MÖVZU

İnformasiya t**ə**hlük**ə**sizliyi (**İ**T) anlay**ışı**.

1.Azərbaycan Respublikas**ının** milli təhlükəsizlik sistemind**ə İ**T.

2.**İ**T n**əzə**riyy**ə**sinin ümumi metodoloji prinsipl**ə**ri.

3.**İ**T-y**ə** olan t**ə**hlük**ələ**rin analizi.

4. **İ**T-nin t**ə**min edilm**ə**sinin metod v**ə** vasit**ələ**ri.

5. **İ**nformasiyanın m**ə**xfililiyinin, taml**ılığın**ın v**ə ə**lçatanl**ılığın**ın pozulması: **səbə**bl**ə**ri, növl**ə**ri, itki kanalları v**ə İ**nformasiyanın t**ə**hrifi.

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 t**ə**hlük**ə**sizliyi 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.

Cəmiyyəti mühüm məlumat və biliklərlə təmin edən informasiya eyni zamanda cəmiyyətə müəyyən ziyanlarda vura bilər. Ona görə də, informasiyanın cəmiyyətdə rolunu bilmək üçün ona iki aspektdən yanaşmaq lazımdır.

1. Mənfi-neqativ informasiyanın yayılmasının qarşısının alınması.
2. İnformasiyanın özünün qorunması.

İnformasiya və informasiya texnologiyaları hər bir ölkənin milli təhlükəsizliyinin təmin olunması üçün mühüm vasitədir. İnformasiyalaşdırma cəmiyyətdə müxtəlif neqativ halların yaranmasına səbəb oldu. Kompüter cinayətkarlığı – qeyri-qanuni informasiya mənbələrinə daxil olmaq, viruslar yaymaq, banklardan "elektron pul" oğurlamaq, parnoqrafiya, "elektron şpionluq" kimi mənfi halların sürətlə yayılmasına başladı.

Hal-hazırda düzgün, keyfiyyətli informasiyaları seçmək və yalan informasiyaların yayılmasının qarşısının alınması problemi yaranmışdır. Ona görə də, şəxsiyyətin, dövlətin təhlükəsizliyini qorumaq üçün daha mükəmməl qanunlar işlənib hazırlanmalıdır.

Təhlükə**s**izlik – şəxsiyyətin, cəmiyyətin, dövlətin daxili və xarici təhlükələrdən qorunması kimi başa düşülür.

Şəxsiyyə**t**in tə**h**lükə**s**izliyi – onun hüquq və azadlıqlarının qorunmasıdır.

Cəmiyyə**t**in tə**h**lükə**s**izliyi – onun maddi və mənəvi dəyərlərinin qorunmasıdır.

Dövlə**t**in tə**h**lükə**s**izliyi – onun konstitusion quruluşunun, suverenliyinin və ərazi bütövlüyünün qorunmasıdır.

Dövlət bu işləri, icra orqanları, məhkəmə qanunverici orqanları vasitəsi ilə hayata keçirir.

İnformasiya tə**h**lükə**s**izliyi – informasiya mühitində neqativ informasiyalardan qorunmaqla inkişafın təmin olunmasıdır. İnformasiya təhlükəsizliyi dövlətin müdafiə, ekoloji, iqtisadi təhlükəsizlik kimi formaları ilə yanaşı durur. Ona görə də, informasiya həm hüquqi həm texniki tərəfdən müdafiə olunmalıdır.

İnformasiya t**ə**hlük**ə**sizliyi – həmçinin televiziya, radio, çap, şəbəkə vasitəsi ilə cəmiyyət həyatında dövr edən neqativ informasiyalardan qorunmaqla da təmin olunmalıdır. Bunun üçün hüquqi qanun bazaları da yaradılmalıdır. Bu qanunlarda informasiyaların oğurlanması, itirilməsinin, dəyişdirilməsinin, qeyri-qanuni məhv edilməsinin, surətinin götürülməsinin qarşısının alınmasının təmin edilməsi maddələri əks olunmalıdır.

İnformasiyanın qorunması üçün müxtəlif üsullar mövcuddur. Müxtəlif xidməti qurumlar və bu informasiyaları tam məxvliyini müəyyənləşdirməklə onun təhlükəsizliyini təmin etməlidirlər.

Texniki tərəfdən informasiyanın qorunması EHM – lərin təhlükəsizliyinin qorunması, açarların (parolların) qoyulması, kriptoqrafik müdafiə vasitələri ilə həyata keçirilir. İnformasiya təhlükəsizliyi inkişaf etmiş dövlətlər tərəfindən yüksək səviyyədə həyata keçirilir. Bu isə onların informasiya müharibəsində, kommersiya məxviliklərində mühüm rol oynayır.

İnformasiya t**ə**hlük**ə**sizliyi *(en. Information Security, ru. Информационная безопасность)* - 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 mühafizəli olmasıdır.

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 İnternet şəbəkəsinin inkişafı;

* minimal təhlükəsizlik tələblərinə belə cavab verməyən proqram vasitələrinin geniş yayılması.

İnformasiyanın mühafizəsi – informasiya təhlükəsizliyinin təmin olunmasına yönəlmiş tədbirlər kompleksidir.

Təhlükə

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

Təhlükələrin əlamətləri 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.

MÖVZU

İnformasiya təhlükəsizliyinin təminatının metod və sistemləri

1. İnformasiya təhlükəsizliyi (İT) anlayışı. Azərbaycan Respublikasının milli təhlükəsizlik sistemində İT. İT-nin əsas anlayışları. İT nəzəriyyəsinin ümumi metodoloci prinsipləri. İT-yə olan təhlükələrin analizi. İT-nin təmin edilməsinin metod və vasitələri. İnformasiyanın məxfililiyinin, tamlılığının və əlçatanlılığının pozulması: səbəbləri, növləri, itki kanalları və İnformasiyanın təhrifi.
2. İnformasiya təhlükəsizliyinin hüquqi təminatı. İT-nin hüquqi bazasının əsasını təşkil edən Azərbaycan Respublikasının qanunları. İT standartları. "Narıncı kitab", Ümumi Meyarlar. İT-nin inzibati təminatı. Təhlükəsizlik siyasəti (TS). TS-nin işlənməsi üzrə standartlar. TS-nin modelləri. İnformasiya təhlükəsizliyinin təşkilati təminatı. İnformasiya təhlükəsizliyinin proqram-apparat təminatı. İnformasiya sistemlərinin mühafizəlilik sinifləri və meyarları. Mühafizə olunan sistemlərin qiymətləndirilməsi standartları.
3. İdentifikasiya və autentifikasiya. Müraciətə nəzarətin əsas anlayışları. Müraciətə nəzarətin formal modelləri: Bella-Lapadula,

Xarrison-Ruzze-Ulman, Biba. Müraciətə nəzarət vasitələri. Rollar əsasında müraciətə nəzarət. Protokollaşdırma və audit. Ekranlaşdırma.
4. İnformasiyanın mühafizəsinin kriptoqrafik metodları. Kriptoqrafiyanın əsas anlayışları. Tarixi şifrlər. Kriptoqrafik mühafizə sistemlərinin nəzəri, praktiki və zamana görə davamlılığı. Psevdotəsadüfi ardıcıllıqların alınması metodları. Müasir axın və blok şifrləmə alqoritmləri. Asimmetrik şifrləmə sistemləri, açıq açar, elektron imza. Tamlığa nəzarət. Açarların qenerasiyası və paylanması məsələləri. Kriptoqrafik mühafizənin etibarlılığının əsaslandırılması metodologiyası.
5. İnformasiyanın texniki kəşfiyyatdan mühafizəsi. İnformasiya sisteminin fəaliyyəti haqqında informasiyanın sızmasının əsas fiziki kanalları. İnformasiya sisteminin texniki kəşfiyyat üçün zəif olan qovşaq və blokları. Kənar siqnalları müasir tutma vasitələrinin texniki parametrləri. Mühəndis-texniki kəşfiyyatdan mühafizə metodları və vasitələri. Mühəndis-texniki mühafizənin keyfiyyətinin qiymətləndirilməsi metodikası.
6. Dağıdıcı proqram təsiri. Kompyuter virusları xüsusi sinif dağıdıcı proqram təsirləri kimi. Virusların təsnifatı. Virusların aşkar olunması və onlardan mühafizə metodlarv. Təcrid edilmiş proqram mühiti. Proqram məhsullarına dəyişiklik edilməsindən mühafizə və onların tamlığına nəzarət, tədqiq edilmədən mühafizə.
7. İnformasiya sistemlərinin proqram realizasiyasının mühafizə alqoritmlərinin analizi metodikası. Proqram məhsullarının mühafizəsi alqoritmlərinin bərpa edilməsi metodları. Tipik proqram məhsullarının kriptoqrafik mühafizə səviyyəsinin qiymətləndirilməsi. Açarların yaradılmasının və paylanmasının xüsusiyyətlərinin analizi. Kriptoqrafik əlfəcinlərin qoyulması imkanlarının analizi. Şəbəkə kompyuterinin uzaq məsafədən şəbəkə üzrə hücumlərdan mühafizəliliyinin ekspres analizi.
8. Şəbəkə resurslarının təhlükəsizliyi: identifikasiya və autentifikasiya vasitələri, resursların bölünməsi metodları və müraciətin məhdudlaşdırılması texnologiyası. Təhlükəsizliyin təmin olunması texnologiyaları, əsas protokollar, tətbiqi proqramların fəaliyyəti, işlənməsi və müşaiyət olunması, müxtəlif platformalarda realizəsinin xüsusiyyətləri, INTERNET şəbəkəsinin standartları. İnkişaf perspektivləri. Təhlükəsizliyin təmin olunmasının və paylanmış resursların idarə edilməsinin əsas mexanizmləri.
9. Müraciətə nəzarətin və ƏS-in resurslarının mühafizəsinin təşkili.

10. Verilənlər bazasının (VB) təhlükəsizliyinin təmin olunması vasitələri: VBİS və baza ƏS-in qarşılıqlı əlaqəsi, VB-nin ehtiyat surətlərin yaradılması və bərpası vasitələri, VB sistemlərinə uzaqdan müraciət texnologiyaları, paylanmış VB sistemlərində nüsxələmə sinxronlaşdırma. VB-nin təhlükəsizlik administratorunun məsələləri və vasitələri.

Siyasət – təşkilatın fəaliyyətinin müəyyən aspektlərini idarə etmək üçün təsbit edilmiş qaydalar məcmusudur. Siyasət biznesin məqsədlərinin, hüquqi tələblərin və ya təşkilatın korporativ normalarının təmin edilməsi üçün nə etmək lazım olduğunu müəyyən edir.

İnformasiya təhlükəsizliyi siyasətinin işlənməsi müəssisənin informasiya təhlükəsizliyi sisteminin təşkil edilməsində ilk tələblərdən biridir. İnformasiya təhlükəsizliyi siyasətinin məqsədi rəhbərliyin informasiya təhlükəsizliyi üzrə idarəçiliyini və dəstəyini biznesin tələblərinə, müvafiq qanunlara və normativlərə uyğun olaraq təmin etməkdir.

ISO 27001 standartına görə informasiya təhlükəsizliyi siyasəti daha ümumi sənədin - informasiya təhlükəsizliyinin idarə edilməsi siyasətinin altçoxluğudur. Bu siyasətlər bir sənəddə də əks oluna bilərlər.Sənədləşdirilmiş informasiya təhlükəsizliyi siyasəti rəhbərliyin münasibətini bəyan etməli və informasiya təhlükəsizliyinin idarə edilməsinə yanaşmanı müəyyən etməli, informasiya təhlükəsizliyi anlayışını, onun əsas məqsədlərini və təsir dairəsini müəyyən etməli, qiymətləndirmənin strukturu və risklərin idarə edilməsi daxil olmaqla nəzarətin məqsədlərini və mexanizmlərini müəyyən etmək üçün əsas müddəaları daxil etməlidir.İnformasiya təhlükəsizliyi siyasəti üzrə sənəd rəhbərlik tərəfindən təsdiq olunmalı, nəşr edilməli və bütün işçilərə və müvafiq xarici tərəflərə çatdırılmalıdır.

İnformasiya təhlükəsizliyi siyasəti müəyyən resursların (məsələn, vacib kompyuter sistemlərinin və verilənlərin) mühafizəsinə məqsədləri, məsuliyyəti və ümumi tələbləri təsvir edir, lakin özlüyündə təşkilatın

tələblərinin yerinə yetirilməsini təmin etməyə qabil deyil. İnformasiya təhlükəsizliyi siyasəti təhlükəsizlik mexanizmləri vəprosedurlar (reqlamentlər) kompleksinin köməyi ilə realizə olunmalıdır.

MÖVZU

İnformasiya təhlükəsizliyinin hüquqi təminatı.

1. İT-nin hüquqi bazasının əsasını təşkil edən Azərbaycan Respublikasının qanunları.

2.İT standartları. "Narıncı kitab", Ümumi Meyarlar. İT-nin inzibati təminatı.

3.Təhlükəsizlik siyasəti (TS). TS-nin işlənməsi üzrə standartlar.

4.TS-nin modelləri. İnformasiya təhlükəsizliyinin təşkilati təminatı.

5.İnformasiya təhlükəsizliyinin proqram-apparat təminatı. İnformasiya sistemlərinin mühafizəlilik sinifləri və meyarları.

6. Mühafizə olunan sistemlərin qiymətləndirilməsi standartları.

Narıncı kitab

İnformasiya təhlükəsizliyi sahəsində tarixən ilk standart ABŞ Müdafiə Nazirliyinin "Etibarlı kompyuter sistemlərinin qiymətləndirilməsi meyarları" olmuşdur. Cildinin rənginə görə çox vaxt "Narıncı kitab" adlanan bu standart ilk dəfə 1983-cü ilin avqustunda nəşr edilmişdi.

"Narıncı kitabda" etibarlı sistemi "giriş hüququnu pozmadan müxtəlif məxfilik dərəcəsinə malik informasiyanın istifadəçilər qrupu tərəfindən eyni zamanda emalını təmin etmək üçün yetərli aparat və proqram təminatı istifadə edən sistem" kimi müəyyən edir.

"Narıncı kitabda" dörd etibar səviyyəsi - D, C, B və A müəyyən edilir. D səviyyəsi qeyri-qənaətbəxş qəbul edilmiş sistemlər üçün nəzərdə tutulub. C səviyyəsindən A səviyyəsinə keçdikcə sistemlərə daha ciddi tələblər irəli sürülür. C və B səviyyələri etibar dərəcəsinin tədricən artması ilə siniflərə bölünür (C1, C2, B1, B2, B3). "Narıncı kitabda" daxil edilmiş təsnifatı qısaca belə ifadə etmək olar:

- C səviyyəsi – girişin ixtiyari idarə edilməsi;

- B səviyyəsi – girişin mandatlı idarə edilməsi;
- A səviyyəsi - təhlükəsizliyin verifikasiya edilə bilməsi.

Əlbəttə, "Narıncı kitabın" ünvanına bir sıra ciddi iradlar söyləmək olar (məsələn, paylanmış sistemlərdə meydana çıxan hadisələrin tamamilə nəzərə alınmaması). Buna baxmayaraq qeyd etmək lazımdır ki, "Narıncı kitabın" nəşri heç bir mübaliğə olmadan informasiya təhlükəsizliyi sahəsində çox böyük əhəmiyyətli hadisə oldu. Hamı tərəfindən qəbul edilən anlayışlar bazisi meydana çıxdı ki, bunlarsız informasiya təhlükəsizliyi məsələlərinin hətta müzakirəsi belə çətin olardı.

ISO/IEC 15408 standartı

Qiymətləndirmə standartlarının içərisində ən tamı və müasiri İSO/İEC 15408 "İnformasiya texnologiyalarının təhlükəsizliyini qiymətləndirmə meyarları" standartıdır (1 dekabr 1999-cu ildə nəşr olunmuşdur). Bu beynəlxalq standart bir neçə ölkə mütəxəssisinin demək olar ki, onillik işinin nəticəsidir, o özündə həmin dövrə mövcud olan beynəlxalq və milli standartların təcrübəsini cəmləşdirmişdir.

Tarixi səbəblərdən bu standartı çox zaman "Ümumi meyarlar" adlandırırlar. Biz də bu qisaltmadan istifadə edəcəyik.

"Ümumi Meyarlar" əslində informasiya sistemlərinin təhlükəsizliyini qiymətləndirmə alətlərini və onların istifadə qaydalarını müəyyən edən metastandartdır. "Narıncı kitabdan" fərqli olaraq Ümumi Meyarlarda əvvəlcədən müəyyən edilmiş " təhlükəsizlik sinifləri" yoxdur. Belə sinifləri konkret təşkilat və/və ya konkret informasiya sistemi üçün mövcud olan təhlükəsizlik tələblərindən çıxış edərək qurmaq olar.

"Narıncı kitab"dakı kimi Ümumi meyarlarda da təhlükəsizlik tələblərinin iki əsas növü var:

- **funksional tələblər** – mühafizənin aktiv aspektinə uyğundur, təhlükəsizlik funksiyalarına və onları realizə edən mexanizmlərə irəli sürülür;
- **zəmanət tələbləri** – mühafizənin passiv aspektinə uyğundur, yaradılma və istismar texnologiyasına və prosesinə irəli sürülür.

Təhlükəsizlik tələbləri irəli sürülür, onların yerinə yetirilməsi isə müəyyən qiymətləndirmə obyekti üçün - aparat-proqram məhsulu üçün və ya informasiya sistemi üçün yoxlanır.

Funksional tələblər

Funksional tələblərin ingilis dilində ixtisarlarla işarə edirlən aşağıdakı sinifləri müəyyən edilir.

Təhlükəsizliyin auditi (FAU). Təhlükəsizlik sisteminin auditi – təhlükəsizlik sisteminə aid informasiyanın tanınması, qeydə alınması, saxlanması və analizidir.

Kommunikasiya (FCO). Bu sinfin tələblərinin yerinə yetirilməsi zəmanət verir ki, informasiyanı göndərən ötürülən informasiyadan, qəbuledən isə onu aldığından imtina edə bilməz.

Kriptoqrafik dəstək (FCS). Sinifdə kriptoqrafik açarların və əməliyyatların idarə edilməsi üzrə tələblər var.

İstifadəçinin verilənlərinin mühafizəsi (FDP). Sinif informasiyanı daxiletmə, xaricetmə və saxlama zamanı istifadəçi verilənlərinin mühafizəsinə aid təhlükəsizlik tələblərini müəyyən edir.

İdentifikasiya və autentifikasiya (FIA). Bu sinfin tələbləri sistemdə istifadəçilərin müəyyən edilməsi və verifikasiyası ilə, onların sistemdə səlahiyyətləri ilə, həmçinin təhlükəsizlik atributlarının hər bir istifadəçiyə düzgün verilməsi ilə işləyir.

Təhlükəsizliyin idarə edilməsi (FMT). Sinfə təhlükəsizlik funksiyaları verilənlərinin və atributlarının, həmçinin təhlükəsizlik rollarının idarə edilməsi üzrə tələblər daxildir.

Konfidensiallıq (**FPR**). Bu sinfin tələblərinin realizə edilməsi istifadəçini onun səlahiyyətlərinin digər istifadəçilər tərəfindən açılmasından və sui-istifadə edilməsindən mühafizə edəcək.

Təhlükəsizlik funksiyalarının mühafizəsi (**FPT**). Sinfə sistemin təhlükəsizlik mexanizmlərinin tamlığına və idarə edilməsinə aid funksional tələblər daxildir (realizə edilən təhlükəsizlik siyasətindən asılı olmayaraq).

Resursların istifadəsi (FRU). Bu sinfin tələbləri lazımi resursların əlyetənliyini (emal və/və ya saxlama imkanı kimi), həmçinin sistemin imtinaları ilə funksional imkanların meydana çıxan bloklanması halında mühafizəni təmin edir.

Qiymətləndirmə obyektinə giriş (FTA). Sinif istifadəçinin təyin edilmiş iş seansına funksional nəzarət tələblərini identifikasiya və autentifikasiya üzrə tələblərdən asılı olmadan müəyyən edir.

Etibarlı marşrut/kanal (FTP). Sinif aşağıdakı tələbləri təmin edir:

- Istifadəçi ilə sistemin təhlükəsizlik funksiyaları arasında etibarlı kommunikasiya marşrutu;
- sistemin təhlükəsizlik funksiyaları arasında etibarlı rabitə kanalı.

Zəmanət tələbləri

Standart ingilis dilində ixtisarlarla adlandırılmış aşağıdakı zəmanət siniflərini daxil edir:

Konfiqurasiyanın idarə edilməsi (ACM). Ümumi Meyarlar qiymətləndirilən obyektin tamlığının saxlanmasını onun dəqiqləşdirilməsi və modifikasiyası zamanı idarəetmə və intizam tələb etməklə təmin edir.

Çatdırılma və istismar (ADO). ADO zəmanət sinfi qiymətləndirilən obyektin etibarlı çatdırılması, qurulması və istismar istifadəsinə aid tədbirlərə, prosedurlara və standartlara tələbləri müəyyən edir.

Yaratma (ADV). Bu zəmanət sinfi qiymətləndirilən obyektin ümumi spesifikasiyasından təhlükəsizlik funksiyalarının faktiki realizəyə yuxarıdan aşağıya addım-addım dəqiqləşdirilməsi üzrə tələbləri müəyyən edir.

Rəhbər sənədlər (AGD). Bu zəmanət sinfi istehsalçının təqdim etdiyi istismar sənədlərinin anlaşıqlıq və tamlıq tələblərini müəyyən edir.

Həyat dövrünün dəstəklənməsi (ALC). Bu sinif qiymətləndirilən obyektin yaradılmasının bütün addımları üçün həyat dövrü modelini, o cümlədən qüsurların aradan qaldırılması prosedurlarını və siyasətini dəqiq müəyyən edir.

Testlər (ATE). Bu zəmanət sinfi təhlükəsizlik funksiyalarının funksional təhlükəsizlik tələblərini ödədiyini nümayiş etdirən sınaqlara tələbləri müəyyən edir.

Boşluqların qiymətləndirilməsi (AVA). Bu zəmanət sinfi istismar zamanı qalan zəif yerlərin identifikasiyasına yönəlmiş tələbləri müəyyən edir.

ISO/IEC 27002 standartı

Hazırda informasiya təhlükəsizliyi sahəsində ən məşhur standartlar ISO/IEC 2700x standartlar seriyasıdır.

Standartlar seriyasının **tarixi** belə başlamışdır. Britaniya Standartlar İnstitutu (BSI) tərəfindən işlənilmiş və fəaliyyət dairəsindən asılı olmayaraq şirkətlərin informasiya təhlükəsizliyinin idarə edilməsi üçün 1998-ci ildə BS 7799 milli standartı qəbul edilmişdi. Britaniya standartı BS 7799 dünyanın 27 ölkəsində, o cümlədən Britaniya Birliyi ölkələrində dəstəklənirdi.

2000-ci ilin sonunda ISO (Beynəlxalq Standartlaşdırma Təşkilatı) Britaniya standartı BS 7799 əsasında ISO/IEC 17799 «Information technology − Information security management» («İnformasiya texnologiyaları − İnformasiya təhlükəsizliyinin idarə edilməsi») beynəlxalq standartını işlədi və qəbul etdi.

2005-ci ildə standartın 2000-ci il redaksiyası ilə müqayisədə yenidən əhəmiyyətli işlənmiş ISO 17799:2005 variantı çıxdı. 2005-ci ildə həmçinin BS 7799 standartının ikinci hissəsi ISO 27001 standartı kimi qəbul edildi. ISO 27001 standartı informasiya təhlükəsizliyi sistemlərinin sertifikastlaşdırılması üçün nəzərdə tutulub.

ISO/IEC 17799:2005 standartı 2007-ci ildən ISO/IEC 27002 adını alıb. Bu standartda informasiya təhlükəsizliyini idarəetmə sisteminin elementləri on bir qrup üzrə bölünüb:

1) Təhlükəsizlik siyasəti – təşkilatın rəhbərliyi tərəfindən informasiya təhlükəsizliyi sahəsində siyasətin dəstəklənməsi;

2) İnformasiya təhlükəsizliyinin təşkili – təşkilatda informasiya təhlükəsizliyi sisteminin iş qabiliyyətini təmin edəcək təşkilati strukturun yadradılması;

3) Resursların idarə edilməsi – informasiya resurslarına onların dəyər dərəcələrinə görə prioritet verilməsi və onlara görə məsuluyyətin paylanması;

4) Əməkdaşların təhlükəsizliyi – insan səhvləri riskinin, oğurluğun və avadanlığın qeyri-düzgün istifadəsinin azaldılması (əməkdaşların təlimi və insidentlərin izlənməsi);

5) Fiziki təhlükəsizlik – avtorizə olunmamış girişin və təşkilatın informasiya sisteminin işinin pozulmasının qarşısının alınması;

6) Kommunikasiyanın və əməliyyatların idarə edilməsi – şəbəkələrin və kompyuterlərin təhlükəsiz fəaliyyətinin təmin edilməsi;

7) Girişin idarə edilməsi – biznes-informasiyaya girişin idarə edilməsi;

8) Sistemin alınması, yaradılması və sistemə xidmət edilməsi – təşkilatın informasiya sisteminin yaradılması və ya inkişafı zamanı informasiya təhlükəsizliyi tələblərinin yerinə yetirilməsi, tətbiqi proqramların və verilənlərin təhlükəsizliyinin dəstəklənməsi;

9) İnformasiya təhlükəsizliyi insidentlərinin idarə edilməsi;

10) Təşkilatın fasiləsiz fəaliyyətinin idarə edilməasi – fövqəladə hallarda təşkilatın fasiləsiz işinin təmin edilməsi üçün fəaliyyət planı;

11) Qanunvericiliyin tələblərinə uyğunluq – müvafiq mülki və cinayət qanunvericiliyinin, müəllif hüquqları və informasiyanın mühafizəsi qanunları daxil olmaqla, tələblərinin yerinə yetirilməsi.

MÖVZU

TƏHLÜKƏSİZLİK SİYASƏTİ

İnformasiya və kommunikasiya texnologiyalarının sürətli inkişafı, geniş yayılması və rəqabətin kəskinləşməsi elmi-metodoloji prinsiplərinə əsaslanan informasiya təhlükəsizliyinin təmin edilməsinin, həmçinin şəbəkə texnologiyalarının müasir inkişaf meyllərinin nəzərdə tutulduğu hüquqi, təşkilati, texniki və fiziki mühafizə tədbirlərini qarşılıqlı surətdə əlaqələndirməklə korporativ şəbəkələrdə vahid informasiya təhlükəsizliyi sisteminin yaradılmasını zəruri edir.

İnformasiya təhlükəsizliyinin təmin edilməsi dedikdə informasiyanın konfidensiallığının, tamlığının və əlyetərliyinin təmin edilməsi başa düşülür. İnformasiyanın konfidensiallığı informasiyaya çıxış yalnız icazə verilmiş şəxslərə verildikdə, tamlıq – verilənlərə razılaşdırılmış dəyişikliklər edildikdə, əlyetərlik – icazə verilmiş şəxslərin lazımi vaxtda informasiya resurslarına çıxış əldə etdikləri halda təmin edilir.

Bu mənada informasiya təhlükəsizliyi siyasəti (Siyasət) - AMEA korporativ şəbəkəsində informasiya təhlükəsizliyinin təmin edilməsi probleminə nəzarət sistemini müəyyən edir, informasiya mühafizəsinin məqsəd və vəzifələrini, təşkilati, texnoloji və prosedur aspektlərini sistemləşdirilmiş şəkildə şərh edir.

2. Siyasətin məqsəd və vəzifələri

Məqsəd

- informasiya təhlükəsizliyinə təhdidlərin AMEA-nın şəbəkə və informasiya resurslarına vura biləcəyi maddi və mənəvi ziyanın minimuma endirilməsi;
- AMEA-nın işgüzar nüfuzunun yüksəldilməsi;
- informasiya təhlükəsizliyi sisteminin qurulması üçün vahid prinsiplərin formalaşdırılması;
- informasiya təhlükəsizliyi sisteminin yaradılması, fəaliyyəti və inkişafı üçün müvafiq təşkilati-metodiki bazanın formalaşdırılması.

İnformasiya təhlükəsizliyi sisteminin yaradılması zamanı həlli vacib olan məsələlər:

- AMEA korporativ şəbəkəsində informasiya təhlükəsizliyinə potensial təhdidlərin siyahısının müəyyənləşdirilməsi və analizi;
- AMEA korporativ şəbəkəsində informasiya resurslarının təsnifatı;
- AMEA korporativ şəbəkəsində tətbiq edilən informasiya texnologiyalarına informasiya təhlükəsizliyi baxımından irəli sürülən vahid tələblərin müəyyənləşdirilməsi;
- İnformasiya təhlükəsizliyi sisteminə dair tələblərin formalaşdırılması.

Təsir dairəsi

Bu Siyasət AMEA-nın Rəyasət Heyətinə və bütün təşkilatlarına məxsus olan informasiya resurslarına, sistemlərinə və şəbəkələrinə, tətbiqi proqramlara hər hansı formada çıxışı olan bütün AMEA əməkdaşlarına şamil edilir.

4. İnformasiya təhlükəsizliyi üzrə məsuliyyət

4.1. Bütün əməkdaşların və bağlanmış müqavilələr çərçivəsində AMEA korporativ şəbəkəsindən istifadə edən şəxslərin Siyasətin tələblərinə əməl etməsi məcburidir.

4.2. İnformasiya təhlükəsizliyi üzrə əsas məsuliyyət təşkilat(lar)ın rəhbər(lər)inin üzərinə düşür, informasiya təhlükəsizliyi üzrə rəsmən təyin edilmiş şəxsdə bilavasitə bu Siyasətin və onunla əlaqəli prosedurların reallaşdırılmasına və idarə edilməsinə görə məsuliyyət daşıyır.

4.3. Təşkilatın struktur bölmə rəhbərləri daimi və müvəqqəti işçilərin aşağıdakılardan məlumatlı olmasının təmin edilməsinə görə cavabdehdirlər:

- onların fəaliyyət sahələrində tətbiq edilə bilən informasiya təhlükəsizliyi siyasətləri;
- informasiya təhlükəsizliyi üzrə əməkdaşların şəxsi məsuliyyəti;

- informasiya təhlükəsizliyi məsələləri üzrə məsləhət üçün müraciət qaydaları.

4.4. Bütün əməkdaşlar verilənlərin konfidensiallığının və tamlığının təmin edilməsi də daxil olmaqla informasiya təhlükəsizliyi prosedurlarını yerinə yetirməlidir. Əks halda, intizam tədbirləri görülə bilər.
4.5. Təşkilatın struktur bölmə rəhbərləri öz sahələrində informasiyanın saxlandığı və ya emal edildiyi mühitin fiziki təhlükəsizliyi üzrə fərdi məsuliyyət daşıyırlar.
4.6. Hər bir əməkdaş istifadə etdiyi informasiya sistemlərinin təhlükəsiz istismarı üçün məsuliyyət daşıyır.
4.7. Sistemin hər bir istifadəçisi müvafiq Siyasətlə müəyyən edilən təhlükəsizlik tələblərini yerinə yetirməlidir, həmçinin istifadə etdiyi informasiyanın konfidensiallığının, tamlığının və əlyetərliyinin yüksək səviyyədə qorunmasını təmin etməlidir.
4.8. Təşkilatın informasiya sisteminə kənar istifadəçilərin daxil olmasına icazə verən müqavilələr öncədən qüvvəyə minməlidir. Bu müqavilələr müvafiq təhlükəsizlik siyasətinin yerinə yetirilməsinə zəmanət verməlidir.

MÖVZU

İdentifikasiya və autentifikasiya.

1.Müraciətə nəzarətin əsas anlayışları.

2.Müraciətə nəzarətin formal modelləri: Bella-Lapadula, Xarrison-Ruzze-Ulman, Biba.

3.Müraciətə nəzarət vasitələri. Rollar əsasında müraciətə nəzarət.

4. Protokollaşdırma və audit. Ekranlaşdırma.

Biz ‘‘informasiya’’ sözünü tez-tez işlədirik. İnformasiya latın sözü olub məlumat, xəbər deməkdir. Abstrakt anlayış, hara çatdırılmasından asılı olmayaraq çoxşaxəli məlumat deməkdir. Bizim hər bir hərəkətimiz gördüyümüz iş informasiya ilə bağlıdır. İnformasiyanın hər hansı şəkildə təhlili onun üzərində iş aparılması informasiyanın emalı və ya işlədilməsi adlanır. İnsan informasiyanı iki yolla - ətraf aləmdən duyğu üzvləri vasitəsilə və beyin fəaliyyətinin nəticəsi kimi əqli mühakimələr əsasında alır. İnsanın təkamül mərhələsini informasiyanın əldə olunması emalı və ötürülməsi üsul və vasitələrinin inkişafı ilə müəyyən olunur. İnsanın ilk

məskənlərindən olan Qobustan qayalarındakı təsvirlər tariximizin öyrənilməsində çox dəyərli informasiya vermişdir. Daha sonra insan öz fikir və düşüncələrini də mücərrəd qrafik təsvirlərlə verməyi öyrəndi. Bu isə əslində informasiyanın yazılı ötrülməsi yadda saxlanılması demək idi. Yazının meydana gəlməsi bəşər mədəniyyəti tarixində ilk informasiya sıçrayışı oldu. Sonralar kağızın icad olunması informasiyanın daha da sürətlə yayılmasına səbəb oldu. İnformasiyanın toplandığı saxlandığı kitablar arxivlər yarandı. Kitabın meydana gəlməsi ikinci informasiya sıçrayışı oldu. Kitab informasiyanin daha geniş və sürətlə yayılmasına imkan verdi. Tarix boyu əldə olunmuş biliklərin həcmi getdikcə artır. Son onilliklərdə elmin texnikanın coşqun inkişafı nəticəsində bu artım daha çox nəzərə çarpır. Bu qədər informasiyanın saxlanılması üçün kitablar kifayət etmir. Digər tərəfdən bir çox hallarda böyük həcimdə informasiyanın təhlili emalı tələb olunur ki, bunu da yalnız kitablardan istifadə etməklə həyata keçirmək demək olar ki, qeyri-mümkündür. İnformasiyanın emalı və saxlanılmasında yeni dövr komputerlərlə bağlıdır. Kompüterlərin yaranması bəşər təfəkkürünün ən böyük nəaliyyətlərindən biridir. Bunu deyək ki, hazırda informatika və hesablama texnikası bölmələrini bu bölmələr arasındakı bağlılıqları ehtiva edən daha geniş bir anlayış- informasiya texnologiyası anlayışı da işlədilir.Təbiətdə və cəmiyyətdə bizi əhatə edən obyektlər, hadisələr, onların xassələri, qarşılıqlı münasibətləri haqqında məlumatlar yığımı olub, onlara dair bilikləri çoxaltmaq məqsədi daşıyır.İnformasiya təbiətdə siqnallar şəklində ötürülür və iki tipə ayrılır: analoq və rəqəmli. İnsanlar öz hissiyyat üzvlərinə görə analoq, kompyuterlər isə rəqəmli informasiyaların

köməyilə fəaliyyət göstərir. İnformasiyanın istifadəyə yararlı olması üçün aşağıdakı şərtlər ödənilməlidir. İnformasiyanın xüsusiyyətləri:

- tam (tam şəkildə təsvir olunmalıdır);
- düzgün (həqiqi situasiyanı əks etdirməlidir);
- qiymətli (maksimum az məsrəflə əldə edilməlidir)
- əhəmiyyətli (istifadəçi üçün vacib olmalıdır);
- aktual (cari vaxtda tələb edilən olmalıdır);
- anlamlı (istifadəçinin başa düşdüyü tərzdə hazırlanmalıdır).

İnformasiya hal-hazırkı və potensial sahibinə hər hansı sahədə (maddi, siyasi, hərbi) mənfəət gətirirsə, bu informasiya qiymətli informasiya sayılır. İnformasiyanın qorunması, informasiyanın itirilməsi, dəyişdirilməsi, silinməsi ehtimallarının qarşısını alır. İnformasiyalar yaranmasına, qəbul edilməsinə, ötürülməsinə, ifadə formalarına və vasitələrinə, istifadəsinə və s. görə müxtəlif cür qruplaşdırıla bilər. İnformasiyaları hər hansı əlifba simvollarının köməyi ilə ifadə etmək və onu digər əlifbaya da keçirmək olar. İnformatikada fakt, məlumat, xəbər terminləri çox vaxt “verilənlər” sözü ilə ifadə olunur. İnformasiyanın mühafizəsi, informasiya təhlükəsizliyi" - informasiyanın toplanması, saxlanması, yenidən işlənməsi, ötürülməsi və yayılması prosesində, həmçinin siyasi, sosial-iqtisadi, müdafiə, mədəni və digər fəaliyyət sahələri obyektlərinin informasiya təhlükəsizliyinin xarici və daxili oğurluq, informasiyanın dağıdılması və/və ya modifikasiyası təhlükəsindən qorunmasının təminində informasiyanın işlənib hazırlanması, təkmilləşdirilməsi və müxtəlif üsulların və müdafiə vasitələrinin tətbiqi problemləri ilə məşğul olan

ixtisasdır. Xalq təsərrüfatı üçün elmi və texniki problemlərinin həllində bu ixtisasın yeni informasiyaların işlənib hazırlanmasında, informasiyanın mövcud mühafizə üsulları və vasitələrinin təkmilləşdirilməsində və informasiya təhlükəsizliyinin təmin olunmasında əhəmiyyəti böyükdür

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.

İcaz**ələ**rin idar**ə** edilm**ə**si. 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 mantiqi 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.

Protokolla**şdı**rma v**ə** 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.

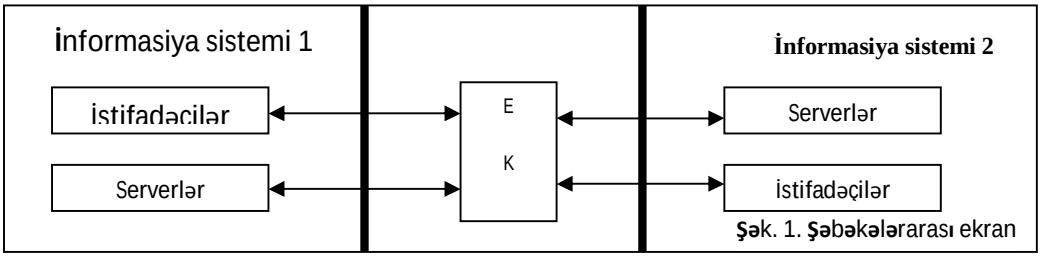
Protokollaşdırma və auditin realizə olunması aşağıdakı məqsədləri güdür:

– 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.

Ekranla**şdı**rma. 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)



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.

Barmaq izlərinə görə identifikasiya.

Barmaq izlərini oxuyan optik skaynerlər noutbukda komputerin siçanında klavyaturada fləş-diskdə quraşdırılır həmçinin ayrıca xarici qurğular və terminallar şəklində tətbiq olunur. Daranmış barmaq izinin naxışı informasiyadan istifadəyə icazəsi olan şəxslərin heç birinin barmaq izlərinin naxışı ilə üst-üstə düşmədikdə informasiya irişilməz olur.

Gözün quzeyli qişasının şəklinə görə identifikasiya.

Gözün quzeyli qişasını hər bir insanın nadir biometrik xüsusiyyətləndirir. O insanda yaşyarımlıqdan formalaşır və əslində bütün ömrü boyu dəyişməz qalır. Gözün təsviri alındıqdan sonra onun üzərinə xüsusi ştrix-kod maskası qoyulur. Nəticədə hər bir insan üçün fərdi matris alınır. Gözün qüzeyli qişasına görə identifikasiya etmək üçün xüsusi skaynerlərdən istifadə olunur.

Nitqin özəlliklərinə görə identifikasiyası.

İnsanın səsə görə identifikasiyası ənənəvi tanınma üsullarından biridir. Telefondakı həmsöhbəti görmədən onu asanlıqla tanımaq olur. Hətta səsinin emosional tonuna görə insanın psixoloji durumunu müəyyənləşdirmək mümkündür. Səsə görə idetifikasiya nitqin tezlik analizinə əsaslanır. Hər bir insan üçün hər bir səsin fərdi tezlik xarakteristikası vardır.

Üzün təsvirinə görə identifikasiya.

Şəxsiyyəti müəyyənləşdirmək üçün üzə görə tanıma texnologiyasından tez-tez istifadə olunur. Bu üsul insanı narahat etmir çünki onun tanınması məsafədən aparılır. İdentifikasiya əlamətləri üzün formasını rəngini həmçinin saçın rəngini nəzərə alır. Mühüm əlamətlər sırasına sifətdə kontrastlığın dəyişdiyi yerlərin koordinatlarını da aid etmək olar. Hazırda yeni xarici pasportların verilməsinə başlanır ki, onlardakı mikrosxemlərdə pasport sahibinin rəqəmli fotoşəkil saxlanılır.

Ovucun cizgilərinə görə identifikasiya.

Biometrikada identifikasiya məqsədilə əlin ölçülərindən və formasından eləcə də əlin üstündə barmaq sümüklərinin qatlanma yerlərindən qan damarlarının yerləşməsindən əmələ gələn naxışlardan və s. istifadə olunur. Ovuca görə identifikasiya skatnerləri bəzi aeroportlarda banklarda atom elektrik stansiyalarında quraşdırılır.

Bütün ciddi tədbirlər kimi informasiyanın mühafizəsidə kompleks şəkildə həyata keçirilməlidir yəni yaxşı nəticələr əldə etmək üçün bütün mühafizə üsulları birləşdirilməlidir.

İnformasiyanın kompleks mühafizəsi sisteminə aşağıdakılar daxildir:

-təşkilati mühafizə yəni müzakirələrdən tutmuş planların hazirlanmasına və informasiyanın qorunması üzrə qurumların yaradılmasına qədər xüsusi tədbirlər;

-proqram-aparat mühafizəsi yəni kompüter sistemləri və xüsusi proqramların quraşdırılması;

-mühəndis texniki mühafizə (video-müşahidə kameraları kənar şəxslərin məxfi otaqlara girişini məhdudlaşdıran intelektual qıfıllar və s.);

-qanunverici mühafizə;

Kütləvi komputerləşmə ən yeni informasiya texnologiyalarının inkişafı və tətbiqi təhsil, biznes, sənaye, istehsal və elmi tedqiqatlar sahəsində irəliyə doğru hiss olunan sıçrayışa gətirib çıxarmış və elmi-texniki inkişaf müasir informasiya cəmiyətinin yaranmasına səbəb olmuşdur.Bu cəmiyyətdə informasiya ən mühum resurs və başlıca amildir. 21-ci əsrdə vətəndaşların, cəmiyyətin və dövlətin həyatında informasiyanın, informasiya resurslarının ve texnologiyalarının rolunun artması milli təhlükəsizliyin təmin olunması sistemində informasiya təhlükəsizliyi məsələrinin önə çıxarır.

İnformasiyanın təhlükəsizliyinin təmin olunması probleminin vacibliyi və aktuallığı aşağıdakı səbəblərdən yaranmışdır. Müasir komputerlərin hesablama surətinin kəskin artması və bununla eyni zamanda onların istismarının sadələşdirilməsi . Kompüterlərin köməyi ilə qəbul edilən, saxlanılan və emal edilən informasiyanın kəskin artması. Hesablama resurslarına və verilənlər massivinə girişi olan istifadəçilər sayının kəskin artması. Minimal təhlükəsizlik tələblərinə cavab verməyən proqram vasitələrinin inkişafı. Şəbəkə

texnologiyalarının bütün sahələrdə yayılmasi və lokal şəbəkələrin qlobal şəbəkələr halında birləşməsi. İnformasiya emalı sisteminin pozulmasına praktiki olaraq mane olmayan internet şəbəkələrinin inkişafı.

İnformasiyanin təhlükəsizliyi dedikdə informasiyaya və ona xidmət edən istifadəçilərə ziyan vurmağa səbəb olan təbii və ya süni xarakterli təsadüfi və ya qəsidli təsirlərdən informasiyanin və ya ona xidmət edən infrastukturun mühafizə olunması nəzərdə tutulur.

olunmasına yönəlmiş tədbirlər kompleksidir. Praktiki olaraq bu informasiyanın və ya verilənlərin daxil edilməsi saxlanılması və ötrülməsi üçün istifadə edilən resursların tamlığının müxtəlifliyinin təmin edilməsi deməkdir.

İnformasiyanin mühafizəsinin əsas məqsədi istehlakçıya aid olan informasiyanın tamlığının əlyetməzliyinin təmin edilməsi və məxfiliyinin pozulması səbəbindən itkilərin minimuma endirilməsidir.

MÖVZU

Azərbaycanda informasiyanın qorunması haqqında qanunlar.

Qeyd olunduğu kimi Azərbaycanda informasiyanın mühafizəsi xüsusi qanunlarla tənzimlənir. Həmin qanun görə informasiyanın mühafizəsinin başlıca məqsədləri bunlardır.

-informasiyanın məhvinin itməsinin saxtalaşdırılmasının qarşısının alınması;

-dövlətin ictimaiyyətin vətəndaşların təhlükəsizliyinin qarşısının alınması;

-informasiyanın məhvi modifikasiyası surətinin çıxarılması təcrid edilməsi ilə bağlı sanksiyalaşdırılmamış hərəkətlərin qarşısının alınması;

-dövlət sirri olan və konfidensial informasiyanın məxfiliyinin qorunması;

-informasiya proseslərində və informasiya sistemlərinin texnologiyalarının və onların təminat verilməsinin işlənməsi istehsalı tətbiqi zamanı fiziki və hüquqi şəxslərin hüquqlarının təmin olunması;

Azərbaycanda müəlliflik hüququ Azərbaycan Respublikasının ‘‘Müəlliflik hüququ və əlaqəli hüquqlar haqqında’’ 8 noyabr 1996-cı il tarixli qanunu ilə tənzimlənir.

Azərbaycan Respublikasının ‘‘Elektron imza və elektron sənəd haqqında’’ Qanunu 2004-cü il martın 9-dan qüvvədədir. Bu qanunda elektron imza anlayışı belə təyin olunur:

Elektron imza – digər verilənlərə əlavə edilən və ya onlarla məntiqi əlaqəli olan imza sahibini identikləşməyə imkan verən verilənlər.

MÖVZU

İnformasiya t**ə**hlük**ə**sizliyinin konseptual modeli.

İnformasiya təhlükəsizliyinə qarşı yönələn təhlükələri bu təhlükələrin mənbəyini onlarin realizə üsullarını və məqsədlərini həmçinin onun təhlükəsizliyini pozan digər hal və hərəkətləri müəyyən etmək lazimdir. Bu zaman təbii olaraq ziyan vurmağa səbəb ola bilən qeyri-qanuni hərəkətlərdən informasiyanın mühafizəsi tədbirlərinin də nəzərdən keçirilməsi vacibdir.

Praktika göstərir ki, çoxlu sayda olan belə mənmələrin obyekt və hərəkətlərin analizi üçün modelləşdirmə metodlarindan istifadə etmək məqsədəuyğundur. İlkin yanaşmada informasiya təhlükəsizliyinin konseptual modelinin asağıdakı komponentlərini təklif etmək olar.

-təhlükənin obyekti

-təhlükələr

-təhlükələrin mənbəyi-bədniyyətli tərəfindən təhlükələrin məqsədləri.

-informasiya mənbələri

-məxfi informasiyanın qeyri-qanuni əldə etmək üsulları

-informasiyanin mühafizə üsulları

-informasiyanın mühafizə vasitələri

MÖVZU

İnformasiya t**ə**hlük**ə**sizliyin**ə** qar**şı** yön**ə**l**ə**n t**ə**hlük**ə**l**ə**r.

Təhlükə dedikdə sistemdə dağılma verilənlərin aşkarlanması və ya dəyişdirilməsi xidmətdən imtina formasinda ziyan vurulmasina səbəb ola bilən istənilən hal və hadisələr nəzərdə tutulur.

Təhlükələri müxtəlif siniflərə bölmək olar. Yaranma səbəblərinə görə təhlükələri təbii və süni xarakterli təhlükələrə ayırmaq olar. Süni xarakterli təhlükələr öz növbəsində bilməyərəkdən və qəsdən törədilən təhlükələrə bölünürlər. Təsir məqsədinə görə təhlükələrin üç əsas növü ayırd edilir.

-informasiyanın məxfiliyinin pozulmasına yönələn təhlükələr.

-informasiyanın tamlığının pozulmsına yönələn təhlükələr.

-sistemin iş qabilyətinin (xidmətdən imtina) pozulmasına yönələn təhlükələr.

Məxfiliyin pozulmasına yönələn təhlükələr məxfi və ya gizli informasiyanın məzmunun açılmasına yönəlir. Belə təhlükələrin reallaşması halında informasiya ondan istifadəsinə icazəsi olmayan şəxslərə məlum olur.

Kompüter sistemində saxlanan və ya rabitə kanalı ilə ötürülən informasiyanın tamlığının pozulmasına yönələn təhlükələr onun dəyişdirilməsinə və ya təhrifinə yönəlir ki, bunlar da onun keyfiyyətinin itməsinə və tam məhvinə səbəb ola bilər. Bu təhlükə informasiyanın ötrülməsi sistemləri komputer şəbəkələri və telekomunikasiya sistemləri üçün xüsusilə aktualdır.

İş qabilyətinin pozulmasina xidmətdən imtina yönələn təhlükələr elə situasiyyalarin yaranmasina yönəlir ki, bu zaman müəyyən qəsdli hərəkətlər ya sistemin iş qabilyətini aşağı salır ya da sistemin müəyyən resurslarına girişi bağlayır.

Bundan əlavə təhlükələr digər əlamətlərinə görə də təsnif oluna bilər.

-vurulmuş ziyanın kəmiyyətinə görə

-baş vermə ehtimalına görə- (müflis, ahamiyyətli, cüzi)

-meydana çıxma səbəblərinə görə-(təbii fəlakətlər, qəsdli hərəkətlər)

- vurulmuş ziyanin xarakterinə görə-(maddi, mənəvi)

-təsir xarakterinə görə-(aktiv, passiv)

-obyektə mənsubiyyətinə görə-(daxili, xarici)

Daxili və xarici təhlükələrin nisbətini təqribi olaraq belə xarakterizə etmək olar

-təhlükələrin 80%faizi təşkilatın öz işçiləri tərəfindən onların bilavasitə və ya dolayısı yolla iştirakı ilə baş verir.

-təhlükələrin 20% kənardan icra olunur.

Kompüter şəbəkələrinin uğradığı təhlükələr üzərində xüsusi dayanmaq lazımdır. İstənilən kompüter şəbəkəsinin əsas xüsusiyyəti kompüterlərin ərazidə paylanmasıdır. Şəbəkələrin qovşaqları arasındakı

əlaqələr fiziki olaraq şəbəkə xətləri vasitəsilə proqram yoluu ilə məlumatlar mexanizmi ilə həyata keçrilir. Bu zaman şəbəkənin qovşaqları arasında ötrülən idarəedici məlumatlar və verilənlər mübadilə paketləri şəklində ötrülür. Kompüter şəbəkələri onunla xarakterikddir ki onlara qarşı uzaq məsafədən hücumlara təşəbüslər edilir. Bu zaman nəinki konkret kompüter həmçinin şəbəkə kanalları ilə ötrülən informasiya da hücuma məruz qala bilər.

MÖVZU

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 bütövlüyünün 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.

- Bütövlük - informasiyanın təhrifsiz şəkildə mövcudolma xassəsidir. İnformasiyanın bütövlüyünün pozulmasına yönələn təhlükələr onun dəyişdirilməsinə və ya təhrifinə yönəlib ki, bunlar da onun keyfiyyətinin pozulmasına və tam məhvinə səbəb ola bilər. İnformasiyanın bütövlüyü 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).
- Lokal kompüter şəbəkələri (LKŞ)-nin əsas aparat komponentləri kimi aşağıdakılardan istifadə edilir:
- İşçi stansiyalar;
- Serverlər;
- İnterfeys plataları;
- Kabellər.
- İşçi stansiyalar (İST) – şəbəkə istifadəçisinin iş yeri kimi istifadə olunan
- fərdi kompüterlərdir. İST – nin tərkibinə olan tələbat şəbəkədə həll olunan məsələlərin xarakteriskaları, hesablama proseslərinin təşkil olunma prinsipi, istifadə olunan ƏS və bir sıra digər amillərlə təyin olunur. Məsələn, əgər şəbəkədə MS Windows for Workgroup ƏS – dən istifadə edilirsə, o zaman İST – nin prosessoru kimi Pentium tipli prosessorlardan istifadə etmək lazımdır.

- Bəzi hallarda İST birbaşa şəbəkə kabelinə qoşulmuş olursa, bu halda
- maqnit disklərində yaddaşa ehtiyac qalmır.Bu cür İST disksiz İST adlanırlar. Lakin bu halda fayl – serverdən İST -ə ƏS yükləndikdə, şəbəkə adapterində uzaq məsafədən yükləməyə imkan verən uyğun mikrosxem olmalıdır. Bu mikrosxem girş – çıxış baza sisteminin (BİOS) genişlənməsi kimi istifadə olunur. Bu mikrosxemdə İST – nin əməli yaddaşına ƏS – nin yüklənməsi proqramı yazılır. Bu cür disksiz İST-in əsas üstün cəhəti onların ucuz olması və burada istifadəçinin proqramına icazə verilmədən daxil olmanın mümkünsüzlüyü və kompüter viruslarının daxil ola bilməməsidir. Mənfi cəhəti isə onun avtonom rejimdə işləyə bilməməsi (serverə qoşulmamaq şərtilə), həmçinin özünün verilənlər və proqram arxivinin olmamasıdır.
- LKŞ – də serverlər – şəbəkə resurslarını paylamaq funksiyasını yerinə yetirirlər. Adətən server funksiyasını kifayət qədər güclü olan fərdi kompüter, meynfreym və ya xüsusi kompüter həyata keçirə bilər. Hər bir server həm ayrıca, həm də İST tərkibində ola bilər. Axırıncı halda serverin tam deyil, yalnız resurslarının bir hissəsi ümumi istifadədə ola bilər.
- LKŞ – də bir neçə server olarsa, o zaman hər bir server ona qoşulan İST -ə xidmət göstərir. Serverin kompüterlər toplusuna və onlara qoşulmuş İST-ə domen dyilir. Bəzi hallarda bir domendə bir neçə server olur. Bu serverlərdən biri baş server, qalanları isə ehtiyat serveri və ya əsas serverin məntiqi genişlənməsi rolunu oynayırlar.
- Kompüter server tipini seçdikdə əsas parametr kimi prosessorun tipi, əməli yaddaşın tutumu, sərt diskin tipi və tutumu, disk kontrollerinin tipi nəzərə alınmalıdır. Bu xarakteriskaların qiymətləri həll olunacaq məsələdən, şəbəkədə hesablamaların təşkil olunmasından, şəbəkənin yüklənmə dərəcəsindən, istifadə olunan ƏS-dən və digər amillərdən asılıdır.
- Serverdə əməli yaddaş nəinki öz proqramını yerinə yetirmək məqsədini güdür, həmçinin disk giriş – çıxışının buferlərini yerləşdirmək məqsədi üçün də istifadə edilir. Buferlərin optimal sayını təyin etməklə, giriş-çıxış əməllərinin yerinə yetirilmə sürətini artırmaq olar.

- Əməli yaddaşı seçdikdə nəzərə almaq lazımdır ki, orada lazımi proqram təminatı, həmçinin şərikli istifadə olunan fayllar və verilənlər bazaları yerləşməlidir.
- İST və serverlər şəbəkənin yerləşdiyi yerlərdə öz aralarında kabel şəklində olan verilənlərin ötürülmə xətti ilə birləşirlər. Kompüterlər kabelə interfeys palatası – şəbəkə adapteri vasitəsilə birləşdirilir. Son zamanlar verilənlərin ötürülmə mühiti kimi istifadə olunan xətsiz şəbəkələr – radiokanallar meydana gəlmişdir.
- Bəzi hallarda kompüterlər bir neçə qonşu otaqlarda yerləşdirilir.
- İstifadə olunan şəbəkə adapteri 3 əsas xarakteriskaya malikdirlər: kompüterin qoşulduğu şinin tipi (İSA, EISA, Micro Channel və s.) mərtəbələr şəbəkəsinin sayı (32,64) və yaradılan şəbəkənin topologiyası (Ethernet, Arcnet, Token - Ring). Məs. Ethernet topologiyalı və Novell Net Ware və ya MS Windowsfor Workgropus ƏS-ə malik şəbəkələr üçün Novell firmasının NE3200 (32 bitli) şəbəkə adapterindən istifadə etmək daha məqsədə uyğun sayılır.
- Şəbəkə kabelinin seçilməsi onun spesifikasiyası ilə əlaqədar olub, şəbəkə adapterinin sənədlərində göstərilir.
- LKŞ-ın əlavə avadanlıqlarına fasiləsiz qida mənbələri, modemlər, transirverlər, repiterlər və müxtəlif kontaktlar sistemi kimi istifadə olunan konnektorlar və terminatporlar daxildirlər.
- Fasiləsiz qida mənbələri (UPS-Unit Power System) – elektrik şəbəkəsinin dayanıqlı işləməsini artırır və elektrik şəbəkəsi açıldıqda serverdə olan verilənlərin itməməsini təmin edir. Dövrədə kompüteri qidalandıran gərginlik açılarsa, o zaman kompüter öz işinə UPS sayəsində davam edəcək, kompüterin əməli yaddaşına yüklənmiş proqram və verilənlər itməyəcək. UPS-i seçdikdə fikir vermək lazımdır ki, onun gücü serverlərin gücündən az olmasın.
- Transiver – İST –ni yoğun koaksil kabelinə qoşan qurğudur.
- Repiter – isə şəbəkə seqmentlərini birləşdirən qurğudur.
- Konnektorlar (birləşdiricilər) kompüterlərin şəbəkə adapterlərini nazik kabellə birləşdirmək üçündür.
- Terminatorlar – açıq kabellərə şəbəkənin qoşulması üçün, həmçinin torpaqlama məqsədilə də istifadə oluna bilər.

- Modem – telefon xətti vasitəsilə LKŞ və ya ayrıca kompüteri qlobal şəbəkəyə qoşan qurğudur.
- Elementlərin şəbəkəyə qoşulma konfiqurasiyalarına topologiya deyilir. Topologiya şəbəkənin bir sıra vacib xarakteriskalarını,o cümlədən etibarlı işləməsini, məhsuldarlığını, dəyərini, mühafizə olunmasını təyin edir.
- LKŞ topologiyasının təsnifatına yanaşmalardan biri topologiyanı 2 əsas sinfə bölməkdir: genişyayılmış və ardıcıl tipli.
- Genişyayılmış topologiya konfiqurasiyasında hər bir kompüterin ötürdüyü siqnal yerdə qalan kompüterlər tərəfindən qəbul olunur. Bu cür konfiqurasiyaya “ümumşin”, “ağacabənzər”, “passiv mərkəzli ulduz” topologiyalarını aid etmək olar.
- Ardıcıl konfiqurasiyalı topologiyada isə hər bir fiziki alt-səviyyə informasiyanı yalnız bir fərdi kompüterə verə bilir. Buna misal olaraq ixtiyari (kompüterlər bir – birilə ixtiyari şəkildə birləşirlər), “iyerarxik”, “halqavari”, “zəncirvari”, “intellektul mərkəzli ulduz”, “qar dənələri şəklində” və s.
- topologiyalarını göstərmək olar.
- LKŞ topologiyasının geniş yayılmış 3 növünü nəzərdən keçirək:
- Mərkəzi qovşaq kimi, passiv birləşdirici və ya aktiv təkrarlayıcıdan istifadə edilə bilər. Bu topologiyanın mənfi cəhəti onun etbarlılığının az olmasıdır, çünki mərkəzi qovşaq işdən çıxan kimi, bütün şəbəkə öz işini dayandırır və həmçinin burada çox böyük uzunluqlu kabeldən istifadə edilir. Bəzi hallarda işləmə etibarlılığını artırmaq üçün mərkəzi qovşaqda xüsusi rele qoyulur ki, bunun vasitəsilə sıradan çıxmış kabellər dövrədən açılır.
- “Ümumişin” topologiyasında bütün kompüterlər bir kabelə qoşulurlar. Burada informasiya kompüterlərə növbə ardıcıllığı ilə verilir.
- Bu halda uzunluğu kiçik olan kabeldən istifadə edilir, “ulduz” topologiyasına nəzərən daha etibarlı işləyir, çünki ayrı-ayrı kompüterlərin işdən çıxması, şəbəkənin ümumi işinə xələl gətirmir. Mənfi cəhəti ondan ibarətdir ki, əsas kabel zədələndikdə bütün şəbəkə öz işçi funksiyasını itirir; həmçinin burada bir kompüterdən digərinə

göndərilən informasiya başqa kompüterlər tərəfindən də qəbul oluna bildiyi üçün fiziki səviyyədə informasiya zəif mühafizə olunur.

- “Halqavari” topologiyada bir kompüterdən digərinə verilənlər “estafet” də olduğu kimi ötürülür
- Əgər hər hansı bir kompüter ona aid olmayan verilənləri qəbul edibsə, o zaman həmin kompüter o verilənlərin halqavari istiqamətdə o biri kompüterlərə ötürəcəkdir.
- Bu topologiyanın üstün cəhəti, kabel sıradan çıxan zaman sistemin iş qabiliyyətinin saxlanmasıdır. Çünki, bu halda hər bir kompüterə daxil olmanın iki yolu olur. Mənfi cəhəti isə kabelin müəyyən qədər uzun olması, “ulduz” – a nisbətən sürəti kiçik olması, həmçinin “ümumi şin” topologiyasında olduğu kimi, informasiyanın zəif mühafizə olunmasıdır.
- Real LKŞ – nin topologiyası yuxarı da göstərilən topologiyalardan və ya onların kombinasiyalarından birinin əsasında qurula bilər. Ümumi halda şəbəkənin strukturu aşağıdakı amillərlə təyin olunur: birləşdirilən kompüterlərin sayı, informasiyanın ötürülməsinin operativliyi və etibarlılığı, iqtisadi amillər və s.
- Lokal şəbəkələrdə mərkəzləşdirilmiş və mərkəzləşdirilməmiş kimi 2 əsas idarə prinsipi mövcuddur.
- Mərkəzləşdirilmiş idarəetmədə verilənlər mübadiləsinin idarəsi fayl – serstansiyaları tərəfindən istifadə edilə bilərlər. Bir işçi stansiyasının faylına digər işçi stansiya müraciət edə bilməz. Əsas daxil olma yolundan istifadə etməməklə, “Net Link” proqramı vasitəsilə işçi stansiyalar arasında fayllar mübadiəsini təşkil etmək olar. Bu proqramın icrası ilə NC proqramında faylı köçürdüyümüz kimi, iki kompüter arasında faylları bir – birinə ötürmək olar.
- Mərkəzləşdirilmiş idarəli şəbəkənin üstün cəhəti şəbəkə resurslarının onlara icazəsiz daxil olmaların yüksək dərəcədə mühafizəsi, daha böyük saylı qovşaqlara malik şəbəkələrin qurulmasının mümkünlüyüdür. Mənfi cəhəti isə, fayl-server öz iş qabiliyyətini itirdikdə, sistemə icazəsiz daxil olmanın mümkünlüyü, həmçinin server resurslarına daha yüksək tələblərin olmasıdır.
- Mərkəzləşdirilməmiş (bir səviyyəli) şəbəkələrdə xüsusi ayrılmış serverlər olmur. Şəbəkənin idarəetmə funksiyası növbə ilə bir İST – dən digər İST – yə ötürülür. Bir İST-nin resurslarından (disklər,

printerlər və digər qurğular) digər İST istifadə edə bilər. Bu cür şəbəkələrdə Windows ƏS-dən istifadə etmək olar.

- Çox da böyük olmayan İST üçün bu cür şəbəkə daha səmərəlidir və real paylanmış hesablama mühitinin qurulmasına imkan verir. Mərkəzləşdirilmiş şəbəkələrə nəzərən burada proqram təminatı daha sadə olur. Burada fayl-serverdən istifadə edilməsi lazım olmur, bu da sistemin daha ucuz yaranmasına səbəb olur. Lakin bu şəbəkədə informasiyanın mühafizəsi və inzibati idarə məsələləri bir qədər zəif alınır.
- Kompüterlər arasında informasiya mübadiləsini təşkil etmək məqsədilə LKŞ-də Elektrotexnika və Radiotexnika sahəsində Beynəlxalq İnstitut (İEEE – İnstute of Electrical and Electroncal Engineers) tərəfindən hazılanmış standart protokollardan istifadə olunur.
- İEEE802.3 və İEEE802.4 standartlarında təsvir edilən və lokal şəbəkələrdə (Ethernet, Arcnet və Token Ring) istifadə olunan mübadilə protokollarına qısa nəzər salaq. Bu protokollar vasitəsilə şəbəkə kanal verilənlərinə daxil olma üsulları götərilir. Bunlar OSI modelinin kanal səviyyəsini hayata keçirirlər.
- "Ethernet" üsulu. Bu Xerox firması tərəfindən təklif edilmiş və burada "ümum şin" topologiyasından istifadə edilmişdir. Ümumi şin ilə ötürülən məlumatların sərlövhəsində ötürülən və qəbul edən mənbələrin ünvanları göstərilir.
- Bu üsul aparıcı tezliyi araşdırmaq və ziddiyitləri yox etməklə, çoxşahəli mübadilə üsuludur (CSMA/CD – Caries Sense Multiple Access with Collision Delection). Bu üsulun mahiyyəti ondan ibarətdir ki, İST yalnız o vaxt məlumatı ötürməyə başlayır ki, kanal boş olsun, əks təqdirdə məlumatın ötürülməsi müəyyən zaman anı üçün gecikdirilmiş olacaq. Eyni zamanda verilənlərin ötürülmə imkanı avtomatik olaraq aparat üsulu ilə həyata keçirilir.
- 80-100 İST eyni vaxtda işlədikdə şəbəkənin işləmə sürəti azlır. Bu, kanalda əmələ gələn münaqişələrlə əlaqədardır.
- "Arenet" üsulu – Datapoint Corp. Firması tərəfindən təklif edilmiş və burada "ulduz" topologiyasından istifadə olunmuşdur. Bu halda bir İST –dən digər iST -ə məlumatların ötürülməsi İST-in birində təşkil edilən markerlər vasitəsilə həyata keçirilir. Məlumat ötürmək

istəyən İST markerin ona gəlməsini gözləyir, göndərənin və qəbuledilənin ünvanları yazılmış sərlövhəyə malik məlumatı buna birləşdirir. Əgər İST qəbulu gözləyirsə , yenə də markerin gəlməsini gözləməlidir. Marker gəldikdən sonra məlumatlarla birlikdə gələn sərlövhə anaiiz olunmalıdır. Əgər alınan məlumatlar bu İST-ə aid olarsa,o zaman İST onu markerdən ayırır.

- "Arcnet" şəbəkəsinin avadanlıqları "Ethernet" və "Token Ring" şəbəkələrinə nəzərən daha ucuz olurlar, lakin həmin avadanlıqların etibarlılığı və məhsuldarlılığı nisbətən aşağı olur.
- "Token Ring" üsulu – "halqavari" topologiyaya malik olub İBM firması tərəfindən təklif edilmişdir. Bu firmadan başqa, bu cür şəbəkələrin avadanlıqlarını Proteon, 3 Com və Undermann – Bass firmaları, şəbəkə proqram təminatını isə 3COM, Novell və Univation firmaları istehsal edirlər. Bu üsul "Arcnet" üsuluna oxşayır. Əsas fərq ondan ibarətdir ki, burada üstünlük mexanizmi vardır. Bunun sayəsində bəzi İST digərlərinə nəzərən daha tez markeri əldə edə bilirlər və onu bir qədər özündə saxlamaq imkanına mail olurlar.
- LKŞ –də tipik proqramlardan istifadə etmək məqsədilə şəbəkədə məlumatların mübadiləsi üçün hansı protokoldan istifadə olunmasını bilmək lazımdır. Belə protokollardan bir neçəsi mövcuddur. Ən geniş yayılmış protokollar bunlardır.
- İPX, SPX və NETBİOS.
- İPX (İnternetwork Packet Exchange) – protokolu OSI modelinin nəqliyyat səviyyəsinin protokoludur. O, şəbəkənin aşağı səviyyələri ilə interfeysə malikdir.
- SPX (Sequenced Packet Exchange) - daha yüksək səviyyə olan seans səviyyəsinin protokoludur. O, İPX, NETBİOS (Network Basic İnput/ Output System – şəbəkə giriş-çıxış baza sistemi) protokolları əsasında yaradılmışdır. Bunun vasitəsilə OSI modelinin şəbəkə, nəqliyyat və seans səviyyələrinin funksiyaları həyata keçirilir.

Müasir dövrdə kompüterlərin tətbiq olunduğu ən mühüm sahələrdən biri də kompüter şəbəkələridir. Şəbəkələr bir çox istifadəçilər üçün vahid informasiya fazasının yaradılmasını təmin edir.

Şəbəkə dedikdə verilənlərin ötürülmə vasitələri ilə öz aralarında birləşmiş kompüterlər toplusu nəzərdə tutulur. Verilənlərin ötürülməsi

vasitələri bir-biri ilə əlaqələndirilmiş kompüterlər, peyk, telefon, radio və s. ötürücülər əsasında qurulmuş rabitə kanallarından, kommutasiya edici aparatlarından, siqnal vericilərinin müxtəlif tiplərindən, retranslyatorlardan və s.dən ibarət ola bilər.

Müasir şəbəkələri bir sıra əlamətlərə - kompüterlər arasındakı məsafəyə görə, təyinatına görə, topologiyaya görə, göstərdiyi xidmətlərin sayına görə,paketlərin və deytaqramların kommutasiya üsullarına görə, ötürmə mühitinə görə və s. əlamətlərə görə təsnifləşdirmək olar.

Kompüterlər arasındakı məsafəyə görə şəbəkələr lokal və qlobal olmaqla iki qrupa bölünür.

Qlobal şəbəkələrə həm lokal şəbəkələr,həm digər qlobal şəbəkələr, həm də ona ayrıca qoşulan və uzaq məsafədə yerləşən kompüterlər və ya ayrıca qoşulan giriş və çıxış qurğuları qoşula bilər. Qlobal şəbəkələr məsafədədən asılı olaraq şəhər, regional, milli və transmilli olur. Bu şəbəkələrdə məsafə daha böyük olur.

Lokal şəbəkələrdə qlobal şəbəkələrdən fərqli olaraq kompüterlər arasındakı qısadır. Bu şəbəklərdə kompüterlər arasındakı məsafə bir neçə kilometrə qədər ola bilər və onlar adətən mübadilə sürəti 1-dən 10-a və daha çox Mbit/s olan sürətli rabitə xətləri ilə əlaqələndirilirlər. Bir çox hallarda lokal kompüterlər şəbəkələri hər hansı bir təşkilat (müəssisə) daxilində fəaliyyət göstərir. Məhz bu xüsusiyyətə görə şəbəkələr çox vaxt korporativ sistemlər və ya şəbəkələr adlanırlar. Belə olan halda kompüterlər bir qayda olaraq, hər hansı bir otaq, bina və ya qonşu binalar daxilində ola bilərlər.

Kompüterlərin hansı şəbəkədə işləməsindən asılı olmayaraq, həmin onlara qoyulmuş proqram təminatının funksiyasına görə kompüterlərin öz resurslarını idarə edən və digər kompüterlərlə mübadiləni idarə edən olmaqla iki qrupa bölünür. Kompüterlərin öz resurslarını əməliyyat sistemi, şəbəkələrin resurslarını isə şəbəkə proqram təminatı idarə edir. Şəbəkə proqram təminatı ya ayrıca paket, ya da şəbəkə əməliyyat sistemi vasitəsilə həyata keçirilir.

Şəbəkə proqram təminatında iyerarxik (ağacabənzər) yanaşmadan istifadə edilir. Burada sərbəst səviyyələr və onlar arasındakı interfeyslər əvvəlcədən təyin olunmalıdır. Bunun sayəsində digər

səviyyələrə əl dəyməmək şərtilə, ixtiyari səviyyənin proqramını təkmilləşdirmək mümkün olur. Şəbəkə proqram təminatı şəbəkənin hər xidmətinin reallaşdırılması və istifadəçinin bu xidmətdən istifadə etməsi üçün yaradılır. Şəbəkədə işləmək üçün təyin olunmuş proqram təminatı istifadəçilər tərəfindən eyni zamanda istifadə oluna bilər.

Şəbəkə proqram təminatının işlənməsini qaydaya salmaq və istənilən kompüter sistemlərinin qarşılıqlı əlaqəsini təşkil etmək məqsədilə Standartlaşdırma üzrə Beynəlxalq Təşkilat (İSO – İnternational Standart Organization) açıq sistemlərin qarşılıqlı əlaqəsini təmin edən Etalon model (OSİ- Open System İnterconnection) təklif edilmişdir.

Şəbəkə təsnifatının digər bir novü də topologiyalara görə kompüterlərin təsnifləşdirilməsidir. Şəbəkə topologiyası dedikdə şəbəkə düyünlərinin əlaqə kanalları ilə birləşdirilməsinin məntiqi sxemi başa düşülür. Lokal şəbəkələrdə üç: monokanallı (ümumşin), dairəvi (halqavari) və ulduzvari topologiyadan istifadə olunur.

Monokanallı topologiyada bütün kompüterlər bir kabelə qoşulur və bu halda uzunluğu kiçik olan kabeldən istifadə edilir. Bu topologiyanın əsas müsbət cəhəti ondadır ki, əgər ayrı-ayrı kompüterlərin işdən çıxması, şəbəkənin işinə xələl gətirmir. Mənfi cəhəti ondadır ki, əsas kabel zədələndikdə bütün şəbəkə öz işçi funksiyasını itirir.

Ulduzvari topologiyada hər bir kompüterlər xüsusi şəbəkə adapteri vasitəsilə ayrıca kabellə mərkəzi qovşağa qoşulur.Mərkəzi qovşaq kimi passiv birləşdirici və ya aktiv təkrarlayıcıdan istifadə edilə bilər. Bu topologiyanın mənfi cəhəti ondadır ki, mərkəzi qoşağın işdən çıxması zamanı btün qovşaq öz işini dayandırır və burada çox böyük uzunluqlu kabeldən istifadə edilir.

Dairəvi topologiyada verilənlər “estafet”də olduğu kimi bir kompüterdən digərinə ötürülür. Əgər hər hansı bir kompüter ona aid olmayan verilənləri qəbul edibsə, onda həmin kompüter o verilənləri dairəvi istiqamətdə o biri kompüterə ötürür.

Kompüter virusları təxminən 1980-ci illərin əvvəllərində meydana çıxmışdır. «Kompüter virusu» termini 1984-cü ildə ABŞ-da keçirilən informasiya təhlükəsizliyi üzrə 7-ci konfransda Fred Koen tərəfindən işlədilmişdi. Kompüter viruslarının ümumi qəbul edilmiş tərifi yoxdur. Biz aşağıdakı tərifdən istifadə edəcəyik. Kompüter virusu – elə

proqramdır ki, özünü təxminən bioloji virus kimi aparır: çoxalır, maskalanır və ziyanlı təsirlər göstərir (əməliyyatlar yerinə yetirir). Virusları aşağıdakı əlamətlərə görə təsnif etmək olar:

I. yaşayış mühitinə görə:

II. fayl virusları (com, exe, bat, doc virusları),

III. yükləmə virusları,

IV. makro viruslar;

- yaşayış mühitini yoluxdurma üsuluna görə: rezident və qeyri-rezident;
- əməliyyat sisteminə görə: MS-DOS virusları, Windows virusları, *NIX virusları və s.;
- destruktiv imkanlarına görə: ziyansız, təhlükəsiz, təhlükəli, çox təhlükəli;
- virus alqoritminin xüsusiyyətlərinə görə: «tələbə» virusları, kompanyon-viruslar, «soxulcanlar» (worm), «stels»-viruslar («görünməz» viruslar), «polimorf»-viruslar (özüşifrlənən viruslar), şəbəkə virusları və s.

Virusların yaradılması. Hər gün 10-15 yeni növ virus meydana çıxır. Virusların miqdarı həndəsi silsilə üzrə artır. Bunu statistika və real həyat təsdiq edir. 1990-cı ildə təxminən 500 virus, 1992-ci ildə - 3 000, 1994-cü ildə - 5 000, 1996 – 9 000, 1999 – 30 000, 2001 – 50 000, 2004-cü ildə 112 000-dən çox virus məlum idi.

Kompüter viruslarının sayının artması ilk növbədə onunla bağlıdır ki, proqramlaşdırmanı bir qədər öyrəndikdən sonra istənilən şəxs virus yaza bilər. Bu işdə ona leqal və qeyri-leqal ədəbiyyat, virusların yazılması üçün xüsusi proqram təminatı kömək edə bilər. Hətta müxtəlif mutasiya generatorları mövcuddur ki, birinci kurs tələbəsinin yaratdığı sadə virusdan onun köməyi ilə mürəkkəb virus yaratmaq olar.

Virusların yayılması. Şəbəkə və kommunikasiya texnologiyalarında hər bir yenilik virusların yaradılması və yayılması üçün yeni imkanlar, yollar

açır. Yaxın vaxtlara kimi viruslar disketlər və digər daşıyıcılar vasitəsi ilə yayılırdı, İnternet viruslar üçün geniş magistral açdı. Kompüter virusları Internetdə bioloci virusların real dünyada yayıdmasından daha sürətlə yayılır. 2003-cü ildə Slammer "soxulcanı" 10 dəqiqə ərzində 75 min kompüter yoluxdurmuşdu. 1999-cu ildə ilk dəfə dünya miqyasında virus epidemiyası yaranmışdı. Melissa virusu on minlərlə kompüteri yoluxdurmuş və 80 milyon dollar ziyan vurmuşdu. Bu insidentdən sonra dünyada antivirus proqramlara böyük tələb yarandı. 2000-ci ilin mayında Melissanın rekordunu bir neçə saat ərzində milyonlarla kompüteri yoluxdurmuş I Love You! virusu təzələdi. Praktik olaraq virusla "yoluxdurmaq" mümkün olmayan fayl növü qalmamışdır. Artıq mobil telefonları və proqram təminatından istifadə edən dizər qurğuları yoluxduran viruslar da sürətlə yayılır.

Virus müəllifləri təkcə texnoloci zəifliklərdən deyil, "psixoloji" zəifliklərdən də istifadə edirlər. Tədqiqatlar göstərmişdir ki, Anna Kournikova, Sean Connery, Julia Roberts, Elvis Presley Lives kimi viruslardan əziyyət çəkmiş hər beşinci İnternet istifadəçisi edilmiş xəbərdarlıqlara baxmayaraq həmin adlı qoşma faylları açmışdılar. Antivirus proqramlarının növləri. Viruslarla mübarizə proqramlarının bir neçə növü var - *skanerlər* (başqa adı: faqlar, polifaqlar), *disk müfəttişləri* (CRC-skanerlər), *rezident monitorlar* və *immunizatorlar.*

Skanerlər. Antivirus skanerlərin iş prinsipi faylların və sistem yaddaşının yoxlanmasına və onlarda məlum və ya yeni (skanerə məlum olmayan) virusların axtarışına əsaslanır. Məlum virusların axtarışı üçün «maska»lardan istifadə edilir. Virusun maskası konkret virus üçün spesifik olan müəyyən sabit kodlar ardıcıllığıdır. Bir çox skanerlərdə həmçinin «evristik skanlama» alqoritmlərindən istifadə edilir, yəni yoxlanan obyektdə komandalar ardıcıllığı analiz edilir, müəyyən statistika toplanır və hər bir yoxlanan obyekt üçün qərar qəbul edilir («ola bilsin yoluxub» və ya «yoluxmayıb»).

Disk müfəttişləri. Disk müfəttişlərinin (CRC-skanerlərin) iş prinsipi diskdə olan fayllar və sistem sektorları üçün CRC-cəmlərin (nəzarət cəmlərinin) hesablanmasına əsaslanıb.

Rezident monitorlar. Rezident monitorlar - daim operativ yaddaşda yerləşən və disklə və operativ yaddaşla aparılan əməliyyatlara nəzarət edən proqramlardır. Məhz bu proqramlar sistemin real yoluxma anına kimi virusu aşkarlamağa imkan verir (əvvəlki ikisindən fərqli olaraq).

İmmunizatorlar. İmmunizatorların iki növü var:

1. yoluxma barədə məlumat verən immunizatorlar
2. hər-hansı növ virusla yoluxmanın qarşısını alan immunizatorlar.

Onlardan birincisi adətən faylların sonuna yazılır və hər dəfə fayl işlədikdə onun dəyişməsini yoxlayır. Bu immunizatorların bir nöqsanı var - stels-virusla yoluxma barədə məlumat verməyə qabil deyil. Buna görə bu immunizatorlar hazırda praktikada istifadə edilmir. İkinci növ immunizator sistemi hər hansı müəyyən növ virusla yoluxmaqdan mühafizə edir. Diskdə fayllar elə modifikasiya edilir ki, virus onları artıq yoluxmuş fayl kimi qəbul edir. Rezident virusdan mühafizə üçün kompüterin yaddaşına virusu imitasiya edən proqram yüklənir. Virus işə düşdükdə onunla rastlaşır və hesab edir ki, sistem artıq yoluxub.

MÖVZU

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 17799 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 autentikasiya. 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. Autentikasiya 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).

Autentikasiyanın 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 autentikasiya 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. Cədvəlin 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.

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.

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.

Müasir kriptoqrafiyanın predmeti informasiyanı bədniyyətlinin müəyyən əməllərindən mühafizə etmək üçün istifadə edilən informasiya çevirmələridir. Kriptoqrafiya konfidensiallığı, bütövlüyə nəzarəti, autentikasiyanı 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:

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.

Asimmetrik kriptoqrafiyada iki açardan istifadə olunur. Onlardan biri - açıq açar (sahibinin ünvanı ilə birlikdə nəşr oluna bilər) şifrləmə üçün istifadə olunur, digəri - gizli açar (yalnız alana məlum) deşifrləmə üçün

istifadə olunur. Rəqəmsal imza alqoritmlərində gizli açar şifrləmə, açıq açar isə deşifrləmə üçün istifadə edilir. Açıq açara görə uyğun gizli açarın tapılması çox böyük həcmdə hesablamalar tələb edir, hesablama texnikasının hazırki inkişaf səviyyəsində bu məsələ qeyri-mümkün hesab edilir.

Asimmetrik şifrləmə sisteminin istifadəsini illüstrasiya edir. Asimmetrik şifrləmə alqoritmlərinə misal olaraq RSA, ElGamal, Şnorr və s. alqoritmlərini göstərmək olar. Asimmetrik kriptoqrafiyanın əsas çatışmayan cəhəti sürətin aşağı olmasıdır. Buna görə onlar simmetrik metodlarla birgə işlədilir. Məsələn, açarların göndərilməsi məsələsini həll etmək üçün əvvəlcə məlumat təsadüfi açarla simmetrik metodla şifrlənir, sonra həmin təsadüfi açarı alan tərəfin açıq asimmetrik açarı ilə şifrləyirlər, bundan sonra məlumat və şifrlənmiş açar şəbəkə ilə ötürülür.

Asimmetrik metodlardan istifadə etdikdə, (istifadəçi, açıq açar) cütünün həqiqiliyinə zəmanət tələb olunur. Bu məsələnin həlli üçün rəqəmsal sertifikatdan istifadə edilir. Rəqəmsal sertifikat xüsusi sertifikasiya mərkəzləri tərəfindən verilir. Rəqəmsal sertifikatda aşağıdakı verilənlər olur: sertifikatın seriya nömrəsi; sertifikatın sahibinin adı; sertifikatın sahibinin açıq açarı; sertifikatın fəaliyyət müddəti; elektron imza alqoritminin identifikatoru; sertifikasiya mərkəzinin adı və s. Sertifikat onu verən sertifikasiya mərkəzinin rəqəmsal imzası ilə təsdiq edilir. Bütövlüyə nəzarət üçün kriptoqrafik heş-funksiyalar istifadə edilir. Heş-funksiya adətən müəyyən alqoritm şəklində realizə edilir, belə alqoritm ixtiyari uzunluqlu məlumat üçün uzunluğu sabit heş-kod hesablamağa imkan verir. Praktikada 128 bit və daha artıq uzunluqda heş-kod generasiya edən heş-funksiyalardan istifadə edilir.

Kompüter şəbəkəsinin yaranması üçün ən azı iki kompüterin bir-birinə qoşulması lazımdır. Şəbəkə harada və nə üçün istifadə olunur? sualını versəniz, bu suala indi çox rahat cavab tapmaq olar. Məsələn, bu gün ofislərdə, nəşriyyatlarda, kompüter klublarında və ya beynəlxalq informasiya mübadilələrində kompüter şəbəkələri vacib rol oynayır. Əgər bir firmanın müdiri ümumi sənədin bütün işçilər üçün əl çatan olmasını istəyirsə, o, kompüter şəbəkəsindən istifadə edərək bu işi

rahatca həyata keçirir. Nəşriyyatda işləyən dizayner öz kompüterində hazırladığı jurnalın üz qabığını çap etmədən şef redaktora göstərmək və rəyini bilmək istəyirsə, sadəcə olaraq şefin kompüterinə jurnalın üz qabığını göndərir və danışıq proqramı vasitəsi ilə onun rəyini alır. Oyun klublarında tək oynamaqdan bezən uşaqlar bir-biriləri ilə şəbəkə vasitəsi ilə oynaya bilirlər. Beynəlxalq kompüter şəbəkələri ilə xüsusi proqram təminatı ilə xaricdə yaşayan qohumlarının üzlərini kompüterdə görə və səslərini rahatca eşidə bilərlər.

Həqiqi şəbəkələrdən çox-çox əvvəl alimlər fərqli iki sistemin məlumatlarının hansı yolla bölüşdürülməsi haqqında müzakirə etməyə başlamışdılar. Yəqin ki siz də ilk kompüter şəbəkəsinin ARPANET olduğunu eşitmisiniz. Amerikanın ARPANET Advanced Research Projects Agency(ARPA) adlı agentliyi tərəfindən qurulmuşdur. ARPA 1958-ci ildə qurulan və Amerika dövləti üçün yüksək texnologiyalar düzəldən agentlik idi. 1972-ci ildə adı DARPA(Defence Advanced Research Agency) kimi dəyişdirildi, 1993-cü ildə təkrar ARPA, 1996-cı ildə isə təkrar DARPA oldu. DARPA kompüter şəbəkələri ilə bağlı fərqli olan fikirləri bir araya gətirərək ümumi sistem düzəltdi. Bu agentlik vasitəsi ilə kompüter şəbəkə layihələri, internetin təməlini qoymuş TCP/IP və buna bənzər texnologiyalar yaradıldı. Əlbəttə, belə sual yarana bilər ki bəs mainframe-lər hara yox oldular. 80-ci illərdə İBM(ay bi em) PC(pi si)Personal Computer- fərdi kompüter fikrini irəli sürdü. Bu kompüterlərdə hətta proqramlaşdırma təminatı da olacaqdı (DOS, Windows).

Nəticədə PC və ya mini-computer adlandırılan bu kompüterlərin dünyadakı sayı milyonlara, milyardlara çatdı. Mainframe-lər texnologiyadakı yeniliklərə baxmayaraq ilk yaradıldıqları məqsədə hələ də xidmət edirlər. Müəyyən hədd daxilində hesablamaya ehtiyacı olan firmalar prosessoru IBM As400 olan maşınlardan və buna bənzər mainframe sistemlərindən hələ də istifadə edirlər.

Mainframe almaq imkanı olmayan firmalar üçün mini-computer/PC şəbəkələri sistemi yaradıldı. Onlardan bəziləri Novell-in Netware (Netveyr) sistemi, Microsoft-un NT-si və onların davamı olan Windows 2000, XP, Vista, Windows 7 buna misal çəkilə bilərlər.

Bu bölmədə kompüter şəbəkələrinin hansı növlərinin olduğunu və şəbəkə quraşdırmağa qərar verərkən hansı sahə üçün, hansı şəbəkə formasından, dizaynından istifadə edəcəyiniz haqda geniş izah verilir.

LAN, WAN və digər Sahə Şəbəkələri (Area Networks)

Müxtəlif tip kompüter şəbəkə dizaynlarının kateqoriyalaşdırılması üçün bir yol var. Onları fiziki sahəsi və miqyasına görə qruplaşdırmaq. İnkişaf tarixi səbəblərindən, bütün dizayn tipləri demək olar ki, müəyyən sahəyə görə yaradılmışdırlar. Aşağıda onları görə bilərsiniz:

LAN - Local Area Network (yerli sahə şəbəkəsi)

WLAN - Wireless Local Area Network (simsiz yerli sahə şəbəkəsi)

WAN - Wide Area Network (geniş sahə şəbəkəsi)

MAN - Metropolitan Area Network (metropoliyan (paytaxt) sahə şəbəkəsi)

SAN - Storage Area Network, System Area Network, Server Area Network və ya bəzən Small Area Network (bir çox adı var əsas Storage Area Network (saxlama sahə şəbəkəsi) kimi tanınır)

CAN - Campus Area Network, *Controller Area Network* bəzən *Cluster Area Network* bir çox adı var. Əsas *Controller Area Network* (nəzarət sahə şəbəkəsi) kimi tanınır)

PAN - Personal Area Network (şəxsi sahə şəbəkəsi)

DAN - Desk Area Network (idarəetmə sahə şəbəkəsi)

LAN və WAN əsas orijinal sahə şəbəkəsi kateqoriyalarıdır, qalanları illər boyunca texnologiyanın inkişafı irəlilədikcə yaradılmışdırlar və yəqinki bundan sonrada yeniləri yaradılıcaqdırlar.

LAN Nədir?

LAN - Local Area Network (Yerli Sahə Şəbəkəsi). Bu forma kiçik ofislərdə, ev daxili və ya kiçik kompüter klublarında istifadə olunur. Bu

tip vasitəsi ilə evdə, işdə və ya klubda oyun oynamaq, o biri kompüterə qoşulmuş printerdən yazı çap etmək olar. Şəbəkə tipi nə qədər böyük olursa olsun onun tərkibində LAN(lar) olur. Bütün böyük şəbəkələr kiçik LAN şəbəkələrini birləşdirmək üçün mövcuddurlar və ya o səbəbdən yaranıblar.

WLAN Nədir?

WLAN - Wireless Local Area Network (simsiz yerli sahə şəbəkəsi). Bu da LAN deməkdir. Həm üstün, həm də mənfi cəhətləri var. Üstün cəhəti evin ya da ofisin içərisində ayağınıza dolaşacaq və ya divarın deşilməsinə səbəb olacaq kabellərin olmamağıdır. Mənfi cəhəti onun hələ inkişaf etməkdə olmasıdır ki, texnologiya kompüter oyunları və həcmi böyük proqramların tələblərini hələ ki ödəyə bilmir. Amma sənədləri şəbəkə vasitəsi ilə bölüşmək onun üçün problem deyildir. Üstün cəhəti ötürmə radiusu üzrə dairəvi formada bağlantı qura bilir. Kabel kimi tək istiqamətli bağlantıdan asılı olmur.

WAN Nədir?

WAN - Wide Area Network (geniş sahə şəbəkəsi). LAN-ın maksimum əhatə sahəsi bir binadırsa, WAN üçün bu əhatə sahəsi şəhərin bir neçə rayonu, yer kürəsinin tamamı desək yalan olmaz. Əlbəttə ki, burada istifadə olunan texnologiyalar LAN-dan fərqlənir və daha bir neçə cihaz əlavə olunur.

İnformasiya Cəmiyyətinin elmi-nəzəri əsaslarının tədqiqi, etibarlı, dayanıqlı və təhlükəsiz elektron idarəetmə (e-hökumət, e-bələdiyyə və s.) texnologiyalarının işlənilməsi sahəsində mühüm elmi nəticələr əldə olunmuşdur. İnformasiya cəmiyyətinin elmi-nəzəri, informasiya iqtisadiyyatı, təhsil prosesinin informasiyalaşdırılması, informasiya təhlükəsizliyi, o cümlədən, informasiya cəmiyyətinin formalaşma mərhələləri, informasiya inqilabları, informasiya ekologiyası, informasiya mədəniyyəti, informasiya menecmenti, İnternet-jurnalistikanın formalaşdırılması problemləri, İnformasiya Cəmiyyətinin onlayn monitorinqi sisteminin işlənilməsi, İnternetdən istifadənin analizi üçün metodların işlənməsi, müxtəlif təyinatlı korporativ informasiya fəzalarının (e-elm, e-mədəniyyət, e-turizm və s.)

formalaşdırılması və reallaşdırılması problemləri, e-hökumət mühitində e-sənədlərin intellektual emalı və dövriyyəsi sisteminin işlənilməsi, informasiya resurslarının həyat tsiklinin idarə olunması, spamlarla mübarizə metodları, İnternet asılılığı ilə mübarizə üsullarının işlənilməsi, informasiya müharibəsi texnologiyaları, elektron demokratik təsisatların reallaşdırılması texnologiyalarının işlənməsi, e-hökumət mühitində dövlət sirrinin təmin olunması mexanizmlərinin işlənməsi, veb-resursların formalaşdırılması və idarə olunması mexanizmlərinin işlənməsi, onlayn təhsil mühitinin formalaşdırılması və idarə olunması, ölkəmizdə İKT iqtisadiyyatının digər iqtisadi sahələrlə qarşılıqlı təsirinin araşdırılması və inkişaf tendensiyalarının modelləşdirilməsi, İnternetin tənzimlənməsi problemlərinin tədqiq olunması istiqamətində elmi-nəzəri və praktiki işlər aparılır. İnformasiya Cəmiyyəti sahəsində dövlət siyasəti istiqamətində qəbul olunmuş dövlət proqramları və qanunlarından irəli gələn məsələlərin həllində bilavasitə iştirak edilmiş, "Elektron Azərbaycan" Dövlət Proqramı çərçivəsində institutun qarşısına qoyulan məsələlərin həlli istiqamətində işlər aparılır.

MÖVZU

Elektron imza.

Elektron imza elektron formada olan verilənlər blokudur, digər verilənlərlə (elektron sənəd, proqram faylları və s.) məntiqi əlaqəli olur və həmin verilənlərin müəllifini birqiymətli identifikasiya etməyə imkan verir. Rəqəmsal imza elektron imzanın növlərindən biridir, müəllifin identifikasiyasından savayı bir neçə əlavə funksiyanı həyata keçirir. Rəqəmsal imza adətən asimmetrik kriptoqrafiyaya əsaslanır. Rəqəmsal imza konkret məlumata (mətnə, fayla və ya ixtiyari uzunluqlu istənilən bitlər yığınına) əlavə olunan və aşağıdakı funksiyaları təmin etməyə imkan verən sabit uzunluqlu informasiya blokudur:

- məlumatın müəllifinin identifikasiyası və autentikasiyası;
- məlumatın bütövlüyünə nəzarət;
- məlumatın müəllifliyindən imtinanın qeyri-mümkünlüyünə zəmanət.

Məlumatın rəqəmsal imzası məlumatın özündən və imzalayanın gizli açarından asılıdır. Rəqəmsal imza iki alqoritm ilə realizə edilir: rəqəmsal imzanın yaradılması alqoritmi və rəqəmsal imzanın yoxlanılması alqoritmi. Rəqəmsal imza alqoritmlərinə misal olaraq RSA, DSA, ECDSA, ElGamal, Şnorr, QOST R 34.10-2001 və s. alqoritmlərini göstərmək olar. Rəqəmsal imzanın iş prinsipi. Açıq açarlı kriptoqrafiya əsasında rəqəmsal imzanın iş prinsipinə baxaq. Tutaq ki, hər hansı A istifadəçisi müəyyən məlumatı imzalamalıdır. Bunun üçün o, heş-funksiyanın köməyi ilə bu məlumatın heş-kodunu hesablayır və onu özünün gizli açarı ilə şifrləyir. Şifrlənmiş heş-kod məlumata əlavə edilir. Beləliklə, məlumatın rəqəmsal imzası alınır. İmzanın yaradılması şəkil 4-də göstərilib.

Sistemin istənilən iştirakçısı imzalanmış sənədi aldıqda A istifadəçisinin imzasını yoxlaya bilər. Bunun üçün o, heş-funksiyanın köməyi ilə alınmış məlumatın heş-kodunu yaradır. Sonra məlumata birləşdirilmiş şifrlənmiş heş-kodu A istifadəçisinin açıq açarı ilə deşifrə edir və alınmış deşifrə edilmiş heş-kodu özünün yaratdığı heş-kodla müqayisə edir. Onlar üst-üstə düşürlərsə, imza həqiqi hesab olunur. Əks halda imza rədd olunur. Gizli açar yalnız A istifadəçisinə məxsus olduğundan

aydındır ki, məlumatı da yalnız o imzalaya bilərdi. İmzanın yoxlanması şəkil 5-də göstərilib

Elektron hökumət - hər hansı bir ölkənin dövlət strukturlarının haması haqqında məlumatların hər bir vətəndaş üçün açıq olan şəbəkədə yerləşdirilməsi deməkdir. Yəni hər bir vətəndaş hər hansı bir nazirlik və komitədən tutmuş, mənzil-təsərrüfat idarəsi ilə məktəbə qədər olan idarənin mövcud durumu, bu qurumlara müraciət etmənin qaydalarını istənilən vaxt əldə edə və bu təşkilatlara elə elektron rabitə vasitəsilə müraciət edə bilər.

Mütəxəssislər hesab edirlər ki, "elektron hökumət"in qurulması ölkədə hakimiyyət strukturlarının şəffaf fəaliyyət göstərməsinə gətirəcək. Dünyanın inkişaf etmiş ölkələrinin əksəriyyətində "elektron hökumət" fəaliyyət göstərir. Azərbaycanda "elektron hökumət" layihəsi "Elektron Azərbaycan" dövlət proqramı çərçivəsində həyata keçirilir.

Azərbaycan MDB məkanında "elektron hökumət" layihəsi üzərində işlərin aparıldığı 4-cü ölkədir. Hazırda həyata keçirilən proqram ölkədə "elektron hökumət"in qurulmasının hazırlıq işlərinin 2008-ci ildə bitəcəyini və bundan sonra daha 4 il ərzində həyata keçəcəyini nəzərdə tutur. Mütəxəssislərin fikrincə, Azərbaycan cəmiyyətində olan kompüter və informasiyadan istifadə mədəniyyəti elektron hökumətinin qurulması üçün bir qədər daha da inkişaf etməlidir.

Elektron imza – elektron formada olan verilənlər yığımıdır, digər verilənlərlə (elektron sənəd, proqram faylları və s.) məntiqi əlaqəli olur və bu verilənlər yığımını yaradan (generasiya edən) şəxsi birqiymətli identifikasiya etməyə imkan verir.

Elektron rəqəm imzas. Elektron imzanın növlərindən biridir, asimmetrik şifrələməyə əsaslanan texnologiyadan ibarətdir. Rəqəm imzası konkret məlumata (mətnə, fayla və ya ixtiyari uzunluqlu istənilən bitlər yığımına) əlavə olunan və xüsusi: məlumatın müəllifinin identifikasiyası və autentikasiyası; məlumatın bütövlüyünün təsdiqi (sanksiyasız

dəyişilmələrin yoxluğu); məlumatın müəllifliyindən imtinanın qeyri-mümkünlüyünə zəmanət kimi şərtləri təmin etməyə imkan verən qeyd olunmuş (sabit) uzunluqlu informasiya blokudur.

Fiziki şəxsin əllə yazılmış imzasının analoqu olub, bağlı ERİ açarından istifadə etməklə elektron verilənlərin kriptoqrafik dəyişmə nəticəsində simvollar ardıcıllığı kimi təsvir edilir. Bağlı ERİ açarı açıq ERİ açar istifadəçisinin informasiyanın tamlığını və dəyişməzliyini təyin etməyə şərait yaradır.

Elektron imza Elektron dünyada şəxsiyyəti müəyyənləşdirmə vasitəsidir.

Elektron imza anlayışı ümumi xarakter daşıyıb, insanların əl imzalarının rəqəmli çeviricilərdən keçirilmiş, barmaq izləri, səs kimi bioloji əlamətlərinin rəqəmli çeviricilərdən keçirilmiş və s. biometrik əlamətlərin elektron halda kimliklərinin doğrulanmasını təmin edən vasitədir.

Elektron imza və elektron sənəd haqqında Azərbaycan Respublikasının Qanunu – Maddə 1

“Elektron imza - digər verilənlərə əlavə edilən və ya onlarla məntiqi əlaqəli olan, imza sahibini identikləşdirməyə imkan verən verilənlərdir”

Maddə 1, bənd 1.1.3:

“Gücləndirilmiş elektron imza (bundan sonra - gücləndirilmiş imza) - imza sahibinin nəzarəti altında olan elektron imza vasitələri ilə yaradılan və yalnız imza sahibinə məxsus olmaqla onu identikləşdirən, əlaqəli olduğu məlumat bildirişinin bütövlüyünü, dəyişməzliyini, təhrif olunmadığını və saxtalaşdırılmadığını müəyyən etməyə imkan verən elektron imzadır”

Maddə 3, bənd 3.5:

“Azərbaycan Respublikasının qanunvericiliyi ilə sənədin notariat qaydasında təsdiqi və (və ya) dövlət qeydiyyatı tələb olunduğu hallar istisna olmaqla, elektron sənəd kağız daşıyıcıda olan sənədə bərabər tutulur və onunla eyni hüquqi qüvvəyə malikdir”

Gücləndirilmiş e-imzanın üstünlükləri:

- gizlilik (confidentiality);
- bütünlük (integrity);
- tanınma (authentication);
- Məsuliyyətdən yayinmanın mümkünsüzlüyü (non-repudiation).

İnformasiya cəhətdən inkişaf etmiş ölkələrin əksəriyyətində elektron imzadan istifadə olunması ilə əlaqədar fəaliyyətlər səlahiyyətli orqan vasitəsilə hökumət tərəfindən tənzimlənir.

Almaniyada səlahiyyətli orqan telekommunikasiya və poçt rabitəsi sahəsində tənzimləmə və nəzarət üzrə dövlət orqanıdır (RegTP).

Okinava xartiyasında müəyyən olunmuş əsas prinsip və yanaşma:

1. Milli qanunvericilik bir neçə vahid qanun şəklində olmalı, həmçinin beynəlxalq və şəffaf xarakter daşımalıdır;
2. Avropa Parlamentinin elektron imza barədə 1999-cu il tarixli Direktivi:
3. Etibarlı elektron imza vasitələrinin köməyilə yaradılmış və etibarlılığı təsdiq olunmuş elektron imzalar üçün aşağıdakılara dair zəmanət verilməlidir:
4. Elektron imza kağız üzərindəki əl imzasına bərabər tutulmalıdır;
5. Elektron imza məhkəmə sübutu kimi qəbul olunmalıdır;
6. AB-nin üzvü olan dövlətlər Direktivə uyğun qanunlar və qanunvericilik aktları qəbul etməlidir

2003-cü ildə Avropa parlamentinin komissiyası Avropa Birliyində elektron imzadan istifadə olunmasına dair vahid metodoloji və texnoloji yanaşma ilə əlaqədar qərar dərc etmişdir. Həmin qərarda EESSI (Elektron imzanın standartlaşdırılmasına dair Avropa təşəbbüsü) çərçivəsində CEN (Avropa standartlaşdırma komitəsi) və ETSİ (Avropa telekommunikasiya standartları institutu) tərəfindən işlənib hazırlanmış texniki standartların elektron imzanın tətbiqində istifadə olunması təklif edilir

Standartlar:

- CWA 14167-1 (mart 2003): elektron imza sertifikatlarının idarə olunması üzrə etibarlı sistemlərin təhlükəsizliyinə dair tələblər – 1-ci Hissə: Sistemin təhlükəsizliyinə dair tələblər;

- CWA 14167-2 (mart 2002): elektron imza sertifikatlarının idarə olunması üzrə etibarlı sistemlərin təhlükəsizliyinə dair tələblər – 2-ci Hissə: elektron imzanın yaradılması üçün kriptoqrafik modul: imzanın təsdiqlənməsi ilə məşğul olan qurumlar tərəfindən istifadə olunur – Müdafiə profili;
- CWA 14169 (mart 2002): elektron imzanın yaradılması üçün təhlükəsiz qurğular (kriptoqrafik açarların yaradılmasına, saxlanılmasına və istifadəsinə dair tələblər daxil olmaqla).

Avropa ölkələrinin əksəriyyətində etibarlı (tam) şəhadətnamələrin verilməsi ilə məşğul olan təsdiqləyici mərkəzlərə dair tələblər müəyyən olunur (məhz bu sertifikatlardan istifadə olunması əllə qeyd edilmiş imzaların elektron imzalarla eyni qüvvəyə malik olmasını və «Elektron imza və elektron sənəd barədə» qanuna uyğun olmasını təmin edir).

Mərkəzlər elektron imzanın yaradılması üçün konkret bir ölkədə yoxlanılmış və sertifikatlaşdırılmış proqram-texniki vasitələrdən istifadə edirlər.

MÖVZU

Dağıdıcı proqram təsiri

Kompüter virusları. Kompüter virusları təxminən 1980-ci illərin əvvəllərində meydana çıxmışdır. «Kompüter virusu» termini 1984-cü ildə ABŞ-da keçirilən informasiya təhlükəsizliyi üzrə 7-ci konfransda Fred Koen tərəfindən işlədilmişdi. Kompüter viruslarının ümumi qəbul edilmiş tərifi yoxdur. Biz aşağıdakı tərifdən istifadə edəcəyik.

Kompüter virusu – elə proqramdır ki, özünü təxminən bioloji virus kimi aparır: çoxalır, maskalanır və ziyanlı təsirlər göstərir (əməliyyatlar yerinə yetirir).

Virusları aşağıdakı əlamətlərə görə təsnif etmək olar:

yaşayış mühitinə görə: fayl virusları (com, exe, bat, doc virusları), yükləmə virusları, makro viruslar;

yaşayış mühitini yoluxdurma üsuluna görə: rezident və qeyri-rezident;

əməliyyat sisteminə görə: MS-DOS virusları, Windows virusları, *NIX virusları və s.;

destruktiv imkanlarına görə: ziyansız, təhlükəsiz, təhlükəli, çox təhlükəli;

virus alqoritminin xüsusiyyətlərinə görə: «tələbə» virusları, kompanyon-viruslar, «soxulcanlar» (worm), «stels»-viruslar («görünməz» viruslar), «polimorf»-viruslar (özüşifrlənən viruslar), şəbəkə virusları və s.

Virusların yaradılması. Hər gün 10-15 yeni növ virus meydana çıxır. Virusların miqdarı həndəsi silsilə üzrə artır. Bunu statistika və real həyat təsdiq edir. 1990-cı ildə təxminən 500 virus, 1992-ci ildə - 3 000, 1994-cü ildə - 5 000, 1996 – 9 000, 1999 – 30 000, 2001 – 50 000, 2004-cü ildə 112 000-dən çox virus məlum idi.

Kompüter viruslarının sayının artması ilk növbədə onunla bağlıdır ki, proqramlaşdırmanı bir qədər öyrəndikdən sonra istənilən şəxs virus yaza bilər. Bu işdə ona leqal və qeyri-leqal ədəbiyyat, virusların yazılması üçün xüsusi proqram təminatı kömək edə bilər. Hətta müxtəlif mutasiya generatorları mövcuddur ki, onun köməyi ilə birinci kurs tələbəsinin yaratdığı sadə virusdan mürəkkəb virus yaratmaq olar.

Virusların yayılması. Şəbəkə və kommunikasiya texnologiyalarında hər bir yenilik virusların yaradılması və yayılması üçün yeni imkanlar, yollar açır. Yaxın vaxtlara kimi viruslar disketlər və digər daşıyıcılar vasitəsi ilə yayılırdı, İnternet viruslar üçün geniş magistral açdı. Kompüter virusları Internetdə bioloji virusların real dünyada yayılmasından daha sürətlə yayılır. 2003-cü ildə Slammer "soxulcanı" 10 dəqiqə ərzində 75 min kompüter yoluxdurmuşdu.

1999-cu ildə ilk dəfə dünya miqyasında virus epidemiyası baş verdi: Melissa virusu on minlərlə kompüteri yoluxdurdu və 80 milyon dollar ziyan vurdu. Bu insidentdən sonra dünyada antivirus proqramlara böyük tələbat yarandı. 2000-ci ilin mayında Melissanın rekordunu bir neçə saat ərzində milyonlarla kompüteri yoluxdurmuş I Love You! virusu təzələdi.

Praktik olaraq virusla "yoluxdurmaq" mümkün olmayan fayl növü qalmamışdır. Artıq mobil telefonları və proqram təminatından istifadə edən digər qurğuları yoluxduran viruslar da sürətlə yayılır.

Virus müəllifləri təkcə texnoloji zəifliklərdən deyil, "psixoloji" zəifliklərdən də istifadə edirlər. Tədqiqatlar göstərmişdir ki, Anna Kournikova, Sean Connery, Julia Roberts, Elvis Presley Lives, Explicit Hot Porn kimi viruslardan əziyyət çəkmiş hər beşinci İnternet istifadəçisi edilmiş xəbərdarlıqlara baxmayaraq həmin adlı qoşma faylları açmışdılar.

Antivirus proqramlarının növləri. Viruslarla mübarizə proqramlarının bir neçə növü var - skanerlər (başqa adı: faqlar, polifaqlar), disk müfəttişləri (CRC-skanerlər), rezident monitorlar və immunizatorlar.

Antivirus skanerlərin iş prinsipi faylların və sistem yaddaşının yoxlanmasına və onlarda məlum və ya yeni (skanerə məlum olmayan) virusların axtarışına əsaslanır. Məlum virusların axtarışı üçün «maska»lardan istifadə edilir. Virusun maskası konkret virus üçün spesifik olan müəyyən sabit kodlar ardıcıllığıdır. Bir çox skanerlərdə həmçinin «evristik skanlama» alqoritmlərindən istifadə edilir, yəni yoxlanan obyektdə komandalar ardıcıllığı analiz edilir, müəyyən statistika toplanır və hər bir yoxlanan obyekt üçün qərar qəbul edilir («ola bilsin yoluxub» və ya «yoluxmayıb»).

Disk müfəttişlərinin (CRC-skanerlərin) iş prinsipi diskdə olan fayllar və sistem sektorları üçün CRC-cəmlərin (nəzarət cəmlərinin) hesablanmasına əsaslanıb.

Rezident monitorlar - daim operativ yaddaşda yerləşən və disklə və operativ yaddaşla aparılan əməliyyatlara nəzarət edən proqramlardır. Məhz bu proqramlar sistemin real yoluxma anına kimi virusu aşkarlamağa imkan verir (əvvəlki ikisindən fərqli olaraq).

İmmunizatorların iki növü var: yoluxma barədə məlumat verən immunizatorlar və hər-hansı növ virusla yoluxmanın qarşısını alan immunizatorlar. Onlardan birincisi adətən faylların sonuna yazılır və hər dəfə fayl işlədikdə onun dəyişməsini yoxlayır. Bu immunizatorların bir nöqsanı var – stels-virusla yoluxma barədə məlumat verməyə qabil deyil. Buna görə bu immunizatorlar hazırda praktikada istifadə edilmir. İkinci növ immunizator sistemi hər hansı müəyyən növ virusla yoluxmaqdan mühafizə edir. Diskdə fayllar elə modifikasiya edilir ki, virus onları artıq yoluxmuş fayl kimi qəbul edir. Rezident virusdan

mühafizə üçün kompüterin yaddaşına virusu imitasiya edən proqram yüklənir. Virus işə düşdükdə onunla rastlaşır və hesab edir ki, sistem artıq yoluxub.

MÖVZU

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

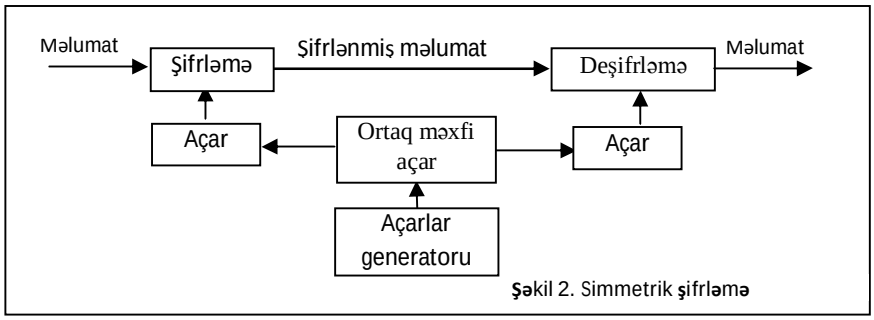
Şifrləmə zamanı A hərfi D hərfi ilə, B hərfi E ilə və beləcə əvəz olunurdu. Məsələn: VENI VIDI VICI $\rightarrow$ YHQL YLGL YLFL. Şifrlənmiş məlumatı alan hərfləri ikinci sətirdə axtarırdı və onların üstündəki hərflərə görə ilkin mətni bərpa edirdi. Sezar şifrində açar əlifbanın ikinci sətrindəki sürüşmənin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

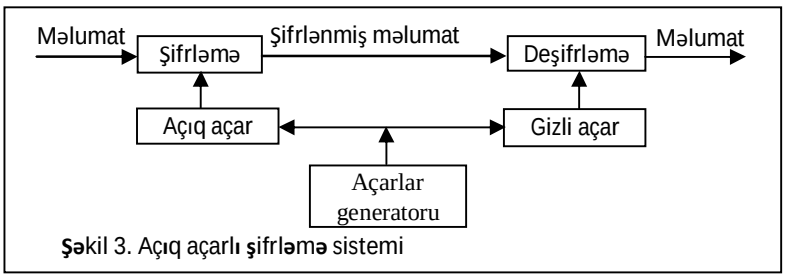
Simmetrik şifrləmənin əsas nöqsanı ondan ibarətdir ki, məxfi açar həm göndərənə, həm də alana məlum olmalıdır. Bu bir tərəfdən məxfi açarların tam məxfi kanalla göndərilməsi problemini yaradır. Digər tərəfdən alan tərəf şifrlənmiş və deşifrlənmiş məlumatın varlığı əsasında bu məlumatı konkret göndərəndən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

Asimmetrik kriptoqrafiyada iki açardan istifadə olunur. Onlardan biri – açıq açar (sahibinin ünvanı ilə birlikdə nəşr oluna bilər) şifrləmə üçün istifadə olunur, digəri – gizli açar (yalnız alana məlum) deşifrləmə üçün istifadə olunur. Rəqəmsal imza alqoritmlərində gizli açar şifrləmə, açıq açar isə deşifrləmə üçün istifadə edilir. Açıq açara görə uyğun gizli açarın tapılması çox böyük həcmdə hesablamalar tələb edir, hesablama texnikasının hazırki inkişaf səviyyəsində bu



Şəkil 2. Simmetrik **şi**frləmə

məsələ qeyri-mümkün hesab edilir. Şəkil 3 asimmetrik şifrləmə sisteminin istifadəsini illüstrasiya edir. Asimmetrik şifrləmə alqoritmlərinə misal olaraq RSA, ElGamal, Şnorr və s. alqoritmlərini göstərmək olar.



Şəkil 3. Açıq açarlı **şi**frləmə sistemi

Asimmetrik kriptoqrafiyanın əsas çatışmayan cəhəti sürətin aşağı olmasıdır. Buna görə onlar simmetrik metodlarla birgə işlədilir. Məsələn, açarların göndərilməsi məsələsini həll etmək üçün əvvəlcə məlumat təsadüfi açarla simmetrik metodla şifrlənir, sonra həmin təsadüfi açarı alan tərəfin açıq asimmetrik açarı ilə şifrləyirlər, bundan sonra məlumat və şifrlənmiş açar şəbəkə ilə ötürülür.

Asimmetrik metodlardan istifadə etdikdə, (*istifadəçi*, *açıq açar*) cütünün həqiqiliyinə zəmanət tələb olunur. Bu məsələnin həlli üçün *rəqəmsal sertifikatdan* istifadə edilir. Rəqəmsal sertifikat xüsusi *sertifikat xidməti mərkəzləri* tərəfindən verilir. Rəqəmsal sertifikatda aşağıdakı verilənlər olur: sertifikatın seriya nömrəsi; sertifikatın sahibinin adı; sertifikatın sahibinin açıq açarı; sertifikatın fəaliyyət müddəti; elektron imza alqoritminin identifikatoru; sertifikat xidməti mərkəzinin adı və s. Sertifikat onu verən sertifikat xidməti mərkəzinin rəqəmsal imzası ilə təsdiq edilir.

Tamlığa nəzarət üçün kriptoqrafik *heş-funksiyalar* istifadə edilir. Heş-funksiya adətən müəyyən alqoritm şəklində realizə edilir, belə alqoritm ixtiyari uzunluqlu məlumat üçün uzunluğu sabit heş-kod hesablamağa imkan verir. Praktikada 128 bit və daha artıq uzunluqda heş-kod generasiya edən heş-funksiyalardan istifadə edilir.

Heş-funksiyanın xassələri elədir ki, onun köməyi ilə alınan heş-kod məlumatla "möhkəm" bağlı olur. Məlumatın hətta bir biti dəyişdikdə belə heş-kodun bitlərinin yarısı dəyişir. Heş-funksiyaya misal olaraq MD2, MD4, MD5, RIPEMD, SHA1 və s. alqoritmlərini göstərmək olar.

Misal. '1234567890' sətri üçün SHA1 heş-funksiya alqoritminin hesabladığı heş-kod 16-lıq say sistemində 01B307ACBA4F54F55AAFC33BB06BBBF6CA803E9A simvollar ardıcıllığıdır.

Ədəbiyyat

1. Галатенко В.А. Основы информационной безопасности, Москва, 2004. – 264 с.

2. Əliquliyev R.M., İmamverdiyev Y.N. Rəqəm imzası texnologiyası, Bakı, Elm, 2003. – 132 с.

3. E.B.Gözəlov. Energetikanın menecmentində kommunikasiya texnikası.-Bakı,AzTu., 2007-179 .

4. E.B.Gözəlov. Energetikanın menecmentində informasiya sistemləri.Dərs vəsaiti.-Bakı, STX-Print. 2007-91 s.

5. С.В.Кунегин. Системы передачи информации.- М.:Радио и связь,1998

6. Кульгин М. " Технологии корпоративных сетей", "Питер",2000г.

7. Марк А.Спортак , Франк Ч.Паппас и др. Высокопроизводительные сети. Киев: ДиаСофт,1998
8. Золотов С.Протоколы Internet.- СПб.:BHV- Санкт – Петербург,1998
9. Фролов А.В., Фролов Г.В. Глобальные сети компьютеров. М.: ДИАЛОГ-МИФИ,1996
10. Компьютерные сети\ В.Г.Олифер – СПб.:Питер ,2001