UOT 004.056

Hacırəhimova M. Ş.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
makrufa@iit.ab.az

ELEKTRON SƏNƏD DÖVRİYYƏSİ SİSTEMLƏRİNİN TƏHLÜKƏSİZLİYİNİN BƏZİ ASPEKTLƏRİ

İnformasiya-kommunikasiya texnologiyalarının (İKT) ən geniş tətbiq sahələrindən biri kargüzarlıqdır. Belə ki, keçən əsrin 90-cı illərindən başlayaraq, informasiya texnologiyalarının (İT) tətbiqi ilə kargüzarlıq fəaliyyətininin elektron formada aparılmasına imkan verən elektron sənədlərin idarə edilməsi üzrə kompüter sistemləri tətbiq olunmağa başlanmışdır. Məqalə hazırda idarəetmə məsələlərinin həllində zəruri bir amilə çevrilmiş bu sistemlərin təhlükəsizlik məsələlərinə həsr olunur. Elektron sənəd dövriyyəsi sistemlərinin təhlükəsizliyini şərtləndirən əsas amillər şərh edilir, təhlükələrin təsnifatına baxılır, əsas təhlükəsizlik aspektləri araşdırılır. Həmçinin bu sistemlərdə təhlükəsizliyin təmin edilməsi üçün istifadə edilən texnologiyalar analiz olunur.

Açar sözlər: *elektron sənəd, elektron sənəd dövriyyəsi sistemi, identifikasiya, autentifikasiya, elektron rəqəm imzası.*

Giriş

Hazırda informasiya texnologiyalarının inkişafı və onun bütün fəaliyyət sahələrinə geniş tətbiqinin nəticəsi olaraq yüz illərlə əsas informasiya daşıyıcısı olan kağız sənədlərə alternativ olan informasiyanın yeni forması – elektron sənədə *(e-sənəd)* keçid reallaşmışdır. Bu tip sənədlərin idarə edilməsində istər özəl, istərsə də dövlət sektorunda elektron sənədlərin idarə edilməsi və ya elektron sənəd dövriyyəsi kompüter sistemləri istifadə olunmağa başlanmışdır [1].

Elektron sənəd dövriyyəsi sistemi (ESDS) kompüter şəbəkələrində e-sənədlərin yaradılması, saxlanması, axtarışı, paylanması prosesini təmin edən, eyni zamanda əlyetərliliyin idarə olunması və təşkilatda sənəd axınına və icrasına nəzarəti həyata keçirən təşkilati-texniki bir sistemdir [2]. Yəni ESDS təşkilatlarda e-sənədlərin (*müəssisəyə daxil olan, müəssisədən çıxan və müəssisədaxili sənədlər*) təşkilinin və idarə olunmasının kompüterləşdirilmiş modelidir və demək olar ki, İT-nin ən sürətlə inkişaf etmiş sahələrindəndir. Müasir dövrdə böyük və kiçikliyindən asılı olmayaraq istənilən təşkilatda elektron sənəd dövriyyəsinin tətbiqi zərurətə çevrilmişdir. ESDS-lərin tətbiqi informasiyanın emalı və saxlanmasında böyük çeviklik və iqtisadi fayda əldə etməyə imkan versə də, yeni tip risklər, kiçik bir ehtiyatsızlıq yeni təhlükələrə gətirib çıxara bilər.

Təbiidir ki, kağız sənədlərdə olduğu kimi, e-sənədlər də müxtəlif məxfilik səviyyəsinə malikdir, tam açıq və təşkilatın kommersiya sirrini, yaxud dövlət sirri daşıyan məlumatlara bölünür. Odur ki, ESDS-nin tətbiqi zamanı, xüsusilə də, dövlət sektorunda sistemin təhlükəsizlik tədbirləri çox ciddi məsələlərdəndir. Ümumiyyətlə, ESDS-lərin təhlükəsizliyi üçün elektron-rəqəm imzasının (ERİ) istifadəsi əsas şərtdir [3,4]. Çünki ERİ-nin istifadəsi sənədlərin təhlükəsizliyi və mühafizəsinin qarantıdır. Ancaq ERİ-dən düzgün istifadə etmək, infrastruktur və onun əsasında təhlükəsizlik xidmətlərini genişləndirmək məsələləri problem olaraq qalır.

Hüquqi əsasların dəyişməsi, standartlarda olan boşluqlar, sürətlə inkişaf edən texnologiya qarşısında təhlükəsiz ESDS-ni müəyyən etmək olduqca çətinləşir. Bu, həm istehsalçılar, həm də istifadəçilərdən sistemin təhlükəsizlik səviyyəsini yüksəltməyə diqqəti artırmağı tələb edir. Ona görə də ESDS-lərin təhlükəsizliyinin bəzi aspektlərini bilmək çox önəmli və vacib məsələdir.

Elektron sənəd dövriyyəsi sistemlərinin təhlükəsizliyini şərtləndirən amillər

DSS Consulting agentliyinin məlumatında qeyd olunduğu kimi, hazırda dövlət sektoru ESDS-nin ən böyük istehlakçısıdır [5]. İnformasiya cəmiyyəti və e-dövlət infrastrukturunun

yaradılması və inkişaf etdirilməsi fonunda dövlət sektorunda ESDS-ə diqqətin artması müşahidə olunur. Belə ki, digər dövlətlərdə olduğu kimi, Azərbaycanda da elektron dövlət (*e-dövlət*) konsepsiyasının həyata keçirilməsi ilə əlaqədar olaraq, əhaliyə və biznes sektoruna daha operativ və şəffaf dövlət xidmətlərinin göstərilməsi üçün, elektron inzibatçılıq reqlamentinə əsaslanan yeni keyfiyyətdə daxili təşkilatlanma düşüncəsi formalaşmaqdadır. Bu baxımdan, elektron sənəd dövriyyəsinin təhlükəsizlik məsələsini şərtləndirən əsas amillləri aşağıdakı kimi təqdim etmək olar:

- ESDS yaradılmaqda və inkişaf etməkdə olan e-dövlət infrastrukturunun ən vacib komponentinə çevrilmişdir; Əgər əvəllər hakimiyyət orqanlarında informasiya sistemləri təşkilat daxilində istifadə üçün yaradılırdısa, hazırda bu sistemlər dövlət idarələri ilə vətəndaşların (*G2C - Government to Citizen*) və qeyri-dövlət sektorunun (*G2B - Government to Business*), eyni zamanda, dövlət idarələrinin bir-biri ilə (*G2G - Government to Government*) elektron qarşılıqlı əlaqəsini təmin edir [2].
- e-dövlət infrastrukturunun yaranması və inkişafı ilə əlaqədar olaraq dövlət qurumlarının birinci şəxslərinin bilavasitə bu işdə fəal iştirakı və dövlətin göstərdiyi elektron xidmətlərin genişlənməsi nəticəsində mübadilə olunan sənədlərin, məxfi informasiyanın, xüsusi halda fərdi verilənlərin qorunması məsələsi vacibdir [6-8];
- sənədlər, bir qayda olaraq, müxtəlif qurumlar arasında mübadilə olunarkən onların üzərində müəyyən əməliyyatlar aparılır ki, bu da hər kəs üçün əlyetərli olmamalıdır [4];
- vətəndaşlar və hüquqi şəxslərlə işləyən dövlət təşkilatlarında ESDS-nin informasiyanın tamlığı və məxfiliyi, e-sənədlərin müəlliflik hüquqlarını təmin etmək üçün təhlükəsizlik vasitələrinin tətbiqinin vacibliyi dərk edilməkdədir [2,7];
- elektron imza haqqında qəbul olunmş qanun e-sənədlərin mühafizəsinə və ESDS-də müxtəlif təhlükəsizlik texnologiyalarının istifadə olunmasına imkan verir. Digər dövlətlərdə olduğu kimi, Azərbaycanda da qəbul olunmuş normativ-hüquqi aktlar [4,9] kağız sənədlərdən elektron sənədlərə keçidin hüquqi əsasını təmin etməklə ESDS-dən təşkilatdaxili və təşkilatlararası sənədlərin dövriyyəsini mümkün etmişdir;
- müəssisə və təşkilatlarda kağız sənədlərə bərabər tutulan e-sənədlərə hüquqi əsas verən mexanizmlərin təmin olunmasına və anlaşılmasına ehtiyac vardır [2].

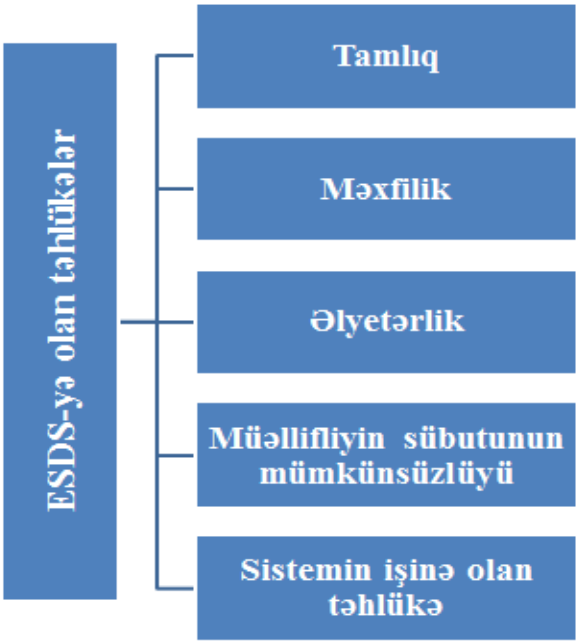
Hazırda bu sistemlərin təhlükəsizliyinə dair baxışlar dəyişmişdir. Əgər əvvəllər hədəf ancaq sənədlərin və ya informasiya resurslarının təhlükəsizliyinin təmin edilməsi idisə, indi e-sənədlərin paylanması, emalını və saxlanmasını təmin edən sistemin özünün təhlükəsizliyinin təmin edilməsi əsas hədəfə çevrilib [10,11]. Məlumdur ki, ESDS-ə çoxlu sayda texniki cəhətdən mürəkkəb funksional altsistemlər, müxtəlif proqram-texniki vasitələr, saxlanma və emal qurğuları, təsdiqlənmiş sertifikat mərkəzləri, idarəetmə mərkəzləri və s. daxildir. Eyni zamanda, ESDS-lər müxtəlif platformalı proqram-texniki vasitələrin köməyi ilə yaradılır ki, bunlar da həm arxitekturuna, həm də sənəd dövriyyəsinin təşkili qaydalarına görə fərqlənir. Bu halda ESDS-də təhlükəsizliyin təmin edilməsi məsələsi texniki cəhətdən interperabelliyin (*uyğunsuzluqların*) olmaması ilə daha da çətinləşir. Odur ki, bütün səviyyələrdə sistemin təhlükəsizliyinin təmin edilməsinə kompleks yanaşmaq lazımdır. İlk növbədə, sistemin aparat təminatının (*kompüterlər, serverlər, şəbəkə qurğuları, kabellər və s.*) təhlükəsizliyi təmin olunmalıdır. Sonra sistem faylları (*proqram təminatı, verilənlər bazaları, sistem faylları və s.*) mühafizə edilməlidir. Əks halda bədniyyətlilər ESDS-nin fayllarına müdaxilə etmək (*faylları köçürmək, əməliyyat sistemini və qurğuları sıradan çıxarmaq*) imkanı əldə edə bilərlər. Nəhayət, sonda sistemdə yerləşdirilmiş sənədlərin təhlükəsizliyinin təmin edilməsi gərəkdir. Belə yanaşma istifadə edildikdə bütün səviyyələrdə təhlükələrdən mühafizə olunmaq və təhlükəsiz ESDS yaratmaq mümkündür. Əlbəttə, belə mühafizə ESDS-nin özünün qiyməti ilə müqayisədə çox baha ola bilər. Odur ki, təhlükəsizliklə qiymət arasında balans axtarmaq lazım gəlir.

Əvvəldə qeyd olunduğu kimi, təşkilat daxilində dövr edən sənədlər açıq və qapalı olur. Burada icazəsi olan və olmayan istifadəçilərin sistemə və sənədlərin emal alətlərinə müraciəti

zamanı təhlükələr də qaçılmazdır. Ona görə də əlyetərliliyin idarə edilməsində hər istifadəçinin əlyetərlik hüquqları minimallaşdırılmaqla, bilavasitə yerinə yetirdikləri xidməti funksiyalar prinsipi əsasında nəzərə alınmalıdır. Bu mərhələdə ikitərəfli autentifikasiya mexanizmi kimi ERİ-nin tətbiqi vacibdir. Bunun üçün açıq açarlar infrastrukturu yaratmaq lazımdır və gizli açarlar sistemi və güclü mühafizə vasitələrinə malik daşıyıcılar istifadə olunmalıdır.

Elektron sənəd dövriyyəsi sistemlərinə olan təhlükələrin təsnifatı

Elektron sənəd dövriyyəsi zamanı müxtəlif təhlükələr yarana bilir. Adətən ESDS-yə olan əsas təhlükələr standart olmaqla aşağıdakı kimi təsnifatlandırılır [10,11] (Şəkil 1).



Şəkil 1. ESDS-ə olan təhlükələr

Tamlıq təhlükəsi təsadüfi və ya məqsədyönlü və pis niyyətlə informasiyaya zərər yetirmək, məhv etmək və ya təhrif etməkdir.

Məxfilik təhlükəsi informasiyanın oğurlanması, ələ keçirilməsi, marşrutunun dəyişdirilməsi kimi istənilən məxfiliyin pozulmasıdır.

Əlyetərlilik. Bu təhdid, istifadə hüquqları olan istifadəçilər üçün məqbul müddət ərzində tələb olunan məlumatları əldə etmək imkanının pozulmasıdır.

Müəllifliyin sübutunun mümkünsüzlüyü sənəd dövriyyəsində ERİ istifadə olunmadıqda verilən sənədin məhz həmin istifadəçi tərəfindən yaradıldığını sübut etməyin çətin olması ilə ifadə olunur. Bu da sənəd dövriyyəsini hüquqi cəhətdən imkansız edir.

Sistemin işinə olan təhlükə və ya *səmərəlilik* isə bilərəkdən, qəsdən həmlə etmək, istifadəçinin səhvi üzündən, eləcə də, avadanlıq və proqram təminatı kəsildikdə sistemin işini pozmaq və ya dayandırmaqdır.

Odur ki, istənilən ESDS-də bu və ya digər dərəcədə qeyd olunan təhlükələrdən mühafizə vasitələri həyata keçirilməlidir, təhlükələri aradan qaldırmaq üçün sistemdə dövr edən e-sənədlərin məzmununa üçüncü şəxs tərəfindən icazəsiz baxmağın mümkünsüzlüyü, e-sənədi göndərənin birmənalı identifikasiyası, e-sənədin icazəsiz modifikasiya edilməsinin mühafizəsi və konfliktlərin həll edilməsini təmin edən mexanizmlər tətbiq olunmalıdır. Bunlardan birinci üçü kriptoqrafik və şifrləmə alqoritmlərin (*RSA, EGSA, DSA, ECDSA* və s.) köməyi ilə həll edilir [3, 12, 13]. Sonuncusu isə sistemin iştirakçıları arasında e-sənədlərin mübadiləsi üçün qoyulmuş reqlamentə uyğun həll edilir [4].

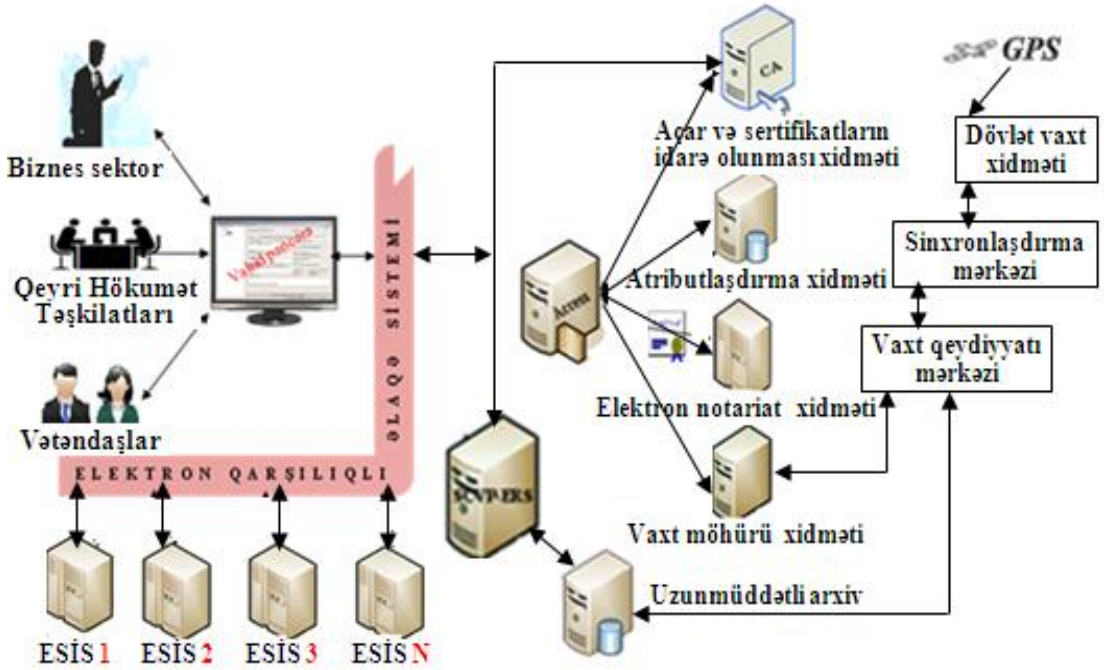
Elektron sənəd dövriyyəsi sistemlərinin təhlükəsizlik aspektləri

İnformasiya texnologiyalarının inkişafı ilə e-sənədlərə qarşı təhlükələr də çoxalır. Bekə ki, bədniyyətlilərin e-sənədləri qeyri-qanuni əldə etməsi, saxtakarlıq, e-sənədlərin istifadəsinə icazəsiz daxil olmalar, marşrutunu dəyişdirərək özlərini elektron qarşılıqlı əlaqənin bir tərəfi kimi təqdim etmək və s. üçün texniki, təşkilati və başqa imkanları artır. Sənədlərin geri tarixlə imzalanması, onların dəyişdirilməsi, qeydiyyatının olmaması və s. kimi xoşagəlməz hallar meydana çıxır [2, 12]. Burada əsas məsələ ondan ibarətdir ki, hər şeydən əvvəl, təhlükəsiz ESDS-yə informasiya sisteminin klassik mühafizəsi nöqteyi-nəzərindən baxılmalıdır [10]. Belə ki, istifadəçilərin autentifikasiyası, əlyetərlilik hüquqlarının bölünməsi, e-sənədin müəllifliyinin təsdiqi, e-sənədin tamlığına nəzarət, məxfilik, hüquqi əsası təmin etmək üçün istifadə olunan proqram təminatının tamlığına nəzarət, kriptoqrafik alqoritmlər, antivirus proqramları və s. kimi mexanizmlərdən istifadə ESDS istehsalçıları arasında elektron sənədlərin qorunması üçün mühüm məsələlərdir.

İstifadəçilərin autentifikasiyası. Autentifikasiya – kriptoqrafik çevirmənin köməyi ilə identifikatorun həqiqiliyinin yoxlanılmasıdır. Autentiklik iki cəhəti özündə əks edir: tamlıq – sənəd dəyişilmədən mühafizə olunmalıdır; sənədi göndərənin identifikasiyası (müəllifliyin yoxlanması) –alanın sənədi kimin göndərdiyini yoxlamaq imkanı olmalıdır. Autentifikasiya son illərdə tez-tez müraciət olunan texnologiyadır. Bəzən istifadəçilər autentifikasiya texnologiyaları əvəzinə identifikasiya, xüsusi hal olaraq biometrik identifikasiya üsullarından (əl izləri, göz, səs kimi biometrik verilənlər) istifadə etməyə üstünlük verirlər. Bu texnologiya cəlbedici (istifadəçi özü ilə smart-kart daşımır, PIN-kodu yadda saxlamaq lazım gəlmir) olsa da bahalıdır və lazımi etibarlılıq səviyyəsini təmin etmir. Bir çox hallarda identifikasiya prosesi birmənalı eyniliyin təmin olunmasına zəmanət vermir (şəxsiyyəti təsdiq edən pasport misalında, şəkli dəyişdirməklə və ya oxşatmaqla baş verə biləcək hadisələr). Ən etibarlı identifikasiya elə autentifikasiyadır. Autentifikasiya əlyetərliliyi ancaq bölmək deyil, həm də fərdiləşdirmək imkanı verir. Yəni, şəxsi verilənlərlə işləyən bütün istifadəçiləri bu verilənlər üzərində etdikləri hərəkətə cavabdeh edir. Fərdiləşdirilmiş əlyetərliliyin təşkili üçün PKI (*Public Key Infrastructure,* açıq açar infrastrukturu) bazası [14], autentifikasiya və imzalanmış sənədin tamlığını yoxlamaq üçün əsas mexanizm kimi ERİ-nin tətbiqi müasir yanaşmalardandır. Deyilənləri ümumiləşdirərək deyə bilərik ki, təhlükəsiz ESDS üçün əsas məsələ: mühafizə və informasiya əhəmiyyətli resurslara əlyetərlilik üçün istifadəçilərin ciddi autentifikasiyası; məxfi informasiya və şəxsi məlumatlara əlyetərliliyin məhdudlaşdırılması, icazəsiz müdaxilələri bloklamaq, ümimi açıq informasiyalara əlyetərliliyi təmin etməkdir.

İnfrastruktur məsələləri. Təhlükəsiz elektron sənəd dövriyyəsini təmin edən infrastruktur elementləri aşağıdakılardır [12,15-22]:

- sənədlərin elektron baza infrastrukturu;
- ERİ infrastrukturu, o cümlədən açıq açarlı infrastruktura əsaslanan vahid sistemə daxil olan səlahiyyətli sertifikatlaşdırma mərkəzi;
- təqdim olunan sənədə vaxt nişanları qoymaq üçün etimad vaxt infrastrukturu, üçüncü etimad tərəflə sənədin nəşr olunduğu yeri müəyyən edən etimad servis infrastrukturu (Şəkil 2);
- qarşılıqlı informasiya əlaqəsinin iştirakçılarının hüquqi statusu, səlahiyyət və imza hüquqlarını təsdiq etmək üçün elektron reyestr infrastrukturu.



Şəkil 2. Sənədlərə etimad servis infrastrukturu

Etimad servis infrastrukturu beynəlxalq standartlar və tövsiyələr əsasında yaradılmalıdır. Bu infrastrukturun texniki konsepsiyası Beynəlxalq Telekommunikasiya İttifaqının *X.842* seriyasından olan *İTU-T* tövsiyəsində ifadə olunmuşdur [15]. *X.842* tövsiyəsində etimad xidmətləri müəyyən edilmişdir, infrastrukturun idarə edilməsi üzrə göstərişlər təqdim edilmiş, etimad infrastrukturun və bu xidmətlərdən istifadə edən şəxslərin rolu və öhdəlikləri təyin edilmişdir. Burada istifadə edilən açıq açar sertifikatının formatı isə *ITU X.509* [16] tövsiyələrinə müvafiqdir. İstifadə olunan təkmilləşdirilmiş rəqəm imzasının (TRİ) formatı isə Avropa Telekommunikasiya Standartları İnstitutunun (*European Telecommunications Standards Institute, ETSI*) standartına – *RFC 5126* "CMS Advanced Electronic Signatures (CAdES)" əsaslanır [17]. Təkmilləşdirilmiş rəqəm imzalarının (TRİ) tətbiqi, e-sənədin imza vaxtının TSP (*Time-Stamp Protocol*) vaxt möhürü protokolu üzrə birmənalı təyin edilməsinə və imzalanma anında açıq açar sertifikatının statusunun onlayn nəzarətinə imkan verir [12,19-24]. Beləliklə, TRİ yalnız e-sənəddə imzasının həqiqiliyini (imzanın sahibinə məxsus olmasını, sənəddə saxtalığın olmamasını) deyil, həm də imzalanma anını, həmçinin rəqəm imzası yaranan zaman imza açarı sertifikatının həqiqiliyini də yoxlayır.

Vaxt möhürü sənədin müəyyən vaxtda mövcudluğunun təsdiq edilməsi üçündür. Bu texnologiya rəqəm imzası və heş-funksiyalara əsaslanır [21]. Vaxt möhürünə e-sənədlərin müəyyən vaxta kimi mövcud olduğu və sonrakı dövrlərdə modifikasiya olunmadığına zəmanət verən rəqəmli sertifikat kimi də baxmaq olar.

Açarların idarə edilməsi məsələsi. Məlumdur ki, informasiya təhlükəsizliyi xidmətləri həyata keçirilərkən rəqəm imzası (Rİ) və digər kriptoqrafik *(*simmetrik və asimmetrik*)* texnologiyalar mühüm rol oynayır [3, 6]. Rİ açıq açarlar infrastrukturu vasitəsi ilə həyata keçirilir və təsdiq edilmiş sertifikat mərkəzləri (*CA – Certificate Authority*) tərəfindən verilən açıq açarlar sertifikatına olan etimada əsaslanır. Asimmetrik kriptoqrafiyada iki – açıq **(public key)** və gizli *(***private key***)* açar generasiya olunur. Açıq açar e-imzanın yoxlanılması üçün istifadə edilir və hər kəs üçün açıqdır. Gizli açar e-imza qoymaq üçündür və yalnız imzanın sahibinə məlum olmalıdır. Açarlar informasiyanın şifrlənməsi və deşifrlənməsinə imkan verir. Yəni açıq açarla şifrlənmiş informasiya ancaq gizli açarla deşifrə oluna bilər. Böyük

hesablamalar tələb etdiyindən açıq açara görə gizli açarın tapılması isə çox çətin məsələdir [3, 12].

Gizli açar rəqəm imzası kriptosistemlərinin ən "həssas" komponentidir. İstifadəçinin gizli açarını əldə etmiş bədniyyətli, bu şəxs adından istənilən sənədi imzalaya bilər. Deməli, imzanın təhlükəsizliyi əsas məsələdir. İstifadəçinin gizli açarının təhlükəsizliyi onun həyat dövrünün bütün mərhələlərində: açıq və gizli açarların generasiyası mərhələsində, gizli açarın saxlanması, istifadəsi və məhv edilməsi müddətində təmin olunmalıdır. Açar cütlərinin (*gizli və açıq*) generasiyası bədxahların təsir imkanlarını, eləcə də, onun sonradan bərpa etmək cəhdləri zamanı istifadə oluna biləcək gizli açar haqqında hər hansı informasiyanı əldə etmək ehtimalını istisna edən mühitdə yerinə yetirilməlidir. Gizli açarın saxlanılması zamanı onun gizliliyi və tamlığı etibarlı şəkildə icazəsiz müdaxilələrdən və modifikasiyalardan mühafizə olunmalıdır. Ona görə də gizli açarın saxlanılmasına ciddi diqqət yetirilməlidir.

Elekrton imza qanununa əsasən, gizli açarların saxlanması onun sahibinin üzərinə düşür. İstifadəçilər gizli açarı öz fərdi kompüterində parolla saxlaya bilər. Bu halda gizli açarın təhlükəsizliyi, bütövlükdə, kompüterin təhlükəsizliyindən asılıdır və istifadəçi sənədi ancaq bu kompüterdə imzalamalıdır.

Gizli açarı saxlamaq üçün disketlər, smart-kartlar, kiçik *USB* qurğuları və s. mövcuddur. Qeyd etmək lazımdır ki, gizli açarların smart-kartlarda saxlanması daha yaxşı hesab olunur. Çünki istifadəçi həm karta sahib olmalıdır, həm də *PIN*-kod daxil etməlidir ki, bu zaman ikifaktorlu autentifikasiya alınsın. Saxlama qurğusunun itməsi və oğurlanması zamanı sertifikat geri çağırılmalıdır. Gizli açardan istifadə zamanı onun ələ keçməsini və icazəsiz istifadəsini aradan qaldırmaq olar (sahibinin arzusu nəzərə alınmaqla). Nəhayət, gizli açarın məhv edilməsi mərhələsində informasiyanın zəmanətli məhvi və onun təkrar istifadə ehtimalını tamamilə aradan qaldırmaq lazımdır.

Tamlığa nəzarət üçün kriptoqrafik heş-funksiyalardan (*MD5, SHA, RIPEMD* və s.) istifadə edilir. Heş-funksiya ixtiyari uzunluqlu informasiya üçün sabit uzunluqlu heş-kod hesablayır ki, bu kod da informasiya ilə bağlıdır, bir bit dəyişdikdə heş-kod da dəyişir [3].

Şübhəsiz, dövlət tərəfindən də ESDS-lərin inkişafına güclü dəstək göstərilməlidir. Əvvəldə də qeyd edildiyi kimi, ESDS e-dövlətin göstərdiyi e-xidmətlərdə əsas rol oynayır. Eyni zamanda, idarələrarası təhlükəsiz elektron sənəd mübadiləsinə olan tələbat artdıqca, ESDS-lərin hüquqi təminatına diqqət də artır. Bu sahədə qanunvericiliklə bağlı yeniliklər "insan – informasiya resursu" qarşılıqlı əlaqəsinin təhlükəsizliyini yüksəltməyə imkan verən perspektiv texnologiyaların inkişafına kömək edir, fırıldaqçılıq və dələduzluq hallarını azaldır.

ESDS-lərdə mobillik, "cloud" texnologiyanın tətbiqi və təhlükələr

Veb-servislərin genişlənməsi, bütün sahələrdə olduğu kimi, elektron sənəd dövriyyəsi sferasının inkişafına da təsir etmişdir. Son illərdə aparılan tədqiqatlardan, analitik şirkətlərin hesabat və proqnozlarından da göründüyü kimi, mobilləşmə və bulud texnologiyalarının tətbiqi ESDS-lərdə perspektiv inkişaf istiqamətləri hesab olunur [5, 25–27]. Baxmayaraq ki, SaaS (*software as a service*, proqram təminatı xidmət kimi) – modeli əsasında yaradılmış ESDS-lər biznes subyektlərində hələlik geniş tətbiq olunmasa da, resursların və xərclərin düzgün idarə edilməsində "bulud"larda ESDS əvəzolunmaz vasitəyə çevrilmişdir. ESDS-lərin bulud texnologiyasına doğru inkişafı – *SaaS* xidmət modelinə keçid təşkilatların kontentlərin idarə olunması sahəsində (serverlərin alınması, proqram təminatlarının lisenziyasının əldə olunması, istifadə olunan resursların ödənilməsinin ancaq istifadəçilərin sayına və saxlanılan sənədlərin həcminə görə olması, mühafizə edilməsi və s. kimi xərcləri əhəmiyyətli dərəcədə azaltmaqla) çevikliyini artırır [25]. "Bulud"larda informasiya təhlükəsizliyi ilə bağlı bütün məsələlər xidmət səviyyəsini təqdim edən (*SLA – service level agreement*) müqavilə, qaydalar, razılaşma və digər sənədlərlə həll edilir. Təbii ki, xidmət göstərən provayderlər də maraqlıdırlar ki, hər cür pozuntulardan uzaq olsunlar. Çünki onların fəaliyyəti etimad üzərində qurulur. Təhlükəsizliyin

təmin edilməsinin vacib hissəsi, sənədləri hüquqi tərəfdən qoruyan, "*Non-Disclosure Agreement*" (Açıqlamama haqqında saziş) adlandırılan sazişdən ibarətdir. Bu sazişdə tərəflərin öhdəlikləri və verilənlərin yayılmasına cavabdehlikləri müəyyən edilir. Kənar istifadəçilərin verilənlərə əlyetərlilik məsələsi də resurslardan birgə istifadənin təşkili ilə reallaşdırılır, ağıllı nəzarət mexanizmi ilə yerinə yetirilir. "Bulud"lar sənədlərin oğurlanması, DDoS hücumlar, xidmətin "sındırılması" kimi ənənəvi təhlükələrdən isə sığortalanmayıb. Bədniyyətlilər verilənləri əldə etmək istəyərkən proqram təminatı səviyyəsində verilənlərin mühafizəsi üçün servis-provayderlərin professional aparat-proqram vasitələri (məsələn, *Cisco ASA 5500 Series* və *IronPort* qurğuları), təhlükəsizlik sahəsində təcrübəli sistem administratorları ilə qarşılaşırlar. "Bulud"larda operatora inamsızlıq problemini isə təhlükəsizlik, əlyetərlilik, verilənlərin emalının tamlığı, məxfiliyin təmin olunmasında istifadə olunan sertifikatlaşdırma standartları ilə həll etmək olar.

Hazırda mobilliyə olan tələbat ESDS-lərin təhlükəsizliyi üçün ciddi riskə çevrilmişdir. Mobillik informasiya təhlükəsizliyinin, demək olar ki, bütün sərhədlərini aşır, yeni təhlükəsizlik problemləri yaradır. Yeni mobil qurğuların yaranması bu problemi daha da ciddiləşdirmişdir [26]. Ümumi əlyetərli şəbəkə ilə xüsusi şəbəkə, mobil qurğu ilə stolüstü qurğu, təşkilatın əməkdaşları ilə kənar istifadəçiləri ayıran sədlər aradan götürülür, kommunikasiya mühiti müəyyən olunmur.

Belə ki, müasir mobil qurğuların funksional imkanlarının genişlənməsi ilə istifadəçilər işçi kompüterləri ilə smartfonları arasında verilənlərin sinxronlaşdırılması funksiyasından istifadə edirlər. Bu halda təhlükəsizliyin təmin edilməsi çətinləşir. Çünki əməkdaş işdə stolüstü kompüterdə, yolda smartfonda, hoteldə noutbukda müxtəlif əməliyyat sistemləri, proqram əlavələri, şəbəkələlərdən və s. istifadə etməklə işləyə bilər. Əgər əməkdaşların mobil qurğuları onların təşkilatlarının nəzarətindən kənarda olan *Wi-Fi, WiMAX* və s. şəbəkələrə qoşulmuşdursa, mobil əlaqə zamanı sistemin təhlükəsizliyini təmin etmək üçün şəbəkələrarası ekran *(brandmauer)* kimi ənənəvi mühafizə mexanizmləri artıq kifayət etmir. Məlumdur ki, şəbəkələrarası ekran "dünyanı" ancaq iki yerə bölür: "ağ" və "qara"; "yad" və "özününkü". Müasir təhlükəsizlik sistemləri isə daha çox amillərə – şəbəkə topologiyalarına, dinamik atributlara (istifadəçinin profilinə, olduğu yer, çox kiçik intervalda şəbəkəyə giriş və s.) baxmalı, daha yeni identifikasiya və autentifikasiya, hüquqların təsdiq edilməsi metodikaları istifadə etməklə istifadəçiləri izləyə bilməlidirlər [23]. Bu yanaşma daha böyük əmək tələb edir. Onlayn informasiya xidmətlərinin artması ilə bu sistemlərin yaradıcıları qismində, fırıldaqçılıqla mübarizədə maraqlı tərəflər kimi iri dövlət, bank, sığorta şirkətləri çıxış edə bilərlər. Ümumiyyətlə, informasiya təhdidlərindən qorunmaq kompleks bir prosesdir. İnformasiya təhlükəsizliyi sistemləri isə bu işdə öndə olmalıdır.

Nəticə

Hazırda ESDS-nin tətbiqi istər özəl, istərsə də dövlət sektorunda idarəetmə məsələlərinin həllində zəruri bir amilə çevrilmişdir. ESDS-lərin təhlükəsizliyinə kompleks yanaşılmalıdır, təhlükələri və riskləri, eyni zamanda, ola biləcək itkiləri düzgün qiymətləndirmək lazımdır. Göründüyü kimi, sistemdə zəif autentifikasiya, kriptoqrafik vasitələrin olmaması, ERİ-nın istifadəsindəki mürəkkəblik mükəmməl, təhlükəsiz ESDS-nin tətbiqinə mane olan amillərdəndir. Bu da, öz növbəsində, kağız sənədlərdən e-sənədlərə keçid prosesini ləngidir.

ESDS təhlükəsizliyi ancaq sənədlərin təhlükəsizliyi və əlyetərliliklə məhdudlaşmır. Burada sistemin aparat vasitələrinin, kompüterlərin, sistemin fəaliyyət göstərdiyi şəbəkə mühitinin qorunması, verilənlərin ötürmə kanallarının qorunması və s. də ciddi məsələlərdəndir. Ona görə də kompleks tədbirlərin görülməsi təhlükəsizliyin bütün səviyyələrində xüsusi rol oynayır. Təəssüflər olsun ki, çox vaxt ona etinazsızlıq göstərirlər. Pis təşkilatçılıq ən müasir texniki tədbirləri belə sıfıra endirə bilər.

Ədəbiyyat

1. Sprague R.H. Electronic document management: challenges and opportunities for Information Systems Managers // MIS Quarterly, 1995, vol.19, no.1, pp. 29–49.
2. Hacırəhimova M.Ş. Elektron dövlət mühitində sənəd dövriyyəsi sistemlərinin aktual problemləri və həll yolları // İnformasiya cəmiyyəti problemləri, Bakı, 2010, №2, s. 21-29.
3. Əliquliyev R.M., İmamverdiyev Y.N. Rəqəm İmzası Texnologiyası, Bakı, "Elm", 2003, 130 s.
4. Elektron imza və elektron sənəd haqqında Azərbaycan Respublikası Qanunu, Azərbaycan qəzeti, 10 mart 2004-cü il.
5. Колесов А., Государство и СЭД: итоги, проблемы, перспективы, 25 марта 2011, http://ecm-journal.ru/post/
6. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. М.: Горячая Линия Телеком, 2004, 280 с.
7. Lambrinoudakis C., Gritzalis S., Dridi F., Pernul G. Security Requirements for e-Government Services: A Methodological Approach for Developing a Common PKI-based Security Policy // Computer Communications, 2003, vol.26, no.16, pp.1873-1883.
8. İdarələrarası elektron sənəd dövriyyəsi sistemi haqqında əsasnamə, 4 sentyabr 2012-ci il, http://www.president.az
9. İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında Azərbaycan Respublikası Qanunu, 3 aprel 1998-ci il, http://www.president.az
10. Булдакова Т.И., Глазунов Б.В., Ляпина Н.С. Оценка эффективности защиты систем электронного документооборота // Доклады ТУСУРа, 2012, № 1 (25), часть 2, с. 52-56.
11. Досмухамедов Б.Р. Анализ угроз информации систем электронного документооборота // Компьютерное обеспечение и вычислительная техника, 2009, № 6, с.140–143.
12. Имамвердиев Я.Н., Гаджирагимова М.Ш. Архитектура инфраструктуры доверия электронным документам в среде электронного государства // Телекоммуникации, 2011, №11, с.18-26.
13. Riverst R.L., Shamir A., Adleman L. A Metod for Obtaining Digital Signatures and Public-Key Criptosystems // Communications of the ACM.-1978. vol.21, no.2, pp.120-126.
14. Liu J.B., Hu X-Q., et.al. Design and Implementation of a PKI-Based Electronic Documents Protection Management System / Proceddings of International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Kaohsiung, Taiwan, 26–28 november, 2007, pp.87-92.
15. ITU-T X.842 Information Technology – Security Techniques – Guidelines for the Use and Management of Trusted Third Party Services, 2000, 50 p.
16. Housley R., Polk W., Ford W., Solo D. RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002, 129 p.
17. Pinkas D., Pope N., Ross J. RFC 5126: CMS Advanced Electronic Signatures (CAdES). 2008, 141 p.
18. Myers M., Ankney R., Malpani A., Galperin S., Adams C., RFC 2560: X.509 Internet Public Key Infrastructure – Online Certificate Status Protocol – OCSP, June 1999, 51 p.
19. Cain A. C., Pinkas P. D., and Zuccherato R. RFC 3161: Internet X. 509 Public Key Infrastructure Time-Stamp Protocol (TSP), august 2001, 26 p.
20. Gatautis R., Mazeika A., Laud P., and Satkauskas R., Enhancing e-Government Services through Digital Time Stamping: Time Stamping System Specifications // Communications of the IBIMA, 2008, vol.5, no.24, pp.204-210.
21. Buldas A., Laur S. Knowledge-binding Commitments with Applications in Time-Stamping / International Conference on Theory and Practice of Public-Key Cryptography (PKC'07), 16-20 April 2007, Beijing, China, LNCS 4450, pp.150-165.

22. Freeman T., Housley R., Malpani A., Cooper D., Polk W. RFC 5055: Server-Based Certificate Validation Protocol (SCVP), December 2007, 88 p.
23. Farrell S., Housley R., Turner S. RFC 5755: An Internet Attribute Certificate Profile for Authorization. January 2010, 50 p.
24. Adams C., Sylvester P., Zolotarev M., and Zuccherato R., RFC 3029: Internet X.509 Public Key Infrastructure. Data Validation and Certification Server Protocols, February 2001, 51 p.
25. Liu N. Cloud technology in the security management of enterprise document / Proceedings of the second International Conference on Innovations in Bio-inspired Computing and Applications, 2011, 16–18 December, pp.267-269.
26. Corazon M.G., Sicat E., et.all Subion iPad: Integrated Paperless Document Checking and Template-based / Proceedings of the Second International Conference on Computer and Electrical Engineering, 2009, pp.189-193.
27. The Digital Universe Decade – Are You Ready?, http://www.emc.com/collateral/ analyst-reports

УДК 004.02

Гаджирагимова Макруфа Ш.
Институт Информационных Технологии НАНА, Баку, Азербайджан
makrufa@science.az

Некоторые аспекты безопасности систем электронного документооборота

Одной из наиболее расширенных областей применения информационно-коммуникационных технологий является делопроизводство в организациях. Начиная с 90-х годов прошлого века, с применением информационных технологий используются компьютерные системы управления электронными документами, позволяющие вести делопроизводство в электронном виде. Статья посвящена вопросам безопасности этих систем, которые стали ключевым фактором в решении задач управления. В статье комментируются основные факторы безопасности этих систем, рассматриваются классификации угрозы, расследуются основные аспекты безопасности. Кроме того, анализируются технологии безопасности, используемые в этих системах.

Ключевые слова: *электронный документ, система электронного документооборота, идентификация, аутентификация, электронная цифровая подпись.*

Makrufa Sh. Hajirahimova
Institute of Information Technology of ANAS, Baku, Azerbaijan
makrufa@science.az

Some aspects of the security of electronic document management systems

One of the most expanded application areas of information and communication technology (ICT) is clerical organizations. So, beginning from the 90s of the last century has been started to using of management of electronic documents computer systems which allowed to organize of clerical activity in an electronic form with application of information technology (IT). The article is dedicated to the security issues of these systems that became a necessary factor in solution of management issues. In this paper main factors are commented which stipulated of security of these systems, are reviewed to the classification of dangers, basic security aspects of the system are investigated. Also, technologies in these systems that are used for the provision of security are analyzed.

Key words: *electronic document, electronic document management system, identification, autentification, electronic digital signature, secure document management system.*