AZƏRBAYCAN MİLLİ ELMLƏR AKADEMİYASI
KİBERNETİKA İNSTİTUTU
İNFORMASİYA TEXNOLOGİYALARI İNSTİTUTU

«İNFORMASİYALAŞDIRMA, KİBERNETİKA VƏ İNFORMASİYA TEXNOLOGİYALARININ MÜASİR PROBLEMLƏRİ»

II Respublika elmi konfransının
(Bakı, 26-28 oktyabr 2004-cü il)

ƏSƏRLƏRİ

I CİLD

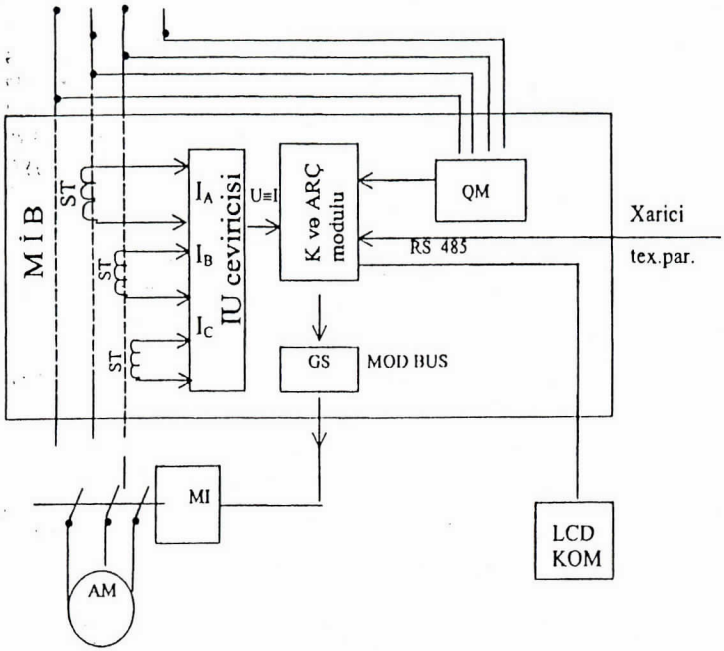
ТРУДЫ

II Республиканской научной конференции
«СОВРЕМЕННЫЕ ПРОБЛЕМЫ ИНФОРМАТИЗАЦИИ, КИБЕРНЕТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»
(Баку,26-28 октября 2004 года)

I ТОМ

KONFRANS AZƏRBAYCAN MİLLİ ELMLƏR AKADEMİYASININ 60 İLLİYİNƏ HƏSR OLUNUR

BAKI-2004



Şək 1. MİB-in struktur və asinxron mühərrikə qoşulma sxemi.

ƏDƏBİYYAT

3. *T.M.Вердиев.* Теоретические основы проектирования скважинной штанговой насосной установки.Баку; ЭЛМ, 2000-88 с.
4. Блочно-модульная станция управления БМС–1УП-70.Паспорт БМС.115.0000000. ОКБ Нефтянного приборостроения. E-mail:postmaster@okbnp.udm.ru
5.Однокристальные микро-ЭВМ.М.:МИКАП, 1994,-400с:ил.-ISBN 5-85959-030-X

R.M. ƏLIQULIYEV, T.X. FƏTƏLIYEV, M.Ə.HACIRƏHIMOVA

KORPORATİV ŞƏBƏKƏ MÜHİTİNDƏ ELEKTRON SƏNƏDLƏRİN DÖVRİYYƏSİNİN MÜHAFİZƏSİ

(Bakı, AMEA, İnformasiya texnologiyaları İnstitutu)

Hal-hazırki dövrdə şəbəkə strukturu və yeni informasiya texnologiyalarının sürətli inkişafı ərazicə paylanmış iri müəssisələrin korporativ şəbəkə və informasiya sistemlərinin yaradılması məsələsini olduqca asanlaşdırmışdır. Bununla yanaşı, eyni zamanda korporativ informasiyanın mühafiəsi məsələsi ön plana çıxmışdır. İşdə AMEA korporativ şəbəkəsi mühitində elektron sənədlərin dövriyyəsinin mühafizəsi məsələlərinə baxılır [1,2]. Sistemin proqram təminatı Windows NT 4.0 və Delphi-də işləndiyindən işdə baxılan məsələlər uyğun təhlükəsizlik mexanizmlərindən istifadə edilməklə həyata keçirilmişdir.

Sistemdə identifikasiya və autentifikasiya. Sistemdə yeni istifadəçinin qeydiyyatı, silinməsi, dəyişdirilməsi və həqiqiliyinin yoxlanması imkanları nəzərə alınmışdır. Bu əməliyyatlar müəyyən məhdud zaman intervalında həyata keçirilir, əks halda sistemə giriş və ya parolun dəyişdirilməsi mümkün olmur. Eyni zamanda yuxarıda göstərilən işlərə edilən təkrar cəhdlərin sayı da məhdudlaşdırılmışdır. Qeyd etmək lazımdır ki, Web-serverə hər bir müraciət zamanı istifadəçinin identifikasiya və autentifikasiyası aparılır. Bu da sorğu formasında daxil olunmuş qeydiyyat informasiyasının serverdə verilənlər bazasındakı (VB) identifikasiya və autentifikasiya informasiyası ilə müqayisəsi həyata keçirilir. Parolların müddaxiləyə davamlılığını təmin etmək məqsədi ilə aşağıdakılar nəzərə alınmalıdır:

- parolun uzunluğu 6 simvoldan az olmamalıdır;
- parol identifikatorlarla üst-üstə düşməməlidir;
- geniş yayılmış tarixlərdən istifadə olunmamalıdır;
- tərsinə yazılan identifikatorlardan istifadə olunmamalıdır və s.

Sənədlərin və verilənlər bazasının mühafizəsi. İnformasiya təhlükəsizliyi baxımından istifadəçilərə sənəd üzərində edə biləcəyi əməliyyatlar (oxumaq, dəyişdirmək, silmək və s.) üzrə icazələr əvvəlcədən dəqiq müəyyən olunur. Həmçinin sənədin kimə və hansı təşkilata məxsus olduğunu müəyyən edən mexanizm nəzərə alınmışdır. Belə ki, yeni sənəd yaradılarkən təşkilatın adı və sistemlə işləyən istifadəçinin adı, soyadı cavabdeh qismində avtomatik olaraq sənədin kartına əlavə olunur. Bununla da digər təşkilatların adından istifadə etməklə sənəd yaratmaq və sənəd göndərmək imkanı məhdudlaşdırılmışdır. Hüquqi baxımdan, konkret işçi yerində yaradıla bilən sənədlərin tipi də sistem tərəfindən avtomatik məhdudlaşdırılır, məsələn, institutlar qanun, fərman, sərəncam və s. tipli sənədlər yaratmaq hüququna malik deyildirlər.

Ayrıca işçi yerində, həmçinin bir işçi yerindən digərinə göndərilərkən sənədlərdə icazəsiz dəyişikliklərin aparılmasına (modifikasiya olunması və ya silinməsinə) yol verməmək üçün sistemdə bir sıra tədbirlər nəzərdə tutulmuşdur. Məlnin dəyişdirilməsinin qarşısını almaq məqsədi ilə sənədin atributları siyahısına avtomatik hesablanan, nəzarət cəmi tipli bütövlük kodu əlavə olunur. Bu kod sənədin kartı ilə birgə göndərilir. Sənədin qəbulundan sonra avtomatik hesablanan bütövlük kodu sənədin kartındakı uyğun kodla müqayisə olunur. Əgər kodlar üst-üstə düşmürsə, sənədin bütövlüyü və həqiqiliyi şübhə altına alınır.

Sənədlər İnternet mühitdə ötürüldüyündən və serverdə fayllar şəklində saxlandığından əməliyyat sistemi və disk redaktorları vasitəsilə onlara yeni təhlükələr yaranır ki, bunu da neytrallaşdırmaq üçün şifrələmədən istifadə olunur.

Sənədlərlə yanaşı eyni zamanda onların göndərildiyi ünvanların qorunması da çox vacibdir. Bunun üçün göndərilən təşkilatların siyahısı dinamiki Web-səhifənin daxilində gizli şəkildə ötürülür.

İnformasiya təhlükəsizliyi baxımından kritik informasiya olan istifadəçilərin psevdonim və parollarının, sənədlər kartının saxlanıldığı VB-nın mühafizəsi xüsusilə vacibdir. Bu baza Web-serverdə saxlanılır. Bazada düzəliş, yeni yazı əlavə etməyə, yazını silməyə yalnız sistem administratorunun hüququ vardır. İstifadəçilərin bu bazaya girişi mümkün qədər məhdudlaşdırılmışdır və yalnız Web-serverə göndərdikləri sorğuların emalı zamanı ondan istifadə etmək imkanları vardır. Sistem administratoru VB ilə əlaqədar aşağıdakı tədbirləri vaxtaşarı həyata keçirməli və onun vəziyyətini daim nəzarətdə saxlamalıdır:

- VB-nın obyektlərinə (cədvəllərə, saxlanan proseduralara və s.) girişə icazə hüququnun pozulması;

- VB-da eyni vaxtda bir neçə administratorun işləməsinin qarşısının alınması;
- ehtiyat surətlərinin çıxarılması alt sisteminin yoxlanılması;
- saxlanan proseduraların yoxlanılması;
-VB idarəetmə sisteminin obyektlərinə giriş hüquqlarının yoxlanılması;
- müxtəlif hücumların həyata keçirilməsi imkanlarının yoxlanılması;
- sistemə VB üçün müxtəlif təzələnmə paketlərinin yazılması və s.

Rəqəm imzasının tətbiqi. Rəqəm imzası sənədin həqiqiliyinin yoxlanmasını həyata keçirən kriptoqrafik çevirmədir.

Sistemdə tətbiq olunmuş rəqəm imzası sxemi açıq açarlı kriptosistem vasitəsilə aşağıdakı kimi həyata keçirilmişdir:

- Sənədi göndərən şəxs MD5 heş-funksiyasından istifadə etməklə, sənədin daycestini yaradır [3];
- Sonra həmin daycesti RSA açıq açarlı şifrləmə alqoritmi ilə məxfi açarından istifadə etməklə şifrləyir [4];
- Şifrlənmiş daycest sənədə birləşdirilir, onun rəqəm imzası alınır və lazımi ünvana göndərilir;
- Alan şəxs sənədə birləşdirilmiş daycesti göndərənin açıq açarından istifadə etməklə RSA alqoritmi ilə deşifrləyir;
- Sonra MD5 alqoritmindən istifadə etməklə aldığı sənədin daycestini yaradır;
- Deşifrə olunmuş daycestlə özünün yaratdığı daycesti müqayisə edir;
- Əgər daycestlər eynidirsə, onda imza həqiqi sayılır. Əks halda sənəd rədd olunur və sistemin administratorunun iştirakı ilə hadisə araşdırılır.

Qeyd etmək lazımdır ki, sistemin mühafizəsi izah olunmuş vasitələrdən düzgün istifadə etməklə yanaşı, eyni zamanda sənədlərə icazəsiz müraciət cəhdlərinə nəzarət və onlara operativ münasibət göstərməklə tam təmin olunur.

ƏDƏBİYYAT

1. *Əliquliyev R.M., Fətəliyev T.X.* Korporativ şəbəkə mühitində elektron sənədlərin dövriyyəsinin avtomatlaşdırılması sistemi. Azərbaycan Milli Elmlər Akademiyasının Xəbərləri. Fizika - texnika və riyaziyyat elmləri seriyası, №3, 2001.
2. *Панасенко С.П.* Защита документооборота в современных компьютерных системах. Информационные технологии, №4, 2001.
3. *Riverst R. L.*, RFC 1321: The MD5 Message-Digital Algoritm. Internet Activities Boad, April 1992.
4. *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-P.120-126.

Ə.M.ƏMİROV, A.H.RZAYEV, Y.H.ƏLİYEV, M.H.RİZVANOV

ÇOXPARAMETRLİ İNTELEKTUAL ÖLÇÜ SİSTEMİ

(Sumqayıt, «Neftqazavtomat» EİB)

Mikroprosessorlar və mikrotexnologiyaların müasir inkişaf sürəti durmadan artır və bu da ölçü sistemlərinin yeni elementlər bazasında qurulmasını aktuallaşdırır. Bu baxımdan «Neftqazavtomat» EİB-də müasir mikrokontrollerlər (MK), analoq rəqəm çeviriciləri (ARÇ) , maye kristallı displeylər (MKD) və kanal elementləri (KE) əsasında kompüter şəbəkələri ilə sadə uzlaşa bilən çoxparametrli intelektual ölçü sistemlərinin (ÇİÖS) yaradılması qarşıya qoyulmuş və müvəffəqiyyətlə həll edilmişdir.