BİOMETRİK İNFORMASİYALAR SİSTEMLƏRİNDƏ XƏTA VƏ İMTİNALARIN TƏDQİQİ

Məhərrəmova M.A.
(BDU, Tətbiqi riyaziyyat və kibernetika fakültəsi)
mmaharramova95@gmail.com

Xülasə: *İşdə informasiyanın ötürülməsi prosesində təhlükəsizliyin təmin edilməsi, biometrik qeydiyyat, verifikasiya, əsas və əlavə biometrik parametrlərə görə identifikasiya məsələləri tədqiq olunmuşdur. Eyni zamanda biometrik identifikasiya sistemlərinin xətaları və bu sistemlərdə baş verən yalnış giriş imtinaları araşdırılmışdır.*

Açar sözlər: *autentifikasiya, biometrik identifikasiya, xətalar, təhlükəsizlik, informasiya*

Biometrik texnologiyalardan istifadə edilməsi maddi obyektlərə və informasiyaya qeyri-qanuni girişi etibarlı şəkildə qorumağa, həmçinin şəxsiyyətin yüksək dərəcədə identifikasiya olunmasını təmin etməyə imkan verir. Biometrik sistemlər informasiya təhlükəsizliyi sistemlərinin vacib elementinə çevrilirlər. Buna görə də onların özləri yüksək təhlükəsizlik tələblərinə cavab verməlidir. Təhlükəsizliyi kəmiyyətcə qiymətləndirmək çox çətindir. Biometrik şəbəkələrdən istifadə etməklə bir sıra təhlükəli təzahürlərin qarşısını almaq olar [1]. Hazırda ölkələrin əksəriyyəti şəxsiyyəti təsdiq edən sənədlərə biometrik əlamətlərin daxil edilməsi üzrə proqramları həyata keçirmək mərhələsindədir. Şübhə yoxdur ki, gələcəkdə biometrik texnologiyaların tətbiq sahələri daha da genişlənəcəkdir. Lakin biometrik texnologiyaların təhlükəsiz

autentifikasiya vasitəsi kimi tətbiq edilməsi ilə eyni vaxtda onlara qarşı bir sıra hücumlar da meydana çıxmışdır. *Autentifikasiya* - subyekt tərəfindən sistemə daxil edilmiş məlumatların həqiqiliyinin yoxlanması prosesidir. Məsələn, subyekt tərəfindən sistemə daxil edilən ID domain istifadəçisinin düzgün şifrəsi, həmin istifadəçi adının, müəyyən dərəcədə əminliklə, həmin subyektə məxsus olduğunu göstərir.

Müasir dövrdə terrorizm və cinayətkarlara qarşı mübarizə kəskin surətdə artmışdır. Bütün dünyanı bürümüş terror aktlarının dalğası aşkarlayıcı və önləyici təhlükəsizlik sistemlərinin təkmilləşdirilməsi ehtiyacını yaratmışdır.

İstənilən biometrik metodun öz üstünlükləri və çatışmamazlıqları vardır. Beləliklə, biometrik identifikasiya sistemlərinin zəifliyi, birinci və ikinci növ səhvlər, saxta hücumlar və biometrik şablonların verilənlər bazasından sızma halları aşkar edilə bilər. Müasir biometrik identifikasiya sistemləri iki növ səhvlərə həssasdır. Birinci növ səhv, sistem qanuni bir istifadəçini tanımadığı zaman baş verir [2]. Bu xidmətdən imtinaya səbəb olur. İkinci növ bir səhv, təcavüzkarın qanuni istifadəçi kimi səhv təyin edildiyi zaman baş verir. Bu cür səhvlər bir sıra səbəblərə görə baş verə bilər [2].

Səhv biometrik identifikasiyanın iki əsas xüsusiyyətinin optimal nisbətini təyin etmək üçün seçilir:

- **FAR** *(Yanlış qəbul etmə dərəcəsi)* - yanlış qəbuletmə əmsalı (yəni, qanuni istifadəçi adı ilə özünü müvəffəqiyyətlə təsdiqləyən şəxs).
- **FRR** *(Yanlış rədd etmə dərəcəsi)* - yanlış rədd etmə dərəcəsi (yəni, sistemin qanuni istifadəçisi olduğu halda sistem onu qəbul etmədi) [1].

Biometrik identifikasiya sistemlərindən istifadə zamanı bunları nəzərə alaraq təhlükəsizlik və etibarlılıq səviyyələrini artırmaq mümkündür. Buna görə də hələ gənc olan biometrik identifikasiya sahəsində yeni texnologiyaları inkişaf etdirməklə yanaşı həmin texnologiyaların təhlükəsizliyi sahəsində yeni metodların işlənməsi də kifayət qədər aktualdır [3].

Ədəbiyyat

3. R.M.Əliquliyev, Y.N.İmamverdiyev, V.Y.Musayev Biometrik Texnologiyalar. Bakı: İnformasiya Texnologiyaları nəşriyatı, 2009,376 s. səh.84.

4. Р.МАлгулиев, Я.Н.Имамвердиев, В.Я.Мусаев Методы обнаружения живучести в биометрических системах // Вопросы защиты информации. 2009, №3 (86), с.16-21.

5. T.Kazımov, Ş.Mahmudova İnformasiya təhlükəsizliyinin təmin olunmasında biometrik texnologiyaların rolu, İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı, 14 may 2015-ci il, səh. 218.