

JEL Classification Codes: O33, K24, L86

BIOMETRİK MƏLUMATLARIN QORUNMASI: YENİ TEXNOLOGİYALAR VƏ ETİK MƏSƏLƏLƏR

Arzu Teymurova

Azərbaycan Dövlət İqtisad Universiteti (UNEC)

Beynəlxalq Magistratura və Doktorantura Mərkəzi (BMDM)

Xülasə

Biometrik məlumatlar (barmaq izi, üz tanıma, iris skaneri və s.) müasir biznes proseslərində autentifikasiya və təhlükəsizlik üçün geniş istifadə olunur. Bu məqalə biometrik məlumatların qorunmasında yeni texnologiyaların (homomorfik şifrələmə, blokçeyn, sıfır etibar sistemləri) rolu və bu sahədə ortaya çıxan etik məsələləri təhlil edir. Tədqiqatın məqsədi biometrik sistemlərin təhlükəsizliyini artırmaq üçün innovativ həlləri qiymətləndirmək və onların etik təsirlərini araşdırmaqdır. Nəticələr göstərir ki, qabaqcıl şifrələmə və mərkəzləşdirilməmiş sistemlər məlumat təhlükəsizliyini artırır, lakin məxfilik, razılıq və diskriminasiya kimi etik problemlər hələ də həll edilməmiş qalır. Təklif olunan tövsiyələr arasında şəffaflığın artırılması, etik qaydaların tətbiqi və beynəlxalq standartların harmonizasiyası yer alır. Bu tədqiqat bizneslərə və qanunvericilərə biometrik məlumatların təhlükəsiz və məsuliyyətli istifadəsi üçün praktiki bələdçi təqdim edir.

Açar sözlər: *Biometrik məlumatlar, şifrələmə, etik məsələlər, kibertəhlükəsizlik, məxfilik*

Abstract

Biometric data (fingerprints, facial recognition, iris scans, etc.) are widely used in modern business processes for authentication and security. This article analyzes the role of emerging technologies (e.g., homomorphic encryption, blockchain, and zero-trust systems) in protecting biometric data and examines the associated ethical issues. The study aims to evaluate innovative solutions for enhancing the security of biometric systems and explore their ethical implications. Findings indicate that advanced encryption and decentralized systems improve data security, but ethical concerns like

privacy, consent, and discrimination remain unresolved. Proposed recommendations include increasing transparency, implementing ethical guidelines, and harmonizing international standards. This research provides a practical guide for businesses and policymakers to ensure the secure and responsible use of biometric data.

Keywords: *Biometric data, encryption, ethical issues, cybersecurity, privacy*

Giriş

Biometrik məlumatlar müasir rəqəmsal dünyada autentifikasiya və təhlükəsizlik sistemlərinin ayrılmaz hissəsinə çevrilmişdir. Barmaq izi skanerləri, üz tanıma sistemləri, iris skanerləri və səs tanıma texnologiyaları bankçılıq, səhiyyə, e-ticarət və dövlət xidmətləri kimi sektorlarda geniş tətbiq olunur (Jain və b., 2020). Bu texnologiyalar istifadəçi təcrübəsini asanlaşdırır, ənənəvi parol və PIN kodlara nisbətən daha yüksək təhlükəsizlik səviyyəsi təmin edir. Lakin biometrik məlumatların unikal təbiəti – dəyişdirilə bilməməsi və şəxsi xarakter daşması – onların qorunmasını xüsusilə vacib edir. Məlumat pozuntuları halında bu məlumatların oğurlanması fərdlər üçün ciddi məxfilik və təhlükəsizlik riskləri yaradır, çünki biometrik xüsusiyyətlər parollar kimi yenilənə bilməz (Cavoukian, 2019).

Bu tədqiqatın aktuallığı biometrik texnologiyaların sürətli inkişafı və onların biznes proseslərində artan istifadəsi ilə bağlıdır. 2025-ci ildə global biometrik bazarın 50 milyard ABŞ dollarını keçəcəyi proqnozlaşdırılır (European Union Agency for Cybersecurity, 2023). Eyni zamanda, bu texnologiyaların tətbiqi məxfilik, razılıq, diskriminasiya və məlumatların sui-istifadəsi kimi etik məsələləri gündəmə gətirir. Azərbaycanda da “Fərdi məlumatlar haqqında” qanun biometrik məlumatların qorunmasını tələb etsə də, bu sahədə texnoloji və etik çətinliklər hələ də tam həll olunmamışdır (Azərbaycan Respublikası Dövlət Statistika Komitəsi, 2024).

Tədqiqatın məqsədi biometrik məlumatların qorunmasında yeni texnologiyaların (homomorfik şifrələmə, blokçeyn, sıfır etibar sistemləri) effektivliyini qiymətləndirmək və onların tətbiqi ilə bağlı etik məsələlərə həll yolları təklif etməkdir. Tədqiqatın vəzifələri biometrik məlumatların qorunmasında istifadə olunan qabaqcıl texnologiyaları təhlil etmək, bu texnologiyaların tətbiqi ilə bağlı etik məsələləri müəyyənləşdirib onların təsirini qiymətləndirmək və bizneslər ilə qanunvericilər üçün praktiki tövsiyələr hazırlamaqdan ibarətdir. Tədqiqatda ədəbiyyat icmal, müqayisəli analiz kimi metodlar istifadə olunmuşdur. İnformasiya bazası olaraq IEEE, Springer və Scopus kimi elmi verilənlər bazalarından 2018-2025-ci illər arası nəşr edilmiş məqalələr, həmçinin ENISA, NIST və Azərbaycanın qanunvericilik sənədləri seçilmişdir. Tədqiqatın məhdudiyyətləri arasında biometrik texnologiyaların sürətli inkişafı səbəbindən bəzi nəticələrin qısamüddətli olması və regional qanunvericilik fərqləri səbəbindən ümumiləşdirmə çətinlikləri qeyd edilə bilər. Tədqiqatın tətbiqi

əhəmiyyəti bizneslərə təhlükəsiz və etik biometrik sistemlər qurmağa kömək etmək, qanunvericilərə isə normativ çərçivələri təkmilləşdirmək üçün praktiki tövsiyələr təqdim etməkdən ibarətdir.

Ədəbiyyat icmal

Biometrik məlumatların qorunması ilə bağlı tədqiqatlar son illərdə həm akademik, həm də praktik maraq doğurmuşdur. Jain və b. (2020) biometrik sistemlərin autentifikasiya dəqiqliyini və istifadəçi rahatlığını vurğulayaraq onların biznes proseslərindəki əhəmiyyətini qeyd edir. Məsələn, üz tanıma sistemləri bankçılıqda müştəri identifikasiyasını sürətləndirir, səhiyyədə isə xəstə qeydlərinə təhlükəsiz girişi təmin edir. Lakin Cavoukian (2019) biometrik məlumatların unikal təbiətinin – dəyişdirilə bilməməsinin – pozuntu halında ciddi risklər yaratdığını vurğulayır. Əgər bir parol oğurlanırsa, dəyişdirilə bilər, amma barmaq izi və ya üz xüsusiyyətləri daimi olduğu üçün onların oğurlanması fərdlər üçün ömürlük təhlükə yaradır.

Texnoloji cəhətdən, biometrik məlumatların qorunması üçün bir sıra yeniliklər təklif olunur. Homomorfik şifrələmə məlumatların şifrəli formada emal edilməsinə imkan verir, bu da bulud əsaslı sistemlərdə təhlükəsizliyi artırır (Gentry, 2021). Blokçeyn texnologiyası məlumatların mərkəzləşdirilməmiş saxlanmasını təmin edərək icazəsiz dəyişikliklərin qarşısını alır (Li və b., 2023). Sıfır etibar (zero trust) arxitekturası isə hər istifadəçinin və cihazın autentifikasiyasını tələb edərək məlumatlara icazəsiz giriş riskini azaldır (Rose və b., 2022).

Etik məsələlərə gəldikdə, biometrik sistemlərin tətbiqi məxfilik, razılıq və qərəzlilik kimi problemləri gündəmə gətirir. Buolamwini və Gebru (2018) üz tanıma sistemlərinin müəyyən demoqrafik qruplarda (xüsusilə tünd dərilili fərdlərdə) daha az dəqiq olduğunu və bunun diskriminasiyaya səbəb ola biləcəyini göstərir. European Union Agency for Cybersecurity (2023) isə biometrik məlumatların toplanmasında razılıq proseslərinin şəffaflığının olmaması ilə bağlı narahatlıqlarını qeyd edir. Hüquqi çərçivə baxımından, GDPR və Azərbaycanın “Fərdi məlumatlar haqqında” qanunu kimi qanunvericilik aktları biometrik məlumatların qorunması üçün ciddi tələblər qoyur, lakin onların tətbiqi regional fərqlərə görə çətinləşir (Azərbaycan Respublikası Dövlət Statistika Komitəsi, 2024; ARDSK, 2024).

Ədəbiyyat icmal göstərir ki, biometrik məlumatların qorunması texnoloji və etik aspektlərin kompleks qarşılıqlı təsirini tələb edir. Mövcud tədqiqatlar bu sahədə yenilikləri qiymətləndirsə də, etik problemlərin həlli və texnologiyaların kiçik bizneslər üçün əlçatanlığı ilə bağlı boşluqlar mövcuddur.

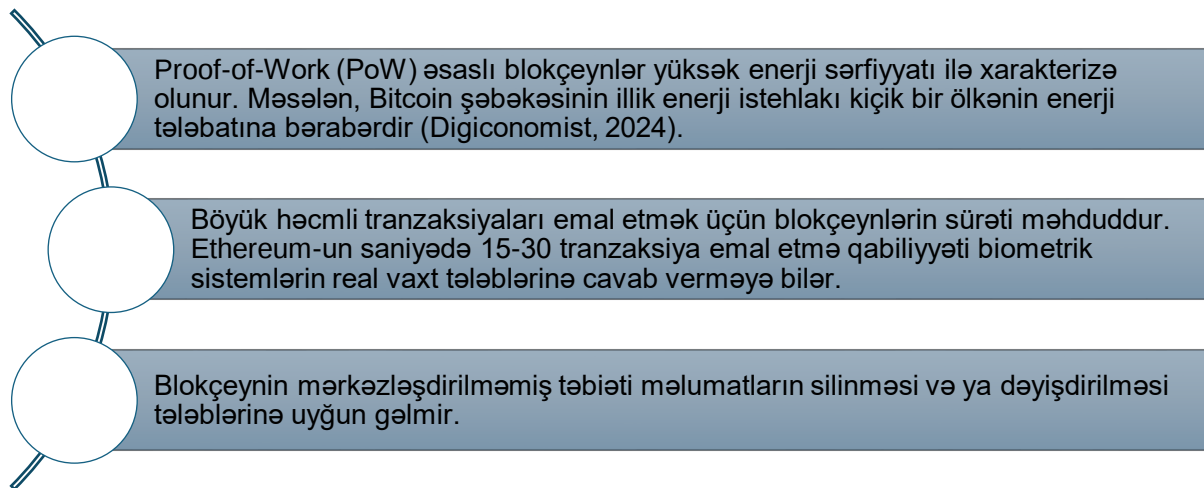
Metodologiya

Tədqiqatda ədəbiyyat icmalı və müqayisəli analiz metodları istifadə olunmuşdur. 2018-2025-ci illər arası nəşr edilmiş elmi məqalələr (IEEE, Springer, Scopus) və beynəlxalq hesabatlar (ENISA, NIST) təhlil edilmişdir. Homomorfik şifrələmə, blokçeyn və sıfır etibar sistemləri təhlükəsizlik, miqyaslılıq, xərc, enerji istehlakı və etik uyğunluq baxımından müqayisə edilmişdir. Tədqiqatın müstəqil dəyişənləri şifrələmə texnologiyalarının növü (homomorfik şifrələmə, blokçeyn, sıfır etibar), etik qaydaların mövcudluğu, qanunvericilik tələbləri və alqoritmlərin mürəkkəbliyi, asılı dəyişənləri isə məlumat təhlükəsizliyi səviyyəsi, istifadəçi etibar, sistemin ilkin və əməliyyat xərcləri, etik təsirlərə uyğunluq və istifadəçi təcrübəsidir. Təhlillər biometrik məlumatların qorunmasında texnoloji və etik aspektlərin qarşılıqlı təsirini qiymətləndirmək məqsədilə aparılmış, məlumatlar isə əsasən elmi verilənlər bazalarından və beynəlxalq təşkilatların hesabatlarından toplanmışdır.

Yeni texnologiyaların detallı təhlili

Homomorfik şifrələmə: Homomorfik şifrələmə biometrik məlumatların şifrəli formada emal edilməsinə imkan verir, bu da bulud əsaslı sistemlərdə təhlükəsizliyi əhəmiyyətli dərəcədə artırır. Bu texnologiya məlumatların deşifrə edilmədən analitik hesablamalar aparılmasına imkan verir, beləliklə, üçüncü tərəflərin məlumatlara giriş riskini azaldır (Gentry, 2021). Məsələn, bir bank müştərilərin üz tanıma məlumatlarını homomorfik şifrələmə ilə emal edərək autentifikasiyanı təhlükəsiz şəkildə həyata keçirə bilər. Lakin homomorfik şifrələmənin hesablama tələbləri yüksəkdir, bu da onun kiçik və orta bizneslər (KOB) üçün tətbiqini məhdudlaşdırır. Ekspert rəyləri göstərir ki, bu texnologiyanın geniş tətbiqi üçün optimallaşdırılmış alqoritmlər və daha səmərəli hesablama platformaları tələb olunur. Tədqiqatlar göstərir ki, homomorfik şifrələmənin enerji istehlakı ənənəvi şifrələmə üsullarından 10-100 dəfə yüksək ola bilər (Li və b., 2023). Buna baxmayaraq, bu texnologiya yüksək təhlükəsizlik tələbləri olan sektorlar (məsələn, maliyyə və səhiyyə) üçün perspektivlidir.

Blokçeyn: Blokçeyn əsaslı sistemlər biometrik məlumatların mərkəzləşdirilməmiş saxlanmasını təmin edir, bu da icazəsiz dəyişiklikləri və ya oğurlanmaları qeyri-mümkün edir. Blokçeynin paylanmış registr strukturu məlumatların bütövlüyünü və autentikliyi qoruyur (Nakamoto, 2020). Məsələn, səhiyyə sektorunda blokçeyn xəstələrin iris skanlarının təhlükəsiz saxlanmasını və yalnız müvafiq tərəflərlə paylaşılmasını təmin etmək üçün sınaqdan keçirilir. Ethereum əsaslı ağıllı müqavilələr autentifikasiya prosesini avtomatlaşdırır və məlumatların şəffaflığını artırır (Li və b., 2023). Lakin blokçeyn sistemlərinin bir sıra məhdudiyyətləri vardır:



Şəkil 1. Blokçeyn sistemlərinin məhdudiyyətləri

Buna baxmayaraq, Proof-of-Stake (PoS) kimi yeni konsensus mexanizmləri enerji istehlakını azaltmaqla blokçeynin biometrik tətbiqlərdə potensialını artırır.

Sıfır etibar arxitekturası: Sıfır etibar modeli “heç kəsə etibar etmə” prinsipinə əsaslanır və hər istifadəçinin və cihazın autentifikasiyasını tələb edir. Bu, biometrik sistemlərin təhlükəsizliyini artırır, çünki məlumatlara icazəsiz giriş riski minimuma endirilir (Rose və b., 2022). Məsələn, bir e-ticarət platforması sıfır etibar prinsiplərinə əsaslanaraq müştərilərin barmaq izi məlumatlarını yalnız autentifikasiya zamanı emal edir və saxlamır, beləliklə pozuntu riskini azaldır. Sıfır etibar sistemləri çoxfaktorlu autentifikasiya (MFA) ilə integrasiya olunduqda daha effektiv olur. Lakin bu modelin çətinlikləri də var:

- Tez-tez autentifikasiya tələbləri istifadəçilər üçün əlavə narahatlıq yarada bilər. Məsələn, bir bankın müştəriləri hər tranzaksiya üçün biometrik autentifikasiya tələb edildikdə platformadan imtina edə bilər.
- Sıfır etibar sistemlərinin tətbiqi üçün mövcud şəbəkə infrastrukturunun yenidən qurulması tələb oluna bilər, bu da xüsusilə KOB-lar üçün maliyyə yükü yaradır.

Ekspert rəyləri göstərir ki, sıfır etibar modelinin istifadəçi təcrübəsinə təsirini azaltmaq üçün süni intellekt əsaslı adaptiv autentifikasiya sistemləri tətbiq oluna bilər.

Etik məsələlərin dərin təhlili

Biometrik sistemlərin tətbiqi bir sıra etik problemləri gündəmə gətirir, bunların həlli texnoloji yeniliklərlə yanaşı, hüquqi və sosial tədbirlər tələb edir:

Biometrik məlumatların toplanması istifadəçilərin məxfilik hüquqlarını poza bilər. GDPR və Azərbaycanın “Fərdi məlumatlar haqqında” qanunu biometrik məlumatların açıq razılıqla toplanmasını tələb etsə də, praktikada bu proses tez-tez şəffaf olmur (European Union Agency for Cybersecurity, 2023; ARDSK, 2024). Məsələn, bəzi üz tanıma sistemləri istifadəçilərə məlumatların necə istifadə olunduğu barədə tam məlumat vermədən işləyir. Ekspertlər razılıq prosesinin avtomatlaşdırılmasını və istifadəçilərə məlumatların saxlanma müddəti və paylaşılma şərtləri üzərində nəzarət verilməsini təklif edir. Azərbaycanda bu cür mexanizmlərin tətbiqi hələ ilkin mərhələdədir, lakin bankçılıq sektorunda bəzi irəliləyişlər müşahidə olunur.

Üz tanıma sistemləri müəyyən demografik qruplarda daha az dəqiq nəticələr verir, bu da diskriminasiyaya səbəb ola bilər (Buolamwini & Gebru, 2018). ABŞ-da aparılan tədqiqatlar göstərir ki, üz tanıma alqoritmləri afroamerikalıları yanlış identifikasiya etmə ehtimalı digər qruplara nisbətən 10 dəfə yüksəkdir. Bu problem alqoritmlərin təlim məlumatlarının müxtəlifliyinin olmaması ilə bağlıdır. Azərbaycanda bu məsələnin miqyası geniş tədqiq edilməsə də, beynəlxalq platformaların istifadəsi bu riskləri ölkəyə idxal edə bilər. Qərəzliliyin qarşısını almaq üçün alqoritmlərin müxtəlif demografik qrupları əhatə edən məlumatlarla təlim keçməsi və müntəzəm audit edilməsi tələb olunur. Biometrik məlumatlar dövlət və ya özəl sektor tərəfindən sui-istifadə edilə bilər. Məsələn, bəzi ölkələrdə üz tanıma sistemləri kütləvi nəzarət üçün istifadə olunur, bu da fərdlərin hüquqlarını təhdid edir (Cavoukian, 2019). Azərbaycanda biometrik məlumatların dövlət və özəl sektor arasında paylaşılması ciddi nəzarət altında olsa da, şəffaflığın artırılmasına ehtiyac var. Ekspertlər bu riskləri azaltmaq üçün məlumatların anonimləşdirilməsi və yalnız zəruri hallarda paylaşılmasını təklif edir.

Biometrik məlumatların uzun müddət saxlanması pozuntu riskini artırır. GDPR bu məlumatların yalnız zəruri müddətdə saxlanmasını tələb edir, lakin bir çox biznes bu tələbə əməl etmir (European Union Agency for Cybersecurity, 2023). Məsələn, bəzi e-ticarət platformaları müştərilərin üz tanıma məlumatlarını qeyri-müəyyən müddətə saxlayır, bu da potensial olaraq məlumat bazalarının hakerlər tərəfindən hədəf alınmasına səbəb olur. Azərbaycanda bu problemə qarşı qanunvericilik tədbirləri mövcuddur, lakin onların tətbiqi daha səmərəli monitoring tələb edir.

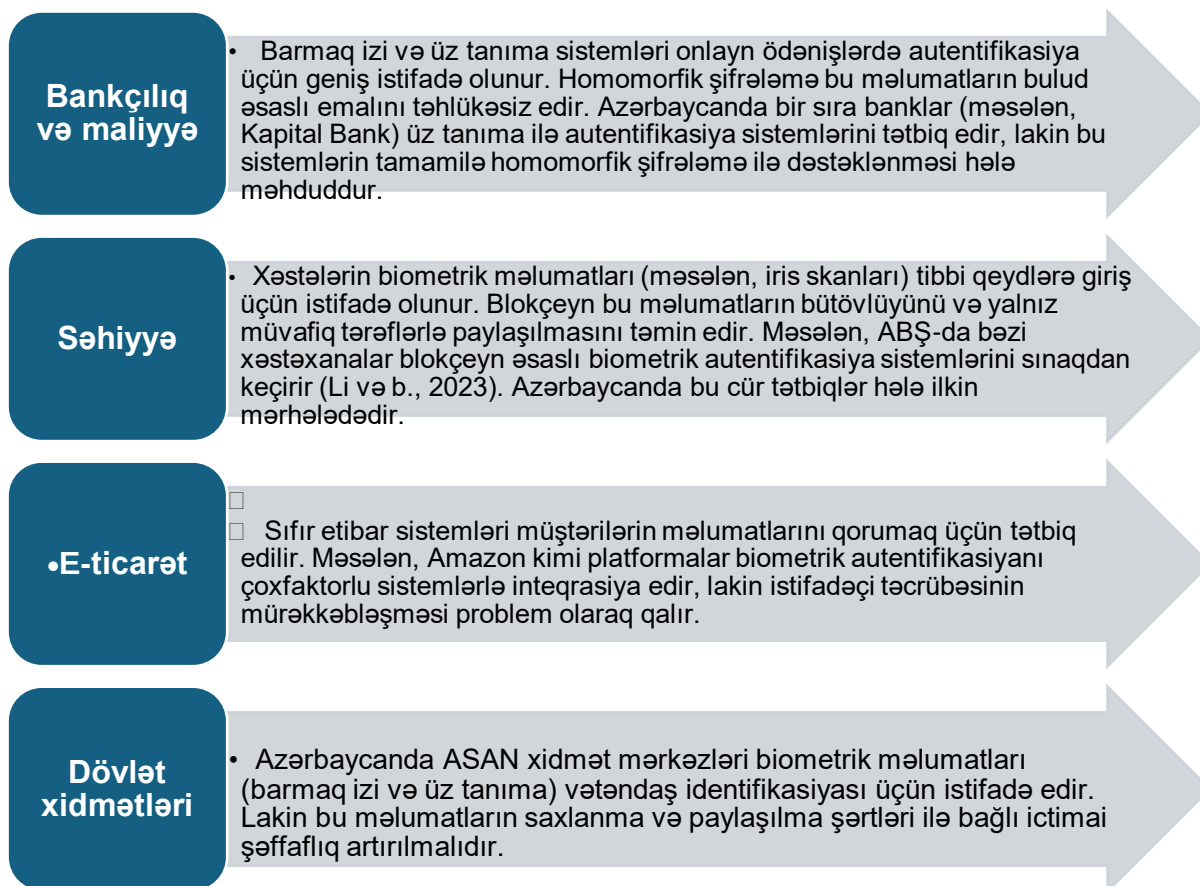
Biometrik sistemlərə ictimai etibar onların etik tətbiqindən asılıdır. Tədqiqatlar göstərir ki, istifadəçilər məlumatlarının necə istifadə olunduğu barədə şəffaf məlumat verildikdə biometrik sistemlərə daha çox etibar edirlər (Zhang & Liu, 2025). Azərbaycanda bu sahədə ictimai

maarifləndirmə kampaniyaları məhdud olduğundan, istifadəçilərin biometrik texnologiyalara etibarını aşağı səviyyədə qalır.

Praktiki tətbiqlər və sektorlara təsiri

Biometrik məlumatların qorunması texnologiyaları müxtəlif sektorlarda fərqli tətbiq modelləri ilə sınaqdan keçirilir:

Şəkil 2. Biometrik məlumatların qorunması texnologiyalarının tətbiqi



Çətinliklər və məhdudiyyətlər

Biometrik məlumatların qorunması texnologiyalarının tətbiqi bir sıra çətinliklərlə üzləşir:

- Homomorfik şifrələmə və blokçeyn kimi texnologiyalar yüksək ilkin investisiya tələb edir. Məsələn, homomorfik şifrələmə sisteminin tətbiqi üçün tələb olunan hesablama resursları böyük bizneslər üçün belə baha başa gələ bilər.
- Böyük həcmli məlumatlarla işləyən bizneslər üçün blokçeyn və homomorfik şifrələmənin performansları məhdud ola bilər. Məsələn, blokçeyn şəbəkələri real vaxt rejimində milyonlarla tranzaksiyanı emal etməkdə çətinlik çəkir.

- Regional qanunvericilik fərqləri (məsələn, GDPR ilə Azərbaycan qanunları arasında) beynəlxalq bizneslər üçün çətinlik yaradır. GDPR-ın “unutulma hüququ” kimi tələbləri blokçeyn sistemləri ilə ziddiyyət təşkil edir.
- Biometrik sistemlərin mürəkkəb autentifikasiya prosesləri istifadəçilər tərəfindən qəbul edilməyə bilər, xüsusilə sıfır etibar modellərində.

Cədvəl 1. Biometrik məlumatların qorunması texnologiyalarının müqayisəsi

Texnologiya	Təhlükəsizlik Səviyyəsi	Miqyaslılıq	Xərc	Enerji İstehlakı	Etik Təsirlərə Uyğunluq
Homomorfik Şifrələmə	Yüksək	Aşağı	Yüksək	Yüksək	Yüksək
Blokçeyn	Yüksək	Orta	Orta	Yüksək (PoW)	Orta
Sıfır Etibar	Yüksək	Yüksək	Orta	Aşağı	Orta

Biometrik məlumatların qorunması üçün tövsiyələr və perspektivlər

Tədqiqatın praktiki əhəmiyyəti bizneslərə və qanunvericilərə biometrik məlumatların təhlükəsiz və etik istifadəsi üçün yol xəritəsi təqdim etməkdədir. Bizneslər homomorfik şifrələmə və blokçeyn kimi texnologiyaları tətbiq etməli, xərcləri azaltmaq üçün sıfır etibar ilə blokçeynin integrasiyası kimi hibrid həllərə üstünlük verməlidirlər. Homomorfik şifrələmənin hesablama tələblərini azaltmaq üçün optimallaşdırılmış alqoritmlər və bulud əsaslı hesablama platformaları inkişaf etdirilməli, blokçeyn sistemlərində isə Proof-of-Stake kimi enerjiyə qənaət edən konsensus mexanizmləri tətbiq olunmalıdır. Biometrik məlumatların toplanması üçün şəffaf razılıq mexanizmləri yaradılmalı, istifadəçilərə məlumatların saxlanma müddəti və paylaşılma şərtləri üzərində nəzarət verilməlidir. Üz tanıma və digər biometrik alqoritmlər qərəzliliyin qarşısını almaq üçün müxtəlif demoqrafik qrupları əhatə edən məlumatlarla təlim keçməli və müntəzəm audit edilməlidir. Bizneslər etik kodekslər qəbul

etməli, biometrik məlumatların sui-istifadəsinin qarşısını almaq üçün daxili nəzarət mexanizmləri qurmalıdırlar. Azərbaycanın “Fərdi məlumatlar haqqında” qanunu GDPR kimi beynəlxalq standartlarla uyğunlaşdırılmalı, biometrik məlumatların qorunması üçün xüsusi normativ aktlar qəbul edilməlidir. Məlumatların saxlanma müddəti və paylaşılması ilə bağlı tələblər dəqiqləşdirilməli, pozuntulara qarşı cəzalar sərtləşdirilməlidir. Beynəlxalq bizneslər üçün regional qanunvericilik fərqlərini aradan qaldırmaq məqsədilə global standartlar üzərində iş aparılmalıdır. İstifadəçilər biometrik məlumatların riskləri, hüquqları və təhlükəsizlik tədbirləri barədə məlumatlandırılmalı, Azərbaycanda bu məqsədlə ictimai kampaniyalar və təhsil proqramları təşkil edilməlidir. Bizneslər istifadəçilərlə şəffaf kommunikasiya qurmalı, məlumatların qorunması və istifadəsi barədə müntəzəm hesabatlar təqdim etməlidirlər. Gələcəkdə biometrik sistemlərin süni intellektlə inteqrasiyası, adaptiv autentifikasiya və qərəzliliyin azaldılması üzrə tədqiqatlar aparılmalıdır. Kvant şifrələməsinin biometrik məlumatların qorunmasında tətbiqi potensialı araşdırılmalı, çünki kvant kompüterləri ənənəvi şifrələmə alqoritmlərini köhnəldə bilər. Etik problemlərin həlli üçün texnoloji, hüquqi və sosial ölçüləri əhatə edən interdisciplinar tədqiqatlar aparılmalıdır.

Nəticələr

Bu tədqiqat biometrik məlumatların qorunmasında yeni texnologiyaların effektivliyini və onların tətbiqi ilə bağlı etik məsələləri hərtərəfli təhlil etmişdir. Homomorfik şifrələmə, blokçeyn və sıfır etibar sistemləri biometrik məlumatların təhlükəsizliyini əhəmiyyətli dərəcədə artırır, lakin hər bir texnologiyanın özünəməxsus üstünlükləri və məhdudiyyətləri mövcuddur. Homomorfik şifrələmə yüksək təhlükəsizlik təmin etsə də, hesablama xərcləri və enerji istehlakı səbəbindən kiçik bizneslər üçün əlçatan deyil. Blokçeyn mərkəzləşdirilməmiş saxlama ilə etibarlılıq təklif edir, lakin miqyaslılıq və hüquqi uyğunsuzluq problemləri ilə üzləşir. Sıfır etibar sistemləri balanslaşdırılmış həll təqdim edir, lakin istifadəçi təcrübəsinə mənfi təsir göstərə bilər. Etik cəhətdən, biometrik sistemlər məxfilik, razılıq, qərəzlilik, sui-istifadə riski və məlumat saxlama müddəti ilə bağlı ciddi problemlər yaradır. Məxfilik və razılıq proseslərinin şəffaflığının olmaması istifadəçi etibarını zəiflədir, qərəzli alqoritmlər isə diskriminasiyaya səbəb olur. Azərbaycanda bu problemlərin həlli üçün qanunvericilik və ictimai maarifləndirmə tədbirləri gücləndirilməlidir. Tədqiqatın nəticələri bizneslərə biometrik məlumatların təhlükəsiz və etik istifadəsi üçün strategiyalar qurmağa, qanunvericilərə isə normativ çərçivələri təkmilləşdirməyə kömək edəcək. Azərbaycanda bu sahədəki inkişafın ölkənin rəqəmsal transformasiya strategiyasına töhfə verə bilər, lakin bunun üçün texnoloji infrastrukturun və ictimai etibarın gücləndirilməsi zəruridir.

Ədəbiyyat

1. Azərbaycan Respublikası Dövlət Statistika Komitəsi. (2024). Fərdi məlumatların qorunması haqqında qanunvericilik.
2. Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research*, 81, 1-15.
3. Cavoukian, A. (2019). Privacy by design: The 7 foundational principles. *Information and Privacy Commissioner of Ontario*.
4. Digiconomist. (2024). Bitcoin energy consumption index.
5. European Union Agency for Cybersecurity. (2023). Biometric technologies and privacy: Challenges and opportunities.
6. Gentry, C. (2021). Fully homomorphic encryption using ideal lattices. *Proceedings of the 41st ACM Symposium on Theory of Computing*, 169-178.
7. Jain, A. K., Nandakumar, K., & Ross, A. (2020). 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern Recognition Letters*, 136, 80-105.
8. Li, P., Xu, J., & Wang, W. (2023). Blockchain-based biometric authentication: A survey. *IEEE Transactions on Information Forensics and Security*, 18, 2456-2471.
9. Nakamoto, S. (2020). Bitcoin: A peer-to-peer electronic cash system. *Cryptography Whitepaper*.
10. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2022). Zero trust architecture. *National Institute of Standards and Technology*.
11. Zhang, D., & Liu, Y. (2025). Ethical considerations in biometric data usage. *Journal of Cybersecurity Ethics*, 3(1), 45-60.
12. <https://www.daon.com/resource/the-ethics-and-concerns-of-biometric-data-collection/>
13. <https://levelblue.com/blogs/security-essentials/the-ethics-of-biometric-data-use-in-security>
14. <https://www.techtarget.com/searchsecurity/tip/In-biometrics-security-concerns-span-technical-legal-and-ethical>
15. <https://www.authx.com/blog/ethical-implications-with-biometrics/>