UOT 32

E-HÖKUMƏT VƏ İDARƏETMƏ SİSTEMLƏRİNDƏ ELEKTRON İMZANIN TƏTBİQİNİN ƏHƏMİYYƏTİ VƏ ÜSTÜNLÜKLƏRİ

Muraz SÜLEYMANOV*

Məqalə redaksiyaya daxil olmuşdur: 6 noyabr 2024; çapa qəbul edilmişdir: 18 noyabr 2024; online-da çap edilmişdir: 19 mart 2025.
Received: 6th of November, 2024; accepted: 18th of November, 2024; published online: 19th of March, 2025.

Açar sözlər: *informasiya, idarəetmə, e-hökumət, e-imza, ASAN imza, SİMA*

Giriş

Elektron hökumətin tətbiqi və inkişafında elektron imza mühüm əhəmiyyətə malikdir. Son illərdə elektron imzadan istifadə həm dövlət qurumları, həm sahibkarlar, həm də vətəndaşlar üçün xüsusi maraq kəsb etməyə başlamışdır. Bu səbəbdən dövlət idarəçiliyinin həyata keçirilməsində e-imzadan istifadə olunması və onun əhəmiyyəti aktual xarakter daşıyır.

Tədqiqatın işlənilməsində müqayisəli təhlil, analiz, sənədlərin öyrənilməsi kimi mühüm metodlardan istifadə edilmiş, eyni zamanda, araşdırma nəticəsində beynəlxalq təcrübənin öyrənilməsinə xüsusi diqqət yetirilmişdir.

Tədqiqat mövzusunun araşdırılması onu göstərir ki, elektron imzanın öyrənilməsi təhlükəsizliyin, operativliyin və həqiqiliyin qorunub saxlanılmasını bir vəzifə kimi qarşıya qoyur, həmçinin, tədqiqatın məqsədi aşağıdakı şəkildə qruplaşdırılır:

- İnformasiya təhlükəsizliyi və məlumat məxfiliyinin təmini;
- Sənədi təsdiq edənin həqiqiliyinin gözlənilməsi;
- İmzanın əldə edilməsinin və istifadəsinin sadələşdirilməsi;
- Vətəndaşlar üçün elektron imzanın əldə edilməsi prosesinin tam olaraq ödənişsiz həyata keçirilməsi istiqamətində işlərin görülməsi.

1. Elektron imza anlayışı və onun əhəmiyyəti

Elektron imza adi əlyazma imzanın rəqəmsal versiyası olaraq mühüm əhəmiyyət daşımaqla, əlyazma imza kimi hüquqi qüvvəyə malikdir. Rəqəmsal transformasiyanın sürətlənməsi nəticəsində təhlükəsizliyi və hüquqiliyi qorumaq prosesində e-imzalar mühüm texnologiyaya çevrilmişdir. Xüsusilə, bu proses biznes əlaqələrinin uzaqdan həyata keçirilməsində və idarə edilməsində xüsusi rola malikdir.

Elektron imzanın yaranması informasiya texnologiyalarının və hüquq elminin birləşməsinin ortaq nəticəsi kimi meydana çıxmışdır. Rəqəmsal mühitin formalaşması nəticəsində 1990-cı illərdən başlayaraq sənədin doğruluğunu yalnız ənənəvi imza ilə deyil,

* *doktorant, Bakı Dövlət Universiteti*
e-mail: murazsuleymanov01@gmail.com
ORCID: 0009-0002-2025-4289
https://doi.org/10.30546/25194011.2025.14.1.018

həm də elektron imza vasitəsilə təsdiq etmək mümkün olmuşdur. İnformasiya və kommunikasiya avadanlıqlarının, eləcə də internetin sürətli inkişafı elektron imzaya tələbatı gücləndirmiş oldu. Bu istiqamətdə elektron imzanın inkişafı aşağıda göstərilən bir neçə inkişaf mərhələsindən keçmişdir:

- İlkin şifrələmə texnologiyalarının tətbiqi və primitiv məlumatların təsdiqi;
- Elektron imzaya dair hüquqi statusun müəyyən edilməsi;
- Elektron imzanın formalaşdırılması, dövlət və özəl təşkilatlar tərəfindən istifadəsi;
- Hüquqi tənzimləmələrin tətbiqi nəticəsində inteqrasiya və rəqəmsal transformasiyanın həyata keçirilməsi;
- Elektron imzaya dair mümkün perspektivlər və gələcək inkişafa uyğunlaşma.

Elektron imza imza sahibini identikləşdirməyə imkan verir, yəni fiziki şəxsin əllə yazılmış imzasına bərabər tutulur və buna görə elektron imza etibarsız sayıla bilməz. Müxtəlif ölkələrdə e-imza ilə bağlı fərqli formatlarda qanunlar hazırlanaraq qəbul edilmişdir. E-imza ilə əlaqəli ilk qanunlar informasiya və kompüter texnologiyalarının sürətli yayıldığı inkişaf etmiş ölkələrdə tətbiq olunmağa başlamışdır. Bu baxımdan XX əsrin 90-cı illərindən etibarən, ABŞ və Avropa dövlətləri kimi inkişaf etmiş ölkələrdə elektron imza ilə bağlı bir sıra qanunvericilik aktları qəbul edilmişdir.

1995-1997-ci illərdə ABŞ-da elektron imzanı tənzimləyən qanunvericilik aktlarına ştat səviyyəsində baxılmışdır. Elektron imzaya dair qəbul edilmiş "Yuta qanunu" e-imzalardan kommersiya istifadəsinin həyata keçirilməsinə icazə vermiş ilk qanun hesab olunur (12, s. 59). Sonrakı illərdə oxşar qanunlar ABŞ-ın digər ştatlarında da qəbul edilmişdir. 1997-ci ildə artıq Almaniya və İtaliyada rəqəmsal imzaya dair qanunların qəbul edilməsinə başlanıldı. Belə ki, 1997-ci il 22 iyul tarixində Almaniya parlamenti "Rəqəmsal İmza Qanun"u təsdiqlədi və burada bu qanunun əsas məqsədi kimi rəqəmsal imzaların təhlükəsiz hesab edilməsi, onun saxtalaşdırılmasının qarşısının alınmasının ümumi şərtlərinin yaradılması göstərilmişdir (8, s. 3). İtaliyada isə elektron imza ilə bağlı fərman verilmiş və prosesin həyata keçirilməsi sertifikatlaşdırma orqanının səlahiyyətinə verilmişdir.

2004-cü ildə Azərbaycanda elektron imza ilə bağlı vacib sənəd hesab olunan "Elektron imza və elektron sənəd haqqında" qanun qəbul edilmişdir. Bu qanun elektron imza və elektron sənədin əhəmiyyətini göstərməklə yanaşı, elektron imzadan istifadə, sertifikatlaşdırma və elektron sənəd dövriyyəsinin həyata keçirilməsi qaydalarını özündə əks etdirir (1). Müvafiq qanun ümumi və yekun müddəalar daxil olmaqla 37 maddə və 7 fəsildən ibarətdir.

2. Elektron imzanın əldə edilməsi və istifadə qaydaları

Elektron imzanın əldə edilməsi və istifadə qaydalarında müəyyən fərqlər olsa da onların mahiyyəti demək olar ki, eyni xarakter daşıyır. Beynəlxalq təcrübədə elektron imzanın aşağıdakı üç əsas formatından (səviyyəsindən) istifadə olunur:

- Sadə elektron imzalar;
- Qabaqcıl elektron imzalar;
- İxtisaslaşdırılmış (sertifikatlaşdırılmış) elektron imzalar (11, s. 80).

Sadə elektron imza dedikdə, skan edilmiş imza və hər hansı planşet və ya digər texnologiyadan istifadə edərək, əl ilə çəkilmiş imza başa düşülür (11, s. 78). Bu cür elektron imzalar üçün hər hansı texniki və hüquqi şərtlər tələb olunmur. Həmçinin, elektron imzanın qeyd olunan növü, əsasən, sadə və tipik sənədlərin imzalanması və hər

hansı məlumatı təsdiq edən zaman istifadə oluna bilər ki, burada hər hansı ciddi təhlükəsizlik tədbirləri nəzərdə tutulmamışdır (16, s.138).

Qabaqcıl elektron imzalar xüsusi texniki tələbləri müəyyən etməklə, imzalayanın şəxsiyyətini müəyyənləşdirməyə imkan yaradır. Sadə elektron imzadan fərqli olaraq təkmil elektron imzalar aşağıdakı tələblərə cavab verməlidir:

- İmza və imza edən şəxs arasında unikal bağın mövcudluğu;
- İmza edənin nəzarəti altında imza yaratma məlumatlarından istifadə;
- İmzalanan sənəd məlumatlarında dəyişiklik olduğu halda imza edənin xəbərdar olması və lazım olarsa bu zaman imzanın etibarsız sayılması;
- İmza edəni müəyyən etmək bacarığı (14, s. 101).

Göründüyü kimi qabaqcıl elektron imza sadə elektron imzaya nisbətdə daha çox təhlükəsiz hesab olunur. Elektron imzanın təkmil formatı rəqəmsal imzaya əsaslansa da, bəzi hallarda məsuliyyətin qorunmasını tam təmin etməyə bilər (11, s. 80). Burada imzanın yoxlanılması prosesi imza sahibinin açıq açarı vasitəsilə yerinə yetirilir. Avropa təcrübəsində təkmil elektron imzalar qəbul edilsə də, onu yaş imzaya ekvivalent hesab etmirlər.

Elektron imzanın təhlükəsizlik baxımdan ən yüksək səviyyəsi ixtisaslı elektron imza hesab edilir ki, o e-İDAS (elektron identifikasiya, autentifikasiya və etibar xidmətləri) qaydasına uyğun olaraq Avropa İttifaqına üzv dövlətlərdə yaş imzaya, yəni əl imzasına hüquqi baxımdan ekvivalent hesab olunan elektron imzanın yeganə növüdür (11, s. 139). İxtisaslı elektron imzanı əldə etmək üçün elektron sertifikatın alınması zəruridir. Elektron sertifikat özündə elektron imza sahibinin şəxsiyyətini onlayn şəkildə sübut etmək məqsədilə istifadə edilən fayldır. Sertifikat elektron imzanın sahibinin şəxsi məlumatlarını və bu məlumatlara aid açıq açar məlumatlarını özündə daşımaqla, şəxsin müəyyən edilməsini və məlumatların doğruluğunu təmin edir.

Elektron imzanın qeyd olunan üç səviyyəsi Avropa İttifaqı tərəfindən qəbul edilmiş qanunda öz əksini tapsa da, bu bölgü praktikada, əsasən, ölkələrin təcrübəsində fərqli formada özünü göstərir. Əlbəttə ki, təhlükəsizliyin təmin edilməsi məqsədilə ixtisaslı elektron imzanın geniş yayılmasına və onun əldə edilməsinin sadələşdirilməsinə üstünlük verilir. Azərbaycan Respublikasında elektron imza ilə bağlı 2004-cü ildə qəbul edilmiş qanunda elektron imza və gücləndirilmiş elektron imza olmaqla, e-imzanın iki səviyyəsi göstərilir. Eyni zamanda, qanunda vurğulanır ki, elektron formada olan, lakin sertifikatlaşdırılmamış olduğuna görə elektron imza etibarsız sayıla bilməz. Sertifikatlaşdırılmış imza vasitələri ilə yaradılmış, qüvvədə olan təkmil sertifikatlı imza əl imzasına bərabər tutulur (1).

Azərbaycanda sertifikatlı elektron imzalardan istifadə geniş yayılmışdır, xüsusilə, dövlət qurumları üçün sertifikatlı (gücləndirilmiş) elektron imzalardan istifadə zəruridir. Respublikamızda elektron imzadan istifadə aşağıdakılar üçün nəzərdə tutulmuşdur:

- Əhali (vətəndaşlar);
- Dövlət qurumları;
- Sahibkarlıq fəaliyyəti ilə məşğul olan fiziki şəxslər;
- Hüquqi şəxslər.

Azərbaycan Respublikasında elektron dövlət xidmətlərindən yararlanmaq, elektron sənədləri imzalamaq, onları təsdiq etmək, həmçinin, elektron portallara daxil olmaq kimi müəyyən məqsədlər üçün elektron imzanın aşağıda göstərilən müxtəlif növlərindən istifadə edilir:

- ASAN imza;

- SİMA rəqəmsal imza;
- SİMA Token;
- İdentifikasiya nömrəsi;
- BSXM elektron imza.

Asan İmza mövcud elektron xidmətlərdən istifadəni mümkün edən, gücləndirilmiş elektron imza hesab olunan, kimliyi təsdiqləmək üçün imza edənin mobil identifikasiyasıdır. Asan İmzadan istifadə etmək üçün ASXM (Asan Sertifikat Xidmətləri Mərkəzi) tərəfindən verilən imza sahibini identikləşdirmək üçün nəzərdə tutulan və elektron imzanı yoxlama məlumatlarının məxsusluğunu göstərən elektron sənədin ("Asan İmza" sertifikatı) əldə edilməsi vacibdir (9, s. 47). Asan İmza əslində elektron mühitdə fiziki İD kart olan sənəd kimi sertifikat məlumatlarını özündə daşıyan mobil telefon SİM-kartıdır (2, s. 151).

ASAN İmza SIM kartının üzərində pozulan qatın altında gizlədilmiş PİN və PUK kodlar vasitəsilə imza təsdiqi həyata keçirilir. Bu kodların istifadəsi təhlükəsizliyin gözlənilməsində mühüm əhəmiyyətə malikdir. Belə ki, imza sahibi PİN 1 vasitəsilə şəxsiyyəti təsdiq edir, PİN 2 ilə isə sənədə imza atmaq prosesini həyata keçirir (5, s. 3). Bu kodları dəyişərkən və ya bir neçə dəfə səhv yığdıqda bloka düşdüyü zaman PUK koddan istifadə olunur.

SİMA Token virtual məkanda şəxsiyyəti təsdiqləmək məqsədilə yaradılmış, beynəlxalq təhlükəsizlik standartlarına uyğunlaşdırılmış elektron imzadır. Bu gücləndirilmiş elektron imzanı əldə edərək elektron sənədləri imzalamaq mümkündür. Bu imzadan istifadə etmək üçün müvafiq proqram təminatı və sertifikatı yükləyib quraşdıraraq SİMA Tokeni kompüterə qoşub sənədləri imzalamaq lazımdır. SİMA isə 2022-ci ildən etibarən Azərbaycan Respublikası Rəqəmsal İnkişaf və Nəqliyyat Nazirliyinin tabeliyində fəaliyyət göstərən "AzInTelecom" MMC tərəfindən yaradılaraq ictimaiyyətə təqdim olunmuş bulud əsaslı rəqəmsal imzadır (3, s. 3). Son dövrlərdə SİMA rəqəmsal imzadan istifadə geniş yayılmış və hər kəs üçün əlçatan olmuşdur. Belə ki, SİMA mobil tətbiqini yükləməklə müvafiq məlumatlar daxil edilərək üz tanınması yolu ilə tətbiqə giriş edilir və sertifikat alınır, daha sonra istənilən vaxt QR skan və imza sahibi tərəfindən təyin edilən gizli kodu daxil etməklə məlumatı və ya əmək müqaviləsi kimi mühüm sənədləri imzalamaq mümkün olur.

Fərdi identifikasiya nömrəsi dedikdə, vətəndaşa məxsus FİN kod, yəni şəxs barəsində dövlət reyestrinə daxil edilmiş məlumatları fərqləndirmək və müəyyən etmək məqsədilə təqdim olunmuş təkrarolunmaz kod başa düşülür. Elektron portaldan identifikasiya nömrəsi vasitəsilə qeydiyyatdan keçərək vətəndaş sistemə daxil edilmiş özünə məxsus məlumatları izləyə bilər.

BSXM elektron imza isə Bank Sertifikat Xidməti Mərkəzi tərəfindən fiziki, hüquqi şəxslərə və dövlət qurumlarına təqdim edilir. Maliyyə sahəsində məlumat mübadiləsi təhlükəsizliyini təmin etmək məqsədilə yaradılmış BSXM elektron imza mühüm əhəmiyyətə malikdir. Respublikada müvafiq xidmətdən istifadə hazırda fərqli kateqoriyalar üzrə müəyyən edilmiş tarif əsasında həyata keçirilir və Bank Sertifikat Xidməti Mərkəzi qanunvericiliyə uyğun olaraq müvafiq qurum tərəfindən akkreditə edilmişdir.

3. Elektron imzanın tətbiqinin üstünlükləri

Son illərdə elektron imzadan istifadə edilməsi geniş vüsət almışdır və bu səbəbdən elektron imza ilə bağlı məsələlərdə təhlükəsizliyin gözlənilməsi amilinə xüsusi diqqət yetrimək lazımdır (4, s. 310). Eyni zamanda elektron imzadan istifadənin geniş yayıldığı

dövrdə əhalinin İKT avadanlıqlarından istifadə imkanları yaradılmalı, bununla bağlı dəstəkləyici mühit və maarifləndirmə ilə bağlı mütəmadi olaraq iş aparılmalıdır. Elektron imzadan istifadənin bir çox üstünlüklərini aşağıdakı şəkildə qruplaşdıra bilərik:

- Operativliyin təmin edilməsi və vaxta qənaət;
- İstənilən məsafədən təsdiq etmə imkanı;
- Kağızdan istifadənin minimuma endirilməsi və sənədlərin elektron təsdiq edilərək elektron formada saxlanılması;
- Təhlükəsizliyin təkmilləşdirilməsi;
- Dəqiqliyin gözlənilməsi;
- Büdcəyə uyğunluq və s.

Məlumdur ki, elektron imzanın tətbiq edilməsinin kifayət qədər üstünlükləri mövcuddur. Bununla yanaşı, elektron imza tətbiqlərində təhlükəsizliyin gözlənilməsi daim nəzarətdə saxlanılmalı və həssas məsələ hesab olunmalıdır. Elektron imza texnologiyalarının hesab olunan zəif nöqtəsi elektron imza açarının saxlanması məsələsidir (6, s. 63). İstifadəçi legitimliyinin və açarın məxfiliyinin təmin edilməsi çox vacib prosesdir. Elektron imza açarı kompüterin sabit diskində və ya portativ tutacaqlarda saxlanıla bilər. Birinci üsulda təhlükəsizlik səviyyəsi aşağıdır və parolu bilən hər kəs tərəfindən məlumatın götürülməsi ehtimalı böyükdür. Digər üsul isə daha məqbul hesab edilir və təhlükəsizlik yüksək səviyyədə gözlənilir. Burada təhlükəsizliyin təmin edilməsi məqsədilə əlavə olaraq PİN kodlardan istifadə olunur.

Elektron imzanın həyata keçirilməsində mahiyyət etibarilə sertifikatlaşdırma xidmətinin təminatçısı, imzalayan və imzanı qəbul edən və bu mübadilənin həyata keçirilməsini təmin edən komputer-kommunikasiya sistemi çıxış edir (12, s. 59). Bu istiqamətdə təhlükəsizliyin gözlənilməsində qanunvericilik bazası ilə yanaşı, sertifikatlaşdırma orqanları tərəfindən meyarların müəyyən edilməsi və məsuliyyətin gözlənilməsi vacibdir (14, s. 104).

Elektron imzanın təhlükəsizliyi həm texnoloji, həm də hüquqi aspektdən əhəmiyyətli olduğu üçün sertifikatlaşdırma orqanları tərəfindən elektron imzanın saxtalaşdırılması və ya mənimsənilməsinə dair baş verə biləcək mümkün halların qarşısının alınması məqsədilə mühüm tədbirlər həyata keçirilməlidir. Elektron imzanın təhlükəsizliyinin artırılması sahəsində sürətli formada inkişaf edən ağıllı texnologiyaların köməyindən istifadə edilməsi zəruri mövqeyə malikdir. Mərkəzləşdirilmiş və şifrələnmiş məlumat bazalarından ibarət olan blokçeyn texnologiyasının tətbiqi elektron imzanın təhlükəsizliyinin təmin edilməsi istiqamətində innovativ üsul hesab oluna bilər. Belə ki, blokçeyn texnologiyası iş quruluşu aşağıdakı prinsiplər əsasında həyata keçirilir:

- Məlumatların dəyişdirilməzliyi;
- Təsdiqlənmiş sənədlərin düzgünlüyü;
- Mərkəzləşdirilməmiş şəbəkə modeli;
- Məlumatların şifrələnməsi;
- Sənədin imza tarixinin qeydinin aparılması;
- Təhlükəsiz sənəd mübadiləsinin aparılması.

Bu texnologiya əsasında məlumatlar bloklar şəklində saxlanılır və bloklar arasında zəncirvari bağ yaradılır ki, hər hansı məlumat dəyişikliyi bütün zənciri poza bilər, eyni zamanda, sənədin təsdiqlənmə tarixçəsi saxlanıldığı üçün məlumatların dəyişdirilməsi qeyri-mümkün olur. Mərkəzləşdirilməmiş şəbəkə modelinin mərkəzləşmiş sistemə nisbətdə üstünlüyü məlumatların bir neçə iştirakçı arasında paylaşılmasıdır ki, bu da serverə hücum zamanı məlumat saxtalaşdırılmasına imkan vermir. Həmçinin, sənədin

imzalandıqdan sonra dəyişdirildiyi zaman əvvəlki məlumatların saxlanması, sənəd mübadiləsi zamanı isə şəxsiyyət doğrulaması prosesi elektron imzanın hüquqi etibarlılığını və orijinallığını təmin edir.

Qeyd edək ki, rəqəmsallaşan dünyada artıq elektron imza bir ölkənin hüdudlarından çıxaraq beynəlxalq ticarətin həyata keçirilməsində mühüm bir istiqamətə çevrilmişdir. BMT-nin Beynəlxalq Ticarət Hüququ üzrə Komissiyası tərəfindən qəbul edilmiş Model qanunu ticarət sahəsində beynəlxalq uyğunlaşmanın təşviqinə əhəmiyyətli kömək etmiş oldu (13, s. 3). Xarici sertifikatlar tərəfindən dəstəklənən imzaların tanınması prosesində də təhlükəsizliyin gözlənilməsi amilinə xüsusi diqqət yetirilmişdir. Göründüyü kimi elektron imzanın istifadəsində və inkişaf etdirilməsi prosesində, həmçinin məlumatların təhlükəsizliyinin gözlənilməsində daxili imkanlarla yanaşı, beynəlxalq təcrübədən faydalanmaq vacib əhəmiyyət kəsb edir.

Nəticə

Rəqəmsallaşan dünyada bütün dövlətlər üçün mühüm əhəmiyyətə malik olan elektron imzanın təkmilləşdirilməsi və mümkün yeniliklərin həyata keçirilməsi istiqamətində vacib işlər həyata keçirilir. Bu baxımdan Azərbaycan Respublikasında dövlət idarəçiliyinin həyata keçirilməsi prosesində elektron imzanın spesifik rolunu nəzərə alaraq, onun təhlükəsizliyi, istifadə qaydaları, tətbiqi və inkişafı ilə bağlı aşağıdakı təkliflər göstərilmişdir:

- Elektron imza açarının təhlükəsizliyi ilə bağlı əlavə tədbirlər;
- Autentifikasiya prosesinin dəqiqliyinin təmini;
- Məlumat məxfiliyi və təhlükəsizliyinin gözlənilməsi;
- Elektron imzanın təşviqi prosesinin həyata keçirilməsi;
- Sertifikat orqanlarının məsuliyyətliliyi ilə bağlı əlavə prinsiplərin müəyyən edilməsi;
- Elektron imzanın əldə edilməsinin asanlığı və tarif qiymətinin minimuma endirilməsi.

ƏDƏBİYYAT

1. Elektron imza və elektron sənəd haqqında Azərbaycan Respublikasının Qanunu. Bakı şəhəri, 9 mart 2004. (https://e-qanun.az/framework/5916).
2. Qafarbəyli T. Elektron imza və kibertəhlükəsizlik // İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı, 14 may 2015, s. 150-152. (https://ict.az/uploads/konfrans/2_ konfrans/40.pdf).
3. Rəhbər şəxs tərəfindən işçiyə (işçilərə) "Asan İmza" "İş" (Biznes) və ya "Dövlət və bələdiyyə" tipli sertifikat vasitəsilə elektron xidmətlərin imzalama prosesinə məhdudiyyətin qoyulması/aradan qaldırılması üzrə İstifadəçi təlimatı. Bakı, 2020. (https://www.taxes.gov.az/uploads/2022/asanimza/3.pdf).
4. Süleymanov M.İ. Elektron hökumətə ictimai etimadın formalaşdırılması və cəmiyyətin informasiyalaşdırılması problemi // NASCO, XXVI, 2023, s. 308-311.
5. Şəxsi tipli "Asan İmza" sertifikatı əsasında İş (Biznes) və Dövlət və bələdiyyə tipli "Asan İmza" sertifikatlarının onlayn əldə olunması üzrə İstifadəçi təlimatı.Bakı, 2021. (https://www.taxes.gov.az/uploads/2022/asanimza/1. pdf).
6. Andrianova V. Electronic signature key storage. Procedia Computer Science Volume 145, 2018, p. 59-63.
7. Constantin A. The electronic signature-technical and legal implications Bulletin of the Transilvania University of Braşov Series VII: Social Sciences Law Vol. 7 (56) No.2,

2014. p. 225-234.
8. Dumortier J. Legal Status of Qualified Electronic Signatures in Europe. 2004. 9 p. (https://www.researchgate.net/publication/228909495_Legal_Status_of_Qualified_Electronic_Signatures_in_Europe).
9. Ibadov N., Mammadli, N. Electronic government: theoretical foundations and directions of an action. Political Science and Security Studies Journal, Vol. 4, No. 2, 2023. p. 43-48. (https://psssj.eu/index.php/ojsdata/ article/view/120).
10. Lax G., Buccafurri, F., Nicolazzo, S., Nocera, A. and Fotia, L. A New Approach for Electronic Signature // In Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP), 2016. p. 440-447. URL: (https://air.unimi.it/retrieve/01ccb108-8d1e-4a65-a7e4247a82651e08/574 34. pdf).
11. Mulder V. et al. (eds.), Trends in Data Protection and Encryption Technologies, 2023. 253 s. (https://doi.org/10.1007/978-3-031-33386-6_1).
12. Pichler D., Tomić, D. Electronic signature in legal theory and practice – new regulation // International Scientific Conference "Economics of Digital Transformation" Rijeka, 2019. p. 57-69.
13. Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods. United Nations Publication Sales No. E.09.V.4 ISBN 978-92-1-133663-4. United Nations Vienna, 2009, 114 p.
14. Scirtocea L. Electronic signature, tool for optimizing the management of information in electronic forma // Proceedings of the international scientific conference strategies XXI - the complex and dynamic nature of the security environment, 2022, p. 101-107. (https://revista.unap.ro/index.php/XXI_ CSSAS/article/view/1357/1317).
15. UNCITRAL Model Law on Electronic Signatures with Guide to Enactment, United Nations Publication Sales No. E.02.V.8 ISBN 92-1-133653-8 UNITED NATIONS New York, 2002. 83 p. (https://uncitral.un.org/sites/uncitral.un.org/files/mediadocuments/uncitral/en/ml-elecsig-e.pdf).
16. Şimşek M., Özcan T., Ergun T., Çelik V. Elektronik İmza Seviyeleri. Bilgi Yönetimi Dergisi Cilt:2 Sayı:2, 2019. s. 136-144. (https://dergipark.org.tr/ en/download/ article-file/899520),

Резюме

Мураз Сулейманов

Важность и преимущества использования электронной подписи в системах электронного правительства и управления

В эпоху современного электронного администрирования широкое распространение получило применение и использование электронной подписи во всех сферах администрирования. В настоящее время в большинстве стран мира используются различные уровни и виды электронной подписи. В статье показана важность применения электронной подписи в электронном государственном управлении, подчеркнуты преимущества использования электронной подписи, в то же время рассмотрен международный опыт относительно законов, принятых в этой сфере, а также значение соответствующего закона, принятого в Азербайджанской Республике об электронной подписи. Также в статье упоминаются правила получения и использования электронных подписей и сертификатов, показаны различные виды электронных подписей, используемых в Азербайджане, и уделено внимание правилам их использования. В частности, уточняются правила безопасности получения подписи ASAN и цифровой подписи SIMA, а также подписания электронных документов и проверки электронной информации как расширенных типов электронной подписи, используемых в Азербайджанской Республике. В современное время спектр электронной подписи расширяется в развитых и развивающихся странах, поэтому в качестве уровня охвата электронной подписью указываются граждане, физические, юридические лица, а также государственные учреждения. В качестве одной из основных проблем в этой сфере было обращено внимание на фактор обеспечения информационной безопасности, использование ПИН- и ПАНК-кодов для защиты персональных данных владельца электронной подписи и обеспечения подлинности лица,

подписавшего договор документально подтвердить или подтвердить, что информация была упомянута. При использовании этих кодов считается важным, чтобы подписывающее лицо не сообщало упомянутые коды постороннему лицу в целях обеспечения безопасности, и в то же время важно обращать внимание на проверочный код при подтверждении любой информации.

В заключение показано важное значение электронной подписи в направлении обеспечения государственного управления в цифровом мире, где широко используется компьютерная техника и информационные технологии, и сделаны соответствующие предложения по ее развитию, а также рассмотрены вопросы предвидя безопасность в этой области.

Ключевые слова: *информация, управление, электронное правительство, электронная подпись, подпись ASAN, SIMA*

Summary

Muraz Suleymanov

The importance and advantages of using electronic signature in e-government and management systems

In the era of modern electronic administration, the application and use of electronic signature in all areas of administration is widespread. Currently, various levels and types of electronic signature are used in most countries of the world. In the article, the importance of the application of e-signature in electronic state administration is shown, the advantages of using e-signature are emphasized, at the same time, the international experience regarding the laws adopted in this field is examined and the importance of the relevant law adopted in the Republic of Azerbaijan on e-signature is shown. Also, the article mentions the rules for obtaining and using electronic signatures and certificates, shows the different types of electronic signatures used in Azerbaijan, and pays attention to their rules of use. In particular, the security rules for obtaining ASAN signature and SIMA digital signature, as well as signing electronic documents and verifying electronic information, as the enhanced electronic signature types used in the Republic of Azerbaijan, are specified. In modern times, the range of electronic signature is expanding in developed and developing countries, so citizens, individuals, legal entities, as well as state institutions are indicated as the level of coverage of electronic signature. As one of the main problems in this field, attention was paid to the factor of expectation of information security, the use of PIN and PUNK codes to protect the personal data of the electronic signature owner and to ensure the authenticity of the person who signed the document or confirmed the information was mentioned. When using these codes, it is considered important that the signatory does not share the mentioned codes with an outsider in order to ensure security, and at the same time, it is important to pay attention to the verification code when confirming any information. In conclusion, the important importance of electronic signature in the direction of ensuring public administration in the digitized world, where the use of computer equipment and information technologies is widespread, is shown, and relevant proposals are made regarding its development, as well as the issues of anticipating security in this field.

Key words: *information, management, e-government, e-signature, ASAN signature, SIMA*

Redaksiya heyətinin üzvü s.e.ü.f.d. Qasımov Səyavuş Kamran oğlunun rəyi əsasında çapa məsləhət görülmüşdür.