**Təhlükəsizlik texnologiyaları.**

**İnformasiya təhlükəsizliyi**

Elmi-texniki inqilab informasiya cəmiyyətinin yaranmasına səbəb olmuşdur. Bu cəmiyyətdə informasiya və biliklər ən mühüm resurs və başlıca əmtəədir. Vətəndaşların, cəmiyyətin və dövlətin həyatında informasiyanın, informasiya resurslarının və texnologiyalarının rolunun artması informasiya təhlükəsizliyi məsələlərini ön plana çıxarır. Müasir cəmiyyət tədricən öz informasiya infrastrukturunun vəziyyətindən asılı olur.

İnformasiyanın təhlükəsizliyinin təmin olunması probleminin vacibliyini və aktuallığını şərtləndirən səbəblərdən aşağıdakıları xüsusi vurğulamaq olar:

* şəbəkə texnologiyalarının geniş yayılması və lokal şəbəkələrin qlobal şəbəkələr halında birləşməsi;
* informasiya təhlükəsizliyinin pozulmasına praktik olaraq mane olmayan qlobal Internet şəbəkəsinin inkişafı;
* minimal təhlükəsizlik tələblərinə belə cavab verməyən proqram vasitələrinin geniş yayılması.

*İnformasiya təhlükəsizliyi* dedikdə, informasiya və ona xidmət edən infrastrukturun sahibi və ya istifadəçilərinə ziyan vurmağa səbəb olan təbii və ya süni xarakterli, təsadüfi və ya qəsdli təsirlərdən informasiya və ona xidmət edən infrastrukturun mühafizəliliyi nəzərdə tutulur.

*İnformasiyanın mühafizəsi* – informasiya təhlükəsizliyinin təmin olunmasına yönəlmiş tədbirlər kompleksidir

. İnformasiyanın təhlükəsizliyi dedikdə informasiya sistemində saxlanan və emal edilən informasiyanın mühafizəsi başa düşülür. İS-də informasiyanın mühafizəsi probleminə proqram və aparat vasitələrinin mühafizəsi problemi ilə birlikdə baxılması məqsədəuyğun hesab edilir, çünki İS-in fəaliyyət mühitinin əsasını proqram və aparat vasitələri təşkil edirlər. Proqraraların və verilənlərin mühafizəsi üçün mövcud olan üsul və vasitələr VB proqramları (VBİS, tətbiqi proqramlar, saxlanan prosedurlar və s.) və VB-də saxlanan verilənlər ücün də tətbiq edilə bilər.

Mühafizə sisteminin qurulma prinsiplərini və hesablama sisteminin (HS) müxtəlif komponentlərinin (əməliyyat sisteminin, xidməti proqramların, VBİS-in, informasiyanın mühafizəsi ücün xüsusi qurğuların və proqramların) imkanlarını yaxşı bilməklə, İS-in zəif yerlərini qiymətəlndirmək və məxvi informasiyanın mühafizəsini yaxşı təşkil etmək olar.

Şəbəkə rejimi kompüterlərdən istifadə edilmənin ümumi halı olduğundan, informasiyanın mühafizəsi probleminə baxarkən, adətən, kompüterlər arasında şəbəkə əlaqələrinin olması nəzərə alınır.

Hesablama sisteminin keyfiyyətli mühafizəsini təmin etmək üçün təkcə onun yerləşdiyi binanın mühafizəsini təşkil etmək və proqram mühafizə vasitələri qurmaq kifayət deyil. Hesablama sisteminin mühafızəsinin təşkilinə onun strukturuna, həll olunan məsələlərə, mühafizənin məqsədinə və imkanlarına uyğun kompleks yanaşma tələb olunur.

Mühafizə sistemini HS-in və onun informasiya-proqram təminatmm yaradılmasına başlayarkən nəzərə almaq və həyat dövrünün bütün mərhələlərində reallaşdırmaq lazımdır. Lakin praktikada bir sıra səbəblər üzündən mühafızə sistemini HS və onun informasiya-proqram təminatı hazır olandan sonra yaradırlar. Yaradılan muhafizə sistemi çoxsəviyyəli olmalı və mövcud vasitələr, metodlar və tədbirlərin rasional təşkil edilmiş toplusundan ibarət olmalıdır. Hesablama sistemi istifadəçilərin və xidmətçi heyətin səriştəsiz əməllərindən mühafızə olunmalıdır.

Hesablama sisteminin səmərəli mühafızə mexanizminin qurulması ücün aşağıdakılar tələb olunur:

- hesablama sisteminin mühafizəyə ehtiyacı olan zəif elementlərini təyin etmək;

- həmin elementlər ücün təhlükələri təyin etmək;

- mühafizə sisteminə qoyulan tələbləri formalaşdırmaq;

- tələblərə cavab verən mühafızə vasitələrini və üsullarını seçmək.

Hesablama sisteminin təhlükəsizliyi bir və ya bir neçə potensial təhlükə nəticəsində pozula bilər. Təhlükə dedikdə hesablama sistemində saxlanan və emal olunan informasiyanın, o cümlədən, proqramların təhlükəsizliyinin pozulmasına gətirən, qəsdən və ya təsadüfən baş verən əməliyyat başa düşülür.

Təhlükələrin əsas növləri aşağıdakılardır:

1. HS-in resurslarından icazəsiz istifadə edilmə:

- verilənlərdən istifadə edilmə (surət çıxarma, dəyişdirmə, silmə, çap etmə və s.);

- proqramların surətlərinin çıxarılması və dəyişdirilməsi;

- sistemə həmlə etmə məqsədilə proqramların araşdırılması.

2. HS-in rezuslarından düzgün istifadə edilməməsi:

- tətbiqi proqramların əsas yaddaşın onlara aid olmayan bölmələrinə təsadüfən müraciət etmələri;

- disk yaddaşının sistem bölmələrinə təsadüfi müraciətlər;

- verilənlər bazasmda səhvən dəyişiliklər edilməsi (səhv verilənlərin daxil edilməsi, verilənlərin istinad tamlığının pozulması);

- istifadəçilərin və xidmətçi heyətin səhv hərəkətləri.

3. Proqram və aparat vasitələrində səhvlərin aşkar edilməsi.

4. Rabitə xətlərində və ötürmə sistemlərində verilənlərin ələ keçirilməsi.

5. Elektromaqnit şüalanmaların icazəsiz qeydə alınması.

6. Hesablama sisteminin qurğularının, informasiya daşıyıcılarının və sənədlərin oğurlanması.

7. Hesablama sisteminin komponentlərinin, informasiyanın ötürülmə vasitələrinin tərkiblərinin icazəsiz dəyişdirilməsi və ya sıradan çıxarılması.

Təhlükəsizliyin pozulmasının mümkün nəticələri aşağdakılar ola bilər:

- məxvi məlumatın ələ keçirilməsi;

- sistemin məhsuldarlığının azalması və ya sistemin bütövlükdə dayanması;

- əməliyyat sisteminin yüklənə bilməməsi;

- maddi ziyan;

- faciəli nəticələr.

Mühafızənin məqsədi hesablama sistemində informasiyanın təhlükəsizliyinin təmini olduğundan, əsas problem təhlükələrin qarşısını əvvəlcədən almaqdan ibarətdir.

Mümkün təhlükələrdən asılı olaraq mühafızənin 3 əsas məsələsini ayırmaq olar:

-informasiyanı oğurlanmaqdan mühafizə etmək;

-informasiyanı itkilərdən mühafızə etmək;

-hesablama sistemini nasazlıqlardan və dayanmalardan mühafizə etmək.

Informasiyanın oğurlanmaqdan mühafizə edilməsi informasiyanı saxlayan qurğuların və daşıyıcıların fıziki oğurlanmasının, informasiyanın icazəsiz alınmasının (surətinin çıxarılması, baxış, ələ keçirilməsi və s.) və proqramların icazəsiz yayılmasının qarşısının alınmasını nəzərdə tutur.

İnformasiyanın itkilərdən mühafızə edilməsi informasiyanın düzgünlüyünün və tamlığının (fıziki, məntigi və semantik baxımdan) qorunmasını nəzərdə tutur. Sistemdə informasiya istifadəçilərin və proqramların (o cümlədən virusların) icazəsiz müraciətləri, istifadəçilərin, proqramlarm və xidmətçi heyətin səhv əmə-liyyatları səbəbindən və həmçinin hesablama sistemindəki nasazlıqlardan və dayanmalardan informasiya itirilə bilər.

Aparat və proqram vasitələrinin nasazlıqlardan və dayanmalardan mühafizə edilməsi sistemin normal fəaliyyətinin vacib şərtlərindən biridir. Sistemin nasazlıqlardan və dayanmalardan mühafizəsinin əsas yükü aparat-proqram komponentlərinin- prosessorun, əsas və xarici yaddaş qurgularının, daxiletmə-xaricetmə qurğularının və həmcinin əməliyyat sisteminin proqramlarının üzərinə düşür. Sistem vasitələrinin etibarlığı kifayət qədər olmadıqda, nasazlıqlardan və dayanmalardan mühafızəni tətbiqi proqramlarda nəzərə almaq lazım qəlir.

Etibarhq dedikdə hesablama sisteminin öz funksiyalarını dəqiq və vaxtında yerinə yetirməsi qabiliyyəti başa düşülür. Proqram təminatının etibarlıq dərəcəsi yaradılma prosesinin avtomatlaşdırılmasının keyfıyyəti və səviyyəsi ilə və həmçinin onun müşayiətinin təşkili ilə təyin olunur. Etibarlığı 100% təmin etmək mümkün olmadığından, nasazlıqları və dayanmaları aradan qaldırdıqdan sonra proqramların iş qabiliyyətlərinin tez bərpa edilməsi ücün vasitələr nəzərə alınmalıdır.

Hesablama sistemlərində informasiyanın kompleks mühafızənin təşkili ücün ümumi halda 4 mühafizə səviyyəsi nəzərə alına bilər:

1. Hesablama sisteminin yerləşdiyi bütün ərazini əhatə edən xarici səviyyə;

2. Hesablama sisteminin qurgularınının və rabitə xətlərinin yerləşdiyi ayrı-ayrı ərazilər səviyyəsi;

3. Hesablama sisteminin komponentlərinin və informasiya daşıyıcılarının səviyyəsi;

4. İnformasiyanın saxlanması, emalı və ötürülməsi texnoloji proseslərin səviyyəsi.

Birinci üç səviyyədə çəpərləmə, siqnalvermə sistemi, keçid rejiminin təşkili, məftillərin ekranlaşdırılması və s. yolları ilə informasiya təhlükəsizliyi fıziki olaraq təmin edilir. Sonuncu səviyyə isə informasiyaya fiziki müraciət mümkün olan halda onu məntiqi mühafızə etməyi nəzərdə tutur.

**Kompüter şəbəkələrində təhlükələrin təsnifatı**

*Təhlükə* dedikdə sistemə dağılma, verilənlərin üstünün açılması və ya dəyişdirilməsi, xidmətdən imtina formasında ziyan vurulmasına səbəb ola bilən istənilən hal, şərait, proses və hadisələr nəzərdə tutulur.

Təhlükələri müxtəlif siniflərə ayırmaq olar. Meydana çıxma səbəblərinə görə təhlükələri *təbii* və *süni* xarakterli təhlükələrə ayırırlar. Süni xarakterli təhlükələr də öz növbəsində *bilməyərəkdən* və *qəsdən* törədilən təhlükələrə bölünür. Təsir məqsədlərinə görə təhlükələrin üç əsas növü ayırd edilir:

* İnformasiyanın *konfidensiallığının* pozulmasına yönələn təhlükələr;
* İnformasiyanın *tamlığının* pozulmasına yönələn təhlükələr;
* *Əlyetənliyin* pozulmasına yönələn təhlükələr (DoS hücumlar, Denial of Service - xidmətdən imtina).

*Konfidensiallıq* informasiyanın subyektiv müəyyən olunan xassəsidir. Verilən informasiyaya müraciət icazəsi olan subyektlərin siyahısına məhdudiyyət qoyulmasının zəruriliyini göstərir. Konfidensiallığın *pozulmasına yönələn təhlükələr* məxfi və ya gizli informasiyanın üstünün açılmasına yönəlib. Belə təhlükələrin reallaşması halında informasiya ona müraciət icazəsi olmayan şəxslərə məlum olur.

*Tamlıq* - informasiyanın təhrifsiz şəkildə mövcudolma xassəsidir. *İnformasiyanın tamlığının pozulmasına* yönələn təhlükələr onun dəyişdirilməsinə və ya təhrifinə yönəlib ki, bunlar da onun keyfiyyətinin pozulmasına və tam məhvinə səbəb ola bilər. İnformasiyanın tamlığı bədniyyətli tərəfindən qəsdən və ya sistemi əhatə edən mühit tərəfindən obyektiv təsirlər nəticəsində pozula bilər.

*Əlyetənlik* – yolverilən vaxt ərzində tələb olunan informasiya xidmətini almaq imkanıdır. Həmçinin əlyetənlik – daxil olan sorğulara xidmət üçün onlara müraciət zəruri olduqda uyğun xidmətlərin həmişə hazır olmasıdır. *Əlyetənliyin pozulmasına* yönələn təhlükələr elə şəraitin yaradılmasına yönəlib ki, bu zaman müəyyən qəsdli hərəkətlər ya sistemin iş qabiliyyətini aşağı salır, ya da sistemin müəyyən resurslarına girişi bağlayır.

Təhlükələr digər əlamətlərinə görə də təsnif oluna bilər:

* Baş vermə ehtimalına görə (çox ehtimallı, ehtimallı, az ehtimallı);
* Meydana çıxma səbəblərinə görə (təbii fəlakətlər, qəsdli hərəkətlər);
* Vurulmuş ziyanın xarakterinə görə (maddi, mənəvi);
* Təsir xarakterinə görə (aktiv, passiv);
* Obyektə münasibətinə görə (daxili, xarici);

Daxili və xarici təhlükələrin nisbətini təqribi olaraq belə xarakterizə etmək olar. Təhlükələrin 80%-i təşkilatın öz işçiləri tərəfindən onların bilavasitə və ya dolayısı yolla iştirakı ilə baş verir. Təhlükələrin 20%-i kənardan icra olunur.

Kompüter şəbəkələrində informasiya təhlükəsizliyinin təmin olunmasının texnoloji aspektləri

İnformasiya təhlükəsizliyinin təmin olunması problemi *kompleks yanaşma* tələb edir. Onun həlli üçün tədbirləri aşağıdakı səviyyələrə bölmək olar:

* **qanunvericilik tədbirləri**;
* **inzibati tədbirlər;**
* **təşkilati tədbirlər;**
* **proqram-texniki tədbirlər.**

***Qanunvericilik tədbirləri*** müvafiq qanunları, normativ aktları, standartları və s. əhatə edir. Təəssüflə qeyd etmək lazımdır ki, qanunvericilik bazası bütün ölkələrdə praktikanın tələblərindən geri qalır. Qanunvericilik səviyyəsinin funksiyalarına aid etmək olar:

* İnformasiya təhlükəsizliyinin pozucularına qarşı neqativ münasibət yaratmaq və onu dəstəkləmək;
* İnformasiya təhlükəsizliyi probleminin vacibliyini hər zaman qeyd etmək;
* resursları tədqiqatların ən mühüm istiqamətlərində cəmləşdirmək;
* təhsil fəaliyyətini koordinasiya etmək.

Qanunvericilik səviyyəsində hüquqi aktlar və standartlar xüsusi diqqətə layiqdir. Standartların arasında «Narıncı kitab», X.800 tövsiyələri, ISO 15408 («Ümumi meyarlar»), ISO 27001 (İnformasiya təhlükəsizliyinin idarə edilməsi) standartları daha geniş yayılıb.

***İnzibati tədbirlərin*** əsas məqsədi təşkilatda informasiya təhlükəsizliyi sahəsində tədbirlər proqramını formalaşdırmaq və onun yerinə yetirilməsini zəruri resurslar ayırmaqla və işlərin vəziyyətinə nəzarət etməklə yerinə yetirilməsini təmin etməkdir. Tədbirlər proqramının əsasını təşkilatın öz informasiya aktivlərinin mühafizəsinə yanaşmasını əks etdirən *informasiya təhlükəsizliyi siyasəti* təşkil edir.

*İnformasiya təhlükəsizliyi siyasəti* – təşkilatda məxfi verilənlərin və informasiya proseslərinin mühafizəsi üzrə qabaqlayıcı tədbirlər kompleksidir. İnformasiya təhlükəsizliyi siyasətinin işlənməsinin əsas istiqamətləri aşağıdakılardır:

**1.** Hansı verilənləri və hansı ciddiyyətlə mühafizə etmək lazım olduğunu müəyyənləşdirmək;

**2.** Müəssisəyə informasiya aspektində kimin və nə həcmdə ziyan vura biləcəyini müəyyənləşdirmək;

**3.** Risklərin hesablanması və onların qəbuledilən səviyyəyədək azaldılması sxeminin müəyyən edilməsi;

**4.** Planlaşdırılan bütün texniki və inzibati tədbirlərin təsviri;

**5.** Baxılan proqramın iqtisadi qiymətinin hesablanması;

**6.** Müəssisənin rəhbərliyi tərəfindən təsdiq olunma və sənədləşdirmə;

**7.** Həyata keçirilmə.

***Təşkilati tədbirlər*** informasiya mühafizəsinin səmərəli vasitələrindən biri olmaqla yanaşı, qurulan bütün mühafizə sistemlərinin əsasını təşkil edir. Təşkilati tədbirlər aşağıdakı mövzuları əhatə edir:

* şəxsi heyətin idarəolunması;
* fiziki mühafizə;
* sistemin iş qabiliyyətinin saxlanması;
* təhlükəsizlik rejiminin pozulmasına reaksiya;
* bərpa işlərinin planlaşdırılması.

Biz aşağıdakı ***proqram–texniki tədbirləri*** nəzərdən keçirəcəyik: identifikasiya və autentikasiya, icazələrin idarəolunması, protokollaşdırma və audit, kriptoqrafiya, ekranlaşdırma.

**İdentifikasiya və autentifikasiya.** *İdentifikasiya* (ingilis dilində identification) istifadəçiyə (və ya müəyyən istifadəçinin adından fəaliyyət göstərən prosesə) özünü adlandırmağa (öz adını bildirməyə) imkan verir.

*Autentikasiya* (ingilis dilində authentication) vasitəsi ilə ikinci tərəf əmin olur ki, subyekt doğrudan da özünü qələmə verdiyi şəxsdir. Autentifikasiya sözünün sinonimi kimi çox vaxt “həqiqiliyin yoxlanması” işlədilir.

Subyekt aşağıdakı mənbələrdən ən azı birini təqdim etməklə özünün həqiqiliyini təsdiq edə bilər:

* bildiyi nəyi isə (parolu, şəxsi identifikasiya nömrəsi, kriptoqrafik açar);
* sahib olduğu nəyi isə (şəxsi kart və ya digər təyinatlı analoji qurğu);
* özünün tərkib hissəsi olan nəyi isə (səs, barmaq izləri və s., yəni özünün biometrik xarakteristikalarını).

Autentifikasiyanın ən geniş yayılmış növü paroldur. Daxil edilmiş parol və istifadəçi üçün əvvəlcədən verilmiş parol müqayisə edilir. Onlar üst-üstə düşdükdə istifadəçinin həqiqiliyi təsdiqlənmiş sayılır.

Parolların ən başlıca nöqsanı onların elektron ələ keçirilməsidir. Praktik olaraq yeganə çıxış yolu rabitə xətləri ilə ötürülməzdən əvvəl parolların kriptoqrafik şifrələnməsidir. Aşağıdakı tədbirlər parol mühafizəsinin etibarını artırmağa xeyli imkan verir:

* texniki məhdudiyyətlər qoyulması (parol çox qısa olmamalıdır, parolda hərf, rəqəm, durğu işarələri olmalıdır və s.)
* parolun fəaliyyət müddətinin idarə olunması, onların vaxtaşırı dəyişdirilməsi;
* parollar faylına icazənin məhdudlaşdırılması;
* sistemə uğursuz daxilolma cəhdlərinin məhdudlaşdırılması;
* istifadəçilərin təlimatlandırılması;
* parol generasiya edən proqramların istifadəsi.

Sadalanan tədbirləri həmişə, hətta parolla yanaşı digər autentifikasiya metodları istifadə olunduğu halda da tətbiq etmək məqsədə uyğundur. Biometrik xarakteristikalara nəzarət qurğuları mürəkkəb və bahadırlar, buna görə də yalnız təhlükəsizliyə yüksək tələblər olan təşkilatlarda istifadə olunurlar.

**İcazələrin idarə edilməsi.** İcazələrin idarə edilməsi *subyektlərin* (istifadəçi və proseslərin) *obyektlər* (informasiya və digər kompüter resursları) üzərində yetinə yetirə biləcəyi *əməliyyatları* müəyyən etməyə və onlara nəzarət etməyə imkan verir. İcazələrin məntiqi idarə edilməsi (icazələrin fiziki idarə edilməsindən fərqli olaraq) proqram vasitələri ilə realizə olunur.

Məsələnin formal qoyuluşuna baxaq. Subyektlər məcmusu və obyektlər toplusu var. İcazələrin məntiqi idarəolunması hər bir (*subyekt*, *obyekt*) cütü üçün yolverilən (mümkün) əməliyyatlar çoxluğunu müəyyən etməkdən və qoyulmuş qaydaların yerinə yetirilməsinə nəzarət etməkdən ibarətdir.

(*Subyekt*, *obyekt*) münasibətini cədvəl şəklində təsvir etmək olar. Jədvəlin sətirlərində subyektlər, sütunlarında obyektlər sadalanır. Sətir və sütunların kəsişdiyi xanalarda verilən icazə növləri və əlavə şərtlər (məsələn, vaxt və hərəkətin məkanı) yazılır.

İcazələrin məntiqi idarə edilməsi mövzusu – informasiya təhlükəsizliyi sahəsində ən mürəkkəb mövzudur. Səbəb ondadır ki, obyekt anlayışının özü (deməli icazə növləri də) servisdən servisə dəyişir. Əməliyyat sistemi üçün obyekt fayl, qurğu və prosesdir. Fayl və qurğular üçün adətən oxuma, yazma, yerinə yetirmə (proqram faylları üçün), bəzən də silmə və əlavə etmə hüquqlarına baxılır. Ayrıca hüquq kimi icazə səlahiyyətlərinin digər subyektlərə vermə imkanına baxıla bilər (sahiblik hüququ). Prosesləri yaratmaq və məhv etmək olar. Müasir əməliyyat sistemləri digər obyektlərin varlığını da mümkün edə bilər.

İcazə hüququna nəzarət proqram mühitinin müxtəlif komponentləri - əməliyyat sisteminin nüvəsi, əlavə təhlükəsizlik vasitələri, verilənlər bazasını idarəetmə sistemi, ara vasitəçi proqram təminatı (məsələn, tranzaksiyalar monitoru) tərəfindən həyata keçirilir.

**Protokollaşdırma və audit.** *Protokollaşdırma* dedikdə informasiya sistemində baş verən hadisələr haqqında məlumatın qeyd edilməsi və toplanması başa düşülür.

*Audit* - toplanan informasiyanın analizidir. Audit operativ (demək olar ki, real vaxtda) və ya dövri (məsələn, gündə bir dəfə) aparıla bilər.

Protokollaşdırma və auditin realizə olunması aşağıdakı məqsədləri güdür:

* istifadəçi və administratorların hesabat verməli olmasını təmin etmək;
* informasiya təhlükəsizliyini pozma cəhdlərinin aşkar olunması;
* problemlərin aşkar olunması və analizi üçün informasiyanın təqdim olunması.

“Narıncı kitabda“ protokollaşdırma üçün aşağıdakı hadisələr sadalanır: sistemə giriş cəhdləri (uğurlu və uğursuz); sistemdən çıxış; kənar sistemlərə müraciətlər; fayllarla əməliyyatlar (açmaq, bağlamaq, adını dəyişmək, silmək); imtiyazların və digər təhlükəsizlik atributlarının dəyişdirilməsi.

**Ekranlaşdırma.** Ekranlaşdırma vacib təhlükəsizlik mexanizmlərindən biridir. Bu mexanizmin *şəbəkələrarası ekran* (ingilis termini firewall) adlanan realizələri olduqca geniş yayılıb.

Ekranlaşdırma məsələsinin qoyuluşu aşağıdakından ibarətdir. Tutaq ki, iki informasiya sistemi var. Ekran − bir çoxluqdan olan istifadəçilərin digər çoxluğun serverlərinə müraciətlərini nizamlayan vasitədir. Ekran öz funksiyalarını iki sistem arasındakı bütün informasiya axınına nəzarət etməklə yerinə yetirir ( şək. 1)

İstifadəçilər

Serverlər

E

K

R

A

N

Serverlər

İstifadəçilər

**İnformasiya sistemi 1**

**İnformasiya sistemi 2**

**Şək. 1. Şəbəkələrarası ekran**

Ən sadə halda ekran iki mexanizmdən ibarətdir, onlardan biri verilənlərin yerdəyişməsini məhdudlaşdırır, digəri isə əksinə, bu yerdəyişməni həyata keçirir. Ən ümümi halda ekranı (yarımşəffaf pərdəni) süzgəclər (filtrlər) ardıcıllığı kimi təsəvvür etmək əlverişlidir. Süzgəclərdən hər biri verilənləri (tutub) saxlaya bilər, və ya onları dərhal "digər tərəfə" "ata bilər". Bundan başqa, analizi davam etdirmək üçün verilənləri növbəti süzgəcə ötürmək, adresatın adından verilənləri emal edərək nəticəni göndərənə qaytarmaq olar.

Çox vaxt ekranı 7-səviyyəli OSI etalon modelinin üçüncü (şəbəkə), dördüncü (nəqliyyat) və ya yeddinci (tətbiqi) səviyyələrində realizə edirlər. Birinci halda ekranlaşdırıcı marşrutizator, ikinci halda − ekranlaşdırıcı nəqliyyat, üçüncü halda − ekranlaşdırıcı şlüz alınır. Hər bir yanaşmanın öz üstünlükləri və nöqsanları var; hibrid ekranlara da rast gəlinir, onlarda göstərilən yanaşmaların ən yaxşı cəhətlərini realizə etməyə çalışırlar.

**Kriptoqrafiya.** Müasir kriptoqrafiyanın predmeti informasiyanı bədniyyətlinin müəyyən əməllərindən mühafizə etmək üçün istifadə edilən informasiya çevirmələridir. Kriptoqrafiya konfidensiallığı, tamlığa nəzarəti, autentifikasiyanı və müəlliflikdən imtinanın qeyri-mümkünlüyünü təmin etmək üçün tətbiq edilir.

«Kriptoqrafiya» sözü *kryptos* ('gizli') və *graphos* ('yazı') yunan sözlərindən yaranmışdır. Şifrləmə proseduru adətən müəyyən kriptoqrafik alqoritmdən və açardan istifadəni nəzərdə tutur. *Kriptoqrafik alqoritm* – məlumatların çevrilməsinin müəyyən üsuludur. *Açar* isə çevirmə üsulunu konkretləşdirir. Müasir kriptoqrafiya o prinsipdən çıxış edir ki, kriptoqrafik çevirmənin məxfiliyi yalnız açarın məxfi saxlanması ilə təmin edilməlidir.

İlk kriptosistemlər artıq bizim eranın əvvəlində meydana çıxır. Məsələn, məşhur Roma sərkərdəsi Yuli Sezar (e.ə. 100-44-cü illər) öz yazışmalarında indi onun adını daşıyan şifrdən istifadə edirdi. Müasir ingilis əlifbasına tətbiqdə bu şifr aşağıdakından ibarət idi. Adi əlifba yazılırdı, sonra onun altında həmin əlifba, lakin sola üç hərf dövri sürüşmə ilə yazılırdı:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC

Şifrləmə zamanı A hərfi D hərfi ilə, B hərfi E ilə və beləcə əvəz olunurdu. Məsələn: VENI VIDI VICI → YHQL YLGL YLFL. Şifrlənmiş məlumatı alan hərfləri ikinci sətirdə axtarırdı və onların üstündəki hərflərə görə ilkin mətni bərpa edirdi. Sezar şifrində açar əlifbanın ikinci sətrindəki sürüşmənin qiymətidir.

Şifrləmənin simmetrik və asimmetrik adlanan iki əsas üsulu var. Simmetrik şifrləmə üsulunda eyni açar (gizli saxlanılan) həm məlumatı şifrləmək, həm də deşifrləmək üçün istifadə olunur. Şəkil 2 simmetrik şifrləmənin istifadəsini illüstrasiya edir. Olduqca effektiv (sürətli və etibarlı) simmetrik şifrləmə metodları var. Simmetrik şifrləmə alqoritmlərindən DES, 3-DES, IDEA, FEAL, Skipcack, RC2, RC4, RC5, CAST, Blowfish kimi *blok şifrləri* və bir sıra *axın şifrləri* (RC4, A5) daha geniş istifadə olunur.

Simmetrik şifrləmənin əsas nöqsanı ondan ibarətdir ki, məxfi açar həm göndərənə, həm də alana məlum olmalıdır. Bu bir tərəfdən məxfi açarların tam məxfi kanalla göndərilməsi problemini yaradır. Digər tərəfdən alan tərəf şifrlənmiş və deşifrlənmiş məlumatın varlığı əsasında bu məlumatı konkret göndərəndən almasını sübut edə bilməz. Çünki belə məlumatı o özü də yarada bilər.

Şifrləmə

Deşifrləmə

Açarlar generatoru

Açar

Açar

Ortaq məxfi açar

Şifrlənmiş məlumat

Məlumat

Məlumat

**Şəkil 2. Simmetrik şifrləmə**