E-sənəd dövriyyəsi sistemlərinin təhlükəsizliyinin təmin edilməsinin bəzi aspektləri

Məkrufə Hacırəhimova

AMEA İnformasiya Texnologiyaları İnstitutu
makrufa@science.az

***Xülasə*— Məqalə hazırda istər özəl, istərsə də dövlət sektorunda idarəetmə məsələlərinin həllində tətbiqi zəruri bir amilə çevrilmiş elektron sənəd dövriyyəsi sistemlərinin təhlükəsizlik məsələlərinə həsr olunur. Bu sistemlərin təhlükəsizliyini şərtləndirən əsas faktorlar şərh olunur, təhlükələrin təsnifatına baxılır, sistemin əsas təhlükəsizlik aspektləri araşdırılır.**

Açar sözlər — elektron sənəd; elektron sənəd dövriyyəsi sistemi; identifikasiya; autentifikasiya; elektron rəqəm imzası; təhlükəsiz elektron sənəd dövriyyəsi sistemi

I. GİRİŞ

Bu bir faktdır ki, informasiya texnologiyaları (İT) insan fəaliyyərinin bütün sahələrinə dərin nüfuz etmişdir. Uzun illər xüsusi çəkiyə malik kağız sənədlərin idarə edilməsində keçən əsrin 90-cı illərindən başlayaraq, İT-nin tətbiqi ilə kargüzarlıq fəaliyyətininin elektron formada aparılmasına imkan verən elektron sənədlərin idarə edilməsi və ya elektron sənəd dövriyyəsi kompüter sistemləri istifadə olunmağa başlanmışdır [1]. Bununla da "kağız sənədlərdən imtina" – elektron sənədlərə (*e-sənəd*) keçid dövrü başlanmışdır. Elektron sənəd dövriyyəsi sistemi (ESDS) kompüter şəbəkələrində e-sənədlərin yaradılması, saxlanması, axtarışı, paylanması prosesini təmin edən, eyni zamanda əlyetərliyin idarə olunması və təşkilatda sənədlərin 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-nın ən sürətlə inkişaf etmiş sahələrindəndir. ESDS-lərin tətbiqi informasiyanın emalı və saxlanmasında böyük çeviklik və fayda əldə etməyə imkan versə də, yeni tip risklər, kiçik bir ehtiyatsızlıq yeni təhlükələrə gətirib çıxara bilər. Odur ki, ESDS-ni tətbiq etməklə, xüsusilə də dövlət sektorunda, sistemin təhlükəsizlik tədbirlərini yaddan çıxarmaq olmaz. ESDS-lərin təhlükəsizliyi üçün elektron-rəqəm imzasının (ERİ) istifadəsi əsas şərtdir [3,4]. Ancaq, bir qayda olaraq ERİ-ni necə düzgün istifadə etmək, hansı infrastruktur və onun əsasında hansı təhlükəsizlik xidmətlərini genişləndirmək lazımdır, arxa planda qalır. Hüquqi əsasların dəyişməsi, standartlarda olan boşluqlar, sürətlə inkişaf edən texnologiya qarşısında təhlükəsiz ESDS-ni müəyyən etmək olduqca çətinləşir. Bu həm istehsalçıları, həm də istifadəçiləri sistemin təhlükəsizlik səviyyəsini yüksəltməyə daha çox diqqət göstərməyə vadar edir. Ona görə də ESDS-lərin təhlükəsizliyinin bəzi aspektlərini bilmək çox önəmli və vacib məsələdir.

II. ESDS TƏHLÜKƏSIZLİYİNİ ŞƏRTLƏNDİRƏN AMİLLƏR

Hazırda elektron sənəd dövriyyəsinin təhlükəsizlik məsələsini şərtləndirən bir çox amilllər mövcuddur.

- ESDS yaradılmaqda və inkişaf etməkdə olan elektron dövlət (*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 aktiv iştirakı və dövlətin göstərdiyi elektron xidmətlərin genişlənməsi nəticəsində mübadilə olunan sənədlərin, məxfi informasiyanın, xüsusi halda fərdi verilənlərin qorunması məsələsi vacibdir [5-7];
- ESDS bazasında toplanmış sənədlər, fiziki və hüquqi şəxslərin sorğularına cavab olaraq hazırlanan sənədlər bir qayda olaraq müxtəlif qurumlar arasında mübadilə olunarkən sənədlər üzərində müəyyən işlər görülür ki, bu da hər kəs üçün əlyetən olmamalıdır [4];
- vətəndaşlar və hüquqi şəxslərlə işləyən dövlət təşkilatlarında ESDS-nin informasiyanın tamlığı və məxfiliyini, e-sənədlərin müəlliflik hüquqlarını təmin etmək üçün təhlükəsizlik vasitələrinin tətbiqinin vacibliyi dərk edilməkdədir [2,6];
- elektron imza haqqında qəbul olunmş qanun elektron sənədlərin mühafizəsinə və ESDS-də müxtəlif təhlükəsizlik texnologiyalarının istifadə olunmasına imkan verir. Digər dövlətlərdə olduğu kimi Azərbaycanda da qəbul olunmuş normativ-hüquqi aktlar [4,8] 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 real ehtiyac vardır [2].

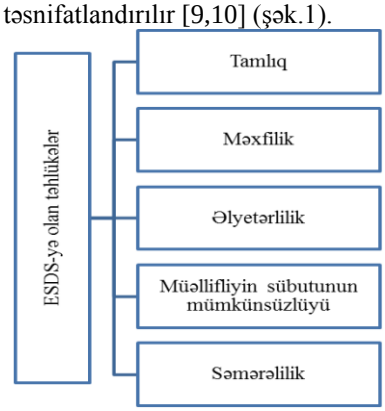
Bu gün sistemin təhlükəsizliyinə olan baxışlar dəyişmişdir. Əgər əvvəllər hədəf ancaq sənədlərin və ya informasiya resurslarının təhlükəsizliyinin təmin edilməsi idisə, indi əsas hədəf e-sənədlərin paylanmasını, emalını və saxlanmasını təmin edən sistemin özünün təhlükəsizliyinin təmin edilməsidir [9,10]. Qeyd edildiyi kimi ESDS-yə 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 fərqlənirlər. Bu halda ESDS-də təhlükəsizliyin təmin edilməsi məsələsi texniki cəhətdən interperabelliyin olmaması ilə daha da çətinləşir. Ona görə də 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 fayllarının (*proqram təminatı, verilənlər bazaları, sistem faylları və s.*) mühafizəsi lazımdır. Əks halda bədxah ESDS-nin fayllarına müdaxilə etmək (*faylları köçürmək, əməliyyat sistemini və qurğuları sıradan çıxarmaq*) imkanı əldə edə bilər. 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.

Təşkilat daxilində dövr edən sənədlər açıq və qapalı olur. Qapalı sənədlərin özləri də məxfi və dövlət sirri daşıyan məlumatlara bölünür. Burada icazəsi olan istifadəçilərin sistemə və sənədlərin emal alətlərinə müraciəti zamanı təhlükələr də qaçılmazdır. Ona görə də əlyetərliyin idarə edilməsində hər istifadəçinin əlyetərlik hüquqları minimallaşdırılmaqla, bilavasitə yerinə yetirdikləri xidməti funksiyalar prinsipi əsasında nəzərə alınmalıdır. Bu mərhələdə ikitərəfli autentifikasiya mexanizmi kimi ERİ tətbiqi vacibdir. Bunun üçün açıq açarlar infrastrukturu yaratmaq və gizli açarlar sistemi və güclü mühafizə vasitələrinə malik daşıyıcılar istifadə olunmalıdır.

III. ESDS-YƏ OLAN TƏHLÜKƏLƏRİN TƏSNİFATI

Adətən ESDS-yə olan təhlükələr standart olmaqla aşağıdakı kimi təsnifatlandırılır [9,10] (şək.1).



Şək. 1. ESDS-yə 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 məxfiliyinin pozulmasıdır.

Əlyetərlik – 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 tərəfiindən yaradıldığını sübut etməyin çətin olması ilə ifadə olunur. Bu da sənəd dövriyyəsini hüquqi cəhətdən imkansız edir.

Sistemin iş qabiliyyətinə 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 [3,13]. Sonuncusu isə sistemin iştirakçıları arasında e-sənədlərin mübadiləsi üçün qoyulmuş reqlamentə uyğun həll edilir.

IV. ESDS TƏHLÜKƏSİZLİK ASPEKTLƏRİ

İnformasiya texnologiyalarının inkişafı ilə e-sənədlərə təhlükələr də çoxalır. Bekə ki, bədxahların 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 [2,11].

Burada əsas məsələ ondan ibarətdir ki, hər şeydən əvvəl təhlükəsiz ESDS-yə informasiya sisteminin klassik mühafizəsi nöqteyi nəzərindən baxılmalıdır [9]. 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 məlum məsələlərdir. Konfrans və seminarlarda ən çox müzakirə mövzularından olan ESDS-lərin təhlükəsizliyinin bəzi aspektlərinə diqqət yetirək.

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. Daha sürətli nəticə əldə etmək məqsədilə

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 (Personal Identification Number) 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 əlyetərliyin təşkili üçün PKI (*Public Key Infrastructure*) bazası, autentifikasiya mexanizmi kimi ERİ proseduru kimi həllərin tətbiqi müasir yanaşmalardandır. Deyilənləri ümumiləşdirərək deyə bilərik ki, təhlükəsiz ESDS üçün əsas məsələ: mühafizə və informasiya əhəmiyyətli resurslara əlyetərlik üçün istifadəçilərin ciddi autentifikasiyası; məxfi informasiya və şəxsi məlumatlara əlyetərliyin məhdudlaşdırılması, icazəsiz müdaxilələri bloklamaq, ümimi açıq informasiyalara əlyetərliyi təmin etməkdir.

İnfrastruktur məsələləri. ESDS-nin təhlükəsizliyini təmin edən infrastruktur elementləri aşağıdakılardır [11,12]:

- müxtəlif qurumlara aid sənədlərin elektron baza infrastrukturu;
- ERİ infrastrukturu, o cümlədən açıq açarlı infrastruktura əsaslanan vahid sistemə daxil olan səlahiyyətli sertifikatlaşdırma mərkəzi;
- e-sənədlərin açıq elektron rabitə kanalları vasitəsi ilə ötürülməsi zamanı onların göndərilmə və alınma məkanını və vaxtını təyin etmək çətinləşir. Odur ki. dövlətin göstərdiyi elektron xidmətlərə vətəndaşların və biznes-sektorun etimadını formalaşdırmaq üçün üçüncü etimad tərəfi, təqdim olunan sənədə vaxt nişanları qoymaq üçün etimad vaxt infrastrukturu, iki və daha çox üçüncü etimad tərəflərilə sənədin nəşr olunduğu yeri müəyyən edən etimad servis infrastrukturu;
- informasiya qarşılıqlı əlaqənin iştirakçılarının hüquqi statusu, səlahiyyət və imza hüquqlarını təsdiq etmək üçün elektron reyestr infrastrukturu.

Açarların idarə edilməsi məsələsi. Məlumdur ki, informasiya təhlükəsizliyi xidmətləri həyata keçirilərkən asimmetrik kriptoqrafik texnologiyalar mühüm rol oynayır [3,5]. 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 acar e-imza qoymaq üçündür və yalnız imzanın sahibinə məlum olmalıdır. Gizli açar vasitəsi ilə həyata keçirilir və təsdiq edilmiş sertifikat mərkəzlər (CA – Certificate Authority) tərəfindən verilən açıq açarlar sertifikatına olan etimada əsaslanır. 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.

Gizli açar rəqəm imzası kriptosistemlərinin ən "həssas" komponentidir. İstifadəçinin gizli açarını əldə etmiş bədxah, 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 tamlıq 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 disketlər, smart-kartlar, kiçik USB qurğular 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 alınır.

Saxlama qurğusunun itməsi və oğurlanması zamanı sertifikat geri çağrılmalıdır.

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 informasiya ilə bağlıdır, bir bit dəyişdikdə heş-kod da dəyişir.

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 əlaqənin təhlükəsizliyini yüksəltməyə imkan verən pespektiv texnologiyaların inkişafına kömək edir, fırıldaqçılıq və dələduzluq hallarını azaldır.

NƏTİCƏ

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 faktorlardandır. Bu da öz növbəsində kağız sənədlərdən e-sənədlərə keçid prosesini ləngidir.

ESDS təhlükəsizliyi ancaq sənədlərin təhlükəsizliyi və əlyetərliklə 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.

ƏDƏBİYYAT

[1] Sprague R.H. Electronic document management: challenges and opportunities for Information Systems Managers // MIS Quarterly, 1995, vol.19, no.1, pp. 29-49. http://www.jstor.org/stable/249710

[2] Hacırəhimova M.Ş. Elektron dövlət mühitində sənəd dövriyyəsi sistemlərinin aktual problemləri və həll yolları // İnformasiya cəmiyyəti problemləri, 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] Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. М.: Горячая Линия Телеком, 2004, 280 с.

[6] 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.

[7] İdarələrarası elektron sənəd dövriyyəsi sistemi haqqında əsasnamə, 4 sentyabr 2012-ci il.

[8] İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında Azərbaycan Respublikası Qanunu, 3 aprel 1998-ci il

[9] 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.

[10] Досмухамедов Б.Р. Анализ угроз информации систем электронного документооборота // Компьютерное обеспечение и вычислительная техника, 2009, № 6, с. 140–143.

[11] Имамвердиев Я.Н., Гаджирагимова М.Ш. Архитектура инфраструктуры доверия электронным документам в среде электронного государства // Телекоммуникации, 2011, №11, с. 18-26.

[12] Pinkas D., Pope N., Ross J. RFC 5126: CMS Advanced Electronic Signatures (CAdES). 2008, 141 p.

[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.