Abdullayev Fətəli Nəriman oğlu,
siy.e.ü.f.d, dosent, Azərbaycan Milli Elmlər Akademiyası nəzdində
Respublika Seysmoloji Xidmət Mərkəzi
Ünvan: AZ1001, Azərbaycan Respublikası, Bakı şəhəri, Nigar Rəfibəyli küç., 25
E-mail: fataliabdullayev66@gmail.com
Qaziyeva Nəzakət Qurban qızı,
fil.ü.f.d., dosent, Azərbaycan Milli Elmlər Akademiyası İ.Nəsimi adına Dilçilik İnstitutu
Ünvan: AZ1073, Azərbaycan Respublikası, Bakı şəhəri, H.Cavid pr., 115
E-mail: n.qazi@inbox.ru
Vəliyev Hümmət Telman oğlu,
Azərbaycan Respublikası Ədliyyə Nazirliyinin Məhkəmə Ekspertizası Mərkəzi
Ünvan: AZ 1000, Azərbaycan Respublikası, Bakı şəhəri, Xaqani küçəsi, 24
E-mail: vel.hummat3@gmail.com
Əliyev Lətif Paşa oğlu,
f.r.ü.f.d., dosent, Azərbaycan Respublikası Ədliyyə Nazirliyinin Məhkəmə Ekspertizası Mərkəzi
Ünvan: AZ 1000, Azərbaycan Respublikası, Bakı şəhəri, Xaqani küçəsi, 24
E-mail: latif_aliyev@mail.ru

UOT: 343.93/94
DOI: https://doi.org/10.30546/2218-9130.041.2026.4021

SƏS BİOMETRİYASI VƏ "SPOOFİNG" ƏLEYHİNƏ TƏDBİRLƏR: MİLLİ KİBERTƏHLÜKƏSİZLİK STRATEGİYASI KONTEKSTİNDƏ

Açar sözlər: *səs biometriyası, kibertəhlükəsizlik, spoofing, autentifikasiya, səs klonlaması.*

Ключевые слова: *голосовая биометрия, кибербезопасность, спуфинг, аутентификация, клонирование голоса.*

Keywords: *voice biometrics, cybersecurity, spoofing, authentication, voice cloning.*

Azərbaycan Respublikası Prezidentinin 23 may 2007-ci il tarixli 2198 nömrəli Sərəncamı ilə təsdiq edilmiş "Azərbaycan Respublikasının milli təhlükəsizlik konsepsiyası" [1] ölkədə şəxsiyyətin, cəmiyyətin və dövlətin xarici və daxili təhdidlərdən qorunmasına yönəlmiş siyasət və tədbirlərin məqsəd, prinsip və yanaşmalarını əks etdirir. Bu konsepsiya Azərbaycan Respublikasının milli maraqlarını və təhlükəsizlik siyasətinin əsas istiqamətlərini müəyyən edir və milli təhlükəsizlik siyasətinin əsasını təşkil edir.

Azərbaycan Respublikasının informasiya məkanının müasir təhdidlərdən qorunması milli təhlükəsizliyin mühüm istiqamətlərindən biri olduğundan, dövlətin, cəmiyyətin və vətəndaşların müasir informasiya-kommunikasiya texnologiyalarından (İKT) təhlükəsiz istifadəsini təmin

etmək məqsədilə hazırlanmış "Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023–2027-ci illər üçün Strategiyası" [2] kritik informasiya infrastrukturlarının təhlükəsizliyinin təmin olunmasına dair tədbirlərin müəyyənləşdirilməsini və həyata keçirilməsini təşkil edir. Həmçinin, bu strategiya fərdi məlumatların qorunmasını təmin edir və Azərbaycan Respublikasının Konstitusiyası ilə təsbit edilmiş insan hüquq və azadlıqlarına riayət edilməsinə daha əlverişli şərait yaradır.

Qloballaşan dünyada informasiya təhlükəsizliyinin və kibertəhlükəsizliyin təmin olunması həm milli, həm də beynəlxalq səviyyədə prioritet məsələyə çevrildiyindən, kibertəhlükəsizlik sahəsində milli ekosistemin formalaşdırılması və inkişafı istiqamətində əməli fəaliyyət xüsusi aktuallıq kəsb edir. Müasir dünyanın əsas problemlərindən biri olan informasiya təhlükəsizliyi, "Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023–2027-ci illər üçün Strategiyası"nda qeyd edildiyi kimi, bir sıra digər trendlərlə yanaşı, konfidensiallığın gücləndirilməsi məqsədilə kritik texnologiyaların, o cümlədən çoxfaktorlu autentifikasiya və texniki vasitələrin identifikasiyasının (2.1.5.) tətbiqini də əhatə edir.

Çoxfaktorlu autentifikasiya tətbiqə və ya rəqəmsal resursa daxil olmaq üçün istifadəçidən iki və ya daha çox identifikasiya metodunun təqdim edilməsini tələb edən təhlükəsizlik mexanizmidir. Bir neçə identifikasiya metodundan istifadə edilməsi kiberhücum ehtimalını əhəmiyyətli dərəcədə azaldır. Çoxfaktorlu autentifikasiya biometrik texnologiyalarla tamamlandıqda isə bu mexanizm daha dayanıqlı və təhlükəsiz xarakter alır.

Kibercinayətkarların barmaq izi və üz maskaları yaratmaq məqsədilə 3D printerlərdən istifadə etməyə cəhd göstərmələrinə baxmayaraq, səsin klonlaşdırılması ilə bağlı faktların mövcudluğu nəzərə alınsa belə, düzgün metodların tətbiqi şəraitində səs biometriyasına əsaslanan autentifikasiya sistemlərini sındırmaq daha çətindir. "Səs izi"nin saxtalaşdırılmasının mürəkkəb olmasının əsas səbəblərindən biri onun fiziki olaraq istifadəçinin özündə mövcud olması və saxlanılmasıdır ki, bu da yoxlama prosesinin istifadə olunan cihazdan asılı olmamasını təmin edir. Bundan əlavə, səs biometriyası spoofinq əleyhinə proqram təminatı ilə təchiz oluna bilər ki, bu da sintetik səslərdən və ya əvvəlcədən qeydə alınmış səs yazılarının səsləndirilməsi yolu ilə həyata keçirilən infiltrasiya cəhdlərini aşkar etməyə və onların qarşısını almağa imkan verir.

Müasir qloballaşma dövründə milli təhlükəsizlik sisteminin təkmilləşdirilməsi, terrorçuluq, qanunsuz miqrasiya və cinayətkarlığın doğurduğu digər təhdidlərə qarşı mübarizədə nitq texnologiyalarının təqdim etdiyi müasir üsulların tətbiqi xüsusi aktuallıq kəsb edir. Biometrik identifikasiya və verifikasiya vasitəsi kimi səs siqnalının təhlili, həmçinin səs nümunəsi əsasında milli mənsubiyyətin müəyyən olunması, gələcəkdə yaradılacaq Vahid Biometrik Sistem çərçivəsində Səs İzi Bazasının tərkib hissəsi kimi həll olunması gözlənilən məsələlərdəndir.

Çoxfaktorlu autentifikasiyada səs biometriyası parolların saxlanılması yükünü, inteqrasiya və arxa plan xərclərini azaldır. Şirkətin sistemində yaradılmış və saxlanılan etibarlı səs izi sayəsində hər zəng üçün real vaxtda risk xalları müəyyən edilə bilir. Real vaxt rejimində əldə olunan bu məlumat qeyri-səs biometriyası istifadəçiləri üçün əlverişlidir, çünki müasir ağıllı cihazların əksəriyyəti artıq səs biometriyasını çoxfaktorlu autentifikasiya amili kimi istifadə etməyə imkan verən mikrofonlarla təchiz olunub. Son tədqiqatlara görə, səs biometriyası dəqiqlik və istifadə rahatlığı baxımından digər biometrik üsullarla müqayisədə ən optimal variant hesab edilə bilər.

Müasir səs biometrik sistemlərdə təhlükəsizliyin təmin edilməsi yalnız statik identifi-

kasiya mexanizmləri ilə məhdudlaşmır və risk əsaslı, adaptiv autentifikasiya modellərinin tətbiqini zəruri edir. Risk əsaslı yanaşma autentifikasiya prosesində istifadəçinin davranış xüsusiyyətlərini, texniki mühitini və kontekstual parametrləri real vaxt rejimində qiymətləndirməyə imkan verir. Bu modeldə səs izi əsas identifikasiya faktoru kimi çıxış etsə də, qərar qəbuletmə prosesi əlavə risk indikatorları ilə tamamlanır.

Adaptiv autentifikasiya mexanizmləri istifadəçinin səs siqnalının keyfiyyəti, fon akustikası, cihaz xüsusiyyətləri və əvvəlki autentifikasiya tarixçəsi kimi parametrləri təhlil edərək risk səviyyəsini müəyyən edir. Risk göstəriciləri yüksəldikdə sistem əlavə təhlükəsizlik tədbirləri – əlavə biometrik yoxlama, təsdiqləyici suallar və ya digər autentifikasiya faktorlarının tətbiqini avtomatik şəkildə aktivləşdirə bilər. Bu yanaşma səs klonlaması və mürəkkəb spoofing hücumları fonunda səs biometriyasının etibarlılığını əhəmiyyətli dərəcədə artırır.

Səs biometriyasında natiqin tanınması şərtləri həm natiqin yoxlanılmasını, həm də spikerin identifikasiyasını əhatə edir. Bu proses istifadəçinin səsindən istifadə etməklə həyata keçirilən autentifikasiya mexanizmidir. Burada iki mühüm mərhələ – qeydiyyat və autentifikasiya fərqləndirilir.

Qeydiyyat mərhələsində istifadəçinin səs çapı funksiyaların çıxarılması prosesindən keçir. Uğurlu qeydiyyatdan sonra, istifadəçi sistemə autentifikasiya etmək istədikdə, onun səs çapı qeydiyyat mərhələsində olduğu kimi funksiyaların çıxarılması prosesinə məruz qalır. Ölçmələrin nəticələri oxşarlığı yoxlamaq məqsədilə verilənlər bazasındakı mövcud modellə müqayisə edilir və sistem istifadəçinin qəbul edilib-edilməməsi barədə qərar verir.

"Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023–2027-ci illər üçün Strategiyası"nda qarşıya qoyulan məqsədlər arasında informasiya təhlükəsizliyinin təmin edilməsi, kibertəhlükəsizlik sənayesinin formalaşdırılması, informasiya mühafizəsi texnologiyaları sahəsində xarici asılılığın minimallaşdırılması, proqram mühəndisliyinin və rəqəmsal iqtisadiyyatın inkişaf etdirilməsi (5.1.4.) və informasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində innovativ həllərin və startapların təşviqi, dəstəklənməsi, yeni məhsul və xidmətlərin yaradılması (5.1.5.) yer alır. Bu məqsədlər səs izi əsasında nitq texnologiyalarının inkişafını aktuallaşdırır.

Səs biometriyasının milli kibertəhlükəsizlik ekosisteminə inteqrasiyası dövlətin rəqəmsal suverenliyinin möhkəmləndirilməsi baxımından strateji əhəmiyyət daşıyır. Yerli səs biometrik texnologiyaların və anti-spoofing həllərinin inkişaf etdirilməsi xarici texnoloji asılılığın azaldılmasına, kritik informasiya infrastrukturunun daha dayanıqlı qorunmasına şərait yaradır.

Bu kontekstdə səs biometriyası yalnız texniki autentifikasiya vasitəsi deyil, həm də milli təhlükəsizlik risklərinin erkən aşkarlanması üçün analitik alət kimi çıxış edə bilər. Kütləvi kommunikasiya kanallarında, çağrı mərkəzlərində və distant xidmət platformalarında səs analitikası əsasında anomaliyaların aşkar edilməsi potensial kibertəhdidlərin operativ şəkildə müəyyən olunmasına imkan verir.

Biometrik əlamətlərə əsaslanan identifikasiya bütün hallarda (DNT, üz tanınması, barmaq izi və s.) mövcud parametrlərin ölçülüb müqayisə olunmasına əsaslanır və bu prinsip səs biometriyası üçün də keçərlidir. Adi identifikasiya vasitələrindən fərqli olaraq, biometrik məlumatlar konkret şəxsin fizioloji xüsusiyyətlərini və ya davranış əlamətlərini əks etdirir ki, bu da saxtakarlığı çətinləşdirir. Hər bir fərdin nitq aparatının həndəsi ölçüləri, səs büküşlərinin quruluşu, ağız və burun boşluqlarının forması onun özünəməxsus səs nümunəsini müəyyən edir. Təcrübələr göstərir ki, səs biometriyası əsa-

sında identifikasiya metodunun dəqiqliyi 97%-ə çatır.

Səs biometriyası şəxsiyyəti müəyyən etmək üçün səsin unikal xüsusiyyətlərindən istifadə edən texnologiyadır. O, bank sistemləri, korporativ proqramlar və təhlükəsizlik xidmətləri daxil olmaqla müxtəlif sahələrdə getdikcə daha geniş tətbiq olunur. Həmçinin, səs biometriyası uzaqdan müştəri xidməti, səs menyusunun avtomatlaşdırılması və əlaqə mərkəzlərində effektiv şəkildə istifadə edilə bilər.

Kibertəhlükəsizlik sahəsində "spoofing" hallarının təhlili və qarşısının alınması istiqamətində tədbirlərin həyata keçirilməsi, dövrün tələbi kimi, qarşıda duran vəzifələrdəndir. "Spoofing" təcavüzkarın özünü başqa bir şəxs kimi təqdim edərək sistemdə müvəffəqiyyətlə autentifikasiya etməyə cəhd etməsi ilə xarakterizə olunur. Bu, e-poçt ünvanları, telefon nömrələri, ünvanlar və digər müəyyənedici məlumatların saxtalaşdırılması vasitəsilə həyata keçirilir.

Müasir dövrdə texniki imkanların inkişafı səs biometriyası ilə bağlı texnologiyaların saxtakarlığa məruz qalması ehtimalını artırır və bu, təhlükəsizlik məsələlərini aktuallaşdırır. Səs biometriyası səs klonlama texnologiyası ilə bağlı risklərin azaldılmasında mühüm rol oynayır, çünki bu texnologiya istifadəçilərin şəxsiyyətini yoxlamaq üçün unikal səs xüsusiyyətlərindən istifadə edir.

Səsin klonlaşdırılması risklərinin azaldılmasında əsas problemlərdən biri saxtakarlıq cəhdlərinin qarşısını almaqdır. Anti-spoofing texnologiyaları süni və ya klonlaşdırılmış səsləri aşkar etmək üçün qabaqcıl alqoritmlərdən istifadə etməyə imkan verir. Bu alqoritmlər səsin "saxta" olduğunu göstərən anomaliyaları müəyyən etmək üçün, təqlid edilməsi çətin olan unikal tələffüz və nitq nümunələri kimi səs xüsusiyyətlərini təhlil edir.

Səsin klonlaşdırılması hallarının artması və onun kibercinayətkarlar tərəfindən hücumlarda istifadəsi ilə bağlı narahatlıqların çoxalması bu sahədə tədbir görülməsini daha da aktuallaşdırır.

Səslə bağlı əsas saxtakarlıq növləri aşağıdakılardır:

1. Təqlid. Bu növ saxtakarlıq bir şəxs tərəfindən digər şəxsin səs xüsusiyyətlərini təqlid etməklə həyata keçirilir. Təqlid digər saxtakarlıq növlərindən fərqlənir, çünki təcavüzkar onu həyata keçirmək üçün əlavə texniki vasitə və üsullardan istifadə etmir. Bu baxımdan, belə saxtakarlığa qarşı mübarizə əlavə əks tədbirlər tələb etmir və səs analizi sisteminin yüksək keyfiyyəti sayəsində aşkarlana bilir.

2. Nitqin cihaz vasitəsilə qeydə alınması (replay hücumu). Nitqin qeydi saxtalaşdırmanın sadə və effektiv formasıdır və bir çox tədqiqatçının fikrincə, bu, səs autentifikasiyası sistemləri üçün ən ciddi təhlükədir. Bu üsul, sonradan autentifikasiya sisteminə təqdim etmək üçün şəxsin nitqinin müəyyən fraqmentinin qeydə alınmasını nəzərdə tutur.

3. Nitqin çevrilməsi. Nitqin konvertasiyası insanın nitqini başqa bir şəxsin nitqinə bənzətmək məqsədilə xüsusi proqram təminatının istifadəsini nəzərdə tutur.

4. Nitqin sintezi. Bu üsul müəyyən bir şəxsin səsinin xüsusiyyətlərinə malik olan, ixtiyari mətn əsasında süni səsin yaradılmasını nəzərdə tutur.

Çoxfaktorlu autentifikasiya istifadəçidən bir neçə fərqli üsuldan istifadə edərək şəxsiyyətini yoxlamağı tələb etməklə əlavə təhlükəsizlik tədbiri təmin edir. Bu, adətən "bildiyiniz bir şey" (məsələn, parol), "sizə əlçatan olan bir şey" (məsələn, autentifikator tətbiqindən gələn kod, USB nişanı) və ya "sizdə olan bir şey" (barmaq izi və ya səs izi kimi biometrik məlumat) birləşməsini əhatə edir.

Çoxfaktorlu autentifikasiya birdən çox yoxlama faktoru təqdim etməyi tələb edən təhlükəsizlik üsuludur. Bu, təhlükəsizliyi əhəmiyyətli dərəcədə artırır, çünki parol ələ keçsə belə, təcavüzkar əlavə giriş məlumatına malik olmalıdır.

Azərbaycan Respublikası Prezidentinin 13 fevral 2007-ci il tarixli 1963 nömrəli Sərəncamı ilə təsdiq edilmiş "Azərbaycan Respublikasında biometrik eyniləşdirmə sisteminin yaradılması üzrə 2007–2012-ci illər üçün Dövlət Proqramı"nda [3] vətəndaşların fərdi biometrik xüsusiyyətləri əsasında identifikasiyası üçün digər xüsusiyyətlərlə yanaşı (barmaq izi, şəkil, dezoksiribonuklein turşusu (DNT) və s.) səs əsasında biometrik informasiya resurslarının formalaşdırılması da nəzərdə tutulmuşdur.

"Biometrik informasiya haqqında" Azərbaycan Respublikasının Qanunu (13 iyun 2008-ci il) [4], "Fərdi məlumatlar haqqında" Azərbaycan Respublikasının Qanunu (11 may 2010-cu il) [5] və "Biometrik informasiya xidmətlərinin sahələr üzrə fəaliyyətinin təşkili və tənzimlənməsi qaydaları" [6] kimi sənədlərdə səs biometriyasının tətbiqinə xüsusi diqqət ayrılması təsadüfi deyil.

"Azərbaycan Respublikasında biometrik eyniləşdirmə sisteminin yaradılması üzrə 2007–2012-ci illər üçün Dövlət Proqramı"nda [3] səs əsasında identifikasiya və verifikasiya servisinin yaradılması (2.4.2.), formalaşmış informasiya resurslarında səs əsasında axtarış və müqayisə imkanlarının təmin edilməsi nəzərdə tutulmuşdur.

Səs biometriyası əsasında nitq texnologiyalarının tətbiqi istiqamətində görüləcək işlər şəxsiyyətin müəyyən edilməsi, nitq əsasında milli mənsubiyyətin müəyyənləşdirilməsi və nitq əsasında regional-lokal xüsusiyyətlərin müəyyən edilməsi sahəsində milli servisin fəaliyyətinin təkmilləşdirilməsinə xidmət edə bilər. Bu da nəticədə "Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023–2027-ci illər üçün Strategiyası"nda [2] qeyd olunduğu kimi, informasiya mühafizəsi texnologiyaları sahəsində xaricdən birbaşa asılılığın minimallaşdırılmasına töhfə verə bilər.

Azərbaycan Respublikasında "Səs izi bazası"nın yaradılması çərçivəsində həyata keçiriləcək əsas tədbirlərdən ilkin olaraq aşağıdakılar qeyd edilə bilər:

1. Səs üzrə biometrik eyniləşdirmə sisteminin elmi-hüquqi baxımdan əsaslandırılmış formalaşdırma mexanizminin, təhlükəsizlik və istifadə siyasətinin hazırlanması və tətbiqi;

2. Səs üzrə identifikasiya və verifikasiya xidmətinin yaradılması;

3. Səs biometriyası ilə bağlı eyniləşdirmə sisteminin elmi-hüquqi baxımdan əsaslandırılmış formalaşma mexanizminin, təhlükəsizlik və istifadə siyasətinin hazırlanması və tətbiqi;

4. Səs biometriyası texnologiyalarının tətbiqi sahələrinin genişləndirilməsi;

5. Biometrik identifikasiya və verifikasiya üçün Səs izi bazasına daxil ediləcək səsin biometrik nümunəsinin cavab verməli olduğu tələblərin müəyyən olunması və müvafiq standartın hazırlanması.

Səs biometriyası sahəsində gələcək inkişaf tendensiyaları süni intellekt və dərin öyrənmə texnologiyalarının daha geniş tətbiqi ilə xarakterizə olunur. Multimodal biometrik sistemlərin – səs, üz və davranış biometrikasının inteqrasiyası autentifikasiya prosesinin dəqiqliyini və dayanıqlığını artıran perspektivli istiqamətlərdən biridir.

Eyni zamanda, səs klonlamasına qarşı dayanıqlı sistemlərin yaradılması məqsədilə sintetik nitqin aşkarlanması üzrə milli tədqiqat proqramlarının təşkili və bu sahədə elmi-eksperimental bazanın formalaşdırılması zəruridir. Bu yanaşma səs biometriyasının milli kibertəhlükəsizlik strategiyasının davamlı və uzunmüddətli komponentinə çevirir.

Biometrik əlamətlər tibb, maliyyə və digər sahələrdə fərdi məlumatların qorunması və məlumatların məxfiliyinin təmin edilməsində mühüm rol oynayır. Səs biometriyası şəxsiyyəti müəyyən etmək üçün səsin unikal xüsusiyyətlərindən istifadə edən texnologiya olduğundan, o, bank sistemləri, korporativ proqramlar və təhlükəsizlik xidmətləri daxil olmaqla müxtəlif

sahələrdə getdikcə daha geniş populyarlıq qazanır. Həmçinin, səs biometriyası uzaqdan müştəri xidməti, səs menyusunun avtomatlaşdırılması və əlaqə mərkəzləri kimi müasir texnologiyalarda da tətbiq edilir.

Beləliklə, səs biometriyası və ona inteqrasiya olunan adaptiv anti-spoofing mexanizmləri milli kibertəhlükəsizlik sisteminin funksional dayanıqlığını artıran strateji texnologiya kimi qiymətləndirilə bilər. Bu texnologiyanın elmi əsaslarla inkişaf etdirilməsi və hüquqi çərçivədə tənzimlənməsi informasiya təhlükəsizliyi sahəsində innovativ və dayanıqlı milli modelin formalaşmasına töhfə verəcəkdir.

Səs biometriyasının genişmiqyaslı tətbiqi biometrik məlumatların qorunması ilə bağlı hüquqi və etik məsələləri də aktuallaşdırır. Səs izi fərdi biometrik məlumat kimi şəxsin identifikasiyasına imkan verdiyindən, onun toplanması, saxlanılması və istifadəsi ciddi normativ tənzimləmə tələb edir. Azərbaycan Respublikasının mövcud qanunvericiliyi biometrik məlumatların yalnız qanuni əsaslar və subyektin razılığı ilə emalını nəzərdə tutur ki, bu, səs biometriyası sistemlərinin layihələndirilməsi və tətbiqi zamanı mütləq nəzərə alınmalıdır.

Etik baxımdan, səs izi bazalarının yaradılmasında şəffaflıq, məqsəd məhdudiyyəti və məlumatların minimallaşdırılması prinsiplərinə riayət olunması vacibdir. Səs biometriyasının tətbiqi şəxsin hüquq və azadlıqlarının məhdudlaşdırılmasına deyil, əksinə, onun təhlükəsizliyinin və hüquqi müdafiəsinin gücləndirilməsinə xidmət etməlidir.

Məhkəmə ekspertizası praktikasında səs biometriyasının rolu getdikcə artır. Səs nümunələrinin identifikasiyası, səs klonlamasının və süni nitqin aşkar edilməsi məhkəmə-linqvistik və fonoskopik ekspertizanın aktual istiqamətlərindən birinə çevrilir. Bu kontekstdə səs biometriyasına əsaslanan texnologiyalar sübutların etibarlılığının qiymətləndirilməsində əlavə elmi əsas rolunu oynayır.

İstifadə edilmiş ədəbiyyat siyahısı:

1. Azərbaycan Respublikasının milli təhlükəsizlik konsepsiyası // Azərbaycan Respublikası Prezidentinin 23 may 2007-ci il tarixli 2198 nömrəli Sərəncamı ilə təsdiq edilmişdir: [Elektron resurs]/URL: https://e-qanun.az/framework/13373

2. Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023–2027-ci illər üçün Strategiyası // Azərbaycan Respublikası Prezidentinin 2023-cü il 28 avqust tarixli Sərəncamı ilə təsdiq edilmişdir: [Elektron resurs]/URL: https://president.az/az/articles/view/60949

3. Azərbaycan Respublikasında biometrik eyniləşdirmə sisteminin yaradılması üzrə 2007-2012-ci illər üçün Dövlət Proqramı // Azərbaycan Respublikası Prezidentinin 2007-ci il 13 fevral tarixli 1963 nömrəli Sərəncamı ilə təsdiq edilmişdir: [Elektron resurs]/URL: https://e-qanun.az/framework/12804

4. "Biometrik informasiya haqqında" Azərbaycan Respublikasının 13 iyun 2008-ci il tarixli 651-IIIQ nömrəli Qanunu: [Elektron resurs]/URL: https://e-qanun.az/framework/15144

5. "Fərdi məlumatlar haqqında" Azərbaycan Respublikasının 11 may 2010-cu il tarixli 998-IIIQ nömrəli Qanunu [Elektron resurs]/URL: https://e-qanun.az/framework/19675

6. Biometrik informasiya xidmətlərinin sahələr üzrə fəaliyyətinin təşkili və tənzimlənməsi qaydaları // Azərbaycan Respublikası Nazirlər Kabinetinin 2009-cu il 1 aprel tarixli 50 nömrəli qərarı ilə təsdiq edilmişdir: [Elektron resurs]/URL: https://e-qanun.az/framework/16491

Абдуллаев Фатали Нариман оглу,
доктор философии по политическим наукам, доцент,
Республиканский центр сейсмологической службы
при Национальной академии наук Азербайджана
Газиева Назакат Гурбан гызы,
доктор философии по филологии, доцент Института лингвистики
им. И. Насими Национальной академии наук Азербайджана
Велиев Хуммет Тельман оглу,
Центр судебно-медицинской экспертизы
Министерства юстиции Азербайджанской Республики
Алиев Латиф Паша оглу,
доктор философии по физико-математическим наукам,
доцент, Центр судебно-медицинской экспертизы
Министерства юстиции Азербайджанской Республики

ГОЛОСОВАЯ БИОМЕТРИЯ И МЕРЫ ПРОТИВ “СПУФИНГ”А: В КОНТЕКСТЕ НАЦИОНАЛЬНОЙ СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ

РЕЗЮМЕ

В статье рассматривается применение голосовой биометрии как одной из мер, направленных на защиту личности, общества и государства от внешних и внутренних угроз в стране в рамках концепции национальной безопасности, а также преимущества этого процесса в направлении противодействия подделки голоса.

Меры, предусматривающие применение многофакторной аутентификации и идентификации с помощью технических средств, демонстрируют актуальность указанного подхода как части стратегии национальной безопасности.

Роль голосовой биометрии в судебно-медицинской практике постоянно возрастает. Идентификация голосовых образцов, выявление клонирования голоса и искусственной речи становятся одним из современных направлений судебно-лингвистической и фоноскопической экспертизы. В этом контексте технологии, основанные на голосовой биометрии, играют роль дополнительной научной основы при оценке достоверности доказательств.

Abdullayev Fatali Nariman,
PhD in Political Sciences, Associate Professor, Republican Seismological Survey Center under the National Academy of Sciences of Azerbaijan
Gazieva Nazakat Gurban,
Candidate of Philological Sciences, Associate Professor,
I. Nasimi Institute of Linguistics, Azerbaijan National Academy of Sciences
Khummet Telman Veliyev,
Forensic Medical Examination Center, Ministry of Justice, Republic of Azerbaijan
Aliyev Latif Pasha,
PhD, Associate Professor, Forensic Medical Examination Center,
Ministry of Justice of the Republic of Azerbaijan

VOICE BIOMETRICS AND ANTI-SPOOFING MEASURES: IN THE CONTEXT OF THE NATIONAL CYBERSECURITY STRATEGY

SUMMARY

The article examines the use of voice biometrics as a measure aimed at protecting individuals, society, and the state from external and internal threats within the framework of national security, as well as the advantages of this process in countering voice forgery.

Measures involving the use of multifactor authentication and technical identification demonstrate the relevance of this approach as part of a national security strategy.

The role of voice biometrics in forensic practice is constantly growing. Voice sample identification and the detection of voice cloning and artificial speech are becoming a modern area of forensic linguistic and phonoscopic examination. In this context, technologies based on voice biometrics provide an additional scientific basis for assessing the reliability of evidence.

Redaksiyaya daxilolma tarixi: 19.12.2025
Təkrar işlənməyə göndərilmə tarixi: 19.01.2026
Çapa qəbul olunma tarixi: 22.01.2026