AZƏRBAYCAN RESPUBLİKASI TƏHSİL NAZİRLİYİ

AZƏRBAYCAN DÖVLƏT İQTİSAD UNİVERSİTETİ (UNEC)

MAGİSTRATURA MƏRKƏZİ

Əlyazması hüququnda

YOLÇİYEVA AYSEL NATİQ

"KOMPÜTER ŞƏBƏKƏLƏRİNDƏ ETİBARLI TƏHLÜKƏSIZLİK SISTEMİNİN YARADILMASI PROBLEMLƏRİNİİN TƏHLİLİ"

mövzusunda

MAGİSTR DİSSERTASİYASI

İxtisasın şifri və adı: 060632 - **"İnformasiya texnologiyaları və sistemləri mühəndisliyi"**

İxtisaslaşma: **"İnformasiya mühafizəsi və təhlükəsizliyi"**

Elmi rəhbər:
f.- r.e.n., dos. T.Ə.ƏLİYEVA

Magistr proqramının rəhbəri:
akad. Ə.M.ABBASOV

Kafedra müdiri: akad. Ə.M.ABBASOV

BAKI – 2020

MÜNDƏRİCAT

GİRİŞ 3

I FƏSİL. İNFORMASİYA SİSTEMLƏRİNİN TƏHLÜKƏSİZLİYİ: METODLAR VƏ TEXNOLOGİYALAR 8

1.1. İnformasiya təhlükəsizliyinin əsas anlayışları 8
1.2. İnformasiya təhlükəsizliyinin problemləri, riskləri və zərərləri 15

II FƏSİL. KOMPÜTER ŞƏBƏKƏLƏRİNİN TƏHLÜKƏSİZ FƏALİYYƏTİNİN TƏMİNİ 20

2.1. Təhlükəsiz fəaliyyətin təmini üçün arxitekturaya qoyulan tələblər ... 20
2.2. İnformasiya təhlükəsizliyini təmin edən yanaşmaların Standartlaşdırılması 24

III FƏSİL. KOMPÜTER ŞƏBƏKƏLƏRİNİN TƏHLÜKƏSİZLİK SİSTEMİ: PROBLEMLƏR VƏ ONLARIN HƏLLİ YOLLARI 42

3.1. İnformasiyanın mühafizə sistemlərinin qurulma mərhələləri 42
3.2. Şəbəkələrdə və sistemlərdə informasiya sistemlərinin təhlükəsizliyini təmin edən alətlər 45
3.3. Kompüter şəbəkələrinin inteqral təhlükəsizliyinin təmin olunma üsulları 52

NƏTİCƏ VƏ TƏKLİFLƏR 71
İSTİFADƏ EDİLMİŞ ƏDƏBİYYATIN SİYAHISI 74
РЕЗЮМЕ 76
SUMMARY 77

Giriş

Mövzunun aktuallığı. Qlobal İnternetin və informasiya texnologiyalarının (İT) sürətli inkişafı insan fəaliyyətinin bütün sahələrinə təsir edən informasiya mühitinin meydana gəlməsinə səbəb oldu. Yeni texnoloji imkanlar məlumatların yayılmasını asanlaşdırır, istehsal proseslərinin səmərəliliyini artırır və işgüzar əlaqələrin genişlənməsinə öz töhfəsini verir. Kompüterlər, şəbəkələr və İnternet gündəlik həyatımızın ayrılmaz hissəsinə çevrilib. Həqiqətən də, indi həyatını elektron qlobal şəbəkə olmadan düşünən az insan tapılar. İnsanlar İnternetdə müxtəlif maliyyə əməliyyatları aparır, məhsul və ya xidmətlər sifariş verir, kredit kartlardan istifadə edir, ödənişlər edir, ünsiyyət qurur, məxfilik və qorunma tələb edən bir çox digər əməliyyatları həyata keçirir. Qeyd etmək lazımdır ki, sürətlə inkişaf edən texnologiya ilə zəngin dünyamız gündən-günə kompüter texnologiyasından və şəbəkələrindən daha çox asılı vəziyyətə gəlir. Ancaq bu asılılıq birdən – birə baş vermədi. Hər il kompüter texnologiyasına qoyulan maliyyə xərcləri xeyli artdı, bu baxımdan texnologiyaların insan fəaliyyətinin demək olar ki, bütün sahələrinə nüfuz etməsi təəccüblü deyil.

Kompüter texnologiyalarının inkişafının ilk mərhələlərində insanların əksəriyyəti bu texnologiyaların çox yaxın gələcəkdə nə qədər geniş tətbiq olunacağını təsəvvür edə bilmirdi. Buna görə, ehtimal ki, bir çoxları, sonda adi əyləncəyə çevrilə biləcək şeyləri mənimsəməyə çox vaxt və səy sərf etməyə cəsarət etmədilər. Müasir əmək bazarının tələbləri ilə müqayisədə texniki vasitələrdən istifadənin ilk dövrlərində kompüter texnologiyaları sahəsində çalışanların sayı əhəmiyyətsiz dərəcədə az idi. Bu cəmiyyətdə çalışan insanlar üçün bir-birilərinə tanış olduqlarından aralarındakı inam - etibar hissinin daha güclü olması xarakterik idi. Bundan əlavə, etibarlı olanlardan yalnız bir neçəsi bu cəmiyyətdə özünə uyğun mövqedə çalışırdı. Beləliklə, o dövrdə kompüter texnologiyaları sahəsində təhlükəsizlik problemləri praktiki olaraq yox idi. Bunun nəticəsidir ki, kompüter texnologiyaları sahəsindəki mütəxəssislər kompüter şəbəkələrinin təhlükəsizliyinə

uzun müddət əhəmiyyət verməmişlər. Bu da özünü müasir dövrlə müqayisədə daha qabarıq surətdə göstərdi.

Yaşadığımız dövrdə də kompüter vasitələrinin və İT-nin intensiv inkişafına baxmayaraq, müasir informasiya sistemləri (İS) və kompüter şəbəkələrinin texniki problemləri təəssüf ki, azalmır. Buna görə də informasiya təhlükəsizliyinin (İT.) təmin edilməsi məsələsi həm kompüter sistemləri və şəbəkələri sahəsində çalışan mütəxəssislərin, həm də çoxsaylı istifadəçilərin, o cümlədən rəqəmsal mühitdə çalışan şirkətlərin diqqətini cəlb edir. Müasir texnologiyaların, standartların, protokolların və məlumatların qorunması vasitələri haqqında müfəssəl bilgi və onların təyinatı üzrə tətbiqi olmadan kompüter sistemlərinin və şəbəkələrinin İT.-nin tələb olunan səviyyəsinə çatmaq mümkün deyil.

Hal - hazırda nəhəng sayda şəbəkələr İnternet üzərindən birləşdirilir və bu şəbəkələr sisteminin etibarlı işinin təmini üçün əməli olaraq müəyyən təhlükəsizlik tədbirlərinin görülməsi zəruridir, çünki praktiki olaraq hər hansı bir kompüterdən istənilən təşkilatın istənilən şəbəkəsinə daxil olmaq mümkündür və kompüterin sındırılması fiziki giriş tələb etmədiyindən təhlükə hər an var və artmaqdadır.

Kompüter Təhlükəsizliyi İnstitutunun (Computer Security Institute) son araşdırmaları nəticəsində əldə olunmuş məlumatlara görə, müasir dövrdə təşkilatların 70% - də şəbəkə təhlükəsizlik sistemləri sındırılır, əlavə olaraq aşkar edilən sındırılma cəhdlərinin 60% -i təşkilatların daxili şəbəkələrininin hesabına baş verir. Bu faktları nəzərə alsaq, şəbəkə təhlükəsizliyi probleminin hələ də həll olunmamış qaldığını söyləmək olar, həqiqətən də, şirkətlərin böyük əksəriyyəti təhlükəsizlik məsələlərini zamanında həll edə bilmir və bunun nəticəsində maliyyə itkiləri ilə qarşılaşırlar.

Adətən, kiçik təşkilatlar İnternetə qoşulmazdan əvvəl informasiya təhlükəsizliyi problemləri ilə qarşılaşmırdılar, tez-tez dəyişən vəziyyətə hazır deyildilər. Bir çox hallarda korporativ şəbəkələrin istifadəçiləri məlumatlarının gözlənilmədən hər hansı bir İnternet istifadəçisi üçün əlçatan olduğuna inam bəsləmirlər.

İnternetə qoşulmanın təhlükəsizlik problemlərindən biri də şəbəkələrarası ekranlardan və virtual özəl şəbəkələrdən (VPN) istifadədir. Şəbəkələrarası ekranlar təşkilatın daxili şəbəkəsi, İnternetin əlaqə nöqtəsində yerləşən və şəbəkələr arasında məlumatların ötürülməsinə nəzarət edən bir hardware-proqram sistemidir, VPN isə müəssisənin uzaqlaşdırılmış düyünləri arasında əlaqənin təşkilinə xidmət edir.

Məlumatın ələ keçirilməsi ilə yanaşı, xidmətdən imtina və xidmət oğurluğu da təhlükəli ola bilər. Bu gün informasiya və hesablama sistemləri sahəsində ən aktual problemlərdən biri İnternetdə məlumatların bütövlüyünün və məxfiiyinin mühafizəsidir. Təqdim olunan bu dissertasiya işi də məhz kompüter sistemləri və şəbəkələrində sadalanan problemlərin tədqiqinə, həmçinin etibarlı təhlükəsizlik sisteminin qurulması zamanı informasiyanın geniş istifadə olunan müasir mühafizə metodlarının, vasitə və texnologiyalarının sistemli təhlilinə həsr edilmişdir.

Tədqiqatın əsas məqsədi və vəzifələri. Etibarlılığın və təhlükəsizliyin təmini üçün kompüter şəbəkələrinin və sistemlərinin qurulmasında qarşıya çıxan problemlərin təhlili dissertasiya işinin əsas məqsədidir, tədqiqat işinin vəzifəsi isə mövcud problemlərin həlli yollarının araşdırılması, tətbiq edilən üsulların mahiyyətinin açılması və bu üsullar içərisindən ən müasir olanlarının tətbiqidir.

Tədqiqatın obyekti və predmeti. Tədqiqatın obyektini kompüter şəbəkələrinin təhlükəsizlik sistemləri, bu sistemlərin yaradılması prinsipləri təşkil edir. Tədqiqatın predmeti isə tədqiq olunan təhlükəsizlik sistemlərinin arxitekturasının işlənilməsində əsas rol oynayan təhlükəsizlik siyasətinin tədiqiqindən, beynəlxalq standartlar və təhlükəsizliyin təmini ilə bağlı yanaşmaların öyrənilməsindən ibarətdir.

Tədqiqatın informasiya bazası və işlənməsi metodları. Tədiqiqatın informasiya bazasını yerli və xarici biblioqrafik mənbələr, İnternet resursları və beynəlxalq standartlara uyğun normativ hüquqi sənədlər təşkil edir. Tədqiqat zamanı araşdırma, təhlil, qruplaşdırma, təsnifat və tətbiqi müşahidə üsullarından istifadə olunmuşdur.

Tədqiqata uyğun elmi yeniliklər. Tədiqiqatın gedişində kompüter şəbəkələrinin etibarlı təhlükəsizlik sistemlərinin qurulması üçün mövcud üsullardan

hər biri tədqiq edilmişdir. Məlumdur ki, əksər ənənəvi kompüter mühafizə sistemlərinin qurulması zamanı hələ 1970-80-ci illərdə işlənilmiş girişin məhdudlaşdırılması metodlarından istifadə olunmuşdur. Girişə nəzarət, identifikasiya, süzmə və bu kimi ənənəvi müdafiə mexanizmlərinin səmərəliliyinin kifayət olmaması onların təşkili zamanı müasir hücumlarla əlaqəli bir sıra aspektlərin nəzərə alınmaması ilə əlaqədardır. Qeyd etmək lazımdır ki, şəbəkələrarası ekranlarda, autentifikasiya serverlərində, girişi məhdud sistemlərdə mövcud mühafizə mexanizmləri yalnız hücumun reallaşması mərhələsində işləyir. Mahiyyət etibarilə bu mexanizmlər artıq icra prosesində olan hücumlardan mühafizə edə bilir. Hücumun ilk mərhələsində mühafizənin təşkilinin təmin olunması daha səmərəli nəticə verər. Yalnız ciddi cari təhlükəsizliyinə nəzarəti və vahid təhlükəsizlik siyasətini təmin edən kompleks yanaşma – adaptiv yanaşma təhlükəsizlik risklərini əhəmiyyətli dərəcədə azalda bilər. Kompüter sistemlərinin təhlükəsizliyinə adaptiv yanaşma real vaxt rejimində təhlükəsizlik risklərini aşkar etməyə, düzgün layihələndirilmiş və yaxşı idarə olunan proses və vasitələrdən istifadə etməklə onlara nəzarət etməyə imkan verir. Alınmış nəticələr bir daha sübut edir ki, kompüter şəbəkələrinin etibarlılığının və təhlükəsizliyinin təmini üçün çox yayılmış bir sıra kriptoqrafik üsullara nisbətən adaptiv yanaşmanı tətbiqi daha aktual və məqsədəuyğundur.

Tədqiqatın praktiki əhəmiyyəti. Dissertasiya mövzusu bu gün şəbəkələrin təhlükəsizliyinin təmini kimi çox aktual olan məsələlərdən birinin tədqiqinə həsr olunmuşdur. Yaşadığımız informasiya cəmiyyətində informasiya axının qarşısını alacaq bir vasitə ola bilməz. İnformasiya proseslərinin təhlükəsiz və etibarlı şəkildə həyata keçirilməsinin təmin edilməsi məhz bu prosesləri həyata keçiriəcək sistemlərin təhlükəsiz fəaliyyəti probleminin həllini şərtləndirir. Bu nöqteyi-nəzərdən tədqiqat mövsu və alınmış nəticələr mühüm praktiki əhəmiyyət daşıyır.

Dissertasiya işinin strukturu və həcmi. Dissertasiya işi girişdən, 3 fəsildən, 7 paraqrafdan, nəticə və təkliflərdən, həmçinin istifadə olunmuş ədəbiyyat siyahısından ibarətdir. Ümumi məzmun 2 sxem, 11 şəkil, 1 cədvəl və 77 səhifədə öz əksini tapır.

Təqdim olunan magistr dissertasiyasının birinci fəslində informasiya təhlükəsizliyinin əsas anlayışları və kriptoqrafik metodlar haqqında məlumat verilmiş, mühafizə olunan sistemlərin fəaliyyəti zamanı qarşıya çıxan çətinliklərin, kompüter sistemlərinin təhlükəsizliyinin təmininə yanaşmaların və təhlükəsizlik siyasətitnin xüsusiyyətlərindən, eləcə də informasiya təhlükəsizliyinin problem və risklərindən bəhs edilmişdir.

Dissertasiya işinin ikinci fəslində kompüter şəbəkələrinin təhlükəsiz iş reyiminin təmin olunması məqsədilə açıq sistemlərin arxitekturaya qoyulan konseptual tələblərə uyğun quruluş prinsiplərindən danışılmış, informasiya sistemlərinin təhlükəsizliyinin təhlil modeli tədqiq olunmuşdur, təhlükəszliyin təminatı olan yanaşmaların və standartların üstünlükləri və fərqli cəhətləri, mühafizə vasitələrinin uyğunluq meyarları və ISO 270 standartlar ailəsinin təkamül istiqamətləri öyrənilmişdir.

Dissertasiya işinin üçüncü fəslində isə kompüter şəbəkələrinin təhlükəsizlik sistemində yaranan mövcud problemlər araşdırılmışdır, mühafizə mexanizmlərinin fəaliyyəti üzrə tətbiq olunan üsulların üstünlükləri və çatışmazlıqları, həmçinin təhlükəsizliyin təmini üçün təşkil edilmiş inteqrasiya edilmiş həllər, virtual özəl şəbəkələrin qurulmasında istifadə olunan beynəlxalq standartlarla yanaşı şəbəkələrdə tətbiq edilən biometrik təhlükəsizlik sistemlərinin imkanları tədqiq edilmiş və adaptiv yanaşma metodunun tətbiqinin məqsədəuyğunluğu əsaslandırılmışdır.

I FƏSİL. İNFORMASİYA SİSTEMLƏRİNİN TƏHLÜKƏSİZLİYİ: METODLAR VƏ TEXNOLOGİYALAR

1.1. İnformasiya təhlükəsizliyinin əsas anlayışları

İnternet bu gün bütün həyat tərzini əsaslı şəkildə dəyişdirən, xüsusi elmi və texnoloji tərəqqi tempinə, fəaliyyət xarakterinə və ünsiyyət üsuluna görə fərqlənən bir texnologiyadır. İT-nin səmərəli istifadə şirkətin rəqabət qabiliyyətinin artmasında hamı tərəfindən qəbul edilmiş strateji amildir. Dünyanın bir çox müəssisəsi, elektron əməliyyatların (İnternet və digər ictimai şəbəkələr üzərindən) ayrılmaz elementi olan İnternet və elektron biznesin geniş imkanlarından istifadə etməyə keçid edir. Elektron ticarət, on-line məlumatların çatdırılması və digər xidmətlər bir çox şirkətlər üçün əsas fəaliyyətə çevrilir və onların korporativ informasiya sistemlərindən (KİS) biznesin və istehsalın idarə edilməsinin ən mühüm vasitəsi kimi geniş istifadə olunur. KİS müəssisələrin inkişafına təsir edən mühüm amil olmaqla rabitə təhlükəsizliyini təmin edərək İnternet vasitəsilə kütləvi və müxtəlif müəssisə əlaqələrinin saxlanmasını təmin edir [2]. Buna görə də İnternet, İntranet və Extranet-in [15] geniş yayılması ilə əlaqəli informasiya təhlükəsizliyi problemlərinin həlli İT-nin təchizatçıları qarşısında duran ən aktual vəzifələrdən biridir. KİS-in informasiya təhlükəsizliyini təmin etmək vəzifəsi, ənənəvi olaraq, onun inşasına qoyulan sərmayələrin qorunub saxlanması üçün informasiya təhlükəsizliyi sisteminin (İTS) yaradılması ilə həll olunur. Başqa sözlə, İTS KİS-də mövcud tətbiqlər üçün tamamilə şəffaf şəkildə işləməli və onda istifadə olunan şəbəkə texnologiyalarına tam uyğun olmalıdır.

Müasir İT-nin əsasını verilənlərin avtomatlaşdırılmış kompüter emalı təşkil edir. İnformasiyanın paylanmış idarəetmə sistemlərini yaradarkən kifayət qədər mübahisəli olan iki problemi həll etmək lazımdır. Bunlardan birincisi minimum dəyəri olan bir sistemin yaradılmasıdır. Analoji sistemlərin təşkilinin dəyəri kollektiv resurslardan istifadə dərəcəsinə mütənasibdir. Bu o deməkdir ki, sistemin

maya dəyərinin minimuma endirilməsi məqsədilə bütün istifadəçilər üçün informasiyanın saxlanmasının dəstək, proqram və aparat vasitələri də daxil olmaqla kollektiv resursun yaradılması məqsədəuyğun hesab edilir. Uğurla seçilmiş daxil olmanın təşkili və resursdan kollektiv istifadə imkanı sistemin fəaliyyətinə qoyulmuş tələblərin reallaşması zamanı onun təşkil və istismar xərclərini əhəmiyyətli dərəcədə azaldır.

Kollektiv bir resursun imkanlarından istifadə edərək məlumatların işlənməsi bu imkanların sistemin hər bir istifadəçisi üçün əlçatan olması demək deyil. Əlçatanlıq sistem yaradılarkən tərtib olunan qaydalarla (tələblərlə) müəyyən edilir. Məhz sistem istifadəçilərini ayrı-ayrı siniflərə bölərkən bu qaydalara riayət edilməsi ikinci problemi həll etmək zərurətini - məlumatların ötürülməsi və işlənməsi prosesini təşkil etmək, hər bir istifadəçi tərəfindən yalnız icazə verilmiş məlumatların alınmasını [5] müəyyənləşdirir.

Sistemin hər bir istifadəçisi üçün resursun hərtərəfli fərdiləşdirilməsi ikinci problemin optimal həlli olsa da, hər hansı verilənlərin emalı sisteminin təşkili və istismarı xərclərini xeyli artırır. Məhz bu anlamda birinci və ikinci məsələnin məqsədləri bir-birinə ziddir. Hesablama texnikasının tətbiqi sahələrinin inkişafı və genişlənməsi ilə hesablama sistemlərində təhlükəsizliyin təmin edilməsi və məlumatın qorunması problemi bir sıra obyektiv səbəblərdən böyüyür. Bunlardan ən başlıcası kompüter sistemlərinə və İT-yə inamın artmasıdır. Onlara ən məsuliyyətli işlər həvalə olunur ki, əksər insanların həyat və rifahı da məhz bunların keyfiyyətindən asılı olur. Kompüter sistemləri müəssisələrdə və atom elektrik stansiyalarında texnoloji proseslərə, təyyarə və raketlərin hərəkətinə nəzarət edir, maliyyə əməliyyatları aparır, məxfi informasiyanı emal edir.

Bu gün fərdi kompüter şəbəkələrinin inkişafı və genişlənməsi ilə əlaqədar kompüter sistemlərinin təhlükəsizliyi problemi daha da aktuallaşır. “İnformasiya təhlükəsizliyi dedikdə informasiyanın və informasiya mühitinin təsadüfi və ya düşünülmüş təbii və ya süni xarakterə malik təsirlərdən müdafiə vəziyyəti başa düşülür” [3]. Bütünlükdə bu termin altında informasiya sisteminin normal işləməsinin, məlumatların mühafizəsinin, bütövlüyünün, məxfiliyinin və

mövcudluğunun təmini məsələləri başa düşülür. İT.-nin əsas komponentləri aşağıdakıları nəzərdə tutur:

- ✓ Məxfilik, yalnız səlahiyyətli istifadəçilərin məlumatı əldə etmə imkanları ola bilər;
- ✓ məlumatın tamlığı, onun təhrif olumadan mövcudluğunun təmin olunması deməkdir;
- ✓ daxil olmanın mümkünlüyü, ehtiyac olduğu halda səlahiyyətli istifadəçilər üçün mənbələrə və əlaqəli aktivlərə çıxış təmin edilə bilər.

Bunlar informasiya təhlükəsizliyinin üç əsas prinsipidir. Bunlara əlavə olaraq orijinallıq prinsipi də vardır ki, bu da predmetin və giriş obyektinin orijinallığının təmin edilməsini tələb edir. Hesablama texnikası vasitələrinin əlçatarlılığı geniş ictimaiyyət arasında kompüter savadlılığının yayılmasına və bu da öz növbəsində dövlət və ticarət sistemlərinin işinə müdaxilə etmək üçün çoxsaylı cəhdlərə səbəb olmuş və nəticədə bu cəhdlərin əksəriyyəti kompüter sistemlərindəki məlumat sahiblərinə ciddi ziyan vurmuşdur.

Mühafizə imkanlarının vahid mənzərəsini yaratmaq olduqca çətindir, çünki İS-nin vahid mühafizə nəzəriyyəsi hələ mövcud deyil. Elmin son nailiyyətlərindən, qabaqcıl texnologiyalardan istifadə etməklə onların qurulması metodologiyası ilə bağlı bir sıra yanaşma və baxış bucağı vardır. Bu baxımdan paylanmış sistemlərdə və uzaqdan girişi olan şəbəkələrdə ötürülən informasiyanın qorunması məsələsi həmişə aktual olaraq qalmaqdadır.

Ofisin girişindəki bir mühafizəçidən tutmuş riyazi olaraq təsdiqlənmiş məlumatın mühafizə vasitələrinə qədər müxtəlif variantlar məlumdur. Bu nöqteyi-nəzərdən daha qlobal miqyasda mühafizə və onun ayrı-ayrı aspektləri - fərdi kompüterlərin, şəbəkələrin, verilənlər bazasının qorunması və s. haqqında da danışmaq olar. Qeyd etmək lazımdır ki, tamamilə etibarlı mühafizə olunan sistemlər yoxdur. Birincisi, sistemin qorunması və etibarlılığı və ikincisi, təcavüzkarların müəyyən kateqoriyalarından qorunma haqqında yalnız müəyyən ehtimal ilə danışmaq olar. Mühafizə - müdafiə və hücumun yarışmasıdır: kim daha çox bilir, investisiya qoyur, o da qalib gəlir. Mühafizə vasitələrinin fəaliyyət zamanı ortaya

çıxardığı bütün rahatsızlıqlara rəğmən onlar sistemin normal fəaliyyəti üçün mütləq zəruridir. İlk növbədə bu, elektron kommersiya və bank sistemlərinə aiddir. Yuxarıda deyilən əsas rahatsızlıqlara bunlar aiddir:

- Əksər mühafizə olunan sistemlərin fəaliyyəti zamanı yaranan əlavə çətinliklər;
- mühafizə olunan sistemin dəyərinin yüksəldilməsi;
- resurslarına əlavə yükləmə, məlumatların əldə edilməsinin yavaşlaması ilə əlaqədar eyni işi icra müddətinin artması;
- mühafizə sisteminin qorunması və dəstəklənməsi üçün məsuliyyət daşıyan əlavə kadrların cəlb edilməsi zərurəti.

Kompüterdə informasiyanın emalı sistemlərinin təhlükəsizliyi, sistemlə rabitə prosesində informasiya ehtiyatlarına ziyan vurma cəhdlərinə qarşı bacarıq qabiliyyəti kimi başa düşülür. Bu cür təhlükəsizlik işlənmiş məlumatların məxfiliyini, həmçinin sistem qaydaları və ehtiyatlarının bütövlüyünü və əlçatanlığını təmin etməklə əldə edilir.

Məxfilik informasiyanın yalnız sistemin müvafiq yoxlamadan keçmiş səlahiyyətli qurumlarına (istifadəçilərə, proqramlara, proseslərə və s.) məlum olma xassəsidir. Sistemin digər subyektləri üçün bu məlumatlar qapalı olur.

Sistemin bir komponentinin (resursunun) tamlığı – onun fəaliyyəti zamanı dəyişilməz qalma xassəsidir. Sistemın komponentlərinin dəyişilməsi səlahiyyətli subyektlər tərəfindən daxil edilə bilər.

Sistemin (resursun) əlçatarlılığı – istənilən anda səlahiyyətli subyektlərin istifadəsi üçün açıq olma xassəsidir.

Məlumat sahibi – subyekt qanunvericilik aktlarına uyğun olaraq informasiyaya sahib olmaq, istifadə, sərəncam vermək səlahiyyətlərini tam şəkildə həyata keçirən bir qurumdur. Məlumat istifadəçisi (istehlakçı), müəyyən edilmiş hüquq və qaydalara uyğun olaraq və ya pozulmaqla sahibindən və ya vasitəçisindən alınan məlumatları istifadə edən bir qurumdur. İnformasiya əldə etmək hüququ qanuni sənədlər və ya məlumat sahibi tərəfindən müəyyən edilmiş məlumatlara daxil olma

qaydalarının məcmusudur. Məlumat əldə etmə qaydası, bir subyektin məlumat əldə etməsi qaydası və şərtlərini tənzimləyən qaydalar toplusudur. Məlumat üçün icazəli və icazəsiz giriş var. Məlumat əldə etmə icazəsi – bu, girişin məhdudlaşdırılması üçün müəyyən edilmiş qaydaları pozmadan məlumat əldə etməkdir. Sistem komponentlərinə giriş hüquqlarını tənzimləmək üçün giriş nəzarət qaydalarından (informasiyaya icazəsiz daxil olma, girişə nəzarət üçün müəyyən edilmiş qaydaların pozulması) istifadə olunur. İnformasiyaya icazəsiz daxil olmanı həyata keçirən bir şəxs və ya proses giriş nəzarət qaydalarını pozucusu kimi tanınır. İcazəsiz daxil olma ən çox yayılmış kompüter pozğunluğu növüdür. Təhlükəsizlik inzibatçısı kompüter sistemini məlumatların icazəsiz əldə edilməsindən qorumaq üçün məsuliyyət daşıyır. Məlumatın əlçatanlığı, eyni zamanda, kompüter sisteminin bir komponentinin və ya mənbəyinin, yəni sistemin hüquqi şəxsləri üçün əlçatan olacağı bir komponentin və ya qaynağın mülkiyyətini də nəzərdə tutur. Mövcud ümumi girişə malik ola biləcək mənbələrin siyahısına printerlər, serverlər, işçi stansiyalar, istifadəçi məlumatları, iş üçün zəruri olan hər hansı bir məlumat daxildir.

Məlumat və sistem resurslarına çıxış ilə identifikasiya, autentifikasiya və avtorizasiya kimi mühüm anlayışların bir qrupu əlaqələndirilir. Sistemin (şəbəkənin) hər bir subyekti ilə əlaqəli olmaqla onu müəyyənləşdirən bəzi məlumatlar (say, simvol sətri) vardır. Bu məlumatlar sistemin (şəbəkənin) subyektinin identifikatorudur. Qeydə alınmış identifikatoru olan bir şəxs hüquqi şəxsdir. Subyektin identifikasiyası subyektin identifikatora görə tanınma prosedurudur. Subyekt sistemə (şəbəkəyə) daxil olmağa cəhd etdikdə identifikasiya aparılır. Sistemin subyekt ilə qarşılıqlı əlaqəsində növbəti addım subyektin identifikasiyasıdır. Subyektin identifikasiyası, subyektin müəyyən bir identifikator ilə uyğunluğunun yoxlanılmasıdır. Autentifikasiya proseduru, subyektin özünü elan etdiyi şəxs olub olmadığını müəyyənləşdirir. Subyektin identifikasiyası və autentifikasiyasından sonra daha bir prosedur - avtorizasiya aparılır. Subyektin avtorizasiyası identifikasiya və autentifikasiyanı uğurla keçmiş hüquqi subyektə müvafiq səlahiyyət və mövcud sistem (şəbəkə) mənbələrinə daxil olma imkanının verilməsi prosedurudur.

Kompüter sistemlərinin təhlükəsizliyi dedikdə onların xarici və daxili təhlükəsizliyi başa düşülür. Xarici təhlükəsizlik sistemi təbii fəlakətdən mühafizə etmə, onun ayrı-ayrı fərdi komponentlərinin oğurlanması, informasiya daşıyıcılarına daxil olmaya cəhdlərin edilməsi və ya sistemin işinin sıradan çıxması məqsədilə xaricdən müdaxiləni nəzərdə tutur. Daxili təhlükəsizliyin predmeti isə sistemin etibarlı və düzgün işləməsini, proqram və məlumatların bütövlüyünü təmin etməkdir.

Kompüter sistemləri üçün daxili təhlükəsizliyin yaradılması ilə bağlı bütün səylər, bütün istifadəçilərin və texniki xidmət işçilərinin fəaliyyətini tənzimləmək üçün, təşkilatda qurulmuş qaynaqlara və məlumatlara birbaşa və ya dolayı çıxış qaydalarına riayət etmək üçün etibarlı və rahat mexanizmlərin yaradılmasına yönəldilmişdir. Hal-hazırda kompüter sistemlərinin təhlükəsizliyini təmin etmək üçün iki yanaşma – fraqmentar və kompleks yanaşma [6] mümkündür.

Fraqmentar yanaşma, müəyyən şərtlər daxilində konkret təhlükələrə qarşı yönəlmişdir. Bu cür yanaşmanın nümunələri ixtisaslaşdırılmış antivirus alətləri, fərdi qeydiyyat və idarəetmə tədbirləri, fərdi şifrələmə vasitələri və s. ola bilər. Fraqmentar yanaşmanın əsas çatışmayan xüsusiyyəti, informasiya emalının vahid mühafizə olunan mühitininin qeyri-mövcudluğudur. Fraqmentar yanaşmanın üstünlüyü isə onun konkret təhlükəyə və müəyyən bir istiqamətdə hərəkətlərin səmərəliliyinə nəzərən yüksək seçiciliyidir, hətta təhdiddəki kiçik bir dəyişiklik də mühafizənin səmərəliliyinin itirilməsinə səbəb olur. Lokal tədbirlər sırasının bütün sistemə genişləndirilməsi praktiki olaraq qeyri-mümkündür.

Kompleks yanaşmanın xüsusiyyəti, təhdidlərə qarşı müxtəlif - hüquqi, təşkilati, proqram təminatı və texniki tədbirləri özündə cəmləşdirən etibarlı məlumat emalı mühitinin yaradılmasıdır. İnformasiya emalı proseslərinin qaydaları əsasında mühafizə olunan məlumat emalı mühiti formalaşır. Təhlükəsiz bir mühitin təşkili, qəbul edilmiş təhlükəsizlik siyasətinin sərhədləri daxilində sistemin lazımi səviyyədə mühafizəsini təmin etməyə imkan verir. Kompleks yanaşma həm də çox istifadəçisi olan böyük dövlət və ya ticarət sistemlərinin, həm də əhəmiyyətli

iqtisadi, siyasi və ya hərbi məlumatları emal edən nisbətən kiçik sistemlərin mühafizəsi üçün istifadə olunur.

Etibarlı mühafizənin təşkili üçün hansı hücum növlərindən qorunmaq lazım olduğunu aydın şəkildə başa düşmək lazımdır. Təhlükəsizliyin təhdidi – sistemə İS-nin resurslarına birbaşa və ya dolayı yolla zərər verə biləcək potensial təsirdir. Təhdidin reallaşdırılması isə hücum adlanır. Təhlükəsizlik təhdidləri aşağıdakı meyarlara görə təsnif edilə bilər:

- hücum məqsədləri;
- sistemə təsir prinsipi;
- hücum obyektləri;
- hücumun aparılması üsulları.

Hər növ hücumlar nəticəsi olaraq ortaya çıxan itkilər, ümumiyyətlə, onların baş vermə tezliyinə tərs mütənasibdir. Laqeydliklə əlaqədar pozuntulardan, sistemi yoxlamaq cəhdlərindən minimal proqram və aparat xərcləri ilə qorunmaq tələb edilir. Mühafizə təhdidlərin həyata keçirilmə ehtimalına və təhdid dərəcəsinə uyğun olmalıdır. Yalnız təhdidlərin hərtərəfli təhlili və İS-nin mühafizə dərəcəsi nisbi təhlükəsizliyi təmin edə bilər.

Təhlükəsizlik siyasətinin iki növü vardır:

- Seçici;
- səlahiyyətli.

Təhlükəsizliyin seçici siyasəti. Bu yanaşmanın əsasını daxil olmanın seçici idarəetməsidir. Sistemin riyazi modeli əsasında daxil olma matrisi tapılır, bu matrisdə sütun sistemin obyektinə, sətir sistemin subyektinə uyğun gəlir. Matrisin sətir və sütunun kəsişməsində yerləşən elementin qiyməti subyektin obyektə icazəli daxil olmasının tipini müəyyənləşdirir.

Təhlükəsizliyinn səlahiyyətli siyasəti aşağıdakı şərtləri nəzərdə tutur:

- Bütün obyekt və subyektlər birqiymətli identifikasiya olunmalıdır.
- Hər bir obyektin informasiyanın dəyərini təyin edən bir kritiklik işarəsi vardır.
- Sistemin hər bir subyektinə şəffaflıq səviyyəsi mənimsədilir.

- Obyekt mühüm olduqca onun kritiklik əlaməti də yüksək olur.

Şəffaflıq səviyyəsindən başqa hər bir subyekt təhlükəsizlik səviyyəsinin cari qiymətinə malikdir; sonuncusu minimal səviyyədən şəffaflığa qədər dəyişə bilər. Daxil olma icazəsi barədə qərar qəbul etmək üçün hər bir obyektin kritik əlaməti şəffaflıq səviyyəsi və subyektin mövcud təhlükəsizlik səviyyəsi ilə müqayisə edilir. İnformasiya yalnız "yuxarı" ötürülə bilər, yəni obyektin cari təhlükəsizlik səviyyəsi, obyektin kritik əlamətindən aşağı deyilsə, obyektə daxil ola bilər. Səlahiyyətli təhlükəsizlik siyasətinin əsas təyinatı müxtəlif kritiklik səviyyələri ilə girişi tənzimləmək və iyerarxiyanın yuxarı səviyyələrindən aşağıya icazəsiz məlumat ötürülməsinin qarşısını almaq, həmçinin aşağıdan yuxarı səviyyələrə mümkün keçidlərin qarşısını almaqdır.

Seçici və səlahiyyətli giriş nəzarəti, həmçinin məlumat axınının idarə edilməsi, həmçinin informasiya axınlarının idarə edilməsi mühafizə metodologiyasının üç tərkib hissəsidir.

Təhlükəsizlik siyasətinin həyata keçirilməsinə cavabdeh olan bütün vasitələr hər hansı bir müdaxilədən qorunmalıdır. Onlar etibarlı hesablama bazalarına birləşdirilir. Bu, təhlükəsizlik siyasətinin həyata keçirilməsi və dəstəklənməsi üçün məsuliyyət daşıyan tam qorunan hesablama sistemi mexanizmidir (hardware və proqram təminatı daxildir). Onun funksiyaları mühafizə mexanizmlərinin bütövlüyünü dəstəkləmək və sistemin subyektləri və obyektlərinin qorunmasını təmin etməkdir [4].

1.2. İnformasiya təhlükəsizliyinin problemləri, riskləri və zərərləri

Məlumatlara təhdid və ya icazəsiz daxil olma üçün bir neçə mənbə mövcuddur. Birincisi, antropogen xarakterli mənbələrdir. Buraya müxtəlif subyektlərin hərəkətləri daxildir. Onlar qəsdən və ya təsadüfi olmaqla xarici və daxili tiplərə bölünürlər. Birincisi, bir şəxsin ümumi təyinatlı xarici şəbəkədən qanunsuz girişini nəzərdə tutur. İkincisi, daxildən, məsələn, bir şirkət işçisi tərəfindən hərəkəti əhatə

edir. Bir proqramın və qurğunun işinin yubanmasına və ya dayandırılmasına səbəb olan hər şey texnogen mənbələrə aiddir. Burada adi bir proqram təminatının səhvləri, köhnəlmiş qurğular və ya sistemlər, aparatdakı çatışmazlıqlar (kabel və ya disk sistemi, serverdəki problem, iş stansiyası) səbəb ola bilər.

Bəzi fövqəladə hallar üçün kortəbii mənbələri fərqləndirirlər. Bunlara hər cür təbii fəlakətlər kimi, fors-major halları da daxildir.

Məlumatın sızmasının və ona icazəsiz daxil olmanın şəbəkələrdə baş verməsinin bir çox səbəbləri vardır [8]:

- İnformasiyanın ələ keçirilməsi;
- informasiyanın dəyişdirilməsi (ilkin sənədin və ya mesajın dəyişdirilməsi və ya mütləq dəyişdirilərək sonradan adresata göndərilməsi);
- müəllifliyin saxtalaşdırılması (başqasının adından hər hansı bir məlumatın göndərilməsi);
- avadanlıqların və ya rabitə xəttlərinin serverə qanunsuz qoşulması;
- kiminsə səlahiyyətli istifadəçi kimi maskalanması, başqasının məlumatlarına və səlahiyyətlərinə sahiblənməsi;
- yeni istifadəçilərin daxil edilməsi;
- təhlükəsizlik tədbirləri aradan qaldırıldıqdan sonra, saxlama vasitələrinin və sənədlərin surətinin çıxarılması;
- arxivləşdirilmiş məlumatların səhv saxlanması;
- personalın və ya istifadəçilərin qeyri-korrekt işi;
- kompüter virusunun tətbiqi;
- əməliyyat sistemindəki və ya tətbiqi proqramdakı çatışmazlıqlardan istifadəçiyə qarşı istifadə edilməsi.

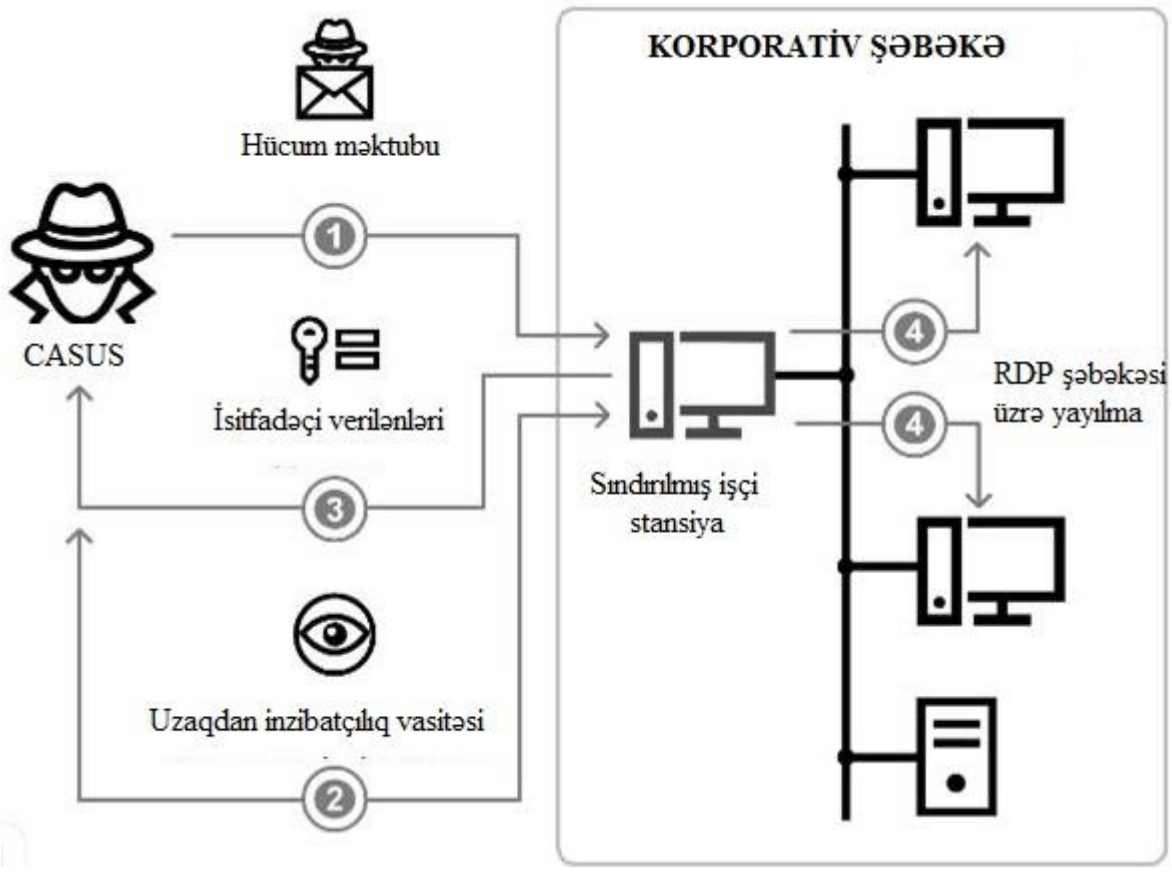
Elmi və texniki tərəqqi sürətlə genişlənir, yeni həllər yaradır və yeni problemlərlə bizi üz-üzə qoyur. İnformasiya texnologiyalarının optimallaşdırılması məlumatların rəqəmsal nüsxələrinin hesabına məhsuldarlığa təsir göstərir, fiziki daşıyıcıya görə məsələn, nüsxələrin son məlumat mənbəyini amortizasiya etmədən uzun müddətə saxlanması, fiziki məkanın qorunması və s. kimi bir sıra üstünlüklərə

malikdirlər. Bu səbəbdən müasir reallıqlarda idarəetməni həyata keçirmək üçün məlumatın qorunması ən mühüm aspektlərdən biridir. Bu fakt korporativ şəbəkələrin fəaliyyətinin bütün mərhələlərində nəzərə alınmalıdır. Təhdidlərə ən çox məruz qalan məhz bu şəbəkədir, çünki müəssisənin fəaliyyəti üçün zəruri olan məlumatlar buradan axıb keçir. Şəbəkənin işinin dayanacağı anda bütün mühasibat və istehsal fəaliyyətlərinin iflic olacağını və bunun da müəssisə üçün böyük itkilərə səbəb olacağını göz önünə almaq heç də çətin məsələ deyil.

İnformasiya təhlükəsizliyi, bir-birini dəstəkləyən və tamamlayan bir neçə paralel işləmə bacarığı olan proqram və aparat həllərinin informasiya təhlükəsizliyinə əsaslanmalıdır. Mütəxəssislər anlamalıdırlar ki, korporativ məlumatların qorunması üçün müasir texnologiyaların düzgün istifadəsi müəssisənin uğurunun açarıdır və buna laqeyd yanaşma mənfi maliyyə və imic nəticələrinə səbəb olur.

Məlum faktdır ki, infomasiya sistemləri üçün bir tərəfdən trojan virusu, digər tərəfdən isə casus proqramı, həmçinin spam da əhəmiyyətli dərəcədə böyük təhlükə yaradır. Məxfi məlumat əldə etməyə yönəlmiş İnternet fırıldaqçılığının bir növü olan fişinq hücumunun nümunəsi sxem 1.1-də verilmişdir [14].

Sistemin təhlükəsizliyini təmin edən mühüm amillərdən biri də təşkilatın işçiləridir. Məsələn, poçt xidmətlərindən savadsız istifadə virusun bütün sistemə nüfuz etməsinə səbəb ola bilər, çünki e-poçt mesajları vasitəsilə zərərli proqramların yayılması ən çox yayılmış hücum növlərindən biridir. Zərərli alqoritmlər sistemin tamamilə bağlanmasına, məlumatların itirilməsinə və sızmasına, uğursuzluğa səbəb olur. İnformasiyanın təhlükəsizliyini təmin etmək üçün məlumatların firewall, kriptoqrafiya, identifikasiya, qeydiyyat, daxil olma və daxil olmaya nəzarət kimi mühafizə üsulları mövcuddur.



Sxem 1.1. Fişinq hücumunun sxemi

Qeyd etmək lazımdır ki, İT.-nin təmini ilə bağlı problemlər hər bir dövlətin və müvafiq mühafizə strukturlarının nəzarəti altındadır. Bu problemlərin həlli yollarının axtarılması və zamanında qərarların qəbul edilməsi bilavasitə dövlətin milli maraqları çərçivəsində tənzimlənir, normativ hüquqi aktların tələblərində əks olunur və həmin maraqların müdafiəsinə yönəlmiş tədbirlərin həyata keçirilməsini nəzərdə tutur [1, səh.22].

Bir qayda olaraq məlumatlar təyinatı üzrə ünvana çatmazdan əvvəl bir sıra server və marşrutlaşdırıcıdan keçir və bu proses marşrut boyunca izlənilir, nəzarətin zəif təşkil olunduğu qovşaqlarda məlumatın tamlığı ilə əlaqədar hər bir hadisə baş verə bilər. İnternet öz arxitekturasına görə təcavüzkarlara tam fəaliyyət azadlığı verir. İnternet sistemi tamamilə korporativ olaraq yaransa da, zaman keçdikcə özlərinə məhdud girişi nəzərdə tutan yalnız tədris, kommersiya, dövlət, idarəçilik və hərbi şəbəkələrlə deyil, eyni zamanda hər hansı bir ev kompüterindən asanlıqla

İnternetə daxil olan sadə istifadəçilərlə də adi modem və ictimai telefon şəbəkəsindən istifadə etməklə fəaliyyətini genişləndirdi. Bu halda vahid TCP / IP protokollar ailəsindən və ünvanlanma məkanından istifadə olunmağa başlanıldı. İnternetə bu qədər asanlıqla daxil olma şəbəkələrdə informasiyanın təhlükəsizliyinə mənfi təsir göstərdiyinə görə faylların və ya proqramların surətinin çıxarılma imkanı olmaqla yanaşı onların pozulma və düzəliş ehtimalının mövcudluğu da hər zaman gözləniləndir. İnternetdə məlumatların qorunması hər hansı bir böyük şirkətin və ya təşkilatın əsas problemlərindən biridir. Daha ehtiyatlı olanlar mühafizənin əvvəlcədən necə həyata keçirilməsini planlaşdırır, digərləri isə ilk xoşagəlməz haldan sonra bu barədə düşünürlər. Ona görə də mühafizə vasitələrindən zamanında istifadə etmək daha məqsədəuyğundur.

II FƏSİL. KOMPÜTER ŞƏBƏKƏLƏRİNİN TƏHLÜKƏSİZ FƏALİYYƏTİNİN TƏMİNİ

2.1. Təhlükəsiz fəaliyyətin təmini üçün arxitekturaya qoyulan tələblər

Açıq sistemlərin ideologiyası mürəkkəb paylanmış İS-nin metodoloji aspektlərinə və inkişaf istiqamətinə əhəmiyyətli dərəcədə təsir göstərmişdir. Bu ideologiya profil, protokol, de-fakto[1] və de jure[2] standartlarının məcmusuna ciddi riayət edilməsinə əsaslanır. Onun proqram və aparat komponentləri portativliyin ən vacib tələblərinə və digər uzaq komponentlərlə əlaqəli, birgə işləmə imkanlarına cavab verməlidir. Bu, müxtəlif məlumat sistemlərinin, eləcə də məlumat ötürmə mühitinin komponentlərinin uyğunluğunu təmin etməyə imkan verir. Məsələ hesablama aparatı platformalarının, əməliyyat sistemlərinin (ƏS) və qarşılıqlı fəaliyyət proseslərinin dəyişilməsi zamanı işlənmiş və sınanmış proqram və məlumat komponentlərinin maksimum şəkildə təkrar istifadəsinə gətirilir.

Paylanmış mürəkkəb İS-nin yaradılması, onun arxitektura və infrastrukturunun layihələndirilməsi, onlar arasındakı komponent və əlaqələrin seçimi zamanı ümumi (açıqlıq, miqyaslılıq, keçiricilik, hərəkətlilik, investisiyanın mühafizəsi və s.) tələblərlə yanaşı verilənlərin və sistemin təhlükəsiz fəaliyyətinin təmin edilməsinə yönəlmiş bir sıra spesifik konseptual tələblər nəzərə alınmalıdır:

- Sistemin arxitekturası kifayət qədər çevik olmalıdır, yəni təməl struktur dəyişiklikləri olmadan, istifadə olunan vasitələrin infrastruktur inkişafı və konfiqurasiya dəyişiklikləri, tətbiq sahələrinin və məsələlərinin genişlənməsinə müvafiq İS –nin funksiya və resurslarının artırılmasına imkan verməlidir;

[1] “De-fakto” termini bəzi hərəkətlərin qanun nəzərə alınmadan həyata keçirildiyinə işarə edir.
[2] "De jure" termininin mənası "qanuna görə" deməkdir, birinciyə əks termindir. Ümumiyyətlə, peşəkar hüquqşünaslar və ya politoloqlar tərəfindən istifadə olunur.

- sistemin müxtəlif təhdidlər altında fəaliyyətinin təhlükəsizliyi, məlumatların layihə səhvlərindən, məlumatların məhv edilməsi və ya itirilməsindən etibarlı qorunması, həmçinin istifadəçi avtorizasiyası, işçi yükün idarə edilməsi, məlumatların və hesablama mənbələrinin ehtiyat nüsxəsi və İS - nin fəaliyyətinin ən sürətli bərpası təmin edilməlidir;
- müasir qrafik alətlər, mnemonik diaqramlar və vizual istifadəçi interfeysləri əsasında İS - nin fəaliyyətinin nəticələrinə və xidmətlərə maksimum dərəcədə əlverişli sadələşdirilmiş daxil olmanı təmin etmək lazımdır;
- sistem İS - nin ixtisaslı istismarını və inkişafının mümkünlüyünü təmin edən yenilənmiş tam sənədlərlə müşayiət olunmalıdır.

Texniki təhlükəsizlik sistemlərinin nə qədər güclü olmasına baxmayaraq, onlar öz növbəsində proqram - texniki təminatının mühafizə səviyyəsinin etibarlılığına zəmanət verə bilməz. Yalnız bir təhlükəsizlik yönümlü İS arxitekturası xidmətlərin inteqrasiyasını təsirli hala gətirə bilər, məlumat sisteminin idarə edilməsini, yüksək performans, sadəlik və istifadə əlverişliliyi kimi xüsusiyyətlərini qoruyarkən yeni təhdidlərə qarşı çıxma qabiliyyətini təmin edə bilər. Bu tələbləri yerinə yetirmək üçün İS - nin arxitekturası aşağıdakı prinsiplər əsasında qurulmalıdır:

- Açıq sistemlərin prinsipləri əsasında İS-nin qurulması, tanınmış standartlardan və sübut edilmiş həllərdən istifadə etməklə, hər səviyyədə az sayda qurum olan İS-nin iyerarxik təşkili - bütün bunlar İS-nin şəffaflığını və yaxşı idarə olunmasını şərtləndirir.
- Məkan və zamanda mühafizənin davamlılığı, mühafizə vasitələrinin öhdəsindən gələ bilməməsi, təhlükəli bir vəziyyətə kortəbii və ya məcburi şəkildə keçidin istisna edilməsi - fövqəladə vəziyyət də daxil olmaqla, mühafizə vasitələri ya öz funksiyalarını tam yerinə yetirir və ya sistemə və ya onun müəyyən hissəsinə girişi tamamilə bloklayır.
- Ən zəif əlaqənin gücləndirilməsi, giriş imtiyazlarının minimallaşdırılması, xidmət funksiyalarının ayrılması kimi vəzifə və öhdəçiliklərin paylaşdırılması nəzərdə tutulur.

Proqram - texniki səviyyəyə münasibətdə güzəştlərin minimuma endirilməsi prinsipi istifadəçilərə və inzibatçılara yalnız rəsmi vəzifələrini yerinə yetirmək üçün lazım olan giriş hüquqlarının verilməsini tələb edir. Bu, istifadəçilərin və inzibatçıların təsadüfən və ya qəsdən səhv hərəkətlərindən ziyanı azaltmağa imkan verir.

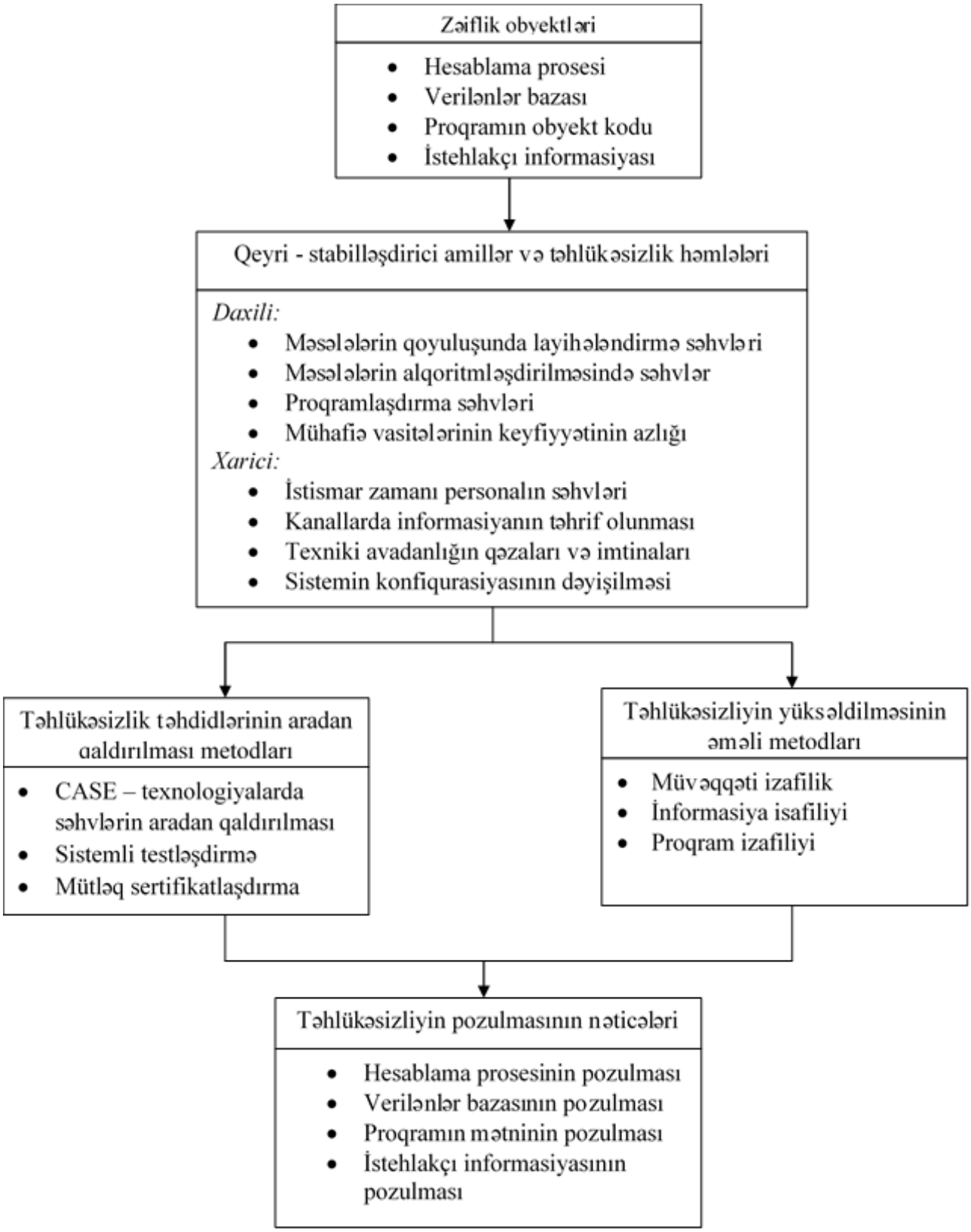
Müdafiənin ayrılması, mühafizə vasitələrinin müxtəlifliyi, İS-nin və təhlükəsizlik sisteminin sadəliyi və idarəediciliyi məsələlərinə diqqət edək. Müdafiənin ayrılması prinsipi nə qədər etibarlı görünsə də, bir müdafiə xəttinə etibar etməməyi tələb edir. Fiziki müdafiə vasitəsi olaraq proqram və aparat vasitələri, identifikasiya və autentifikasiya olaraq girişə nəzarət, protokollaşdırma və audit olmalıdır.

Ayrılmış mühafizə nəinki təcavüzkarın ötürülməsinə imkan vermir, eyni zamanda bəzi hallarda giriş və audit vasitəsilə onu müəyyənləşdirə bilir. Mühafizə vasitələrinin müxtəlifliyi təbiətinə görə fərqli olan müdafiə xətlərinin yaradılmasını nəzərdə tutur ki, bu da potensial təcavüzkardan müxtəlif və mümkün qədər müvafiq olmayan bacarıqların mənimsənilməsini tələb edir.

İS – nin layihələndirilməsi mərhələsində arxitektura və infrastrukturun formalaşması üçün yüksək tələblər, bu mərhələdə proqram, verilənlər bazası və rabitə sistemlərinin təhlükəsizliyinə təsir edən təsadüfi sabitləşdirici amillərlə əlaqəli zəifliklərin sayının əhəmiyyətli dərəcədə azaldılması ilə müəyyən edilir.

Zərərli amillər olmadıqda İS-nin təhlükəsizliyinin təhlili onun əsas komponentləri arasında qarşılıqlı əlaqə modelinə əsaslanır (şək.2.1) [10].

Bu təhdidlərin tamamilə aradan qaldırılması prinsipcə mümkün deyil. Məsələ onların asılı olduqları amilləri müəyyənləşdirmək, İS təhlükəsizliyinə təsirlərini azaltmaq üçün metod və vasitələr yaratmaq, eyni zamanda bütün mənfi təsirlərə bərabər olan mühafizəni təmin etmək üçün ehtiyatların səmərəli paylanmasıdır.



Şəkil 2.1. Zərərli təhdid olmadıqda İS-nin təhlükəsizliyinin təhlili modeli

2.2. İnformasiya təhlükəsizliyini təmin edən yanaşmaların standartlaşdırılması

İnformasiya təhlükəsizliyi problemi istifadəçi üçün dəyəri yüksək olan məlumatları kompüterdə emal etməyə başlandığı andan etibarən meydana çıxdı. Kompüter şəbəkələrinin inkişafı və elektron xidmətlərə artan tələb ilə, informasiya təhlükəsizliyi sahəsindəki vəziyyət ciddi şəkildə kəskinləşdi və onun həllinə yanaşmaların standartlaşdırılması həm İT vasitələrini yaradanlar, həm də İT istifadəçiləri üçün aktual oldu.

İnformasiya təhlükəsizliyi standartlarının əsas məqsədi İT məhsullarının kvalifikasiyası üzrə istehlakçılar, istehsalçılar və ekspertlərlər arasında qarşılıqlı təsir üçün əlverişli zəmin yaratmaqdır. Bu qruplardan hər birinin informasiya təhlükəsizliyi probleminə özünəməxsus maraqları və baxışları vardır.

İstehlakçılar, ehtiyaclarına cavab verən və problemlərini həll edən, təhlükəsizlik reytinqi miqyasına ehtiyac duyduqları məhsulun seçimini mümkün edən metodologiyaya maraq göstərirlər. İstehlakçıların öz tələblərini istehsalçılara çatdıra biləcək bir alətə daima ehtiyacları vardır. Eyni zamanda istehlakçılar yalnız son məhsulun əldə olunma üsulları və vasitələri ilə deyil, məhz onların xüsusiyyətləri və xassələri ilə maraqlanırlar. Təəssüflə qeyd etmək lazımdır ki, əksər istehlakçılar təhlükəsizlik tələblərinin mütləq funksional tələblərə (istifadənin asanlığı, sürət və s.) zidd olduğunu, uyğunluğa müəyyən məhdudiyyətlərin tətbiq edildiyini və bir qayda olaraq, geniş yayılmış və buna görə mühafizəsi zəif olan tətbiq proqram vasitələrindən məcburi imtina etməyin zəruriliyini başa düşmürlər.

İstehsalçılar istehsal etdikləri məhsulların imkanlarını müqayisə etmək, həmçinin müştərinin müəyyən bir məhsul haqqında təsəvvürünü məhdudlaşdıra bilən və onu bu seçim üzrə tələbləri qəbul etməyə məcbur edən təhlükəsizlik tələblərinin müəyyən bir dəstini standartlaşdırmaq məqsədilə sertifikatlaşdırma prosedurunun xüsusiyyətlərinin obyektiv qiymətləndirilməsi mexanizmi kimi standartlara böyük ehtiyac duyurlar. İstehsalçının nöqteyi-nəzərindən təhlükəsizlik

tələbləri mümkün qədər konkret olmalı və müəyyən vasitələrdən, mexanizmlərdən, alqoritmlərdən və s. istifadənin zəruriliyi tənzimlənməlidir.

Bundan əlavə, tələblər informasiya emalının mövcud paradiqmalarına, kompüter sistemlərinin arxitekturasına və informasiya məhsullarının təşkili texnologiyalarına zidd olmamalıdır. Lakin bu yanaşma da dominant olaraq qəbul edilə bilməz, çünki istifadəçilərin ehtiyaclarını nəzərə almır və mühafizə tələblərini mövcud sistem və texnologiyalara uyğunlaşdırmağa cəhd edir.

Kvakifikaisyalı ekspertlər və ixtisas üzrə sertifikasiya olunmuş mütəxəssislər standartlara onlara İT məhsulları ilə təmin olunan təhlükəsizlik səviyyəsini qiymətləndirməyə və istehlakçılara əsaslandırılmış seçim imkanı təqdim edən bir alət kimi baxırlar. Kvakifikasiyalı ekspetlər ikili mövqedədirlər: bir tərəfdən, istehsalçılar kimi, aydın və sadə meyarlarla maraqlanaraq onların konkret məhsula tətbiqi barədə düşünmək istəmirlər, digər tərəfdən isə istifadəçilərə məhsulun qarşı tərəfin ehtiyaclarını ödəyib-ödəməməsi barədə əsaslandırılmış cavab verməlidirlər.

Beləliklə, informasiya təhlükəsizliyi standartları qarşısında üç fərqli nöqteyi-nəzəri uzlaşdırmaq və bütün tərəflərin qarşılıqlı təsir mexanizmini yaratmaq kimi çətin bir vəzifə durur. Belə ki, bunlardan ən azı birinin ehtiyaclarının pozulması qarşılıqlı anlaşmanın və əlaqənin qeyri – mümkünlüyünə gətirib çıxaracaq və buna görə də ümumi problemin həllinə - informasiyanın təhlükəsiz emalı sisteminin yaradılmasına imkan verməyəcəkdir.

Bu cür standartlara olan ehtiyac uzun müddət öncə tanınmış və 1990-cı illərin inkişaf sənədlərində təsbit edildiyi kimi, bu istiqamətdə də ciddi irəliləyiş əldə edilmişdir. İlk və ən məşhur sənəd Narıncı Kitab (örtük rənginə görə), ABŞ Müdafiə Nazirliyinin "Kompüter Sistemlərinin Təhlükəsizliyi meyarları" idi. Bu sənəd 4 təhlükəsizlik səviyyəsini - D, C, B və A səviyyələrini müəyyənləşdirir. D səviyyəsindən A səviyyəsinə keçid sistemin etibarlılığına daha ciddi tələblər qoyulur. C və B səviyyələri Cl, C2, B1, B2 və B3 siniflərinə bölünür.

Sertifikatlaşdırma proseduru nəticəsində sistemin müəyyən bir sinfə aid edilməsi üçün onun mühafizəsi razılaşdırılmış tələblərə cavab verməlidir. Bu nəslin digər mühüm informasiya təhlükəsizliyi standartlarına aşağıdakılar daxildir:

"Avropa İnformasiya Texnologiyaları Təhlükəsizliyi Meyarları",

"ABŞ Federal İnformasiya Texnologiyaları Təhlükəsizliyi Meyarları",

"Kanada Kompüter Sistemləri Təhlükəsizlik Meyarları" [9, 12].

Son zamanlarda müxtəlif ölkələrdə şirkətin İT.-nin idarə edilməsinin praktik məsələlərinə həsr olunmuş yeni nəsil standartlar meydana çıxdı. Əvvəla, bunlar ISO 15408, ISO 17799 və digərləri kimi İT.-nin beynəlxalq idarəetmə standartlardır. Bu sənədlərin içərisindən ən mühümünü təhlil etmək, tələbləri və meyarları müqayisə etmək, həmçinin İT.-nin praktiki tətbiqinin səmərəliliyini qiymətləndirmək məqsədəuyğundur.

Beynəlxalq və milli standartlara uyğun olaraq hər hansı bir şirkətdə İT.-nin təmini məsələsi aşağıdakıları əhatə edir:

- Kompüter sistemlərinin informasiya təhlükəsizliyini təmini məqsədlərinin müəyyən edilməsi;
- effektiv informasiya təhlükəsizliyi idarəetmə sisteminin yaradılması;
- İT.-nin hədəflərə uyğunluğunun qiymətləndirilməsi üçün detallı keyfiyyət və kəmiyyət göstəricilərinin hesablanması;
- informasiya təhlükəsizliyini təmin etmə və mövcud vəziyyətini qiymətləndirmə vasitələrindən istifadə;
- informasiya aktivlərinin təhlükəsizliyinin obyektiv qiymətləndirilməsi və şirkətin informasiya təhlükəsizliyinin idarə edilməsi üçün təhlükəsizlik idarəetmə metodlarından istifadə.

Daha çox istifadə edilə bilən və informasiya təhlükəsizliyi sahəsində ən məşhur beynəlxalq standartları nəzərdən keçirək [11]. BMT-nin cinayətlərin qarşısının alınması və mübarizə komitəsinin məlumatına görə, kompüter cinayətləri beynəlxalq problemlərdən biri səviyyəsinə çatmışdır. Buna görə texniki baxımdan əsaslı fərqləri olmayan və əsasən miqyası və açıqlığı ilə fərqlənən qlobal İnternet və əlaqəli İntranet şəbəkələrində kommersiya məlumatlarının təhlükəsizliyinin təmini problemlərinin səmərəli həllinə nail olmaq olduqca vacibdir. IP / TCP rabitə

protokolu vasitəsilə şəbəkələrdə kommersiya məlumatlarının təhlükəsizliyinin təmini prosesinin standartlaşdırma xüsusiyyətlərini nəzərdən keçirək [19].

İT təhlükəsizliyinin təmin edilməsi, dövlət sirri olmayan məhdud daxil olma məlumatlarını emal edən kommersiya təyinatlı açıq sistemlər üçün xüsusilə vacibdir. Açıq sistemlər dedikdə beynəlxalq standartların tələblərinə müvafiq müxtəlif istehsala uyğun olan və birgə işləməsi təmin olunan hər cür hesablama və telekommunikasiya avadanlıqlarının toplusu başa düşülür.

"Açıq sistemlər" termini eyni zamanda bir kompüter sisteminin standartlara uyğun olacağı təqdirdə eyni standartlara uyğun hər hansı digər sistemlə əlaqəyə açıq olacağını ifadə edir. Bu, xüsusi halda məlumatın kriptoqrafik qorunması mexanizmlərinə və ya məlumatların icazəsiz əldə edilməsindən qorunmağa aiddir.

İnternetin mühüm xidməti bu cür texnologiyaları yenidən ortaya gətirməsidir. Birincisi, İnternet böyük maraq kəsb edən açıq standartların tətbiq edilməsini təşviq edir. İkincisi, dünyada müxtəlif kompüterlərin birləşdirildiyi nəhəng və yeganə şəbəkədir. Nəhayət, İnternet dünya bazarında sürətlə dəyişən yeni məhsulların və yeni texnologiyaların təqdimatı üçün ümumi qəbul edilmiş bir vasitəyə çevrilir. İnternetdə təklif edilən texnologiyaları standartlaşdırma prosesindən keçirən bir sıra könüllü təşkilatlardan ibarət komitələr vardır. IETF (Internet Engineering Task Force) – İnternet mühəndislərinin işçi qrupunun əsas hissəsini təşkil edən bu komitələr İnternetdə onların tətbiqini sürətləndirməklə bir neçə mühüm protokolun standartlaşdırılmasını həyata keçirir. IETF səylərinin bilavasitə nəticələri verilənlərin ötürülməsi üçün TCP / IP protokollar ailəsi, elektron poçt üçün SMTP (Simple Mail Transport Protocol) və POP (Post Office Protocol), həmçinin şəbəkənin idarə edilməsi üçün SNMP (Simple Network Management Protocol) protokollarıdır. İnternetdə verilənlərin təhlükəsiz ötürülməsi üçün SSL, SET və IPSec protokolları da çox populyardır. Sadalanan protokollar qlobal şəbəkədə qiymətli məlumatların qorunması zərurəti kimi meydana çıxmış və dərhal de-fakto standartlarına çevrilmişdir.

SSL (Secure Socket Layer) şəbəkə üzərində təhlükəsiz ötürülmə üçün məlumatın şifrələnməsini həyata keçirən şəbəkə protokoludur, təhlükəsiz əlaqə qurmağa, məlumatların bütövlüyünə nəzarət etməyə və müxtəli müvafiq vəzifələri həll etməyə imkan verir. SSL protokolu müasir kriptovalyutadan istifadə edərək HTTP, FTP və s. kimi xidmət protokolları və TCP/IP nəqliyyat protokolları arasında verilənlərin qorunmasını təmin edir.

SSL İnternetin texniki əlaqələndirici institutlarından kənarda inkişaf etmiş sənaye protokoluna çevrildi. SSL protokolu aparıcı Qərb şirkətlərinin istehsal etdiyi server və müştəri proqramları tərəfindən dəstəklənir. SSL protokolunun ən çatışmayan cəhəti ondan ibarətdir ki, SSL ixrac məhdudiyyətləri səbəbindən onu dəstəkləyən məhsullar ABŞ xaricində yalnız məhdud variantda mövcuddur.

SSL müəyyən şərtlər daxilində identifikasiya və şifrələmə üçün eyni düymələrdən istifadə edir, bu da potensial zəifliyə səbəb ola bilər. Belə bir həll müxtəlif açarlarla identifikasiya və şifrələmə ilə müqayisədə daha çox statistik material toplamağa imkan verir.

Protokol SET (Security Electronics Transaction) – İnternet vasitəsilə elektron ticarətin təşkili üçün hazırlanmış və İnternetdə təhlükəsiz elektron əməliyyatlar üçün perspektivli standartdır. SET protokolu X.509 standartına uyğun rəqəmsal sertifikatların istifadəsinə əsaslanır.

Təhlükəsiz əməliyyat protokolu SET MasterCard və Visa tərəfindən, həmçinin müəyyən dərəcədə IBM, GlobeSet və digər şirkətlər tərəfindən işlənilmiş standartdır. Müştərilərə təhlükəsiz bir ödəmə mexanizmindən istifadə edərək İnternet üzərindən məhsul alma imkanı verir. SET İnternetdə plastik kartlardan istifadə etməklə təhlükəsiz ödənişlər üçün açıq olan çoxtərəfli standart bir protokoldur. SET kart sahibinin hesabı, satıcı və bankın ödəmə hazırlığını, mesajın bütövlüyünü və məxfiliyini, qiymətli və həssas məlumatların şifrələnməsini yoxlamaq üçün çarpaz identifikasiyasını təmin edir. Buna görə SET daha düzgün bir standart texnologiya və ya İnternet üzərindən plastik kartlardan istifadə edərək etibarlı ödənişlərin aparılması üçün protokollar sistemi adlandırıla bilər. SET istehlakçılara və satıcılara rəqəmsal sertifikatların tətbiqi vasitəsilə kriptoqrafiyadan

istifadə etməklə İnternetdə baş verən hər bir əməliyyatın bütün iştirakçılarının həqiqiliyini yoxlamağa imkan verir.

Daha əvvəl də qeyd edildiyi kimi, informasiyanın mühafizəsinin əsas məsələləri onun əldə olunmasını, məxfiliyini, bütövlüyünü və hüquqi əhəmiyyətini təmin etməkdir. SET digər protokollardan fərqli olaraq məlumatların qorunması ilə bağlı bu problemləri həll etməyə imkan verir. Xüsusi halda elektron ticarət əməliyyatlarını qorumaq üçün aşağıdakı xüsusi tələbləri təmin edir:

- Ödəniş məlumatları ilə birlikdə ötürülən məlumatların və sifariş məlumatlarının məxfiliyi;
- ödənişlərin bütövlüyünün qorunma imkanı, belə ki, ödəniş məlumatlarının bütövlüyü rəqəmsal imza ilə təmin edilir;
- identifikasiya üçün xüsusi açıq açar kriptovalyutası;
- kredit kartı üzrə sahibinin identifikasiyası. Bu rəqəmsal imza və kart sahibi sertifikatlarının istifadəsi ilə təmin edilir;
- satıcı identifikasiyası, rəqəmsal imzalardan və satıcı sertifikatlarından istifadə etməklə plastik kart ödənişlərini qəbul etmə imkanı;
- satıcı bankının kart emalı sistemi ilə əlaqə vasitəsilə plastik kartlarla ödənişləri qəbul edə bilən aktiv bir təşkilat olduğunu təsdiqləmək. Satıcı bankının identifikasiyası rəqəmsal imza və satıcı bankın sertifikatları ilə təmin edilir;
- bütün tərəflər üçün açıq açar sertifikatının təsdiqlənməsi nəticəsində əməliyyatlar üçün ödəməyə hazır olma;
- kriptoqrafiyanın güzəştli istifadəsi ilə məlumat ötürülməsi təhlükəsizliyi.

Mövcud digər məlumat təhlükəsizliyi sistemlərindən SET-in əsas üstünlüyü kart sahibi, satıcı və satıcı bankını Visa və Mastercard ödəmə sistemlərinin bank təşkilatları ilə əlaqələndirən rəqəmsal sertifikatlardan (X509 standartı, versiya 3) istifadəsidir. Bundan əlavə, SET bank, kart sahibləri və satıcılar arasında mövcud münasibətləri qoruma və mövcud sistemlərlə inteqrasiya imkanı verir.

PKI (Public Key Infrastructure - Açıq açarları olan idarəetmə infrastrukturu) açıq açaqları olan kriptoqrafiyanın tətbiqinə əsaslanan elektron sənəd dövriyyəsinin kriptoqrafik açarlarının etibarlı idarə olunması üçün nəzərdə tutulmuşdur. Bu infrastruktur, X.509 beynəlxalq standartının tövsiyələrinə cavab verən rəqəmsal sertifikatlardan, bu sertifikatların verilməsini və saxlanılmasını təmin edən geniş sertifikatlaşdırma mərkəzlərindən istifadəni əhatə edir.

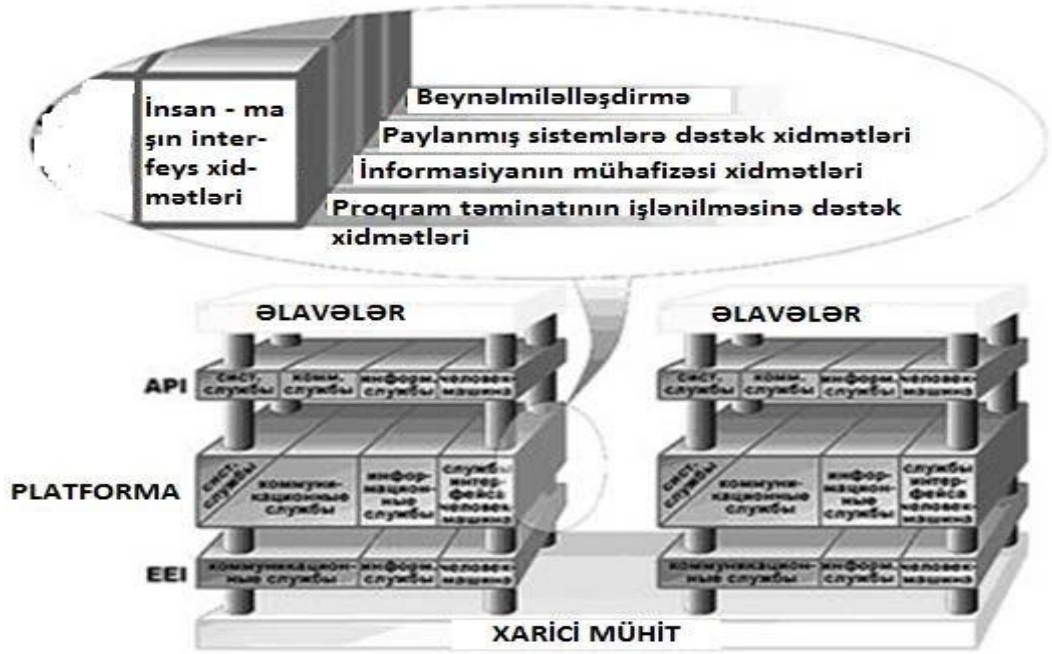
Bu gün təhlükəsizlik sahəsi mütəxəssislərinin müvafiq təhlükəsizlik profilləri, standartları və spesifikasiyaları haqda məlumatsız olması praktiki olaraq qeyri-mümkündür. Bunun da səbəbi müəyyən standartlara riayət edilməsinin zəruriliyinin qanunla müəyyənləşdirilməsidir. Digər inandırıcı və əsaslı səbəblər ilk növbədə, informasiya təhlükəsizliyi və İT-nin prosedur və proqram və texniki səviyyələri haqqında biliklərin toplanması və tətbiqi formalarından biri olan standart və spesifikasiyalardır, onların tərkibində proqram təminatı və təhlükəsizlik sahəsində ən ixtisaslı şirkətlər tərəfindən hazırlanmış və sübut edilmiş yüksək keyfiyyətli həllər və metodologiyalar mövcuddur.

Yuxarı səviyyədə bir-birindən əhəmiyyətli dərəcədə fərqlənən standartlar və spesifikasiyaların iki qrupunu ayırmaq olar:

1. İS və mühafizə vasitələrinin təhlükəsizlik tələblərinə uyğun olaraq qiymətləndirilməsi və təsnifatı üçün hazırlanmış qiymətləndirmə standartları;

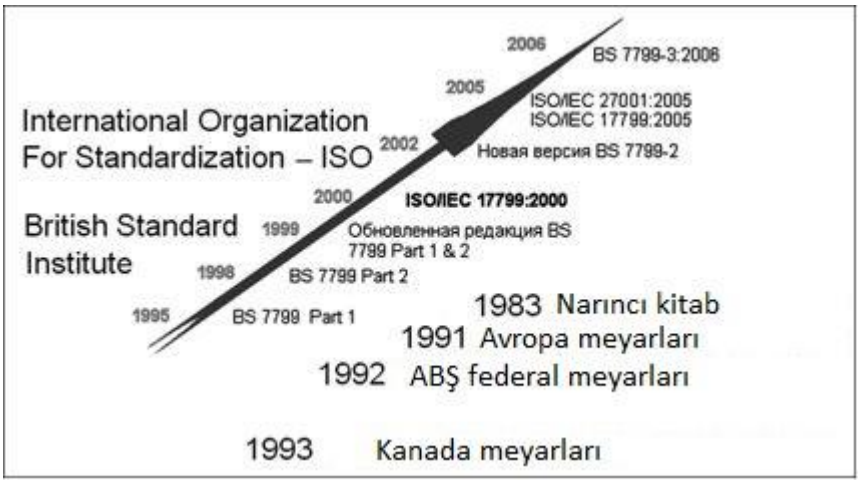
2. mühafizə vasitə və metodlarının tətbiqi və istifadəsinin müxtəlif aspektlərini tənzimləyən xüsusiyyətlər.

Bu qruplar bir-birini tamamlayır. Qiymətləndirmə standartları təşkilati və arxitektura spesifikasiyalarının rolunu oynayan informasiya təhlükəsizliyi və İS aspektləri baxımından ən mühüm anlayışları təsvir edir. (şək. 2.2).



Şək. 2.2. Açıq məlumat sistemində standartlaşdırma obyektləri

Xüsusi standartlar və spesifikasiyalar müəyyən edilmiş İS-nin arxitekturasının qurulmasını və informasiya təhlükəsizliyini təmin etmək üçün təşkilati və texniki tələblərin yerinə yetirilməsini müəyyənləşdirir (şək. 2.3).



Şək. 2.3. İnformasiya təhlükəsizliyi sahəsində standartlaşmanın xronologiyası

Qiymətləndirmələr arasında standart "Etibarlı kompüter sistemlərinin qiymətləndirilmə meyarları" və onun şəbəkə konfiqurasiyaları üçün təfsiri (ABŞ Müdafiə Nazirliyi), "Avropa ölkələri üçün uyğunlaşdırılmış meyarlar", beynəlxalq "İnformasiya texnologiyalarının təhlükəsizliyini qiymətləndirmə meyarları" və

əlbəttə ki, Dövlət Texniki Komissiyasının "Təlimat sənədləri"ni qeyd etmək lazımdır. İT.-nin müəyyən, lakin çox mühüm və mürəkkəb bir aspektini tənzimləyən ABŞ Federal Standartı "Kriptoqrafik modullar üçün təhlükəsizlik tələbləri" də bu qrupa aiddir.

Müasir paylanmış İS-yə tətbiq olunan texniki şərtlər ilk növbədə İnternet texnologiyaları üzrə tematik qrup (*Internet Engineering Task Force - IETF*) və onun təhlükəsizlik üzrə işçi qrupu tərəfindən yaradılmışdır. Texniki spesifikasiyaların əsasını İP - səviyyədə təhlükəsizlik sənədləri (IPSec) təşkil edir. Bundan əlavə, nəqliyyat (*Transport Layer Security* - TLS) və tətbiqetmə səviyyələrində(GSS-API spesifikasiyası, Kerberos) mühafizə təhlil edilir.

IPSec spesifikasiyası IP v.6 standartının bir hissəsidir və TCP/IP protokollarının cari versiyasına münasibətdə əlavə hesab edilir, IPSec hazırda müvafiq RFC standartlarını təmsil edən 3 alqoritmə görə asılı olmayan baza spesifikasiyasını ehtiva edir. IPSec protokolu IP şəbəkə (üçüncü) səviyyəsində trafikin şifrələnməsinin standart bir üsulunu təqdim edir və məlumatları sonda şifrələməyə əsaslanaraq saxlayır: işləyən əlavədən asılı olmayaraq, kanaldan keçən hər bir məlumat şifrələnir. Bu, təşkilatlara İnternetdə VPN yaratmağa imkan verir. İPsec aşağıdakıları təmin edir:

- Autentifikasiya - ortaq bir tərəfdaş, yəni müştərək sirrin sahibi tərəfindən paket göndərilməsinin sübutu;
- bütövlük - bir paketdə məlumatların dəyişdirilməsinin qeyri-mümkünlüyü;
- məxfilik - ötürülən məlumatların açıqlanmaması;
- açarlarla etibarlı idarəetmə;
- yalnız qəbuledici və paket göndərənə məlum olan müştərək sirr;
- tunel - müəssisənin lokal şəbəkəsinin topologiyasını tamamilə örtmənin mümkünlüyü.

IPSec standartları çərçivəsində iş göndərəndən qəbuledicіyə verilən məlumat axınının tam müdafiəsini təmin edir, aralıq müşahidəçilər üçün trafikin qarşısını alır.

İnternet birliyi "Müəssisənin informasiya təhlükəsizliyi üzrə təlimatı", "İnternet xidməti təminatçisini necə seçmək olar?", "İnformasiya təhlükəsizliyi pozuntularına necə cavab vermək olar?" kimi bir sıra təlimatlar və tövsiyələr hazırlayaraq inzibati və prosedur səviyyələrinə lazımi diqqət yetirir.

Şəbəkə təhlükəsizliyi məsələlərində X.800 "Açıq sistemlərarası əlaqə üçün təhlükəsizlik arxitekturası", X.500 "Kataloq xidməti: anlayışların, modellərin və xidmətlərin xülasəsi" və X.509 "Kataloq xidməti: Açıq açar və atribut sertifikatlarının çərçivələri" tələb olunur.

Son on beş ildə İS-nin və onların komponentlərinin təhlükəsizliyini təmin etmək üçün International Organization for Standardization - ISO tərəfindən bir sıra standartlar təsdiq edilmişdir. Bu standartların böyük əksəriyyəti paylanmış sistemlərdə məlumat mübadiləsi və icazəsiz daxil olmadan qorunmaq üçün telekommunikasiya, proses və protokollara aiddir. Bu baxımdan, bir mühafizə və təhlükəsizlik sistemi hazırlayarkən, müəyyən bir layihənin bütün həyat dövrü üçün ən uyğun standartlar seçilməlidir.

Birinci standart qrupu - İSO / IEC JTC1 / SC22 - "Açıq sistemlərin (OSI) qarşılıqlı əlaqəsi (OSI) üçün məlumatların axtarışı, ötürülməsi və idarə edilməsi" - SC22 altkomitəsinin rəhbərliyi altında yaradılmış və inkişaf etdirilmişdir. Bu qrupun standartları OSI konsepsiyasının inkişafına və saflaşdırılmasına həsr edilmişdir. Bu qrupdakı məlumatların mühafizəsi bu konsepsiyanın tam həyata keçirilməsini təmin edən komponentlərdən biri hesab olunur. Bunun üçün xidmətlər və mühafizə mexanizmləri əsas OSI modelinin səviyyələri ilə müəyyən edilir, məlumatların qorunmasının metodoloji əsaslarını və açıq sistemlərin müxtəlif səviyyələrində xüsusi mühafizə protokollarını ardıcıl şəkildə əks etdirən standartlar dərc olunur və hazırlanır.

Standartların ikinci qrupu - ISO / IEC JTC1 / SC27 - SC27 altkomitəsinin rəhbərliyi altında hazırlanmış və əsasən məlumatların mühafizəsinin xüsusi metod və alqoritmlərinə yönəldilmişdir. Bu qrup OSI modelindən asılı olmayaraq informasiya təhlükəsizliyi və kriptovalyutasının əsas metodoloji standartlarını

özündə birləşdirir. Müdafiənin özünəməxsus üsul və vasitələri İS – nin mühafizəsinin təşkili və idarə edilməsi sistemində ümumiləşdirilmişdir.

İS -nin mühafizə sisteminin planlaşdırılması və layihələndirilməsi prosesində metodoloji standartların aşağıda təqdim olunan ən geniş yayılmış üçüncü qrupundan istifadə edilməsi tövsiyə olunur. Standartların yaxın məqsədləri səbəbindən onların konsepsiyaları və məzmunu qismən üst-üstə düşür və bir-birini tamamlayır. Buna görə standartları birlikdə istifadə etmək (standartların profilini yaratmaq), komponentlərini müəyyən bir İS layihəsinin tələblərinə uyğun olaraq təcrid etmək və uyğunlaşdırmaq tövsiyə olunur.

1. İSO 10181: 1996. Hissə 1-7. "OSI. Açıq sistemlərdə təhlükəsizliyi təmin etmək üçün işin strukturu". Hissə 1. Xülasə. Hissə 2. Autentifikasiya üzrə işin strukturu. Hissə 3. Girişə nəzarət üzrə işin strukturu. Hissə 4. İmtinaya davamlılıq üzrə işin strukturu. Hissə 5. Məxfilik üzrə işin strukturu. Hissə 6. Tamlığın təmini üzrə işin strukturu. Hissə 7. Təhlükəsizliyin auditi üzrə işin strukturu.
2. İSO 13335: 1996-1998. Hissə 1-5. "Təhlükəsizlik İdarəçiliyi." Hissə 1. İnformasiya texnologiyaları təhlükəsizliyi konsepsiyası və modelləri. Hissə 2. İnformasiya texnologiyalarının planlaşdırılması və təhlükəsizliyinin idarə edilməsi. Hissə 3. İT təhlükəsizliyini idarəetmə texnologiyası. Hissə 4. Təhlükəsizlik vasitələrinin seçimi. Hissə 5. Xarici əlaqələrin təhlükəsizliyi.
3. ISO 15408: 1999. 26-cı hissə 1-3. "Təhlükəsizliyi təmin etmə üsulları və vasitələri. İnformasiya texnologiyalarının təhlükəsizliyini qiymətləndirmə meyarları." Hissə 1. Giriş və ümumi model. Hissə 2. Funksional tələblərin mühafizəsi. Hissə 3. Keyfiyyətə dair tələblərin mühafizəsi.

ISO 10181 standartı yeddi hissədən ibarətdir və açıq məlumat sistemlərinin təhlükəsizliyini təmin edən ümumi konsepsiya ilə başlayır və ISO 7498-2 standartının müddəalarını inkişaf etdirir. Birinci hissədə mühafizə metodlarının əsas anlayışları və ümumi xüsusiyyətləri verilir və tətbiq edildikdə bir İS təhlükəsizlik sisteminin sertifikatlaşdırılmasına ehtiyac duyulur.

İkinci standart, ISO 13335, istənilən İS üçün təhlükəsizlik sistemlərini layihələndirərkən həll ediləcək geniş metodoloji vəzifələri əks etdirir. Onun bütün hissələrində diqqət müxtəlif növ təhdidlərə qarşı bərabər güclü İS –nin mühafizəsi sistemlərinin əsas prinsiplərinə və dizayn metodlarına yönəldilmişdir. Bu təlimat, İS – nin fəaliyyətinin təhlükəsizliyini təmin etmək üçün inteqrasiya edilmiş xüsusi sistemin sonrakı inkişafı üçün mühafizə layihəsinin hazırlanmasının əsas metodlarını və proseslərini kifayət qədər sistemləşdirir.

1999-cu ildə qəbul edilmiş "İnformasiya Texnologiyaları təhlükəsizliyinin qiymətləndirilməsinin ümumi meyarları" (The Common Criteria for Information Technology Security Evaluation) beynəlxalq ISO 15408-1999 standartında proqram - texniki səviyyədə təhlükəsizlik mexanizmlərini qiymətləndirmə meyarları təqdim edilmişdir. Bu standart informasiya təhlükəsizliyi sahəsində standartlaşdırmanın əsas müddəalarını özündə cəmləşdirmişdir.

Standartın birinci hissəsi təhlükəsizlik məqsədləri və konsepsiyasını, eləcə də İS – nin mühafizəsi üçün ümumi bir modeli təqdim edir. Konsepsiya kompleks sistemlərin tipik bir həyat dövrü diaqramına, tələblərin və komponent spesifikasiyalarının ardıcıl detallaşdırılmasına əsaslanır. Bu standartda ətraf mühit, obyektlər, tələblər, funksiyanın xüsusiyyətləri və mühafizə sistemi vasitələrinin vəzifələri, bölmələri vardır; mühafizə nəticələrinin qiymətləndirilməsi meyarlarına ümumi tələblər, təhlükəsizlik profili, tələblərin qiymətləndirilmə məqsədləri və nəticələrinin istifadəsi göstərilir. İS - nin təhlükəsizliyini təmin etmək üçün ümumi məqsəd, vəzifə və meyarlar toplusu layihəsi təklif olunur.

İkinci hissədə İS - nin qorunması komponentlərinə qoyulmuş funksional tələblərə uyğun paradiqma təqdim olunur. İS-nin təhlükəsizliyinin təmini üzrə əsas məsələlərin on bir qrupu (sinifləri) təsnif edilir. Hər bir sinif təhlükəsizlik məqsədlərinin müəyyən bir hissəsini həyata keçirən və öz növbəsində müəyyən problemlərin həlli üçün daha kiçik komponentlərdən ibarət tələblər dəsti ilə ətraflı təsvir edilmişdir. Siniflərə təhlükəsizlik funksiyalarına tələblərin - kriptoqrafik dəstək; rabitənin qorunması və məlumatların tranzaksiyası; istifadəçi məlumatlarının daxil edilməsi, çıxışı və saxlanması; istifadəçi identifikasiyası və

autentifikasiyası; təhlükəsizlik funksiyalarını idarəetmə prosesləri; hesablama resurslarının istifadəsinə məhdudiyyətlərin tətbiqi; təhlükəsizlik funksiyaları, habelə tələblərin bəzi digər sinifləri arasında marşrutlaşdırma və əlaqənin etibarlılığının təmin edilməsi kimi prinsip və metodlar daxildir.

Məsələlərin hər bir qrupu üçün İS-nin təhlükəsizliyinin təmini üzrə ən səmərəli komponent və prosedurların tətbiqinə dair tövsiyələr verilir. Müəyyən bir mühafizənin keyfiyyətinə zəmanətin səviyyəsi ilə İS - nin təhlükəsizlik məqsədlərinə nail olmaq üçün funksional tələblərin və onların həyata keçirilmə metodlarının komponentlərinin vahid "Çoxqat istifadə üçün mühafizə profilləri"ndə birləşdirilməsi tövsiyə olunur.

Bu "Profillər" müəyyən bir İS layihəsi üçün "Təhlükəsizlik üzrə texniki məsələ"də funksional tələblərin daha da dəqiqləşdirilməsi üçün əsas ola bilər və bu cür tələblərin formalaşmasında kobud səhvlərin qarşısını almağa kömək edə bilər. "Təhlükəsizlik üzrə tapşırıqlar" üçün tələblər spesifikasiyasının qiymətləndirmələrinin yekunlaşdırılması sifarişçilərə, tərtibatçılara və layihə testerlərinə onun funksional tələblərə və IS –nin zəmanətli qorunması tələblərinə uyğunluq səviyyəsi barədə ümumi nəticə çıxarmaq imkanı verməlidir. Geniş əlavələr əsas funksional məqsədlərə və təhlükəsizlik tələblərinə nail olmaq üçün vasitələrin tətbiqi ilə bağlı tövsiyələr verir.

Standartın üçüncü hissəsi IS-nin təhlükəsizliyinin təmin edilməsi funksiyalarına tələblərin həyata keçirilməsi üçün proseslərin keyfiyyət zəmanətini təmin etmək məqsədlərinə, metodlarına və səviyyələrinə həsr edilmişdir. Mühafizə komponentlərinin həyat dövrünün düzgün həyata keçirilməsi və onların səmərəli tətbiqi üçün istifadəyə əlverişli olan metod və vasitələr müəyyən edilmişdir. Təhlükəsizlik sistemlərinin keyfiyyətli təşkilinin və tətbiqinin təmini üçün mühafizə qurğularının konfiqurasiya rəhbərliyinin işlənilməsi; İS - nin qorunmasını həyata keçirən komponentlərin həyat dövrünü, inkişafını, çatdırılmasını və istismarını dəstəkləyən proseslər; sənədlərin və təlimatların düzgünlüyü; İS zəiflik testi və qiymətləndirilməsi barədə təfsilatı ilə tövsiyələr verilmişdir. İS təhlükəsizlik

zəmanətlərini mühafizə və dəstək paradiqması, həmçinin onun realizasiya üsulları təqdim olunur.

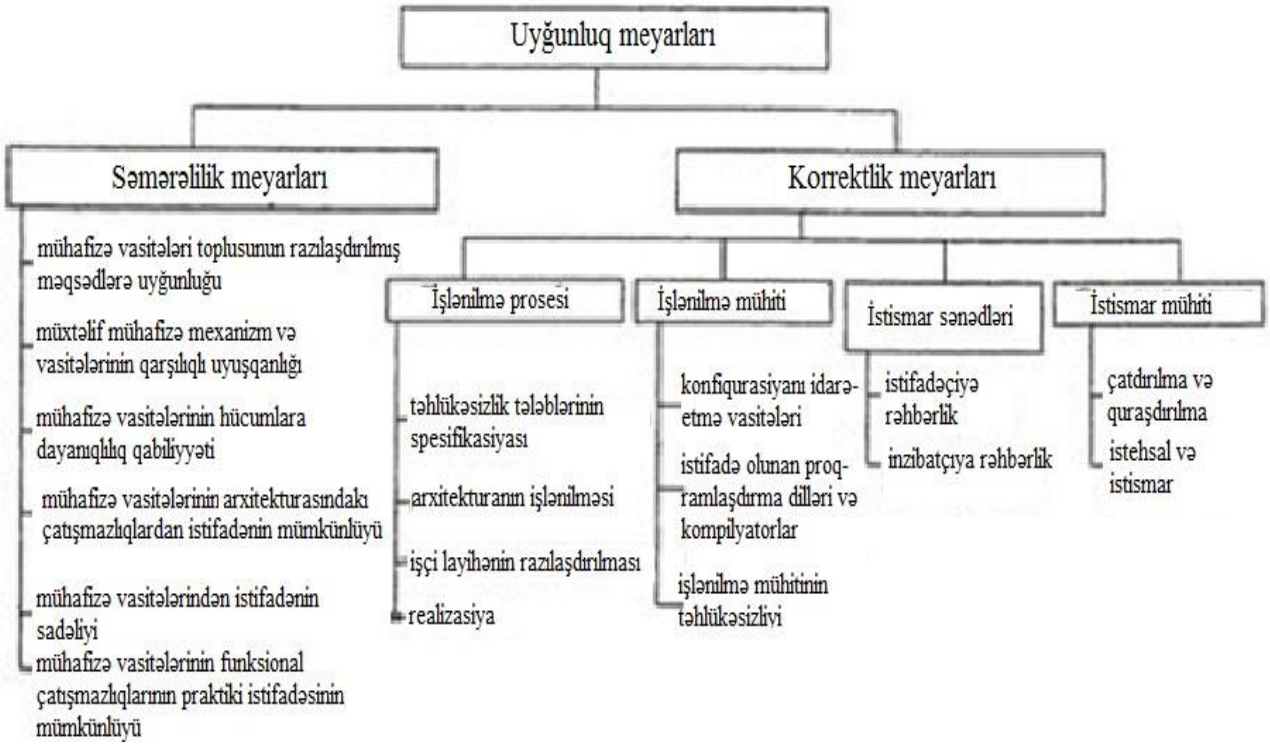
Ümumiyyətlə, standart mühafizə sistemlərinin praktik dizaynında istifadə edilməli müasir İS təhlükəsizlik metod və vasitələrinin keyfiyyətinə zəmanət funksiya və metodlarına olan tələbləri əhatə edir.

"Ümumi meyarlar" ("ÜM") təhlükəsizliyin funksional tələblərini (Security Functional Requirements) və təhlükəsizlik funksiyalarının reallaşdırılmasının adekvatlığına olan tələbləri (Security Assurance Requirements) müəyyənləşdirir. "ÜM" təhlükəsizlik tələblərinin iki əsas növünü ehtiva edir (şək.2.4):

1. Mühafizə funksiyalarına (xidmətlərinə) və onları həyata keçirən mexanizmlərə təqdim olunan aktiv qorunma aspektinə uyğun funksional tələblər;

2. passiv aspektə uyğun inam tələbləri; texnologiya və inkişaf və istismar prosesinə təqdim olunur.

Təhlükəsizlik tələbləri tərtib edilir və onların icrası müəyyən bir qiymətləndirmə obyekti - aparat-proqram məhsulu və ya İS üçün yoxlanılır. "ÜM"dəki təhlükəsizliyə statik deyil, qiymətləndirmə obyektinin həyat dövrünə uyğun olaraq baxılır. Bundan əlavə, araşdırılan obyekt təcrid vəziyyətində deyil, müəyyən zəifliklər və təhdidlərlə xarakterizə olunan "təhlükəsizlik mühitində" görünür. Təhlükəsizliyin səviyyəsini daxilində həyata keçirilən təhlükəsizlik funksiyalarının tamlığı və bu funksiyaların yerinə yetirilməsinin etibarlılığı baxımından qiymətləndirmək üçün "ÜM" istifadə edilməlidir. "ÜM"-nin tətbiqetmə qabiliyyəti proqramın və texniki səviyyənin təhlükəsizlik mexanizmləri ilə məhdudlaşsa da, təşkilati səviyyənin təhlükəsizlik mexanizmlərinə və təsvir olunan təhlükəsizlik funksiyaları ilə birbaşa əlaqəli fiziki qorunma tələblərinə müəyyən tələblər daxildir.



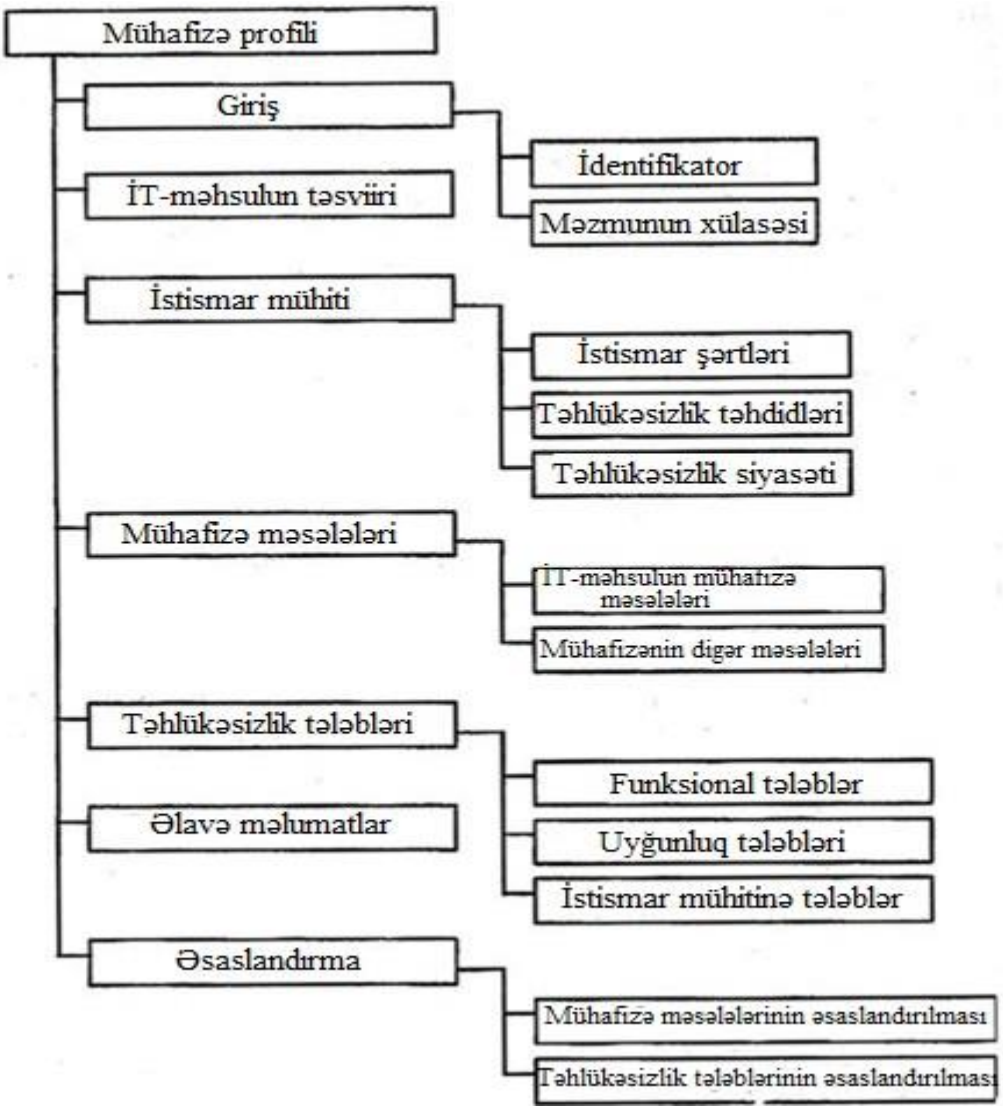
Şəkil 2.4. Mühafizə vasitələrinin uyğunluq meyarları

BS 7799 ingilis standartı "İnformasiya təhlükəsizliyinin idarə edilməsi. Praktiki qaydalar" ISO / IEC 17799: 2000 "İnformasiya təhlükəsizliyinin idarə edilməsi üçün praktiki qaydalar" ("İnformasiya təhlükəsizliyinin idarə edilməsi üçün təcrübə kodeksi") beynəlxalq standartında əks etdirilib. Bu standart İT.-nin idarə edilməsi qaydalarını ümumiləşdirir, onlardan inzibati, prosedur və fiziki təhlükəsizlik tədbirləri daxil olmaqla təşkilati səviyyəli təhlükəsizlik mexanizmlərini qiymətləndirmək üçün meyar kimi istifadə edilə bilər. Praktiki qaydalar on hissəyə bölünür:

1. Təhlükəsizlik siyasəti.
2. Mühafizənin təşkili, təsnifatı və onlara nəzarət.
3. Kadrların təhlükəsizliyi.
4. Fiziki təhlükəsizlik.
5. Kompüter sistemləri və şəbəkələrinin inzibatçılığı.
6. Giriş nəzarəti.
7. İnformasiya sistemlərinin işlənilməsi və müşayiət olunması.

8. Təşkilatın fasiləsz fəaliyyətinin planlaşdırılması.
9. Təhlükəsizlik siyasətinin tələblərinə icrasına nəzarət.

Bu bölmələrdə hazırda bir çox ölkələrdə dövlət və ticarət təşkilatlarında tətbiq olunan müvafiq mühafizə profilləri şəklində tətbiq olunan təşkilati səviyyə mexanizmləri təsvir edilmişdir (şək. 2.5).



Şəkil 2.5. IT məhsulunun profilinin quruluşu

İSO 17799-da təklif olunan əsas nəzarət vasitələri (İS nəzarət mexanizmləri) xüsusilə mühüm hesab olunur.

Bəzi idarəetmə vasitələrindən, məsələn, şifrələmədən istifadə edərkən təhlükəsizlik və riskin qiymətləndirilməsi üzrə mütəxəssislərin tövsiyəsi istifadə oluna bilər. Dəyərli resursların nühafizəsi və ya ciddi təhlükəsizlik təhdidlərinə xüsusilə qarşı olmaq üçün bəzi hallarda ISO 17799-dan kənara çıxan daha güclü nəzarət tələb oluna bilər.

İSO 17799-a uyğun olaraq İS-nin təhlükəsizlik auditi proseduruna sadalanan əsas idarəetmə vasitələrinin mövcudluğunun yoxlanması, həyata keçirilməsinin tamlığının və düzgünlüyünün qiymətləndirilməsi, habelə bu əməliyyat mühitində mövcud olan risklərə uyğunluğunun təhlil edilməsi kimi funksiyalar daxildir. Audit işinin ayrılmaz bir hissəsi də risklərin idarə olunması və təhlilidir. Təhlükəsizliyin təmini və mühafizənin auditi üzrə ISO 27000 standartları ailəsi fəal şəkildə inkişaf etdirilir (cəd.2.1).

ISO 270... standartlar ailəsinin inkişafı

Cədvəl 2.1

Standartlar	**Təyinat**
ISO 27000	Əsas müddəalar və terminlər
ISO 27001:2005	İnformasiya təhlükəsizliyinin idarə olunması sistemlərinə tələblər
ISO 27002:2007	İnformasiya təhlükəsizliyinin idarə olunmasının praktiki qaydaları
ISO 27003	İnformasiya təhlükəsizliyinin idarə olunması sistemlərinin tətbiqi üzrə rəhbərlik
ISO 27004	İnformasiya təhlükəsizliyinin idarə olunmasının səmərəliliyinin ölçülməsi
ISO 27005	İnformasiya təhlükəsizliyinin risklərinin idarə olunması üzrə rəhbərlik
ISO 27006:2007	İnformasiya təhlükəsizliyinin idarə olunması sistemlərinin sertifikasiyasını və auditini yerinə yetirən orqanlar üçün tələblər

Standartlar	Təyinat
ISO 27007	İnformasiya təhlükəsizliyinin idarə olunması sistemlərinin auditi üzrə rəhbərlik
ISO 27031	Biznesin kəsilməzliyinin təmini üzrə rəhbərlik
ISO 27032	Kompüter təhlükəsizliyinin təmini üzrə rəhbərlik
ISO 27033	Şəbəkə texnologiyalarının təhlükəsizliyinin təmini üzrə rəhbərlik
ISO 27034	Proqram əlavələrinin təhlükəsizliyinin təmini üzrə rəhbərlik

Aşağı səviyyədə, müxtəlif şirkətlərdə yüzlərlə sənaye standartları, normativ sənədlər və məlumat təhlükəsizliyi üçün texniki sənədlər hazırlanır ki, bu da milli şirkətlər tərəfindən proqram vasitələrinin, İS – nin işlənilməsində, onun keyfiyyətinin və təhlükəsizliyinin təmin edilməsində istifadə olunur.

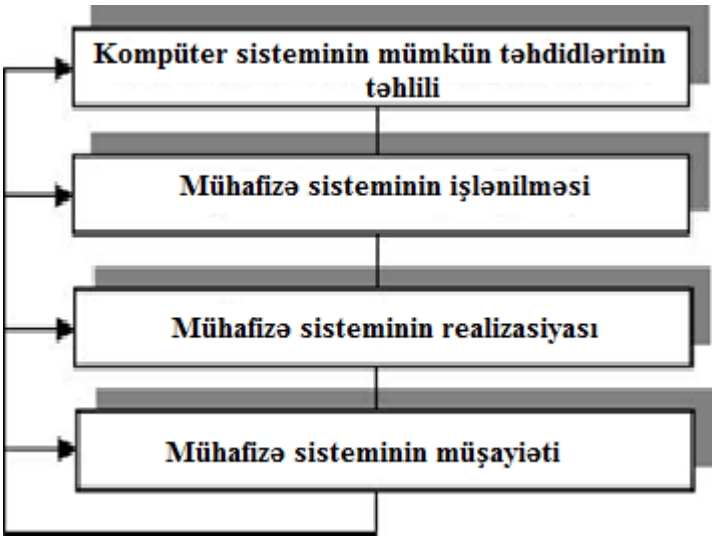
III FƏSİL. KOMPÜTER ŞƏBƏKƏLƏRİNİN TƏHLÜKƏSİZLİK SİSTEMİ: PROBLEMLƏR VƏ ONLARIN HƏLLİ YOLLARI

3.1. İnformasiyanın mühafizə sistemlərinin qurulma mərhələləri

İT - nin istifadəsi informasiya təhlükəsizliyi məsələlərinə diqqətin artırılmasını tələb edir. Məlumat mənbəyinin məhv edilməsi, müvəqqəti və ya icazəsiz istifadəsi şirkətə ciddi maddi ziyan vura bilər. İnformasiyanın mühafizəsinin zəruri səviyyəsi olmadan İT – nin tətbiqi kompüter şəbəkələrində saxlanan və işlənmiş məxfi məlumatların əhəmiyyətli dərəcədə itkisi nəticəsində iqtisadi cəhətdən səmərəsiz ola bilər. İnformasiya mənbələrinin təhlükəsizliyini təmin edən həllərin tətbiqi, bir təşkilatda bütün informasiyalaşma prosesinin lokal və qlobal informasiya mühitində dolaşan informasiyanın səmərəliliyini, tamlığını, orijinallığını və məxfiliyini təmin edir.

Kompüterdəki informasiyanın mühafizə sistemi - sistemin normal işləməsi üçün istifadəçilərin və sistem sahiblərinin mümkün maddi və mənəvi itkilərini minimuma endirmək məqsədilə təhdidlərə qarşı yönəlmiş hüquqi normaların, təşkilati, inzibati və proqram və texniki vasitələrin məcmusudur.

Mühafizə sisteminin qurulmasının əsas mərhələləri şək. 3.1.- də verilmişdir:



Şək. 3.1. Mühafizə sisteminin qurulma mərhələləri

Kompüterin informasiyanın emalı sisteminə mümkün təhdidlərin təhlili mərhələsi zamanın müəyyən anında sistemin vəziyyətinin qeydə alınması (aparat və proqram konfiqurasiyaları, məlumat emalı texnologiyaları) və onun hər bir komponenti üçün mümkün zərərli hərəkətlərin müəyyənləşdirilməsi üçün zəruridir. Mümkün olan çoxsaylı hərəkətlərdən yalnız real olaraq sistemin istifadəçilərinə və sahiblərinə zərər verə biləcək hərəkətlər seçilir.

Planlaşdırma mərhələsində mühafizə sisteminin quruluşu müxtəlif xarakterli əks tədbirlər şəklində formalaşır. İS-nin mühafizəsininin universal üsulları o qədər də çox deyil. Onlardan daha səmərəli olanlar aşağıdakılardır:

- Sistemin subyektlərinin identifikasiyası və autentifikasiyası;

- sistemin resurslarına giriş nəzarəti;

- sistemdə baş verən hadisələrin qeydiyyatı və təhlili;

- sistem obyektlərinin bütövlüyünə nəzarət;

- məlumatların şifrələnməsi;

- sistemin komponentlərnin və resurslarının ehtiyat nüsxələrinin çıxarılması.

Bu universal metodlardan fərqli variasiyalarda və müxtəlif mühafizə tədbirlərində tətbiq oluna bilər.

Planlaşdırma mərhələsinin nəticəsi İS-nin mühafizə planıdır, elə bir sənəddir ki, sistemdə informasiyanın emalını prosesini əhatə edir. Sistemin realizasiyası zamanı onun mühafizəsi üzrə tələb olunan bütün komponentlərin daxil edilməsi və onlara bütün mümkün təsirlər üzrə tədbirlər və onların dəyəri formalaşdırılır.

İnformasiya sistemlərinin mühafizə mexanizmlərinin realizasiyası üzrə iki əsas üsul vardır:

- ✓ "Əlavə" mühafizə - sistemin informasiyanın emalı üzrə əsas proqram və aparat vasitələrinə əlavə olunan mühafizə vasitələri; müvafiq yanaşmadan, məsələn, İBM firmasının təhlükəsiliyin təminində təcrübəsi vardır.

- ✓ “quraşdırılmış” mühafizə - mexanizmləri təhlükəsizlik tələbləri nəzərə alınmaqla İS-nin ayrılmaz hissəsi. Müühafizə mexanizmləri sistemin ayrı-ayrı komponentləri formasında reallaşa və onun tərkib hissələri arasında paylana bilər. Bu halda mühafizə vasitələri bütün sistemin təhlükəsizliyinə cavab verən vahid mexanizmi təşkil edir. Bu üsuldan DEC şirkəti tərəfindən VAX/VMS sisteminin hazırlanmasında istifadə olunmuşdur.

Hər bir üsulun öz üstünlükləri və çatışmazlıqları vardır. Əlavə mühafizə daha çevikdir, zərurət olduğu halda onun mexanizmlərini və konfiqurasiyasını dəyişmək olar. Quraşdırılmış mühafizənin əsas üsyünlüyü – etibarlılıq və lokal optimallıqdır. Bu halda mühafizə vasitələri işlənilir və sistemin özü ilə bərabər reallaşdırılır. Bununla yanaşı, quraşdırılmış mühafizə ciddi qeyd olunmuş və genişləndirilməsi və ya funksional dəyişdirilməsi mümkün olmayan funksiyalar yığımına malikdir. Bəzi funksiyaları yalnız istisna etmək olar.

“Əlavə” və “Quraşdırılmış” mühafizələrə ayrı-ayrılıqda çox az hallarda təsadüf edilir. Bir qayda olaraq onların kombinasiyasından istifadə olunur ki, bu da onların üstünlüklərini birləşdirməyə və ayrı-ayrılıqda olan çatışmazlıqlarını kompensasiya etməyə imkan verir.

Təhlükəsizlik siyasətinin reallaşdırma mexanizmləri və modelləri, informasiyann mühafizəsi üzrə qaydalar və praktiki tövsiyələr məcmusu təhlükəsizlik siyasətini təyin edir. Bu siyasət fərdi və konkret informasiyanın emalı texnologiyasından, proqram və texniki vasitələrdən asılı ola bilər. Təhlükəsizlik siyasətinin əsasını sistemin obyektlərinə subyektlərin daxil olmasının idarəetmə üsulu təşkil edir. Subyekt – sistemin öz vəziyyətini dəyişə bilən komponentidir. Obyekt – sistemin informasiyanı qəbul edən, ötürən və saxlayan passiv komponentidir.

Daxil olmanı idarəetmə sisteminin realizasiyası üçün İS-nin riyazi modeli təşkil olunur. Bu model onun bütün vəziyyətlərini, bir vəziyyətdən digər vəziyyətə keçidini modelləşdirə bilər, həmçinin təhlükəsiz vəziyyətləri göstərə bilər. Bunun üçün modelləşdirmənin riyazi metodlarının geniş spektrindən istifadə etmək olar.

3.2. Şəbəkələrdə və sistemlərdə informasiya sistemlərinin təhlükəsizliyini təmin edən alətlər

İS –də məlumatları saxlayan və emal edən hər hansı bir təşkilat və ya şirkətin informasiyanın mühafizəsi vasitələrinə ehtiyacı var:

- ✓ Maliyyə və kredit təşkilatları;
- ✓ ümumi təyinatlı şəbəkələrdə əlaqələri olan ticarət və hökumət təşkilatları;
- ✓ coğrafi cəhətdən paylanmış şirkətlər;
- ✓ məlumat mənbələrinə xarici çıxışı təmin etmək məcburiyyətində qalan təşkilatlar;
- ✓ telekommunikasiya operatorları

Əlbəttə ki, bu, tam siyahı deyil. Məlumat verilənlərinin təhlükəsizliyini təmin etmək məcburiyyətində qalan şirkətlər şəbəkələrdə işin səmərəliliyi və onun zəruri mühafizə səviyyəsi arasında seçim problemi ilə üzləşirlər. Çox vaxt istifadəçilər və ya istehlakçılar bu təhlükəsizlik tədbirlərini girişin məhdudlaşdırılması və ya səmərəliliyin azaldılması kimi qiymətləndirə bilər. Buna görə hər bir təşkilat məlumatları qorumaq üçün vasitələr seçimini fərdi qaydada həyata keçirir.

Təhlükəsizliklə əlaqəli problemlərin, habelə təhdid mənbələrinin fərqli olduğuna görə fərqli təhlükəsizlik növlərinin yaradılması zərurəti yaranmışdır. Bunlar bir neçə qrup üzrə təsnif edilir:

- ✓ Hardware və ya texniki vasitələr;
- ✓ müdafiənin mühafizə tədbirləri;
- ✓ qarışıq təsnifata aid edilən vasitələr;
- ✓ təşkilati və ya inzibati tədbirlər.

Birinci qrupa fərqli qurğular daxildir - bunlar elektron, mexaniki və ya elektromexaniki ola bilər, lakin onların işləmə spesifikliyi aparat vasitələrinin köməyilə informasiyanın mühafizəsini əhatə edir. Bu qurğulardan istifadə giriş açıq olduqda fiziki daxil olma və ya məlumatların maskalanmasının qarşısını alır. Texniki vasitələr etibarlıdır, subyektiv amillərdən asılıdır və modifikasiyaya çox

davamlıdır, bununla yanaşı onların çatışmazlıqları da vardır. İlk növbədə bunların olduqca yüksək dəyərə malik olmasıdır. Onlar həm də kifayət qədər çevik deyillər və demək olar ki, həmişə böyük çəki və həcmə malikdirlər.

İkinci növ, girişə nəzarət etmək, istifadəçilərin identifikasiyası, məlumatların mühafizəsi sisteminin yoxlanılması üçün müxtəlif proqramlarla işləyir. Bundan əlavə, bu qrupdakı alətlər məlumatları şifrələyə bilər və işçi (qalıq) məlumatları (məsələn, müvəqqəti faylları) silə bilər. Sistem mühafizə üçün proqram vasitələrindən istifadə edirsə, o, bir çox üstünlük əldə edir. Onlar çevik, etibarlı və universal və quraşdırma üçün olduqca sadədirlər, həmçinin onların modifikasiya imkanları vardır və inkişaf etdirilə bilər. Vasitələrin bu növü təsadüfi və qəsdən dəyişikliklərə çox həssasdır. Proqram mühafizəsinin digər çatışmazlıqları fayl serverinin və işçi stansiyaların resurslarının bir hissəsinin istifadəsi, şəbəkənin məhdud funksionallığı və onun vasitələrinin kompüter və onun aparat vasitələrinin tipindən asılılığıdır.

Üçüncü qrup ilk iki qrupun xüsusiyyətlərini özündə birləşdirir. Sonuncu növə təşkilati-texniki və təşkilati - hüquqi xarakterli məlumatların mühafizə vasitələri daxildir. Bunlara aşağıdakılar daxil ola bilər:

- Binalara daxil olmağa, onların hazırlanmasına və avadanlıqlarına nəzarət;
- şirkət təhlükəsizlik strategiyalarının işlənməsi;
- milli qanunvericiliyin sonrakı tətbiqi ilə seçilməsi və öyrənilməsi;
- iş qaydalarının yaradılması və onlara əməl olunmasına nəzarət.

İnternetdəki məlumatların tam qorunmasına bu vasitələrin kompleks istifadəsi ilə nail olmaq olar.

Adətən, zəruri məxfiliyin təmini məqsədilə kriptoqrafiya və ya məlumat şifrələmə mütəxəssislərinə müraciət edirlər. Şifrəli məlumatları yaradarkən, müəyyən bir alqoritm və ya reallaşdırıcı qurğudan istifadə olunur. Dəyişilən açar kodu şifrələmənin idarə edilməsini təmin edir. Onun köməyilə məlumatı əldə etmək olar.

İstifadə olunan klassik alqoritmlər arasında bir neçəsi mühüm hesab olunur:

- Əvəz etmə - ən sadə, tək əlifbalı və ya çox əlifbalı, kompleks ola bilər.
- Yerini dəyişmə - sadə və mürəkkəb ola bilər.
- Qammalama - uzun, qısa və qeyri-məhdud maskadan istifadə edə bilən qarışıqdan bəhs olunur.

Birinci halda, ilkin əlifba alternativləri ilə əvəz olunur. Bu, şifrələmənin ən asan yoludur. Yerini dəyişmə alqoritmi ilə şifrələnmiş verilənlər daha etibarlı olacaq, çünki onlarda rəqəmsal açarlardan və ya ekvivalent sözlərdən istifadə olunur. Qammalamaya üstünlük verən sistem, məlumatın etibarlılığına və təhlükəsizliyinə zəmanət alacaq, çünki bu şifrələmə metodunu tətbiq etmək üçün ciddi kriptoqrafik işlər görüləcəkdir.

Mühafizə üçün verilənlərin qeyri-xətti məlumatların çevrilməsi, kompüter stenoqrafiyası və s. kimi metodlardan istifadə olunur. Bundan əlavə, simmetrik və asimmetrik şifrələmə arasında fərq var. Birincisi göstərir ki, şifrələmə və deşifrələmə üçün eyni açar götürülür (buna qapalı açarları olan sistem deyilir). Açıq açarları olan sistem dedikdə şifrələmə üçün açıq və deşifrələmə üçün qapalı açardan istifadə nəzərdə tutulur.

Mümkün dəyişikliklərdən və ya məlumatların dəyişdirilməsindən özünüzü qorumaq istəyirsinizsə, onda elektron rəqəmsal imzadan istifadə etməyə dəyər. Buna şifrəli mesaj da deyilir, onu şifrələmək üçün yalnız qapalı açar alınır. Autentifikasiya etməyə də dəyər. Bu o deməkdir ki, identifikator təqdim edən hər bir istifadəçinin orijinallığı müəyyənləşdirilməli və ya yoxlama aparılmalıdır. Axı, bu identifikator iddia etdiyi istifadəçi tərəfindən deyil, tamamilə fərqli bir qurğu (şəxs) tərəfindən də təqdim oluna bilər. Bu məqsədlə, adətən, paroldan və təhlükəsizlik suallarından istifadə olunur. Birdəfəlik parol sxemi bu halda səmərəli hesab olunur. Autentifikasiyanı avtorizasiya ilə qarışdırmaq olmaz. Avtorizasiya zamanı istifadəçinin icazəsi və ya müəyyən bir mənbəyə daxil olma və orada hər hansı bir əməliyyatı həyata keçirmə səlahiyyətləri yoxlanır.

Əgər biz bütün mövcud mühafizə vasitələrini şərti olaraq bölsək, onda hər hansı bir sistem daxili informasiya resurslarının təhlükəsizliyini təmin etməli və verilənləri

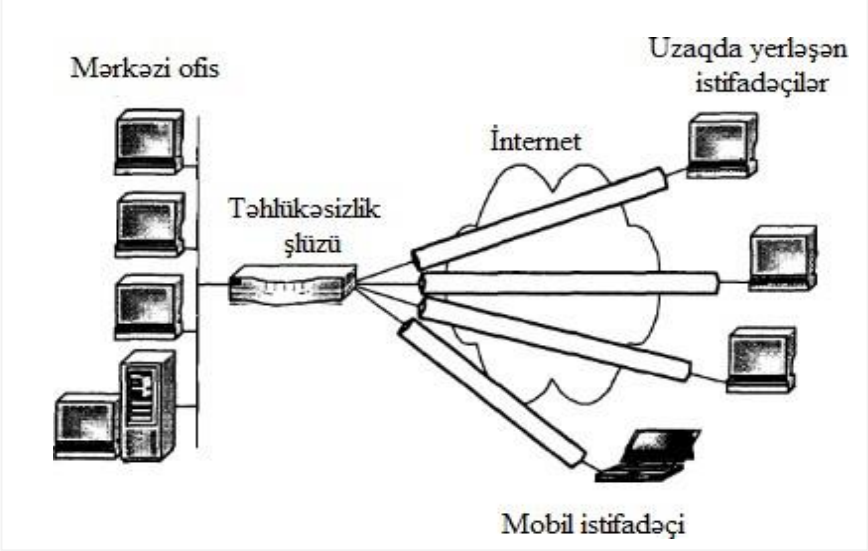
İnternetdə ötürüldüyü zaman qorumalıdır. İlk növbədə sahənin funksiyalarına şəbəkəyə daxil olan və şəbəkədən çıxan məlumat paketlərini izləmək məqsədilə müvafiq trafiki təyin etmək üçün qurulmuş qaydalara uyğun onları bloklayan və ya icazə verən firewall (branmauerlər və ya firewalls) daxildir.

Sistemə öz resursuna hər hansı bir müdaxilə səbəbindən zərər dəyə bilər, çünki təcavüzkarlar bunu etmək üçün hər cür vasitələrdən istifadə edirlər. Məlumatlarınızı virus silə bilər, kimsə adınızdan əməliyyat sisteminə giriş əldə edər, məxfi məlumatları oxuyar, saxta məlumatlarla əvəz edər və bütün qurğu və avadanlıqları işlək vəziyyətdən çıxarar. Buna görə *firewall*, istifadəçilərin qanuni olub olmadığını, zərərli fəaliyyətlərin qarşısını almaq üçün şəbəkə fəaliyyətini düzgün təsnif etməyi bacarmalıdır. Yaradılacaq qaydalar dəsti, paketlərin şəbəkənin bir hissəsindən digər hissəsinə keçmə şərtlərini müəyyənləşdirməyə kömək edəcəkdir. Bu alətlər sahəsində istifadə olunan üsullar da fərqli ola bilər. Trafikin fərqliliyi, şifrələməsi var, buna görə də hətta kimsə istifadəçinin IP paketinə özü çatdığı anda məlumatları oxumadan, təhrif etmədən və dəyişdirmədən onu yalnız silə bilər. Ötürülən məlumatların təyinat nöqtələrinə çatmadan, kənar şəxslər tərəfindən təhrif edilməməsi, məhv edilməməsi və görünməməsi çox vacibdir. Resurslarını ən etibarlı şəkildə qorumaq istəyən bir şirkət inteqrasiya olunmuş bir yanaşma etməlidir. Yuxarıda göstərilənlərə əlavə olaraq, müdaxiləni aşkarlayan, qarşısını alan və məxfi məlumatların sızmasının qarşısını alan bir sistem lazımdır.

Hal - hazırda virtual təhlükəsiz özəl şəbəkələrin qurulması texnologiyaları böyük şirkətlərin - bankların, şöbələrin, böyük dövlət qurumlarının və s. diqqətini daha çox cəlb edir. Bu marağın səbəbi, VPN texnologiyalarının, həqiqətən, uzaq bölmələrlə ayrılmış rabitə kanallarının saxlanmasına çəkilən xərcləri əhəmiyyətli dərəcədə azaltmaqla yanaşı, məlumat mübadiləsinin məxfiliyini artırmaq imkanı yaratmasıdır. VPN texnologiyaları şirkət ofisləri arasında olduğu kimi fərdi iş stansiyalarına və serverlərə təhlükəsiz tunelləri təşkil etməyə imkan verir, həm də potensial müştərilərə virtual təhlükəsiz şəbəkələr yaratmaq üçün inteqrasiya olunmuş çoxfunksiyalı və ixtisaslaşdırılmış cihazlardan sırf proqram məhsullarına qədər geniş çeşidli avadanlıq və proqramlar təklif edir.

Virtual özəl şəbəkələrin bir çox növləri vardır. Onların növləri provayder şəbəkələrindən fərqlənir, bu da birbaşa platformada müştəri xidmətlərini idarə etməyə imkan verir. VPN-nin üç əsas növünü ayırd edirlər: məsafədən girişi olan VPN (Remote Access VPN), daxili korporativ VPN (İntranet VPN) və korporativlərarası VPN (Extranet VPN) [7].

Məsafədən girişi olan VPN (şək.3.2) kommutasiya və icarəyə götürülmüş xətlərin istifadəsinin aylıq dəyərini xeyli azalda bilər. Onların iş prinsipi sadədir: istifadəçilər qlobal şəbəkə ilə lokal bir giriş nöqtəsi vasitəsilə əlaqə qururlar, bundan sonra zənglər İnternet vasitəsilə əlaqələndilirilir, bu da uzun beynəlxalq zənglərin və ya pulsuz şəhərlərarası nömrələrin sahiblərinin göndərmə xərclərini aradan qaldırır; sonra bütün zənglər müvafiq qovşaqlarda cəmlənir və korporativ şəbəkələrə ötürülür.



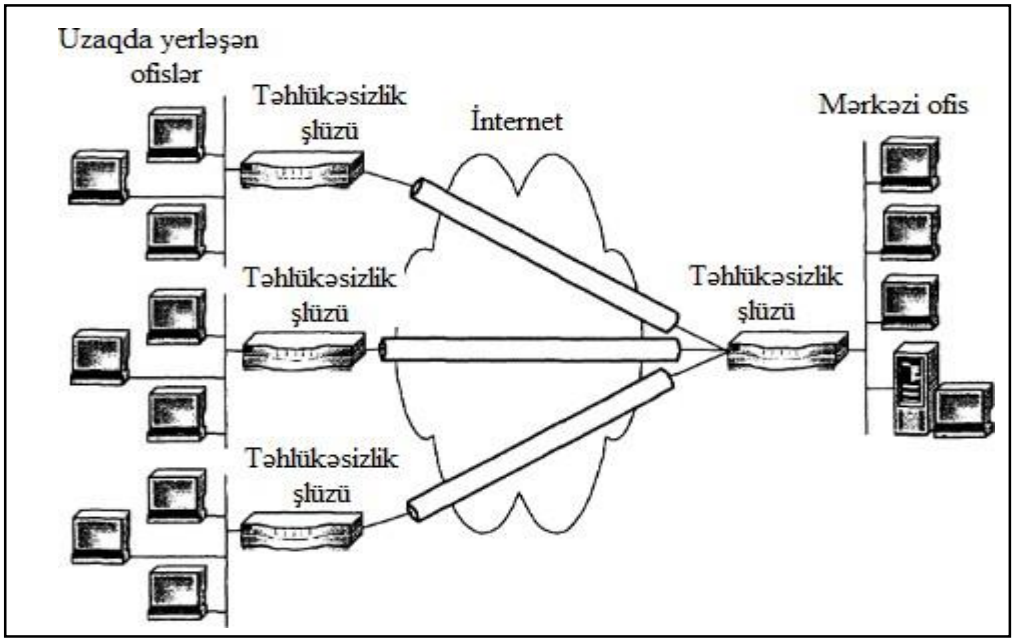
Şəkil 3.2. Məsafədən girişə malik özəl virtual şəbəkə

Özəl idarə olunan Dial Networks - dan Remote Access VPN-ə keçməyin üstünlükləri:

- ✓ Uzaq məsafəli zənglər əvəzinə yerli Dial Networks-dan istifadə imkanı uzun məsafəli telekommunikasiya xərclərini əhəmiyyətli dərəcədə azalda bilər;

- ✓ uzaq və mobil istifadəçilər üçün səmərəli identifikasiya sistemi etibarlı autentifikasiya prosedurunu təmin edir;
- ✓ şəbəkəyə əlavə olunmuş yeni istifadəçilər üçün yüksək miqyaslılıq və yerləşdirmə rahatlığı təmin edilir;
- ✓ şəbəkənin işinin təmini problemlərinə cəlb olunma əvəzinə korporativ biznes məqsədləri əsasında şirkətin diqqətini məqkəzləşdirməyə imkan verir.

Remote Access VPN – in istifadəsi əhəmiyyətli dərəcədə qənaət üçün güclü bir stimuldur, lakin açıq İnternetin həssas korporativ trafikin daşınması üçün bir dayaq olaraq istifadəsi getdikcə geniş yayılmaqdadır, bu da informasiyanın mühafizə mexanizmlərinin adı çəkilən texnologiyanın mühüm elementlərinə çevirir. Korporasiyadaxili VPN şəbəkələri (şək. 3.3) xidmət təminatçıları tərəfindən təqdim olunan İnternetdən və ya müştərək şəbəkə infrastrukturlarından istifadə edilməklə qurulur.



Şək. 3.3. Intranet VPN texnologiyası vasitəsilə şəbəkə qovşaqlarının birləşdirilməsi

Şirkətin daha ucuz İnternet rabitəsi ilə əvəzlənərək bahalı icarəyə götürülmüş xətlərin istifadəsindən imtina etməsi kifayətdir. Bu, buraxılış zolağından istifadə

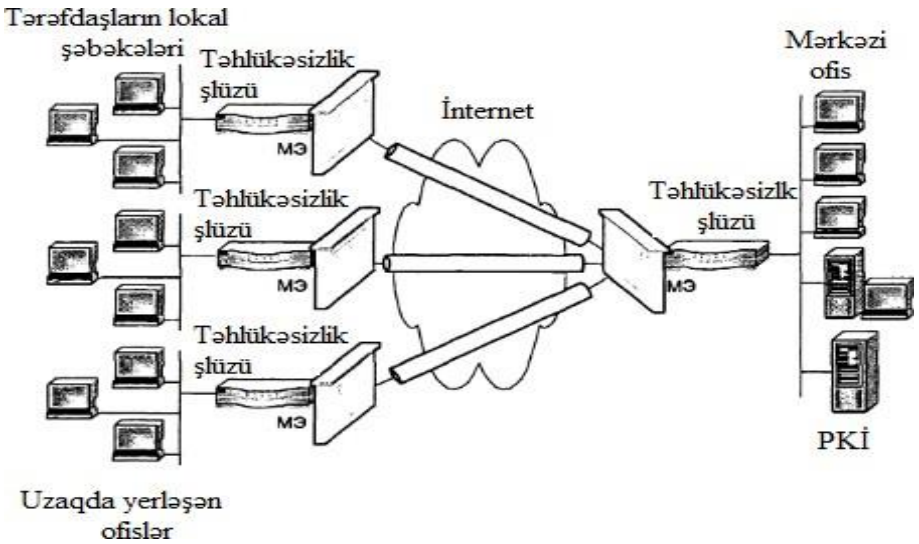
xərclərini əhəmiyyətli dərəcədə azaldır, çünki İnternetdə məsafə əlaqənin dəyərinə təsir göstərmir.

İntranet VPN-nin üstünlükləri aşağıdakılardır:

- Məxfi məlumatları qorumaq üçün güclü kriptoqrafik məlumat şifrələmə protokollarından istifadə;
- avtomatlaşdırılmış satış sistemləri və verilənlər bazası idarəetmə sistemləri kimi kritik tətbiqləri yerinə yetirərkən etibarlı fəaliyyət;
- sürətlə böyüyən yeni sayda istifadəçinin, ofis və proqram əlavələrinin səmərəli yerləşdirilməsinin idarəetmə çevikliyi.

İnternetdən istifadə edərək İntranet VPN –nin qurulması VPN texnologiyasını həyata keçirməyin ən səmərəli üsuludur. Lakin İnternetdə xidmət səviyyələrinə ümumiyyətlə zəmanət verilmir. Zəmanətli xidmət səviyyəsi tələb edilən şirkətlər, xidmət təminatçıları tərəfindən təqdim olunan müştərək şəbəkə infrastrukturlarından istifadə edərək özəl VPN-lərinin yerləşdirilməsini düşünməlidirlər.

Şirkətlərarası VPN (şək.3.4), bir şirkətin şəbəkəsindən digər şirkətin şəbəkəsinə birbaşa çıxışı təmin edən və bununla da işgüzar əməkdaşlıq zamanı dəstəklənən rabitə etibarlılığını artıran bir şəbəkə texnologiyasıdır.



Şəkil 3.4. Şirkərtlərarası Extranet VPN şəbəkəsi

Extranet VPN şəbəkələri, ümumiyyətlə, korporasiyadaxili virtual özəl şəbəkələrə bənzəyirlər, yeganə fərq informasiya təhlükəsizliyi probleminin onlar

üçün daha kəskin olmasıdır. Extranet VPN üçün işgüzar tərəfdaşların şəbəkələrində istifadə edə bildikləri müxtəlif VPN həlləri ilə qarşılıqlı əlaqə qurma qabiliyyətini təmin edən standart VPN məhsullarından istifadə xarakterikdir. Bir neçə şirkət birlikdə işləməyi və şəbəkələrini bir-birləri üçün açmağı qərara alarkən yeni tərəfdaşlar tərəfindən yalnız müəyyən məlumatların əldə olunmasına diqqətlə yanaşmalıdırlar. Eyni zamanda məxfi məlumatlar icazəsiz istifadədən etibarlı şəkildə qorunmalıdır. Buna görə korporativ şəbəkələrdə açıq şəbəkədən daxil olmaya nəzarətə böyük əhəmiyyət verilir. İstifadəçinin identifikasiyası yalnız məlumat əldə etmək üçün icazə verilən şəxslərin olmasını təmin etmək üçün vacibdir. Eyni zamanda, icazəsiz girişdən qorunan inkişaf sistemi özünə diqqəti cəlb etməməlidir.

Şəbəkə monitorinqi vasitələrindən, məlumat axınlarının təhlili və modelləşdirilməsindən, yüksək keyfiyyətli antivirus proqramlarından istifadə etmək, məlumatların arxivləşdirilməsini və ehtiyat nüsxələrini, protokol analizatorlarını, kənar şəxslərin məlumatlarına fiziki daxil olmasının qarşısını almağa kömək edəcək təşkilati və inzibati tədbirləri yerinə yetirmək arzuolunandır.

3.3. Kompüter şəbəkələrinin inteqral təhlükəsizliyinin təmin olunma üsulları

KİS üçün informasiya təhlükəsizliyini təmin etmək vəzifəsi ənənəvi olaraq onun qurulmasına qoyulan investisiyaların mühafizəsini təmin edən İTS - nin yaradılması ilə həll olunur. Başqa sözlə, İTS KİS-də mövcud tətbiqlər üçün tamamilə şəffaf şəkildə işləməlir və KİS-də istifadə olunan şəbəkə texnologiyalarına tam uyğun olmalıdır.

Müəssisənin yaradılmış informasiya təhlükəsizlik sistemi yeni texnologiyaların və xidmətlərin ortaya çıxmasını nəzərə almalı və bu gün KİS-nin hər hansı bir elementi üçün:

- Açıq standartların tətbiqi;

- inteqrasiya olunmuş həllərin istifadəsi;
- informasiya təhlükəsizliyi vasitələrinin inkişafındakı əsas tendensiyalar kimi ümumi tələblərə cavab verməlidir.

IPSec və PKI kimi standartlar müəssisələrin xarici əlaqələrinin təhlükəsizliyini və tərəfdaş müəssisələrin və ya uzaq müştərilərin müvafiq məhsulları ilə uyğunluğu təmin edir. X.509 rəqəmsal sertifikatları da bu gün istifadəçilər və cihazların identifikasiyası üçün standart əsasdır. Ümidverici vasitələr, şübhəsiz ki, bu gün bu standartları dəstəkləməlidir.

İnteqrasiya edilmiş həllər dedikdə təhlükəsizlik alətlərinin digər şəbəkə elementləri (ƏS, marşrutlaşdırıcılar, qovluq xidmətləri, QoS siyasət serverləri və s.) ilə inteqrasiyası, həmçinin müəssisə məlumat mənbələrinin hərtərəfli qorunmasını, məsələn, şəbəkənin inteqrasiyasını təmin etmək üçün müxtəlif və IP ünvanlarının translyatoru ilə VPN şlüzü olan ekranla öz aralarında təhlükəsizlik texnologiyalarının inteqrasiyası başa düşülür. KİS böyüdükcə və inkişaf etdikcə İTS bütövlüyünü və idarəçiliyini itirmədən asanlıqla miqyaslanmağı bacarmalıdır. Mühafizə vasitələrinin miqyaslılığı mühafizə sisteminin imkanlarının tədricən genişlənməsi yolu ilə dəyərinə və etibarlılığına görə optimal həll yolu seçməyə imkan verir. Miqyaslılıq müəssisənin çoxsaylı filialları, onlarla tərəfdaş müəssisələri, yüzlərlə uzaq işçiləri və milyonlarla potensial müştərisi olduğu halda onun səmərəli fəaliyyətini təmin edir.

İS-nin inteqral təhlükəsizliyinə aşağıdakı komponentlər daxildir:

- Fiziki təhlükəsizlik – binaların, mobil qurğuların, insanların, həmçinin aparat vasitələrinin (kompüterlərin, saxlanma vasitələrinin, şəbəkə avadanlığının, kabel təsərrüfatının, dəstəkləyici infrastrukturun) mühafizəsi;
- şəbəkələrin və telekommunikasiya qurğularının təhlükəsizliyi - rabitə kanallarının hər cür təsirdən qorunması;
- sistem və tətbiqi proqram təminatlarının təhlükəsizliyi – viruslardan, məntiqi "minalar"dan, sistem konfiqurasiyasında və proqram kodunda icazəsiz dəyişikliklərdən mühafizə;

- verilənlərin təhlükəsizliyi – verilənlərin məxfiliyinin, bütövlüyünün və əlçatanlığının təmini.

İnteqral informasiya təhlükəsizliyinin təmini məsələsi informasiyanın etibarlı saxlanması və istifadəçiyə təhlükəsiz ötürülməsi problemi ilə birlikdə ortaya çıxdı. İndiki mərhələdə inteqral yanaşma bütün mümkün təhdid növləri (icazəsiz daxil olma, məlumatın alınması, terrorizm) nəzərə alınmaqla həm zaman (İS-nin həyat dövrü müddətində), həm də məkan üzrə (bütün texnoloji fəaliyyət dövrü ərzində) təhlükəsizlik prosesinin məcburi davamlılığını nəzərdə tutur.

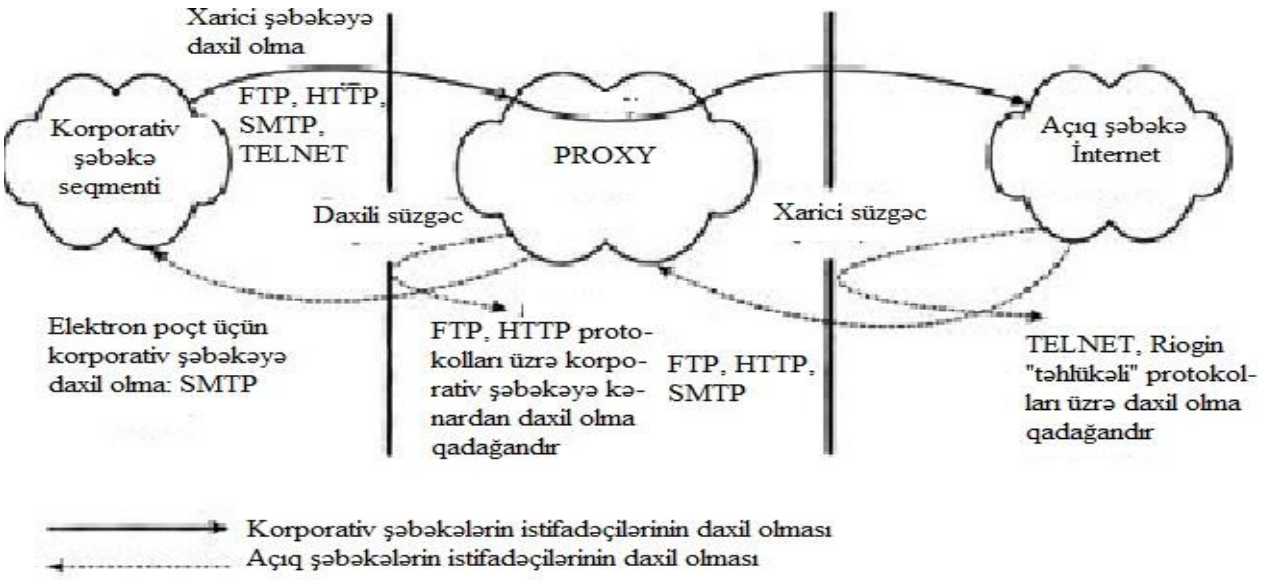
İnteqral yanaşmanın hansı formada tətbiq olunmasından asılı olmayaraq bu, bir sıra mürəkkəb, müxtəlif özəl problemlərin sıx münasibətlərdəki həlli ilə əlaqələndirilir. Bunlardan daha mühüm olanlar informasiyaya daxil olma, onun texniki və kriptoqrafik "bağlanması", texniki vasitələrin yayılmış ziyanverici şüalanmasının aradan qaldırılması, obyektlərin texniki və fiziki möhkəmləndirilməsi, onların mühafizəsi və siqnalizasiya sistemləri ilə təmin edilməsi kimi vəzifələrdir [17].

Müasir İS-nin tərkibində informasiyanın standart inteqrasiya olunmuş mühafizə vasitələrinin məcmusuna, adətən, aşağıdakı komponentlər daxildir:

- Fayl səviyyəsində mühafizə texnologiyasından (File Encryption System - FES) istifadə edərək məlumatın etibarlı saxlanmasını təmin etmə vasitələri;
- məlumat mənbələri üçün avtorizasiya və giriş vasitələri, habelə biometrik avtorizasiya sistemləri və texnologiyalarından istifadə etməklə məlumatlara icazəsiz daxil olmadan mühafizə vasitələri (smart kartlar, touch-yaddaş, USB portları üçün açarlar, gizli rəqəmsal markerlər və s.);
- ümumi girişli rabitə şəbəkələrinə (İnternet) qoşulduqda xarici təhdidlərdən mühafizə vasitələri, həmçinin firewall və məzmunlu süzmə (Content Inspection) texnologiyasından istifadə edərək İnternetdən çıxışı idarəetmə vasitələri;
- ixtisaslaşdırılmış antivirus profilaktika komplekslərindən istifadə edərək viruslardan mühafizə vasitələri;

- təhlükəsiz VPN texnologiyasından istifadə edərək açıq rabitə kanalları vasitəsilə ötürülən məlumatların məxfiliyini, bütövlüyünü, əlçatanlığını və orijinallığını təmin etmə vasitələri;
- həmlələrin aşkar edilməsi (Intrusion Detection) texnologiyasından istifadə edərək informasiya resurslarının təhlükəsizliyi ilə bağlı fəal tədqiqinin aparılması vasitələri (sxem 3.1.).

Fayl səviyyəsində informasiyanın mühafizəsi. Bu texnologiyalar, faylların, qovluqların və disklərin məzmununu kodlaşdıraraq kompüterin sərt diskində və ya şəbəkə disklərində istifadəçinin şəxsi məlumatlarını gizlətməyə imkan verir. Bu məlumatlara daxil olma klaviaturadan, smart-kartdan, HASP - və ya USB - açarlarından daxil edilə bilən bir açar təqdim edildikdə təmin edilir.



Sxem 3.1. Şirkətin daxili şəbəkəsinin İnternetin xarici məkanı ilə qarşılıqlı əlaqə sxemi

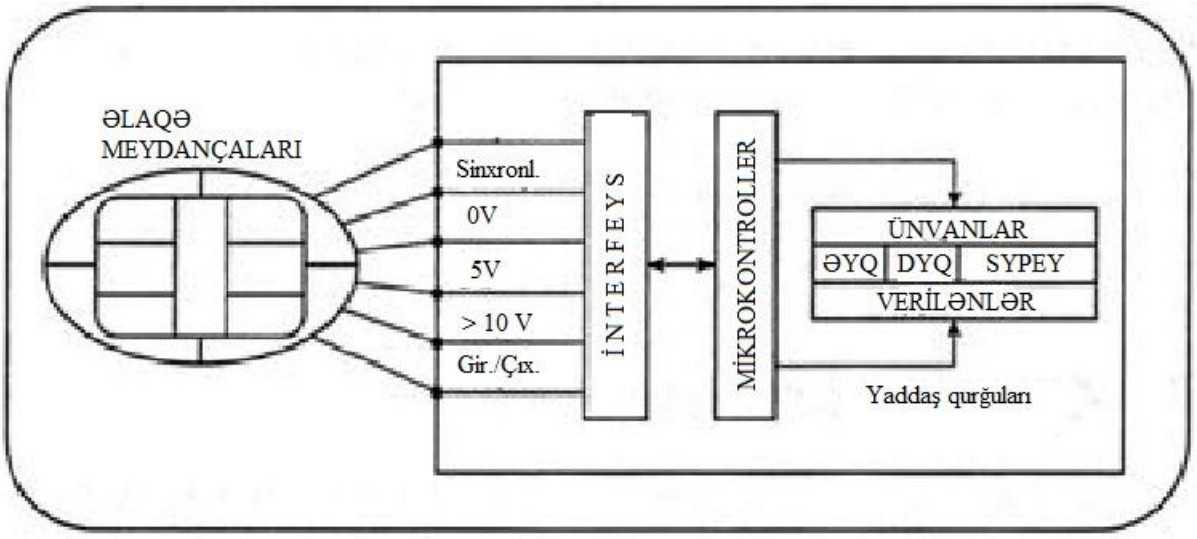
Token texnologiyaları (smart kartlar, touch-yaddaş, USB portları üçün açarlar, gizli rəqəmsal markerlər). Elektron jetonlar – açarlar (Token) zəmanətli istifadəçi identifikasiyası əsasında məlumatların qorunmasının etibarlılığını artıran bir vasitədir. Tokenlər sistem istifadəçisinin şəxsi məlumatlarını və bəzi şifrələrini saxlamaq üçün "konteynerlər"dir.

Tokenin əsas elementi, unikal xüsusiyyətlər dəsti ilə açarları yaratmağa imkan verən mikrokontrollerdir. Mikrokontroller sayəsində açarın işinin məntiqi mürəkkəbləşdirilir, bu onu daha intellektual edir (şək. 3.5).

Müasir tokenlərin baza imkanları bunlardır:

- Sistemlərə, şəbəkələrə və s. daxil olma üçün şifrələrin saxlanması;
- məxfiliyi təmin etmək üçün şifrələmə açarlarının saxlanması;
- autentifikasiya məqsədləri üçün açarların saxlanması;
- informasiyanın autentifikasiyası və məxfiliyinin şifrələmə alqoritmlərinin icrası;
- informasiyanın təhlükəsiz saxlanması.

Tokenin əsas üstünlüyü ondan ibarətdir ki, fərdi məlumatlar həmişə daşıyıcıda olur (smart kart, açar və s.) və yalnız sistemə və ya kompüterə giriş zamanı təqdim olunur.



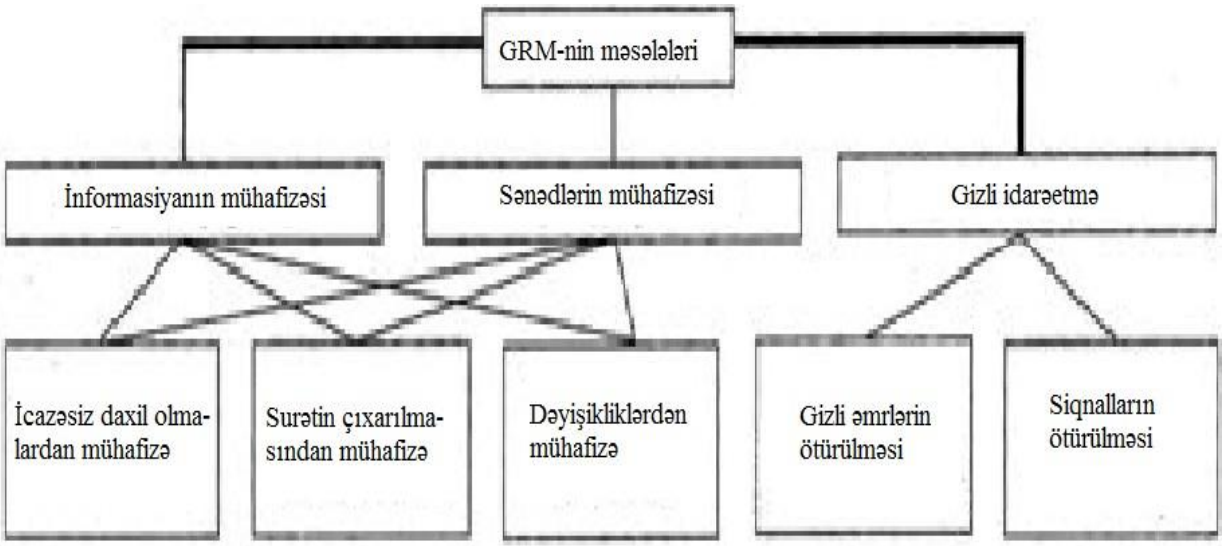
SYPEY - Silinən yenidən proqramlaşdırılan elektrik yaddaş

Şək. 3.5. Smart – kartın arxitekturası

Smart kart texnologiyası məlumatların kodlaşdırılması və dekodlaşdırılması üçün müxtəlif qurğulara və sistemlərə daxil olma üçün giriş qaydalarının birləşdirməyə və parol sistemini bir fərdi elektron mühitdə yerləşdirməyə imkan verir.

Hal-hazırda müxtəlif növ smart kartlar istifadəçinin əlindən oxunan biometrik məlumatlara əsaslanan fərdi identifikasiya sistemi ilə paylanır.

Gizli rəqəmsal markerlər qorunan obyektə daxil edilmiş xüsusi proqramlardır. Belə markerlər obyekti "fərdiləşdirir", bununla dəyişdirilmədən və düzəldilmədən qoruyur və ya icazəsiz oxunmadan və surətin çıxarılmasından ümumi mühafizə funksiyalarını yerinə yetirir (şək. 3.6).



Şək. 3.6. Gizli rəqəmsal marker texnologiyası bazasında ümumi mühafizə funksiyaları

Firewalls. Firewall texnologiyasının istifadəsi aşağıdakı kimi problemlərin həlli üçün təklif olunur:

- Extranet və İntranet şəbəkələrində yerləşən istifadəçilər və informasiya mənbələrinin xarici şəbəkələrlə təhlükəsiz qarşılıqlı əlaqəsi;
- müəssisə bölmələrinin paylanmış və seqmentləşdirilmiş yerli şəbəkələri üçün texnoloji baxımdan vahid mühafizə tədbirlərinin təşkili;
- korporativ şəbəkənin müxtəlif qapalılıq dərəcəsi üzrə seqmentləri üçün adekvat təhlükəsizlik vasitələrini təmin edən iyerarxik təhlükəsizlik sisteminin qurulması.

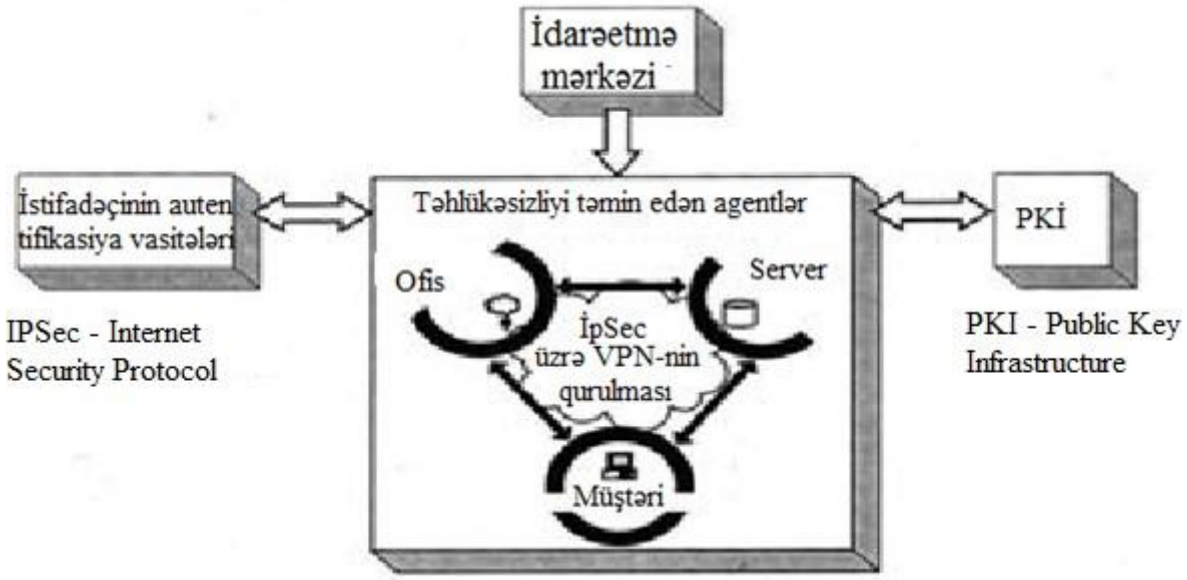
Təşkilatın ölçüsündən və qurulmuş təhlükəsizlik siyasətindən asılı olaraq funksionallığına və dəyərinə görə fərqlənən (CheckPoint Firewall-1, Cisco Şəxsi

İnternet Birjası (PIX) firewall və s.) Firewalls tövsiyə olunur. Məzmun Süzgəz qurğuları (*Content Inspection*), adətən, bir reklam xarakterli (Spam) çox sayda e-poçt abunəçisinə zorla göndərilən çox sayda təhlükəli olmayan, lakin praktik olaraq yararsız məlumatların qarşısını almaq üçün poçt serverlərinin girişlərinə quraşdırılır.

Antivirus vasitələr. Yuxarıda qeyd edildiyi kimi, virusların geniş şəkildə yayılması ("qurdlar", "Trojan atları") əksər şirkətlər və dövlət qurumları üçün böyük problemə çevrilmişdir. Əksəriyyətin düşündüyünə görə, kompüterləri "yoluxdurmağın" əsas yolu İnternetdir, buna görə də bir çox menecerin fikrincə ən yaxşı həll yolu korporativ şəbəkəni Ümumdünya hörümçək torundan çıxarmaq və ya əksər işçilərin istifadəsini qadağan etməkdir, həmin şəsxlər virusların müəyyən bir kompüterə daxil olmasının bir sıra digər yolunun da olduğunu, məsələn, başqasının fleş və disklərindən, pirat proqramlardan və ya fərdi kompüterlərdən (məsələn, ev və ya tələbə kompüterlərindən daha çox olduqda təhlükəli olduğunu) daxil olduğunu nəzərə almır. Müvafiq İTS-nin və lisenziyalı antivirus vasitələrinin (məsələn, Kaspersky Laboratoriyası və ya Dr.Web) sistematik tətbiqi "virus" infeksiyası riskini əhəmiyyətli dərəcədə azaldır.

Mühafizə olunan virtual özəl şəbəkələr. TCP / IP protokollarını dəstəkləyən açıq rabitə kanalları üzərindən ötürülən məlumatları qorumaq üçün beynəlxalq İnternet Təhlükəsizlik Protokolu standartlarına əsaslanan təhlükəsiz virtual özəl şəbəkələrin (VPN) qurulması üçün hazırlanmış bir sıra proqram məhsulları mövcuddur (şək. 3.7).

Virtual şəbəkələr ən çox ictimai şəbəkələrdə (İnternet) icarəyə verilən və kommutasiya edilmiş rabitə kanalları əsasında yaradılır. Kiçik və orta şirkətlər üçün, təcrid olunmuş korporativ şəbəkələrə yaxşı bir alternativdir, çünki yüksək zəmanətli etibarlılıq, dəyişkən topologiya, konfiqurasiyanın sadəliyi, miqyaslılığın asanlığı, şəbəkədəki bütün hadisələrə və fəaliyyətlərə nəzarət, kanallar və rabitə avadanlıqlarını nisbətən aşağı qiymətlə icarəyə götürmə kimi aşkar üstünlüklərə malikdirlər.



Şək. 3.7. Beynəlxalq standartlara və protokollara əsaslanan VPN konfiqurasiyası

Məhsullar Windows və Solaris ƏS-də işləyir və:

- şəbəkələr vasitəsilə ötürülən məlumatların qorunmasını (məxfiliyini, həqiqiliyini və bütövlüyünü);
- qorunan şəbəkənin perimetrinə giriş nəzarətini;
- şəbəkə obyektlərinin istifadəçilərinin identifikasiyası və autentifikasiyasını;
- korporativ şəbəkə təhlükəsizlik siyasətinin mərkəzləşdirilmiş idarə edilməsini

təmin edir.

Açıq kriptoqrafik interfeysə malik şifrələmə sistemləri kriptoqrafik alqoritmlərin müxtəlif tətbiqlərindən, dünyanın istənilən ölkəsində qəbul edilmiş milli standartlara uyğun məhsullardan istifadə etməyə imkan verir. Müxtəlif modifikasiyaların mövcudluğu (məhsul xətti müştəri, server platformaları üçün, ofis məlumatı şəbəkəsi üçün birdən çox məhsulu əhatə edir, əsas məlumatlar yaratmaq üçün), sistemin gücünü tədricən artırmaq imkanı ilə dəyərliliyi və etibarlılığı baxımından optimal olan həll yolu seçməyə imkan verir.

Hücumu aşkarlama texnologiyaları (*Intrusion Detection*). Daimi şəbəkə dəyişiklikləri (yeni iş stansiyalarının ortaya çıxması, proqram vasitələrinin yenidən konfiqurasiyası və s.) yeni zəif nöqtələrin, təhdidlərin və hücumların, informasiya mənbələrinin və qoruma sisteminin özünün meydana gəlməsinə səbəb ola bilər. Bununla əlaqədar onları vaxtında müəyyənləşdirmək və informasiya kompleksinin və onun altsistemlərinin, o cümlədən mühafizə altsisteminin müvafiq parametrlərinə dəyişiklik etmək xüsusilə vacibdir. Bu o deməkdir ki, sistem inzibatçısının iş yerləri şəbəkələri araşdırmaq və "kənar" və "hücumlar" üçün zəif nöqtələri ("dəliklərin" olması) müəyyənləşdirmək üçün xüsusi proqram təminatı ilə təchiz olunmalıdır. Məsələn, ELVIS + və Net Pro VPN məhsullarına geniş ticarət paketləri ailəsi arasında İnternet təhlükəsizlik sistemlərinin *Internet Scanner* və *System Security Scanner* kimi ən güclü məhsulları həmçinin NetRanger icazəsiz giriş aşkaretmə sistemi və NetSonar təhlükəsizlik zəifliyi skaneri kimi Cisco məhsulları daxildir [18].

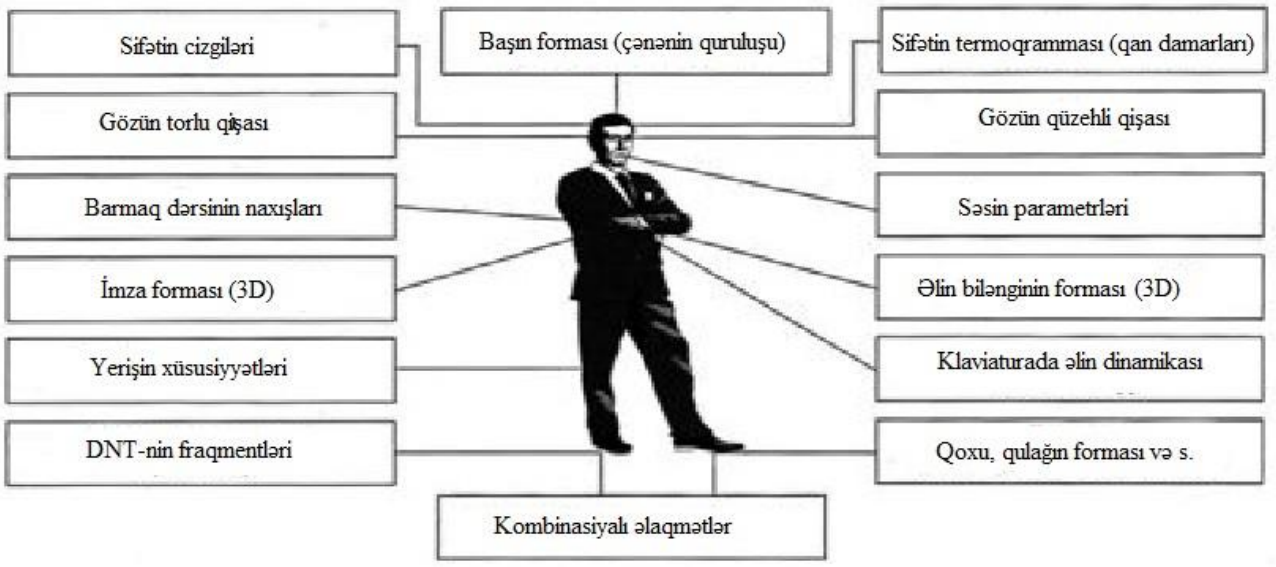
Açıq açar infrastrukturu (*PKI — Public* Key Infrastruture). PKI-nin əsas funksiyaları bunlardır: rəqəmsal açarların və sertifikatların həyat dövriyyəsinə dəstək (yəni onların yaradılması, paylanması, ləğvi və s.), istifadəçilərin identifikasiyası və autentifikasiyası prosesinə dəstək, mövcud tətbiqlərin və təhlükəsizlik altsisteminin bütün komponentlərinin inteqrasiya mexanizminin tətbiqi. PKI sisteminin fəaliyyətini müəyyənləşdirən və müxtəlif informasiya təhlükəsizliyi vasitələri ilə qarşılıqlı əlaqəsini asanlaşdıran mövcud beynəlxalq standartlara baxmayaraq, təəssüf ki, hər bir mühafizə vasitəsi, istehsalçısının standartlara uyğun olduğunu bəyan etsə də, istənilən PKI sistemi ilə işləyə bilməz. Hal-hazırda, IPSec və PKI-yə əsaslanan inteqrasiya olunmuş həllər getdikcə daha çox istifadə olunur (bax: şək. 3.7).

Hal-hazırda yuxarıda göstərilən məlumatların qorunması vasitələri ilə yanaşı, biometrik təhlükəsizlik sistemləri də şəbəkələrdə geniş istifadə olunur. Frost & Sullivan analitik şirkətinin məlumatına görə, 2000-ci ildə Amerikada biometrik avadanlıqların ümumi satış dəyəri 86,8 milyon dolları keçdi, 2001-ci ildə 160.3

milyon dollara yüksəldi və 2012-ci ildə 9 milyard dolları keçdi. Cari dövr üçün bu cür qurğuların bazarı ildə on milyardlarla dolları keçib.

Biometrik identifikasiya texnologiyaları ənənəvi vasitələrə nisbətən bir sıra üstünlüklərə malikdir. Biometriya dedikdə fizioloji və ya davranış xüsusiyyətlərinə əsaslanan şəxsin avtomatik eyniləşdirilməsi və şəxsiyyətin təsdiqlənməsi üsulları başa düşülür (şək. 3.8).

Ən çox istifadə olunan üç əsas biometrik metod - insanın barmaq izləri, gözün bəbəyi və üzün təsviri ilə tanınmasıdır. Nyu-Yorkdan olan Beynəlxalq Biometrik Qrup konsaltinq şirkətinə görə, ən çox yayılmış texnologiya barmaq izlərinin aşkarlanması hesab olunur.



Şəkil 3.8. Fərdi identifikasiya üçün biometrik parametrlər sistemi

Qeyd olunur ki, biometrik qurğuların satışından əldə olunan 127 milyon dollar gəlirdən 44% -i barmaq izi skanerləridir. Üz tanıma sistemləri tələb baxımından ikinci yeri (14%) tutur, daha sonra ovucun formasına (13%), səsə (10%) və gözün bəbəyinə (8%) görə tanıma qurğuları gəlir. Bu siyahıdakı imza yoxlama qurğuları 2% -dir.

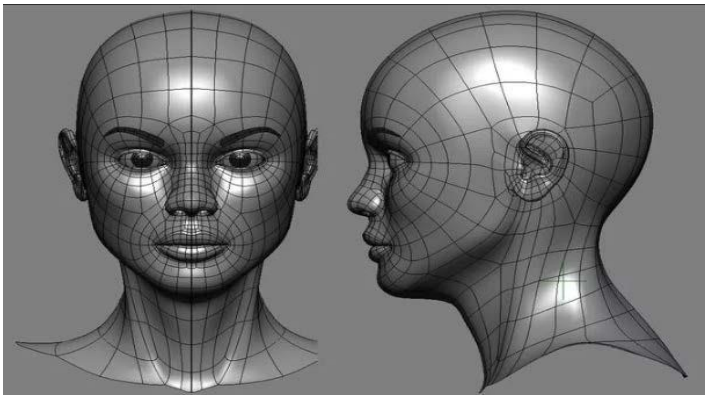
Biometrik təhlükəsizlik sistemlərinin faydaları göz qabağındadır. Bənzərsiz insan keyfiyyətləri onunla seçilir ki, onları saxtalaşdırmaq, həmçinin öz əlimizlə

saxta barmaq izi buraxmaq və ya gözün bəbəyini başqasının görünüşünə çevirmək çətindir.

Kağız identifikatorlarından (pasport, sürücülük vəsiqəsi və ya digər şəxsiyyət vəsiqəsi), paroldan və ya fərdi identifikasiya nömrəsindən (PİN) fərqli olaraq biometrik xüsusiyyətləri unutmaq və ya itirmək olmur. Bundan əlavə, unikallığına görə, oğurluq və ya saxtakarlığın qarşısını almaq üçün istifadə olunur.

Üz tanıma metodları ikiölçülü və ya üçölçülü şəkillərlə (sözdə 2D və 3D fotoşəkilləri) işləyə bilər. İnsanın üz cizgilərinə görə identifikasiyası biometrik sənayenin ən dinamik inkişaf edən sahələrindən biridir. Bu metodun cəlbediciliyinə görə insanların ümumiyyətlə bir-birlərini tanıma xüsusiyyətlərinə anolojidir. Multimedia texnologiyalarının yayılması sayəsində şəhər küçələrində və meydanlarda, qatar stansiyalarında, hava limanlarında və digər izdihamlı yerlərdə videokameralar quraşdırılaraq bu istiqamətdə getdikcə daha çox işlər görülür.

Üzün tanınması aşağıdakı funksiyaların hər hansı birinin yerinə yetirilməsini ehtiva edir: autentifikasiya (“birin-birə”) və ya identifikasiya (“çoxdan biri”nin uyğunluğunun axtarışı). Sistem üzün tanınması üçün görüntü keyfiyyətini avtomatik olaraq qiymətləndirir və zəruri hallarda onu inkişaf etdirməyə qadirdir. Ayrıca məlumat seqmentlərindən bir üz görünüşü,həmçinin rəqəmsal kod və ya hər bir fərdə xas olan daxili bir şablon yaradır (şək. 3.9).



Şəkil 3.9. İnsanın identifikasiyası sistemində üzün 3D görüntüsü

Üçölçülü fotoqrafiya, təxminən beş il əvvəl yaradılmış ən son biometrik texnologiyadır. Cəmi 5KB olan üçölçülü bir foto biometrik pasportda qeyd edilə bilər; o, fərdi identifikasiyanın dəqiqliyini yüksəldir və sənədlərin avtomatik uzlaşdırılmasının etibarlılığını artırır. Mütəxəssislər qeyd edirlər ki, üçölçülü fotoşəkillərin tanınma səviyyəsi 90% - dən çoxdur, ikiölçülü bir görüntüdə bu göstərici nadir hallarda 50% -i aşır.

Biometrik texnologiyalar sənədlərin uzlaşdırılmasının etibarlılığını və səmərəliliyini artırmaq üçün nəzərdə tutulmuşdur, bütün sənədlərin elektron sənədləşdirilməsi (qeyd edilməsi) üçün, habelə geniş şəraitdə bir fərdin şəxsiyyətinin səmərəli və etibarlı identifikasiyası üçün nəzərdə tutulmuşdur (şək. 3.10).

Şək. 3.10. Hava limanında biometrik nəzarət

Bu problemi həll edərkən iki ssenari mümkündür: ikiqat və ya üçqat yoxlama. İkiqat yoxlama, elektron pasportda və ya vizada qeyd olunan biometrik şablonun yoxlanılan obyektin biometrik xüsusiyyətləri ilə uzlaşdırılmasını nəzərdə tutur.

Üçqat yoxlama, öz növbəsində, bu iki xüsusiyyətin biometrik məlumatların milli reyestrində saxlanılan şablonla əlavə yoxlanılmasına əsaslanır. Bu ssenaridə sənədin saxtalaşdırılması üçün edilən hər hansı bir cəhd mənasız olacaq, çünki üçqat yoxlama sənəd verildiyi zaman dövlət reyestrində qeyd olunan şablonla uyğunsuzluğu aşkar edəcəkdir.

Əsasən pasport və ya viza verilməsi ilə əlaqəli başqa bir məsələ oxşar sənədin əvvəllər eyni biometrik məlumatları olan bir vətəndaşa verilməməsinin, fərqli bir ad altında qeydiyyatdan keçməsinin, habelə vətəndaşın biometrik məlumatlarının yoxlanılmasıdır. Hər iki halda problemin həlli identifikasiya rejimində biometrik metodların istifadəsini nəzərdə tutur, halbuki verilənlər bazasının ölçüsü çox böyük ola bilər.

Birinci məsələni (ikiqat və üçqat yoxlama) həll etmək üçün məqbul dəqiqliyi təmin edən üç üsuldan (üz fotoşəkilləri, barmaq izləri və ya irislərdən istifadə etməklə) istifadə etməyə icazə verilir. İkinci məsələni (böyük bir məlumat bazası ilə vətəndaşın şəxsiyyətini) həll etmək üçün kombinasiyalı metodlara ehtiyac duyulur.

Mütəxəssislərin fikrincə, biometrik metodlar tətbiq edilərkən ən əsaslandırılmış həll barmaq izi məlumatlarının (iki barmaqla) və üzün iki formada şəkillərinin (ikiölçülü və üçölçülü) elektron identifikasiya sənədlərində olduğu kimi ilkin toplanması və vahid dövlət reyestrinə daxil edilməsidir. Eyni zamanda, vətəndaşların sərhədləri keçdikdə sənədləri uzlaşdırmağı özündə cəmləşdirən yoxlama məsələsini həll etmək üçün kombinasiyalı (2D + 3D) üz tanıma metodu kifayətdir. Bu təmasda olmayan metod, maksimum ölçülə bilən biometrik xüsusiyyətləri (başqa sözlə, yoxlama və keçidin maksimal sürəti) təmin edir, buna görə də yavaşlamayacaq, əksinə nəzarət nöqtələri vasitəsilə sərnişin daşımalarını sürətləndirəcəkdir.

3D və xüsusilə kombinasiyalı metodun dəqiqliyi yüksəkdir və yoxlama rejimində, eləcə də çox böyük olmayan (10 min nəfərə qədər) əməliyyat məlumat bazası olan identifikasiya rejimində (məsələn, axtarışda olanların siyahısı) tələblərə cavab verir. Bundan əlavə, adi ikiölçülü fotonun istifadəsi, birincisi, ümumiyyətlə, qəbul edilmiş təcrübədir və ikincisi, operatora son qərar vermək və ya verilənlər bazasından ən bənzər bir neçə şəxslə vizual müqayisə etmək imkanı verir. Bunun sayəsində əməliyyat identifikasiyası üçün məlumat bazasının ölçüsünü bir neçə yüz min insana artırmaq olar.

Barmaq izi məlumatlarının istifadəsi yalnız şəxsiyyətin təsdiqlənməsi zamanı sənədin verilməsinə qədər, habelə zərurət yarandıqda vətəndaşın tutulması və ittihamların təqdim edilməsinə qədər nəzərdə tutulur. Bu, pasportda qeyd olunan barmaq izi məlumatlarını yalnız müvafiq hüquq mühafizə orqanlarının işçilərinə əldə etmək hüququ olan insanların dairəsini məhdudlaşdıraraq məlumatların qorunması səviyyəsini artırmağa imkan verir.

Ölkəmizdə ictimai açar infrastrukturunun təhlili, dizaynı və inkişafı üçün xidmətlər göstərən şirkətlər meydana çıxmağa başlayır. Bölmə və korporativ

şəbəkələr genişləndiyindən VPN məhsulları PKI olmadan işləyə bilmirlər, yalnız VPN təminatçıları bu sahədə təcrübəyə malikdirlər.

Şirkət fəaliyyətinin miqyasından asılı olaraq, informasiya təhlükəsizliyini təmin etmə üsulları və vasitələri dəyişə bilər, lakin istənilən İT xidmət mütəxəssisi informasiya təhlükəsizliyi sahəsində hər hansı bir problemin birtərəfli həll edilə bilməyəcəyini söylər, çünki bu halda hərtərəfli, inteqrasiya olunmuş bir yanaşma tələb olunur.

Təəssüf hissi ilə qeyd etmək lazımdır ki, nəhəng biznes şirkətlərinin top menecerləri və böyük dövlət qurumlarının rəhbərləri çox vaxt informasiya təhlükəsizliyi sahəsində bütün problemlərin heç bir xüsusi təşkilati, texniki və maliyyə səyləri olmadan həll edilə biləcəyinə inanırlar. Bir çox təşkilatlarda, menecerlər və hətta mütəxəssislər, səylərini ayrı-ayrı, əlaqəsiz texniki vasitələrin istifadəsinə cəmləşdirərək beynəlxalq standartlara və bərabər standartlara cavab verən sistemlərin metodlarına laqeyd yanaşırlar ki, bu da müvafiq yerli standartların və rəhbər sənədlərin olmamasına gətirib çıxarır.

KİS mənbələrinin etibarlı qorunmasını təmin etmək üçün, İTS-də ən mütərəqqi və perspektivli informasiya təhlükəsizliyi texnologiyaları tətbiq edilməlidir. Bunlara aşağıdakılar daxildir:

- informasiaynın məxfiliyini, bütövlüyünü və həqiqiliyini təmin etmək üçün kriptoqrafik məlumatların qorunması;
- istifadəçilərin və şəbəkə obyektlərinin identifikasiyası üçün identifikasiya texnologiyaları;
- ümumi rabitə şəbəkələrinə qoşulduqda korporativ şəbəkəni xarici təhdidlərdən qorumaq üçün firewall texnologiyaları;
- açıq rabitə kanalları vasitəsilə ötürülən məlumatları qorumaq üçün virtual təhlükəsiz kanallar və VPN;
- USB portlar üçün açarlar və s.) və digər təsdiqləmə vasitələri;
- istifadəçi səviyyəsində giriş nəzarəti və məlumatlara icazəsiz daxil olmaqdan qorunma;

- idarəetmə infrastrukturuna dəstək IaPKI ictimai düymələri informasiya ehtiyatlarının təhlükəsizliyinin fəal istintaq texnologiyası (Intrusion Detection);
- xüsusi virus təhlükəsinin qarşısının alınması və qorunması sistemlərindən istifadə edən viruslardan mühafizə texnologiyaları;
- vahid müəssisələrin təhlükəsizlik siyasətinə əsaslanan məlumat təhlükəsizliyi sistemlərinin mərkəzləşdirilmiş idarə edilməsi;
- məlumat təhlükəsizliyini təmin etmək üçün vahid yanaşma, məlumat qoruma texnologiyaları və vasitələrinin rasional birləşməsinin təmini.

Şəbəkələrdə iş zamanı informasiya təhlükəsizliyi problemlərinin həlli yollarını tapmaq üçün İSTF (Internet Security Task Force) - müstəqil konsorsium yaradılmışdır. Bu, informasiya təhlükəsizliyi şirkətlərinin, elektron müəssisələrin və İnternet provayderlərinin nümayəndələrindən və mütəxəssislərindən ibarət ictimai bir təşkilatdır. Konsorsiumun məqsədi İnternet təhlükəsizliyi üçün texniki, təşkilati və əməliyyat qaydalarını inkişaf etdirməkdir. İSTF konsorsiumu informasiya təhlükəsizliyinin e-biznes yaradıcılarının ilk növbədə səmərəliliyin təmin olunması üçün diqqət etməli olduğu aşağıdakı sahələri ayırmışdır:

- ✓ autentifikasiya (məlumatın obyektiv təsdiqlənməsi mexanizmi);
- ✓ fərdi informasiya hüququ (informasiyanın konfidensiallığının təmini);
- ✓ təhlükəsizlik hadisələrinin tərifi;
- ✓ korporativ perimetrin qorunması;
- ✓ hücumların təyini;
- ✓ potensial təhlükəli məzmuna nəzarət;
- ✓ daxil olmaya nəzarət;
- ✓ idarəetmə;
- ✓ hadisələrə reaksiya (insidentə reaksiya).

ISTF tövsiyələri mövcud və ya yeni yaradılan e-ticarət və e-biznes şirkətləri üçün nəzərdə tutulmuşdur. Onların həyata keçirilməsi, e-biznes sistemindəki məlumatların kompleks mühafizəsini təmin edirdi.

Təhdidlərdən hərtərəfli qorunmaq və elektron biznes üçün rabitə resurslarından səmərəli və etibarlı istifadəyə zəmanət vermək üçün aşağıdakıları etmək lazımdır:

- Elektron biznes sistemindəki təhlükəsizlik təhdidlərini təhlil etmək;
- informasiya təhlükəsizliyi siyasətini inkişaf etdirmək;
- informasiyanın konfidensiallığını və tamlığını təmin etməklə xarici ötürmə kanallarını mühafizə etmək;
- şəbəkələrin və İnternetin açıq mənbələrinə təhlükəsiz daxil olma imkanını sığortalamaq;
- ötürüldüyü kanallardan asılı olmayaraq ayrıca kommersiya əhəmiyyəti olan verilənləri qorumaq;
- korporativ sistemlərin informasiya resurslarına məsafədən daxil olmanı personala təqdim etmək;
- şəbəkəni mühafizə vasitələri ilə mərkəzləşdirilmiş etibarlı idarəetməni təmin etmək.

ISTF tövsiyələrinə əsasən, məlumat təhlükəsizliyi sisteminin inkişafında ilk və ən mühüm mərhələ ictimai şəbəkələrə giriş və idarəetmə mexanizmləri tərəfindən tətbiq olunan təhlükəsiz rabitə prosedurları və mühafizə olunan virtual VPN şəbəkələrinin məhsullarıdır, bütün açarlar üçün inteqrasiya və idarəetmə vasitələri ilə müşayiət olunan və mərkəzləşdirilmiş şəkildə idarə olunan bir məlumat sistemidir.

Təhlükəsizlik tədbirləri, həmçinin kriptoqrafik məlumatların qorunması vasitələri və rəqəmsal imzaya əsasən yerinə yetirilir. Elektron iş üçün təhlükəsizlik sisteminin əsas funksional komponentlərini həyata keçirmək məqsədilə məlumatların qorunması üçün müxtəlif üsul və vasitələrdən istifadə olunur:

- ✓ Etibarlı rabitə protokolları;
- ✓ kriptoqrafiya vasitələri;
- ✓ autentifikasiya və avtorizasiya mexanizmləri;
- ✓ şəbəkənin iş stansiyalarına və ictimai şəbəkələrdən daxil olmağa nəzarət vasitələri;

- ✓ virus əleyhinə sistemlər;
- ✓ hücumların aşkarlanması və yoxlanılması üçün proqramlar;
- ✓ istifadəçi girişi nəzarətinin mərkəzləşdirilmiş idarə edilməsi üçün vasitələr, habelə məlumat paketləri və hər hansı bir tətbiqin mesajlarının təhlükəsiz mübadiləsi.
- ✓ açıq IP-şəbəkələri.

Korporativ sistemin bütün səviyyələrində bir sıra müdafiə vasitələrindən istifadə, məlumat təhlükəsizliyini təmin etmək üçün effektiv və etibarlı bir sistem qurmağa imkan verir.

Çox vaxt özünü İT mütəxəssisi kimi təqdim edən insanlar: "Biz şirkətimizdə informasiya təhlükəsizliyi problemlərini artıq həll etdik - təhlükəsizlik divarı quraşdırdıq və antivirusdan qorunma üçün lisenziya aldıq. İnanırıq ki, bu kifayətdir" deyirlər. Belə bir yanaşma problemin mövcudluğunun onsuz da tanındığını göstərir, lakin onu həll etmək üçün zəruri təxirəsalınmaz tədbirlərin miqyası və mürəkkəbliyi dəyərləndirilmir. Rəhbərliyin və mütəxəssislərin işlərini necə təmin etmələri və maliyyə itkilərinin qarşısını almaq barədə ciddi düşündükləri şirkətlərdə lokal tədbirlər və ya köklü "əl altında olan" vasitələrlə artıq edilə bilməyəcəyi qəbul edilir, bunu üçün sistemli birləşmiş yanaşma tətbiq etmək lazımdır.

Beləliklə, mühafizə bütün informasiya sisteminin əsas, funksional vəzifələrinin səmərəli həllinin hərtərəfli təmin edilməsinə yönəldilməlidir. Metodik olaraq bu problemlərin həlli mürəkkəb, kifayət qədər avtonom bir proqram və aparat sisteminin dizaynı və ətrafdakı İS –nin funksional vəzifələri ilə qarşılıqlı əlaqədə aparılmalıdır. Bu vəziyyətdə, İS-nin funksional komponentlərini zəruri mühafizə dərəcəsinə görə müəyyənləşdirmək və sıralamaq, müxtəlif xarici və daxili təhlükəsizlik təhdidlərinin şiddətini qiymətləndirmək, təhdid növlərinə və tələb olunan qorunmaya adekvat olan metodlar, alətlər və tənzimləyici sənədlər ayırmaq və müxtəlif növ zəruri mənbələri qiymətləndirmək lazımdır. Proqramın mühafizə sistemi layihəsinin planlaşdırılması və inteqrasiya edilmiş inkişafı bütün İS-nin sonrakı həyat dövrünün yüksək keyfiyyətini təmin etməlidir.

Şəbəkə təhlükəsizliyi ilə məşğul olan bir sıra aparıcı xarici təşkilatlar yalnız mövcud zəiflikləri və hücumları tanımağa deyil, dəyişdirilmiş köhnə və ya yeni zəiflikləri də müəyyən etməyə imkan verən yanaşmalar hazırlamışlar. Xüsusilə, ISS (Internet Security Systems) şirkəti bu yanaşmaları inkişaf etdirərək Adaptive Şəbəkə Təhlükəsizliyi Modelini (Adaptive Network Security) hazırlamışdır. Bu yanaşmalar informasiya təhlükəsizliyi vasitələri bazarında məşhur bəzi digər şirkətlər tərəfindən də inkişaf etdirilir.

Təhlükəsizliyə adaptiv yanaşma düzgün layihələndirilmiş və yaxşı idarə olunan proses və vasitələrdən istifadə edərək real vaxt rejimində izləmə, aşkarlama və təhlükəsizlik risklərinə cavab vermək imkanı verir.

Adaptiv şəbəkə təhlükəsizliyi üç əsas elementdən ibarətdir:

- Təhlükəsizliyin qiymətləndirilməsi texnologiyaları (security assessment);
- hücumların aşkarlanması texnologiyası ((intrusion detection);
- risklərin idarə edilməsi texnologiyaları (risk management).

Adaptiv şəbəkə təhlükəsizlik modelindən istifadə praktiki olaraq bütün təhdidləri idarə etməyə imkan verir və eyni zamanda onlara yalnız səmərəli şəkildə vaxtında cavab vermir, eyni zamanda zəifliklərə səbəb olan şərtləri təhlil edir. zəiflikləri aradan qaldırmağa imkan vermir. Adaptiv şəbəkə təhlükəsizliyi modeli onlayn zorakılığı azaltmaq, istifadəçilərin, idarə edənlərin və şirkət rəhbərliyinin şəbəkə təhlükəsizliyi hadisələri haqqında məlumatlılığını artırmağa imkan verir.

Adaptiv təhlükəsizlik modeli istifadə edilmiş təhlükəsizlik mexanizmlərindən imtina edir (girişə nəzarət, identifikasiya və s.). O, yeni texnologiyaların hesabına fəaliyyət imkanlarını genişləndirir.

Sonda bir daha qeyd etmək lazımdır ki, bazarın dinamik inkişafı və onun infrastrukturunun mürəkkəbliyi şəraitində informasiya ənənəvi maddi və enerji mənbələri ilə eyni strateji mənbəyə çevrilir. Məlumatların tapılmasına, yaradılmasına, saxlanmasına, işlənməsinə və məlumat verilməsinin effektiv yollarını təmin etməyə imkan verən müasir texnologiyalar rəqabət qabiliyyətliliyinin vacib amilinə və ictimai həyatın bütün sahələrini idarəetmə səmərəliliyinin

artırılması vasitəsinə çevrilmişdir. Məlumatlandırma səviyyəsi bu gün istənilən müəssisənin uğurlu inkişafında əsas amillərdən biridir. Bu baxımdan XXI əsrin ilk illərinin əvvəllərindən cari dövrə kimi məxfi və rəsmi dövlət və korporativ məlumatlarının qorunması, İS və kompüter şəbəkələrinin təhlükəsizliyinin təmini məsələsi son dərəcə aktuallaşmışdır.

NƏTİCƏ VƏ TƏKLİFLƏR

Yeni İT xalq təsərrüfatının bütün sahələrində fəal şəkildə tətbiq olunur. Lokal və qlobal informasiya şəbəkələrinin meydana gəlməsi kompüter istifadəçilərinə sürətli məlumat mübadiləsi üçün yeni imkanlar qazandırır. İnternetin inkişafı ilə yanaşı informasiya şəbəkələrinin geniş vüsət tapması hər kəsin gündəlik həyatının bir parçasına çevrilmiş və hər bir istifadəçinin bundan maksimum dərəcədə yararlanmasına səbəb olmuşdur. İnformasiya emalı proseslərinin avtomatlaşdırılması vasitələri, metodları və formaları inkişaf etdikcə və mürəkkəbləşdikcə cəmiyyətin istifadə olunan İT-nin təhlükəsizlik dərəcəsindən asılılığı artır. İnformasiyanın mühafizəsi və informasiya təhlükəsizliyinin əsas anlayışları, informasiyanın işlənməsi, ötürülməsi və toplanmasının müasir üsulları itkisi, təhrifi və açıqlanması ehtimalı ilə əlaqəli təhdidlərin yaranmasına şərait yaranır. Buna görə kompüter sistemləri və şəbəkələrinin informasiya təhlükəsizliyinin təmin edilməsi İT inkişafının aparıcı sahələrindən biridir.

Kompüter şəbəkələrinin təhlükəsizliyin təmini məsələsi KİS-nin təşkilinə qoyulan investisiyaların qorunması şərti daxilində ənənəvi olaraq İTS-nin qurulması ilə həll edilir. Başqa sözlə, İTS KİS-nin mövcud tətbiqləri üçün tamamilə şəffaf şəkildə işləməli və istifadə olunan şəbəkə texnologiyalarına tam uyğun olmalıdır. Yaradılmış İTS yeni texnologiyalar və xidmətləri nəzərə almalı, habelə bu gün KİS-nin hər hansı bir elementi üçün açıq standartların tətbiqi, inteqral həllərin istifadəsi və miqyaslılıq kimi ümumi tələblərə cavab verməlidir. Açıq standartlara keçid informasiya təhlükəsizliyi vasitələrinin əsas inkişaf tendensiyalarıdır. IPSec və PKI kimi standartlar müəssisələrin xarici əlaqələrinin təhlükəsizliyini, tərəfdaş müəssisələrin və ya uzaq müştərilərin müvafiq məhsullarla uyğunluğunu təmin edir.

KİS böyüdükcə və inkişaf etdikcə informasiya təhlükəsizliyi sisteminin bütövlüyə və idarəetməyə xələl gəlmədən asanlıqla genişlənməyə imkanı olmalıdır. Mühafizə vasitələrinin miqyaslılığı mühafizə sisteminin tədricən artması yolu ilə dəyərlilik və etibarlılıq üzrə optimal qərar qəbul etməyə imkan verir. Miqyaslılıq

çoxsaylı filialları, onlarla tərəfdaş müəssisələri, yüzlərlə məsafədən çalışan işçiləri və milyonlarla potensial müştərisi olduğu halda müəssisənin səmərəli fəaliyyətini təmin edir.

KİS mənbələrinin etibarlı qorunmasını təmin etmək üçün ən mütərəqqi və perspektivli informasiya təhlükəsizliyi texnologiyaları İTS-də tətbiq edilməlidir. Bunlara aşağıdakılar daxildir:

- Məlumatların məxfiliyini, bütövlüyünü və həqiqiliyini təmin etmək üçün məlumatların kriptoqrafik qorunması;
- istifadəçilər və şəbəkə obyektlərinin düzgünlüyünün identifikasiya üçün və autentifikasiya texnologiyaları;
- korporativ şəbəkəni qorumaq üçün firewall texnologiyası;
- açıq rabitə kanalları vasitəsilə ötürülən məlumatları qorumanması üçün virtual təhlükəsiz kanalları və VPN texnologiyaları;
- tokenlərin (smart kartların, touch-yaddaşın, USB-portların açarlarının və s.) və digər təsdiqləmə vasitələrinin tətbiqi ilə istifadəçinin zəmanətli identifikasiyası;
- istifadəçi səviyyəsində girişin idarə olunması və məlumata icazəsiz daxil olmadan mühafizə;
- PKI açıq açar idarəetmə infrastrukturunun dəstəklənməsi;
- informasiya resurslarının mühafizəsinin fəal araşdırılması üçün müdaxilələrin aşkarlanması texnologiyaları;
- antivirus profilaktikası və mühafizənin ixtisaslaşdırılmış komplekslərindən istifadə edərək virusdan qorunma texnologiyaları;
- müəssisənin vahid təhlükəsizlik siyasəti əsasında KİS-nin mərkəzləşdirilmiş idarə edilməsi;
- informasiya təhlükəsizliyini təmin etmək üçün məlumatların qorunması vasitələrinin rasional birləşməsini təmin edən inteqrasiya olunmuş yanaşma.

İnformasiya təhlükəsizliyi sistemini müasir tələblərə uyğunlaşdırmaq üçün təşkilatlar mövcud həlləri təhlükəsizlik təhlilinə, hücumların aşkarlanması və risklərin idarə edilməsinə cavab verən komponentlərə əlavə etməlidirlər.

Şirkətin informasiya sistemləri, əsasən, müxtəlif istehsalçıların proqram və aparat məhsullarının əsasında qurulur. Elə bir şirkət hələ yoxdur ki, müasir İS-nin qurulması üçün bütün vasitələrin toplusunu təqdim etmiş olsun. Ona görə də müxtəlif cinsli İS - nin etiabarlı mühafizəsini təmin etmək üçün onun hər bir komponentinin təhlükəsizliyinə cavab verən yüksək kvalifikasiyalı mütəxəssislər olmalıdır. İS müxtəlif cinsli olduğundan onun təhlükəsizliyini təmin etmək də mürəkkəbdir. Eyni zamanda şəbəkələrarası ekranların, şlüzlərin və VPN – in bir arada olması çox vaxt uyuşqanlığı olmayan mürəkkəb bir mühafizə mühitinin yaranmasına səbəb olur. Bu nöqteyi-nəzərdən mühafizə vasitələri istehsalçılarının vahid standartlara uyğun məhsullarının hazırlanması və təqdim olunması bu məsələnin həllini sürətləndirir.

Təşkilatlarda çox vaxt belə bir faktdan yayınırlar: inzibatçılar və istifadəçilər müntəzəm şəkildə İS-nin konfiqurasiyasını dəyişirlər. Bu dəyişikliklər nəticəsində ƏS və onun əlavələri ilə bağlı zəif nöqtələr meydana çıxa bilir. Ayrıca təhlükəsizlik üzrə inzibatçılar yalnız anladıqları təhlükəsizlik risklərinə cavab verməyə meyllidirlər, faktiki olaraq bu cür risklər əhəmiyyətli dərəcədə çox ola bilər. Bundan əlavə, informasiya və şəbəkə texnologiyaları çox sürətlə inkişaf edir, mütəmadi olaraq yeni proqram təminatları meydana gəlir. Şəbəkə texnologiyalarının fasiləsiz inkişafı onların daimi təhlilinin olmaması və mühafizənin təmini üçün ehtiyatların çatışmazlığı ona gətirib çıxarır ki, zaman keçdikcə KİS-nin mühafizəsi aşağı səviyyəyə enir, sistemin zəifləməsinə və dəqiqləşdirilməmiş təhdidlərə səbəb olur. Əksər hallarda mühafizə ilə bağlı problemləri həll etmək üçün təşkilatlarda xüsusi yanaşmalardan istifadə edirlər. Bu yanaşmalar, adətən, mövcud mənbələrin cari səviyyəsinə əsasən müəyyən edilir.

İSTİFADƏ EDİLMİŞ ƏDƏDBİYYATIN SİYAHISI

1. Qasımov V.Ə. İnformasiya təhlükəsizliyinin əsasları. Dərslik. Bakı: MTN Maddi-texniki Təminat Baş İdarəsinin Nəşriyyatı, Poliqrafiya Mərkəzi. 2009, 340 səh.
2. Quliyev R.A., Əliyeva T.Ə., Rzayeva Ü.Ş., Xəlilova C.M. Korporativ informasiya sistemləri. Dərs vəsaiti. Bakı: "İqtisadUniversiteti" Nəşriyyatı - 2016 - 226 səh.
3. Əlizadə Mətləb Nuruş oğlu, Bayramov Hafiz Məhərrəm oğlu, Məmmədov Əlövsət Suliddin oğlu. İnformasiya təhlükəsizliyi. Dərslik, Bakı, "İqtisad Universiteti" nəşriyyatı, 2016, 384 səh.
4. INFORMATION SECURITY POLICY. UNIVERSITY OF EDINBURGH, OCTOBER 31, 2017.
5. Баранов А.А., Брыжко В.М., Базанок Ю.К. Права человека и защита персональных данных. К.: Госкомсвязи Украины, 2000, 280 с.
6. В.И.Литвиненко, Евгений Козлов. Основы информационной безопасности. Учебное пособие, КноРус: 2020, 200 с.
7. Галицкий А. В., Рябко С.Д., Шаньгин В. Ф. Защита информации в сети — анализ технологий и синтез решений М.: ДМК Пресс, 2004.
8. Гудков Ю.И., Шепитько Г.Е., Прокофьев М. SWOT-анализ с позиций информационной безопасности. Под редакцией: О. Макаров М.: МФЮА, 2014, с. 176-180.
9. Иванов П. IPSec: защита сетевого уровня // Сети. 2000. No 2.
10. Липаев В.В., Филинов Е.Н. Мобильность программ и данных в открытых информационных системах 1997.
11. Петренко С. А. Реорганизация корпоративных систем безопасности // Конфидент. 2002. No 2.
12. Симонов С. В. Методология анализа рисков в информационных системах // Конфидент. 2001. No 1.

13. Шаньгин D. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. — М.: ИД «ФОРУМ»: ИНФРА-М, 2011. — 416 с.: ил. — (Профессиональное образование).

İnternet resursları

14. АО «Лаборатория Касперского»: официальный сайт. [Электронный ресурс]. Режим доступа: https://securelist.ru/statistics/ (дата обращения: 30.08.2019)
15. https://az.wikipedia.org/wiki/%C4%B0ntranet
16. Barsukov, V. http://www.jetinfo.ru
17. Беляев А. В. Методы и средства защиты информации, http:// www.citforum.ru/internet/infsecure/its2000_01.shtml
18. http://www.extrim.ru/instruments_vpn.asp.
19. Скородумов Б.И. Стандарты для безопасности электронной коммерции в сети Интернет, http://www.stcarb.comcor.ru
20. http://ks-211.blogspot.com/2015/06/informasiya-thluksizliyi.html

РЕЗЮМЕ

Применение комплексных мер безопасности на всех уровнях компьютерных сетей требует создания надежной и эффективной системы защиты информации. Предлагаемая магистрская диссертационная работа посвящена именно изучению проблем создания надежной и безопасной системы защиты компьютерных сетей.

Первая глава магистерской диссертации содержит информацию об основных понятиях информационной безопасности и криптографических методах, трудностях, возникающих при эксплуатации защищенных систем, о подходах к безопасности компьютерных систем и политике безопасности, а также проблемах и рисках информационной безопасности.

Вторая глава диссертации посвящена принципам построения открытых систем в соответствии с концептуальными требованиями архитектуры для обеспечения безопасной и надежной работы компьютерных сетей, модели анализа безопасности информационных систем, преимуществам и отличиям подходов и стандартов безопасности, критериям соответствия и стандартам ISO 270, которые были изучены эволюционные направления этого семейства.

В третьей главе диссертации рассматриваются существующие проблемы в системе безопасности компьютерных сетей, преимущества и недостатки методов, используемых для работы механизмов безопасности, а также интегрированные решения безопасности, биометрические системы безопасности, используемые в сетях, наряду с международными стандартами, используемыми в виртуальных частных сетях и изучены их возможности. Изучены особенности адаптивного подхода, применяемого для обеспечения надежной системы безопасности компьютерных сетей и обоснована возможность его использования с целью повышения надежности и эффективности работ сетей.

SUMMARY

The use of comprehensive security measures at all levels of computer networks requires the creation of a reliable and effective information protection system. The proposed master's thesis is devoted specifically to the study of the problems of creating a reliable safe system for protecting computer networks.

The first chapter of the master's thesis contains information on the basic concepts of information security and cryptographic methods, difficulties encountered during the operation of protected systems, approaches to the security of computer systems and security policies, as well as problems and risks of information security.

The second chapter of the dissertation is devoted to the principles of building open systems in accordance with the conceptual requirements of architecture to ensure the safe and reliable operation of computer networks, a model for analyzing the security of information systems, the advantages and differences of security approaches and standards, compliance criteria and ISO 270 standards that have been studied the evolutionary directions of this family.

The third chapter of the dissertation discusses the existing problems in the security system of computer networks, the advantages and disadvantages of the methods used to operate security mechanisms, as well as integrated security solutions, biometric security systems used in networks, along with international standards used in virtual private networks and are studied their capabilities. The features of the adaptive approach used to ensure a reliable security system for computer networks are studied and the possibility of its use with the aim of increasing the reliability and efficiency of network operations is substantiated.