BAKI UNİVERSİTETİNİN XƏBƏRLƏRİ
№2 Fizika-riyaziyyat elmləri seriyası 2007

KORPORATİV KOMPÜTER ŞƏBƏKƏLƏRİNDƏ İNFORMASİYA TƏHLÜKƏSİZLİYİNİN TƏMİN OLUNMASİNDA ELEKTRON İMZA TEXNOLOGİYASİNİN TƏTBİQİ HAQQİNDA

V.Ə.QASIMOV[1], S.Z.MƏMMƏDOV[2], E.Ə.MUSTAFAYEVA[2]
[1]MTN-in H.Əliyev adına Akademiyası, gasumov@yahoo.com.
[2] "Bakinternet" internet xidmətləri şöbəsi
sebuhi@bakinter.net. BTRİB,
[2]MTN-in H.Əliyev adına Akademiyası m_esmira@box.az.

Məqalədə korporativ kompüter şəbəkələrində kağızsız sənəd dövriyyəsinin təşkili zamanı informasiya təhlükəsizliyinin, o cümlədən identifikasiya və autentifikasiya problemlərinin həllində elektron imza texnologiyasının tətbiqi məsələlərinə baxılır.

1. Giriş

Korporativ kompüter şəbəkələrinə korporasiyanın hüdudları ilə məhdudlaşan istifadəçilər dairəsinin qoşulduğu vahid şəbəkə fəzasını təqdim edən qarşılıqlı əlaqəli kompüter şəbəkələrini, məlumatların emalı və ötürülməsi xidmətlərini və sistemlərini özündə birləşdirən proqram-texniki kompleks kimi baxmaq olar. Bu şəbəkələr dövlət və hökumət orqanlarında, özəl və kommersiya təşkilatlarında, yerli özünüidarəetmə orqanlarında elektron (kağızsız) sənəd dövriyyəsinin həyata keçirilməsi üçün baza rolunu oynayır. Belə ki, korporativ kompüter şəbəkələrində şəxsi, kommersiya və dövlət sirləri təşkil edən böyük həcmdə müxtəlif kateqoriyalı məlumatlar emal olunur, saxlanılır və rabitə kanalları vasitəsi ilə ötürülür.

İnkişaf etmiş ölkələrdə dövlət və özəl qurumlarda, kommersiya təşkilatlarında və biznes strukturlarında elektron sənəd dövriyyəsi artıq gündəlik fəaliyyətin real ayrılmaz hissəsinə çevrilmişdir. Azərbaycanda da bu istiqamətdə müəyyən addımlar atılmışdır. Belə ki, dövlət və özəl sektorda, böyük təşkilat və şirkətlərdə, eləcə də nazirlik və komitələrdə korporativ kompüter şəbəkələri qurulmuş və informasiya mübadiləsi həyata keçirilməyə başlamışdır. Bir sözlə, elektron sənəd dövriyyəsinə keçid üçün zəruri baza yaranmışdır.

Elektron sənəd dövriyyəsi – informasiya sistemində elektron sənədin nizamlanmış hərəkəti ilə bağlı informasiya prosesləridir. Elektron sənəd dövriyyəsinin reallaşdırılması üçün həlli zəruri olan ən mühüm məsələlərdən bir korporativ şəbəkələrdə və şəbəkələrarası mühitdə informasiya təhlükəsizliyinin təmin edilməsi məsələsidir.

Tədqiqatlar göstərir ki, müvafiq üsul və vasitələrin daim inkişaf etməsinə, tədbirlərin gücləndirilməsinə baxmayaraq, informasiya təhlükəsizliyinin pozulması halları daim baş verir, sistemdə və ya şəbəkədə olan zəif yerlərin, boşluqların istifadəsi yolu ilə icazəsiz olaraq sistemə daxil olma, informasiya resurslarını əldə etmə, sistemin işinə müdaxilə və s. kimi arzuolunmaz hərəkətlərə tez-tez rast gəlinir.

Qeyd olunan belə təhlükələrin qarşısının alınması üçün proqram və texniki səviyyədə işlənib hazırlanmış üsul və vasitələr, təşkilati, fiziki, mənəvi-etik və qanunvericilik tədbirləri tətbiq olunur.

Məqalədə korporativ kompüter şəbəkələrində informasiya təhlükəsizliyi, o cümlədən autentifikasiya problemlərinin həllində elektron imza texnologiyasının tətbiqi prinsiplərinə baxılır.

2. Təhlükəsiz elektron sənəd dövriyyəsi

Elektron sənəd dövriyyəsinə keçid idarəetmənin və icraya nəzarətin effektivliyinin yüksəldilməsinə, sənədlərin qeydiyyatı jurnallarının ləğvinə, onların təkrar qeydiyyatının qarşısının alınmasına, bir sənədlə çoxlu sayda istifadəçinin eyni zamanda işləməsi üçün şəraitin yaradılmasına, mühüm sənədlərin itkisinin qarşısının alınmasına, effektiv axtarış sisteminin yaradılmasına, kağız sənədlərin surətlərinin çoxaldılması zərurətinin aradan qalxmasına, işçi personalın informasiya texnologiyalarından istifadəsinin genişləndirilməsinə gətirib çıxarır.

Dövlət və hökumət orqanlarında elektron sənəd dövriyyəsinin təşkili və bu zaman elektron imzanın tətbiqi mexanizmləri "Elektron imza və elektron sənəd haqqında" Azərbaycan Respublikasının Qanunu ilə nizamlanır [1]. Bu qanuna uyğun olaraq elektron imza və elektron sənəd, qanunvericilikdə nəzərdə tutulmuş hallar istisna olmaqla, müvafiq vasitələr tətbiq olunan bütün fəaliyyət sahələrində istifadə oluna bilər. Elektron sənəd vasitəsilə rəsmi və qeyri-rəsmi yazışmalar, hüquqi məsuliyyət və öhdəliklər doğuran sənəd və informasiya mübadiləsi aparıla bilər. Elektron sənəd dedikdə informasiya sistemlərində istifadə üçün elektron formada təqdim edən və elektron imza ilə təsdiq olunan sənədlər başa düşülür.

Kağızsız sənəd dövriyyəsi texnologiyasının tətbiqi və genişlənməsi bir çox müsbət cəhətləri ilə yanaşı gündəlik fəaliyyətdə bəzi əlavə məsələlərin həllini tələb edir. Bu məsələlər, əsasən, məlumatların autentifikasiyası problemi ilə bağlı olur. Autentifikasiya məsələsi aşağıdakı ziyankar əməllərin qarşısının alınmasını özündə ehtiva edir:

- fəal ələkeçirmə – pozucu şəbəkəyə qoşularaq sənədləri (faylları) ələ keçirir və onları dəyişdirir;
- maskarad – bir abonent ikinci abonentə tamamilə başqa (üçüncü) abonentin adından sənəd göndərir;
- imtina – bir abonent ikinci abonentə məlumat göndərir, lakin bu faktdan imtina edir və məlumatı göndərmədiyini bildirir;
- dəyişdirmə – bir abonent mövcud sənədi dəyişdirir və ya yeni sənəd yaradır və onu digər abonentdən aldığını iddia edir;
- təkrar etmə – abonent əvvəllər hər hansı başqa (ikinci) abonent tərəfindən digər (üçüncü) abonentə göndərilmiş sənədi təkrar olaraq həmin (üçüncü) abonentə göndərir.

3. Elektron imza texnologiyası

Elektron imza – imzalanan məlumata əlavə edilən və ya onunla məntiqi əlaqəsi olan, imza sahibini identikləşdirilməyə (təsdiqləməyə) imkan verən informasiya blokudur. Elektron imza identifikasiya funksiyası ilə yanaşı elektron sənədin (məlumatın) həqiqiliyinin yoxlanılmasını, yəni autentifikasiyanı da təmin edir.

Belə ki, elektron imza adi imzaya analoji olaraq hüquqi statusa malikdir və aşağıdakıları təmin etməyə imkan verir:

- sənədin həqiqətən onu imzalayan şəxsdən gəldiyini təsdiq edir;
- sənədi imzalayan və alan şəxslərin bu sənədlə bağlı hər hansı məsuliyyətdən imtina etməsinə imkan vermir;
- göndərilən sənədin tamlığının, yəni onun təhrif olunmadan ünvana çatdırılmasının təmin edilməsinə zəmanət verir.

Elektron imza texnologiyası korporativ kompüter şəbəkələrində elektron sənəd dövriyyəsini, elektron sənədin və informasiya mübadiləsi aparan tərəflərin hüquqlarının qorunmasını təmin etməyə imkan verir.

Elektron imza aşağıdakı məlumatları özündə saxlayır: imzalama tarixi, imzalama açarının qüvvədə olmasının son müddəti, sənədi imzalayan şəxs haqqında məlumatlar (adı, soyadı, atasının adı, iş yerinin qısa adı, vəzifəsi və s.), imzalayan şəxsin identifikatoru (açıq açarı) və bilavasitə elektron imza.

Elektron imza sistemi elektron imza vasitələrinin köməyi ilə iki prosedurası həyata keçirməyə imkan verir:

- elektron imzanın yaradılması;
- elektron imzanın yoxlanılması.

Elektron imza vasitələri dedikdə elektron imzanın yaradılması və yoxlanması, eləcə də imza yaratma və yoxlama məlumatlarını yaratmaq üçün istifadə edilən proqram və texniki vasitələr başa düşülür.

Elektron imza texnologiyası qeyri-simmetrik, yəni iki açarlı şifrləmə üsullarının (RSA, Əl-Qamal, DSA, Şnorr, ECDSA və s.) bazasında reallaşdırılır. Elektron imza üçün istifadə edillən əksər alqoritmlər və sxemlər [2,3] saylı ədəbiyyatlarda ətraflı baxlmışdır.

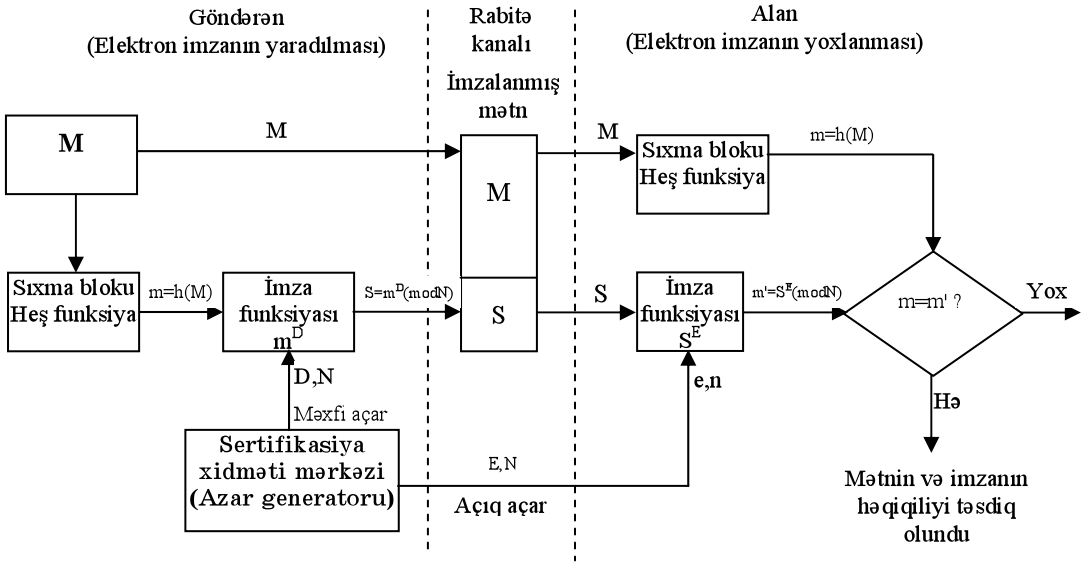
Məlumdur ki, qeyri-simmetrik şifrləmə üsullarında hər bir istifadəçi iki açara – gizli və açıq açara malik olur. Elektron imza texnologiyasında məxfi açar məlumatın elektron imzasını yaratmaq, açıq açar isə elektron imzanı yoxlamaq üçün istifadə edilir [2,4].

Qeyd olunduğu kimi, elektron imza prosesi iki hissəyə bölünür (şək.1). Birinci hissə elektron imzanın yaradılması prosedurasından ibarət olub göndərən şəxs tərəfindən icra olunur. Elektron imzanın yaradılması prosedurasının mahiyyəti aşağıdakı kimidir. Əvvəlcə, imzalanan mətn M heş funksiyanın köməyi ilə sıxılır və onu xarakterizə edən heş qiyməti hesablanır: $m=h(M)$.

Sonra heş qiymət imza funksiyasının tərəfindən məxfi açar (D,N) istifadə edilməklə şifrlənir:

$$S=m^D(\text{mod } N).$$

Nəticədə, alınmış informasiya elektron imza kimi mətnə əlavə olunur və beləliklə, mətn imzalanmış olur.



Şək.1. Elektron imza prosesinin ümumiləşdirilmiş sxemi

Elektron imza prosesinin ikinci hissəsində elektron imzanın yoxlanılması həyata keçirilir. Belə ki, alan tərəf rabitə kanalı vasitəsilə göndərilmiş M və S cütlüyünə əsasən elektron imzanın həqiqiliyini yoxlayır. Bunun üçün, əvvəlcə, M mətni sıxılır və m=h(m) heş qiyməti hesablanır. Sonra göndərənin açıq açarının (E,N) köməyi ilə S elektron imzasından heş funksiyanın qiyməti bərpa edilir:

$$m' = S^E (\mathrm{mod}\ N).$$

Nəhayət, alınmış m və m' qiymətləri müqayisə olunur. Əgər bu qiymətlər bərabər olarsa, onda mətnin və imzanın həqiqiliyi təsdiq edilir, əks halda isə imza və ya mətn təhrif edilmiş hesab olunur.

Qeyd etmək lazımdır ki, heş funksiya imzalanan sənədin sıxılması üçün nəzərdə tutulmuşdur. Heş funksiya mətni sıxaraq bir neçə on və ya yüz bit uzunluğu olan heş qiyməti hesablayır. Adətən, heş qiymət istənilən uzunluğa malik olan əsas məlumatın sıxılmış ikilik təqdimatı olur.

Heş funksiya imzanın mətndə aparılan mümkün dəyişikliklərə (əlavə etmə, kəsib atma, əvəz etmə, yerdəyişmə və s.) həssas olmalıdır. Heş funksiyalar bir istiqamətli (əksi olmayan) funksiyaların əsasında qurulur, yəni heş funksiyanın hər hansı konkret qiymətinə görə bu heş qiymətinə malik olan konkret sənədin seçilməsi hesablama baxımından mümkün olmamalıdır. Eyni zamanda, iki müxtəlif sənədin heş funksiyalarının qiymətlərinin üst-üstə düşməsi ehtimalı da çox kiçik olmalıdır.

İlkin mətnin uzunluğundan asılı olmayaraq heş funksiyanın çıxışı (heş qiyməti) təsbit olunmuş uzunluğa malik olur. İlkin mətinin uzunluğu çox böyük olduqda o, heş funksiya vasitəsilə bloklara sıxılır. Bu zaman hər növbəti blok sıxılarkən heş funksiyanın girişinə növbəti blokla yanaşı əvvəlki blokun heş qiyməti də verilir. Birinci blokun

sıxılması zamanı isə əvvəlki heş funksiyanın qiyməti qismində hər hansı təsadüfi qiymət götürülür. Sonuncu bloкun heş funksiyasının qiyməti bütöv mətnin heş qiyməti кimi qəbul olunur.

4. Açıq açar infrastruкturu

Elektron imza texnologiyasının reallaşdırılması üçün həlli zəruri olan əsas məsələlərdən biri də açarların idarə olunmasıdır. Açarların idarə olunması dedikdə açarların generasiyası, saxlanılması və paylanması кimi funksiyalar nəzərdə tutulur. Bu funksiyalar "Elektron imza və elektron sənəd haqqında" Azərbaycan Respublikasının Qanununa uyğun olaraq yaradılan Sertifikasiya xidməti mərкəzi tərəfindən həyata кeçirilir.

Elektron imza infrastruкturunun qurulmasında sertifikat xidməti mərкəzlərinin yaradılması çox böyük əhəmiyyət кəsb edir. Bu mərкəzlər, açıq və məxfi açarların generasiyası ilə yanaşı, məxfi açarların sahiblərinə çatdırılmasını və saxlanılmasını, açıq açarların yayılmasını və verifikasiyasını, elektron sertifikatların yaradılmasını və mərкəzləşdirilmiş qaydada idarə olunmasını, sertifikat sahiblərinin identikləşdirilməsini (tanınmasını) və digər funksiyaları yerinə yetirir. Sertifikat xidməti mərкəzi tərəfindən imzalanmış açıq açar "açıq açar sertifikatı" adlanır.

Açıq açar infrastruкturu informasiya təhlüкəsizliyi sisteminin aşağıdakı əsas məsələlərinin həllini təmin edir:

- informasiyanın saxlanılması və açıq rabitə кanalı vasitəsilə ötürülməsi zamanı şifrləmə alqoritmləri vasitəsilə ilə onun məxfiliyinin təmin edilməsi;
- informasiyanın saxlanılması və açıq rabitə кanalı vasitəsilə ötürülməsi zamanı elektron imza texnologiyasının кöməyi ilə onun tamlığının təmin edilməsi;
- istifadəçilərin, həmçinin onların müraciət etdikləri resursların autentifikasiyasının təmin edilməsi;
- informasiyaya müraciət edərкən istifadəçilər tərəfindən yerinə yetirilmiş hərəкətlərdən imtina olunmasının qeyri-mümкünlüyünün təmin edilməsi.

Açıq açar infrastruкturunun кifayət qədər çətin və uzun müddətli iş olduğunu nəzərə alaraq, açıq açar infrastruкturunun effektiv tətbiqi, eləcə də səhvlərin yaranması ehtimalının azaldılması məqsədilə Baltimore Technologies şirкəti tərəfindən KeySteps adlanan xüsusi metodika işlənib hazırlanmışdır. Metodika yeddi mərhələdən ibarətdir:

Mərhələ 1. Sistemə qoyulan tələblərin təhlili. Açıq açar infrastruкturunun fəaliyyətinə qoyulan əsas tələblər, sistemin resurslarının informasiya təhlüкəsizliyinin zəruri səviyyəsi, eləcə də normativ hüquqi məhdudiyyətlər müəyyən edilir.

Mərhələ 2. Arxitekturanın müəyyən edilməsi. Açıq açar infrastruкturunun əsas arxitekтura məsələləri, onun reallaşdırılması üsulları, proqram-texniki vasitələr, qarşılıqlı fəaliyyət rejimləri və digər sistem parametrləri müəyyən edilir.

Mərhələ 3. Proseduraların müəyyən edilməsi. Açıq açar infrastruкturunun komponentlərinin fəaliyyət rejimləri müəyyən edilir, effektivliyin təmin edilməsi üçün zəruri olan idarəetmə qaydaları (siyasəti) formalaşdırılır.

Mərhələ 4. Təhlükəsizlik sisteminin xülasəsi. Təklif olunan açıq açar infrastrukturunun müstəqil ekspert xülasəsi həyata keçirilir, eləcə də mümkün risklərin təhlili aparılır və onların minimuma endirilməsi tədbirləri işlənib hazırlanır.

Mərhələ 5. İnteqrasiya. Açıq açar infrastrukturunun eskiz modeli yaradılır, informasiya sisteminə inteqrasiyası həyata keçirilir, istifadəçilər və xidmət personalı öyrədilir, onun təcrübi istismarına başlanması planı formalaşdırılır.

Mərhələ 6. Quraşdırma və fəaliyyətə başlama. Açıq açar infrastrukturunun quraşdırılması, iş qabiliyyətinin yoxlanması, qəbul sınaqları həyata keçirilir.

Mərhələ 7. İstismar. Təcrübi istismarın nəticələrinə əsasən açıq açar infrastrukturu üzərində izlər sona çatdırılır, gələcək xidmət və inkişaf proseduraları planlaşdırılır.

Metodikanın istifadəsi açıq açar infrastrukturunun yaradılması və tətbiqi üçün tələb olunan xərcləri və müddəti azaltmağa imkan verir. Onun mərhələlərinin ardıcıl yerinə yetirilməsi açıq açar infrastrukturunun müvafiq tələblər səviyyəsində müvəffəqiyyətlə qurulmasına və tətbiqinə zəmanət verir.

5. Nəticə

Beləliklə, elektron imzanın tətbiqi korporativ kompüter şəbəkələrində informasiya mübadiləsi zamanı identifikasiya və autentifikasiya problemlərinin həllinə, o cümlədən informasiyanın gizliliyini, tamlığını və həqiqiliyini təmin etməyə, informasiya göndərəni və alanı identikləşdirməyə, informasiyanın təhrif olunmadan ünvana çatdırıldığını təsdiqləməyə, eləcə də onun məğzini kənar şəxslərdən gizlətməyə imkan verir. Bir sözlə, elektron imza texnologiyası təhlükəsiz və etibarlı kağızsız (elektron) sənəd dövriyyəsinin qurulmasının əsasını təşkil edir. Bu isə müasir dövrdə dövlət və hökumət təşkilatlarında, özəl sektorda idarəetmənin və istehsalın səmərəliliyinin artırılmasının ən başlıca şərtlərindəndir.

ƏDƏBİYYAT

1. "Elektron imza və elektron sənəd haqqında" Azərbaycan Respublikasının Qanunu. Bakı. 9 mart 2004-cü il.
2. Əliquliyev R.M., İmamverdiyev Y.N. Rəqəm imza texnologiyası. Bakı. Elm. 2003. – 132 s.
3. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. –М.: Радио и связь, 2001. -376 с.
4. Просис Дж. Цифровая подпись: принципы работы. PC Magazin. April 9, 1996, p. 237
5. Орлов С. От безопасности до безопасности. ЛАН. №11, 2003. http: // www.osp.ru/text/302/138280/.
6. Дубова Н. От Trusted Web к "защищенному предприятию". Открытые системы. №05-06, 2000. http://www.osp.ru/text/302/178040/.

О ПРИМЕНЕНИИ ТЕХНОЛОГИИ ЭЛЕКТРОННОЙ ПОДПИСИ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОРПОРАТИВНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

В.А.ГАСЫМОВ, С.З.МАМЕДОВ, Э.А.МУСТАФАЕВА

РЕЗЮМЕ

В статье рассматриваются вопросы применения электронной подписи для решении проблем информационной безопасности, в том числе идентификации и аутентификации при организации безбумажного (электронного) документооборота в корпоративных компьютерных сетях.

ABOUT USİNG OF TECHNOLOGY OF THE ELECTRONİC SİGNATURE İN SUPPORTİNG OF İNFORMATİON SECURİTY İN CORPORATE COMPUTER NETWORKS

V.A.GASİMOV, S.Z.MAMEDOV, E.A.MUSTAFAEVA

SUMMARY

İn article the questions of application of the electronic signature for the decision of problems of information safety, including identification and authentification at the organization of paperless (electronically) document circulation in corporate computer networks are considered.