar bazasi            | 50 ta                | 40-50/2300  | 9,0                                     | 91,0               |
| Aksiadorlik tijorat "ALOQABANK" da ovozli signallar bazasi | 20 ta                | 20-30/955   | 10                                      | 90                 |
| SERVERCONF MCHJ Ovozli signallar bazasi                    | 60 ta                | 50-60/2755  | 9,1                                     | 90,9               |
| "Kiberxavfsizlik markazi" DUK                              | 30 ta                | 30-40/1850  | 9,1                                     | 91,1               |

Jadvaldan ko‘rinib turibdiki, ishlab chiqilgan dasturiy majmua soha korxonalarida identifikatsiyalash masalasini yechishda qo‘llanilib, o‘rtacha 90% aniqlik ko‘rsatkichi va 9% ga yaqin yolg‘ondan rad etish xatoligini ko‘rsatdi.

## XULOSA

“Axborot tizimlari foydalanuvchilarining ovozi bo‘yicha biometrik autentifikatsiyalash modeli va algoritmlari” mavzusidagi dissertatsiya ishi bo‘yicha olib borilgan tadqiqotlar natijasida quyidagi xulosalar taqdim etildi:

1. STRIDE metodologiyasi yordamida ovozga asoslangan tizimlar uchun tahdid modeli ishlab chiqildi va DREAD modeli asosida tahdidlarning risk darajalari hisoblandi. Ilmiy tadqiqot natijasida mikrofoniga nisbatan soxtalashtirish va ovozga asoslangan ilovaning mijoz qismini foydalanishdan bosh tortishga majburlash tahdidlari eng yuqori risk darajasiga egaligi aniqlandi.

2. Ovoz ma‘lumotiga dastlabki ishlov berish, belgilarni ajratish va chuqur neyron tarmoqqa asoslangan matnga bog‘liq va bog‘liq bo‘lmagan ovoz asosidagi autentifikatsiya usullari ishlab chiqildi. Ilmiy tadqiqot natijasida matnga bog‘liq ovoz asosidagi autentifikatsiya usuli yuqori xavfsizlik darajasiga egaligini ko‘rsatdi.

3. Analog shakldagi signalni raqamli shaklga o‘tkazish, ovozda harakatsiz sohalarni olib tashlash va filtrlashga asoslangan nutq signallarga dastlabki ishlov berish algoritmi ishlab chiqildi. Ilmiy tadqiqot natijasida turli shovqinlar mavjud ovozdan ham, aktiv bo‘lmagan qismlarga ega ovozdan ham foydalanuvchilarni identifikatsiyalashda foydalanish mumkinligi ta‘minlandi.

4. Mel-chastotali kepral koefitsiyentlar usuliga asoslangan nutq signali belgilarini ajratish algoritmi ishlab chiqildi. Ilmiy tadqiqot natijasida har bir shaxs uchun ovoz modelini hosil qilish uchun kerakli belgilarni ajratish imkoniyati yaratilgan.

5. Har bir shaxsning ovoz modelini hosil qilish maqsadida shaxsni nutqi asosida identifikatsiyalashning chuqur neyron tarmoqli modeli ishlab chiqildi. Ilmiy tadqiqot natijasida o‘ramli neyron tarmoqqa asoslangan identifikatsiyalash modeli diskretlash uchun A2 va belgilarni shakllantirish uchun A3 algoritmlaridan foydalanganda 95,78% aniqlik va 0,292% ga teng xatolik darajasini ko‘rsatgan.

6. Ovozli ma‘lumotlarga asoslangan identifikatsiya tizimining har bir algoritmlarini alohida modul sifatida ifodalashga asoslangan nutq signallari orqali axborot tizimlari foydalanuvchilarini biometrik identifikatsiyalashning dasturiy majmuasi yaratildi. Ishlab chiqilgan dasturiy majmua soha korxonalarida identifikatsiyalash masalasini yechishda qo‘llanilib, o‘rtacha 90% aniqlik ko‘rsatkichi va 9% ga yaqin yolg‘ondan rad etish xatoligini ko‘rsatdi.

**НАУЧНЫЙ СОВЕТ DSc.13/30.12.2019.Т.07.02  
ПО ПРИСУЖДЕНИЮ УЧЕНЫХ СТЕПЕНЕЙ ПРИ ТАШКЕНТСКОМ  
УНИВЕРСИТЕТЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

---

**ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ  
ТЕХНОЛОГИЙ**

**ЮЛДАШЕВА НАФИСА САЛИМОВНА**

**МОДЕЛЬ И АЛГОРИТМЫ БИОМЕТРИЧЕСКОЙ  
АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ  
СИСТЕМ ПО ГОЛОСУ**

**05.01.05 - Методы и системы защиты информации. Информационная безопасность**

**АВТОРЕФЕРАТ ДИССЕРТАЦИИ  
ДОКТОРА ФИЛОСОФИИ (PHD) ПО ТЕХНИЧЕСКИМ НАУКАМ**

**Ташкент-2024**

**Тема диссертации доктора технических наук (DSc) зарегистрирована в Высшей аттестационной комиссии при Министерстве высшего образования, науки и инноваций Республики Узбекистан за номером B2023.4.PhD/T4177.**

Диссертация выполнена в Ташкентском университете информационных технологий.

Автореферат диссертации на трех языках (узбекский, русский, английский (резюме)) размещён на веб-странице научного совета ([www.tuit.uz](http://www.tuit.uz)) и в Информационно-образовательном портале «ZiyoNet» ([www.ziyo.net](http://www.ziyo.net)).

**Научный руководитель:**

**Ташев Комил Ахматович**

кандидат технических наук, доцент

**Официальные оппоненты:**

**Керимов Камил Фикратович**

доктор технических наук, профессор

**Юсупов Баходир Караматович**

доктора философии по техническим наукам (PhD), доцент

**Ведущая организация:**

**ООО “Центр научно-технических и маркетинговых исследований - UNICON.UZ”**

Защита диссертации состоится « 16 » ноября 2024 года в 10<sup>00</sup> часов на заседании Научного совета DSc.13/30.12.2019.T.07.01 при Ташкентском университете информационных технологий. (Адрес: 100202, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-64-43, факс: (99871) 238-65-52, e-mail: [info@tuit.uz](mailto:info@tuit.uz)).

С диссертацией можно ознакомиться в Информационно-ресурсном центре Ташкентского университета информационных технологий (регистрационный номер № \_\_\_\_). (Адрес: 100084, г.Ташкент, ул. Амир Темура, 108. Тел.: (99871) 238-65-44).

Автореферат диссертации разослан 4 ноября 2024 года.

(протокол рассылки № 16 от «\_\_» ноября 2024 года)

**Б.Ш. Махкамов**

Председатель Научного совета по присуждению ученых степеней, доктор экономических наук, профессор

**М.С. Саиткамоллов**

Ученый секретарь Научного совета по присуждению ученых степеней, доктор экономических наук, доцент

**Б.Ф. Абдурахимов**

Председатель Научного семинара при Научном совете по присуждению ученых степеней, доктор физико-математических наук, профессор

## **ВВЕДЕНИЕ (аннотация диссертации доктор философии (PhD))**

**Актуальность и востребованность темы диссертации.** В настоящее время большое внимание уделяется разработке приложений, основанных на биометрических технологиях, направленных на обеспечение безопасности. Одним из важнейших вопросов в этом направлении остаётся разработка методов, алгоритмов и приложений, основанных на обработке и распознавании речевых сигналов пользователей информационных систем. В частности, по данным GITNUX «доход от продаж биометрических систем по всему миру к 2025 году достигнет 15,1 миллиарда долларов <sup>1</sup>». А это, в свою очередь, требует исследования систем аутентификации на основе биометрических параметров, в частности, на основе речи пользователей. В настоящее время в таких странах, как США, Китай, Индия, Англия, Германия, Российская Федерация, Южная Корея большое внимание уделяется решению теоретических и практических вопросов направлений обработки речевых сигналов, составляющих основу речевых систем идентификации пользователей информационных систем, а также идентификации личности по речи.

В мире проводятся обширные научно-исследовательские работы, направленные на разработку или совершенствованию методов и алгоритмов обработки речевых сигналов, формирования признаков речевых сигналов, идентификации личности на основе речи, а также построение быстрых алгоритмов вычисления. В этой сфере проводятся научные исследования по совершенствованию методов и алгоритмов идентификации личности, предварительной обработки речевых сигналов, определения участков речи и извлечения информативных признаков, характеризующих речь, а также создание речевых моделей и систем автоматизации идентификации. В нашей стране в данном направлении особое внимание уделяется разработке и внедрению интеллектуальных систем биометрической идентификации личности на основе цифровой обработки и анализа речевых сигналов.

В нашей республике реализуются комплексные меры, направленные на совершенствование системы идентификации физических лиц при оказании государственных и банковских услуг. В Постановлении Президента Республики Узбекистан №ПП-113 “Национальная стратегия модернизации и ускоренного развития системы оказания государственных услуг на 2022 - 2026 годы” от 20 апреля 2022 года определены приоритетные задачи такие, как “внедрение единой системы идентификации в сфере оказания банковско-финансовых и государственных услуг”, “внедрение альтернативных способов идентификации личности при предоставлении государственных, банковских, социальных услуг и прохождении других административных процедур”. При реализации этих задач совершенствование подходов, моделей, методов и

---

<sup>1</sup> <https://gitnux.org/biometric-statistics/#:~:text=As%20of%202019%2C%2087%25%20of.increase%20in%20biometric%20data%20breaches.>

алгоритмов обработки и анализа речевых сигналов, распознавания личности по речи и обработки речевых сигналов с учетом оптимального набора признаков, а также применение в системах ограничения несанкционированного доступа к информационным системам, управления и контроля пользователей является одной из важных задач.

Настоящее диссертационное исследование в определенной степени служит выполнению задач, предусмотренных в Указах Президента Республики Узбекистан № УП-5349 от 19 февраля 2018 года «О мерах по дальнейшему совершенствованию сферы информационных технологий и коммуникаций», № УП-6079 от 5 октября 2020 года «Об утверждении Стратегии «Цифровой Узбекистан-2030» и мерах по ее эффективной реализации» и Постановление № ПП-167 от 31 мая 2023 года «О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан», а также в других нормативно-правовых актах, связанных с данной деятельностью.

**Соответствие исследования приоритетными направлениями развития науки и технологий республики.** Данное исследование выполнено в соответствии с приоритетными направлениями развития науки и технологий республики IV. «Развитие информатизации и информационно-коммуникационных технологий».

**Степень изученности проблемы.** Отдельное внимание заслуживают научные работы зарубежных ученых L.R. Rabiner, H. Beigi, D.A. Reynolds, P. Nguyen, J.D. Markel, A.H. Grey, J.R. Vacca, J. Chirillo, Y. Liu, Y. Xian, X. Chen, T. Fu, A.A. Lanne, B.M. Lobanov, A.B. Agranovskiy, D.A. Lednov, A. Kozlov, O. Kudashev<sup>1</sup> и других по совершенствованию моделей, методов и алгоритмов биометрической идентификации человека, цифровой обработке речевых сигналов, а также разработки и внедрения их в практику.

С.К.Ганиев, М.М.Каримов, Д.Т.Мухамедиева, М.М.Мусаев, Н.С.Маматов, З.Т.Худойкулов, Ш.З.Ислотов и другие вносят свой вклад в разработку теоретических основ информационной безопасности и идентификации пользователей информационных систем в нашей республике.

В настоящее время бурно развиваются приложения биометрической идентификации личности, основанные на обработке и анализе речевых

---

<sup>1</sup> L.R. Rabiner and R.W. Schafer “Introduction to Digital Speech Processing”; H. Beigi “Fundamentals of Speaker Recognition”; D.A Reynolds, T.F. Quatieri, R.B. Dunn “Speaker verification using adapted Gaussian mixture models”; Ch.Ch. Chiu, T.N. Sainath, Y. Wu, R. Prabhavalkar, P. Nguyen, Z. Chen, A. Kannan, R.J Weiss, K. Rao, E. Gonina, N. Jaitly, B.Li, J. Chorowski, M. Bacchiani “State-of-the-art speech recognition with sequence-to-sequence models”; J.D. Markel, A.H. Gray “Linear Prediction of Speech”; J.R. Vacca “Computer Forensics : Computer Crime Scene Investigation”; J. Chirillo, S. Blaul “Implementing Biometric Security”; K. Chen, D. Zhang, L. Yao, B. Guo, Z. Yu, Y. Liu “Deep learning for sensor-based human activity recognition: Overview, challenges, and opportunities”; Y.Xian, Y. Pu, Z. Gan, L. Lu, A. Thompson “Adaptive DCTNet for audio signal classification”; D. Yu, X. Chen, L. Deng “Factorized Deep Neural Networks for Adaptive Speech Recognition”; Y.Liu, Y. Qian, N. Chen, T. Fu, Y. Zhang, K. Yu “Deep feature for text-dependent speaker verification”; A.A. Lanne, T.V. Merkucheva “Filters with Double Symmetry”; B. Lobanov, L. Tsirulnik, D. Zhadinets, E. Karnevskaya “Language-and speaker specific implementation of intonation contours in multilingual TTS synthesis”; A.B. Agranovskiy, D.A. Lednov “Teoreticheskie aspekti algoritmov obrabotki i klassifikatsii rechevix signalov”; G. Lavrentyeva, S. Novoselov, E. Malykh, A. Kozlov, O. Kudashev, V. Shchemelinin “Audio replay attack detection with deep learning frameworks”

сигналов, а также технологии защиты информации, связанной с речью. Исследования в этой области показали, что биометрические технологии являются одной из перспективных технологий защиты информационных систем. В частности, приложения идентификации личности по речи являются наиболее удобным для пользователя методом идентификации, обеспечивает высокоточную идентификацию и значительно снижает затраты. В настоящее время, несмотря на то, что разработано множество методов и алгоритмов идентификации личности по речи, проблема обеспечения идентификации по речевым сигналам в неидеальных условиях, а также совершенствования методов и алгоритмов, отвечающих требованиям реального времени или разработки новых методов и алгоритмов изучена недостаточно.

**Связь диссертационного исследования с планами научно-исследовательских работ учреждения, при котором выполнена диссертация.** Диссертационное исследование выполнено в рамках планов проекта научно-исследовательских работ Ташкентского университета информационных технологий имени Мухаммада ал-Хоразмий BV-Atex-2018 (240+147) «Разработка алгоритмов и программного обеспечения идентификации личности на основе потоковой обработки изображений лиц», Научно-исследовательского института развития цифровых технологий и искусственного интеллекта «Создание алгоритмов и программных продуктов распознавания личности на основе обработки речевых сигналов»(2021-2023).

**Целью исследования является** разработка методов, алгоритмов и программного комплекса, биометрической идентификации пользователей информационных систем на основе предварительной обработки и анализа речевых сигналов.

**Задачи исследования:**

разработка модели угроз для голосовых систем и расчет уровня риска угроз;

усовершенствование методов текстозависимой и независимой аутентификации по голосу;

усовершенствование алгоритма предварительной обработки речевых сигналов пользователей в информационных системах;

разработка алгоритма извлечения признаков речевого сигнала при аутентификации пользователей;

разработка глубокой нейросетевой модели идентификации личности на основе речи;

разработка программного комплекса биометрической идентификации пользователей информационных систем на основе речевых сигналов.

В качестве **объекта исследования** был взят процесс биометрической идентификации пользователей информационных систем.

**Предметом исследования** является модель, методы и алгоритмы биометрической идентификации личности на основе речи.

**Методы исследования.** В ходе исследования использовались методы системного анализа, дискретной математики, теории вероятностей и

математической статистики, цифровой обработки сигналов, распознавания образов и машинного обучения.

**Научная новизна исследования заключается в следующем:**

разработана модель угроз для голосовых систем с использованием методологии анализа угроз STRIDE и рассчитаны уровни риска угроз на основе модели DREAD;

усовершенствованы методы предварительной обработки речевых данных, извлечения признаков, текстозависимой и независимой аутентификации по голосу на основе глубоких нейронных сетей;

усовершенствован алгоритм предварительной обработки речевых сигналов, основанный на цифровом преобразовании речевого сигнала, удалении и фильтрации статических участков в голосе;

разработан алгоритм извлечения признаков речевого сигнала на основе метода мел-частотных кепстральных коэффициентов и глубокая нейросетевая модель идентификации личности по речи при создании модели голоса;

разработан программный комплекс биометрической идентификации пользователей информационной системы, основанного на представлении в виде отдельного модуля каждого алгоритма системы идентификации на основе голосовых данных.

**Практические результаты исследования** заключаются в следующем:

разработано алгоритмическое обеспечение биометрической идентификации по речи для контроля и управления доступом к информационным системам, а также создания систем идентификации пользователей в компьютерных сетях;

разработаны алгоритмы предварительной обработки речевых сигналов, алгоритмы формирования вектора признаков и алгоритм построения голосовой модели личности на основе глубокой нейронной сети, а также программный комплекс, предназначенный для решения задач идентификации.

**Достоверность результатов исследования** подтверждается корректным применением математического аппарата обработки и идентификации речевых сигналов при разработке методов и алгоритмов, составляющих основу системы, а также положительными результатами экспериментальных и практических исследований.

**Научная и практическая значимость результатов исследования.**

Научная значимость результатов исследования обусловлена вкладом разработанных алгоритмов в развитии теоретических основ технологий биометрической идентификации личности по речи на основе цифровой обработки речевых сигналов.

Практическая значимость результатов исследования обусловлена использованием, разработанного программного комплекса при решении задач идентификации пользователей систем контроля и управления доступом в информационных системах.

**Внедрение результатов исследования.** На основе программного комплекса, созданного на основе существующих и предлагаемых подходов,

моделей, методов и алгоритмов цифровой обработки и идентификации речевых сигналов:

разработанное программное средство, на основе научно-теоретических данных диссертации, а также алгоритма создания кодовых книг для идентификации личности и алгоритма генерации последовательности слов для решения задачи двухфакторной аутентификации было внедрено в практическую деятельность Агентства по оценке знаний и квалификаций при Министерстве высшего образования, науки и инноваций Республики Узбекистан. (Агентство по оценке знаний и квалификаций протокол от 2 января 2024 года, Справка Министерства цифровых технологий Республики Узбекистан № 33-8/1867 от 19 марта 2024 года) В результате применения данного программного комплекса уровень безопасности использования сотрудником рабочей станции повышен в два раза;

разработанное программное средство, на основе алгоритма создания кодовых книг идентификации говорящего и алгоритма генерации последовательности слов для решения задачи двухфакторной аутентификации, было внедрено в практическую деятельность акционерно-коммерческого банка «Алокабанк». (АК «Алокабанк» протокол от 30 января 2024 года, Справка Министерства цифровых технологий Республики Узбекистан № 33-8/1867 от 19 марта 2024 года) Программное средство, разработанное на основе достигнутых научных результатов, позволило сократить время, затрачиваемое на контроль входа и выхода сотрудников в организацию в среднем на 15%;

разработанное программное средство, на основе научных результатов диссертации, было внедрено в практическую деятельность общества с ограниченной ответственностью «SERVER CONF». (ООО «SERVER CONF» протокол от 15 января 2024 года, Справка Министерства цифровых технологий Республики Узбекистан № 33-8/1867 от 19 марта 2024 года) Программное средство, разработанное на основе научных результатов диссертации, позволило повысить уровень безопасности специальных помещений в организации.

система идентификации пользователей на основе речевых данных была внедрена локальную сеть ГУП «Центр кибербезопасности» («Центр кибербезопасности» ГУП протокол от 12 февраля 2024 года; Справка Министерства цифровых технологий Республики Узбекистан № 33-8/1867 от 19 марта 2024 года). Разработанный программный инструмент позволил сократить затраты времени в среднем на 15% для контроля и управления доступом к информационным системам, а также контроля доступа пользователей в компьютерных сетях

**Апробация результатов исследования.** Результаты исследования докладывались и обсуждались на 2 международных и 4 республиканских научно-практических конференциях.

**Опубликованность результатов исследования.** По теме диссертации опубликовано всего 20 научных работ, рекомендованных Высшей

аттестационной комиссией Республики Узбекистан для публикации основных научных результатов докторских диссертаций, из них 5 опубликованы в зарубежных и 6 в республиканских научных журналах, получены 3 свидетельства об официальной регистрации программы для ЭВМ.

**Структура и объем диссертации.** Диссертация состоит из введения, четырех глав, заключения, списка использованной литературы и приложений. Объем диссертации составляет 99 страниц.

## ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

**Во введении** обоснована актуальность и востребованность темы диссертации, приведено степень изученности проблемы, сформулированы цель и задачи, определены объект и предмет исследования, указано их соответствие приоритетными направлениями развития науки и технологий Республики Узбекистан, раскрыто теоретическая и практическая значимость полученных результатов, приведены сведения о внедрении в практику результатов исследования, об опубликованных работах и структуре диссертационной работы.

В первой главе «**Технологии распознавания личности на основе биометрических параметров**» проанализированы технологии распознавания личности на основе биометрических параметров. Также были изучены угрозы, направленные на идентификацию личности по голосу, а также области применения и проблемы технологии идентификации личности по речи.

В первом параграфе представлен анализ технологий распознавания личности на основе биометрических параметров. Биометрические методы идентификации обычно делят на две группы: физиологические и поведенческие. Методы физиологической идентификации включают использование признаков таких, как отпечатки пальцев или ладоней, зрачок или радужная оболочка глаза, 2-мерное и 3-мерное изображение лица и т.д., параметры, основанные на поведении, могут включать человеческий голос, клавиатурный почерк набора текста и манера движений.

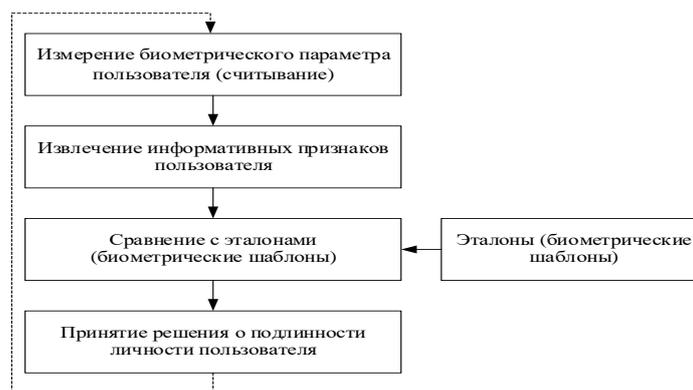
На основе любой биометрической системы лежит следующая цепочка действий: (рисунок 1):

– *запись* – биометрические данные пользователя считываются с помощью сканера;

– *извлечение* – из предоставленных биометрических данных выбирается уникальная информация, и эта информация считается биометрический «образ» конкретного лица;

– *сравнение* – проводится сравнение предоставленного биометрического образа с одним или несколькими эталонами (шаблонами), хранящимися в базе данных системы;

– *принятие решения* – система принимает решение о завершении процедуры идентификации, повторении или изменении условий проведения, решая, совпадают биометрические изображения или нет.



**Рисунок 1. Процедура биометрической идентификации**

Во втором параграфе проведен анализ угроз, направленных на системы идентификации личности по голосу. На практике в системах идентификации по голосу распространено множество угроз, в частности, подделка голоса, копирование и повторное использование голоса, обман системы и отказ в обслуживании. Поэтому в следующей главе будет подробно представлена разработка модели угроз для системы идентификации по голосу и определение существующих уровней риска.

В третьем параграфе проведен анализ области применения технологии идентификации личности по голосу и их проблемы. Было установлено, что приложения безопасности, основанные на распознавании голоса, в основном используются в финансовой сфере, пассивном контроле мошенничества, решении задач криминалистики, при контроле доступа в организациях, индексировании аудио и видеоконтента, а также видеонаблюдении. Кроме того, в результате анализа в этих системах наблюдалось множество проблем, связанных с краткостью предложений, наличием фонового шума и их работой в системе реального времени.

Во второй главе диссертации, озаглавленной «Современное состояние биометрической идентификации личности по голосу», представлены основные проблемы системы идентификации личности по голосу и модели угроз для голосовых приложений, а также предложены методы текстозависимой и независимой аутентификации по голосу.

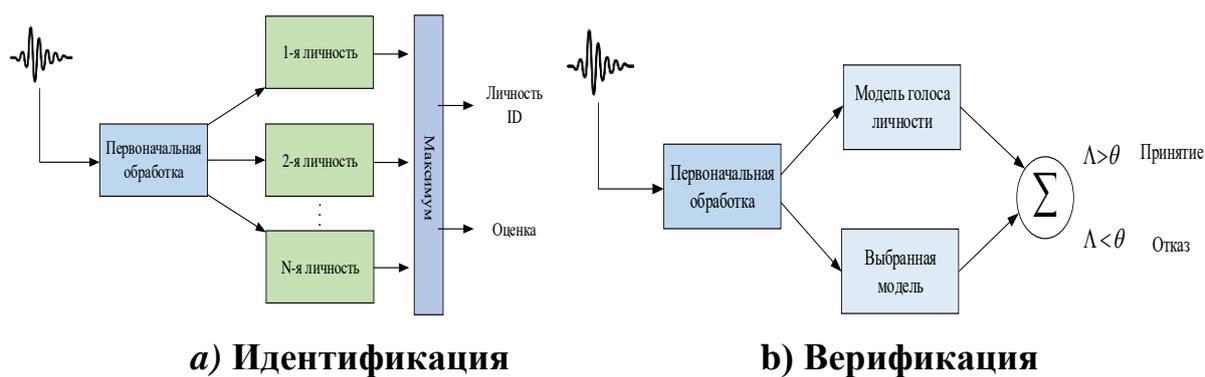
В первом параграфе проведен анализ основных задач системы идентификации личности по голосу. В целом при распознавании личности решается множество задач, наиболее важные из которых представлены на рисунке 2.



**Рисунок 2. Проблемы, решаемые системой идентификации личности по голосу**

Одной из наиболее широко используемых из этих задач является идентификация личности по голосу, которая связана с сопоставлением неизвестного лица с конкретным лицом из заранее определенного набора лиц на основе голоса. Режим верификации (аутентификации) личности по голосу соответствует задаче двухклассовой (бинарной) классификации, где представляется вопрос о принадлежности множества тестовых образцов одним и тем же лицам.

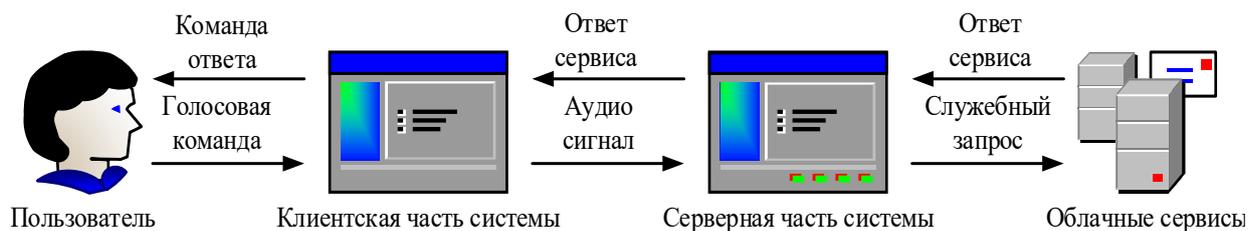
Основные структуры систем идентификации и верификации личности показаны на рисунках 3 (а) и (б) соответственно, в обеих системах сначала обрабатывается речевой сигнал для выбора признаков, предоставляющих информацию о личности.



**Рисунок 3. Структура систем идентификации и верификации**

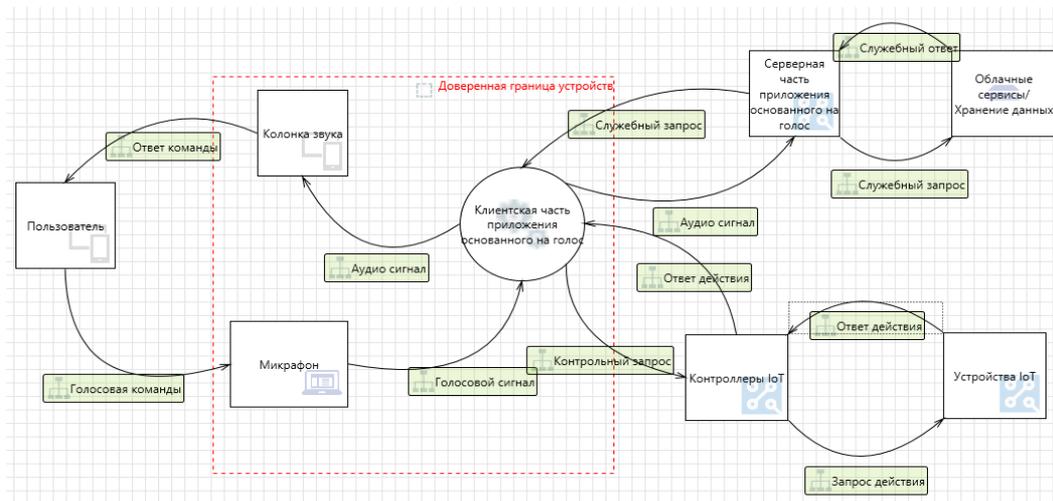
Во втором параграфе представлен анализ возможных угроз и рисков при выполнении для голосовых приложений. В частности, рассматриваются вопросы классификация угроз по методологии STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of privileges), оценки риска угроз и принятия защитных мер от них по модели DREAD (Damage Potential, Reproducibility, Exploitability, Affected Users, Discoverability).

В целом голосовые приложения можно описать, как показано на рисунке 4. Согласно этому, первоначально подаваемая пользователем команда (сигнал) вводится в клиентскую часть системы на стороне пользователя. Данная подсистема преобразует полученную голосовую команду в звуковой сигнал и отправляет ее на обработку серверной части системы. На основе введенных данных сервер формирует соответствующий ответ и может вернуть его клиенту или выполнить действие в системе контроля доступа (например, предоставить разрешение). Облачный сервис может быть реализован в этой архитектуре по выбору, сможет хранить информацию или оказывать некоторые услуги.



**Рисунок 4. Архитектура голосовых приложений**

Одним из первых шагов в моделировании угроз является выявление существующих угроз с помощью автоматизированных систем. Для выполнения этой задачи был использован инструмент Microsoft Threat Modeling Tool v.7.3.31026.3. В целом для голосовых приложений DFD (Data Flow Diagram) представление показано на рисунке 5.



**Рисунок 5. DFD для голосовых приложений. Красный прямоугольник представляет устройства в системах, основанных на голосе.**

В этом случае первоначально произнесенная пользователем команда доставляется в виде аудиосигнала через микрофон в клиентскую часть системы. Клиентская часть приложения играет важную роль и отправляет данные на серверную часть системы и на основании полученного от нее ответа на IoT-контроллер. Кроме того, он уведомляет пользователя о совершаемых действиях через голосовой динамик. В свою очередь, серверная часть приложения может использовать облачные сервисы или системы хранения данных для выполнения своей деятельности. А IoT-контроллер, управляя несколькими устройствами IoT, может выполнять действие по обеспечению безопасности (например, открывать дверь).

Результаты анализа и уровни риска угроз, полученные с помощью инструмента Microsoft Threat Modeling Tool v.7.3.31026.3 приведены в таблице 1. Серьезность угрозы, принадлежащей к каждой из пяти описанных ниже категорий, может быть определена по числовым значениям (0 (низкая, сложная), 5 (средняя) и 10 (высокая, легкая)) с использованием модели DREAD. При расчете итогового рейтинга неопределенный уровень угрозы и его числовые значения определялись в следующем порядке: высокий (8-10), средний (4-7) и низкий (0-3).

Согласно таблице, существуют угрозы с 2 уровнями низкого риска, 10 уровнями среднего риска и 4 уровнями высокого риска. Например, при отсутствии механизма аутентификации в соответствии с угрозой подделки микрофона, можно получить привилегии законного пользователя из-за возможности подмены настоящего пользователя или дискредитация голоса. Поэтому, D = 10. E = 10 поскольку данная угроза требует недорогие

инструменты для проведения,  $R = 10$  из-за легкости реализации атаки. В большинстве систем по причине отсутствия внимания к вопросам безопасности и неспособности системы определить подлинность голоса  $D = 10$ . Наконец,  $A = 10$ , поскольку этот тип угроз оказывает серьезное влияние на пользователя. Общий уровень риска для этой угрозы будет равен 10.

Таблица 1

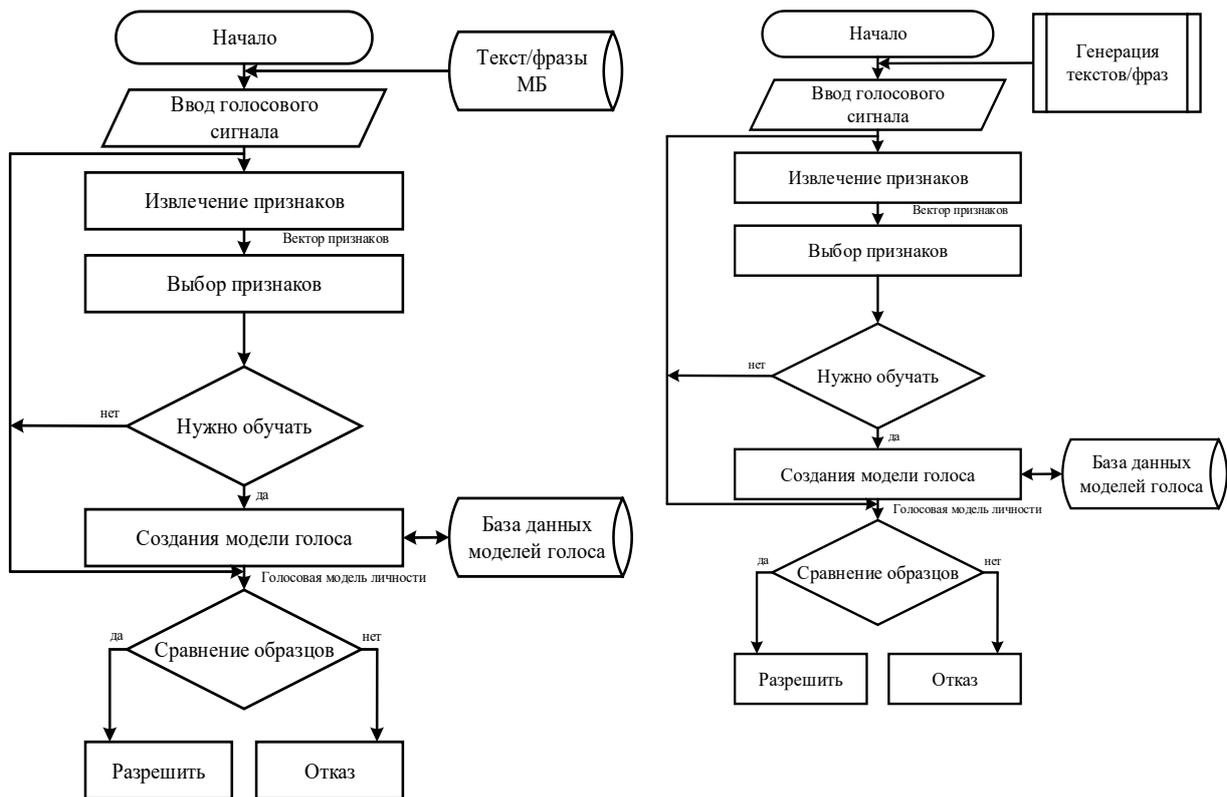
**Угрозы и их анализ рисков в системах, основанных на голосе**

| Поток данных                                     | Угроза                            | D         | R         | E         | A         | D         | Общий<br>(D+R+E+A+D)/5 |
|--|-----------------------------------|-----------|-----------|-----------|-----------|-----------|------------------------|
| Аудиосигнал<br>(M→C)                             | Подделка                          | 0         | 0         | 10        | 5         | 0         | 3                      |
| Голосовая команда<br>(пользователь→<br>микрофон) | <b>Подделка</b>                   | <b>10</b> | <b>10</b> | <b>10</b> | <b>10</b> | <b>10</b> | <b>10</b>              |
|  | Изменение                         | 10        | 0         | 0         | 10        | 0         | 4                      |
|  | Отказаться от обслуживания        | 0         | 10        | 0         | 10        | 0         | 4                      |
| Ответ службы<br>(S→M)                            | <b>Изменение</b>                  | <b>10</b> | <b>10</b> | <b>10</b> | <b>10</b> | <b>5</b>  | <b>9</b>               |
|  | Раскрытие информации              | 10        | 10        | 10        | 10        | 0         | 8                      |
|  | Отказаться от обслуживания        | 0         | 10        | 5         | 10        | 10        | 7                      |
|  | Повышенные привилегии             | 10        | 10        | 0         | 10        | 0         | 6                      |
| Запрос контроля                                  | Подделка                          | 10        | 10        | 5         | 10        | 0         | 7                      |
|  | <b>Изменение</b>                  | <b>10</b> | <b>10</b> | <b>5</b>  | <b>10</b> | <b>10</b> | <b>9</b>               |
| Ответ действия                                   | Подделка                          | 0         | 10        | 5         | 10        | 10        | 7                      |
|  | Изменение                         | 0         | 10        | 0         | 10        | 10        | 6                      |
|  | Раскрытие информации              | 10        | 10        | 5         | 5         | 0         | 6                      |
|  | <b>Отказаться от обслуживания</b> | <b>10</b> | <b>10</b> | <b>10</b> | <b>10</b> | <b>10</b> | <b>10</b>              |
|  | Повышенные привилегии             | 10        | 0         | 0         | 0         | 0         | 2                      |
| Ответ команды                                    | Раскрытие информации              | 0         | 10        | 10        | 10        | 0         | 6                      |

В третьем параграфе, рассмотрена задача разработки методов текстозависимой и независимой аутентификации по голосу. Модель говорящего (обычно значение распределения признаков) - человеческая характеристика, записанная в системе аутентификации по голосу. Системы распознавания в зависимости от вида ввода речи можно разделить на два типа: текстозависимые и независимые системы. В текстозависимой системе распознавания речи пользователь должен заранее произнести определенный текст/фразу. При устном знании текст/фраз, достигается хорошему уровню точности, однако злоумышленник намеренно может записать текст настоящего пользователя и затем исследовать для взлома системы.

В текстонезависимой системе распознавания речи от пользователя не ожидается никаких predetermined текстов/фраз. Пользователь может произносить случайно выбранный текст/фразы. Текстонезависимая система распознавания речи является гибкой в использовании, но менее точной, чем текстозависимая система. Как и текстозависимая система, текстонезависимая система уязвима для атаки повторного воспроизведения.

Блок-схемы процесса аутентификации этих двух случаев приведена на рисунках 6(а) и 6(б).



а) Схема процесса текстозависимой аутентификации по голосу

б) Схема процесса текстонезависимой аутентификации по голосу

Рисунок 6. Схемы текстозависимой и текстонезависимой аутентификации по голосу

В третьей главе диссертации «Методы и алгоритмы обработки речевых сигналов также распознавания личности по речи» представлен речевой сигнал, алгоритмы предварительной обработки и извлечения признаков речевого сигнала, а также предложена модель идентификации личности по голосу на основе глубокой нейронной сети.

В первом параграфе предложен алгоритм предварительной обработки речевого сигнала (7-рисунок). Данный алгоритм состоит из 3 этапов: преобразования аналоговых сигналов в цифровые, VAD и фильтрации.



Рисунок 7. Алгоритм предварительной обработки

Предварительная обработка выполняется для подготовки сигнальных признаков к этапу извлечения. На сигнал могут влиять шумы, вызванные внутренними органами, движениями тела или рук и т.д. Предварительная обработка выполняется в следующих этапах обработки:

- 1) В фильтрах низких частот отсекаются ненужные высокочастотные шумы, используется эллиптический фильтр нижних частот 300 Гц.
- 2) При удалении шума значения выше определенного порога выравниваются с порогами для минимизации взрывного шума.
- 3) При нормализации амплитуды все сигналы приводят в диапазон  $[-1,1]$ .

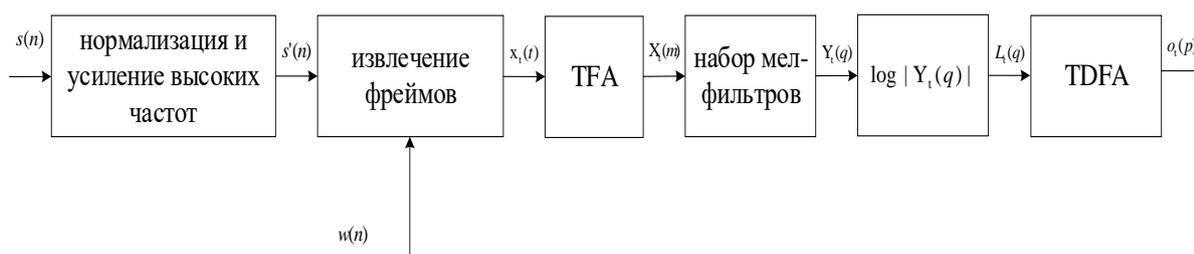
Преобразование аналогового сигнала в цифровой. При преобразовании аналоговых сигналов в цифровую форму можно выделить следующие три процесса: дискретизация, квантование и кодирование.

*VAD.* В голосовой связи пространство, в котором находится речевая информация, называется активным участком речи. Интервалы, не содержащие речевой информации, независимо от наличия или отсутствия фонового шума, называются остановками. В источниках литературы алгоритм обнаружения границ времени речевой активности называется VAD (Voice Activity Detection). Алгоритм VAD позволяет разделить сигнал на два сегмента: активный A (activity) и тихий S (silence).

*Фильтрация.* Следующим этапом предварительной обработки речевого сигнала является фильтрация в частотной области для уменьшения частей звука, которые не слышны человеку. Для этого использован фильтр верхних частот с амплитудными характеристиками (фильтр Чебышева 2-го рода 22-го порядка). В этом случае параметры фильтра были выбраны с помощью процесса оптимизации.

*Во втором параграфе* рассмотрен вопрос разработки алгоритмов извлечения признаков речевого сигнала. Эффективность систем распознавания напрямую зависит от извлеченных признаков. Чем точнее формируется исходный набор признаков, тем точнее будет распознавание. Необходимо извлекать такие признаки речевого сигнала, чтобы с их помощью можно было различать разные фонемы языка.

Для решения этой задачи был использован самый популярный на сегодняшний день метод извлечения признаков - мел-частотных кепстральных коэффициентов. Вычисление мел-частотных кепстральных коэффициентов проводится в несколько этапов (8-рисунок).



**Рисунок 8. Этапы вычисления мел-частотных кепстральных коэффициентов**

Алгоритм формирования вектора признаков речевого сигнала представлен на рисунке 9(а) (алгоритм А1). На рисунке 9(б) предложен алгоритм, позволяющий сократить время, затрачиваемое на работу системы (алгоритм А2).



**Рисунок 9. Алгоритмы формирования и извлечения вектора символов речевого сигнала**

Сравнительный анализ рассмотренных выше алгоритмов представлен на 2-таблице. Были использованы речи 100 лиц (74 мужчин и 26 женщин). На каждого человека имеется по 10 речевых файлов, 5 из которых использовались для обучения, а остальные 5 - для тестирования. Каждый файл длится 2-5 секунд.

**Таблица 2**

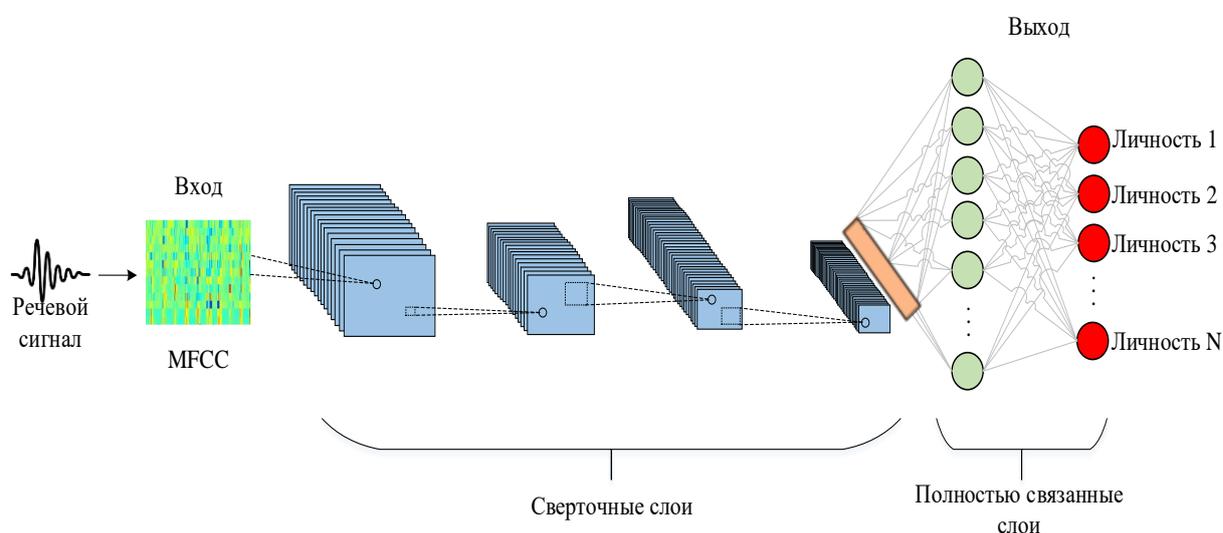
**Сравнительный анализ алгоритмов**

| Показатели<br>Алгоритм | Размер данных (МБ) | Результат (%) | Время, потраченное на обучение (сек.) | Время, потраченное на распознавание (сек.) |
|------------------------|--------------------|---------------|---------------------------------------|--|
| Основной (А1)          | 285,3              | 99,6          | 45,3                                  | 69,3                                       |
| Предложенный (А2)      | 31,5               | 98,4          | 6,7                                   | 13,1                                       |

Как видно из таблицы, сокращение времени, затрачиваемого на работу системы, достигнуто в основном за счет уменьшения количества признаков.

В *третьем параграфе* рассмотрена задача разработки модели голосовой идентификации личности по голосу на основе глубокой нейронной сети.

В этой работе для создания модели личности по голосу была использована глубокая нейронная сеть. Глубокая нейронная сеть основана на сверточных нейронных сетях CNN и в нем использован d-векторный подход. Несмотря на вариацию слоев и нейронов, все системы включают в себя одни и те же важные элементы, а именно (convolution) работающая на уровне кадра, объединение (pooling), полносвязные слои (fully connected) на уровне сегмента для расчета местоположения моделей в гиперпространстве. Основная идея слоя объединения - собрать данные по всем входным фреймам, путем вычисления среднего значения (average polling) или среднего стандартного отклонения (statistical polling). Архитектура сверточной глубокой нейронной сети представлена на 10-рисунке.



**Рисунок 10. Архитектура сверточной глубокой нейронной сети**

В целях повышения устойчивости модели распознавания личности по голосу, на основе глубокой нейронной сети к внешнему шуму при обработке речевых сигналов, было использовано аугментация данных.

Для экспериментов использовались два типа функций разделения наборов символов: банк фильтров мел-масштабирования (*A3 алгоритм*) и (*A4 алгоритм*) мел-частотных кепстральных коэффициентов. Аудиосегменты длительностью менее 4 секунд были исключены из набора обучающих данных перед обработкой данных. Один и тот же конвейер обработки применен к каждому предложению в наборах данных для обучения и тестирования.

В первой части экспериментов было получено 60 банк фильтров мел-масштабирования для каждого кадра на основе алгоритма A3, а во второй части — 20 мел-частотных кепстральных коэффициентов для каждого кадра на основе алгоритма A4. На рисунке 11 показана модель идентификации личности, основанная на обучение глубокой нейронной сети.



**Рисунок 11. Модель идентификации личности на основе обучения глубокой нейронной сети**

Экспериментальные исследования по обучению глубокой нейронной сети проводились на языке программирования Python. Каждая модель обучалась в течение 100 эпох на графическом процессоре GeForce GTX 1080.

Результаты обучения глубокой нейронной сети представлены в таблице 3.

**Таблица 3  
Результаты обучения глубокой нейронной сети**

| Дискретизация | Формирование признаков | Точность (%) | Ошибка (Loss) |
|---------------|------------------------|--------------|---------------|
| A1            | A3                     | 94,74        | 0,302         |
| A2            | A3                     | 95,78        | 0,292         |
| A1            | A4                     | 92,62        | 0,351         |
| A2            | A4                     | 93,95        | 0,321         |

Как видно из таблицы, при использовании предложенных алгоритмов A2, A3 в обучении глубоких нейронных сетей и модели глубокой нейронной сети лучший результат был достигнут с точностью 95,78% и ошибкой 0,292, при использовании алгоритмов A2, A4 и модели глубокой нейронной сети лучший результат был достигнут с точностью 93,95% и ошибкой 0,321.

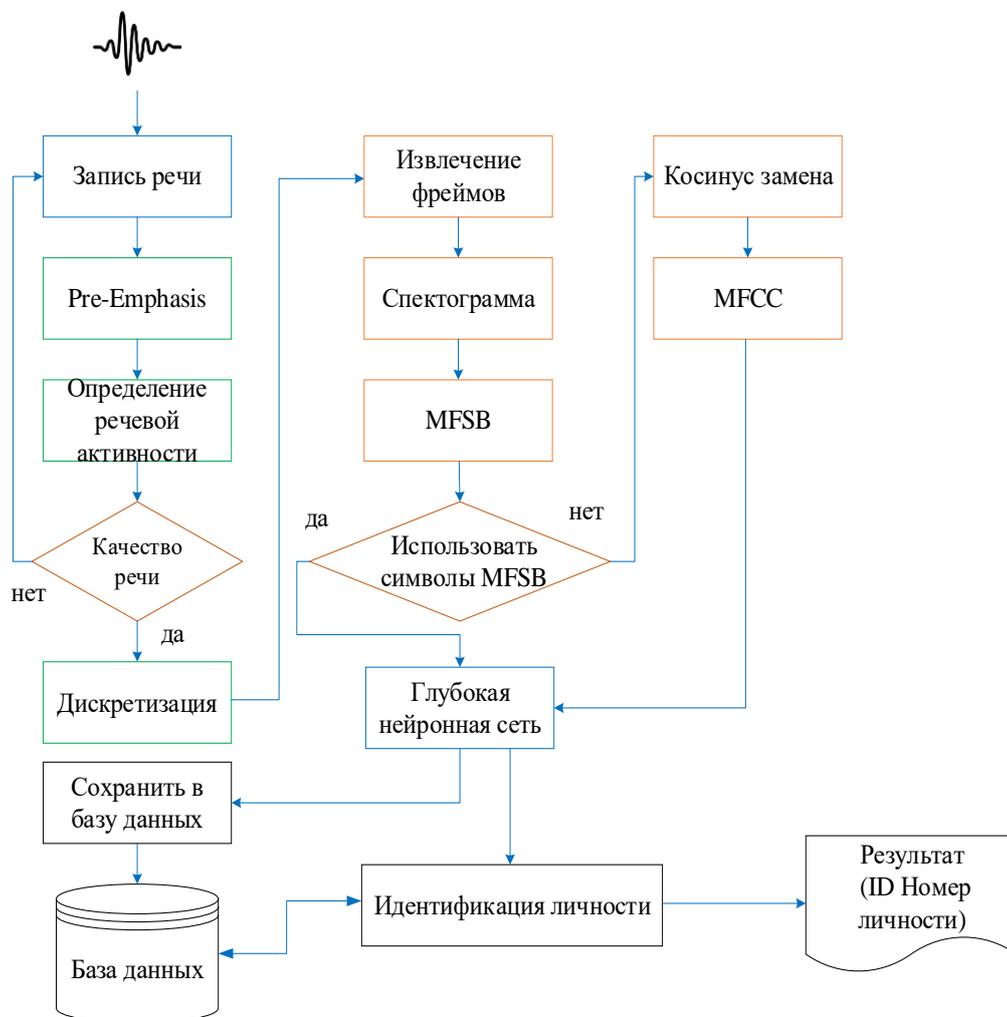
В четвертой главе диссертации, озаглавленной «**Программное обеспечение и его применение в практических задачах**» разработан программный комплекс биометрической идентификации пользователей информационных систем на основе речевых сигналов, а также подробно описаны модули программного комплекса. Также представлены результаты экспериментальных исследований разработанного программного комплекса и практического применения.

В первом параграфе представлена задача создания программного комплекса биометрической идентификации пользователей информационных систем на основе речевых сигналов и ее описания. В программном комплексе создана база данных для хранения данных зарегистрированных лиц,

использована система управления базами данных SQLite и библиотека PyTorch в работе с глубокими нейронными сетями.

На рисунке 12 представлена, обобщенная схема разработанного программного комплекса биометрической идентификации/аутентификации личности по речи, на основе принципа модульности.

Во втором параграфе описаны модули программного комплекса.



**Рисунок 12. Обобщенная схема программного комплекса идентификации человека по голосу**

Разработанный программный комплекс состоит из модулей таких, как нормализация, удаление шума, сглаживание, банки фильтров мел-масштабирования, Delta-delta.

В третьем параграфе представлены результаты экспериментальных исследований программного комплекса и его практическое внедрение.

Программный комплекс идентификации/аутентификации на основе звуковых сигналов, разработанный в рамках диссертационной работы, был применен в отраслях экономики нашей страны, а полученные результаты представлены в таблице 4.

## Показатели распознавания

| Характеристики<br>База голосовых<br>сигналов                           | Количество<br>лиц | Количество<br>обучаемых<br>голосовых<br>сигналов.<br>Одно лицо/Всего | Ошибка<br>ложного<br>отклонения, % | Точность,<br>% |
|--|-------------------|--|------------------------------------|----------------|
| База звуковых сигналов<br>Агентства по оценке знаний и<br>квалификаций | 50                | 40-50/2300   | 9,0                                | 91,0           |
| База звуковых сигналов<br>АК «Алокабанк»                               | 20                | 40-50/955  | 10,0                               | 90,0           |
| База звуковых сигналов<br>ООО «SERVER CONF»                            | 60                | 40-50/2755   | 9,1                                | 90,9           |

Как видно из таблицы, разработанный программный комплекс использовался для решения задачи идентификации на предприятиях отрасли и показал среднюю точность 90 % и ошибку ложного отклонения около 9 %.

## ЗАКЛЮЧЕНИЕ

В результате диссертационного исследования, доктора философии (PhD) на тему “Модель и алгоритмы биометрической аутентификации пользователей информационных систем по голосу” представлены следующие выводы:

1. Разработана модель угроз для голосовых систем с использованием методологии STRIDE и рассчитаны уровни риска угроз на основе модели DREAD. В результате исследования было установлено, что наибольшую опасность представляют угрозы подмены микрофона и отказа в обслуживании клиентскую часть голосового приложения.

2. Усовершенствованы методы предварительной обработки речевых данных, извлечения признаков, текстозависимой и независимой аутентификации по голосу на основе глубоких нейронных сетей. В результате научного исследования было установлено, что текстозависимый метод аутентификации по голосу имеет высокий уровень безопасности.

3. Усовершенствован алгоритм предварительной обработки речевых сигналов, основанный на цифровом преобразовании речевого сигнала, удалении и фильтрации статических участков в голосе. В результате научных исследований было установлено, что для идентификации пользователей можно использовать как голос с различными шумами, так и голос с неактивными участками.

4. Разработаны алгоритм извлечения признаков речевого сигнала на основе метода мел-частотных кепстральных коэффициентов и глубокая нейросетевая модель идентификации личности по речи при создании модели голоса. В результате научных исследований удалось извлечь необходимые признаки для создания модели голоса личности, модель идентификации на основе сверточной нейронной сети показала точность 95,78% и ошибок

0,292% при использовании алгоритмов А2 для дискретизации и А3 для формирования признаков.

5. Разработан программный комплекс биометрической идентификации пользователей информационной системы, основанного на представлении в виде отдельного модуля каждого алгоритма системы идентификации на основе голосовых данных разработанный программный комплекс, использовался для решения задачи идентификации на предприятиях отрасли и показал среднюю точность 90 % и ошибку ложного отклонения около 9 %.

**SCIENTIFIC COUNCIL AWARDING SCIENTIFIC DEGREES  
DSc.13/30.12.2019.T.07.02 AT TASHKENT UNIVERSITY OF  
INFORMATION TECHNOLOGIES**

---

**TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES**

**YULDASHEVA NAFISA SALIMOVNA**

**MODEL AND ALGORITHMS OF BIOMETRIC AUTHENTICATION OF  
USERS OF INFORMATION SYSTEMS BY VOICE**

**05.01.05 - Methods and systems of information protection. Information security**

**DISSERTATION ABSTRACT FOR THE DOCTOR OF PHILOSOPHY DEGREE (PhD)  
OF TECHNICAL SCIENCES**

**Tashkent-2024**

**The theme of the dissertation of doctor of philosophy (PhD) on technical sciences was registered at the Supreme attestation commission at the Ministry of higher education, science and innovations of the Republic of Uzbekistan under number B2023.4.PhD/T4177.**

The dissertation was has been prepared at the Tashkent university of information technologies named after Muhammad al-Khwarizmi.

The abstract of the dissertation is posted in three languages (Uzbek, Russian, English (summary)) on the Scientific Council website [www.tuit.uz](http://www.tuit.uz) and on the website «ZiyoNet» of Information and educational portal [www.ziyo.net](http://www.ziyo.net).

|                              |  |
|------------------------------|--|
| <b>Scientific adviser:</b>   | <b>Tashev Komil Akhmatovich</b><br>Candidate of Technical Sciences, assistant professor  |
| <b>Official opponents:</b>   | <b>Kerimov Kamil Fikratovich</b><br>Doctor of Technical Sciences, professor<br><br><b>Yusupov Bahodir Karamatovich</b><br>Doctor of Philosophy in Technical Sciences (PhD),<br>assistant professor |
| <b>Leading organization:</b> | <b>“UNICON.UZ - Scientific, technical and marketing research center” LLC</b>   |

The defense will take place on “ 16 ” november 2024 at 10<sup>00</sup> the meeting of Scientific Council DSc.13/30.12.2019.T.07.01 at Tashkent university of information technologies. (Address: 100084, Tashkent city, Amir Temur street, 108. Tel.: (99871) 238-64-43, e-mail: [info@tuit.uz](mailto:info@tuit.uz)).

The dissertation could be reviewed in the Information Resource Center of Tashkent university of information technologies (registration number №. \_\_\_\_). (Address: 100084, Tashkent city, Amir Temur street, 108. Tel.: (99871) 238-64-15).

The abstract dissertation is distributed on “ 4 ” november 2024.  
(register protocol of distribution №. 16 “ \_\_\_ ” november 2024)

**B.Sh. Makhkamov**

Chairman of the Scientific Council awarding scientific degrees, doctor of economical sciences, professor

**M.S. Saitkamolov**

Scientific Secretary of Scientific Council awarding scientific degrees, doctor of economical sciences, assistant professor

**B.F. Abdurakhimov**

Chairman of the academic Seminar under the Scientific Council awarding scientific degrees, doctor of physical and mathematical sciences, professor

## INTRODUCTION (abstract of PhD dissertation)

**The aim of the research work** is the improvement and development of models, methods and algorithms for biometric identification of the person, digital processing and recognition of speech signals and their implementation.

**The object of the research work** is biometric identification process of identification of information systems.

**The scientific novelty of the research work:**

A threat model for voice-based systems was developed using the STRIDE methodology, and risk levels of threats were calculated based on the DREAD model;

improved voice data preprocessing, character extraction, and deep neural network-based text-dependent and independent voice-based authentication methods;

improved speech signal preprocessing algorithm based on digital transformation of the speech signal, removal of static areas in the sound and filtering;

a speech signal separation algorithm based on the method of mel-frequency cepstral coefficients and a deep neural network model for identifying a person based on his speech was developed in creating a voice model;

a software complex of biometric identification of information system users based on the expression of each algorithm of the identification system based on voice data as a separate module has been created.

**Implementation of the research results.** Implementation of the research results. Based on the software package created on the basis of existing and proposed approaches, models, methods and algorithms for digital processing and identification of speech signals:

the developed software tool, based on the scientific and theoretical data of the dissertation, as well as the algorithm for creating code books for personal identification and the algorithm for generating a sequence of words to solve the problem of two-factor authentication, was implemented in the practical activities of the Agency for the Assessment of Knowledge and Qualifications under the Ministry of Higher Education, Science and Innovation of the Republic of Uzbekistan. (Agency for the Assessment of Knowledge and Qualifications protocol dated January 2, 2024, Certificate of the Ministry of Digital Technologies of the Republic of Uzbekistan No. 33-8 / 1867 dated March 19, 2024) As a result of the use of this software package, the level of security of the employee's use of the workstation has been doubled;

The developed software, based on the algorithm for creating speaker identification code books and the algorithm for generating a sequence of words to solve the problem of two-factor authentication, was implemented in the practical activities of the joint-stock commercial bank "Aloqabank". (JSC "Aloqabank" minutes dated January 30, 2024, Certificate of the Ministry of Digital Technologies of the Republic of Uzbekistan No. 33-8 / 1867 dated March 19, 2024) The software, developed on the basis of the achieved scientific results, made it possible to reduce the time spent on monitoring the entry and exit of employees to the organization by an average of 15%;

The developed software, based on the scientific results of the dissertation, was implemented in the practical activities of the limited liability company “SERVER CONF”. (LLC “SERVER CONF” protocol dated January 15, 2024, Certificate of the Ministry of Digital Technologies of the Republic of Uzbekistan No. 33-8 / 1867 dated March 19, 2024) The software tool developed on the basis of the scientific results of the dissertation made it possible to increase the level of security of special premises in the organization.

User identification system based on speech data was implemented in the local network of the State Unitary Enterprise “Cybersecurity Center” (“Cybersecurity Center” State Unitary Enterprise protocol dated February 12, 2024; Certificate of the Ministry of Digital Technologies of the Republic of Uzbekistan No. 33-8 / 1867 dated March 19, 2024). The developed software tool made it possible to reduce time costs by an average of 15% for monitoring and managing access to information systems, as well as monitoring user access in computer networks.

**The outline of the dissertation.** The dissertation consists of an introduction, four chapters, a conclusion, a list of references and appendices. The volume of the dissertation is 99 pages.

**E'LON QILINGAN ISHLAR RO'YXATI**  
**СПИСОК ОПУБЛИКОВАННЫХ РАБОТ**  
**LIST OF PUBLISHED WORKS**

**I bo'lim (I часть; I part)**

1. Tashev K.A., Gulomov Sh.R., Yuldasheva N.S., “Security Scheme and Conceptual Model of Internet Banking System”// International Conference on Information Science and Communications Technologies (ICISCT), IEEE, Toshkent 2021. -P.1-4 (05.00.00; 30.10.2021, №308/6-son rayosat qarori). (Scopus, DOI: 10.1109/ICISCT52966.2021.9670283).

2. Fayziyeva D.S., Yuldasheva N.S., “A Study on the Methods and Algorithms Used for the Separation of Speech Signals” // Intelligent Communication Technologies and Virtual Mobile Networks, March, 2024, Tirunelveli, India, -P.1-4. (Scopus, DOI: 10.1109/ICICV62344.2024.00086)

3. Tashev K.A., Fayziyeva D.S., Yuldasheva N.S., “Speaker modeling by preprocessing speech signals” // International Scientific Journal “Science and Innovation”, Volume 2 | Issue 10 | October 2023, ISSN: 2181-3337, -P. 130-139. (23, Scientific Journal Impact Factor, SJIF=2023: 5.608).

4. Fayziyeva D.S., Yuldasheva N.S., “Voice identification systems” // International Scientific Journal “Science and Innovation”, Volume 2 | Issue 9 | September, 2023, ISSN: 2181-3337 (P), -P. 135-138. (23, Scientific Journal Impact Factor, SJIF=2023: 5.608).

5. Tashev K.A., Yuldasheva N.S., “Шахсни идентификацияловчи биометрик тизимлар” // Muhammad al-Xorazmiy avlodlari ilmiy-amaliy va axborot-tahliliy jurnali, №1(23), 2023, -Б. 23-28. (05.00.00; №10).

6. Tashev K.A., Fayziyeva D.S., Yuldasheva N.S., “Bank tizimlarida zaifliklar va tahdidlar tahlili” // Muhammad al-Xorazmiy avlodlari ilmiy-amaliy va axborot-tahliliy jurnali, №4(26), 2023, -Б. 219-223. (05.00.00; №10).

7. Yuldasheva N.S., “Shaxsni ovozi asosida identifikatsiyalash tizimining asosiy masalalari”// “Al-Farg‘oniy avlodlari” elektron ilmiy jurnali Vol.1, Iss.2, 2024 y. ISSN 2181-4252.

8. Yuldasheva N.S., “A threat model for voice-based applications” // The American Journal of Engineering and Technology, Volume 6 | Issue 05 | September, 2023, (ISSN –2689-0984), -P. 37–42. (doi.org/10.37547).

9. Yuldasheva N.S., Muminova S.Sh., Safojev N.N., “Aspects of information security in the electronic document management system (EDMS) for bank system”// Research and Education, ISSN: 2181-3191 (E), Volume 1 | Issue 9, December, 2022, -P. 331-340. (23, Scientific Journal Impact Factor, SJIF=2023: 5.789).

10. Юлдашева Н.С., Холимтаева И.У., “Банк тизимида содир этилган фирибгарликни техник усулларининг тахлили” // Educational Research in Universal Sciences, ISSN: 2181-3515 (E), Volum 1 | Issue 6 | November, 2022, -P. 158-162. (23, Scientific Journal Impact Factor, SJIF=2023: 5.564).

11. Файзиева Д.С., Юлдашева Н.С., “Шахнинг нутқи асосида таниб олиш ёндашувлари” // Educational Research in Universal Sciences, ISSN: 2181-3515 (E), Volume 2, Issue 8, August, 2023, –P. 131-138. (23, Scientific Journal Impact Factor, SJIF=2023: 5.564).

## **II bo‘lim (II часть; II part)**

12. Сагатов М.В., Юлдашева Н.С., “Банк тизимларида ахборотни химоялашнинг ўзига хос хусусиятлари” // “Иқтисодийётнинг тармоқларини инновацион ривожланишида ахборот-коммуникация технологияларининг аҳамияти” республика илмий-техник анжуманининг маърузалар тўплами, 2-қисм, Тошкент-2019, 14-15 март, -Б. 241-242.

13. Ташев К.А., Файзиева Д.С., “Масофавий банк хизматларида хавфсизлик масаласи” // “Iqtisodiyot tarmoqlarining innovatsion rivojlanishida axborot kommunikatsiya texnologiyalarining ahamiyati” respublika ilmiy-texnik anjumani, Toshkent-2022, 10-11-mart, -B. 366-369.

14. Юлдашева Н.С., Кудратиллаев М.Б., “Кибербезопасность в банковской сфере” // “Iqtisodiyot tarmoqlarining innovatsion rivojlanishida axborot kommunikatsiya texnologiyalarining ahamiyati” respublika ilmiy-texnik anjumani, Toshkent-2022, 10-11-mart, -C. 400-402.

15. Yuldasheva N.S., Tashmatova Sh.S., Qurbonova K.E., “Графическая систем аутентификации для безопасной передачи файлов в банковской системе”// Scientific horizon in the context of social crise, September 24, 2022, Tokyo, Japan, -P. 179-189.

16. Yuldasheva N.S., Tashmatova Sh.S., Qurbonova K.E., “Разработка приложения для мобильного банкинга с усилением безопасности” // Scientific horizon in the context of social crise, September, 2022, Tokyo, Japan, -P. 190-195.

17. Юлдашева Н.С., “Шахсни овози асосида идентификациялаш тизимини ишлаб чиқишдаги муаммолари” // “Smart armiyada axborot - kommunikatsiya texnologiyalari intellektual tizimlar va innovatsiyalarni joriy qilish istiqboli” respublika ilmiy-amaliy konferensiyasi, Toshkent 2023, –B. 337-340.

18. Ganiyev S.K., Yuldasheva N.S., Niyozmatova N.A., Samijonov A.N., Dusonov X.T., “Shaxsni identifikatsiyalash va autentifikatsiyalash mobil ilovasi” // Elektron hisoblash mashinalari uchun yaratilgan dasturning rasmiy ro‘yxatdan o‘tkazilganligi to‘g‘risidagi guvohnoma №DGU 33187, 07.02.2024.

19. Yuldasheva N.S., Niyozmatova N.A., Samijonov A.N., Nuritdinov N.D., “Shaxsni ovozi asosida tanib olishning klient-server dasturi” // Elektron hisoblash mashinalari uchun yaratilgan dasturning rasmiy ro‘yxatdan o‘tkazilganligi to‘g‘risidagi guvohnoma №DGU 33421, 13.02.2024.

20. Fayziyeva D.S., Mamatov N.S., Samijonov A.N., Jalelov K.M., “Nutq signallari belgilarini shakllantirish va shaxs modelini qurish” // Elektron hisoblash mashinalari uchun yaratilgan dasturning rasmiy ro‘yxatdan o‘tkazilganligi to‘g‘risidagi guvohnoma №DGU 33421, 12.02.2024.

Avtoreferat « Muhammad al-Xorazmiy avlodlari » jurnali tahririyatida tahrirdan o'tkazilib, o'zbek, rus va ingliz tillaridagi matnlar o'zaro muvofiqlashtirildi.

**Bosmaxona litsenziyasi:**



**9338**

Bichimi: 84x60 <sup>1</sup>/<sub>16</sub>. «Times New Roman» garniturası.  
Raqamli bosma usulda bosildi.  
Shartli bosma tabog'i: 3. Adadi 100 dona. Buyurtma № 41/24.

Guvohnoma № 851684.  
«Tipograff» MCHJ bosmaxonasida chop etilgan.  
Bosmaxona manzili: 100011, Toshkent sh., Beruniy ko'chasi, 83-uy.