AZƏRBAYCAN TEXNİKİ UNİVERSİTETİNİN nəzdində

BAKI TEXNİKİ KOLLECİ

“İnformasiya təhlükəsizliyinin əsasları” fənnindən

Mühazirələr konspekti

Mündəricat

Giriş

Bu gün təhlükəsizliyin təmin edilməsi bütövlükdə bəşəriyyətin ən əsas və qlobal problemlərindən biridir. Adi həyatda təhlükəsizlik anlayışı özündə normal (təhlükəsiz) yaşayış, iş, məişət, istirahət şəraitinin təmin olunmasını ehtiva edir. Bütövlükdə isə *təhlükəsizlik* – havanın təmizliyi, ərzağın və suyun keyfiyyəti, mənzil şəraiti, kriminala və terrorçuluğa qarşı effektiv mübarizə, nəqliyyatda, küçədə və ictimai yerlərdə təhlükəsizlik, tibbi təminatın və sosial müdafiənin səviyyəsi, xidmət sahə-lərində mənəvi-etik mühitin yaradılması, əməkhaqqının sərf edilən əməyə uyğunluğu və s. ilə xarakterizə olunur.

Milli təhlükəsizlik termini rəsmi olaraq ilk dəfə 1947-ci ildə ABŞ-da meydana gəlmişdir. Həmin dövrdə ABŞ-da prezidentin milli məsələlər üzrə xüsusi köməkçisi dövlət vəzifəsi təsis edilmiş və Milli Təhlükəsizlik Şurası yaradılmışdır.

Milli təhlükəsizlik – milli maraqların ona yönəlmiş təhdidlərdən qorunmasının təmin edilməsidir.

Özündə şəxsin, təşkilatın, cəmiyyətin və dövlətin mühüm (həyat əhəmiyyətli) maraqlarının daxili və xarici təh-didlərdən qorunması vəziyyətini ehtiva edən təhlükəsizlik aşağıdakı komponentlərlə xarakterizə olunur:

- personal;
- maddi və maliyyə vəsaitləri; - informasiya.

Yaranmış təhdidlər bu komponentlərdən birinə təsir etməklə digər komponentlər və bütövlükdə obyekt üçün təhlükə yaradır. İnformasiya təhdidləri isə obyektə və onun təhlükəsizliyinin digər komponentlərinə təsiri, bir qayda olaraq, onun informasiya mühitinə, o cümlədən informa-siyasına və informasiya ehtiyatlarına təsir vasitəsilə həyata keçirir.

Sovet İttifaqı dağıldıqdan sonra müstəqillik qazanmış Azərbaycan Respublikası sosializmdən yeni münasibət formasına keçid dövründə iqtisadi, siyasi-sosial və hərbi böhranlarla müşayiət olunan bir sıra problemlərlə üzləşdi. Bu problemlər respublikanın iqtisadiyyatının səviyyəsinin aşağı düşməsinə, əhalinin həyat səviyyəsinin pisləşməsinə, elm, təhsil və tibb sahəsində böhranlı vəziyyətin yaran-masına, Azərbaycanın sərhədlərinin pozulmasına və mü-haribənin baş verməsinə gətirib çıxardı.

Respublikanı belə böhranlı vəziyyətdən çıxarmaq məq-sədilə ölkə rəhbərliyi tərəfindən daxili və xarici təhlükə-sizliyin təmin olunması, regional və beynəlxalq təhlükə-sizlik üzrə tədbirlərdə iştirak edilməsi, iqtisadiyyatın, sosial vəziyyətin, elmin, təhsilin, mədəniyyətin səviyyə-sinin yüksəldilməsi istiqamətində atılan addımlar Azər-baycanın müstəqilliyinin və dövlətçiliyinin qorunması, milli təhlükəsizliyinin təmin edilməsinə yönəlmişdir.

Azərbaycan Respublikasının milli təhlükəsizliyi məsələləri və milli maraqları Azərbaycan Respublikasının Konstitusiyası, Milli Təhlükəsizlik Konsepsiyası və "Milli təhlükəsizlik haqqında" Azərbaycan Respublikasının Qa-nunu ilə müəyyən olunmuşdur.

3 avqust 2004-cü ildə qəbul edilmiş “Milli təhlükəsizlik haqqında” Azərbaycan Respublikasının Qanununda qeyd olunur ki, *Azərbaycan Respublikasının milli təhlükəsizliyi* – dövlətin müstəqilliyinin, suverenliyinin, ərazi bütövlü-yünün, konstitusiya quruluşunun, xalqın və ölkənin milli maraqlarının, insanın, cəmiyyətin və dövlətin hüquq və mənafelərinin daxili və xarici təhdidlərdən qorunmasının təmin edilməsidir.

Azərbaycan Respublikasının milli maraqları dedikdə Azərbaycan xalqının fundamental dəyər və məqsədlərini, habelə insanın, cəmiyyətin və dövlətin inkişaf və tərəqqisini təmin ed$_ə$n siyasi, iqtisadi, sosial, hərbi, informasiya, ekoloji, elm, t$_ə$hsil, m$_ə$d$_ə$ni v$_ə$ m$_ə$n$_ə$vi tələbatları nəzərdə tutulur.

Qeyd olunduğu kimi, informasiya cəmiyyətinin for-malaşması və inkişafı prosesində insan fəaliyyətinin bütün sahələrində müxtəlif informasiya-kommunikasiya texno-logiyaları (İKT) işlənib hazırlanır və tətbiq edilir. İnfor-masiya və informasiya ehtiyatları insanın, cəmiyyətin və dövlətin inkişafının həlledici amillərindən birinə çevril-mişdir. İKT-nin, o cümlədən kompüter texnikasının geniş imkanları dövlət, iqtisadiyyat, sosial, müdafiə və digər sahələrdə obyekt və sistemlərin monitorinqi və idarə olun-ması proseslərini avtomatlaşdırmağa, bu proseslər haqqında böyük həcmdə məlumatları yüksək sürətlə almağa, toplamağa, emal etməyə və ötürməyə imkan verir. Belə-liklə, tam əminliklə demək olar ki, bu gün informasi-yalaşdırma bəşəriyyətin inkişafında müsbət həlledici rol oynayır.

Qeyd etmək lazımdır ki, elmi nailiyyətlər, o cümlədən müasir informasiya texnologiyalarının imkanları heç də həmişə insanların, cəmiyyətin və dövlətin maraqları baxımından istifadə olunmur. Belə ki, ayrı-ayrı insanlar, təşkilatlar, dövlətlər və onların birlikləri tərəfindən öz maraqlarının ödənilməsi, eləcə də iqtisadi, kommersiya, hərbi qarşıdurmada ehtimal olunan rəqiblərinin maraq-larına əks təsir (müqavimət) göstərmək məqsədilə infor-masiyanı, informasiya ehtiyatlarını, vasitələrini və texno-logiyalarını əldə etməyə can atması təbiidir. Göründüyü kimi, informasiya, informasiya ehtiyatları və İKT rəqib tərəflərin maraqlarına müəyyən təhdidlər qismində çıxış edir. Qeyd olunan vəziyyət informasiya təhlükəsizliyi problemini doğurur. İnformasiya təhlükəsiz-liyinin konseptual və elmi metodiki əsasları son dövrlərdə işlənib hazırlanmağa başlanmışdır. Ona görə də, termi-nologiyanın dəqiqləşdirilməsi, informasiya təhlükəsizliyi probleminin elmi əsaslandırılması, bu sahədə həyati vacib maraqların və informasiya təhdidlərinin mənbələrinin təsnif edilməsi, informasiya təhlükəsizliyinin göstəriciləri, meyarları, normativləri, eləcə də digər xarakteristika və xassələri elmi-tədqiqat obyekti kimi gələcəkdə hələ çox tədqiqatların mövzusu olacaqdır.

İnformasiya təhlükəsizliyi, informasiya təhlükəsi, infor-masiya təhdidləri, informasiyanın qorunması, informasiya maraqları, informasiya mühiti və s. baza anlayışlarının da daxil olduğu anlayışlar sisteminin yaradılması informasiya təhlükəsizliyi nəzəriyyəsinin yaradılmasının ilk məsələlə-rindən biridir.

Qeyd etmək lazımdır ki, təhlükəsizlik heç də həmişə qoruma nəticəsində təmin edilmir. Belə ki, təhlükəsizlik obyektlərin uyğun davranış və qarşılıqlı əlaqə qaydalarına riayət olunması, yüksək peşəkar personalın hazırlanması, texnikanın işinin sazlığının və informasiya təhlükəsizliyi obyektlərinin fəaliyyətinin etibarlılığının təmin edilməsi yolu ilə əldə oluna bilər.

1. İnformasiya təhlükəsizliyi anlayışı və əsasları

İnformasiya təhlükəsizliyi probleminin daha ətraflı şərhinə keçməzdən əvvəl, informasiya cəmiyyətinin əsasını təşkil edən informasiya anlayışı haqqında məlumatın verilməsi zəruridir. Belə ki, informasiya anlayışı olduqca geniş və müxtəlif anlamlarda işlədilir. Elə fəaliyyət sahəsi tapmaq mümkün deyil ki, orada informasiya anlayışı istifadə olunmasın. Burada informasiya anlayışı aşağıdakı kimi başa düşülür.

İnformasiya - təqdimat formasından asılı olmayaraq şəxslər, əşyalar, faktlar, hadisələr, təzahürlər, proseslər və anlayışlar haqqında məlumatlar və biliklərdir.

İnformasiya kompüterə daxil edilmiş verilənlər, proqram kodları, məktub, yaddaş qeydləri, işlər, düsturlar,sxemlər, çertyojlar, diaqramlar, dissertasiyalar, məhkəmə sənədləri və s. formalarda ola bilər.

İnformasiya proseslərinə — informasiyanın toplanması, ötürülməsi, saxlanması, emalı və istifadəçiyə çatdırılması aiddir.

İnformasiyanın toplanması öyrənilən obyektin vəziyyəti haqqında məlumatın alınması məqsədi ilə aparılır. İnformasiyanın toplanması adi halda insan tərəfindən, avtomatlaşdırılmış halda isə texniki vasitələr və sistemlər tərəfindən yerinə yetirilir.

İnformasiyanın ötürülməsi — toplanan informasiyanın emal edilməsi üçün emal vasitələri ilə ötürülməni nəzərdə tutur. Adi halda informasiyanın emalı insan tərəfindən, avtomatlaşdırılmış halda isə kompüterlər vasitələrlə aparılır. İnformasiyanın ötürülməsi məsafədən asılı olaraq müxtəlif vasitələrlə yerinə yetirilə bilər. Yaxın məsafəli ötürmələrdə kabellərdən, uzaq məsafəli ötürmələrdə isə rabitə kanallarından (telefon, teleqraf, peyk rabitəsi və s.) istifadə edilir. Müasir kompüterlərdə informasiyanın telefon kanalı vasitəsilə uzaq məsafədən qəbulu və ötürülməsi üçün modem (modulyator - demodulyator) adlanan xüsusi qurğudan istifadə edilir.

İnformasiyanın saxlanması — informasiya emal edilməzdən əvvəl və sonra daşıyıcılarda saxlanılmasını nəzərdə tutur. İnformasiya daşıyıcısı kimi kağızdan,

köhnə kompüterlərdə perfolentdən, perfokartdan, maqnit lentindən, müasir kompüterlərdə isə maqnit və lazer disklərindən və kartlardan istifadə olunur.

İnformasiyanın axtarışı və emalı adi halda insan tərəfindən, avtomatlaşdırılmış halda isə kompüter vasitəsilə aparılır.

İnformasiyanın emalı başqa sözlə qarşıya qoyulan məsələnin həlli deməkdir. Bunun üçün əvvəldən hazırlanmış alqoritmlərdən və proqramlardan istifadə olunur. İnformasiyanın emalından alınan nəticələr tələb olunan formada istifadəçilərə çatdırılır. Avtomatlaşdırılmış üsulla (kompüterlə) emal olunan informasiya istifadəçilərə adətən kompüterin xaricetmə qurğuları ilə (monitor, printer, plotter və s.) mətn, cədvəl, qrafik və s. şəklində çatdırılır.

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 mühafizəsi – informasiya təhlükəsizliyinin təmin olunmasına yönəlmiş tədbirlər kompleksidir.

İnformasiya təhlükəsizliyi dedikdə təhlükəsizliyin pozulmasına gətirib çıxaran şərait və hərəkətlərin vaxtında aşkar edilməsi və qarşısının alınması başa düşülür.

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 tələbatı - qeyri-maddi tələbatların bir növü olub özündə konkret

məsələnin həlli və ya hər hansı məqsədin əldə olunması üçün zəruri olan informasiya tələbatı əhatə edir.

İnformasiya təhlükəsizliyi sahəsində anlayışlara mövzu sahəsindən asılı olaraq bir neçə aspektdən yanaşılır və müxtəlif ədəbiyyatlarda informasiya təhlükəsizliyi sahəsində mövcud anlayışlara müxtəlif təriflər verilir. Ona görə də burada bəzi anlayışların bir neçə tərifi verilmişdir. Konteksdən asılı olaraq bu təriflərdən biri istifadə olunur.

İnformasiya təhlükəsizliyi – informasiya mühitində dövlətin, fiziki və hüquqi şəxslərin qorunmasının vəziyyətidir.

İnformasiyanın qorunması – informasiyanın gizliliyinin, tamlığının və ona girişin (əlyetərliliyin) təmin edilməsinə yönəlmiş fəaliyyətdir.

İnformasiyanın qorunmasının məqsədləri aşağıdakılar-dan ibarətdir:

- dövlətin, ictimaiyyətin, vətəndaşların təhlükəsizliyi-nin təmin edilməsi; - dövlət sirri təşkil edən və məxfi informasiyanın məx-filiyinin qorunması;
- informasiyanın məhvinin, itməsinin, təhrif edilməsi-nin, saxtalaşdırılmasının, surətinin çıxarılmasının, təc-rid edilməsinin qarşısının alınması;
- informasiya proseslərində və informasiya sistemləri-nin, texnologiyalarının və onların təminat vasitələrinin işlənməsi, istehsalı, tətbiqi zamanı fiziki və hüquqi şəxslərin hüquqlarının təmin olunması.

İnformasiya təhlükəsi anlayışına iki mənada – təhlükəni yaradan və təhlükəyə məruz qalan obyektlər baxımından tərif verilir.

İnformasiya təhlükəsi – informasiya mühitinə təsir et-mək yolu ilə əhəmiyyətli zərər və ya ziyan vura biləcək imkanların mövcud olduğu obyektin və ya onun ətraf mü-hitinin vəziyyətidir.

İnformasiya təhlükəsi – obyektin hər hansı başqa ob-yektin informasiya mühitinə təsir etməklə ona əhəmiyyətli zərər və ya ziyan vura bilmək qabiliyyətini xarakterizə edən xassəsidir.

Praktikada informasiya təhlükəsi anlayışı ilə yanaşı informasiya təhdidi anlayışından da istifadə olunur. Bu anlayışlar bəzən səhvən eyniləşdirilir. Lakin qeyd olun-malıdır ki, bu anlayışlar tamamilə fərqli mahiyyətə ma-likdirlər və onları eyniləşdirmək olmaz.

İnformasiya təhdidi – obyektin hər hansı başqa obyektin informasiya mühitinə təsir etmək yolu ilə ona əhəmiyyətli zərər vurmaq niyyəti, yəni həmin obyektə qarşı yaratdığı təhlükədir. Başqa sözlə, informasiya təhdidi dedikdə obyekt üçün informasiya təhlükəsi yaradan amil və ya amillər toplusu başa düşülür.

2. Informasiya təhlükəsizliyi, standart təyinatları

İnformasiya təhlükəsizliyi dedikdə təhlükəsizliyin pozulmasına gətirib çıxaran şərait və hərəkətlərin vaxtında aşkar edilməsi və qarşısının alınması başa düşülür.

İnformasiyanın qorunması — informasiyanın gizliliyinin, tamlığının və ona girişin (əlyetənliliyin) təmin edilməsidir.

İnformasiyanın qorunmasının məqsədləri aşağıdakılardan ibarətdir:

- dövlətin, ictimaiyyətin, vətəndaşların təhlükəsizliyinin təmin edilməsi;
- dövlət sirri təşkil edən və məxfi informasiyanın məxfiliyinin qorunması;
- informasiyanın məhvinin, itməsinin, təhrif edilməsinin, saxtalaşdırılmasının, surətinin çıxarılmasının, qarşısının alınması;

INFORMASIYA-T**İnformasiya təhlükəsizliyi üzrə standartlar** 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 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.

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.

3.Informasiya təhlükəsizliyinin təmini üsulları

"Kasperski Laboratoriyası" informasiya təhlükəsizliyinin sistemlərinin hazırlaması sahəsində fəaliyyət göstərən Rusiya şirkəti. Yaradıcısı Yevgeni Kasperskidir.

"Kasperiski laboratoriyası" ekspertlərinin fikrincə informasiya təhlükəsizliyi məsələləri sistemli həll olunmalıdır. Bu o deməkdir ki, müxtəlif mühafizə vasitələri (aparat, proqram, fiziki, təşkilati və s.) eyni vaxtda mərkəzi idarə olunmaqla tətbiq olunmalıdır. Bu zaman sistemin mühafizə vasitələri bir-birinin mövcüd olmasını bilməli, qarşılıqlı təsirli olmalı və həm xarici, həm də daxili həmlələrdən mühafizəsini təmin etməlidir.

Bu gün informasiya təhlükəsizliyini təmin edən çoxlu sayda üsullar mövcuddur. Bunlara misal olaraq aşağıdakı üsulları göstərmək olar:

- istifadəçilərin identifikasiyası və autentifikasiyası (buna 3A kompleksi deyilir) vasitələri;
- kompyuterdə saxlanılan və şəbəkə ilə ötürülən informasiyanın şifrləmə vasitələri;
- şəbəkəarası ekranlar;
- virtual şəxsi şəbəkələr;
- kontent filtirləmə vasitələri;
- disklərin məzmunlarının tamlığını yoxlayan alətlər;
- antivirus mühafizə vasitələri;
- şəbəkələrin zəif yerlərinin aşkarlanma sistemləri və şəbəkə hücumları analizatorları.

Qeyd edilən vasitələrin hər birisi həm sərbəst, həm də başqalarına inteqrasiya olunması formasında istifadə oluna bilərlər. Bu isə istifadə olunan platformadan asılı olmayaraq istənilən mürəkkəb və konfiqurasiyalı şəbəkələr üçün informasiya mühafizəsi sistemini yaratmağa imkan verir.

"3A kompleksi" autentifikasiyadan (və identifikasiyadan), avtorlaşma və administratorlaşmadan ibarətdir. İdentifikasiya və avtorlaşma-bunlar informasiya təhlükəsizliyinin əsas elementləridirlər. İnformasiya aktivlərinə dostup zamanı id-

entifikasiya funksiyası belə suallara cavab verir: “Siz kimsiniz?” və “siz haradasınız”, siz şəbəkənin avtorlaşmış istifadəçisinizmi? Avtorlaşma funksiyası konkret istifadəçini hansı resurslara dostupunun olmasına cavab verir. Administratorlaşma funksiyasının vəzifəsi verilmiş şəbəkə daxilində istifadəçinin müəyyən identifikasiya xüsusiyyətlərinə görə bölmək və onun üçün icazəli olan həcmi müəyyən etməkdir.

Şifrələmə sistemi sərt diskdə və ya başqa bir daşıyıcıda saxlanılan verilənlərə sanksiya olunmamış (icazəsiz) dostuplar zamanı itgiləri, eyni zamanda, elektron poçt və ya şəbəkə protokolları vasitəsilə informasiyanı göndərən zaman onun ələ keçirilməsini minimuma endirməyə imkan verir. Bu mühafizə vasitələrinin vəzifəsi konfidensiallığın təminidir. Şifrələmə sisteminə qoyulan əsas tələblər-kriptodayanıqlılığın yüksək səviyyəsi və dövlətin ərazisində istifadəsinin leqallığıdır.

Şəbəkəarası ekran iki və ya daha çox şəbəkə arasında mühafizə hasarı təşkil edən sistem və sistemlər kombinasiyasıdır. Verilənlər paketinin sanksiyasız şəbəkəyə düşməsinin və ya ondan çıxmasının qarşısını alır. Şəbəkəarası ekranların əsas iş prinsipi-hər bir verilənlər paketinin daxil olan və xaric olan İP-ünvanların icazə verilmiş ünvanlar bazasına uyğunluğunu aşkarlamaqdan ibarətdir. Beləliklə, şəbəkəarası ekranlar informasiya şəbəkələrinin seqmentləşməsinə və verilənlərin dövr etməsinə nəzarət imkanını kifayət qədər genişləndirir.

Kriptoqrafiya və şəbəkəarası ekranlar haqqında danışanda mühafizə olunan virtual şəxsi şəbəkələrdən (VPN) də danışmaq lazımdır. VPN-dən istifadə verilənləri açıq kommunikasiya kanalları vasitəsilə ötürən zaman onların konfidensiallıq və tamlıq problemlərini həll etməyə imkan verir:

- kompaniyanın müxtəlif ofisləri arasında informasiya axınlarının mühafizəsi (informasiyanın şifrələnməsi yalnız xarici şəbəkəyə çıxış zamanı aparılır);
- uzaq şəbəkə istifadəçilərinin kompaniyanın resurslarına dostupu, adətən, internet üzərindən aparılır;
- korporativ şəbəkə daxilində ayrı-ayrı əlavələr arasında informasiya axınının mühafizəsi vasitəsi

- daxil və xaric olan elektron poçtların məzmununun filtrləşdirilməsidir. Kontent filtrasiya vasitələri istifadə olunan bütün formatları, o cümlədən sıxılmış və qrafiki yoxlamağa imkan verir. Bu zaman şəbəkənin buraxma qabiliyyəti praktiki olaraq dəyişmir.

İşçi stansiyada və ya serverdə bütün dəyişikliklər sərt diskin məzmununun tamlığının yoxlanması texnologiyasına əsasən şəbəkə administratoru və ya başqa avtorizasiya olunmuş istifadəçilər tərəfindən izlənə bilər. Bu fayllarla olan istənilən hərəkətləri və virusların aktivliyini identifikasiya edir, sanksiya olunmamış dostupları və ya avtorlaşmış istifadəçilərin verilənləri oğurlamasını aşkarlamağa imkan verir. Nəzarət fayllar cəminin analizi (CRC cəmi) əsasında aparılır.

4. İnformasiya təhlükəsizliyi vasitələri

İndi isə əvvəlki paraqrafda qeyd olunmuş prinsip və ya mexanizmlərin hansı vasitələr və ya alətlər vasitəsilə reallaşdırılmasına qısa da olsa aydınlıq gətirək. Təbiidir ki, burada belə vasitə və alətlərin tam siyahısını vermək mümkün deyildir. Belə ki, bunlar informasiya təhlükəsizliyi aspektinə baxılan konkret vəziyyətdən asılıdır. Ona görədə buradakı mülahizələr aşağıdakı bazisə əsaslanır. Hesab edirik ki, personal (işçi personal)-bu vasitədir, audit-mexanizmdir, qeydiyyat (hesabat) isə məqsəddir. Başqa bir halda autentifikasiyanı təmin edən parollar şifrələnmiş formada saxlanılır, autentifikasiya öndə gəlir (sələfdir), misal üçün, modifikasiyaya icazə üçün. Deməli, kriptoqrafiya parolların mühafizə vasitəsidir, parollar autentifikasiya mexanizmi üçün istifadə edilir, autentifikasiya tamlığın təminindən öndə olur.

Beləliklə, informasiya təhlükəsizliyinin əsas vasitələri (alətləri) aşağıdakılardır:

- **personal** - bütün aspektlərdə, başqa sözlə, işləmək, tətbiq etmək, dəstəkləmək, nəzarət etmək və yerinə yetirmək informasiya təhlükəsizliyini həyata keçirən insanlardır;
- **normativ təminat** - informasiya təhlükəsizliyinin işlənməsi üçün hüquqi fəzanı yaradan sənədlər;
- **təhlükəsizlik modelləri** - verilmiş konkret informasiya sisteminə və ya mühitinə qoyulmuş informasiya təhlükəsizliyinin təmini sxemləri;
- **kriptoqrafiya** - informasiyanın elə çevrilmə üsul və vasitələridir ki, onunla sanksiya olunmamış əməliyyatları (oxuma və ya modifikasiya etmə) çətinləşdirir və ya imkan vermir. Təbii ki, bu üsul və vasitələr bu sanksiyaları reallaşdıran xüsusi informasiya obyektləri-açarların yaradılması, saxlanması və paylanması üsul və vasitələri ilə birgə işləyirlər;
- **antivirus təminatı** - təhlükəli kodların (viruslar, troyan proqramları və s.) aşkarlayıb məhv etmək üçün vasitələr;
- **şəbəkəarası ekranlar** - bir informasiya şəbəkəsindən başqasına dostupa nəzarət qurğusu;

- **təhlükəsizlik skanerləri -** konkret informasiya sistemi üçün təhlükəsizlik modelinin işləmə keyfiyyətini yoxlayan qurğu;
- **həmlələri aşkarlayan sistemlər -** informasiya mühitində aktivlik monitorinqi qurğusu (bəzi hallarda göstərilən aktiv fəaliyyətdə sərbəst iştirak etmək imkanı ilə);
- **ehtiyat kopiyalaşdırma -** mümkün olan itirmə və ya zədələnmə zamanı istifadə etmək üçün informasiya resurslarının izafi nüsxələrinin (kopiyalarının) saxlanması;
- **rezervləşdirmə -** əsas qurğuların işdən çıxdığı zaman informasiya mühitinin işlək olması üçün lazım olan alternetiv qurğuların yaradılması;
- **qəza planı -** informasiya təhlükəsizliyi plan və vasitələrində nəzərdə tutulmuş qaydalardan kənar hallarda həyata keçirmək üçün nəzərdə tutulmuş tədbirlər yığımı;
- **istifadəçilərin öyrədilməsi -** informasiya təhlükəsizliyi tələblərinə uyğun şəraitdə işləmək üçün informasiya mühitinin aktiv iştirakçılarının hazırlanması.

İnformasiyanın texniki vasitələrlə mühafizəsi

İnformasiyanın mühafizəsinin texniki vasitələr qrupuna apartat və proqram vasitələri aid edilir.

Texniki tədbirlərin kompleksinə, kompüter sistemlərinin və şəbəkəsinin obyektlərinin fiziki əlçatanlığını təmin etmək üçün tədbirlər, məsələn, kamera avadanlıqları və siqnalizasiya kimi praktiki üsullar da daxildir.

İnformasiyanın qorunmasının qeyri-texniki vasitələri Qeyri-texniki qoruma vasitələrini üç əsas hissəyə bölürlər:

- təşkilati qoruma tədbirləri;
- hüquqi qoruma tədbirləri;
- mənəvi-etik normalar.

5.Kompüter sistemləri və 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 var**:

- 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.

Təhlükələrin əlamətlərinə görə təsnif olunması.

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.

İnformasiya təhlükəsizliyinin konseptual modelinə aşa-ğıdakı əsas komponentlər daxil edilir:

- təhlükəyə məruz qala biləcək obyektlər;
- qorunması tələb olunan informasiya;
- təhlükələr;
- təhlükələrin mənbələri;
- təhlükələrin mənbələrinin məqsədləri;
- qorunan informasiyanın qanunazidd şəkildə yayılması (sızması) yolları;
- informasiya t$_{ə}$hlük$_{ə}$sizliyinin t$_{ə}$min edilm$_{ə}$sinin isti-qam$_{ə}$tl$_{ə}$ri;
- informasiyanın qorunması üsulları və vasitələri.

6. Kompütersistemlərində təhlükələrin əsas növləri və əlamətləri

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

Təhlükələrin əsas növləri aşağıdakılardır:

1. HS-in resurslarından icazəsiz istifadə edilmə:

- verilənlərdən istifadə edilmə (surət çıxarma, dəyişdirmə, silmə, çap etmə və s.);
- proqramların surətlərinin çıxarılması və dəyişdirilməsi;
- sistemə həmlə etmə məqsədilə proqramların araşdırılması.

2. HS-in rezuslarından düzgün istifadə edilməməsi:

- tətbiqi proqramların əsas yaddaşın onlara aid olmayan bölmələrinə təsadüfən müraciət etmələri;
- disk yaddaşının sistem bölmələrinə təsadüfi müraciətlər;
- verilənlər bazasında səhvən dəyişiliklər edilməsi (səhv verilənlərin daxil edilməsi, verilənlərin istinad tamlığının pozulması);
- istifadəçilərin və xidmətçi heyətin səhv hərəkətləri.

3. Proqram və aparat vasitələrində səhvlərin aşkar edilməsi.

4. Rabitə xətlərində və ötürmə sistemlərində verilənlərin ələ keçirilməsi.

5. Elektromaqnit şüalanmaların icazəsiz qeydə alınması.

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

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

Təhlükəsizliyin pozulmasının mümkün nəticələri aşağdakılar ola bilər:

- Məxfi məlumatın ələ keçirilməsi;
- sistemin məhsuldarlığının azalması və ya sistemin bütövlükdə dayanması;
- əməliyyat sisteminin yüklənə bilməməsi;
- maddi ziyan;
- faciəli nəticələr.

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

Mümkün təhlükələrdən asılı olaraq mühafizənin 3 əsas məsələsini ayırmaq olar:

-informasiyanı oğurlanmaqdan mühafizə etmək;

-informasiyanı itkilərdən mühafizə etmək;

-hesablama sistemini nasazlıqlardan və dayanmalardan mühafizə etmək.

Informasiyanın oğurlanmaqdan mühafizə edilməsi informasiyanı saxlayan qurğuların və daşıyıcıların fiziki oğurlanmasının, informasiyanın icazəsiz alınmasının (surətinin çıxarılması, baxış, ələ keçirilməsi və s.) və proqramların icazəsiz yayılmasının qarşısının alınmasını nəzərdə tutur.İnformasiyanın itkilərdən mühafizə edilməsi informasiyanın düzgünlüyünün və tamlığının (fiziki, məntigi və semantik baxımdan) qorunmasını nəzərdə tutur. Sistemdə informasiya istifadəçilərin və proqramların (o cümlədən virusların) icazəsiz müraciətləri, istifadəçilərin, proqramlarm və xidmətçi heyətin səhv əməliyyatları səbəbindən və həmçinin hesablama sistemindəki nasazlıqlardan və dayanmalardan informasiya itirilə bilər.Aparat və proqram vasitələrinin nasazlıqlardan və dayanmalardan mühafizə edilməsi sistemin normal fəaliyyətinin vacib şərtlərindən biridir. Sistemin nasazlıqlardan və dayanmalardan mühafizəsinin əsas yükü aparat-proqram komponentlərinin- prosessorun, əsas və xarici yaddaş qurgularının, daxiletmə-xaricetmə qurğularının və həmcinin əməliyyat sisteminin proqramlarının üzərinə düşür. Sistem vasitələrinin etibarlığı kifayət qədər olmadıqda, nasazlıqlardan və dayanmalardan mühafizəni tətbiqi proqramlarda nəzərə almaq lazım qəlir.Etibarlıqdedikdə hesablama sisteminin öz funksiyalarını dəqiq və vaxtında yerinə yetirməsi qabiliyyəti başa düşülür. Proqram təminatının etibarlıq dərəcəsi yaradılma prosesinin avtomatlaşdırılmasının keyfiyyəti və səviyyəsi ilə və həmçinin onun müşayiətinin təşkili ilə təyin olunur.

7.Kompütersistemlərində informasiya təhlükəsizliyi və mühafizəsinin üsulları və vasitələri

İnformasiyanın mühafizəsi informasiya təhlükəsizliyinin təmin olunmasına yönəlmiş tədbirlər kompleksidir.

İnformasiya mühafızəsinin üsullarını dörd sinfə ayırmaq olar:

fiziki,aparat, proqram və təşkilati üsullar.

Fiziki mühafizə əsasən mühafızənin yuxarı səviyyələrində istifadə edilir və kənar şəxslərin hesablama sisteminin yerləşdiyi əraziyə daxil olmalarının qarşısını almaqla həyata keçirilir. Fiziki mühafizə ücün aşağıdakı vasitələrdən istifadə edilir:

- hərəkət edən obyektləri müəyyənləşdirmək, onların ölçülərini, sürətlərini və hərəkət istiqamətlərini təyin etmək üçün yüksək tezlikli, ultrasəs və infraqırmızı aşkarlama sistemləri;
- işıq şüaları ilə kəsişməyə reaksiya göstərən lazer və optik sistemlər;
- qorunan obyektlərin telesistemlər ilə müşahidə edilməsi;
- çox da böyük olmayan obyektləri kabellə əhatə etməklə onlara yaxınlaşan şəxslərə reaksiya verən kabel sistemləri;
-icazəsiz girişin qarşısmı almaq, müşahidə etmək və qulaq asmaq üçün qapı və pəncərələrinmühafizə sistemi
- qapı və darvazalar ücün mexaniki və elektron qıfıllar;
- şüalanmaları neytrallaşdıran sistemlər.

Aparat mühafizəsi kompüterin tərkibindəki aparatura və ya xüsusi qurğular vasitəsilə reallaşdırılır. Aparat mühafizə vasitələrinə əsasən prosessorların və əsas yaddaşın, daxiletmə-xaricetmə qurgularının, rabitə kanalları vasitəsilə verilənlərin ötürülməsi sistemlərinin, elektrik təminatı sistemlərinin, xarici yaddaş qurğularının mühafizə vəsitələri aiddir.

Prosessorların aparat mühafızə vasitələri icra olunan proqramlardakı əmrlərin mümkünlüyünə nəzarət edirlər. Yaddaşın mühafizə vasitələri proqramların icrası zamanı əməli yaddaşdan birgə istifadə edilməsinə və yaddaşın məhdudluğuna nəzarət edirlər. Daxiletmə-xaricetmə qurğularının mühafızə vasitələrinə onlardan icazəsiz istifadə etməyi bloklaşdıran müxtəlif sxemlər aiddir. Verilənlərin rabitə

kanalları ilə ötürülməsinin mühafizəsi vasitələri informasiyanı məxviləşdirən (şifrləyən) sxemlərdən ibarət olurlar.

Proqram mühafizə metodları müxtəlif proqramlar vasitəsilə reallaşdırılır. Həmin proqramlara aşağıdakılar aiddir:

-əməliyyat sistemlərinin proqramları;

-xidməti proqramlar;

-antivirus proqramları;

-instrumental sistem proqramları: VBİS, elektron cədvəllər, mətn prosessorlan, proqramlaşdırma sistemləri və s.

-xüsusi mühafızə proqramları;

-hazır tətbiqi proqramlar.

İnformasiyanın təşkilatı mühafizəsi təşkilatı-texniki tədbirlər, informasiyanın mühafizəsi məsələlri üzrə qanunvericilik aktlannın yaradılması və qəbul edilməsi, cəmiyyətdə informasiyanın istifadə edilməsi üzrə məntiqi-etik normaların təsdiq edilməsi ilə reallaşdırılır.

İnformasiya mühafızəsinin ən çevik və güclü metodlan aparat-proqram metodlar hesab olunur.

Aparat-proqram vasitələri ilə müəyyən səviyyədə həm avadanlığm mühafızəsi məsələlərini (avadanlığı oğurlamaqdan, itkilərdən, nasazlıqlardan və dayanmalardan qorumaq), həm də proqramların səhvlərdən mühafızəsi məsələsini həll etmək olar. Mühafızə sistemində bu məsələlərin həlli aşağıdakı üsullarla təmin edilir:

1) istifadəçilər və proqramlar tərəfindən resurslara icasəsiz müraciətlərin qarşısının alınması;

2) müraciətin mümkünlüyü halında resurslardan icazəsiz istifadənin qarşısının alınması;

3) resurslardan düzgün istifadə olunmamasının qarşısının alınması;

4) struktur, funksional və informasiya izafiliyinin tətbiqi;

5) aparat-proqram vasitələrinin yüksək keyfiyyətlə yaradılması.

Bu üsullara və onların yerinə yetirilməsi metodlarına daha ətraflı baxaq.

1. Resurslara icazəsiz müraciətiərin qarşısını almaq ücün istifadəçilər və proqramlar tərəfindən sistemə müraciət cəhdlərinin qeydiyyatı sistemi və həmcinin hesablama sisteminin təhlükəsizliyinə cavab verən şəxslərə bu barədə dərhal siqnal verən vasitələr olmalıdır. Resurslara icazəsiz müraciət zamanı etibarlı qeydiyyat və siqnal sisteminin olmaması və həmcinin hesablama sisteminə dolayı yolların olması sistemə qeyri-qanuni girməyə səbəb olur. Sistemə qoşulma hadisələrinin qeydiyyatını aparmaq ücün, adətən, xüsusi jurnaldan və ya verilənlər bazasmdan istifadə edilir.

İcazəsiz istifadənin qarşısının alınması.

İstifadəçilər tərəfindən resurslardan icazəsiz istifadənin qarşısım almaq ücün müasir sistemlərdə əsasən iki üsuldan istifadə olunur: 1) parol üsulu; 2) identifıkasiya və autentifıkasiya üsulu.

Şifrlənməyən sadə parol mühafizəsi zəif mühafizə vasitəsi hesab olunur. Onun əsas çatışmazlığı ondan ibarətdir ki, eyni paroldan istifadə edən bütün istifadəçilər hesablama sistemi nöqteyi-nəzərdən fərqlənmirlər. İstifadəçi üçün parol mühafizəsinin münasib olmaması onun yadda saxlanması ilə əlaqədardır. Əqər parol sadə və qısadırsa, onu asan açmaq olar, əgər mürəkkəbdirsə, onu harasa yazmaq lazımdır. Məsuliyyətsizliyə yol verildikdə icazəsiz istifadəçilər parola asan yol tapa bilirlər.

Bəzən sistemdə bir neçə paroldan istifadə edilir. Bu halda hər bir parola uygun müraciət hüquqi verilrir.

Sistemə müraciətin daha ciddi nəzarət üsulu istifadəçilərin identifıkasiyası və autentifikasiyası hesab olunur. Bu halda sistemə qoşulmaq istəyən hər bir istifadəçi əvvəlcə identifikasiya olunur, sonra isə onun doğrudan da həmin istifadəçi olması yoxlanır (autentifıkasiya). İstifadəçilərin identifıkasiyası parol vasitəsilə aparıla bilər. Autentifıkasiya, yəni istifadəçinin həqiqiliyinin yoxlanması, əsasən aşağıdakı üsullarla aparılır:

-gizli parol sorğusu;

-xalis fərdi informasiya sorğusu;

-elektron açarla;

-mikroprosessor kartları vasitəsilə;

-tanınmanın aktiv vasitələrindən istifadə etməklə;

-biometrik vasitələrlə.

Autentifikasiya üçün soruşulan əlavə informasiya istifadəçinin və ya onun qohumlarının şəxsi həyatı ilə bağlı olan istənilən məlumat və ya hadisə ola bilər məsələn, bankda hesab nömrəsi, pasport nomrəsi, arvadının və ya ərinin soyadı.

Elektron açara misal olaraq maqnit zolaqlı plastik kartı göstərmək olar. Kartın yaddaş təbəqəsində görünməyən parol rolunu oynayan kod saxlanır. Elektron açarın daha mürəkkəb variantı jeton adlanan və təsadüfi parolu generasiya edən xüsusi cihaz ola bilər. Jetonun çatışmayan cəhətlərindən biri ondan ibarətdir ki, o, istifadəçinin yanında olmadıqda həmin istifadəçinin sistemə müraciəti mümkünsüz olur. Bu halda çıxış yolu bir neçə müvəqqəti jetonların yaradılması ola bilər.

ABŞ-in standartlar və texnoloqiyalar institutunda hazırlanmış mikroprosessor kartları rəqəmsal imzaları formalaşdırmağa imkan verirlər. Sifırlənmə alqoritmi elektron imzaları saxtalaşdırmağın qarşısını alır.

Daha perspektivli autentifikasiya üsulu tanınmanın aktiv vasitələri ilə reallaşdırılr. Bu cür vasitəyə misal olaraq zəif siqnallı miniatür radioötürücüdən və uyğun radioqəbuledicidən ibarət olan sistemi göstərmək olar. Sistemə qoşulan zaman istifadəçi ona məxsus olan ötürücünü yaxın məsafədən (bir neçə dm) qəbuledicіyə yaxınlaşdırmalı və onu işə salmalıdır. Əgər qəbuledici siqnalı tanıyarsa istifadəçi sistemə qoşula bilər. Bu cür sistemin üstünlüyü onda fiziki kontaktların olmamasıdır.

Mövcud autentifikasiya vasitələri içərisində ən etibarlısı (və bahalısı) biometrik vasitələr hesab olunur. Bu vasitələrlə şəxsiyyətin tanınması insanın barmaq izi ilə, əl içinin forması ilə, gözün tor qişası ilə, imza ilə, səslə və digər fizioloji parametrlərlə əldə edilir. Bəzi sistemlər insanı onun klaviaturada işləmə vərdişi ilə təyin edir. Bu cür sistemlərin əsas üstünlüyü autentiifikasiyanm yüksək etibarlılığıdır. Mənfi cəhətləri işə avadanlığın baha başa gəlməsindən, tanınmaya müəyyən vaxt sərf edilməsindən və istifadəçi üçün rahat olmamasından ibarətdir.

Sistemə qoşulan istifadəçinin və ya proqramın ziyankar olmaması onların iş ərəfəsində özlərini təhlükəsiz aparmalarına tam zəmanət vermir, odur ki, bir çox mühafizə sistemlərində iş seansı ərzində resurslara müraciətin məhdudlaşdırılması nəzərə alınır.

İş seansı qurtardıqdan sonra qoşulma parametrləri haqqında informasiya, o cümlədən, parollar sistemdən silinməlidir ki, sonra onlardan icazəsiz istifadəçilər və proqramlar istifadə edə bilməsinlər.

Sanksiyasız proqram növlərindən biri də kompüter viruslarıdır. Məlum kompüter viruslarının sayı daima artır. Hətta yeni mühəndislik sahəsi də yaranmışdır: kompüter virusologiyası. Kompüter viruslarının nəticələri müxtəlif ola bilər: kompüterin monitorunda görünən qeyri adi effektdən və kompüterin işinin yavaşımasından başlamış, hesablama sisteminin və ya şəbəkənin tam dağılmasına qədər. Odur ki, kompüter viruslarının inkişafının bütün mərhələlrində və, ələlxüsus, onların sistemə daxil olması və çoxalması ərəfəsində kompüter viruslarından mühafizə olmaq gərəkdir. Buna görə də, mühafizə sisteminə proqram-aparat vasitələrinin vəziyyətinin diaqnostikası, virusların lokallaşdırılması və kənarlaşdırılması və onların nəticələrinin aradan qaldırılması üçün vasitələr daxil edilməlidir.

2. Resursların icazəsiz istifadədən mühafizəsi icazəsiz müraciətdən mühafizədə olduğu kimi, mühafizə olunan resurslara sorğuların qeydiyyatını və icarəsiz istifadəyə cəhd göstərilmə zamanı siqnal verməyi tələb edir. Qeyd edək ki, söhbət mühafizəsi çox vacib olan resurslardan gedir.

İnformasiya-proqram resurslarının icazəsiz istifadədən mühafızəsi aşağıdakiları nəzərdə tutur: surət çıxarmaqdan mühafizə, proqramlara müdaxilə etmədən mühafızə, verilənlərə baxışdan mühafızə, proqramları və verilənləri dəyişdirmədən və silinmədən mühafizə.

8.İnformasiya mühafizəsi aparat vasitələri

Qorumanın aparat vasitələrinin məqsədi fəaliyyət sahəsində istifadə olunan texniki vasitələrlə məxfi informasiyanın yayılması və sızması, eləcə də ona icazəsiz girişin əldə olunması təhlükələrindən qorunmasıdır.

Aparat vasitələri – verilənlərin emalı üçün istifadə olunan texniki vasitələrdir. Buraya daxildir: fərdi kompyuterlər, hesablama və informasiya məsələlərinin həlli zamanı informasiyanın avtomatik emalı üçün nəzərdə tutulmuş texniki vasitələr kompleksi;

– periferiya qurğuları – EHM-nin xarici qurğular kompleksi;

– fiziki maşın informasiya daşıyıcıları;

Aparat mühafizəsi vasitələrinə müxtəlif elektron, elektro-mexaniki, elektron-optik qurğular aiddirlər. İndiyədək kifayət qədər müxtəlif təyinatlı aparat vasitələri işlənib hazırlanmışdır. Buna baxmayaraq, onlardan aşağıdakılar daha geniş yayılmaqdadır:

– mühafizə rekvizitlərini (kodları, şifrləri və ya gizlilik (məxfilik) səviyyəsini identifikasiya edən) saxlamaq üçün xüsusi registrlər;

– qurğunun identifikasiya kodunu avtomatik generasiya edən kod generatorları;

– insanın identifikasiyası üçün onun fərdi xarakteristikalarını (səs, barmaq izləri) ölçən qurğular;

– yaddaş qurğusunda saxlanan qiymətləri informasiyanın məxfiliyi səviyyəsini təyin edən xüsusi məxfilik bitləri;

– verilənlərin ötürmə (verilmə) ünvanlarını periodik olaraq yoxlamaq məqsədilə əlaqə xətlərində informasiya ötürülməsinin qırılma sxemləri. Aparat mühafizəsi vasitələrindən xüsusi yeri olan və geniş tətbiq sahəsi verilmiş informasiyanı şifrələmək üçün olan qurğularıdır (kriptoqrafik üsullara əsaslanan).

Hazırda informasiya təhlükəsizliyinin təmin edilməsi məqsədilə praktikada çoxlu sayda aparat vasitələrindən istifadə olunur.

Funksional təyinatına görə aparat vasitələrini aşağıdakı kimi təsnif etmək olar:

- aşkarlama və müəyyənetmə vasitələri;

- axtarış və dəqiq ölçmə vasitələri;
- fəal və passiv müqavimət vasitələri.

Texniki imkanlarına görə isə informasiyanın qorunmasının aparat vasitələrini iki qrupa bölmək olar:

1. *ümumi təyinatlı vasitələr* - ilkin qiymətləndirmə məq-sədilə qeyri-peşəkarlar tərəfindən istifadə üçün nəzər-də tutulmuş vasitələrdir.

2. *peşəkar komplekslər* - sənaye casusluğu vasitələrinin mükəmməl axtarışını, aşkarlanmasını və onların bütün xarakteristikalarının çox dəqiq ölçülməsini həyatakeçirməyə imkan verən aparat vasitələridir.

İnformasiyanın qorunmasının aparat vasitələri KSŞ-nin, eləcə də telekommunikasiya sistemlərinin təhlükəsizliyinin təmin edilməsi üçün də geniş istifadə olunur. Belə vasitə-lər, əsasən, serverlərin, işçi stansiyaların, yaddaş qurğuları-nın və informasiya daşıyıcılarının, terminalların, giriş-çıxış qurğularının, o cümlədən kompüterlərə və sistemə, onların saxlandığı yerə girişin təhlükəsizliyinin təmin edilməsi üçün istifadə olunur. Aparat vasitələrinin serverlərdə və işçi stansiyalarda tətbiqi informasiya resurslarına istifadəçilərin girişinə nə-zarət edilməsinə, kənar şəxslərin girişinin qarşısının alın-masına, kompüter texnikasının və digər qurğuların işində proqram-texniki səhvlərin aşkarlanmasına və qarşısının vaxtında alınmasına imkan verir. Bundan əlavə, informasiya resurslarının, o cümlədən yaddaş qurğularının və informasiya daşıyıcılarının xarici və daxili təhlükələrdən qorunmasını təmin etmək məqsə-dilə də aparat vasitələrindən istifadə olunur. Xarici təhlükəsizliyin təmin edilməsi məqsədilə aparat vasitələri ərazinin, binanın, otağın qorunması, istifadəçilə-rin müşahidəsinin və tanınmasının təşkili və s. üçün tex-niki imkanları özündə reallaşdırır. Bu vasitələr bəzən fiziki qoruma vasitələri kimi qəbul edilir. Burada daxili təh-lükəsizlik dedikdə sistemin və şəbəkənin proqram-texniki kompleksi çərçivəsində informasiya təhlükəsizliyinin tə-min edilməsi başa düşülür. Aparat vasitələrinin inkişafına aşağıdakı amillər bilava-sitə təsir edir: - aparat vasitələrinin proqram vasitələrinə nisbətən sür-ətlə işləməsi; - aparat vasitələrinin element bazasının intensiv və sür-ətlə inkişafı; - aparat vasitələrinin və element bazasının

qiymətinin (maya dəyərinin) ciddi aşağı düşməsi və s. Aparat vasitələrinin qiymətinin digər təhlükəsizlik vasi-tələrinə nisbətən yüksək olması səbəbindən informasiya resurslarının təhlükəsizliyinin təmin edilməsi üçün yalnız bu növ vasitələrin tətbiqi məqsədəuyğun hesab olunmur.

Aparat vasitələrinin proqram vasitələri, fiziki mexa-nizmlər və təşkilati tədbirlərlə birgə tətbiqi avadanlıqların, texniki vasitələrin, informasiya resurslarının fiziki məhv olmadan, sıradan çıxmalardan, eləcə də icazəsiz və qeyri-qanuni girişlərdən və istifadədən daha etibarlı qorunmasını təmin etməyə imkan verir.

9.İnformasiya mühafizəsini təmin edən proqram vasitələri

Aparat vasitələrimüəyyən nəticəni almaq üçün kompyuterlərin və kompyuter qurğularının normal işini təmin etmək məqsədilə verilənlər və əmrlər yazımınınobyektiv təsvir formasıdır. Eyni zamanda buraya hazırlanmış və fiziki materiallarda fiksasiya edilmiş materiallar və onların yaratdığı audiovizual əksetmələr aiddirlər. Bunlara aşağıdakılar aiddir: proqram təminatı (idarəedici və emaledici proqramlar yığımı). Tərkibi: sistem proqramları (əməliyyat sistemləri, texniki xidmət proqramları); tətbiqi proqramlar (müəyyən növ məsələləri həll etmək üçün proqramlar); instrumental proqramlar (proqramlaşdırma dillərindən ibarət olan proqramlaşdırma sistemləri: Turbo C, Microsoft Basic və s., translya-torlar avtomatik olaraq alqoritmik və simvollu dillərdən maşın kodlarına tərcümə edən proqramlar kompleksi); mülkiyyətçinin, istifadəçinin maşın məlumatı.

Belə xırdalıqlara yol verməkdə məqsəd gələcəkdə baxılan məsələnin mənasını daha dəqiq başa düşmək, kompyuter cinayətinin baş vermə səbəblərini, alətlərini və cinayətə təhrik edən alət və vasitələrini daha aydın seçməkdən ibarətdir və bununla yanaşı kompyuter texnikası vasitələri terminləri arasında olan qeyri mü-əyyənliyi aradan qaldırmaqdan ibarətdir. Belə ki, kompyuter cinayətinin başa düşülməsini təsvir edən əsas komponentlərin dəqiq analizindən sonra kompyuter cinayətinin kriminalstik xarakteristikasının əsas elementlərinə aid olan məsələlərə baxmaq olar.

Proqram mühafizə vasitələrinə mühafizə funksiyasını yerinə yetirən və verilənlərin emalı sisteminin proqram təminatı tərkibinə daxil olan xüsusi proqramlar aiddirlər. Proqram mühafizəsi mühafizənin nisbətən geniş yayılmış növüdür. Səbəb kimi bu vasitənin unversallığı, elastikliyi, sadə reallaşması, prak-tiki olaraq istənilən dəyişmə və inkişaf imkanlarını və s. göstərmək olar. Funksiyanın təyinatına görə onları aşağıdakı qruplara bölmək olar:

– texniki vasitələrin (terminallar, giriş-çıxışı, EHM-i, informasiya daşıyıcılarının qrup şəklində idarə qurğularını) məsələ və istifadəçilərin identifikasiyası;

– texniki vasitələrin (tarix və iş vaxtı, istifadə üçün icazə verilən məsələlərdən istifadə) və istifadəçilərin hüquqlarının təyini;

– texniki vasitələrin və istifadəçilərin işlərinə nəzarət;

– İstifadəsi məhdud informasiyaların emalı zamanı texniki vasitələrin işinin qeydiyyatı;

– istifadədən sonra yaddaş qurğusundan informasiyanın silinməsi;

– sanksiya olunmamış hərəkətlər zamanı siqnalın verilməsi;

– müxtəlif təyinatlı köməkçi proqramlar: mühafizə mexanizminin işinə nəzarət, veriləcək sənədlərə məxfilik şifrələrinin təqdim olunması.

Proqram vasitələri məxfi informasiyanın və proqram təminatının, əsasən, aşağıdakı təhlükələrdən qorunması üçün tətbiq edilir:

- informasiyanın, proqramın və sistemin icazəsiz giriş-dən qorunması;
- informasiyanın və proqramın köçürülmədən qorunması;
- informasiyanın, proqramın, sistemin və şəbəkənin viruslardan qorunması;
- rabitə kanallarının qorunması.

Ümumi halda, informasiyanın qorunmasının proqram vasitələrini aşağıdakı qruplara bölmək olar: - ümumi proqram təminatlarında nəzərdə tutulan özünüqoruma vasitələri – proqram təminatlarının özləri-nə məxsus olan, istehsalçılar tərəfindən işlənib hazır-lanan, onun satışını müşayiət edən və qeyri-qanuni hərəkətlərin qarşısını alan qoruma mexanizmləridir; - hesablama sistemlərinin tərkibində reallaşdırılan qoruma vasitələri – avadanlıqların, yaddaş qurğularının, şəbəkə və telekommunikasiya vasitələrinin, mülki qurğuların qorunması vasitələridir. - informasiya sorğusu ilə qoruma vasitələri – informa-siyanın qorunmasını həyata keçirmək üçün istifadə-çilərin səlahiyyətlərinin identifikasiyası məqsədilə əla-və informasiyanın daxil edilməsini tələb edən qoruma vasitələridir. - fəal qoruma vasitələri – müstəqil proqram şəklində reallaşdırılan və xüsusi vəziyyətlər yarandıqda işə düşən qoruma vasitələridir. Burada xüsusi vəziyyət dedikdə parolun düzgün daxil edilməməsi, proqram yüklənən zaman tarixin və vaxtın səhv göstərilməsi, icazə olmadan informasiyaya girişin əldə edilməsinə cəhd göstərilməsi və s. nəzərdə tutulur. - passiv qoruma vasitələri – cinayətlərin açılmasına yardım etmək (onların açılmasının qaçılmazlığını göstərmək) məqsədilə ehtiyat və nəzarət tədbirlərinin görülməsinə, sübut və dəlil axtarışına yönələn qoruma mexanizmləridir.

10. Kompüter sistemlərində təhlükəsizliyin 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:

- İnformasiyatəhlükəsizliyininpozucularınaqarşı neqativmünasibətyaratmaqvə onudəstəkləmək;
- İnformasiyatəhlükəsizliyiprobleminin vacibliyiniHərzamanqeydetmək;
- resursları tədqiqatların ənmühümistiqamətlərində 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.

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 "Dəqiqiliyin yoxlanması" işlədilir. Subyekt aşağıdakı mənbələrdən ən azı birini təqdim etməklə özünün Dəqiqiliyini 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:

- texnikiməhdudiyyətlərqoyulması (parol çoxqısaolmamalıdır, paroldaHərf, rəqəm, durğuişarələriolmalıdırvə s.)
- parolunfəaliyyətmüddətininidarəolunması, onlarınvaxtaşırı 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.

11.Kompüter sistemlərində təhlükəsizliyin təmin olunmasinda icazələrin idarə edilməsi

İnformasiya sistemlərində subyektlərin(insanların, şəxslərin) hərəkətlərinə münasibətə görə informasiya mühafizəsinə daxildir:

1. Icazəsiz daxil olmalardan informasiya mühafizəsi və təhlükəsizliyin qorunması vasitələri;
2. Kompüter şəbəkələrində informasiyanın mühafizəsi və təhlükəsizliyi;
3. Kriptoqrafiki informasiya mühafizəsi və təhlükəsizliyi;
4. Elektron rəqəmli imza;
5. Kompüter viruslarından informasiya mühafizəsi və təhlükəsizliyi

Kompyüter şəbəkələrinin informasiya mühafizəsi- Müəsisələrin Lokal şəbəkələri çox vaxt İnternet şəbəkəsinə qoşulur. Şirkət və təşkilatların lokal şəbəkələrinin mühafizəsi üçün şəbəkələr arası ekrandan(ŞE) brandmauzerlərdən(firewalss) istifadə edilir. ŞE- icazələrə və ya daxil olmalara məhdudiyyətlərin qoyulması üçün vasitədir. Bu ŞE şəbəkəni iki hissəyə bölünməsinə imkan verir və bir sıra qaydalar formalaşdırır ki, buda paketlərin bir hissədən digər hissəyə ötürülməsi şərtlərini təyin edir. Həm proqram vasitəsi kimi və Həmdə aparat vasitəsi kimi realizə edilə bilər.

İnformasiyanın kriptoqrafiki mühafizəsi -İnformasiyanın məxfiliyinin qorunması və saxlanmasını təmin etmək üçün onun şifrələnməsi və ya kriptoqrafiyadır. Şifrləmə üçün üçün alqoritm və ya qurğudan istifadə edilirvə bu müəyyən edilmiş alqoritm əsasında realizə edilir. Şifirləməni idarə edilməsi açarın kodunun dəyişdirilməsi ilə aparılır.

Kriptoqrafiya –bu çox effektiv metoddur. Bu kompüter şəbəkələri və uzaq məsafəli kompüterlər arasında informasiya mübadiləsi zamanı ötürülən verilənlərintəhlükəsizliyinin təmin edilməsini artırır

Elektron rəqəmli imza -İlkin məlumatların modfikasiya edilməsi və ya bu məlumatın başqası ilə əvəz edilməməsi üçün məlumatın elektron imza ilə birlikdə ötürülməsi lazımdır. Elektron rəqəmli imza- bu simvollar ardıcılığı olub, ilkin

məlumatların kriptoqrafiki çevrilmələrin köməyi məxfi və açıq açarlardan istifadə edərək bütövlüyünün təmin edilməsidir.

Başqa sözlə məxfi açarın köməyi ilə şifrələnmiş məlumat elektron rəqəmli imza adlanır. Qəbul edən məlumatı açıq açarla deşifrə edir. Müqaisə aparır.

İnformasiyanın kompüter viruslarından mühafizəsi -Kompyüter virusu- çoxda böyük olmayan kiçik ölçülü zərərli proqramdır. Bu sərbəst şəkildə özünün surətini yaradır və daşıyıcıların yüklənmə(başlanğıc) sektoruna yüklənir və ya əlaqə kanalları vasitəsi ilə yayılırlar. Növlərindən asılı olaraq kompyüter virusları hesab edilir:

- Viruslu proqramlar(com və exe genişləndirilməli fayılları zədələyir)
- Yüklənən viruslar
- Makroviruslar
- Şəbəkə virusları

12.Təhlükəsizliyin və mühafizənin təşkilində audit və protokollaşdırma

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.

Təhlükəsizlik siyasəti kompüter sistemi və onun komponentlərinin işinə nəzarəti nəzərdə tutur və bu halda **audit jurnalı** kimi xüsusi jurnallarda hadisələrin qeydiyyatı və sonrakı təhlili yerinə yetirilir.

Əməliyyat sisteminin inzibatçısı və ya auditor kimi xüsusi istifadəçi tərəfindən həmin jurnala müntəzəm olaraq baxış keçirilir və orada toplanan məlumatlar təhlil edilir.

Əgər uğurlu hücum aşkar olunarsa, o zaman yaxşı olardı ki, audit jurnalına əsasən həmin hücumun nə vaxt və nə cür baş verdiyi aydınlaşdırılmış olsun.

Audit altsisteminə qarşı aşağıdakı tələblər irəli sürülürlər

1. Yalnız kompüter sistemi özü audit jurnalına yazıları əlavə edə bilər. Bu da digər istifadəçilərin auditor tərəfindən nüfuzdan salınmasını istisna edir.
2. Daxil olmanın heç bir subyekti, o cümlədən də, kompüter sistemi özü jurnaldakı yazıları nə redaktə edə bilər, nə də ləğv edə bilər.
3. Yalnız uyğun imtiyazlara malik olan auditorlar jurnala baxış keçirə bilərlər.
4. Yalnız auditorlar jurnalı təmizləyə bilərlər. Jurnal təmizləndikdən sonra oraya mütləq jurnalı təmizləyən şəxsin adı və təmizləmə vaxtı haqqında yazı daxil edilməlidir. Təmizlənməmişdən əvvəl jurnalın sığorta surəti yaradılmalıdır. Jurnal

həddindən artıq dolduqda əməliyyat sistemi öz işini dayandırır və sonrakı işlər jurnal təmizlənməmişdən əvvəl yalnız auditor tərəfindən həyata keçirilir.

5. Daxil olmanı məhdudlaşdırmaqdan ötrü xüsusi mühafizə vasitələri tətbiq olunmalıdır; onlar inzibatçının daxil olmasının və istənilən faylın tərkibinin dəyişdirilməsi üzrə onun imtiyazının qabağını alır. Yaxşı olardı ki, jurnalın sığorta surəti verilənlərin dəyişdirilməsini istisna edən WORM-CD-də saxlanılmış olsun.

Əməliyyat sisteminin etibarlı mühafizəsinin təminatı üçün jurnalda aşağıdakı hadisələr qeyd edilməlidir:

1) istifadəçilərin sistemə daxil olma və sistemdən çıxma cəhdləri;

2) istifadəçilərin siyahısının dəyişdirilməsi üçün edilən cəhdlər;

3) təhlükəsizlik siyasətinin, o cümlədən də audit siyasətinin də dəyişdirilməsi üçün edilən cəhdlər.

Jurnalda qeyd olunan hadisələr toplusunun nəticəvi seçimi auditorun boynuna düşür və sistem tərəfindən emal olunan informasiyanın xüsusiyyətindən asılı olur. Qeyd olunan hadisələrin həddindən artıq toplusu təhlükəsizliyi artırmayıb, əksinə azaldır, çünki çoxlu sayda yazılar içərisində mühafizə üçün təhlükəli ola bilən yzaıları nəzərdən qaçırtmaq mümkün ola bilər.

Təhlükəsizlik auditinin tətbiqi ardıcıl mərhələlərlə yerinə yetirilir:

- Audit prosedurlarının yaradılması (**inisializasiya** olunması);
- Auditlə bağlı informasiyanın toplanması;
- Auditlə bağlı verilənlərin analızı;
- Tövsiyyələrin işlənib hazırlanması;
- □ Audit hesabatlarının aparılması.

Sisteminin təhlükəsizliyi monitoringi.

İnformasiya sistemlərinin təhlükəsizlik monitoringinin funksiyası edilmiş hücumların təhlilini və onların avadanlıqlardan istifadə etməklə aşkar olunmasını yerinə yetirir. Müdafiəni yerinə yetirən avadanlıqlar işçi stansiyalarda və serverlərdə əməliyyat sistemi elementlərinin və verilənlər bazasının müdafiə olunmasını icra edirlər. Avadanlıqlar şəbəkənin topologiyasını araşdırır, şəbəkədə düzgün yerinə yetirilməyən birləşmələri və həmin birləşmələrin müdafiəsini təmin edir və nəhayət şəbəkələrarası ekranların sazlanmasını təhlil edirlər.

13.Ziyanverici proqramalar

İlk vaxtlar kompüterlər binalardakı çoxlu sayda otaqları zəbt edən, bahalı, nəhəng texniki sistemlər olduğundan, onlardan yalnız iri dövlət müəssisələri və xüsusi şirkətlər istifadə edə bilirdilər. Müəyyən müddətdən sonra informasiya mübadiləsinə zərurət meydana çıxdı – ilk şəbəkələr yarandı. Lakin həmin vaxtlarda kompüterlər qapalı sistemlər idi və ağ xalatlı ciddi insanlar tərəfindən idarə edilirdi. Buna görə də o vaxtlar xuliqanlıq və ziyankarlıq barədə heç kim düşünməmişdi

İstifadəçi İnternetə qoşulan zaman İnternetdən fərdi kompüterə daxil olan ziyanverici viruslara qarşı həyata keçirilən müdafiə tədbirləri şəbəkələrarası avadanlıqların köməkliyi ilə yerinə yetirilir. Belə avadanlıqlara nümunə olaraq şəbəkələrarası ekran proqramlarını göstərmək mümkündür. Hesablama texnikasında bu tip proqramları *brandmayer* və ya *Firewall* adlandırırlar.

Brandmayerlərin hansı funksiyanı yerinə yetirməsi onların necə sazlanmasından asılıdır. Adətən onlar digər kompüterlərin Sizin istifadə etdiyiniz fərdi kompüterin resurslarına daxil olma cəhdinin qarşısını alır və Sizin kompüterinizdə istifadə olunan proqramlara və İnternetə göndərilən informasiyaya nəzarət edirlər. Məsələn, troya adlanan viruslar İnternetdən və ya elektron poçtundan Sizin kompüterə daxil olub kompüterinizdə olan fayllar haqqında informasiya toplayaraq pisfikirli (bədəməlli) kompüter istifadəçisinə göndərir. Burada məqsəd müxtəlif ola bilir: heç bir fəaliyyətə ziyan vurmadan mümkün kommersiya təkliflərinin qiymətləndirilməsi üçün məlumatların toplanması naminə və ya ciddi sənaye cəsusluğu ilə məşğul olmaq üçün tutarlı səviyyədə əhəmiyyət kəsb edən informasiyaların əldə olunması xatirinə. Belə proqramlar Sizin kompüterə daxil etdiyiniz parolları izləməklə yanaşı digər məxfi (konfidensial) proqramları da nəzarətdə saxlaya bilir.

Brandmayerlərdən başqa İnternetlə bağlı təhlükələrin qarşısını almaqdan ötrü (cəsus proqramların axtarılmasıvə neytrallaşdırılması) *spyware* adlanan proqram təminatından da istifadə edilir.

Troya viruslarından başqa İnternetdən rəsmi şəkildə təqdim edilən proqram təminatı təşkilediciləri (komponentləri) bir çox hallarda proqram modullarına malik olurlar ki, onlarda Sizin istifadə etdiyiniz kompüter haqqında məlumat toplamaqla yanaşı Sizin icanəniz olmadan (Sizdən xəbərsiz) Sizə məxsus olan informasiyanı proqram istehsalçılarına göndərə bilirlər. Bir çox hallarda istehsalçı şirkətlər bu şəkildə informasiya toplanmasını və İnternet vasitəsi ilə onlara çatdırılmasını istifadəçinin işinə ziyan vurmayacağını sübut etməyə cəhd göstərirlər və bu əməliyyatın hətta istifadəçiyə müəyyən qədər xeyir gətirəcəyini də sübut etmək istəyirlər. Nəzərə alınmalıdır ki, istənilən kompüter istifadəçisi ona məxsus olan informasiyanı gizli saxlamaqla yanaşı digər kompüter istifadəçisinə göndərməməyə də tam ixtiyarı vardır. Bu baxımdan da kompüter istifadəçisinin brandmayerdən istifadəsi məsləhətdir. Bununla o, fərdi kompüterini casus proqramlarından müdafiə etmişolur.

Windows əməliyyat sisteminin bütün versiyalarında fərdi kompüterin viruslardan müdafiə edilməsi üçün sistemin proqram təşkilediciləri əlavə olunmuşdur. Onların arasında brandmayerlərə də rast gəlmək mümkündür (kompüterlərin susma rejimində brandmayer qoşulmuşvəziyyətdədir).

Bir çox hallarda istifadəçilər fərdi kompüterlərinin təhlükəsiz işləmələri üçün əlavə proqramlardan da istifadə edirlər, məsələn, kompüterə antivirus və ya anticəsus proqramlarının yüklənməsi məsəhətdir.

İstifadəçi nəzərə almalıdır ki, istehsal olunan bir çox antivirus proqramları bir-biri ilə uzlaşmır və bununda nəticəsində bir-birinə maneçilik edərək işləyirlər. Nəticədəhərbir antivirus proqramı digərinə mane olur, virusun aşkarlanaraq aradan götürülməsində birinci olmaq istəyir.

Bu baxımdan da fərdi kompüter istifadəçisi istehsal olunan antiviruslardan birinə üstünlük verməli və seçdiyi antivirus proqramını fərdi kompüterinə yükləməlidir.

Bir çox hallarda fərdi kompüter istifadəçisinə dövrü olaraq digər antivirus proqramlarından (onlardan daim istifadə etməsələrdə) bəhrələnməyi məsləhət bilirlər.Əksər antivirus və anticəsus proqramlarını fərdi kompüterə yükləmək tələb

olunur. Onlar mütəmadi olaraq istifadəçinin fərdi kompüterini yoxlayır, istifadə zamanı açıq qalmış fayllara virusların daxil olmasına maneçilik göstərirlər. Bununla da Sizin kompüterinizin tutarlı səviyyədə təhlükəsiz iş rejimi təmin edilimişolur.

Bu təsnifat ilə yanaşı virusları yayılma mexanizminə görə də təsnifatı vardır: fayl virusları, makroviruslar, yükləmə virusları və şəbəkə soxulcanları.

Əksər istifadəçilər fərdi kompüterlərə düşən virusları bir-birindən fərqləndirə bilmir. Onlar ümumi halda bütün virusları ancaq ziyan vuran kompüter virusu kimi tanıyır. Bu sözsüz ki, düzgün fikir deyil. Nəzərə almaq lazımdır ki, viruslar müxtəlif ziyanverici proqramtəminatıdır.

Virus nədir?

*K*ompüter virusu kompüterdəki fayla və ya proqrama bərkidilmiş (yapışdırılmış), bir kompüterdən digərinə keçməklə yayılan proqramdır. Viruslar kompüterə düşməklə onun işinə maneçilik edir, kompüterdə yerinə yetirilən əməliyyatları ləngidir, kompüterin əməliyyat sistemini tamamilə korlayır. Virusların yayılmasında əsas rolu kompüterlərdə istifadə edilən fləş qurğuları, bir istifadəçinin digərinə məktub göndərdiyi zaman istifadə etdiyi e-mail, istifadəçilər arasında piratlıq (oğurluq) yolu ilə birindən digərinə ötrülən, çox istifadə edilən virus yoluxmuş proqramlar oynayır.

Heç kimə sirr deyil ki, hər bir müasir kompüterin ən böyük və qorxulu düşməni viruslardır. Virus üçün fərdi kompüterin hansı məqsədlə istifadə edilməsi, İnternetə və ya lokal şəbəkəyə qoşulub-qoşulmaması vacib deyildir. Bu gün müxtəlif ziyanverici proqramlar o qədər çoxdur ki, demək olar ki, hər bir kompüter təhlükəaltındadır.

Əslində, bu ad altında bir-neçə növ ziyanverici proqramlar gizlənir ki, bunların da çoxdandır ki, hər birinin özünəməxsus kompüterə daxil olmaqmetodikası vardır. Bu günə 50 minə yaxın kompüter virusu məlumdur. Bu kiçik ziyanverici proqramlar aşağıdakı 3 qayda ilə yaşayırlar:

- Çoxalmaq;

- Gizlənmək;
- Pozmaq (xarabetmək).

Troya atı nədir?

Troya atı yalanlardan ibarətdir. İlk baxışda troya atı istifadəçiyə özünü lazımlı proqram kimi göstərir. Amma fərdi kompüteri işə salandan sonra hər şey alt-üst olur. Əməliyyat sistemi işə düşdükdən sonra troya atı faylları proqramdan kənarlaşdırmaqla onlarda olan informasiyaları məhv edir. Troya atının digər növü də mövcuddur, o, kompüterlərə düşərək istifadəçidə qıcıqlanma yaratmaqla onu əsəbləşdirir (istədiyi ölkənin himnini çalır, mənasız sözlər ilə istifadəçini əsəbləşdirir, hazırlanmış materialı müxtəlif rənglərlə rəngləyir və s.), kompüterdən heç bir faylı kənarlaşdırmır, sadəcə olaraq istifadəçinin işinə maneçilik edir. Viruslardan və soxulcanlardan fərqli olaraq troya atı faylları korlamaqla yayılmır, özü-özünü artırmır.

Troya atı ziyanverici proqram olsada (viruslardan fərqli olaraq) və özünüçoxaltmaq qabiliyyətinə malik deyil. Troya atı faydalı funksiya yerinə yetirən proqramların altında gizlənməklə özünü maskalayır. Beləliklə, virusunun yayılması bir-başa istifadəçi ilə bağlı olur, çünki o belə virusları İnternetdən istifadə edərkən öz kompüterinə "çəkmiş" olur. İstifadəçi İnternetə qoşulanda və ya sistem resurslarından istifadə edəndə "troya atı"nı işə salan kimi lazım olan səlahiyyətləri ona verir.

Fayl virusları kompüterdə fayldan istifadə etdikdə tətbiq edilir və özlərini ya faylın əvvəlinə, ya ortasına, ya da ki, axırına yazırlar. Deməli, istifadəçi faylı açanda viruslar da onunla birlikdə işə düşür. Qeyd etmək lazımdır ki, bir virusun kompüterə daxil olması kifayətdir ki, bir müddətdən sonra kompüterdəki bütün fayllar virusa yoluxmuş olsunlar.

Soxulcan nədir?

Soxulcanları da müəyyən dərəcədə virus saymaq olar. Soxulcanlar kompüterdən kompüterə yayılırlar. Onların viruslardan əsas fərqi istifadəçinin köməkliyi (fəaliyyəti) olmadan kompüterlərdə səyahət etməsidir. Soxulcanın ən

böyük qorxusu sistemdə özü-özünü modifikasiya etməsidir (kopiyalamasıdır). Soxulcan çoxalmaqla minlərlə kompüterə öz kopiyasını göndərə bilir.

Qurdlar və ya *Şəbəkə soxulcanları* müasir viruslar hesab olunur. Belə virusların məqsədi (daha doğrusu marağı) kompüterdə çoxlu sayda faylları yoluxdurmaqdan ibarət deyil. Onların əsas məqsədi İnternetə qoşulmuş kompüterlərə daxil olmaqdır. Bu zaman iki şərt yerinə yetirilməlidir:

1. Virus avtomatik işə düşməlidir (yaxşı olar ki, əməliyyat sistemi ilə birlikdə işədüşsün);
2. Viruisa yoluxmuş fayl istifadəçidəngizlənməlidir.

Avtomatik işə düşən, operativ yaddaşda daim müəyyən funksiya yerinə yetirən virus *rezident* adlanır. İnternetdə və ya lokal şəbəkədə öz surətlərini (kopiyalarını) yayan viruslar *Şəbəkə soxulcanları* adlanır. Əksər Şəbəkə soxulcanları rezident viruslardır.

İnternetdən istifadə etməklə yayılmış viruslar daha qorxuludurlar. Onlar qurbanları olan kompüterə iki mexanizm vasitəsilə daxilolurlar:

1.Standart kommunikasiya servisləri vasitəsilə;

2.Şəbəkə əlavələrində yaranmış "boşluqlar" vasitəsilə, həmçinin Əməliyyat sisteminin özündən istifadə etməklə.

İstifadəçinin nəzərinə çatdırmaq kifayətdir ki, virusların hücumuna qarşı "dayanmaq" və onlarla müəyyən səviyyədə mübarizə aparmaq üçün kompüterdə vaxtlı-vaxtında yenilənmə aparmaq lazımdır.

Qurdlar və ya soxulcanlar Windows əməliyyat sisteminin sistem qovluqlarında özlərinə "yuva salırlar" və indiki zamanda o qədər virus vardır ki, istifadəçi demək olar ki, onların əksəriyyəti haqqında heç bir məlumatı yoxdur. Hələ viruslarla universal və etibarlı mübarizə vasitəsi yoxdur.

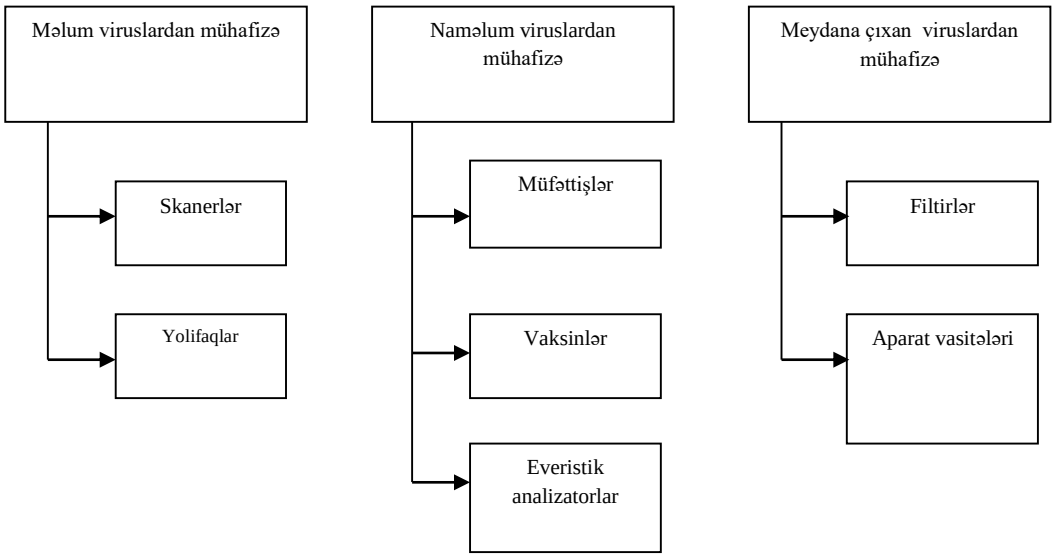
Araşdırmalar göstərir ki, 2005-ci il ərzində troya proq-ramlarının sayı təxminən iki dəfə çoxalmış, antivirus proqramlarının həcmi də bir o qədər artmışdır. Ziyanverici proqramların yalnız 5%-i zövq almaq, 75%-i pul əldə etmək, qalan 20% isə digər məqsədlər üçün yaradılmışdır. Ziyanverici proqramlara aşağıdakılar aid edilir: kompüter virusları; şəbəkə qurdları; troya proqramları; spamlar; haker utilitləri.

14. Antivirus proqramları

Antiviruslar informasiya təhlükəsizliyinin proqram-aparat vasitələrindən olub üç əsas səviyyədə virusların təyin edilməsinə ayrılırlar.

- məlum olan virusların axtarılıb tapılması, məhv edilməsi (silinməsi) və mühafizəsi (skanerlər, polifaqlar);
- məlum olmayan virusların axtarılması və məhv edilməsi mühafizəsi (rezervlər, vakansiyalar, evriki analizatorlar);
- viruslar yarandıqda (özlərini biruzə verdikdə və ya meydana gəldikdə) blakirovka edilmə ilə mühafizəsi.

Antivirus vasitələrini və səviyyələrini sxematik olaraq aşağıdakı qruplara bölmək olar (şəkil).



Fəaliyyətlərindən asılı olaraq antivirus proqramlarıbir neçə sinfə ayrılır:

Detektorlar hər hansı məlum virusa yoluxmuş faylları aşkarlamağa imkan verir.

Doktorlar (faqlar) təkcə yoluxmuş faylları aşkarlamır, həm də onları İlkin duruma qaytarmağa çalışır.

Müfəttişlər kompüter hücumları mümkün olan yerlərdəki dəyişikliklərə nəzarət edir; bu məqsədlə proqramların və disklərin sistem sahələrinin ilkin, yoluxmamış hesab

' edilən durumları haqqında məlumat yadda saxlanılır, sonra istifadəçinin müəyyən etdiyi vaxtda onları cari vəziyyətlə müqayisə edir.

Doktor-müfəttişlər yuxarıda göstərilən iki növ proqramın imkanlarını özündə birləşdirir.

Süzgəclər virusların çoxalma və zərərvurma məqsədi ilə əməliyyat sisteminə etdikləri müraciətləri tutur.

Vaksinlər, yaxud immunizatorlar iş qabiliyyətlərini saxlamaqla proqramları elə dəyişdirirlər ki, onlar viruslar üçün yoluxmuş kimi görünsün. Belə olduqda, viruslar həmin fayllara "ilişmir".

Kompüterdə virusların axtarışı verilənlər daşıyıcılarının, yaxud axınının daranması [scan] yolu ilə yerinə yetirilir. Darama prosesində operativ yaddaşda, daşıyıcılarda virusa yoluxmanın əlamətlərinin olub-olmaması yoxlanılır. Aşkarlanmış viruslar deaktivləşdirilir və məhv edilir. Mümkün olduqda dəyişdirilmiş (yoluxmuş) faylların ilkin vəziyyəti bərpa olunur.

Bu gün Symantec Norton Antivirus, Kasperski antivirusu, Dr. Web, AcAfee VirusScan, Panda Titanium Antivirus kimi antivirus proqramları daha çox tanınır

Antivirius proqramları ilə informasiya təhlükəsizliyinin qorunması üç səviyyədə formalaşdırılır:

- **Yüksək**-təhlükəsizliyin bu səviyyəsindən əgər siz tez-tez spamlar alırsınızsa istifadə edilir;
- **Orta**-təhlükəsizliyin bu səviyyəsindən çox vaxt istifadə edilir;
- **Aşağı**-təhlükəsizliyin bu səviyyəsindən əgər siz təsadüfi hallarda spama rast gəlirsinizsə, məsələn, korporativ poçt xidmətlərində istifadə etdikdə istifadə edilir.

Antivirusun aşağıdakı növləri var:

- Fayl antivirusları
- Poçt antivirusları
- WEB antivirusları
- Proqramlara nəzarət antivirusları

- Şəbəkə ekranları
- Şəbəkə hücumlarından mühafizə antivirusları
- Anti-Spam
- Şəbəkə monitorinqi
- Anti fişinqlər
- Anti-Banerlər və s.

Poçt xidmətlərini təhlükəsizliyinin təmini və yoxlanması üçün protokollardan istifadə edilir. Bu protokollar:

* IMAP, SMTP, POP3, poçt müştəriləri xidmətlərində müstəqil istifadə edilirlər;

* NNTP, poçt müştərilərindən asılı olmayan (независимо от почтового клиента);

* MAPI, HTTP poçt xidməti proqramları olan Microsoft Office Outlook və The Bat! proqramlara daxil edilir.

Antiviruslarından olan Kasperski İnternet Security-2010 proqramının yüklənməsi üçün minimal tələblərə aiddir:

1. 375-500 Mbaytdan az olmayan daimi yaddaş HDD
2. Microsoft İnternet Explorer 6.0 və ya sonrakı seriyalar
3. Windows XP
4. Prosessor 300 MHs-dən yuxarı
5. 256-512 Mbayt RAM və s.

Antivirus mühafizə vasitələrinə aşağıdakılar aiddir: fayllar, fərdi verilənlər, sistemlər və şəbəkədə işləmə:. Virusların yoxlanması və yeniləmək.

Hal hazırda geniş yayılmış antiviruslar aşağıdakılar hesab olunur. Kasperski İnternet Security 2010, 2011, Avast, Avira, Nod-32, Dr.Web və s. bunların istifadəsi zamanı onları yoluxmuş fayllardan təmizləmək, almaq, silmək kimi funksiyaların yerinə yetirilməsi verilmişdir.

Kompyuter virusları sistemin işinin pozulmasına və verilənlərin korlanmasına istiqamətlənmiş ayrı proqram sinfidir. Viruslar arasında bir sıra növlər məlumdur.

Onlardan bəziləri daimi olaraq kompyuterin yaddaşında olurlar, bəziləri birdəfəlik “zərbə” ilə destruktiv hərəkətlər istehsal edirlər. Bunlardan əlavə xaricdən tam əlverişli, əslində isə sistem korlayan proqramlar sinfi məlumdur. Belə proqramları “troyan atları”adlandırırlar. Kompyuter viruslarının əsas xüsusiyyətlərindən biri onların “çoxalma”ğa, yəni kompyuter daxilində və kompyuter şəbəkələrində sərbəst yayılmağa meyilli olmasıdır. Müxtəlif tətbiqi ofis proqram vasitələrinin xüsusi olaraq onlar üçün yazılmış proqramlarla imkanına malik olduqdan sonra zərərli proqramların yeni növləri - marko viruslar meydana gəldi. Bu növ viruslar adi fayl sənədləri ilə birgə yayılırlar və onların tərkibində adi antiproqram kimi olurlar.

Kasperiski antivirusunu (AVP) bütün antivirus mühafizə növləri istifadə edirlər: antivirus skanerləri, monitorlar, blokiratorlar və dəyişmə revizorları. Məhsulun müxtəlif versiyalarını bütün populyar əməliyyat sistemləri, poçt şlyuzləri, şəbəkə-arası ekranlar (firewalls), web-serverləri dəstəkləyirlər. Sistem virusların istifadəçinin kompyuterinə, İnternet, e-poçt, mobil informasiya daşıyıcılarıda daxil olmaqla mümkün olan daxilolma yollarına nəzarət etməyə imkan verir. Kasperiski antivirus idarə vasitələri mərkəzləşmiş quraşdırma və idarəetmə kimi əsas əməliyyatlara həm lokal kompyuterdə, həmdə müəssisənin şəbəkəsinin kompleks mühafizəsi zamanı nəzarət etməyə imkan verir. Kasperiski laboratoriyası əsas istifadəçi kateqoriyasına hesablanmış üç hazır antivirus mühafizə həllini təklif edir:

– ev istifadəçiləri üçün antivirus mühafizəsi (bir kompyuterə bir lisenziya);
– kiçik biznes üçün antivirus mühafizəsi (şəbəkədə 50 işçi stansiya);
– böyük şirkətlərdə və İnternet üzərindən verilənlərin antivirus mühafizəsi.

15.Kompüter cinayətkarlığı

Kiber təhlükəsizlik –verilənlərin əlyetənliyinin, bütövlüyünün və konfidensiallığının təmin edilməsi üçün təhlükəsizlik tədbirlərinin istifadə edilməsi prosessləridir. Sistem administratorun əsas vəzifəsi lokal şəbəkənin kompyüterlərinin, serverlərin və aktiv istifadəçilərin mühafizəsini təmin etməkdir. Kibertəhlükəsizliyiyn məqsədi verilənlərin mühafizəsidir. Verilənlərin təhlükəsizliyinin təmin edilməsi üçün əks tədbirlər görülə bilər.

Bu gün biz qlobal qarşılıqlı əlaqələr dünyasında yaşayırıq. Biz bir an içində dünyanın o biri başındakı insanlarla söhbət edə, yaxud böyük məbləğdə pul əməliyyatları həyata keçirə bilirik. Fərdi komputerlərin sayının görünməmiş surətlə artması, İnternetə sərbəst çıxış və yeni kommunikasiya qurğularının surətli inkişafı həm asudə vaxtın keçirilməsi, həm də biznesin aparılması üsullarını dəyişdirdi. Eyni zamanda qaraniyyətli insanlar üçün də yeni imkanlar açıldı, yeni cinayət üsulları meydana çıxdı. Bəşəriyyət yeni cinayət növü ilə – ***kibercinayətkarlıqla***qarşılaşdı.

Kibercinayətkarlıq dedikdə, İnternet, yaxud başqa kompüter şəbəkələrindən istifadə olunmaqla törədilən cinayətlər nəzərdə tutulur**.** "Kibercinayətkarların" hücum obyektləri, əsasən, banklar, birjalar, İnternet-mağazalar olur. Cinayətin həyata keçirilməsində komputerlər, yaxud şəbəkələrdən aşağıdakı kimi istifadə oluna bilər:

- Kompüter, yaxud şəbəkə cinayət aləti ola bilər, başqa sözlə, cinayətin həyata keçirilməsində onlardan istifadə oluna bilər.
- Kompüter, yaxud şəbəkə cinayətin hədəfi ("qurbanı") ola bilər.
- Kompüter, yaxud şəbəkə cinayətli məqsədlərə çatmaq üçün yardımçı vasitə ola bilər.

Hakerlər. Komputerlər yenicə meydana çıxanda **"haker"** sözü hörmətlə çəkilirdi. Əməliyyat sisteminin daha yaxşı işləməsi üçün onun nüvəsinin bir hissəsini yenidən yazan, yaxud hamının unutduğu administrator parolunu "ləğv edən" kompüter dahilərini belə adlandırırdılar. Qeyri-standart düşünmə qabiliyyətlərinə və ən mürəkkəb problemlərin ağıllı həllini tapdıqlarına görə bu,

onlara hörmət əlaməti idi. Lakin zaman ötdükcə bu söz əsl mənasını itirdi, çünki "hakerlərin" heç də hamısı öz ənənəvi işləriylə kifayətlənmədilər. Onların bəziləri pis mühafizə olunmuş kompüter sistemlərinə girməyə və bununla da "bunun mümkünlüyünü sübut etməyə" başladılar. Başqaları isə hər hansı mühüm informasiyanı oğurlamaq məqsədilə sistemləri "sındırmaqla" məşğul oldular. "Haker" termininin öz mənasını itirdiyini görən komputer ictimaiyyəti əlavə terminlər (məsələn, "script kiddie" və "cracker") daxil etdilər. **"Script kiddie" (ssenari uşağı)** termini ilə hakerlik sahəsində o qədər də biliyi olmayan və"sındırmaq" üçün digər hakerlərin utilitlərindən istifadəedən adamları adlandırırlar. **"Cracker" (kreker)** isə bilik səviyyəsinə görə ***"script kiddie"***ilə ***haker***arasında olan şəxsə deyilir. O, proqramların üzününçıxarılmaması üçün qoyulmuş müdafiəni "sındıra" bilir, ancaq proqramda yenizəif yerlər tapmaq, yaxud haker utilitləri yazmaq üçün onun biliyi kifayət etmir.

Proqram təminatı piratçılığı. Proqram məhsulunun alıcısı əslində yalnız həmin proqramın istifadə hüququnu əldə edir. Proqramın özü isə onun mülkiyyətinə keçmir. Ona görə də proqram məhsulunun üzünün çıxarılıb yayılması qanun pozuntusu hesab olunur. Belə hərəkətlərə ***kompüter piratçılığı***, yaxud ***proqram təminatı piratçılığı***deyilir.

Kompüter piratçılığı proqram təminatı bazarı üçün çox böyük problemdir. İstifadədə olan hər bir lisenziyalı (qanuni yolla əldə olunmuş) proqrama ən azı bir lisenziyasız, yaxud "pirat" nüsxə düşür. Bəzi ölkələrdə isə bu, 1:9 nisbətinə çatır. Piratçılıq proqram təminatı istehsalına çox mənfi təsir göstərir, yeniliyin qarşısını alır, proqram məhsulunu hazırlayanları və istehsalçıları planlaşdırdıqları gəlirdən məhrum edir.

Proqramların üzünün icazəsiz koçürülməsinin qarşısını almaq üçün xüsusi vasitələrdən istifadə oluna bilər. Lisenziyalı proqramın distributiv dəstinə daxil olan bəzi verilənlər proqramın özünə daxil olmur. Belə proqramın üzü çıxarılarkən həmin verilənlər itə bilər ki, bu da mühafizə üsullarından biridir.

Müəlliflik hüququ. İnformasiya-kommunikasiya texnologiyalarının dinamik inkişafı və komputerlərin çox surətlə insanların həyatına daxil olması ilk

vaxtlar qanunvericilərin buna hazır olmadığını göstərdi. Bir müddət kompüter proqramlarının hüquqi müdafiəsi məsələsi açıq qaldı. Lakin getdikcə bu boşluqlar doldurulmağa başlandı. Belə ki, hazırda kompüter proqramları (kompilyatorlar, redaktorlar, verilənlər bazası və s.) əmtəə məhsulu statusu almışdır və onlar da intellektual mülkiyyət kimi qorunur. Kompüter proqramlarının müəlliflik hüququnun tanınması üçün onların hər hansı qurumda qeydiyyatdan keçirilməsi vacib deyil. Proqrama müəlliflik hüququ avtomatik olaraq onun yaradılması zamanı meydana çıxır. Proqramın yaradıcısı öz hüquqlarını elan etmək üçün proqramın ilk buraxılışında üç elementdən ibarət olan müəlliflik hüququnun qorunması işarəsindən istifadə edə bilər:

- çevrənin icərisində, yaxud mötərizədə “C” hərfi – ©, (C);
- hüquq sahibinin adı;
- proqramın ilk buraxılış ili.

16.Elektron rəqəmsal imza

Rəqəmli imza və sertifikat. Kriptoqrafiya üsulları təkcə məlumatları məxfiləşdirməyə imkan vermir. Həmçinin, məlumatın tamlığını qorumaq üçün onun dəyişdirilməsi, yaxud mətnin başqası ilə əvəz edilməsi faktını, o cümlədən, məlumatın mənbəyinin həqiqiliyini aşkarlamağa imkan verən üsullar da mövcuddur. Son zamanlar ***rəqəmli imza***texnologiyası meydana çıxmışdır ki, bu da imzalanmış sənədi ancaq kağız şəklində çatdırmaq zərurətini aradan qaldırmışdır. Rəqəmli imza dedikdə, aydındır ki, söhbət imzanın skaner vasitəsilə üzünün çıxarılmasından getmir.

Rəqəmli imza, yaxud **elektron imza** şəxsi gizli şifrdir və onun açarı yalnız onun sahibinə məlumdur. Rəqəmli imza üsullarında çox zaman asimmetrik şifrləmə alqoritmlərindən – şifrləmə üçün gizli açardan, deşifrləmə üçün isə açıq açardan istifadə olunur. Rəqəmli imza məlumatın həqiqiliyinin imza sahibi tərəfindən təsdiq olunduğunu bildirir. Əgər rəqəmli imza ilə təsdiq olunmuş sənəd almısınızsa, onda sizə şifri açmaq üçün imza sahibinin vermiş olduğu açıq açar da lazımdır. Bəs, almış olduğunuz açıq açarın sənədi imzalaması tələb olunan şəxsə məxsus olduğuna necə əmin olmalı? Burada rəqəmli sertifikat köməyə gəlir.

Rəqəmli sertifikat səlahiyyətli orqan tərəfindən imzalanmış elə məlumatdır ki, orada açıq açarın həqiqətən də, imza sahibinə aid olması və deşifrləmə məqsədilə istifadə oluna bilməsi təsdiqlənir. Sertifikatlaşmaya səlahiyyəti olan orqandan sertifikat almaq üçün həmin orqana ərizəçinin kimliyi ilə bağlı müxtəlif sənədlər təqdim olunmalıdır.

Elektron rəqəmsal imza

Elektron sənədləri ilə mübadiləni yerinə yetirdikdə alınmış sənədin müəllifinin, onun doğru olub-olmamasını və informasiyanın bütöv olmasının quraşdırılması vacib əhəmiyyət kəsb edir. Bu cür məsələnin həlli elektron sənədini müşayiət edən rəqəmsal imzanın üzərinə düşür.

Funksional cəhətdən o, adi əl ilə çəkilən imza ilə analoji olur və onun aşağıdakı əsas üstün cəhətlərinə malik olur:

1) təsdiq edir ki, imzalanmış mətn onu imza edən şəxsə məxsusdur;

2) mətnə imza atan şəxsə imzalanmış mətn ilə əlaqəli olan öhdəliklərdən boyun qaçırmağa imkan vermir;
3) imzalanmış mətnin bütövlüyünə zəmanət verir.

Elektron rəqəmsal imza sənəd ilə birlikdə ötürülən nisbətən çox da böyük olmayan əlavə informasiya deməkdir. Adətən rəqəmsal imza açıq açar üsulunun tətbiq olunması ilə şifrlənir və məzmunu, imzanın özünü və bir cüt açarları əlaqələndirir. Bu elementlərdən heç olmazsa birinin dəyişdirilməsi rəqəmsal imzanın doğruluğunu təsdiq etməyə iman vermir.

Rəqəmsal imzanın formalaşması mərhələsində məxfi və açıq açar kimi iki açar generasiya olunur. Açıq açar elektron sənədinin göndərildiyi bütün abonentlərə paylaşdırılır. Sənədə əlavə olunan imza məktub göndərənin aşağıdakı parametrlərinə malik olur: imza tarixi, məktub göndərən barəsində informasiya və açıq açarın adı. Bütün sənədə tətbiq edilən xeş-funksiyanın köməkliyi ilə bütövlükdə bütün mətni xarakterizə edən çox da böyük olmayan ədəd hesablanır. Bu ədəd sonra məxfi açarla şifrlənir və elektron rəqəmsal imza rolunu oynayır. Məktub alana açıq şəkildə sənədin özü və elektron imza göndərilir.

Yoxlama zamanı məktub alana məlum olan açıq açarla rəqəmsal imzanın şifri açılır. Əldə edilmiş açıq sənədə xeş-funksiya çevirməsi tətbiq edilir. Onun işinin nəticəsi göndərilmiş elektron imza ilə müqayisə edilir. Əgər hər iki ədəd üst-üstə düşərsə, o zaman əldə edilmiş sənəd həqiqi olacaqdır. Aydındır ki, sənədə istənilən icazə verilməmiş dəyişiklik edilməsi açıq sənəd üzrə hesablanan xeş-funksiyanın qiymətinin dəyişilməsinə gətirib çıxaracaqdır, amma məxfi açarla şifrlənmiş elektron imzanı başqası ilə əvəz etmək cinayətkar üçün çox çətin olacaqdır.

Elektron imza sistemi elektron imza vasitələrinin köməyi ilə aşağıdakı iki proseduranı özündə birləşdirir:

- **elektron imzanın yaradılması;**
- **elektron imzanın yoxlanılması.**

Asan İmzailə şəxsiyyət vəsiqəsini təqdim etmədən kimliyinizi təsdi qedə ,eyni zamanda mobiltelefondan istifadə edərək sənədləri electron qaydada imzalaya bilərsiz. Yəni, sənədlərə rəqəmsal imza ata bilərsiz.

Asan İmza (Mobilimza) ilə bütünmövcude-xidmətlərdənistifadə etmək mümkündür. Asan İmzailə hökumətvətəndaş arasında bürokratik əngəlləri aradanqaldırmaq olur. Bu, o deməkdirki, Azərbaycan hökuməti telefon vasitəsilə hər zaman öz vətəndaşları ilə birlikdədir.

Asan İmza (Mobilimza) əslində electron mühitdə fiziki İD-karta bərabər sənəd kimi sertifikatlarabağlı olan mobil telefon SİM-kartınızdır.

Qeydedək ki, Asan İmzaVergilərNazirliyivə Mobil operator tərəfindən verilir.Asan İmza xidmətindən istifadə etmək üçün Asan İmza Sim kartını əldə etmək lazımdır.

Abunəçi olmaq üçün şəxsiyyət vəsiqəniz ilə (şəxsiyyət vəsiqəsi Asan İmza (Mobil imza) xidmətini aktivləşdirmək üçün lazımdır) "ASAN Xidmət" mərkəzində fəaiyyət göstərən Azercell ofisinə, Azercell Ekspres və Müştəri Xidmətləri ofislərinə (yaxın gələcəkdə isə digər mobil operatorların ofislərinə) müraciət edə bilərsiniz. Abunəçi olandan sonra siz mobil telefona daxil edilməli olan yeni Asan İmza (Mobil imza) SIM kartını alacaqsınız. Sonrakı mərhələdə tələb olunan sənədlər ilə birlikdə ASXM (Vergi ödəyicilərinə Xidmət Mərkəzlərinə, Bakı şəhər Vergilər Departamentinə.

Asan İmza (Mobil imza) PIN kodları Asan İmza (Mobil imza) SIM kartının üzərində çap olunaraq, pozulan qat altında gizlədilir. Yeni Asan İmza (Mobil imza) SIM kartının pozulan sahəsi zədələnməməlidir. Yadda saxlayın ki, şəxsiyyətin təsdiqlənməsi üçün PIN1 və imza üçün yalnız PIN2 tələb olunur.

Asan İmza (Mobil imza) elektron imza sertifikatlarının üç növü vardır: fiziki şəxslər (vətəndaşlar) üçün elektron imza sertifikatları, hüquqi və sahibkarlıq fəaliyyəti ilə məşğul olan fiziki şəxslər üçün və dövlət qulluqçuları üçün elektron imza sertifikatları.

Fiziki şəxslər (vətəndaşlar) üçün elektron imza sertifikatları şəxsi istifadə üçün nəzərdə tutulub. Siz bu sertifikatdan yalnız şəxsi identifikasiyanız üçün istifadə edə bilərsiniz.

Hüquqi şəxslər və sahibkarlıq fəaliyyəti ilə məşğul olan fiziki şəxslər, həmçinin dövlət qulluqçuları üçün nəzərdə tutulan elektron imza sertifikatları isə kommersiya və ya dövlət təşkilatını təmsil etmək və onun adından çıxış etmək səlahiyyətləriverir.

Qeyd edək ki, Asan İmza (Mobil imza) sertifikatları 3 il ərzində etibarlıdır.

Asan İmza (Mobil imza) xidmətinin istifadəsi pulludur. Xidmətlərin qiymət siyahısı sizin mobil operatorunuzun internet səhifəsində mövcuddur: Azercell, Bakcell, Nar Mobile.

17.Təhlükəsizlik siyasəti

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.

İnformasiya təhlükəsizliyi Siyasəti – təşkilatın fəaliyyətinin müəyyən aspektlərini idarə etmək üçün təsbit edilmiş qaydalardır. **İnformasiya təhlükəsizliyi siyasəti**nin 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 siyasəti**nin altçoxluğudur. Müəssisədə istifadə edilən sistem və vasitələrdən asılı olaraq informasiya təhlükəsizliyi siyasətinin tərkibinə aşağıdakı bölmələr daxil ola bilər:

- informasiya risklərinin idarə edilməsi siyasəti;
- parollardan istifadə siyasəti;
- giriş hüquqlarının verilməsi siyasəti;
- antivirus təhlükəsizliyi siyasəti;
- İnternetdən istifadə siyasəti;
- elektron poçtdan istifadə siyasəti;
- informasiya təhlükəsizliyinin monitorinqi siyasəti;
- fiziki təhlükəsizlik siyasəti;
- informasiyanın kriptoqrafik mühafizəsi siyasəti;
- şəxsi heyətin təhlükəsizliyi siyasəti;
- sistemdə dəyişiklik edilməsi siyasəti;
- şəbəkə təhlükəsizliyi siyasəti;
- korporativ informasiya sistemi resurslarına naqilsiz müraciət siyasəti;
- informasiyanın üçüncü şəxslərə və təşkilatlara verilməsi siyasəti;
- resursların təkrar istifadəsi və məhv edilməsi siyasəti;
- kompyuterlərin təşkilatdan kənarda istifadəsi siyasəti

18.Kompüter şəbəkələrində təhlükəsizlik. Şəbəkələrin informasiya təhlükəsizliyinin təmin olunması

Kompyuter şəbəkələrindən ilk vaxtlar, hətta demək olar ki ilk onillikdə unversitet tədqiqatçıları və korperasiyanın əməkdaşları arasında elektron poçtla mübadiləni aparmaq, printerdən birgə istifadə üçün istifadə edilirdi. Sözsüz, belə halda təhlükəsizlik məsələsi diqqəti cəlb etmirdi. İlk yaxınlaşmada şəbəkələrin təhlükəsizliyi şəbəkələrini bir-birilə kəsişən dörd sahəyə: məxfilik, autentifikasiya öhdəliklərin ciddi olaraq yerinə yetirilməsinin təmini və tamlığın təmininə ayırmaq olar. İkinöqtəli xətlə ötürülən paketlər verilənləri ötürmə səviyyəsində, xəttə ötürülən zaman kodlaşdırıla və qəbul zamanı əks kodlaşdırmaya məruz qala bilərlər. Bu hadisənin bütün hissələri yalnız verilənləri ötürmə səviyyəsinə məlum ola bilər. Bu zaman hətta daha yüksək səviyyələr arada nə baş verdiyindən xəbərsiz ola bilər.

Kriptoqrafiya. Kriptoqrafiya sözü “gizli məktub” mənasını daşıyan yunan sözlərindən əmələ gəlmişdir. Kriptoqrafiyanın bir neçə minilliyi əhatə etdiyi uzun və yaxşı tarixi vardır. Kompyuterlər yaranana kimi kriptoqrafiyada ən əsas faktorlardan biri şifrələyicinin lazımı çevirmələri aparmaq imkanına malik olmaması idi. Kriptoqrafiyanın əsas qanunu ondan ibarətdir ki, kriptoanalitikə (yəni kodu sındırana) istifadə olunan şifrələmə üsulu məlum olur. Yerinə qoyma üsuluna əsaslanan rəqəmlərdə hər bir simvol və ya simvollar qrupu başqa simvol və ya simvollar qrupu ilə əvəz olunur. Ən qədim şifrələrdən biri Yuli Sezar tərəfindən yaradılan Yuli Sezar şifrələridir. Bu üsul yerinə qoyma üsuluna əsaslanır, simvollar sırasını saxlayır, ancaq onları əvəz edir (əvəzləyir). Yerdəyişmə üsulunu istifadə edən şifrələr, simvolların gəlmə cərgəsini dəyişir, ancaq simvolların ölçülərini dəyişmirlər. Sınması mümkün olmayan şifrə yaratmaq əslində çox sadədir. Bunun üçün lazım olan üsul artıq bir neçə ön illərdir ki, məlumdur. Belə ki, açar kimi istənilən bit sətri götürülür. Bu sətrin uzunluğu verilmiş mətnin uzunluğu ilə üst-üstə düşür. Maraqlı budur ki, şəbəkədə bir dəfəlik ardıcıllıqla ötürmə probleminin həlli çox qədim tarixi olan kvant mexanikasından gəlir.

Birinci kriptoqrafik prinsip belədir: bütün şifrələnmiş materiallar müəyyən izafiliyə malik olmalıdır, başqa sözlə məlumatı anlamaq üçün lazım olan informasiyaya malik olmalıdır. Başqa sözlə, məlumatı əks şifrələmə zamanı qəbuledici onun doğruluğunu analiz vasitələri, hətta sadə hesablamalar aparmaqla aydın etmək imkanına malik olmalıdır. İzafilik qəbulediciləri yanlış məlumatlarla (tərkibində zibil olan, arxivləşdirmə ehtiyyat nüsxəsinin hazırlanması, bazanın sıxılması, korlanmış bazanın bərpası) aldatmağa çalışan pisniyyətlilərin həmlələrinə qarşı durmaq üçün lazımdır.

Verilənləri şifrələyən DES standartı: 1977-ci ilin yanvarında ABŞ hökuməti gizli olmayan məlumatlar üçün rəsmi standart kimi İBM firması tərəfindən işlənmiş məlumat şifrəsini qəbul etmişdir. Verilənləri şifrələyən DES yarandığı gündən ziddiyyətlərlə zəngindir. DES İBM korporasiyası tərəfindən işlənmiş və patentlənmiş Lyusufer (Lusifer) şifrəsinə əsaslanır. Fərqi bundan ibarətdir: İBM 56-mərtəbəli açar əvəzinə 128-mərtəbəli açardan istifadə edirdi.

Şifrələmə rejimi: Özünün mürəkkəbliyinə baxmayaraq AES (və ya DES yaxud da başqa bir blok kodu) faktiki olaraq uzun simvolu monoəlifbalı yerinəqoyma şifrəsindən ibarətdir (AES-də 128 bitli simvollardan, DES-də isə 64 bitli simvollardan istifadə edilir).

Kriptoanaliz: Kriptoqrafiyada simmetrik açardan istifadə haqqında fikir və mülahizələri yekunlaşdırmadan əvvəl kriptoanalizin inkişafının dörd istiqaməti ilə tanış olaq.

1976-ci ildə Stenford unversitetinin iki tədqiqatçısı, Diffi və Xellman yeni radikal kriptosistemi təklif etdilər. Burada şifrələmə və deşifrələmə açarları ayrı-ayrı olmaqla yanaşı, deşifrələmə açarını şifrələmə açarından almaq olmaz.

RSA alqoritmi: Elə bir alqoritm tapmaq lazımdır ki, bütün üç tələbi ödəsin. Açıq açarlı şifrələmə alqoritminin üstünlüyü aydın olduğundan bir sıra tədqiqatçılar uyğun alqoruitmlərin yaratmağa başladılar. Onların əksəriyyəti artıq məlumdur.

Açıq açarlı başqa alqoritmlər: RSA alqoritminin geniş yayılmasına baxmayaraq, o, açıq açarlı vahid alqoritm deyildir. Açıq açarlı ilk alqoritm "rants alqoritmi" adlanır. Burada da xoşbəxtlikdən, açıq açarla şifrələmə kömək edə bilər.

Sertifikatlar: Açarlarla mühafizə olunan mübadiləni təşkil etmək üçün ilk addım sutka ərzində internet mərkəzlə tələbata görə açarların yayımlanmasını təşkil etmək ola bilər. Sertifikat açıq açarı yalnız prinsipalla yox, atributlarla da əlaqələndirə bilər. Sertifikatlar abstrakt sintaksis 1 (ASN-Abstract Syntax Notation) OSİ yazma sistemindən istifadə etməklə şifrələnirlər.

Açıq açarlı sistemin infrastrukturu bu kompanentlərin struktur təşkilinə imkan verir və müxtəlif sənəd və protokollara aid olan standartları təyin edir. Bununla yanaşı açıq açarlı sistemin infrastrukturu sertifikatların saxlanması məsələsini də həll etməlidir. İstifadəçiləri məcbur etmək olar ki, sertifikatların özlərində saxlasınlar.

Brandmauerlər: İstənilən kompyuteri bir-biri ilə birləşdirmə imkanı bəzi hallarda yaxşı, bəzi hallarda isə pisdir. İnternetdə gəzmək əksər istifadəçilər üçün xüsusi fərəh doğurur. Belə konfiqurasiyada brandmauer iki kompanentdən ibarət olur: iki marşurutlaşdırıcı, filtrləşmə paketləri, və tətbiqi səviyyə şlüzləri. Ancaq daha sadə konstruksiyalar da məlumdur. Belə yanaşmanın üstünlüyü ondan ibarətdir ki, daxil olmaq və ya xaric olmaq arzusunda olan hər bir paket hökmən iki filtrdən və bir tətbiqi səviyyəli şlyüzündən keçməlidir. Brandmauer mexanizminin ikinci toplananı tətbiqi səviyyə şlyüzünü əks etdirir.

Xüsusi (Şərti) virtual şəbəkələr: Bir sıra kompaniyalar çoxlu sayda ayrı-ayrı şəhərlərdə, bəzi hallarda ayrı-ayrı ölkələrdə yerləşən bölmələrə, təşkilatlara malik olurlar. Verilənlərin ötürülməsi üçün ümumi müraciətli şəbəkələrin yaranmasına qədər bu təşkilatlar arasında əlaqəni yaratmaq üçün ayrılmış telefon xəttinin kirayə edilməsi adi hal idi.

Naqilsiz şəbəkələrdə təhlükəsizlik: E802.11 şəbəkələrində WEP (Wired Equivalent Privacy-naqilli şəbəkələrə ekvivalent məxfilik) adlanan verilənlərin ötürmə səviyyəsi təhlükəsizlik protokolunu əks etdirir (yazır).

Bu protokol naqilsiz lokal şəbəkələrin naqilli şəbəkələrdə olduğu kimi təhlükəsizliyini təmin edir. Buna baxmayaraq əgər bütün istifadəçilərə müxtəlif açarlar paylansa belə WEP asanlıqla sındırıla bilər. Açarlar nisbətən böyük zaman periodunda dəyişmədiklərindən, WEP standartı təkrar istifadə etmək aktından yaxa qurtarmaq üçün hər bir paketi göndərən zaman inisiallaşma vektorunu dəyişməyi təklif (məcbur yox) edir.

Bluetooth sistemində təhlükəsizlik: Bluetooth sisteminin təsir radiusu 802.11 şəbəkəsinə nisbətən kifayət qədər azdır. Ona görə də pisniyyətliyə binaya yaxın saxlanmış maşında qoyulmuş noutbukdan həmlələr etmə nəsib olmur. Buna bax-mayaraq, burada da təhlükəsizlik məsələsi əsasdır.

Elektron yazışmanın konfidensiallığı: Bir-birindən kifayət qədər uzaqda yerləşən istifadəçilər arasında yazışmalar aparılan zaman məlumatlar onlarla başqa maşınlardan keçməli olurlar. Onların hər biri daxil olan məlumatı oxuya və yaza bilərlər. **Stenoqrafiya:** Hansı ölkədə senzura geniş miqyasda istifadə olunursa daşma, xüsusi dissidentlər bu senzuranı aşmaq üçün öz üsullarından istifadə edirlər. Stenoqrafik kanal belə işləyir. Konfidensiallıq və senzura bunlar elə sahələrdir ki, burada texnoloji aspektlər arasında ciddi mübarizə gedir.

Kompüter şəbəkələrində bütün hücumlar iki sinifə bölünür: **passiv və aktiv.**

Passiv hücumlar o hücumlar hesab edilir ki, əks tərəf(bədniyyət) ötürülən məlumatı modfikasiya edə bilmir və qəbul edici ilə ötürücünün informaiya kanalına öz məlumatını yerləşdirə bilmir. Bunun məqsədi ötürülən məlumatlara qulaq asmaq və trafiki analiz etməkdir.

Aktiv hücumlar isə bunun əksinə olaraq əkstərəf(bədniyyət) ötürülən məlumatı modfikasiya edə bilir və öz məlumatı ilə əvəzləyə bilir. Aktiv hücumlarda özlüyündə fərqlənirlər.

19.Kriptoqrafiya. Kriptoqrafik şifrələnmə üsulları.

Haker hücumlarının əsas məqsədi təkcə kompüterdə olan informasiyanın məhv edilməsi deyil, həm də onların icazəsiz "ələ keçirilməsidir". Əgər bunun qarşısını texniki vasitələrin köməyilə almaq mümkün olmursa, onda ***şifrləmə*** sistemindən istifadə olunur. Şifrləmə üsulları ilə **kriptoqrafiya** məşğul olur.

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

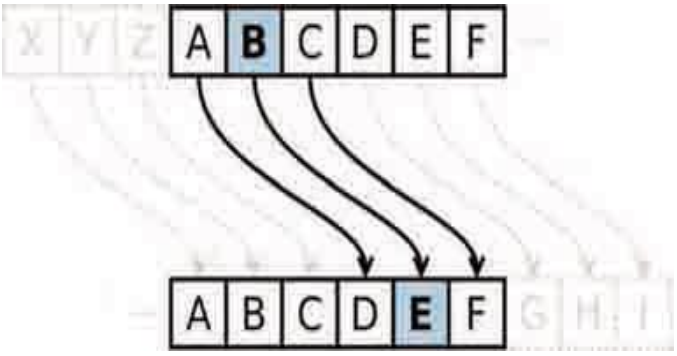
Şifrləmə zamanı A hərfi D hərfi ilə, B hərfi E ilə və beləcə əvəz olunurdu. Məsələn: VENI VIDI VICI sətri şifrləmə zamanı YHQL YLGL YLFL sətrinə keçir. Şifrlənmiş məlumatı alan hərfləri ikinci sətirdə axtarırdı və onların üstündəki hərflərə görə ilkin mətni bərpa edirdi. Sezar şifrində açar əlifbanın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

Kompüter texnikasının inkişafı ilə əlaqədar olaraq "əski" kriptoqrafiya yenidən gündəmə gəldi. Mövcud şifrləmə üsulları iki qrupa ayrılır: ***gizli***

(qapalı)açarla şifrləməvə ***açıq açarla şifrləmə***. Şifrin açılması (deşifrləmə) alqoritmini ***açar***müəyyənləşdirir.

Gizli açar elə açara deyilir ki, gizli olaraq yazışan iki abonent əvvəlcədən onu bir-birlərinə verirlər (bildirirlər). Həm şifrləmə, həm də deşifrləmə bu vahid açar vasitəsilə aparılır. Gizli yazışmada əsas məsələ bu açarı üçüncü şəxslərdən gizli saxlamaqdır.

İndi gizli açar vasitəsilə şifrləməyə aid bir misala baxaq. 1 və 32 ədədləri arasında hər hansı bir *k* ədədi götürülür. Əlifbanın hərfləri çevrə boyunca saat əqrəbi istiqamətində yazılır (belə ki, "a" hərfi "b" və "z" ilə qonşu olur). Sonra şifrlənəcək mətndə hər bir hərf "hərflər çevrəsində" ondan saat əqrəbi istiqamətində *k* sayda hərfdən sonra yerləşən hərflə əvəz olunur. Boşluq və durğu işarələri dəyişdirilmir. Belə şifrləməyə ***sürüşmə üsulu ilə şifrləmə,*** yaxud ***Sezar şifri***deyilir. Məsələn, *k* = 3 olduqda Azərbaycan əlifbasında "a" hərfi "ç" ilə, "b" hərfi "d" ilə və s. əvəz olunar. Bu cür şifrləmədən istifadə etsək, "KRİPTOQRAFİYA" sözü "MTQŞVRNTÇHQBÇ" şəklinə düşəcək.



Şəkil 4. Sezar üsulu ilə şifrələmə

Aydındır ki, belə şifri açmaq o qədər də çətin deyil. Müasir kriptoqrafiyada qat-qat mürəkkəb açarlardan istifadə olunur. XX əsrdə kriptoqrafiyaya yeni anlayış – ***asimmetrik şifrləmə alqoritmləri*** daxil oldu. **Asimmetrik alqoritmlər**, yaxud **açıq açarlı alqoritmlər** iki ayrı-ayrı açardan – ***şifrləmə* (*açıq*)** və ***deşifrləmə* (*gizli*)** açarından istifadəyə əsaslanır. Açıq açarlı alqoritmlərdə əsas tələb odur ki, açıq açara görə gizli açarı hesablayıb tapmaq mümkün olmasın. Belə olduqda şifrləmə açarı hər kəsə bildirilə bilər, onsuz da şifri açmaq üçün başqa açar gərəkdir.

Misal

Sezar üsuluna görə açıq mətin "LERİK" sözüdür. Bu mətni şifrələdikdə məlumat necə olur? Əgər Açar sözü k=3 olarsa. Şirələnmiş informasiya OHULN olur.

A	B	C	D	E	F	G	H	İ	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Sezar üsuluna görə şifrələnmiş mətin "EDNL" sözüdür. Bu mətni deşifrələdikdə məlumat necə olur? Əgər Açar sözü k=-3 olarsa. Şifrələnmiş informasiya BAKI Kimi olur.

İnformasiyanın Qronsfeld şifrinin köməyi ilə şifrələnmiş məlumat aşağıdakılardan hansı ola bilər? İnformasiya TALEH və Açar: 13512 olduqada Şifrələnmiş söz(informasiya) UDQFJ kimi olur.

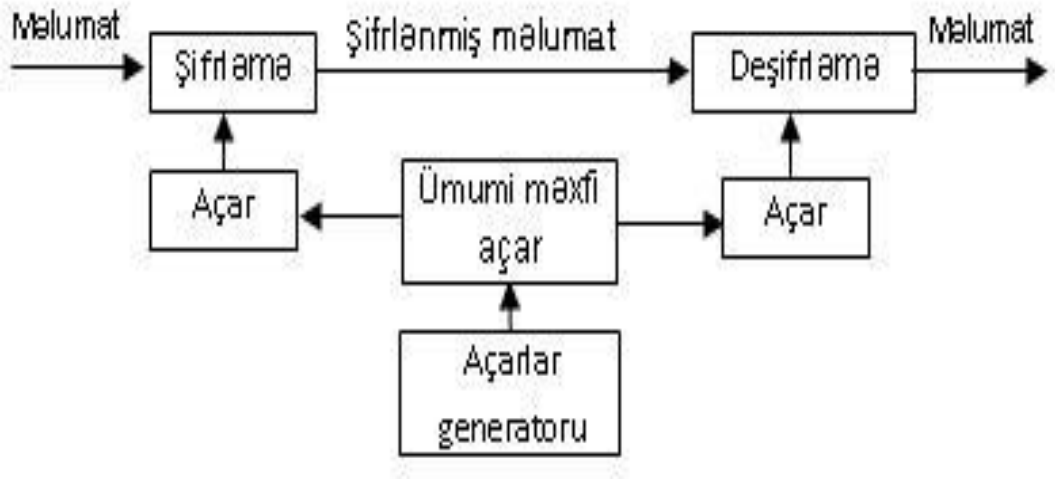
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

İnformasiyanın Qronsfeld şifrinin köməyi ilə şifrələnmiş məlumat UDQFJ ı ola bilər?Açar: 13512 olduqada deşifrələnmiş söz(informasiya) TALEH kimi olur.

20.İnformasiyanın kriptoqrafik müdafiəsinin prinsipləri

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_5 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

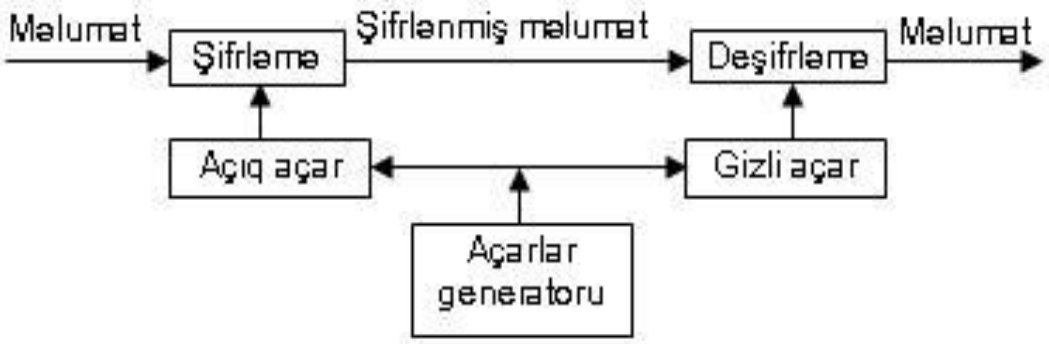


Şəkil_5. Simmetrik şifrləmə sistemi

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. Şəkil_6 asimmetrik şifrləmə sisteminin

istifadəsini illüstrasiya edir. Asimmetrik şifrləmə alqoritmlərinə misal olaraq RSA, ElGamal, Şnorr və s. alqoritmlərini göstərmək olar.



Şəkil_6. Açıq açarla şifrləmə 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 *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.

Heş-funksiyadan istifadə

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.

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.

İnformasiya gizlədilməsinin kriptoqrafik üsullarının **təsnifatı** aşağıdakı şəkildə verilmişdir:

Kompüter sisteminin istifadəçilərinin parollarını şifrləmək və elektron imza yaratmaqdan ötrü xeşləmə funksiyasından geniş istifadə olunur.

Onlar istənilən uzunluqlu məlumatı qeyd edilmiş ölçülü sətirdə təsvir edirlər. Onun tətbiqinin xüsusiyyəti ondan ibarət olur ki, sıxlaşdırılmış təsvirə görə ilkin məlumatın bərpa edilməsi mümkün olmur – buna bir tərəfli xeş-funksiya deyilir.

İstifadəçilərin parollarının olduqları və xeş-funksiya vasitəsilə çevrilmiş faylı öz əlinə keçirən cinayətkar onun əsasında parolları əldə etmək imkanına malik olmur; bu məqsədlə o, simvolların parol kombinasiyalarını bir-bir seçməli, onlara xeş-funksiya tətbiq etməli və alınmış sətirlərin və xeşləndirilmiş parollar faylının sətri ilə uyğunluğunu yoxlamalıdır. Bu iş onunla çətinləşir ki, parolunun uzunluğu da məlum olmur.

21.İnformasiya təhlükəsizliyinin və mühafizəsinin biometrik məsələləri

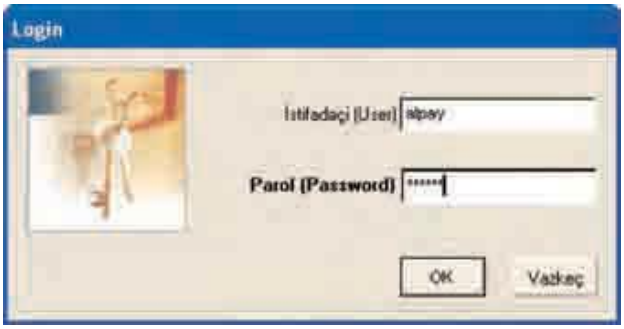
İdentifikasiya (ingilis dilində identification) istifadəçiyə (və ya müəyyən istifadəçinin adından fəaliyyət göstərən prosesə) özünü adlandırmağa (öz adını bildirməyə) imkan verir.

Autentifikasiya −identifikasiya olunan (tanınan) subyektin kim olduğunu təsdiq edən parol (**Parol** [password], yalnız verilənlərdən istifadə etmək hüququ olan şəxsin bildiyi simvollar yığınıdır), biometrik parametrlər (barmaq izlərinə görə identifikasiya, gözün qüzehli qişasının şəklinə görə identifikasiya, nitqin özəlliklərinə görə identifikasiya, üzün təsvirinə görə identifikasiya, ovucun cizgilərinə görə identifikasiya) və s. kimi məlumatların subyektdən əldə edilməsi.

Authenticate (autentifikasiya, həqiqiliyin yoxlanması)

1) İstifadəçinin, qurğunun və ya sistemin digər komponentinin həqiqiliyinin yoxlanılması; adətən sistemin resurslarına girişə icazə qərarının qəbul edilməsi üçün istifadə edilir;
2) İcazəsiz dəyişdirilməni aşkarlamaq üçün saxlanılan və ya ötürülən verilənlərin tamlığının yoxlanılması.

Verilənləri icazəsiz istifadədən qorumaq üçün, adətən, ***parol***-dan istifadə edilir. (şəkil 7). **Parol** [password], yalnız verilənlərdən istifadə etmək hüququ olan şəxsin bildiyi simvollar yığınıdır. İstifadəçi verilənlərdən istifadə hüququnu təsdiq etmək üçün özünü tanıtmalı və parolunu təqdim etməlidir.



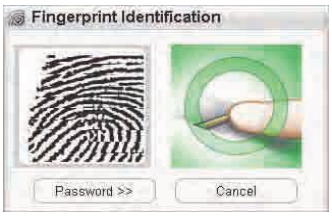
Şəkil 7. İstifadəçinin tanınması üçün dialoq boksu

Bəzən parol əvəzinə texniki vasitələrdən – elektron açarlardan, smart-kartlardan və s. istifadə olunur. ***Biometrik informasiyaya***əsaslanan mühafizə sistemləri də mövcuddur. Bu sistemlərdə istifadə olunan əlamətlər insanın

dəyişməyən xususiyyətlərinə əsaslanır və ona görə də biometrik informasiya itirilə, yaxud saxtalaşdırıla bilməz. İnformasiyanın biometrik mühafizə sistemlərinə aşağıdakı ***identifikasiya***(şəxsin tanınması) sistemləri aiddir:

a) barmaq izlərinə görə identifikasiya;
b) gözün qüzehli qişasının şəklinə görə identifikasiya;
c) nitqin özəlliklərinə görə identifikasiya;
d) üzün təsvirinə görə identifikasiya;
e) ovucun cizgilərinə görə identifikasiya.

Barmaq izlərinə görə identifikasiya. Barmaq izlərini oxu yan optik skanerlər noutbukda, kompüterin siçanında, klaviaturada, fləş diskdə quraşdırılır, həmçinin ayrıca xarici qurğular və terminallar şəklində tətbiq olunur (məsələn, aeroportlarda, banklarda və s.). Daranmış (skanerdən keçirilmiş) barmaq izinin naxışı, informasiyadan istifadəyə icazəsi olan şəxslərin heç birinin barmaq izlərinin naxışı ilə üst-ustə düşmədikdə, informasiya irişilməz olur.



Şəkil 8. Barmaq izinə görə identifikasiya

Barmaq izləri. Barmaq izlərinə (şəkil 8) görə identifikasiya texnologiyası ən geniş yayılmış biometrik texnologiyadır. Bu metodun əsasında hər bir insanın əl barmaqlarında papilyar naxışların unikallığı ideyası durur Barmaq izini papilyar xətlər əmələ gətirir, onların quruluşu dərinin şırımlarla ayrılmış qılıc çıxıntılarının sıraları ilə şərtlənir. Bu xətlər mürəkkəb naxışlar əmələ gətirirlər (qövs, ilgək və spiral), onların aşağıdakı xassələri var:

− fərdilik və təkraredilməzlik;

− zamana görə sabitlik (bətndaxili inkişafdan meyidin çürüməsinədək);

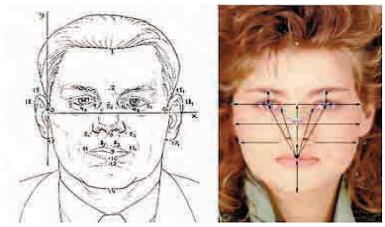
− bərpa olunma (dəri qatının səthi zədələndikdə xətlərin quruluşu əvvəlki şəklində bərpa olunur).

Barmaq izinin tanınması və onun alqoritm tərəfindən düzgün emalının keyfiyyəti barmaq səthinin vəziyyətindən və skaner elementinə nəzərən onun yerləşməsindən çox asılıdır. Müxtəlif sistemlər bu iki parametrə müxtəlif tələblər irəli sürür. Tələblərin xarakteri xüsusi halda tətbiq edilən alqoritmdən asılıdır.

Gözün qüzehli qişasının şəklinə görə identifikasiya. Gözün qüzehli qişası hər bir insanın nadir biometrik xususiyyətlərindəndir. O, insanda yaşyarımlıqdan formalaşır və əslində bütün ömrü boyu dəyişilməz qalır. Gözün təsviri alındıqdan sonra onun uzərinə xüsusi ştrix-kod maskası qoyulur. Nəticədə hər bir insan üçün fərdi matris alınır. Gözün qü zehli qişasına görə identifikasiya etmək üçün xüsusi skanerlərdən istifadə olunur.

Nitqin özəlliklərinə görə identifikasiya. İnsanın səsə görə identifikasiyası ənənəvi tanınma üsullarından biridir. Telefondakı həmsohbəti gormədən onu asanlıqla tanımaq olur. Hətta, səsinin emosional tonuna görə insanın psixoloji durumunu müəyyənləşdirmək mümkündür. Səsə görə identifikasiya nitqin tezlik analizinə əsaslanır. Hər bir insan üçün hər bir səsin (fonemin) 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 (insan saxlanılmır, onun hərəkət sərbəstliyi məhdudlaşdırılmır).



Şəkil 9. Üzün təsvirinə görə identifikasiya

İnsanın uzunə görə onun tarixcəsini, simpatiya və antipatiyasını, xəstəliklərini, emosional durumunu, ətrafdakılara bəslədiyi hissləri və onlara qarşı məqsədlərini bil mək olar. Bunların hamısı, məsələn, potensial cinayətkarı aşkara çıxarmaq üçün xüsusi maraq kəsb edir. İdentifikasiya əlamətləri üzün formasını, rəngini, həmcinin saçın rəngini nəzərə alır. Mühüm əlamətlər sırasına sifətdə

kontrastlığın dəyişildiyi yerlərin (qaşlar, gozlər, burun, qulaqlar, ağız və s.) koordinatlarını da aid etmək olar. Hazırda yeni xarici pasportların verilməsinə başlanır ki, onlardakı mikrosxemlərdə pasport sahibinin rəqəmli fotoşəkli saxlanılır.

Ovucun cizgilərinə görə identifikasiya. Biometrikada identifikasiya məqsədilə əlin olculərindən və formasından, eləcə də əlin ustundə barmaq sumuklərinin qatlanma yerlərindən, qan da mar larının yerləşməsindən əmələ gələn naxışlardan və s. istifadə olunur. Ovuca görə identifikasiya skanerləri bəzi aeroportlarda, banklarda, atom elektrik stansiyalarında quraşdırılır. Bütün ciddi tədbirlər kimi, informasiyanın mühafizəsi də kompleks şəkildə həyata keçirilməlidir, yəni yaxşı nəticələr əldə etmək üçün bütün mühafizə üsulları birləşdirilməlidir.

Səsin xarakteristikasına görə identifikasiya . Səs – sifət və ya barmaq izləri kimi hər bir insanın ayrılmaz əlamətidir. Rabitə vasitələrinin genişyayılması (stasionar və mobil telefon şəbəkələri, IP-telefoniya və s.) bu biometrik identifikatorun tətbiqi üçün böyük imkanlar açır; bundan başqa səs üzrə tanıma istifadəçilər üçün çox rahatdır və onlardan minimal səylər tələb edir. İnsanın nitqi ayrıca «səs kadrlarına» bölünür (şəkil 8), sonra onları rəqəmsal modelə çevirirlər. Bu modelləri «səs izləri» (voiceprint) adlandırırlar (barmaq izləri ilə analogiya). Yaradılan «səs izi» bazada qeydə alınır. Səs üzrə identifikasiya kodunun qurulması üçün olduqca çox sayda üsul vardır, bir qayda olaraq onlar nitqin tezlik və statistik xarakteristikalarının müxtəlif cür əlaqələndirilməsidir. İdentifikasiya zamanı əvvəl qeydə alınmış və yeni yaradılmış «səs izləri» müqayisə edilir. Etibarlığı artırmaq və tanımanı sürətləndirmək üçün çox vaxt istifadəçidən əvvəlcədən razılaşdırılmış suallara cavab verməsi və ya parolu tələffüz etməsi xahiş edilir.

22.İnformasiya təhlükəsizliyi sahəsində etik və mənəviyyat problemləri

Mənəvi-etik tədbirlər şəbəkə və informasiya texnologiyalarının yayılması və istifadəsi dövründə ənənəvi olaraq yaranmış və ya yaranmaqda olan davranış normalarından ibarətdir.

Mənəvi-etik təsirlər vasitəsilə təhlükəsizliyin təmin edilməsi istifadəçilər və xidməti personal, eləcə də ziyankarlar və bədniyyətli şəxslər tərəfindən ölkədə və cəmiyyətdə illərlə formalaşmış mənəvi-etik normalara riayət olunmasının təmin edilməsini nəzərdə tutur. Bu normaların yerinə yetirilməsi qanunvericilik tədbirlərindən fərqli olaraq məcburi deyildir, lakin bu normaların pozulması nüfuzun, hörmətin, etibarın və s. itirilməsinə gətirib çıxarır.

Daha ciddi rejimli təşkilatlarda zərurət yarandıqda qorunan informasiyanın saxlanılması, emalı və ötürülməsi üzrə müəyyən edilmiş qaydalara istifadəçilər və xidməti personal tərəfindən riayət olunmasını təmin etmək məqsədilə məcburi tədbirlər sistemi (bu, informasiya təhlükəsizliyi siyasətinin tərkibinə də daxil edilə bilər) işlənib hazırlanır və tətbiq edilir. Burada istifadəçilərin və xidməti personalın icazəsiz və qeyri-qanuni hərəkətlərinə görə maddi, inzibati və cinayət məsuliyyətinə cəlb olunması nəzərdə tutula bilər.

Qanunvericilik tədbirləri məhdud girişli informasiyanın istifadəsi, emalı, saxlanması və ötürülməsi qaydalarını nizamlayan, eləcə də bu qaydalar pozulduqda məsuliyyət tədbirlərini nəzərdə tutan hüquqi aktlarla müəyyən edilir.

Qanunvericilik tədbirləri özündə dövlət orqanlarının, təşkilatların, əhalinin (ayrı-ayrı şəxslərin) həyat və fəaliy-yətinin ayrı-ayrı sahələrinə münasibətdə dövlət tərəfindən müəyyən olunmuş və təsdiq edilmiş ümumi məcburi davranış qaydaları və normaları toplusunu, eləcə də bu normaların pozulduğu təqdirdə həyata keçirilən tədbirlər sistemini ehtiva edir.

İnformasiyanın qorunmasının hüquqi forması dedikdə dövlətin konstitusiyasının və qanunlarının maddələrinin, mülki və cinayət məcəllələrinin müddəalarının, habelə informatika, informasiya münasibətləri və informasiyanın qorunması sahəsində digər normativ- hüquqi sənədlərə əsaslanan qoruma mexanizmlərinin tətbiqi başa düşülür.

23.Əməliyyat sistemlərində təhlükəsizliyin təminatı

Əksər informasiyanın proqram müdafiə vasitələrinin çoxu tətbiqi proqramlardır. Onların yerinə yetirilməsi üçün mütləq Əməliyyat sistemindən (ƏS) dəstək lazımdır. Əməliyyat sistemlərinə məxsus olan funksiyaların yerinə yetirilməsinin əhatə dairəsi etibarlı hesablama bazası (EHB) adlanır. Etibarlı hesablama bazası informasiya təhlükəsizliyini təmin edən elementlər toplumundan ibarətdir. Bura proqramlar, şəbəkə avadanlıqları, vəsaitlərin fiziki müdafiəsi və təşkilatı prosedurlar daxildir. Əmələ gələn piramidanın əsas müdafiəsi əməliyyat sistemidir.

Əməliyyat sisteminin effektiv və etibarlı müdafiəsinin təşkili mümkün hədələrin və onların təhlükəsizliyinin öncədən təhlili olmadan mümkün deyil. Əməliyyat sistemlərinin hədələrdən təhlükəsizliyi sistemin istimar şərtlərindən, hansı informasiyanın yaddaşda saxlanılmasından, hansı informasiyanın sistemdə təhlil edilməsindən və buna bənzərlərdən hiss ediləcək dərəcədə asılıdır. Məsələn, əgər əməliyyat sistemi müəssisədə elektron sənəd dövriyyəsi üçün istifadə edilirsə, onda ən təhlükəli hədə qeyriqanuni əlçatanlığın fayllara vurduğu ziyandır. Əgər əməliyyat sistemi İnternet xidmətin provayder platformasinda istifadə edilirsə, onda ən qorxulu hücumlar əməliyyat sisteminin şəbəkə proqram təminatına edilən hücumlardır.

Əməliyyat sistemlərinin hədələrdən təhlükəsizliyini onların istifadə edilmə baxımından təsnifləşdirmək olar.

1.Hücumun məqsədinə görə:

- İnformasiyanın qeyriqanuni oxunmasına görə;
- • İnformasiyanın qeyriqanuni dəyişdirilməsinə görə;
- İnformasiyanın qeyriqanuni məhv edilməsinə görə;
- Əməliyyat sisteminin tam və ya hissə-hissə dağılmasına görə.

2.Əməliyyat sisteminə təsir prinsipinə görə:

İnformasiyanın əldə edilməsi üçün məşhur (leqal)• kanallardan istifadə edilməsi, məsələn, faylların qeyriqanuni oxunmasına hədələr və s.;

İnformasiyanın əldə edilməsi üçün gizli kanalların istifadə olunması, məsələn, bədniyyətli insanın əməliyyat sisteminin sənədləşdirilməmiş imkanlarından istifadə etmək üçün hədələrdən istifadə etməsi; Proqram əlavələrinin köməyilə informasiyanın əldə edilməsi üçün yeni kanalların yaradılması.

3.Bədniyyətli insan tərəfindən müdafiənin pis vəziyyətə salınması növünə görə: Uyğun olmayan təhlükəsizlik siyasəti, o cümlədən system inzibatçısının səhvləri;

4.Əməliyyat sisteminə etdiyi təsirin xarakterinə görə:

Aktiv təsir – pisniyyətli insanın sistemə qeyriqanuni təsir göstərməsi;

Passiv təsir – sistemdə baş verən proseslərin qeyriqanuni şəkildə pisniyyətli insan tərəfindən müşahidə edilməsi.

Əməliyyat sisteminin təhlükəsizlik hədələrini onların əlamətlərinə görə təsnif edirlər. Bunlara: pisniyyətli insan tərəfindən edilən təsirin üsulu, istifadə edilən hücum vasitələri, hücum obyektləri, hücuma məruz qalan obyektə edilən təsirin üsulları, hücum edilən obyektdə istifadə edilən əməliyyat sisteminin hücum zamanı vəziyyəti aiddir. Əməliyyat sistemi aşağıdakı hücumlara məruz qala bilər:

Fayl sisteminin skanerə edilməsi. Bədniyyətli insan kompüterin fayl sisteminə nəzər salır və bütün faylları ardıcıl oxumağa (və ya surətini almağa) cəhd göstərir. Gec və ya tez inzibatçının heç olmasa bir səhvi aşkar olunur. Nəticədə pisniyyətli insan ona qadağa qoyulmuş informasiyaya əlçatanlıq edir;

- Parolun seçilməsi. Parolun seçilməsində bir neçə üsuldan istifadə edilir:

> Ümumi izafə (izafə - normadan artıq alınmış (götürülmüş) şey anlamını verir);

> Statistikada rast gəlinən simvolların optimallaşdırılması və ya lüğətdan istifadə etməklə ümumi izafə;

> İstifadəçini tanımaqla parolun seçilməsi (onun adı, soyadı, doğum günü, telefon nömrəsi və s.);

- Açar informasiyanın oğurlanması. Pisniyyətli insan istifadəçi tərəfindən yığılmış parola baxa bilər və yaxud da, istifadəçının klaviatura üzərində əlinin

hərəkətini izləməklə onun yığdığı parolu bərpa edə bilər. Bununla yanaşı açar informasiya (smartkart, Touch Memory və başqaları) pisniyyətli insan tərəfindən sadəcə oğurlana bilər;

- "Zibil qutu"suna atılmışın toplanması. Bir çox əməliyyat sistemlərində istifadəçi tərəfindən ləğv edilmiş informasiya fiziki olaraq ləğv olunmur, sadəcə olaraq "Zibil qutusu" adlanan qutuya atılır. Bədniyyətli insan atılmış informasiyanı bərpa edir, ona baxış keçirir və ona lazım olan hissələrin (ola bilsin tam faylın) surətini alır;

- Səlahiyyətini aşma. Bədniyyətli insan əməliyyat sistemində proqram təminatındakı səhvdən və təhlükəsizlik siyasətindən istifadə etməklə özü üçün səlahiyyət əldə edir. Adətən belə hallar proqramı işə salarkən başqa istifadəçinin adından istifadə etdikdə baş verir;

- Proqrama qoşulma. Əməliyyat sistemlərində istifadə olunan proqrama qoşulma digər proqrama qoşulmalar sinifindən fərqlənmir;

- Proqrama acgözlük. Bu proqram kompüterin bəzi resurslarını ələ keçirə bilir, nəticədə digər proqramlar ya yerinə yetirilə bilmirlər, ya da ki, ağır sürətlə yerinə yetirilirlər. Acgöz proqramın işə salınması məhvə gətirib çıxarır.

Əməliyyat sistemi o vaxt müdafiə olunan sayılır ki, o kanardan edilən müxtəlif sinif hücumları dəff edə biləcək vasitələrdən istifadə edə bilsin. Müdafiə olunan əməliyyat sistemi mütləq şəkildə istifadəçinin onun resurslarına əlçatanlıq etməsinə məhdudiyyət qoyan vasitələrə malik olmalıdır. Bununla yanaşı əməliyyat sistemində istifadəçinin həqiqiliyini yoxlaya biləcək vəsaitdə olmalıdır. Əməliyyat sistemi təsadüfi təsirlərə və ya onun işini pozacaq (işdən çıxara biləcək) hallara da hazır olmalıdır.

Bəzən elə olur ki, əməliyyat sistemi bütün baş verə biləcək hədələrdən deyil, onlardan bəzilərindən müdafiə olunur. Belə olan halda əməliyyat sistemi qismən müdafiə olunan əməliyyat sistemi adlandırılır.

Windows Brandmouer - Microsoft Windows əməliyyat sisteminin təqdim etdiyi təhkükəsizlik xidmətidir. Brandmouer Windows komplektinə daxildir və sistem təzə yükləndikdə aktiv rejimdə olur. İlk dəfə Windows XP SP2 versiyasında

buraxılmışdır. Brandmauer özündə kompleks şəkildə proqram təminatı cəmləşdirir ki, bu da kompüterə internetdən və lokal şəbəkədən daxil olan bütün məlumatları yoxlayır, proqramın parametrindən asılı olaraq bəzi məlumatları kompüterə buraxır, bəzilərinə isə qadağaqoyur. Brandmouer antivirus proqramlarından fərqli olaraq kompüterə müdaxiləni də bloklaşdırır. Brandmouer ilə yanaşı antivirus proqramlarının da olması zəruridir.

Əməliyyat sistemi o vaxt müdafiə olunan sayılır ki, o kanardan edilən müxtəlif sinif hücumları dəff edə biləcək vasitələrdən istifadə edə bilsin. Müdafiə olunan əməliyyat sistemi mütləq şəkildə istifadəçinin onun resurslarına əlçatanlıq etməsinə məhdudiyyət qoyan vasitələrə malik olmalıdır. Bununla yanaşı əməliyyat sistemində istifadəçinin həqiqiliyini yoxlaya biləcək vəsaitdə olmalıdır. Əməliyyat sistemi təsadüfi təsirlərə və ya onun işini pozacaq (işdən çıxara biləcək) hallara da hazır olmalıdır. Bəzən elə olur ki, əməliyyat sistemi bütün baş verə biləcək hədələrdən deyil, onlardan bəzilərindən müdafiə olunur. Belə olan halda əməliyyat sistemi qismən müdafiə olunan əməliyyat sistemi adlandırılır.

Əməliyyat sisteminin müdafiəsinin proqram-aparat vasitələri mütləq inzibatı tədbirlər ilə tamamlanmalıdır. İnzibatçı tərəfindən daim ixtisaslaşdırılmış dəstək yerinə yetirilməsə ən etibarlı proqram-aparat müdafiəsi belə nəticəsiz alına bilər. Aşağıda əsas inzibatı tədbirlər verimişdir: 1.Əməliyyat sisteminin daim işlək olmasına nəzarətin korrektliyi xüsusilə onun altsisteminin müdafiəsi ilə bağlıdır. Belə nəzarəti təşkil etmək əlverişlidir. Bu əsasən o zaman baş verir ki, əməliyyat sistemi əsas hadisələrin (event logging) xüsusi jurnalda avtomatik olaraq qeyd olunmasını dəstəkləyir.

2. Adekvat (tam uyğun) təhlükəsizlik siyasətinin təşkili və dəstəklənməsi. Əməliyyat sisteminin təhlükəsizlik siyasəti daim korrektə edilməlidir, çünki bədniyyətli insan əməliyyat sisteminə ziyan vura bilər, onun quruluşunu dəyişər, tətbiqi proqramların qurulmasına və ya sistemdən kanarlaşdırılmasına maneçilik edə bilər.

3.İstifadəçinin əməliyyat sistemindən istifadəsinin təlimatlandırılması əməliyyat sisteminin işlədiyi zaman ərzində təhlükəsizlik tədbirlərinə riayət

edilməsinə və bu tədbirlərin həyata keçirilməsinə nəzarətin yerinə yetirilməsinə imkan verir.

4.Mütamadi olaraq ehtiyat surətlərin və əməliyyat sistemi verilənlərinin yaradılması və təzələnməsi.

5.Əməliyyat sisteminin, verilənlərin təhlükəsizlik siyasətinin və quruluşunun dəyişməsinə daim nəzarət. Belə dəyşiklikləri qeyrielektrik informasiya daşıyıcılarında saxlamaq məsləhətdir, çünki bədniyyətli insanın əməliyyat sisteminin müdafiəsini dağıdaraq sistemə daxil olması və özünü maskalayaraq qeyriqanuni fəaliyyət göstərməsi mümkün olmaz.

Əməliyyat sisteminin müdafiə altsistemi əsasən aşağıdakı funksiyaları yerinə yetirir. 1.**İdentifikasiya və autentufikasiya**. Heç bir istifadəçi özünü identifikasiya etməmiş əməliyyat sistemi ilə işə başlaya bilməz. İstifadəçi işə başlayan zaman sistemə autentifikasiya olunmuş informasiyanı təqdim etməlidir. Bununla yanaşı istifadəçi sistemə onun varlığını (yəni bu doğurdan da həmin istifadəçidir) təsdiq edəcək informasiyanı da təqdim etməlidir. 2.**Məhdudlaşdırılmış əlçatanlıq.** Hər bir istifadəçinin əməliyyat sisteminin o obyektlərinə əlçatanlığı olur ki, ona cari təhlükəsizlik siyasəti həmin obyektlərə əlçatanlığa icazə verir. **3.Audit.** Əməliyyat sistemi sistemin təhlükəsizliyini dəstəkləyən potensial qorxulu xüsusi hadisələr jurnalına reaksiya verir.

4.**Təhlükəsizlik siyasətinin idarə edilməsi.** Təhlükəsizlik siyasəti daim adekvat vəziyyətdə saxlanılmalıdır, yəni əməliyyat sisteminin işləməsi şərtlərinin dəyişməsinə çevik reaksiya verməlidir. Təhlükəsizlik siyasətinin idarə edilməsi sistem administratoru (inzibatçı) tərəfindən həyata keçirilir, administrator bunun üçün uyğun əməliyyat sisteminə qurulmuş vəsaitlərdən istifadə edir.

5.**Kriptoqrfaik funksiyalar.** İnformasiyanın müdafiə olunmasını kriptoqrafik vəsaitlərdən istifadə etmədən təsəvvür etmək mümkün deyil. Əməliyyat sistemlərində şifrələmə istifadəçinin parollarını və sistemin təhlükəsizliyini, həmçinin qorxulu olan digər verilənləri rabitə kanalları vasitəsilə ötürülməsi və saxlanması zamanı istifadə olunur.

6.**Şəbəkə funksiyaları.** Müasir əməliyyat sistemləri lokal və ya qlobal kompüter şəbəkələrin tərkibində izolə edilməmiş işləyirlər. Bir şəbəkəyə daxil olan kompüterlərin əməliyyat sistemləri müxtəlif məsələlərin həll edilməsində bir-birinin arasında qarşılıqlı əlaqədə olurlar.

Ədəbiyyatlar

1. Алгулиев Р.М. Методы синтеза адаптивных систем обеспечения информационной безопасности корпоративных сетей. – Москва, 2001. 248 с.
2. Əliquliyev R.M., İmamverdiyev Y.N. Rəqəm imzası texnologiyası, Bakı, Elm, 2003. – 132 c.
3. Галатенко В.А. Основы информационной безопасности, Москва, 2004. – 264 с.
4. Qasımov V.Ə. İnformasiya təhlükəsizliyi: kompüter cinayətkarlığı və kiberterrorçuluq, Bakı, Elm, 2007. -192 s.
5. Musayev V.H, Qənbərov M.M. «İnformasiya təhlükəsizliyi və kompüter şəbəkələri», Bakı, 2015.