Azərbaycan Respublikası Təhsil Nazirliyi
Azərbaycan Dövlət İqtisad Universiteti

MAGİSTRATURA MƏRKƏZİ

Əl yazması hüququnda

Dadaşova İntizar Rasim qızı

" **Komputer şəbəkələrində informasiyanın qorunması məsələləri "** mövzusunda

MAGİSTR DİSSERTASİYASI

İxtisasın şifri və adı: **060509 "Kompüter Elmləri"**

İxtisaslaşma : **"İqtisadi informasiya sistemləri"**

Elmi rəhbər: **dos.H.M. Bayramov**

Magistr proqramının rəhbəri: **dos. Bayramov H.M.**

Kafedra müdiri: **t.e.n,dos. Bayramov H.M.**

Bakı 2016

M Ü N D Ə R İ C A T

G i r i ş

Hal-hazırda kompüterləşmə insan fəaliyyətinin bütün sferalarını əhatə etmişdir. Həm iqtisadi, həm elmi-texniki, həm də sosial problemlərin həlli qərarları informasiyanın nə dərəcədə məqsədəuyğun emalından asılı olmuşdur. İnformasiya sistemləri müxtəlif elmi araşdırmalara, iqtisadi tədqiqatlara, maliyyə-bank sistemlərinə və inzibati idarəetmə sisitemlərinə tətəbiq edilərək dünya iqtisadiyyatının inteqrasiyasında böyük nailiyyətlər əldə edilmişdir. Dünya iqtisadiyyatının və müasir insan cəmiyyətinin əldə etdiyi ən böyük və son nəaliyyətləri ona görə böyük müqayisəlidir ki, artıq idarəetmənin əlində ayrı-ayrı lokal sistemlərinin deyil, dünyanı əhatə etmiş paylanmış informasiya sistemlərinin məhsulları vardır. Paylanmış informasiya emalı sistemləri dedikdə, bir-birindən coğrafi uzaq məsafələrdə dayanan məlumatlarla qarşılıqlı qidalanan və məlumat üçün ötürülməsi, axtarışı məsələlərini həll edən kompüter şəbəkələri başa düşülür.

Mövzunun aktuallığı. Müasir komputer şəbəkələri (KŞ) cəmiyyətin və qlobal iqtisadiyyatın idarəedilməsində özünəməxsus qeyri-adi funksiyaları olduqundan belə sistemlərin etibarlılıqı, səmərəliliyi çox aktual məsəslədir. Bu sistemlərdə hər hansı pozuntu faktorları: texniki qurğuların sıradan çıxması, xidməti heyətin düzgün olmayan hərəkəti, ətraf şəraitin dəyişməsi və s. təsir edir. Ona görə də çox təssüf olsun ki, komputer şəbəkələrinin tam sıradan çıxmadan fəaliyyətinə həmişə nail olmaq mümkün deyildir. Bununla əlaqədar olaraq sıradan çıxmayan, davamlı fəaliyyət göstərən KŞ-in yaradılması çox aktual məsələdir. KŞ-nin sıradan çıxmadan işləməsini təmin edən çoxlu üsullar mövcuddur. İnformasiya sistemlərinin tamlığını qoruyan etibarlı mexanizmlərin işlənib hazırlanması müasir dövrün informatika elminin ən aktual məsələlərindən biri olmuşdur. Hal-hazırda poseslərin paralelliyindən informasiya sistemlərinin sıradan çıxma-bərpa mexanizminin reallaşmasına vahid yanaşmalar mövcud deyildir. Bütün bu deyilənlərlə əlaqədar komputer şəbəkələrinin etibarlılığının öyrənilməsini, bu istiqamətin daha dərindən tədqiqatına böyük ehtiyac duyulmaqdadır.

Mövzunun öyrənilmə vəziyyəti. KŞ-nin etibarlığı məsələləri 90-cı illərdən, yəni bu sistemlər yaradıldıqdan sonra elmi-tədqiqat obyektinə çevrilmişdir. Lakin məsələnin öyrənilmə yeniliyinə baxmayaraq dünya alimlərinin və Azərbaycan kibernetiklərinin diqqətindən yayınmamışdır. Bu sahədə elmi araşdırmaları ilə elm aləminə daxil olan akademik Ə.M.Abbasov, akademik T.Əliyev, müxbir üzv R.Ə.Əliyev, prof. Ə.Ə.Əliyev , Dos.E.H.Hüseynov və digər alimlərimizi qeyd etmək mənəvi borcumuzdur. Həmçinin gənc alimlər V.Qasımov, Ə.Əliyev, N.İmanova və bir çox başqalarının elmi araşdırmaları KŞ-nin etibarlığı məsələlərinə həsr edilmişdir.

Tədqiqatın məqsədi: KŞ-in etibarlığı, informasiya sistemlərində verilənlərin qorunması, texniki vasitələrin sıradan çıxmadan işləmə göstəricilərinə dair elimi işləri öyrənmək, ümumiləşdirərək praktiki əhəmiyyəti olan təkliflər verməkdir. Həmçinin informasiya sistemlərinin uzunmüddətli fəaliyyətini təmin edə biləcək məsələləri bir araya gətirərək təlimat hazırlamaq tədqiqatın məqsədinə daxildir.

İnternet şəbəkəsində işləyərkən praktikada rast gəlinən çatışmamazlıqların bu və ya digər dərəcədə qarşısının alınması yollarını axtarıb aramaq da məqsədlərimizdən biri olmuşdur.

Tədqiqatın obyekti kimi informasiya sistemlərinin səmərəlilik və etibarlılıq göstəriciləri götürülmüşdür. Klassik göstəricilərlə yanaşı KŞ-də informasiyanın qorunması, proqram vasitələrinin keyfiyyət göstəriciləri də tədqiqat obyekti kimi araşdırılmışdır.

Dissertasiya işinin tədqiqat metodu birbaşa rizayi hesablama üsulları, differensial tənliklər sisteminin həll üsulları və KŞ-in etibarlıq və səmərəlilik göstəricilərinin təhlili olmuşdur. Nəzəri biliklərin praktikada yoxlanılması və alınmış nəticələrin təhlili vasitəsilə müəyyən elmi fikrə gəlmək işin üsullarından biridir.

Tədqiqatın mənbələri. Etibarlılıq və səmərəlilik nəzəriyyələri, KŞ-in etibarlılığı və sıradan çıxmadan işləməsi haqqında elmi tədqiqat işləri və müəllifin İnternet sistemində işləyərkən praktiki əldə etdiyi informasiya dissertasiya işinin mənbəsi rolunu oynamışdır.

Tədqiqatın elmi yeniliyi və praktiki əhəmiyyəti onunla bağlıdır ki, etibarlılıq nəzəriyyəsi öyrənilmiş, etibarlılıq göstəricilərinin qiymətindən asılı olaraq informasiya sistemlərinin səmərəlilik mənbələri müəyyən edilmişdir. Həmçinin, Markov sxeminin modelinin parametrləri: sıradan çıxma tezliyi - $\lambda(t)$, bərpa tezliyi $\mu(t)$ zamandan asılı olan halda həll variantlarının müəyyən edilməsinə cəhd edilmişdir.

Digər tərəfdən KŞ-in texniki vasitələrinin sıradan çıxma-bərpa mexanizminə aid olan «domino effekti»nə qarşı mübarizə sxemlərinin əlavə imkanları müəyyən edilmiş, bu sistemlərdə informasiyanın qorunması üçün səmərəli təkliflər verilmişdir.

Dissertasiya işi giriş, üç fəsil, nəticə və təkliflərdən ibarət olub, məzmunu 78 səhifədə verilmişdir. Dissertasiya işi istifadə olunan elmi ədəbiyyatların və veb saytların siyahısı ilə tamamlanmışdır.

Fəsil 1. Komputer sistemlərinin etibarlılıq və səmərəlilik problemləri

1.1. Etibarlıq nəzəriyyəsinin əsas anlayışları

İnformasiyanın işlənməsi sistemlərinin texniki və proqram təminatlarının dayanıqlılığının öyrənilməsi zəruriliyi həyati praktika ilə sübut edilmişdir. Texniki sistemlərin etibarlılığı sahəsində böyük sayda işlər görülmüşdür. Mürəkkəb sistemlərin etibarlığını təmin edən çoxlu sayda üsullar işlənib hazırlanmışdır. Bu modellər nəinki texniki vasitələrin hazırlılığını, etibarlılıq göstəricilərini qiymətləndirir, hətta qazanılmış təgrübə nəticəsində etibarlılıq göstəricilərinin qiymətlərini əvvəlcədən deyə də bilirlər. Bundan əlavə bəzi modellər normal işləmə şəraitindən əyinmələr zamanı iş rejimini necə qurmağı təklif edirlər. Sistemin təmiri, normal vəziyyətə gətirilməsi yolunu öyrədirlər.

Komputer şəbəbkələrinin proqram təminatının və texniki vasitələrin etibarlığının miqdari qiymətləndirilməsi böyük əhəmiyyət kəsb edir. Bu əhəmiyyə çox vacib olur, o vaxt ki, real zaman rejimində işləyən böyük proqram təminatı bloklarının qiymətləndirilməsi zəruri olur.

Beləliklə, etibarlılıq nəzəriyyəsi dedikdə bir-biri ilə müəyyən alqoritmlər vasitəsi ilə qarşılıqlı bağlı olan sistemlər və elementlərdən ibarət mürəkkəb sistemlərin möhkəmliliyi nəzəriyyəsi başa düşülməlidir. Etibarlılıq nəzəriyyəsi də bu sistemləri onların altsistemləri və elementlər vasitəsilə tədqiq edir və öyrənir.

Sistemlərdə etibarlılıq o vaxt olur ki, onlar qarşıya qoyulmuş məsələni həll etmiş olsunlar. Əks halda, yəni qarşıya qoyulan məsələ həll edilə bilinməyəndə deyirlər ki, sistem etibarsızdır, möhkəm deyil.

Proqram təminatı (PT) sistemlərində rəddetmə dedikdə proqramda buraxılmış səhv başa düşülür. Bu səhvin düzəldilməsi prosesi isə sistemin sistemin təmiri prosesi kimi başa düşülür. PT-da səhv dedikdə proqram işləyərkən bütün arzu olunmayan nəticələrə gətirib çıxaran vəziyyətlər küllüsünü başa düşəcəyik

(məsələn, başqa fayla müraciət, informasiyanın yaddaşın tutulmayan hissəsində saxlanılması və s.)

PT-nın etibarlılığı onun keyfiyyətində asılıdır. Pt-nın keyfiyyətliliyi dedikdə isə onun şarşıya qoyulmuş funksional məsələnin etibarcasına yerinə yetirmək bacarığı nəzərdə tutulur.

Pt-nın keyfiyyəti bu göstəricilərlə ölçülə bilər: vahid zamandakı səhvlərin sayı; səhvlər arası vaxt; hər əmrə düşən səhvlərin sayı; səhvlərin son məqsədə təsiri.

Bilirik ki, müasir kompüterlər inkişaf etmiş mürəkkəb PT-na malikdirlər.

Hesablama sistemlərinin etibarlılığı özündə iki ayrılmaz aspektə malikdir: element etibarlılığı; funksional etibarlılıq.

Bunlardan birincisi texniki təminata aiddir və ənənəvi möhkəmlilik nəzəriyyəsi ilə öyrənilir.

Funksional etibarlılıq isə PT sisteminin işlənməsinin səhvsizliyini, düzlüyünü göstərir. Bu anlayışların təbiətindəki fərq ondan ibarətdir ki, texniki təminat möhkəmliliyini öyrənən metod və üsullar PT-nın möhkəmliyində hər zaman istifadə oluna bilmir.

Bəs sistemin funksional möhkəmliyi nədir? Bunun üçün sistemin quruluşu anlayışını başa düşmək lazımdır.

Quruluş – sistemin quruluşu dedikdə hər şeydən əlavə PT sisteminin modullara və bu modullar arasındakı əlaqələrə bölünməsi nəzərdə tutulur. Modul dedikdə, bir və ya bir neçə proqramçı üçün iş vahidi nəzərdə tutulur.

Spesifik modulların yığım sistemin quruluşunu əmələ gətirir.

Əgər sistemdən lazım olan xidmətin alınma ehtimalı böyükdürsə, onda belə sistemə çox dayanıqlı sistem deyilir. Əgər xüsusi hallarda sistem sıradan çıxma, xarab olma verirsə, ona etibarsız sistem deyilir.

Əgər, 1) proqramlaşdırma səhvi sistemin düzgün işlənməsinə mane olmursa, (məsələn, çıxış zamanı tekstdə səhv)

2) səhvin təsiri olan hallar gec-gec baş verirsə, və bu halların baş vermə ehtimalı kiçikdirsə, yenə sistemə dayanıqlı sistem demək olar. Lakin səhvsmiz sistem möhkəm olmaya bilər.

Modullar qurularkən «hər şey qaydasındadır» prinsipi PT sisteminin dayanıqlılığını aşağı salır. Aşağıdakı hallarda bu baş verə bilir:

- PT sisteminin quruluşu ətraf mühitin korrekt olmasına arxayınlaşır;
- Sistem quruluşu PT-da səhvin olmadığına əsaslanır;
- Sistemin quruluşu «hər şey və ya heç nə»prinsipinçə əsaslanır.

Sistem quruluşunun təsviri modullar arası interfeyslərin spesifikləşdirilməsi deməkdir.

Dayanıqlı PT-nı almağın bir-birini tamamlayan iki müxtəlif istiqaməti vardır.

Birinci halda etibarsız anlayışı «səhvi olan» mənasında başa düşülür və səhvin tapılmasını təmin edən korrekt proqramların yazılması nəzərdə tutulur.

İkinci halda ona əsaslanır ki, hesablma sistemləri üçün dayanıqlı və «korrekt» anlayışları sinonim deyillər, yəni eyni deyillər. Bu ona gətirib çıxarır ki, layihələşdirmə prosesində möhkəmliyi artıran, lakin korrektliyə təsir etməyən tədbirlər həyata keçirilir.

Dayanıqlılıq göstəriciləri dedikdə, biz sistemin qarşıya qoyduğuq məsələlərin yerinə yetirmək bacarığının dərəcəsini göstərən kəmiyyət və keyfiyyət göstəricilərini nəzərdə tutacağıq.

Sistemin möhkəmliliyinin üç cür göstəriciləri vardır: keyfiyyət göstəriciləri; ardıcıllıq göstəriciləri; kəmiyyət göstəriciləri.

Keyfiyyət göstəriciləri ədədlərlə ifadə oluna bilmir və müxtəlif sistemlərin bir-biri ilə müqayisəsində və onların üstünlüyü və ya qeyri üstünlüyü haqqında heç bir informasiya vermirlər. Dayanıqlılığın keyfiyyət göstəriciləri baxılan sistemin qarşıya qoyulan məsələnin həlli üçün zəruri lazım olan keyfiyyətlərdir. Keyfiyyət

göstəriciləri imkan verir ki, sistemləri fərqləndirək, lakin qoyulan məsələnin həlli dərəcəsi hansı sistemin daha yaxşılığını göstərə bilmirlər.

Ardıcıllıq göstəriciləri sistemin hər hansı bir variantına üstünlük verməyi əsaslandıran informasiyanı özündə saxlayırlar. Ardıcıllıq göstəriciləri imkan verirlər ki, sistemin variantlarını onların möhkəmliliyinin artan sırası ilə düzək. Lakin bu sırada variantların bir-birindən nə nədər etibarlı olduğunu demək mümkün olmur.

Dayanıqlığın miqdari (kəmiyyət) göstəriciləri sistemlərin etibarlı, digərinə nisbətən möhkəmliyi qədəri haqqında informasiyaya malikdirlər. Kəmiyyət göstəriciləri etibarlılığı ədədlərlə göstərirlər.

Dayanıqlıq göstəriciləri mütləq və ya nisbi ölçü vasitələri ilə ölçülürlər, qiymətləndirilirlər. Sistemin tətbiqi və ya sınağı zamanı kəmiyyət göstəriciləri statistik müşahidələr yolu ilə müəyyən olunurlar. Onlar dayanıqlığı etibarlılığın əsas göstəriciləridir və sistemin işə yararlığı haqqında qiymətli informasiyanı özündə saxlayırlar.

Etibarlılıq göstəriciləri aşağıdakı kimi seçilə bilərlər.

Sistemin elementinin sınağı zamanı birinci sıradan çıxmaya qədərki vaxt müəyyən müsbət ədəddir. Elementin xidməti vaxtı – t_i – onun etibarlılığını xarakterizə edir. Rədd etmələrin və ya sıradan çıxmanın səbəbini araşdırarkən görərik ki, t_i–lər müəyyən bir təsadüfi T kəmiyyətinin – dayanıqlı statistik paylanmaya malik kəmiyyətin alınmasına gətirib çıxarır.

Müəyyən paylanmanın statistik dayanıqlılığını

$$q(t) \approx F(t) \qquad (1),$$

təqribi bərabərliyi uyğun gəlir. Burada q(t)- müəyyən zaman daxilində elementin sıradan çıxma tezliyidir. F(t)- [0,t] - zamanında sıradan çıxmanın ehtimalıdır və T təsadüfi kəmiyyətin paylanma funksiyasıdır. Statistik müşahidələrin sayı artdıqca (1) –in doğruluğu artır.

F(t) – sıradan çıxmanın ehtimalıdırsa, onda səhvsiz, yəni sıradan çıxmadan ehtimalı

P(t) – 1- F(t)

R(t) və F(t) –ni hesablayarkən paylanmanın sıxlığı istifadə oluna bilər:

$f(t) = \frac{dF(t)}{dt} = -\frac{dP(t)}{dt}$,

buradan,

$F(t) = \int_0^t f(x)dx$

$P(t) = \int_t^\infty f(x)dx$

Sistemin etibarlılığının ümumi göstəricisi kimi, onun qarşısına qoyulmuş məsələnin vaxtında və istismar qaydalarına riayət edərək yerinə yetirmək ehtimalı qəbul olunur. Tutaq ki, τ_{pr} – sistemin tətbiqi, yəni işləmə vaxtıdır. PT-i sistemləri üçün $P(\tau_{pr})$ – etibarlılıq göstəricisi deyil, (çünki τ_{pr} – qeyri-müəyyən vaxtdır) sıradan çıxmadan sistemin iş vaxtı – T_0, sıradan çıxmalar arasındakı orta vaxt – T_s və sıradan çıxmaların intensivliyi - $\lambda(t)$ – kimi göstəricilərdən istifadə edilir.

$\lambda(t) = \frac{1}{P(t)} \cdot \frac{dF(t)}{dt}$;

$$P(t) = 1 - F(t) \Rightarrow \lambda(t) = \frac{1}{P(t)}(-\frac{dP(t)}{dt}) = -\frac{d}{dt}\ln P(t)$$

İnteqrallasaq,

$P(t) = e^{-\int_0^t \lambda(x)dx}$ (2)

Alınmış ifadə bütün paylanma qanunları üçün doğrudur və buna görə də o etibarlılığın əsas qanunudur.

Xarab olmadan işləmənin orta vaxtı aşağıdakı kimi müəyyən oluna bilər.

$$T_0 = \int_0^{\infty} t \cdot f(t)dt$$

İnteqrallasaq,

$$T_0 = \int_0^{\infty} P(t)dt \qquad (3).$$

Tutaq ki, sistem müəyyən t_1 zamanında sıradan çıxmamışdır və bu zaman onun orta $T_0(t_1)$ – kəmiyyətini hesablayaq. $T_0(t_1)$- i müəyyən etmək üçün sistemin $t_1 + \tau$ - zamanında xarab olmadan işləməsini qeyd edək. Onda ehtimalların hasili teoreminə görə

$$P(t_1 + \tau) = P(t_1) \cdot P(\tau(t_1)) \qquad (4),$$

burada, $P(t_1)$ - t_1 zamanında sistemi xarab olmamaq şərti ilə τ-da işləmə ehtimalıdır.

(4) - dən alırıq:

$$P(\tau(t_1)) = \frac{P(t_1 + \tau)}{P(t_1)}$$

Onda (3)-dən alırıq:

$$T_0(t_1) = \frac{1}{P(t_1)} \int_0^{\infty} P(t_1 + \tau)dt \qquad (5)$$

Etibarlılığın əsas qanununa əsasən,

$$P(t_1) = e^{-\int_0^{t_1} \lambda(t)dt} \quad \text{və} \quad P(t_1 + \tau) = e^{-\int_0^{t_1+\tau} \lambda(t)dt},$$

onda (5) ifadəsinə görə

$$T_0(t_1) = \frac{1}{e^{-\int_0^{t_1}\lambda(t)dt}} \cdot \int_0^{\infty} e^{-\int_0^{t_1+\tau}\lambda(t)dt} \quad (6)$$

$\lambda(t)$ sabit olarsa, yəni $\lambda(t) = const$, onda (6) ifadəsi aşağıdakı kimi olar:

$$T_0(t_1) = \int_0^{\infty} e^{-\lambda\tau}d\tau = \frac{1}{\lambda}.$$

Buradan belə çıxır ki, əgər sistem xarab olmasına qədərki vaxt eksponensial paylanma qanununa tabedirsə, sistemin sonrakı xarab olmadan işləmə vaxtı onun əvvəlcə nə qədər işləməyindən asılı deyil.

1.2. İnformasiya texnologiyalarının səmərəliliyinin qiymətləndirilməsi

Komputer şəbəkələrinin yaradılması və istifadəsinin əsas məqsədlərindən biri də iqtisadi səmərənin əldə edilməsindən ibarətdir.

Şəbəkədə iqtisadi səmərəni əldə etmək üçün aşağıdakı mənbələr vardır:

- idarəetmə funksiyalarının nizamlanma səviyyəsinin yüksəldilməsi;
- rəqiblərin və ətraf mühitin öyrənilməsi imkanlarının artırılması;
- alternativ qərarlar layihəsinin hazırlanması;
- idarəetmə operativliyinin artırılması;
- obyektin istehsal və ya xidmət gücünün artırılması;
- KŞ-də sıradançıxmaların azaldılması;
- istehsal obyektinin təchizatının və təminatının təşkilinin yaxşılaşdırılması.

KŞ-nin iqtisadi səmərəsinin kəmiyyətcə qiymətləndirilməsi onun yaradılmasının bütün mərhələlərində -texniki məsələdən sənaye istismarına kimi həyata keçirilir. Həm də sənaye istismarı zamanı səmərəlilik göstəriciləri statistik üsulla, eksperimental yolla müəyyən edildiyi halda, layihələşdirmə zamanı yalnız və yalnız hesablama yolu ilə müəyyən edilə bilərlər.

Qeyd edək ki, KŞ-nin iqtisadi səmərəsinin hesablanması texniki tapşırıq və ya texniki layihə hazırlanarkən daha vacibdir, nəinki sənaye istismarı zamanı, çünki layihələşdirmə zamanı sistemin yaradılmasının məqsədəuyğunluğu məsələsi, onun quruluşu, elementlərinin komplektləşdirilməsi və s. həll olunur. Məhz buna görə də, iqtisadi səmərənin hesablanması üsulları mühüm rol oynayırlar.

Məlum olan üsullar böyük çatışmamazlıqlara malikdirlər. Belə ki, bu üsullar KŞ-in etibarlılıq göstəricilərini nəzərə almadan səmərəliliyi hesablayırlar. Bu isə iqtisadi səmərəlilik göstəricilərinə mənfi təsir göstərir.

KŞ-nin layihələşdirilməsi zamanı etibarlılıq göstəricilərini nəzərə alaraq iqtisadi səmərəliliyin göstəricilərinin qiymətləndirilməsi məsələsindən başqa, bir məsələ də ortaya çıxır ki, bu da iqtisadi səmərənin maksimum prinsipinə əsasən KŞ-nin etibarlılığına qarşı qoyulan optimal tələblərin müəyyən edilməsidir.

KŞ-nin xalq təsərrüfatındakı vacib rolunu nəzərə alaraq bu iki məsələnin həlli üçün vahid metodikanın – üsulların işlənməsi zəruridir.

Bu metodika elə olmalıdır ki, hər cür quruluşlu və hər cür iqtisadi obyektlər üçün olan KŞ-də tətbiq edilə bilsin. Digər tərəfdən isə bu metodka dəqiq hesablama düsturlarına və təkliflərə malik olmalıdır ki, ondan etibarlıq nəzəriyyəsi sahəsində mütəxəssis olmayan mühəndis, iqtisadəçı və başqaları istifadə edə bilsinlər.

Müxtəlif KŞ-nin iqtisadi səmərəliliyini müqayisə etmək üçün mütləq kəmiyyət göstəricilərini hesablamaq lazımdır. Belə müqayisə adətən aşağıdakı kimi aparılır: müqayisə olunan sistemlərin iqtisadi səmərəliliyinin məhəlli göstəriciləri alınır; alınan göstəriciləri qarşılaşdırırlar və qərar çıxarırlar.

İki KŞ-lərinin müqayisəsinin başqa – ikinci yolu da vardır. Müqayisə olunan sistemlərin müəyyən iqtisadi göstəricilərini götürüb, bir sistemin o birinə nisbətən iqtisadi səmərəsini müəyyən edən ümumi göstəricini də hesablamalq olar. Belə göstəriciləri sistemlərarası göstəricilər adlandırırlar. Məsələn, bir sistemin digəri ilə əvəz edərkən illik iqtisadi səmərə belə göstəricdir.

Birinci yolla müqayisədə mütləq səmərəlilik göstəriciləri alınır. Çoxlu sayda müxtəlif iqtisadi səmərə göstəriciləri mövcuddur. Lakin bu göstəricilərin bir sırası 1969-cu ildə «Kapital qoyuluşunun iqtisadi səmərəsini müəyyən edən tipik metodika»da müəyyən olunmuşlar. Əgər onlara «Yeni texnikanın tətbiqindən alınan iqtisadi səmərənin müəyyən edilməsi metodikası»ndan bir neçə göstəriciləri əlavə etsək, KŞ-in iqtisadi göstəricilərinin tam və aydın çoxluğunu alacağıq.

Birinci müğləq göstərici: kapital qoyuluşunun iqtisadi səmərəliliy əmsalı:

$$E_{k.p.} = \frac{P}{K}, \qquad (2.1.),$$

burada, K – KŞ-nə kapital qoyuluşu,

P – illik xalis gəlir,

$$P = S - C \qquad (2.2.),$$

harada ki, S – illik buraxılan məhsulun dəyəri (topdapnsatış dəyəri), C – illik məhsulun maya dəyəri. Hər hansı bir obyektə KŞ-i tətbiq edilərkən, onun məhsulunun yeni dəyərivə yeni maya dəyəri əmələ gəlir. Əgər onları S_2 və C_2 ilə işarə etsək, onda iqtisadi səmərə əmsalı:

$$E_{k.p.} = \frac{\Delta P}{K} = \frac{P_2 - P_1}{K} = \frac{(S_2 - C_2) - (S_1 - C_1)}{K} = \frac{(S_2 - S_1) - (C_1 - C_2)}{K}, \qquad (2.3.)$$

burada, P_1 və P_2, S_1 və S_2 uyğun olaraq illik xalis gəlir, dəyər və maya dəyəridir. P_1, S_1, C_1 – KŞ-in tətbiqindən əvvəl, P_2, S_2, C_2 – KŞ-in tətbiqindən sonrakı qiymətlərdir.

$E_{k.p.}$ – göstəricisi kapital qoyuluşunun özünü doğrultması səviyyəsini göstərir. Buradan çıxır ki,

1) $E_{k.p.}$ – qiymətinə görə bütün obyektləri müqayisə etmək o lar;
2) $E_{k.p.}$ –ni hesablayarkən müxtəlif obyektlərin məhsullarının həcmini bərabərləşdirmək zəruri deyil.
3) (2.3.)-dən gö.ründüyü kimi, xalis gəlirin mənbəy buraxılan məhsulun maya dəyərinin aşağı düşməsi $C_1 > C_2$ və ya illik məhsulburaxılışının həcminin artırılması və keyfiyyətin yüksəldilməsidir ki, bu da özünü dəyərdə ifadə edir. $S_2 > S_1$.

KŞ-nin iqtisadi səmərəsini müəyyənedərkən (2.3.) düsturundan istifadə olunur.

Kapital qoyuluşunun iqtisadi səmərəsi göstəricilərindən biri də $E_{k.p.}$ – ilə birqiymətli müəyyən edilən, $T_{o.k.}$ - kapital qoyuluşunun özünüalma vaxtıdır.

$$T_{o.k.} = \frac{1}{E_{k.m.}} = \frac{K}{P} \qquad (2.4.)$$

KŞ-ləri üçün bu göstəricinin

$$T_{o.k.} = \frac{K}{C_1 - C_2} \qquad (2.5.)$$

düsturu ilə hesablanması təklif edilir. Bu zaman nəzərdə tutulur ki, obyektin təkmilləşməsi illik məhsul buraxılışına və onun keyfiyyətinə təsir göstərmir, ancaq və ancaq maya dəyərinin C_1-dən C_2-yə düşməsinə təsir edir.

Üçüncü göstərici (iqtisadi səmərəlilik göstəriciləri) gətirilmiq xərclər göstəricisidir:

$$U = U(V) = C + E_nK \quad (2.6.)$$

V – qeyd olunmuş illik məhsulun miqdarıdır. E_n – xalq təsərrüfatının müxtəlif sahələri üçün müxtəlif qiymət alan iqtisadi səmərənin nomrativ əmsalıdır. $E_n \geq 0{,}12$. Buradan belə çıxır ki, ən böyük özünü alma vaxtı

$$T_{o.k.} = \frac{1}{0{,}12} = 8{,}33$$

Gətirilmiş xərclər hətta vahid məhsula görə də hesablana bilər:

$$\underline{U_0} = U(1) = \frac{U(V)}{V} = \underline{C_0} + E_0 \underline{K_0} \qquad (2.7),$$

burada, C_0, K_0 – vahid məhsulun maya dəyəri və kapital qoyuluşudur.

U-nun $E_{k.p.}$-dən üstünlüyü ondan ibarətdir ki, U-nun hesablanması üçün vahid məhsulun qiymətini bilmək lazım deyil. Elə bu üstünlüyü ilə də gətirilmiş xərclər göstəricisinin çatışmamazlığı meydana çıxır. Gətirilmiş xərclər göstəricisi yalnız oxşar, uyuşan məhsullar buraxan obyektlər üçün hesablanır.

Bu göstərici KŞ üçün hesablanarkən onun tətbiqindən əvvəlki və sonrakı göstəricilər müqayisə olunurlar.

$$U_2 = C_2 + E_n (K_{ob} + \Delta K) \qquad (2.8),$$

Burada, K_{ob} - obyektə çəkilən məcmu xərclər, ΔK – MİS-ə çəkilən xərclərdir.

MİS-in iqtisadi səmərə verməsi üçün

$$U_2 < U_1 \qquad (2.9.)$$

olmalıdır və ya

$$C_1 - C_2 > E_n \Delta K \qquad (2.10.)$$

ödənməlidir.

Gətirilmiş xərclər göstəricisindən törəmə illik iqtisadi səmərə göstəricisidir.

$$E = (U_{01} - U_{02})V_2 = [(C_{01} + E_n K_{01}) - (C_{02} + E_n K_{02})]\, V_2 \qquad (2.11.)$$

U_{01} , C_{01}, K_{01} - uyğun olaraq birinci obyektin,

U_{02} , C_{02}, K_{02} və V_2 - ikinci obyektin göstəricisidir. V_2 - buraxılan məhsulun illik həcmidir.

Daha bir obyektarası göstərici texniki həllin mütərəqqilik əmsalıdır.

$$\xi_n = \frac{E_{kp2}}{E_{kp1}} \qquad (2.12),$$

E_{kp2} - ikinci texniki həllin iqtisadi səmərəlilik əmsalı, E_{kp1} - birinci texniki həllin iqtisadi səmərəlilik əmsalıdır.

Yuxarıda verilən iqtisadi səmərənin əsas göstəriciləri müqayisə etmənin (optimallaşdırmanın) aşağıdakı iki kriteriyasını verir:

$$E_{kp} \to \max \qquad (2.13.)$$

$$U_0 \to \min \qquad (2.14.)$$

Eyni bir məsələnin texniki həllinin müxtəlif variantlarında bu iki nəticə çox zaman üst-üstə düşə bilmir.

Göstərək ki, (2.14.) və (2.13.) meyarları ilə bir obyektin iki informasiya sisteminin müqayisəsi heç də həmişə üst-üstə düşmür. Tutaq ki, V_1, C_1, K_1 və V_2, C_2, K_2 məlumdur və S_0 – hər iki sistem üçün eynidir:

$$E_{k.p.1} = \frac{1}{K_1}(V_1 S_0 - C_1); \quad E_{k.p.2} = \frac{1}{K_2}(V_2 S_0 - C_2) \qquad (2.15)$$

Tutaq ki, $E_{k.p.1} > E_{k.p.2}$.

Aşağıdakı əmsalları daxil edərək və bərabər məhsul buraxılışı həcmləri V_{pvc} olan oblastlar üçün gətirilmiş xərcləri müqayisə edək:

$$\alpha_1 = \frac{V_{pvc}}{V_1} \quad \text{və } \alpha_2 = \frac{V_{pvc}}{V_2}$$

(2.15.)-dən alırıq ki,

$$E_{k.p.1} = \frac{1}{\alpha_1 K_1}(\alpha_1 V_1 W_0 - \alpha_1 C_1); \qquad (2.16)$$

$$E_{k.p.2} = \frac{1}{\alpha_2 K_2}(\alpha_1 V_2 W_0 - \alpha_2 C_2); \qquad (2.17)$$

1.3. Komputer sistemlərinin səmərəliliyin etibarlılıqla birgə araşdırılması.

KŞ-in iqtisadi səmərəliliyinin qiymətləndirilməsi elə texnoloji obyektin istismara qədərki iqtisadi səmərəsinin qiymətləndirilməsindən asılıdır. KŞ yalnız inflrmasiyasına emal etdiyi obyektin vasitəsilə iqtisadi səmərə verə bilər. KŞ-in istismarından gələn gəlir yalnız bir mənbəyə malikdir ki, bu da obyektin istismarının iqtisadi göstəricilərini yaxşılaşdırmaqdır. Başqa sözlə desək, KŞ-dən gələn gəlir, obyektin istismarından alınan gəlirə əlavə gəlirdir.

KŞ-in istismarından alınan səmərə miqdarca, sənaye obyektlərinin səmərəsi hesablanan iki əsas iqtisadi göstərici ilə E_{kII} və U_0 ilə ölçülür. Doğrudan da, bir tərəfdən sənaye obyektinə KŞ-in tətbiqi nəticəsində vahid məhsula düşən gətirilmiş xərclər aşağı düşür, digər tərəfdən isə sistemin alınması və layihələndirilməsinə qoyulan kapital xərcləri iqtisadi səmərəli olmalıdır.

KŞ-in iqtisadi səmərəsi və etibarlılığını araşdırmaq iki əsas məsələyə - 1) iqtisadi səmərənin etibarlığı nəzərə alaraqdan hesablanması; 2) iqtisadi kriteriyalara görə etibarlığın optimallaşdırılması məsələlərinə malikdir.

Gəlin bu məsələlərə bir də baxaq.

Tutaq ki, avtomatlaşdırılmış obyektin iqtisadi səmərəlilik göstəriciləri aşağıdakılardır:

$\overline{E'_{k,Pob}}$ $\overline{Y'_{r,Pob}}$, K_{ob}, S_{ob}, $\overline{R_{ob}}$, P_{ob}, C_{ob}, V_{ob}.

Gəlin, ATK halında, yəni obyekt üçün KŞ-nin olduğu hala baxaq – $Y'_{0\Sigma}$.

KŞ-in olmadığı halda $\overline{Y'_{ob}}$ aşağıdakı düstür ilə hesablanır:

$$\overline{Y'_{ob}} = S_{ob} + \frac{S + \overline{R_{ob}} + \overline{R_{rob}} + R_{pr} + E_n K}{V - V_{sn.pr}}$$

ATK = (O+İS) üçün isə $Y'_{0\Sigma}$ -= $S_{0,0\Sigma}$ + $Y'_{0\Sigma}$ düsturu ilə hesablanır. Bu zaman obyektin etibarlığına aid olan (S_{ob}, R_{brob}, $\overline{R'_{remob}}$, $\overline{R'_{pr.ob}}$) parametrləri KŞ-nin obyektə təsirini nəzərə alaraqdan hesablanmalıdır. Ümumi halda bilirik ki, KŞ-nin istismarı obyektin bütün göstəricilərinə, o cümlədən, etibarlıq göstəricilərinə də təsir edir.

KŞ istismar olunarkən obyektin iqtisadi parametrlərini «′» indeksi ilə işarə edək.

$\overline{Y'_{0\Sigma}}$ və $\overline{Y'_{ob}}$ müqayisəsi gətirilmiş xərclərə görə sistemin səmərəliliyi haqqında problemi həll etməyə imkan verir.

$\overline{Y'_{0\Sigma}}$ ifadəsi obyektin və KŞ-in ayrı-ayrı parametrlərinin məcmu gətirilmiş xərclərinin hesablanmasındakı rolunu aydın göstərir.

İndi isə KŞ-in iqtisadi səmərəlilik əmsalına baxaq.

$E_{k,p}$ –nin (1) düsturunda hesablanarkən K dedikdə KŞ-nin istismarı və hazırlanması ilə əlaqədar əlavə kapital xərci başa düşülür, P- əlavə illik gəlirdir.

Yuxarıdakıları nəzərə alsaq,

$$\overline{E'_{k.p.c.}} = \frac{P_c}{K_c} = \frac{P_\Sigma - P_{ob}}{K_c} = \frac{(C_\Sigma - C_{ob}) + (S_{ob} - S_\Sigma)}{K_c} = \frac{1}{K_c}(\Delta S + \Delta C) \qquad (3.1.)$$

etibarlığı nəzərə alaraq:

$$P_c' = P_\Sigma' - P_{ob}' \qquad (3.2.)$$

və əvvəlki düsturu $\overline{P'} = P_0 - (S + \overline{R})$ nəzərə alsaq,

$$P_c' = (P_{0\Sigma} - S_z - \overline{R_Z}) - (P_{oob} - S_{ob} - \overline{R_{ob}}) \qquad (3.3.),$$

burada,

$S_\Sigma = S_{ob1} - S_c$; $\overline{R_\Sigma} = \overline{R_{ob1}} + \overline{R_c}$;

S_{ob1} və $\overline{R_{ob1}}$ TO-nun etibarlılığının KŞ olarkən dəyəri və qiymətidir.

$$(P_{0\Sigma} - P_{oob}) + (S_{ob} - S_{ob1}) + (\overline{R_{ob}} - \overline{R_{ob1}}) = P_{oc} \qquad (3.4.)$$

işarə etsək, onda (3)-dən alırıq ki,

$$\overline{P'_c} = P_{oc} - (P_c + \overline{R_c}) \qquad (3.5.)$$

və $\overline{E'_{k.p.c.}}$ üçün ifadə hesablamaq və təhlili üçün asan olan kanonik forma alır:

$$\overline{E'_{k.p.c.}} = \frac{1}{K}(P_{oc} - S_c - \overline{R_c}) \qquad (3.6.)$$

$\overline{E'_{k.p.c.}}$ - hesablanarkən əsas çətinlik KŞ-in tətbiqindən alınan «ideal» P_{oc} – gəlirini hesablamaqdır. S_c və $\overline{R_c}$ kəmiyyətləri adətən (3.2.) və (3.9.) düsturları ilə hesablanırlar.

(4) ifadəsində birinci toplanan avtomatlaşdırılmış obyektin ideal gəlirini göstərir. Bu ifadə onu göstərir ki, ideal gəlir (KŞ-in) tətbiqindən yalnız avtomatlaşdırılmış obyektin gəlir artımından deyil, həm də onun etibarlığının təmin xərclərinin azalması S_{ob} və onun etibarlılığının qiymətinin aşağı düşməsi yolu ilə də alınır. Beləliklə, P_{oc}-nin təyini, yaradılmasının KŞ-in avtomatlaşdırılan TO–in bütün texniki və iqtisadi parametrlərinə təsirini araşdırmaq yolu ilə mümkündür.

Müxtəlif KŞ-lər üçün P_{oc}-nin təyininə aid bir neçə xüsusi hallara baxaq.

Misal 1. Müəyyən KŞ-in tətbiqindən müsbət səmərə obyektin idarə edilməsindənalınan xüsusi məhsuldarlıqdan və ΔV_0 –dan ibarətdir, yəni

$V_{0\Sigma} = V_0 + \Delta V$.

Tutaq ki, xərclərə (obyektlə əlaqədar) KŞ-in tətbiqi heç bir təsir göstərmir. (S_{ob}, $\overline{R_{ob}}$). Deməli, buraxılan məhsulun vahid həcminin qiyməti dəyişmir, yəni

$C_{o\Sigma} = C_{oob} = C_o$;

Həmçinin maya dəyərinin dəyişən hissəsi də

$S_{o,o\Sigma} = S_{o,o\ ob} = S_{o,o}$ və texniki obyektin il ərzində iş vaxtı da dəyişməz qalır: ($\theta_\Sigma = \theta_{ob} = \theta$).

Bu şərtlər daxilində (4) düsturundan və (3.8) ifadəsini nəzərə alsaq,

$$P_{oc} = (P_{o\Sigma} - P_{oob}) + O + O = (S_{o\Sigma} - C_{o,o\Sigma})\theta_\Sigma\ Vo_\Sigma - (S_{o\ ob} - C_{o,o\ ob})\theta_{ob}\ V_{o\ ob} =$$

$$= (S_o - C_{o,o})\theta\ \Delta V_o \qquad (3.7.)$$

Misal 2. KŞ-in tətbiqi obyektin xüsusi məhsuldarlığını ΔV_o qədər artırdığı ilə bərabər həm də vahid məhsulun qiymətini ΔC_o qədər artırır. Bundan başqa, KŞ

tətbiq edərkən işçi qüvvəsinin qənaəti alınır ki, bu da maya dəyərinin $\Delta S_{o,o}$ qədər aşağı düşməsinə gətirib çıxarır. Obyektin illik iş fondu dəyişmir.

Əvvəlkinə analoji olaraq:

$$P_{oc} =[(C_{o\Sigma} - S_{o,o}) \Delta V_o + (\Delta C_o - \Delta S_{o,o})(\Delta V_o + \Delta V_o)] \theta \quad (3.8.)$$

Misal 3. Əvvəlki xüsusi hala onu da əlavə edək ki, KŞ-in tətbiqi həm də illik iş vaxtı fondunu artırır: $\Delta\theta$ ($\theta_\Sigma = \theta_{ob} + \Delta\theta$).

Bundan əlavə KŞ imkan verir ki, TO-nun illik profilaktika seanslarının sayı azalır ki, bu da etibarlığı təmin etmək üçün xərcləri ΔS qədər azaldır, həm də $\Delta \overline{R}$.

(4) –ə əsasən alırıq:

$$P_{oc} =(C_{o\Sigma} - S_{o,o}) \theta\Delta V_o + (C_o - \Delta S_{o,o}) \Delta\theta (\Delta V_o + \Delta V_o) + (\Delta C_o - \Delta S_{o,o}).$$

$$.(\theta +\Delta\theta) \ (V_o + \Delta V_o) \ +\Delta S +\Delta \overline{R} \qquad (3.8.)$$

Analoji üsullarda $P_{o,c}$ üçün müxtəlif hallarda hesablama düsturları almaq olar.

İndi isə KŞ-in etibarlılığının optimallaşdırılması məsələsinə baxaq:

(3.6.) düsturundan aşağıdakı asılılığı almaq olar:

$$\overline{E'_{k.p.c.}}(a_c)= \frac{1}{K(a_c)}\left[P_{oc} - S_c(a_c) - \overline{R_c}(a_c)\right] \qquad (3.9.)$$

Bu ifadə $E_{k.p.} \rightarrow$ max meyarına görə a_c-nin təyini üçün başlanğıc ifadədəir.

Analoji olaraq $\overline{Y'_{o\Sigma}}$ üçün olan ifadədən $Y_0 \rightarrow$min meyarına görə etibarlığın optimal səviyyəsini müəyyən etmək üçün əsas asılılığı almaq olar:

$$\overline{Y'_{o\Sigma}} \qquad (a_c) \qquad =$$

$$= S_{o,o\Sigma} + \frac{1}{V - V_{sn.kr}(a_c)} [S_{ob}(a_c) + \overline{R_{brob}}(a_c) + \overline{R_{regiob}}(a_c) + E_n \cdot K_{ob} + S_c(a_c) + \overline{R_{br,c}}(a_c) + \overline{R_{regic}}(a_c) +$$

$$+ \overline{R_{pr,c}}(a_c) + E_n \cdot K_c(a_c)]$$

Fəsil 2. İnformasiya sistemlərinin proqram vasitələrinin (Soft) etibarlığı

2.1. Sistemin etibarlığı

Bütün MİS-də əsas rolu informasiya prosesləri oynayırlar. İdarə olunan obyekt haqqında informasiyanın alınmasından ta idarəedici informasiyanın alınmasına qədər olan proses müxtəlif informasiya sistemlərini köməyi ilə alınır. Deməli, hər bir AİS-in işlənməsi bir neçə ardıcıl informasiya sistemlərinin yaradılmasından ibarətdir.

Bu deyilənlər tamamilə etibarlılıq məsələlərinin tədqiqinə də aiddir. KŞ-in etibarlığı məsələsinin və onun həllinin özünəməxsusluğu mövcuddur. Bu onunla əlaqədardır ki, hər bir KŞ-nin konkret parametrləri və xassələri vardır. Göründüyü kimi, KŞ-nin etibarlığını təsvir, tədqiq edən və qiymətləndirən ümumi üsulların işlənməsi vacibdir. Bu üsullar ayrıca KŞ-nin və ya hər hansı AİS-in tərkibindəki KŞ-nin araşdırılması zamanı tətbiq oluna bilərlər.

KŞ dedikdə, biz informasiya üzərində aşağıdakı əməliyyatların yerinə yetirilməsini təmin edən sistemlər başa düşəcəyik: ötürmə; qeyd etmə; saxlama; işlənmə; inikas.

KŞ sadə və kompleks ola bilər:

a) fəaliyyət formasına görə:

- texnoloji KŞ;
- təşkilatı-inzibati;

b) İnformasiyanın təqdim formasına görə:

- kəsilməz KŞ;
- diskret KŞ.

Funksional: - istehsal xidməti paylanma mərkəzi.

İndi isə KŞ-nin etibarlılıq xarakteristika və göstəricilərinə nəzər salaq.

Etibarlılığın uzunmüddətlilik və saxlanıla bilmək kimi tərkib hissələri başqa obyektlərdə necə varsa, KŞ-də də eynidir. Buna görə də bu göstəricilərin hər birinə kursumuzun əvvəlində KŞ üçün dediklərimiz eyni ilə aiddir.

KŞ üçün ayrıca öyrənilməli sıradan çıxmamaq göstəricisidir.

Diskret KŞ üçün sıradan çıxmanın iki cür forması vardır:

1) KŞ-nin komponentlərinin möhkəm sıradan çıxması, KŞ-nin fəaliyyətinin uzun müddət dayandırılmasına gətirib çıxarır;
2) Öz-özünü düzəldən sıradan çıxma və ya dayanmalar, bunlar KŞ-nin ayrı-ayrı mərhələsinin dayanmasına səbəb olur.

Qeyd etmək lazımdır ki, KŞ-nin sıradan çıxması intensivliyinin dəyişməsi istifadə olunan element bazasından asılıdır.

KŞ-də sıradan çıxma və dayanmaların səbəbləri müxtəlif olduqlarından KŞ-nin sıradan çıxmamaq xassəsi bu iki formaya görə ayrıca öyrənilməlidir. Sıradan çıxmamağın miqdarı xarakteristikası KŞ-nin iş vaxtının dayanmaya qədərki miqdarıdır – T_{otk} və bu kəmiyyət $f_{otk}(t)$, $P_{otk}(t)$ və ya $\lambda_{otk}(t)$ vasitəsilə verilə bilər. əgər T_{otk} –nın paylanması eksponensial və ya normaldırsa, onda sıradan çıxmanın məlum ədədigöstəricilərindən T_{otk} , λ_{otk}, $P_{otk}(t_{fiks})$ istifadə etmək olar. Beləliklə, ciddi sıradan çıxma zamanı KŞ-nin və MİS-nin sıradan çıxmamaq xassəsi eynidir.

KŞ-nin cüzi dayanmalarına nəzərən, onun sıradan çıxmamaq xassəsi KŞ-nin əməliyyat tezliyindən və doğruluğundan asılıdır.

Əgər müəyyən KŞ üçün əməliyyat tezliyi ν və çevirmənin doğruluğu – q_1 verilərsə, onda standart sıradan çıxmamaq göstəricilərinə gəlib çıxmaq çox da çətin deyildir.

Tutaq ki, T_{sb} – KŞ-nin sıradan çıxana qədərki iş vaxtıdır və təsadüfi kəmiyyətdir.

KŞ-nin standart sıradan çıxmamaq göstəriciləri T_{sb}–nin paylanması nəticəsində alınan $f_{sb}(t)$, $P_{sb}(t)$ və ya $\lambda_{sb}(t)$ –dir.

Əgər dayanmaların bir-birindən asılılığı yoxdursa, onda

$$P_{sb}(t) = (1-g_{sb1})^{\nu t} = e^{-\lambda sbt} \qquad (1),$$

burada,

$$\lambda_{sb} = -\nu\ln(1-g_{sb1}) \qquad (2)$$

(1) –dən göründüyü kimi, T_{sb} - paylanması eksponensialdır və parametri λ_{sb} –dir. Buna görə də KŞ-nin sıradan çıxmamaq göstəricisi, sabit əməliyyat tezlikli λ_{sb} – kəmiyyətidir ki, bu da (2) ilə təyin olunur.

Bir çox KŞ üçün xarakterik olan odur ki, diskret informasiyanın daxil olunması və işlənməsi tam massivlər vasitəsilə olur.

Belə ki, KŞ üçün etibarlılıq xarkteristikaları kimi bütün massivin düzgün işlənməsi ehtimalı əsasdır. Başlanğıc verilən kimi massivin bloklarının (və ya işlənmə taktlarının) sayı – m verilməlidir - $\tau_k = m/\nu$;

Əgər sıradan çıxma və ya dayanma asılı deyilsə, onda massiv üçün:

$$P = P_{otk}.P_{sb} \qquad (3)$$

buradan,

$$P = P_{otk}.(\tau_k)e^{-\lambda sb\tau k} \qquad (4)$$

alarıq.

KŞ-də prinsipcə, etibarlığı artırmağın bütün üsulları istifadə edilir: daha etibarlı hissələrin tətbiqi; ayrı-ayrı birləşmə və elementlərin ehtiyat variantların olması; profilaktoriya xidməti; istismar şəraitinin yaxşılaşdırılması; xarici maneələrin səviyyəsinin aşağı salınması.

Bu üsullar içərisində bir qrupunu ayırmaq olar ki, onlar KŞ-nə tətbiqdə daha səmərəli və məxsusidirlər. Belə üsullardan biri əlavə informasiyanın sistemə daxil edilməsi üsuludur, bəzən də düzəldən – korreksiya edən kodlar üsulu da deyilir.

KŞ-nin etibarlığını artıran üsulların bəzisi MAİS-də, bəzisi TPAİS-də, bəzisi isə ayrıca götürülmüş KŞ-də səmərəlidir.

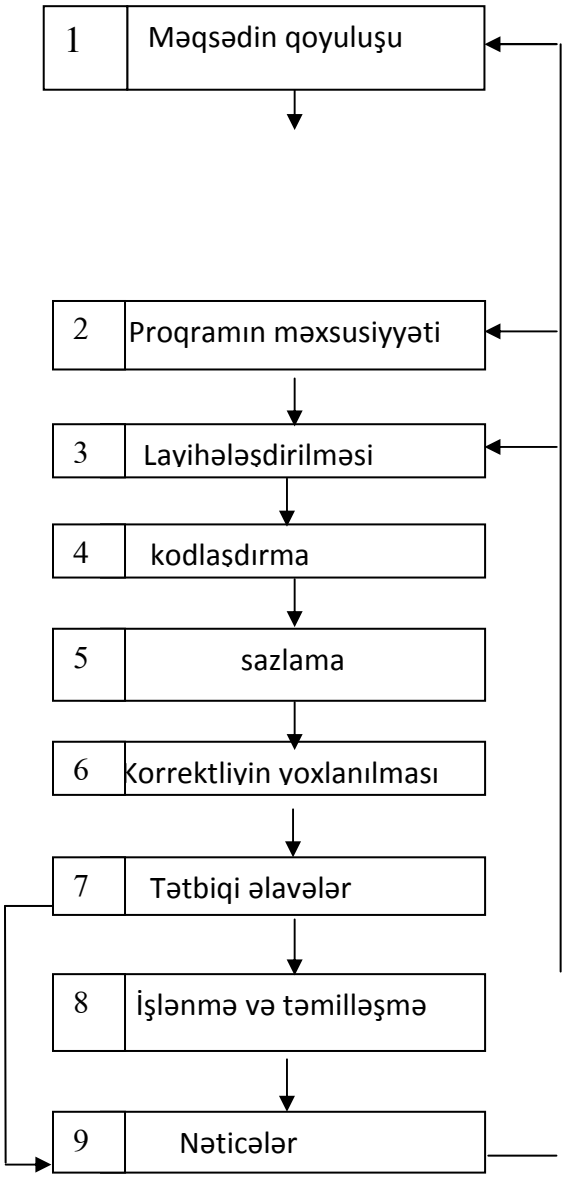
2.2. Proqram vasitələrində səhvlərin axtarışı

Etibarlıq proqram əldə etmək üçün proqramında rast gəlinən səhvlər tipini dəqiq bilmək lazımdır.

Səhvlərin təsnifatını və onların öyrənilməsi üçün kompüterin proqram təminatının (PT)-nın ayrı-ayrı elementlərinin layihəsi sxeminə baxaq.

Aydındır ki, hər hansı proqramın işlənməsi və ya tutulması məqsədin müəyyən olunmasından başlanır. Məqsədin işlənib hazırlanması qeyri-müəyyənlik və ikimənalılıq kimi xarakterik xüsusiyyətlərə malikdir. Məsələn, məqsəd müəyyən cədvəlin alınması və ya uçuşu idarə etmək olar. Məqsəd daha sonra müəyyən dilə çevrilməli və proqramın nə edəcəyi dəqiq göstərilməlidir. Proqramın məxsusiyyəti müəyyən edildikdən sonra onu layihələşdirmək, kodlaşdırmaq və sazlamaq zəruridir.

Layihələşdirmə mərhələsi sistemin etibarlığının səviyyəsini müəyyən etmək mərhələsidir. Bu mərhələdə sənədlərdə sistemin etibarlığını təmin edəcək əsas üsullar seçilir. Bu mərhələdə sistemin etibarlığının tədqiqinin əsas mərhələləri, etibarlığı təmin edən müxtəlif üsulların səmərəsinin müqayisəli təhlili, verilmiş etibarlılığa malik variantların seçilməsi məsələləridir. Sadalanan məsələlərin əsas həlli üsulları, etibarlığın səviyyəsinin qiymətləndirilməsi üsulları, müxtəlif variantların etibarlığa görə müqayisəli təhlili üsulları və optimallaşdırma üsullarıdır. Araşdırma modellər əsasında aparılır. Sonrakı



PT-nın işlənməsinin ümumi sxemi.

mərhələdə tutulmuş proqram məqsədə müvafiq yoxlanılır ki, onun məqsədi yerinə yetirib yetirməyəcəyi məlum olsun. Bu yoxlama gözlə üzəvari yoxlamadan ta korrektliyi sərbəst yoxlamaya (validasiya) qədər uzana bilər.

Nəzərdə tutulur ki, validasiyadan sonra tutulan proqram qarşıya qoyulan məqsəd üçün tətbiq edilə bilər.

Əvvəlki mərhələlərdən fərqli olaraq sazlama və istismara qəbul zamanı real istismar şəraitində sistemin işlənməsini müşahidə etmək olar. Bu zaman əsas məsələlər təcrübələrin vaxtını və həcmini planlaşdırmaq, əldə olunmuş etibarlıq

səviyyəsinin qiymətləndirilməsi və sistemin etibarlılığına qoyulmuş tələblərin yerinə yetirilməsini yoxlamaqdan ibarətdir.

Əgər təcrübələr zamanı sistemin tam şəkildə istismara qəbulu mümkünsə, onda etibarlığın araşdırılmasının əsas üsulları riyazi statistika üsullarıdır.

Əgər bütöv sistemin istismarı mümkün deyilsə, onda etibarlılığı araşdırmaq üçün etibarlılığın riyazi modellərindən istifadə olunur.

İşlənmə və təkmilləşmə mərhələsində proqramın korrektliyi, müəyyən məqsəd üçün əlavələr və ya qısaltmalar və s. yerinə yetirilir.

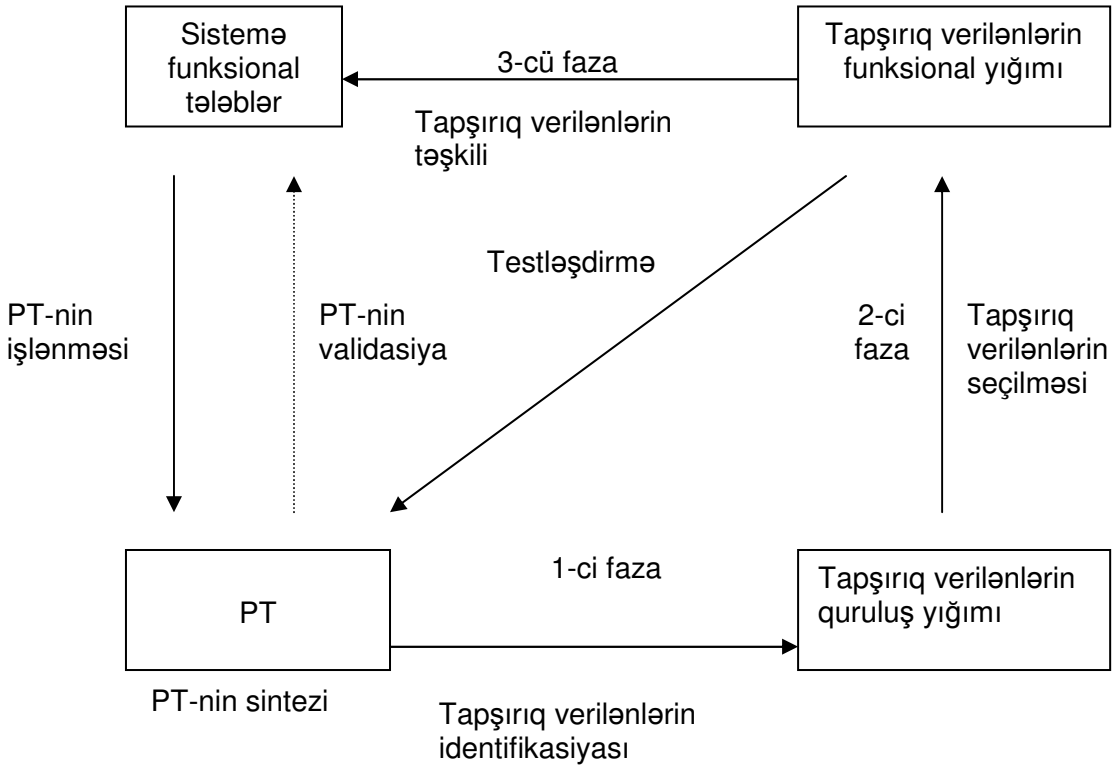
Sxemdən göründüyü kimi, proqramın işçi vəziyyətinə gətirilməsinə qədər olan proses məxsusiyyətdən axıra qədər bir neçə dəfə təkrar oluna bilər.

PT-nın işlənməsində ən qısa vacib momentlərdən biri proqramın validasiyasıdır.

Sxemdə validasiyanın üç əsas fazası göstərilmişdir: tapşırıq verilənlərin identifikasiyası; tapşırıq verilənlərin seçilməsi; tapşırıq verilənlərin təhlili.

Tapşırıq verilənlərinin yığımı alındıqdansonra o (3-cü faza) sistemin funksonal məxsusiyyətləri ilə tutuşdurulur. Bu zaman aşağıdakı nəticələr alına bilər:

- əgər tapşırıq verilənlərin funksional yığımı sistemin funksional məxsusiyyətinə uyğun gəlirsə, deməli proqram yoxlanıldı;



PT-nın ümumi validasiyası

- əgər elə funksional tapşırıq veriləni olarsa ki, ona sistemin funksional tələbi uyğun gəlməsin, onda səhvə gətirən müəyyən kod vardır;
- əgər sistemin müəyyən funksional məxsusiyyəti varsa ki, ona uyğun tapşırıq veriləni yoxdur. Onda PT sistemi ixtiyari variantda çatışmamazlığa malikdir.

2.3. Aşkarlanmış səhvlərin təhlili sxemləri

PT-da ümumi halda səhvlər proqramın qarşıya qoyduğu məqsd və alınan nəticələr arasındakı fərq kimi müəyyən edilirlər. Bu səhvlər proqramda onun bütün mərhələlərində düzəldilə bilərlər.

Prinsipcə, PT-da səhvlərin miqdarını iki üsulla təsvir etmək olar:

Birinci üsul: - layihə və validasiya zamanı meydana çıxan səhvlərin toplanması və öyrənilməsindən ibarətdir. Real proqramların tam və məqsədyönlü araşdırılması kifayət qədər vaxt və dəyərli xərc tələb edir və bəzi bu əsas işə – PT-nın layihəsinin yaradılmasına mane olur. Bundan əlavə statistik qəbuledilən nəticələrin alınması üçün təcrübə sxeminin xırdalıqlarla yaradılması, eksperiment iştirakçılarının seçilməsi və məlumatların yığılması və ümumiləşdirilməsi tələb olunur.

Bu cür yanaşma real təcrübədən çıxmış proqram nəticələri ilə tutuşdurma yolu ilə dəyişdirilə də bilər. İmkan yaranır ki, kompüterin tətbiqi və PT-nın işlənməsi sahəsində bir sıra məxsus əlavələr əhatə olunsun.

İkinci üsul: səhvlərin aşkara çıxarılması üçün xüsusi nəzarətçi proqramların tutulmasını tələb edir. Bu üsulun bir sıra çatışmamazlıqları vardır ki, onlardan ən əsasları aşağıdakılardır:

- məlumatların yığılması dəyərinə qoyulmuş məhdudiyyətlər nəzarətçi proqramın kiçik ölçülü olmasına gətirib çıxarır. Kiçik proqramların istifadəsi isə imkan verir ki, nəticələrin yalnız qarışdırılmış qiymətlənməsi alınsın;
- nəzarətçi proqram real prosesdə uzun müddət istifadə edilmədiyindən tam səhvlər külliyyatı haqqında bir şey demək mümkün olmur.

Səhvlər qrupunun müxtəlif əlamətlərinə görə təsnifatları mövcuddur.

Məsələn, səhvlər əməliyyat tipinə görə qruplara ayrıla bilərlər: hesabi, məntiqi, məlumatlara müraciət, yaddaşlarda məlumatlarla dəyişmə və s. səhvləri ola bilər.

Səhvlər PT-nın işlənməsi mərhələlərinə görə də təsnifata malik ola bilərlər: məxsusiyyət səhvi, layihə səhvi, istifadə shvi və s.

Səhvlər, onları meydana çıxarmaq üsullarına görə də təsnifata bölünə bilərlər: - təhlil nəticəsində, yerinə yetirilmə nəticəsində və s. alınan səhvlər.

Təsnifat PT-nın işlənməsi və səhvlərin rədd edilməsi üçün əlavə material kimi istifadə oluna bilər.

PT-da səhvlərin çoxu modulların ayrıca testləşdirilməsi və inteqrasiyası zamanı meydana çıxa bilər. aşağıdakı səbəblərə görə bu mərhələ tədqiqat obyekti kimi götürülə bilər:

- PT-nın işlənib hazırlanmasının ümumi vaxtının çox hissəsi EHM-lər üçün böyük proqramların testləşdirilməsinə və inteqrasiyasına sərf olunur. Təcrübə göstərir ki, testləşdirmə və inteqrasiya əsas vaxtın 50 %-ni təşkil edir. Bundan əlavə, maşın vaxtının çox hissəsini aldığından xərc də böyüyür;
- PT-nın etibarlığının miqdarı qiymətləndirilməsi üçün başlanğıc zəminlərin hazırlanması. Proqramçıların əksəriyyəti ya ən axırıncı səhvi ya da ən çətin və maraqlı səhvi müqayisəsini saxlayırlar. Buna görə də səhvlərin müqayisəsini, hansının öyrənilməsinin daha vacib olduğunu nəzərə almaq lazımdır. Çox kobud səhv tez-tez rast gəlinən cüzi səhvlərdən daha vacib ola bilər;
- Testləşdirmə və inteqrasiya üçün ehtiyatların bölünməsinə başlanğıc zəminin hazırlanması. P-nın sazlanması üçün iki üsul mümkündür;
- Stol arxasında proqramın «oxunması» ilə proqram üçün müxtəlif testləşdirmə kombinasiyalarının layihələşdirilməsi və EHM-də yerinə yetirilmə ilə nəticələrin yoxlanılması üsulu.

Validasiya mərhələsində aşkara çıxan səhvlər qalan səhvlərin aşkara çıxarılması və aradan götürülməsi üçün proqramın sazlanmasında istfadə olunan üsullardan fərqli olan xüsusi validasiya ciddi sayılır ki, ya proqramın yerinə yetirilməsi dayansın, ya da nəticə səhv alınsın.

- Orta səhv – nəticə arzu olunandan fərqlidir, lakin fərq azdır;
- Kiçik səhv – proqramın məhsuldarlığına heç bir təsir göstərmir.

HTTP protokol cavab kodlarını və onların qarşılıqı verilmiş cədvələ baxaq:

Kod	Məlumat	Mənası
1xx		
100	Continue	Davam
101	Switching Protocols	Şifrələmə protokolu
2xx		
200	OK	Oldu
202	Accepted	Qəbul olundu
204	No Content	Boş məzmun
3xx		
304	Not Modified	Yenilənmədi
305	Use Proxy	Proxy işlət
4xx		
403	Forbidden	Qadağan olundu
404	Not Found	Səhifə tapılmadı

Bu nömrəli kodlar , Veb axtarış proqramları tərəfindən avtomatik olaraq işlənərək başa düşülən bir mesaja çevrilir.

Kod nömrəsinin birinci xanası, cavabın beş kateqoriyadan hansına aid olduğunu bildirir. 200, 301, 302, 404 və 500 kodları ən çox istifadə olunan

kodlardır. Bəzi kodlar hələ işlənilməsə də gələcəkdə çox işlənən kodlar olması gözlənilir. Bu tip kodlara misal olaraq 200 kodunu göstərmək olar.

Verilən cədvələ əsasən aşağıdakı nəticələri çıxarmaq olar:

1) PT-nın etibarsızlığının yeganə səbəbi yoxdur və buna görə də bütün səhvləri aşkara sıxaran vahid vasitə təklif olunur.
2) Məxsusiyyətdən razılaşdırılmış kənara çıxmalar və proqramlaşdırma standartlarının pozulması nəticəsində ciddi səhvlər alınır.

Səhvlərin təibətini öyrənərkən, onların nə vaxt və harada meydana çıxmasını bilmək çox vacibdir. Hər şeydən əvvəl, bu, hansı validasiya üsullarının və analizinin tətbiqini bilmək üçün zəruridir.

2.4. Dayanıqlı proqram vasitələrinin etibarlıq modelləri.

t=0 anından işə başlayan PT sisteminə baxaq. Tutaq ki, sistem sıradan çıxana qədər əvvəlcədən müəyyən olunmuş kriteriyaya uyğun işləyir. Sıradan çıxmanın təsadüfi t – vaxtı

$t(\varphi) = \varphi$; φ ≥ 0 kimi müəyyən oluna bilər; burada φ eksperimentin diskret zaman oxunda nöqtələrin yeridir. Tutaq ki, t – təsadüfi dəyişəni paylanma funksiyasına malikdir: F (t) = P {φ: t(φ) ≤t}, onda sıxlıq funksiyası:

$$f(t) = \frac{dF(t)}{dt}.$$

Sistemin etibarlığı – R(t) (0,t) intervalında sıradan çıxmanın olmaması ehtimalı ilə müəyyən olunur:

$$R(t) = \{t \geq t\} \qquad (3.1.)$$

t anında sistemin hazırlığı dedikdə onun t zamanı ərzində işçi vəziyyətdə olması ehtimalı başa düşülür:

$$A(t) = P \qquad (3.2)$$

Aşağıdakı kimi müəyyən edilən riskin dərəcəsi göstəricisi də müəyyən əhəmiyyət kəsb edir.

$Z(t)\,\Delta t = P\,\{t < t \le t + \Delta t\}$

Onda sistemin etibarlığı

$$R(t) = EXP\,[-\int_0^t Z(x)dx\,] \qquad (3.3)$$

kimi təyin oluna bilər, sıradan çıxma vaxtının qiymətini isə

$$t_w = \int_0^t R(x)dx \qquad (3.4.)$$

hesablamaq olar.

Riskin dərəcəsi sabit olarsa, $-Z(t) = \lambda$, onda bütün hesablanan asılılıqlar:

$$f(t) = \lambda e^{-\lambda t}, \qquad (3.5.)$$

$$R(t) = e^{-\lambda t}, \qquad (3.6.)$$

$$t_w = 1/\lambda \qquad (3.7.)$$

şəklində olar.

Tutaq ki, t=0 anında sistemin məlum olmayan n sayda səhvi vardır. Sistemin işləməyə başlama vaxtı olaraq testləşdirmə fazasının başlanğıcını götürək, çünki sazlama vaxtına qədər sintetik səhvlərin varlığı sazlamanı kifayət qədər qeyri-müəyyən edir. Tutaq ki, səhvlərin tapılması və düzəldilməsi ardıcıl və fasiləli yerinə yetirilir.

Sistemin vəziyyətinin sırası {n, n-1, n-2, …} səhvlərin aşkara çıxarılması prosesinə uyğun gəlir.

Analoji olaraq, sistemin səhvlərinin aradan qaldırılması prosesinə uyğun vəziyyətin {m, m-1, m-2, …} sırası ilə işarələyək.

Əgər (k-1) səhvi düzəlib və k səhvi hələ tapılmayıbsa, onda deyəcəyik ki, sistem (n-k) vəziyyətindədir. K səhvi tapıldıqda, lakin hələ düzəlməyibsə, onda sistem (m-k) vəziyyətindədir.

Tutaq ki, t anında sistemin vəziyyəti hər hansı təsadüfi S(t) dəyişəni ilə ifadə olunur. Esperimenti elə aparaq ki, sistemn işçi vəziyyətinin və dayanma hallarının bir-birini əvəz etməsi baş versin. S mümkün vəziyyətləri fəzada aşağıdakı kimi olar:

S = {n, m, n-1, m-1, n-2, m-2, …}

İndi isə tutaq ki, $t_1 < t_2 < \dots t_1 < \dots t$ anlarında $S(t_1)$, $S(t_2)$, $S(t_3)$ … $S(t_1)$….S(t) təsadüfi kəmiyyətləri ∀l üçün aşağıdakı bərabərlikləri ödəyir:

$P\{S(t)=r/\ S(t_1)=r-1,\ S(t_{1-1}) = r-2, \dots S(t_1)=r-1\} = P\{S(t)=r/\ S(t_l)=r-1\}$,

burada, r, r-1, r-2, …r-l (n-k), (m-k+1), (n-k+1), …(n-2), (m-1), (n-1), m, n vəziyyətlərinin ardıcıllığına uyğun gəlir.

Beləliklə, baxılan modelin ixtiyari vəziyyəti $\{P_{ij}\}$ keçid ehtimallarının sırası ilə müəyyən olunurlar. Burada P_{ij} – sistemin i vəziyyətindən j vəziyyətinə keçməsinin ehtimalıdır.

(n-k) vəziyyətindən (m-k) vəziyyətinə keçmə ehtimalı $\lambda_{n-k}\,\Delta t$-dir, k = 0,1,2, … Analoji olaraq (m-k)-dan (n-k-1)-ə keçmə ehtimalı $\mu_{n-k}\,\Delta t$-dir, k = 0,1,2, … Keçidin λ_j və μ_j intensivliyi sistemin cari vəziyyətindən asılıdır.

PT sistemləri üçün λ_j - səhvlərin əmələ gəlmə intensivliyi, μ_j isə səhvlərin aradan götürülmə intensivliyidir.

Buradan sistemin keçid ehtimallarının tam matrisasını alarıq :

$1-\lambda_n \Delta t$ $\lambda_n \Delta t$ 0 0 … … … 0 … 0 … 0

0 $1-\mu_m \Delta t$ $\mu_m \Delta t$ 0 … … … 0 … 0 … 0

0 0 $1-\lambda_{n-1} \Delta t$ $\lambda_{n-1} \Delta t$ …. 0 … 0 …. 0

……………………………………… …… ……………….. …. ..

…………………………………………………………………..

0 0 0 … … $1-\lambda_{n-k} \Delta t$ $\lambda_{n-k} \Delta t$

0 0 0 … … 0 $1-\mu-_{n-k} \Delta t$

Daha sonra sistemin hazırlığı A(t) və etibarlığı R(t) üçün vəziyyətlərin ehtimallarından asılı ifadələr alaq:

$P_{n-k}(t) = P\{S(t) = n-k\};$ $k=0, 1, 2, \dots$

$P_{m-k}(t) = P\{S(t) = m-k\};$ $k=0, 1, 2, \dots$

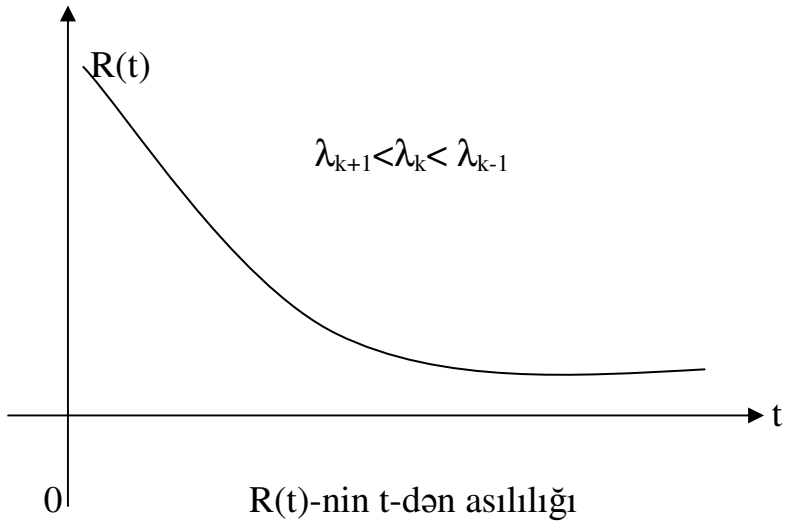
A(t) sistemin hazırlığı üçün ifadəni t ($t \geq 0$) anında (2) düsturundan istifadə edərək alırıq:

$$A(t) = \sum_{k=0}^{\infty} P_{n-k}(t) \quad (3.8.)$$

t anında sistemn hazırlığı, sadəcə olaraq sistemin işlək vəziyyətlərinin ehtimallarının toplanması vasitəsilə alınır.

Sistemin etibarlılığı onun sazlanma dərəcəsindən asılıdır, yəni, sazlanma dərəcəsi yüksək olduqca etibarlılıq da çox olur.

Əgər t anında sistem (n-k) vəziyyətində olarsa, yəni k səhvi düzəldildi və k+1 meydana çıxa bilər, bu vaxtı τ ilə işarə etsək, bu halda (5)-ə əsasən $R(t) = e^{-\lambda t}$, $\Rightarrow$ alarıq $R_k(\tau) = e^{-\lambda(k)\tau}$, $0 \le \tau \le T_{k+1}$; k= 0,1, 2, …



R(t)-nin t-dən asılılığı

Tutaq ki, səhvlərin aşkar edilməsi intensivliyi λ və aradan qaldırma intensivliyi μ, sistemin sazlanması dərəcəsindən asılı deyil, bu halda λ və μ -nün sabit halında – modelin həllini öyrənək. Aydındır ki, belə məhdudiyyət çox güclüdür, lakin dəqiq həlli olmağa imkan verir. Modelin yoxlanılması məqsədi ilə differensil tənliklər sisteminin həllini araşdırmaq lazımdır.

Modelin həlli zamanı aşağıdakı müddəalar əsas götürülür:

1. ixtiyari səhv təsadüfi hesab edilir;
2. vahid vaxt ərzində səhvlərin əmələ gəlməsi intensivliyi λ sabitdir;
3. vahid vaxt ərzində səhvlərin düzəldilməsi intensivliyi μ sabitdir;
4. sistemni bir vəziyyətdən digərinə keçid vaxtı sonsuz kiçikdir.

Markov sxemindən və λ, μ- const olduğundan model aşağıdakı kimi olar:

$$\left\{\begin{array}{l} \dfrac{d\,P_n(t)}{dt} = -\lambda\,P_n(t); \\ \dfrac{d\,P_{n-k}(t)}{dt} + \lambda\,P_{n-k}(t) = \mu\,P_{m-k+1}(t), k = 1,2,... \\ \dfrac{d\,P_{m-k}(t)}{dt} + \mu\,P_{m-k}(t) = \lambda\,P_{n-k}(t); k = 0,1,2 \end{array}\right\}$$

Fəsil 3. Komputer sistemlərində informasiyanın qorunması

3.1. Komputer şəbəkələrində dayanıqlığın və etibarlılığın göstəriciləri

Komputer şəbəkələrinin texniki və proqram təminatlarının dayanıqlılığının öyrənilməsi zəruriliyi həyati praktika ilə sübut edilmişdir. Texniki sistemlərin etibarlılığı sayəsində böyük sayda işlər görülmüşdür. Mürəkkəb sistemlərin etibarlılığını təmin edən çoxlu sayda üsullar işlənib hazırlanmışdır. Bu modellər nəinki texniki vasitələrin hazırlılığının, etibarlılıq göstəricilərini qiymətləndirir, hətta qazanılmış təcrübə nəticəsində etibarlılılq göstəricilərinin qiymətlərinin əvvəlcədən deyə də bilirlər. Bundan əlavə bəzi modellər normal işlənmə şəraitindən yayınmalar zamanı iş rejimini necə qurmağı təklif edirlər. Sistemin təmiri, normal vəziyyətə gətirilməsi yolunu öyrədirlər.

Paylanmış informasiya sistemlərinin proqram təminatının və texniki vasitələrin etibarlılığının miqdari qiymətləndirilməsi böyük əhəmiyyət kəsb edir. Bu əhəmiyyət çox vacib olur, o vaxtki real zaman rejimində böyük proqram təminatı bloklarının qiymətləndirilməsi zəruri olur.

Beləliklə, etibarlılıq nəzəriyyəsi dedikdə bir-biri ilə müəyyən alqoritmlər vasitəsi ilə qarşılıqlı bağlı olan sistemlər və elementlərdən ibarət mürəkkəb sistemlərin möhkəmliliyi nəzəriyyəsi başa düşülür. Etibarlılıq nəzəriyyəsi də bu sistemləri onların alt sistemləri və elementləri vasitəsi ilə tədqiq edir və öyrənir.

Sistemlərdə etibarlılıq o vaxt olur ki, onlar qarşıya qoyulan məsələni həll etmiş olsunlar. Əks halda, yəni qarşıya qoyulan məsələ həll edilə bilmədikdə deyirlər ki, sistem etibarsızdır, möhkəm deyil.

Proqram təminatı (PT) sistemlərində rəddetmə dedikdə proqramda buraxılmış səhv başa düşülür. Bu səhvin düzəldilməsi prosesi isə sistemin təmiri prosesi kimi başa düşülür. PT-da səhv dedikdə proqram işləyərkən bütün arzuo-

lunmayan nəticələrə gətirib çıxaran vəziyyətlər küllüsünü başa düşəcəyik (məsələn, başqa fayla müraciət, informasiyanın boş hissəsində saxlanılması və s.).

PT-nin etibarlılığı onun keyfiyyətindən asılıdır. PT-nın keyfiyyətliliyi dedikdə isə onun qarşıya qoyulmuş funksional məsələnin etibarcasına yerinə yetirmək bacarığı nəzərdə tutulur.

PT-nin keyfiyyəti aşağıdakı göstəricilərə bölünə bilər:

1.Vahid zamandakı səhvlərin sayı;

2.Səhvlər arası vaxt;

3.Hər əmrə düşən səhvlərin sayı;

4.Səhvlərin son məqsədə təsiri.

Bilirik ki, müasir komputerlər inkişaf etmiş mürəkkəb PT-a malikdirlər.

Paylanmış hesablama sistemləri etibarlılığı özündə iki aspektə malikdir:

- element etibarlılığı;
- funksional etibarlılıq.

Bunlardan birincisi texniki təminata aiddir və ənənəvi möhkəmlilik nəzəriyyəsi ilə öyrənilir.

Funksional etibarlılıq isə PT sisteminin işlənilməsinin səhvsizliyini, düzgünlüyünü göstərir. Bu anlayışların təbiətindəki fərq ondan ibarətdirki texniki təminat möhkəmliliyini öyrənən metod və üsullar PT-nın möhkəmliliyində hər zaman istifadə oluna bilmir.

Bəs sistemin funksional möhkəmliliyi nədir? Bunun üçün sistemin quruluşu anlayışını başa düşmək lazımdır.

Qurulmuş sistemin quruluşu dedikdə hər şeydən əlavə PT sisteminin modullara və modullar arasındakı əlaqlərə bölünməsi nəzərdə tutulur. Modul dedikdə, bir və ya bir neçə proqramçı üçün iş vahidi nəzərdə tutulur.

İşlənən informasiyanın gizlilik dərəcəsinə görə komputer şəbəkələri çoxsaylı siniflərə bölünərlər. Bu sinifləri üç cür qruplaşdırırlar. Üçüncü qrup isə üç Б və üç A kimi iki yerə bölünürlər, ikinci qrup isə iki Б və iki A kimi siniflərə bölünür.

Həmçinin üçüncü qrup şəbəkələr beş sinifə- bir D, bir Г, bir В, bir Б və bir А. Beləliklə, komputer şəbəkələri əsasında fəaliyyət göstərən informasiya sistemləri əlyetənliliyin sanksiyalaşdırılmasından doqquz müdafiə dərəcəsinə malik olurlar. Deməli, komputer şəbəkəsini yaradan layihəçi informasiyanın qorunması dərəcəsinə görə sistemin hansı sinifə daxil olacağını əsaslandırmalıdır. Gizlilik dərəcəsi üç B-dən bir A-ya qədər yüksələn gizlilik dərəcəsinə malik olur. İnformasiyanın qorunması sistemi ilə sanksiyalaşdırılmamış əlyetərlilikdən müdafiənin texniki-proqram və təşkilati tədbirlər vasitəsilə reallaşdırılır. İnformasiyanın qorunması sisteminin aşağıdakı 4 altsistemini xüsusi qeyd etməliyik:

- əlyetənliliyin idarə edilməsi altsistemi;
- qeydiyyat və uçot altsistemi;
- kriptoqrafik (şifrələmə) altsistemi;
- tamlılığın təmin olunması altsistemi.

1999-cu ildə İSO beynəlxalq standartlaşdırma təşkilatı " İnformasiya texnologiyalarının təhlükəsizliyinin ümumi kriteriyaları" satndartı qəbul edilmişdir. " İSO/İEC 1548: 1999- informasiyanın qorunması üsul və vasitələri - İT-nin təhlükəsizliyinin qiymətləndirilməsi kriteriyaları " satandartına görə komputer şəbəkələrinin təhlükəsizliyinə qoyulan tələblər iki qrupa bölünmüşdür:

- informasiya texnologiyalarının təhlükəsizliyini təmin edən funksionallıq;
- funksional tələblərin reallaşdırılmasının düzgünlüyünü və effektivliliyini qiymətləndirən təminatlara tələblər.

Komputer şəbəkələrinin müdafiəsinin təhlilinə daha yaxın yanaşma Britaniya standartı olan BS 7799 " İnformasiya təhlükəsizliyinin idarəedilməsinin praktik qaydaları″ 1995-ci ildə yaradılmışdır. Məqsəd müxtəlif təyinatlı informasiya sistemlərinin informasiya təhükəsizliyi ilə təmin etmək üçün olan təcrübənin ümumiləşdirilməsidir. Bu standart 2000-ci ildə daha yeni İSO 1799 standartının qəbul edilməsinə xidmət etmişdir.

Komputer şəbəkələrində informasiya sistemlərinin daha yüksək səviyyəli təhlükəsizliyini təmin etmək aşağıdakı tədqiqatların aparılmasını zəruri edir:

- informasiya sisteminə təhlükə yarada bilən bütün risklərin identifikasiyası;
- idendifikasiya edilmiş informasiya sistemlərinin resurslarının uzlaşdırılması;
- təlükələrin identifikasiyası və onların səviyyəsinin qiymətləndirilməsi;
- əks tədbirlərin effektivliliyinin təqdimatı;
- informasiya sistemlərinin informasiya təhlükəsizliliyinin təminatına çəkilən xərclərin dəyərləndirilməsi.

İnformasiya sistemlərinin təhükəsizliyinin tədqiqatının tam metodikası-CRAMM sistemin təhlilinin üç mərhələsini nəzərdə tutur:

1. Birinci mərhələdə informasiya sisteminin modelinin və resurslarının identifikasiyası həyata keçirilir. Bu mərhələ aşağıdakı məsələlərin həllini özündə birləşdirir:

- informasiya sisteminin tədqiqinin sərhədlərinin müəyyən edilməsi;
- informasiya sistemlərinin resurslarının(hard, data, soft) identifikasiytası;
- təhlükəsizliyi təsvir edən informasiya sisteminin modelinin yaradılması;
- resursların qiymətliliyinin müəyyən edilməsi;
- hesabatın yazılması və onun sifarişçi tərəfindən qəbulu;

İkinci mərhələdə informasiya sistemlərinə təhlükə və uzlaşmalar təhlili edilir. Bu mərhələ aşağıdakı məsələləri əhatə edir:

- informasiya sisteminin müəyyən resurslarında istifadəçi servisin asılılığının qiymətləndirilməsi;
- təhlükələrin və uzlaşmaların səviyyəsinə uyğun qiymətlənidirilmənin aparılması;
- risklərin səviyyələrinin hesabatının aparılması;

3. 3-cü mərhələdə əks tədbirlər seçilir. Bu tədbirlər informasiya sisteminin təhlükəsizliyinə təhlükələrin qarşısını almaq üçün reallaşdırılır.

Avtonom şəbəkələrə qoşulan şəbəkələr regional şəbəkələr olaraq fəaliyyət göstərirlər. İnternetin ən vacib parametrlərindən biri şəbəkənin ehtiyatlarını əldə etmək sürətidir. Sürət şəbəkədə avtonom sistemlər arasındakı əlaqə kanallarının buraxma bacarığından asılıdır. Modem birləşmələri üçün kanalın ötürücülük qabiliyyəti saniyədə 19,2-57,6 Kbitdir, lokal şəbəkədə isə saniyədə 64 Kbitdən - 2 Mbitə qədərdir. Peyk və intiqal kanallarda isə saniyədə 2 Mbit və ondan yuxarıdır.

İnternet tipli şəbəkələrdə informasiyanın təhlükəsizliyi ən vacib problemlərdən biridir. Bu sistemdə maliyyə əməliyyatları, əmtəə sifarişi, kredit kartlarından istifadə, qapalı informasiya resurslarından istifadə, məxfi telefon danışıqlarından istifadə və s. problemlər İnternetdə informasiyanın qorunmasını vacibləndirən şərtlərdir. İnformasiyanın təhlükəsizliyinin müəyyən səviyyəsini əldə etmədən qlobal şəbəkədə iş hər cür hərc-mərcliyə gətirib çıxara bilər. Adətən şəbəkədə nəqliyyatçılar onların məntəqəsindən keçən informasiyanı izləmirlər, ola bilər ki, informasiya seli başqa «məntəqə» və ya «şəxs»lər tərəfindən oğurlansın. Həmçinin informasiya seli dəyişdirilə bilər, ünvana başqa formada ötürülə bilər. çox təəssüflər olsun ki, İnternetin quruluşu həmişə belə məsələlərin baş verməsinə imkan yaradır.

Ona görə də İnternetdə informasiyanın zəruri qorunma səviyyəsi isə sistemin səmərəliliyi arasında bir problem var. Çox hallarda təhlükəsizlik və etibarlılıq orqanları sistemin səmərəli fəaliyyətinə mənfi təsir edən məcburi məhdudiyyətlər ortaya atırlar.

Lakin kriptoqrafiya vasitələri informasiyanın qorunması səviyyəsini yüksəltsələr də, sistemin səmərəli fəaliyyətinə az təsir etmiş olurlar.

Paylanmış informasiya şəbəkələrində - İnternetdə informasiyanın qorunması problemlərini üç qrupa bölmək olar:

- informasiyanın oğurlanması, tutulması – bu zaman informasiyanın tamlığı saxlanılır, lakin onun ötürülmə ünvanı dəyişdirilir;

- informasiyanın modifikasiyası – başlanğıc məlumatlar ya qismən dəyişdirilir, ya da tam dəyişdirilir və ünvana göndərilir;
- informasiyanın müəllifinin dəyişdirilməsi. Bu problem çox ciddi nəticələrə gətirib çıxara bilər. Məsələn, kimsə Sizin adınızdan məktub göndərərək özünü elektron mağaza kimi təqdim edib əmtəə sifariş verər, kredit kartın nömrələrini təqdim edə bilər, lakin heç bir əmtəə göndərməz.

Yuxarıda sadalanan problemlərlə əlaqədar təhlükəsizliyin təmini aşağıdakı üç müxtəlif xarakteristikaların küllüsünü təhlil etməyi nəzərdə tutulur:

1. Autentifikasiya - bu sistemin istifadəçisinin tanınması və ona müəyyən hüquqların və səlahiyyətlərin verilməsi prosesidir. Hər dəfə autentifikasiyanın səviyyəsi və keyfiyyətindən söhbət getdikdə, sistemin kənar şəxslər tərəfindən bu səlahiyyət və hüquqlardan istifadə edə bilməməsi və onlardan qorunma səviyyəsi başa düşülür.
2. Tamlıq – verilənlərin öz informasiya dolğunluğunu və birqiymətli interpretasiya olunmaq qabiliyyətini özündə saxlamaq vəziyyəti başa düşülür. Xüsusi halda bu ötürülən və alınan informasiyanın eyniliyini, uyğunluğunu təmin etmək deməkdir.
3. Gizlilik – informasiyanı icazəsiz əldə etmək, adətən məlumatın ötürülməsi zamanı onun kənar şəxs və ya ünvan tərəfindən oğurlana bilməməsi başa düşülür.

Gizliliyi təmin etmək üçün kodlaşdırma və kriptoqrafiyadan – şərti işarələrdən istifadə etmək – istifadə olunur. Bu imkan verir ki, informasiya kodlaşmış şəkildə şəbəkəyə ötürülür və uyğun açarı olmayan onu əldə edə bilmir. Kodlaşdırmanın əsasını iki əsas anlayış təşkil edir: alqoritm və açar. Alqoritm ilkin məlumatı kodlaşdırır və nəticədə ünvana kodlaşdırılmış informasiya daxil olur ki, bunu da - əgər açar varsa – interpretasiya edərək qəbul edirlər.

Məlumatın kodlaşdırılması üçün alqoritm kifayət edir. Ancaq kodlaşdırma zamanı açarın istifadəsi iki qiymətli üstünlüyə malik olmağa imkan verir:

- eyni bir alqoritmi müxtəlif açarlarla müxtəlif ünvanlara göndərmək olar;
- əgər açarın gizliliyi pozularsa, onu asanca dəyişmək olar ki, bu zaman kodlaşdırma alqoritmi dəyişməsin.

Beləliklə, kodlaşdırma sisteminin təhlükəsizliyi istifadə olunan açarların gizliliyindən daha çox asılıdır, nəinki kodlaşdırma alqoritminin gizliliyindən. Hər hansı bir alqoritm üçün açarların mümkün variantlarının sayı açardakı bitlərin sayından asılıdır. Məsələn, 8 bitlik açar 256 (2^8) açarlar variantlarına malikdir.

İndiki zamanda şəbəkə texnologiyalarının sürətli inkişafı ilə əlaqədar olaraq avtomatlaşdırılmış autentifikasiyadan hər yerdə geniş şəkildə istifadə olunur.

Kompüterlərin bir – birini "tanıma" əməliyyatı açıq-bağlı açar texnologiyasına (public-private key encryption) əsaslanan kripto sistemlə təmin olunur. Bu sistemdə iki təşkil olunan bir açar cütü mövcuddur. Bunlardan açıq açar (public key) hər kəsə məlum olan və göndərilən məlumatın şifrələnməsində istifadə olunan rəqəmsal açardır. Ancaq, açıq açar ilə şifrələnən məlumat yalnız bu açarın digər cütü olan "bağlı açar" (private key) tərəfindən açıla, yəni deşifrələnə bilər. Bağlı açar da yalnız məlumatı göndərənə məlum olduğuna görə onun etibarlılığı təmin olunmuş olur. Məsələn, siz sizə məlumat göndərmək istəyən birinə öz açıq açarınızı göndərirsiniz. Qarşı tərəf bu açardan istifadə edərək məlumatı şifrələyir və sizə göndərir. Şifrələnən məlumat yalnız sizə məlum olan bir açar, yəni bağlı açar tərəfindən açılıb oxuna bilər. Verilənlərin mübadiləsi zaman istifadə olunan şifrələmənin gücü açarın uzunluğundan asılıdır.

Açarın uzunluğu məlumatların mühafizəsi üçün çox önəmlidir. SSL protokolunda 40 bit və 128 bitlik şifrələnmədən istifadə olunur. 128 bitlik şifrələnmədə 2128 dəyişik açar vardır və bu şifrənin açılması üçün böyük bir maliyyə vəsaitlərinə və zamana ehtiyac duyulur. Pis niyyətli bir insanın 128 bitlik şifrəni açа bilməsi üçün 1 milyon dollarlıq vəsait qoyduqdan sonra 67 ilə qədər

zaman müddətində xərcləməsi tələb olunurdu. Bu misaldan aydın olur ki, SSL etibarlı sistemi tam və dəqiq bir mühafizəni təmin edir.

SSL protokolun geniş yayılma səbəblərindən biri də odur ki, o, bütün məşhur brauzer və Veb-serverlərin aparıcı tərkib hissəsidir, yəni faktiki olaraq hər bir kart sahibi İnternetə standart çıxış vasitələrindən istifadə edir və bu zaman SSL protokolundan istifadə etməklə tranzaksiyaları həyata keçirmək imkanı əldə edir. SSL protokolunun üstünlüyü onun sadəliyi və yüksək əməliyyat göstəriciləri (tranzaksiyanın reallaşma sürəti), həmçinin onun məlumtların ötürülməsi zamanı eyni kriptodavamlılıq səviyyəsində assimetrik alqoritmlərə nisbətən 2-4 dəfə tez işləyən simmetrik şifrələmə alqoritmlərindən istifadə etməsidir.

SSL protokolu bir sıra çatışmazlıqlara da malikdir. SSL protokolundan istifadəni məhdudlaşdıran əsas iki mənfi cəhət bunlardır:

- Ondan istifadənin klassik variantında istifadəçilərin mobilliyinə nail olunmur və autentifikasiyanı həyata keçirməkdə əsas faktor olan istifadəçinin sertifikatından bağlı açarın oğurlanması təhlükəsi mövcud olur;
- Onun istifadəsinə əsaslanmış elektron kommersiya protokolları İnternet mağaza tərəfindən müştərinin autentifikasiyasını dəstəkləmir, belə ki, bu cür protokollarda müştərinin sertifikatlarından demək olar ki istifadə edilmir.

SSL sxemlərində müştərilər tərəfindən "klassik" sertifikatlardan istifadə praktiki olaraq faydasızdır. Müştəri tərəfindən məşhur sertifikasiya mərkəzlərinin birindən əldə edilmiş bu cür sertifikat yalnız müştərinin adına və çox nadir hallarda onun şəbəkə ünvanına malik olur. Müştərilərdən çoxu dinamik İP ünvana malik olurlar. Bu şəkildə sertifikat tranzaksiyaların keçirilməsi ticarətdə az faydalıdır, çünki, asanlıqla cinayətkarlar tərəfindən əldə edilə bilər. Müştərinin sertifikatının ticarət nöqtəsi üçün hər hansı bir əhəmiyyətə malik olması, onun müştərinin kart nömrəsi ilə onun bank emitenti arasında əlaqə yaratması zəruridir. Bununla belə, sertifikata malik olan kart sahibinin alış üçün müraciət etdiyi istənilən İnternet-mağaza özünün xidmətedici bankın köməyindən istifadə etməklə bu əlaqəni

yoxlamaq imkanına malik olmalıdır. Başqa sözlə, bü cür sertifikat müştəri tərəfindən özünün bank emitentindən əldə edilməlidir. Bu halda sertifikatın formatı, sertifikatda kartın nömrəsinin gizlədilməsi (aydındır ki, kartın nömrəsi sertifikatda açıq şəkildə görünməməlidir), sertifikatların yayılma və geri çağırılma prosedurları və bir sıra digər hallar tranzaksiyanın bütün iştirakçıları arasında müzakirə edilməlidir. Başqa sözlə desək, sertifikasiya mərkəzlərinin iyerarxik infrastrukturunun yaradılmasına ehtiyac vardır. Bu cür infrastruktur yaradılmadan tranzaksiyanın bütün iştirakçıları arasında qarşılıqlı autentifikasiyadan söhbət gedə bilməz.

SSL sxemlərində müştərinin autentifikasiyasının yoxluğu bu protokolun ən böyük çatışmazlığıdır və bu çatışmazlıq cinayətkarlara sadəcə olaraq kartın rekvizitlərindən xəbərdar olmaqla tranzaksiyanı uğurla həyata keçirməyə imkan verir. Bu əsasən SSL protokolunun xidmətedici bank tərəfindən müştərinin autentifikasiyasını həyata keçirməyə imkan vermədiyini nəzərə aldıqda baş verir.

Bütün bunlara baxmayaraq SSL protokolunun kifayət dərəcədə geniş tətbiq sferası mövcuddur. SSL protokolu daha çox Veb-brauzerlərlə Veb-serverlər arasında məlumatların mübadiləsinin mühafizəsi məqsədilə istifadə olunur. Bu mühafizə protokolunun əsas təyinatı aşağıdakılardna ibarətdir:

- Serverin autentifikasiyası – bu istifadəçilərə onların həqiqətən də istədikləri Veb-düyünü ziyarət etdiklərinə zəmanət verir;
- İnformasiyanın serverlə brauzer arasında kodlaşdırılmış şəkildə ötürülməsinə imkan verən mühafizə edilmiş kanalın yaradılması. Bu ötürülmə zamanı informasiyanın təhrif olunmasının qarşısını alır.
- Verilənlərin tamlığı.

Ötürülən informasiya hətta kodlaşdırılsa belə, yenə də təhlükəsizlik problemindən yaxa qurtarmaq çətindir. Çünki, hər halda, ilkin informasiyanın dəyişilməsi ehtimalı qalır. Bunun qarşısının alınması yollarından biri də elektron imza üsuludur. Məzmunu onunla bağlıdır ki, ünvana informasiyanın qısa xülasəsi

«nəzarətedici cəm» də ötürülür. Bəzən bu cəm «daycest» də adlanır. Daycest, adətən, qeyd olunmuş uzunluqda olan informasiyanın qısa xülasəsi kimi başa düşülür. Nəzarətedici cəmin hesablanması, alqoritmi hər bir unikal məlumat üçün unikal qiymət müəyyən edir. Bu cəm elektron imzaya daxil edilir və bunula da informasiya alanın ötürənin həqiqi müəllifliyinə inamı artır.

Şəbəkələrdə informasiyanın qorunmasının təşkili komponentlərindən ən vaciblərindən biri də autentifikasiyadır. Şəbəkə ehtiyatlarından istifadə edərkən, hər şeydən əvvəl müəyyən etmək lazımdır ki, «bu o resursdurmu?» Hər hansı bir resursa sorğu zamanı cavabı təqdim edən server əvvəlcə autentifikasiya serverinə müraciət edir. Müsbət cavabdan sonra istifadəçiyə sorduğu məlumat təqdim edilir. Autentifikasiya zamanı «o nə bilir» prinsipi ilə işlənilir, yəni istifadəçi parolu bilirmi? Əlavə xərc tələb etməyən, lakin kifayət qədər yüksək səviyyəli qorumağa malik sadə sistemlərdən biri də S/Key sistemidir. Bu sistem vasitəsilə birdəfəlik parolların təqdim olunma prosesini göstərmək mümkündür. S/Key sistemi vasitəsilə autentifikasiyada iki tərəf – istifadəçi və server iştirak edir. Server istifadəçinin kompüterinə dəvət göndərir, bu dəvət açıq tipli olur. Əgər server istifadəçidən cavab alırsa, onu yoxlayır və idarəetməni istifadəçinin tələb etdiyi serverə göndərir.

Autentifikasiya istifadəçi tərəfindən təqdim edilən identifikatorun əsl (həqiqi) olmasının yoxlanması prosesidir. Autentifikasiya (ingiliscə authentication) – real, həqiqi, müəllif anlamlarını verir.

Qədim zamanlardan insanlar qarşısında mürəkkəb bir məsələ dürürdü – vacib bir məlumatın dəqiqliyinə əmin olmaq. Bu məqsədlə müxtəlif formalı möhürlərdən, danişiq vaxtı deyilən parollardan istifadə edilirdi. Mexaniki qurğulardan istifadə etməklə autentifikasiya üsullarının yaranması bu problemi müəyyən qədər aradan qaldırdı (məsələn, müxtəlif qıfılların və açarların hazırlanması, yazılan müəyyən şriftlərlə kodlaşdırılaraq yazılması və s.). Autentifikasiya misal kimi yaşından asılı olmayaq bütün insanlar tərəfindən sevilə-

sevilə oxunan “Əlibaba və qırx quldur” nağılını göstərmək olar. Quldurlar sadə bir sözdən (“Sim-Sim açıl”) istifadə etməklə iri bir qayanı yerindən oynadırdılar.

Aşağıda adları sadalanan İnternet-servislərə daxil olduqda autentifikasiya tələb olunur:

- Elektron poçt;
- Veb-forum;
- Sosial şəbəkə;
- İnternet-bankinq;
- Ödəmə sistemləri;
- Korporativ saytlar;
- İnternet-mağazalar.

Autentifikasiyanın müsbət nəticələrindən biri istifadəçinin müəlliflik huqunun tanınmasıdır. Yəni istifadəçiyə ona tapşırılmış müəyyən məsələlərin həll edilməsi üçün bu məsələlərin həllində istifadə olunacaq vəsait mənbəyindən istifadə hüququnun verilməsidir. Resursun vacibliyindən və ona yaxınlaşma (daxil olma) üsullarından asılı olaraq autentifikasiyanın müxtəlif üsulları istifadəçilərə təqdim edilir.

Rus dilində termin əsasən informasiya texnologiyalarında istifadə edilir. Bu baxımdan sistemin təhlükəsizlik siyasətinin həyata keçirilməsi və inamın (etibarın) yerinə yetirilməsi bir tərəfli və ya qarşılıqlı ola bilir. Bütün bunlar kriptoqrafiyanın köməkliyi ilə yerinə yetirilir.

Autentifikasiyanı müəlliflik (subyektə müəyyən hüququn verilməsi) və identifikasiya (subyektin ona məxsus identifakatoru ilə tanınması) ilə qarışıq salmaq olmaz.

Autentifikasiyaya aşağıda verilənlərin həqiqiliyinin sübut edilməsi prosedurlarını aid etmək olar. Məsələn:

-İstifadəçinin həmin şəxs olduğunun yoxlanması. Bunun üçün verilənlər bazasındakı parol ilə istifadəçinin parolu tutuşdurulur;

-Yola salınmış elektron məktubların həqiqiliyinin yoxlanması. Bunun üçün göndərənin ona məxsus açarı ilə məktubun rəqəmsal imzası tutuşdurulur;

-Faylların kontrol məbləğləri ilə müəliif tərəfindən təqdim edilmiş faylların məbləqləri tutuşdurulur.

3.2. Kompüter şəbəkələrində təhlükələrin təhlili

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

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

- İnformasiyanın konfidensiallığının pozulmasına yönələn təhlükələr;
- İnformasiyanın bütövlüyünün pozulmasına yönələn təhlükələr;
- Əlyetənliyin pozulmasına yönələn təhlükələr (DoS hücumlar, Denial of Service - xidmətdən imtina).
- Konfidensiallıq informasiyanın subyektiv müəyyən olunan xassəsidir. Verilən informasiyaya müraciət icazəsi olan subyektlərin siyahısına məhdudiyyət qoyulmasının zəruriliyini göstərir. Konfidensiallığın pozulmasına yönələn təhlükələr məxfi və ya gizli informasiyanın üstünün açılmasına yönəlib. Belə təhlükələrin reallaşması halında informasiya ona müraciət icazəsi olmayan şəxslərə məlum olur.
- Bütövlük - informasiyanın təhrifsiz şəkildə mövcudolma xassəsidir. İnformasiyanın bütövlüyünün pozulmasına yönələn təhlükələr onun dəyişdirilməsinə və ya təhrifinə yönəlib ki, bunlar da onun keyfiyyətinin pozulmasına və tam məhvinə səbəb ola bilər. İnformasiyanın bütövlüyü

bədniyyətli tərəfindən qəsdən və ya sistemi əhatə edən mühit tərəfindən obyektiv təsirlər nəticəsində pozula bilər.

- Əlyetənlik – yolverilən vaxt ərzində tələb olunan informasiya xidmətini almaq imkanıdır. Həmçinin əlyetənlik – daxil olan sorğulara xidmət üçün onlara müraciət zəruri olduqda uyğun xidmətlərin həmişə hazır olmasıdır. Əlyetənliyin pozulmasına yönələn təhlükələr elə şəraitin yaradılmasına yönəlib ki, bu zaman müəyyən qəsdli hərəkətlər ya sistemin iş qabiliyyətini aşağı salır, ya da sistemin müəyyən resurslarına girişi bağlayır.
- Təhlükələr digər əlamətlərinə görə də təsnif oluna bilər:
- Baş vermə ehtimalına görə (çox ehtimallı, ehtimallı, az ehtimallı);
- Meydana çıxma səbəblərinə görə (təbii fəlakətlər, qəsdli hərəkətlər);
- Vurulmuş ziyanın xarakterinə görə (maddi, mənəvi);
- Təsir xarakterinə görə (aktiv, passiv);
- Obyektə münasibətinə görə (daxili, xarici).
- Kompüter server tipini seçdikdə əsas parametr kimi prosessorun tipi, əməli yaddaşın tutumu, sərt diskin tipi və tutumu, disk kontrollerinin tipi nəzərə alınmalıdır. Bu xarakteriskaların qiymətləri həll olunacaq məsələdən, şəbəkədə hesablamaların təşkil olunmasından, şəbəkənin yüklənmə dərəcəsindən, istifadə olunan ƏS-dən və digər amillərdən asılıdır.
- Serverdə əməli yaddaş nəinki öz proqramını yerinə yetirmək məqsədini güdür, həmçinin disk giriş – çıxışının buferlərini yerləşdirmək məqsədi üçün də istifadə edilir. Buferlərin optimal sayını təyin etməklə, giriş-çıxış əməllərinin yerinə yetirilmə sürətini artırmaq olar.
- Əməli yaddaşı seçdikdə nəzərə almaq lazımdır ki, orada lazımi proqram təminatı, həmçinin şərikli istifadə olunan fayllar və verilənlər bazaları yerləşməlidir.
- İST və serverlər şəbəkənin yerləşdiyi yerlərdə öz aralarında kabel şəklində olan verilənlərin ötürülmə xətti ilə birləşirlər. Kompüterlər kabelə interfeys

palatası – şəbəkə adapteri vasitəsilə birləşdirilir. Son zamanlar verilənlərin ötürülmə mühiti kimi istifadə olunan xətsiz şəbəkələr – radiokanallar meydana gəlmişdir.

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

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

əsas kabel zədələndikdə bütün şəbəkə öz işçi funksiyasını itirir; həmçinin burada bir kompüterdən digərinə göndərilən informasiya başqa kompüterlər tərəfindən də qəbul oluna bildiyi üçün fiziki səviyyədə informasiya zəif mühafizə olunur.

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

malik şəbəkələrin qurulmasının mümkünlüyüdür. Mənfi cəhəti isə, fayl-server öz iş qabiliyyətini itirdikdə, sistemə icazəsiz daxil olmanın mümkünlüyü, həmçinin server resurslarına daha yüksək tələblərin olmasıdır.

- Mərkəzləşdirilməmiş (bir səviyyəli) şəbəkələrdə xüsusi ayrılmış serverlər olmur. Şəbəkənin idarəetmə funksiyası növbə ilə bir İST – dən digər İST – yə ötürülür. Bir İST-nin resurslarından (disklər, printerlər və digər qurğular) digər İST istifadə edə bilər. Bu cür şəbəkələrdə Windows ƏS-dən istifadə etmək olar.
- Çox da böyük olmayan İST üçün bu cür şəbəkə daha səmərəlidir və real paylanmış hesablama mühitinin qurulmasına imkan verir. Mərkəzləşdirilmiş şəbəkələrə nəzərən burada proqram təminatı daha sadə olur. Burada fayl-serverdən istifadə edilməsi lazım olmur, bu da sistemin daha ucuz yaranmasına səbəb olur. Lakin bu şəbəkədə informasiyanın mühafizəsi və inzibati idarə məsələləri bir qədər zəif alınır.
- Kompüterlər arasında informasiya mübadiləsini təşkil etmək məqsədilə LKŞ-də Elektrotexnika və Radiotexnika sahəsində Beynəlxalq İnstitut (İEEE – İnstute of Electrical and Electroncal Engineers) tərəfindən hazılanmış standart protokollardan istifadə olunur.
- İEEE802.3 və İEEE802.4 standartlarında təsvir edilən və lokal şəbəkələrdə (Ethernet, Arcnet və Token Ring) istifadə olunan mübadilə protokollarına qısa nəzər salaq. Bu protokollar vasitəsilə şəbəkə kanal verilənlərinə daxil olma üsulları götərilir. Bunlar OSI modelinin kanal səviyyəsini hayata keçirirlər.
- "Ethernet" üsulu. Bu Xerox firması tərəfindən təklif edilmiş və burada "ümum şin" topologiyasından istifadə edilmişdir. Ümumi şin ilə ötürülən məlumatların sərlövhəsində ötürülən və qəbul edən mənbələrin ünvanları göstərilir.
- Bu üsul aparıcı tezliyi araşdırmaq və ziddiyitləri yox etməklə, çoxşahəli mübadilə üsuludur (CSMA/CD – Caries Sense Multiple Access with Collision Delection). Bu üsulun mahiyyəti ondan ibarətdir ki, İST yalnız o vaxt məlumatı

ötürməyə başlayır ki, kanal boş olsun, əks təqdirdə məlumatın ötürülməsi müəyyən zaman anı üçün gecikdirilmiş olacaq. Eyni zamanda verilənlərin ötürülmə imkanı avtomatik olaraq aparat üsulu ilə həyata keçirilir.

- 80-100 İST eyni vaxtda işlədikdə şəbəkənin işləmə sürəti azlır. Bu, kanalda əmələ gələn münaqişələrlə əlaqədardır.
- "Arenet" üsulu – Datapoint Corp. Firması tərəfindən təklif edilmiş və burada "ulduz" topologiyasından istifadə olunmuşdur. Bu halda bir İST –dən digər iST -ə məlumatların ötürülməsi İST-in birində təşkil edilən markerlər vasitəsilə həyata keçirilir. Məlumat ötürmək istəyən İST markerin ona gəlməsini gözləyir, göndərənin və qəbuledilənin ünvanları yazılmış sərlövhəyə malik məlumatı buna birləşdirir. Əgər İST qəbulu gözləyirsə , yenə də markerin gəlməsini gözləməlidir. Marker gəldikdən sonra məlumatlarla birlikdə gələn sərlövhə anaiiz olunmalıdır. Əgər alınan məlumatlar bu İST-ə aid olarsa,o zaman İST onu markerdən ayırır.
- "Arcnet" şəbəkəsinin avadanlıqları "Ethernet" və "Token Ring" şəbəkələrinə nəzərən daha ucuz olurlar, lakin həmin avadanlıqların etibarlılığı və məhsuldarlılığı nisbətən aşağı olur.
- "Token Ring" üsulu – "halqavari" topologiyaya malik olub İBM firması tərəfindən təklif edilmişdir. Bu firmadan başqa, bu cür şəbəkələrin avadanlıqlarını Proteon, 3 Com və Undermann – Bass firmaları, şəbəkə proqram təminatını isə 3COM, Novell və Univation firmaları istehsal edirlər. Bu üsul "Arcnet" üsuluna oxşayır. Əsas fərq ondan ibarətdir ki, burada üstünlük mexanizmi vardır. Bunun sayəsində bəzi İST digərlərinə nəzərən daha tez markeri əldə edə bilirlər və onu bir qədər özündə saxlamaq imkanına mail olurlar.
- LKŞ –də tipik proqramlardan istifadə etmək məqsədilə şəbəkədə məlumatların mübadiləsi üçün hansı protokoldan istifadə olunmasını bilmək lazımdır. Belə protokollardan bir neçəsi mövcuddur. Ən geniş yayılmış protokol-lar bunlardır.

- İPX, SPX və NETBİOS.
- İPX (İnternetwork Packet Exchange) – protokolu OSI modelinin nəqliyyat səviyyəsinin protokoludur. O, şəbəkənin aşağı səviyyələri ilə interfeysə malikdir.
- SPX (Sequenced Packet Exchange) - daha yüksək səviyyə olan seans səviyyəsinin protokoludur. O, İPX, NETBİOS (Network Basic İnput/ Output System – şəbəkə giriş-çıxış baza sistemi) protokolları əsasında yaradılmışdır. Bunun vasitəsilə OSI modelinin şəbəkə, nəqliyyat və seans səviyyələrinin funksiyaları həyata keçirilir.

Şəbəkə proqram təminatında iyerarxik (ağacabənzər) yanaşmadan istifadə edilir. Burada sərbəst səviyyələr və onlar arasındakı interfeyslər əvvəlcədən təyin olunmalıdır. Bunun sayəsində digər səviyyələrə əl dəyməmək şərtilə, ixtiyari səviyyənin proqramını təkmilləşdirmək mümkün olur. Şəbəkə proqram təminatı şəbəkənin hər xidmətinin reallaşdırılması və istifadəçinin bu xidmətdən istifadə etməsi üçün yaradılır. Şəbəkədə işləmək üçün təyin olunmuş proqram təminatı istifadəçilər tərəfindən eyni zamanda istifadə oluna bilər.

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

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

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

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

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

Kompüter virusları təxminən 1980-ci illərin əvvəllərində meydana çıxmışdır. «Kompüter virusu» termini 1984-cü ildə ABŞ-da keçirilən informasiya təhlükəsizliyi üzrə 7-ci konfransda Fred Koen tərəfindən işlədilmişdi. Kompüter viruslarının ümumi qəbul edilmiş tərifi yoxdur. Biz aşağıdakı tərifdən istifadə edəcəyik. Kompüter virusu – elə proqramdır ki, özünü təxminən bioloji virus kimi aparır: çoxalır, maskalanır və ziyanlı təsirlər göstərir (əməliyyatlar yerinə yetirir). Virusları aşağıdakı əlamətlərə görə təsnif etmək olar:

I. yaşayış mühitinə görə:
II. fayl virusları (com, exe, bat, doc virusları),
III. yükləmə virusları,
IV. makro viruslar;

- yaşayış mühitini yoluxdurma üsuluna görə: rezident və qeyri-rezident;
- əməliyyat sisteminə görə: MS-DOS virusları, Windows virusları, *NIX virusları və s.;

- destruktiv imkanlarına görə: ziyansız, təhlükəsiz, təhlükəli, çox təhlükəli;
- virus alqoritminin xüsusiyyətlərinə görə: «tələbə» virusları, kompanyon-viruslar, «soxulcanlar» (worm), «stels»-viruslar («görünməz» viruslar), «polimorf»-viruslar (özüşifrlənən viruslar), şəbəkə virusları və s.

Virusların yaradılması. Hər gün 10-15 yeni növ virus meydana çıxır. Virusların miqdarı həndəsi silsilə üzrə artır. Bunu statistika və real həyat təsdiq edir. 1990-cı ildə təxminən 500 virus, 1992-ci ildə - 3 000, 1994-cü ildə - 5 000, 1996 – 9 000, 1999 – 30 000, 2001 – 50 000, 2004-cü ildə 112 000-dən çox virus məlum idi.
Kompüter viruslarının sayının artması ilk növbədə onunla bağlıdır ki, proqramlaşdırmanı bir qədər öyrəndikdən sonra istənilən şəxs virus yaza bilər. Bu işdə ona leqal və qeyri-leqal ədəbiyyat, virusların yazılması üçün xüsusi proqram təminatı kömək edə bilər. Hətta müxtəlif mutasiya generatorları mövcuddur ki, birinci kurs tələbəsinin yaratdığı sadə virusdan onun köməyi ilə mürəkkəb virus yaratmaq olar.

Virusların yayılması. Şəbəkə və kommunikasiya texnologiyalarında hər bir yenilik virusların yaradılması və yayılması üçün yeni imkanlar, yollar açır. Yaxın vaxtlara kimi viruslar disketlər və digər daşıyıcılar vasitəsi ilə yayılırdı, İnternet viruslar üçün geniş magistral açdı. Kompüter virusları Internetdə bioloci virusların real dünyada yayıdmasından daha sürətlə yayılır. 2003-cü ildə Slammer "soxulcanı" 10 dəqiqə ərzində 75 min kompüter yoluxdurmuşdu. 1999-cu ildə ilk dəfə dünya miqyasında virus epidemiyası yaranmışdı. Melissa virusu on minlərlə kompüteri yoluxdurmuş və 80 milyon dollar ziyan vurmuşdu. Bu insidentdən sonra dünyada antivirus proqramlara böyük tələb yarandı. 2000-ci ilin mayında Melissanın rekordunu bir neçə saat ərzində milyonlarla kompüteri yoluxdurmuş I Love You! virusu təzələdi. Praktik olaraq virusla "yoluxdurmaq" mümkün ol-

mayan fayl növü qalmamışdır. Artıq mobil telefonları və proqram təminatından istifadə edən dizər qurğuları yoluxduran viruslar da sürətlə yayılır.

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

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

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

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

İmmunizatorlar. İmmunizatorların iki növü var:

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

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

3.3. Kompüter şəbəkələrində informasiya təhlükəsizliyinin təmin olunmasının texnoloji aspektləri

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

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

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

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

- təhsil fəaliyyətini koordinasiya etmək.

Qanunvericilik səviyyəsində hüquqi aktlar və standartlar xüsusi diqqətə layiqdir. Standartların arasında «Narıncı kitab», X.800 tövsiyələri, ISO 15408 («Ümumi meyarlar»), ISO 17799 standartları daha geniş yayılıb.

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

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

1. Hansı verilənləri və hansı ciddiyyətlə mühafizə etmək lazım olduğunu müəyyənləşdirmək;
2. Müəssisəyə informasiya aspektində kimin və nə həcmdə ziyan vura biləcəyini müəyyənləşdirmək;
3. Risklərin hesablanması və onların qəbuledilən səviyyəyədək azaldılması sxeminin müəyyən edilməsi;
4. Planlaşdırılan bütün texniki və inzibati tədbirlərin təsviri;
5. Baxılan proqramın iqtisadi qiymətinin hesablanması;
6. Müəssisənin rəhbərliyi tərəfindən təsdiq olunma və sənədləşdirmə;
7. Həyata keçirilmə.

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

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

Biz aşağıdakı proqram–texniki tədbirləri nəzərdən keçirəcəyik: identifikasiya və autentikasiya, icazələrin idarəolunması, protokollaşdırma və audit, kriptoqrafiya, ekranlaşdırma. İdentifikasiya və autentikasiya. İdentifikasiya (ingilis dilində identification) istifadəçiyə (və ya müəyyən istifadəçinin adından fəaliyyət göstərən prosesə) özünü adlandırmağa (öz adını bildirməyə) imkan verir.

Autentikasiya (ingilis dilində authentication) vasitəsi ilə ikinci tərəf əmin olur ki, subyekt doğrudan da özünü qələmə verdiyi şəxsdir. Autentikasiya sözünün sinonimi kimi çox vaxt "həqiqiliyin yoxlanması" işlədilir. Subyekt aşağıdakı mənbələrdən ən azı birini təqdim etməklə özünün həqiqiliyini təsdiq edə bilər:

bildiyi nəyi isə (parolu, şəxsi identifikasiya nömrəsi, kriptoqrafik açar);

sahib olduğu nəyi isə (şəxsi kart və ya digər təyinatlı analoji qurğu);

özünün tərkib hissəsi olan nəyi isə (səs, barmaq izləri və s., yəni özünün biometrik xarakteristikalarını).

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

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

- texniki məhdudiyyətlər qoyulması (parol çox qısa olmamalıdır, parolda hərf, rəqəm, durğu işarələri olmalıdır və s.)

- parolun fəaliyyət müddətinin idarə olunması, onların vaxtaşırı dəyişdirilməsi;
- parollar faylına icazənin məhdudlaşdırılması;
- sistemə uğursuz daxilolma cəhdlərinin məhdudlaşdırılması;
- istifadəçilərin təlimatlandırılması;
- parol generasiya edən proqramların istifadəsi.

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

İcazələrin idarə edilməsi. İcazələrin idarə edilməsi subyektlərin (istifadəçi və proseslərin) obyektlər (informasiya və digər kompüter resursları) üzərində yetinə yetirə biləcəyi əməliyyatları müəyyən etməyə və onlara nəzarət etməyə imkan verir. İcazələrin məntiqi idarə edilməsi (icazələrin fiziki idarə edilməsindən fərqli olaraq) proqram vasitələri ilə realizə olunur. Məsələnin formal qoyuluşuna baxaq. Subyektlər məcmusu və obyektlər toplusu var. İcazələrin məntiqi idarəolunması hər bir (subyekt, obyekt) cütü üçün yolverilən (mümkün) əməliyyatlar çoxluğunu müəyyən etməkdən və qoyulmuş qaydaların yerinə yetirilməsinə nəzarət etməkdən ibarətdir.

(Subyekt, obyekt) münasibətini cədvəl şəklində təsvir etmək olar. Cədvəlin sətirlərində subyektlər, sütunlarında obyektlər sadalanır. Sətir və sütunların kəsişdiyi xanalarda verilən icazə növləri və əlavə şərtlər (məsələn, vaxt və hərəkətin məkanı) yazılır. İcazələrin məntiqi idarə edilməsi mövzusu – informasiya təhlükəsizliyi sahəsində ən mürəkkəb mövzudur. Səbəb ondadır ki, obyekt anlayışının özü (deməli icazə növləri də) servisdən servisə dəyişir. Əməliyyat sistemi üçün obyekt fayl, qurğu və prosesdir. Fayl və qurğular üçün adətən oxuma, yazma, yerinə yetirmə (proqram faylları üçün), bəzən də silmə və əlavə etmə

hüquqlarına baxılır. Ayrıca hüquq kimi icazə səlahiyyətlərinin digər subyektlərə vermə imkanına baxıla bilər (sahiblik hüququ). Prosesləri yaratmaq və məhv etmək olar. Müasir əməliyyat sistemləri digər obyektlərin varlığını da mümkün edə bilər.

İcazə hüququna nəzarət proqram mühitinin müxtəlif komponentləri - əməliyyat sisteminin nüvəsi, əlavə təhlükəsizlik vasitələri, verilənlər bazasını idarəetmə sistemi, ara vasitəçi proqram təminatı (məsələn, tranzaksiyalar monitoru) tərəfindən həyata keçirilir. Protokollaşdırma və audit. Protokollaşdırma dedikdə informasiya sistemində baş verən hadisələr haqqında məlumatın qeyd edilməsi və toplanması başa düşülür. Audit - toplanan informasiyanın analizidir. Audit operativ (demək olar ki, real vaxtda) və ya dövri (məsələn, gündə bir dəfə) aparıla bilər. Protokollaşdırma və auditin realizə olunması aşağıdakı məqsədləri güdür:

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

Ekranlaşdırma. Ekranlaşdırma vacib təhlükəsizlik mexanizmlərindən biridir. Bu mexanizmin şəbəkələrarası ekran (ingilis termini firewall) adlanan realizələri olduqca geniş yayılıb. Ekranlaşdırma məsələsinin qoyuluşu aşağıdakından ibarətdir. Tutaq ki, iki informasiya sistemi var. Ekran - bir çoxluqdan olan istifadəçilərin digər çoxluğun serverlərinə müraciətlərini nizamlayan vasitədir. Ekran öz funksiyalarını iki sistem arasındakı bütün informasiya axınına nəzarət etməklə yerinə yetirir.

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

etdirmək üçün verilənləri növbəti süzgəcə ötürmək, adresatın adından verilənləri emal edərək nəticəni göndərənə qaytarmaq olar. Çox vaxt ekranı 7-səviyyəli OSI etalon modelinin üçüncü (şəbəkə), dördüncü (nəqliyyat) və ya yeddinci (tətbiqi) səviyyələrində realizə edirlər. Birinci halda ekranlaşdırıcı marşrutizator, ikinci halda - ekranlaşdırıcı nəqliyyat, üçüncü halda - ekranlaşdırıcı şlüz alınır. Hər bir yanaşmanın öz üstünlükləri və nöqsanları var; hibrid ekranlara da rast gəlinir, onlarda göstərilən yanaşmaların ən yaxşı cəhətlərini realizə etməyə çalışırlar.

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

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

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

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

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

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

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

Kompüter şəbəkəsinin yaranması üçün ən azı iki kompüterin bir-birinə qoşulması lazımdır. Şəbəkə harada və nə üçün istifadə olunur? sualını versəniz, bu suala indi

çox rahat cavab tapmaq olar. Məsələn, bu gün ofislərdə, nəşriyyatlarda, kompüter klublarında və ya beynəlxalq informasiya mübadilələrində kompüter şəbəkələri vacib rol oynayır. Əgər bir firmanın müdiri ümumi sənədin bütün işçilər üçün əl çatan olmasını istəyirsə, o, kompüter şəbəkəsindən istifadə edərək bu işi rahatca həyata keçirir. Nəşriyyatda işləyən dizayner öz kompüterində hazırladığı jurnalın üz qabığını çap etmədən şef redaktora göstərmək və rəyini bilmək istəyirsə, sadəcə olaraq şefin kompüterinə jurnalın üz qabığını göndərir və danışıq proqramı vasitəsi ilə onun rəyini alır. Oyun klublarında tək oynamaqdan bezən uşaqlar bir-biriləri ilə şəbəkə vasitəsi ilə oynaya bilirlər. Beynəlxalq kompüter şəbəkələri ilə xüsusi proqram təminatı ilə xaricdə yaşayan qohumlarının üzlərini kompüterdə görə və səslərini rahatca eşidə bilərlər.

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

Nəticədə PC və ya mini-computer adlandırılan bu kompüterlərin dünyadakı sayı milyonlara, milyardlara çatdı. Mainframe-lər texnologiyadakı yeniliklərə bax-

mayaraq ilk yaradıldıqları məqsədə hələ də xidmət edirlər. Müəyyən həddaxilində hesablamaya ehtiyacı olan firmalar prosessoru IBM As400 olan maşınlardan və buna bənzər mainframe sistemlərindən hələ də istifadə edirlər.

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

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

İnformasiya Cəmiyyətinin elmi-nəzəri əsaslarının tədqiqi, etibarlı, dayanıqlı və təhlükəsiz elektron idarəetmə (e-hökumət, e-bələdiyyə və s.) texnologiyalarının işlənilməsi sahəsində mühüm elmi nəticələr əldə olunmuşdur. İnformasiya cəmiyyətinin elmi-nəzəri, informasiya iqtisadiyyatı, təhsil prosesinin informasiyalaşdırılması, informasiya təhlükəsizliyi, o cümlədən, informasiya cəmiyyətinin formalaşma mərhələləri, informasiya inqilabları, informasiya ekologiyası, informasiya mədəniyyəti, informasiya menecmenti, İnternet-jurnalistikanın formalaşdırılması problemləri, İnformasiya Cəmiyyətinin onlayn monitorinqi sisteminin işlənilməsi, İnternetdən istifadənin analizi üçün metodların işlənməsi, müxtəlif təyinatlı korporativ informasiya fəzalarının (e-elm, e-mədəniyyət, e-turizm və s.) formalaşdırılması və reallaşdırılması problemləri, e-hökumət mühitində e-sənədlərin intellektual emalı və dövriyyəsi sisteminin işlənilməsi, informasiya resurslarının həyat tsiklinin idarə olunması, spamlarla mübarizə metodları, İnternet asılılığı ilə mübarizə üsullarının işlənilməsi, informasiya müharibəsi texnologiyaları, elektron demokratik təsisatların reallaşdırılması texnologiyalarının işlənməsi, e-hökumət mühitində dövlət sirrinin təmin olunması mexanizmlərinin işlənməsi, veb-resursların formalaşdırılması və

idarə olunması mexanizmlərinin işlənməsi, onlayn təhsil mühitinin formalaşdırılması və idarə olunması, ölkəmizdə İKT iqtisadiyyatının digər iqtisadi sahələrlə qarşılıqlı təsirinin araşdırılması və inkişaf tendensiyalarının modelləşdirilməsi, İnternetin tənzimlənməsi problemlərinin tədqiq olunması istiqamətində elmi-nəzəri və praktiki işlər aparılır. İnformasiya Cəmiyyəti sahəsində dövlət siyasəti istiqamətində qəbul olunmuş dövlət proqramları və qanunlarından irəli gələn məsələlərin həllində bilavasitə iştirak edilmiş, "Elektron Azərbaycan" Dövlət Proqramı çərçivəsində institutun qarşısına qoyulan məsələlərin həlli istiqamətində işlər aparılır.

N ə t i c ə

Müasir dövrün informasiya sistemlərinin ən böyük problemlərindən biri informasiyanın qorunması problemidir. Bu problem ona görə aktualdırki müasir informasiya sistemləri açıq kommunikasiya (OSİ) sistemləridir və onun milyonlarla müxtəlif səviyyəli profisional və qeyri-profisional istifadəçiləri vardır. Bu mənada tədqiqatın nəticələri olaraq aşağıdakı təklifləri diqqətinizə çatdırrıq:

-hər bir biznes-prossesdə istifadə üçün yaradılmış informasiya sistemi requlyar olaraq sistemin etibarlılığı və informasiya selində qorunma məsələlərinin aktif diqqətdə saxlanılmalıdır;

-yaradılan və istifadəyə verilən hər bir kompiter şəbbəkəsinin Azərbaycan Respublikasınının informasiya sistemlərində qorunma və müdafiə haqqındakı hüquqi sənədlərin tələblərinə uyğun olması çox vacibdir;

- informasiya sistemlərinin təhlükəsizliyini sistemin adaptasiya və funksional məsəslənin həllinin xassəsi kimi onun keyfiyyətinə təsir göstərən faktor kimi öyrənilməlidir;

- məqsədi daha çox biznes əldə etmək olan komouter şəbəkəsinin səmərəliliyinin onun etibarlıq göstəricilərindən asılı öyrənilməsi vacibdir;

İnformasiya sistemlərinin təhlükəsizlik məsəslələri üç aspektə tədqiq olunmalıdır:

- sistemdə mövcud olan informasiya bazalarının (disklərin, qovluqların, faylların və s.) tamlığının qorunması;

- informasiya massivlərinin müəlliflərinin və istifadəçilərin hüquqlarının qorunması;

- sistemdə mübadilə zamanı itkilərin, dəyişmələrin və sıradançıxmaların qarşısını alınması üçün audentifikasiya məsələlərinin həlli.

Komputer şəbəkələrində informasiyanın qorunması təhlükəsizlik siyasətinin normalarına və qaydalarına uyğun olaraq kompaniyaların və şirkətlərin ayrıca

fəaliyyət növü olmalıdır. Müasir komputer şəbəkələrində iki baza təhlükəsizlik modelləri daha geniş tədbiq olunur:

- diskretləşdirmə;

- mondatlaşdırma;

Hər iki model aşağıdakı ilkin şərtlərə söykənir:

1. Hər bir paylanmış informasiya sistemi (komputer şəbəkəsi) subyekt və obyektlərin real qarşılıqlı fəaliyyəti ilə məzmunlaşır;

2. Sistemin tələkəsizliyi subyektlərin obyektlərə əlyetənliyi ilə müəyyən edilir, burada obyektlər informasiyanı özündə əxz edən kimi təsfir olunur, subyektlər isə bu obyektlərdə prosseslәri yerinə yetirən kimi görünürlər;

3. Sistemdə subyektlər və obyektlər arasındakı qarşılıqlı əlaqələr münasibətlərin modelləşməsi yolu ilə həll edilir;

4. Obyektlər və subyektlər arasındakı münasibətlər toplusu sistemin vəziyyətinin müəyyən edir.

Beləliklə, bir daha onu öyrənmiş olduq ki, komputer şəbəkələrində təhlükəsizlik və etibarlılıq problemləri üç bir-bri ilə qarşılıqlı əlaqəsi olan məsələlərin həllini müəyyən edir: - gizlilik (konfisiallıq) ;- tamlıq ;- əlyetənlilik.

Ədəbiyyat siyahısı

1. Konğyuxovski. «Ekonomiçeskaya informatika». Piter, SPb, 2001.
2. «Ekonomiçeskaya informatika». Pod red. V.V.Evdokimova. Piter, SPb, 1997 q.
3. V.V.Şurakov. Nadejnost, proqrammnoe obespeçenie. M., 1986 q.
4. V.A.Zarenin. Nadejnost ASU. Kiev, 1986 q.
5. V.M.Qluşkov Osnovı bezbumajnoy informatiki. M., Nauka, 1982.
6. Y.Abdullayev, İ.Musayev, B.Qurbanov. Məlumat bazalarının layihələndirilməsi. Bakı, 2001.
7. Kərimov S.Q., Babanlı Ə.Y., Məmmədxanov R.Q., Vəliyev N.N., İbrahimova S.N. İnformatika üzrə rusca-ingiliscə, azərbaycanca-türkcə izahlı lüğət. Bakı, ADNA, 1996-529 s.
8. Kərimov S.Q., Rüstəmov N.S., Həbibullayev S.B., Rəhimova Y.Q. Windows sisteminin əsasları. Bakı., ADNA, 1999-180 s.
9. Norton P. Personalnıy kompyuter firmı IBM i operasionnaya sistema MS-DOS. Moskva, 1991
10. Axmetov K. Kurs molodoqo boysa. M., 1996.
11. Artamonov B.N. i dr. Osnovı sovremennıx kompyuternıx texnoloqiy. – S.Pb.: Korona print, 1998-448 s.
12. Kudrəvsyev E.M. MATNSAD 8. Simvolnoe i çislennoe reşenie raznoobraznıx zadaç. DMK, Moskva, 2000.
13. Qrızlov V.İ., Qrızlova T.P. Turbo Paskal 7.0. – M., DMK, 1998-400 s.
14. Deyt K.Vvedenie v sistemı baz dannıx. – 6-e izdanie. – K.: Dialektika, 1998 – 750 s.
15. Qluşakov S.V., Lomotko D.V. Bazı dannıx – Xarkov: Folio, 2000 – 504 s.
16. O.Yefimova, M.Moiseeva, Y.Şafrin. Praktikum po kompyuternoy texnoloqii. Moskva, 1997.
17. İnformatika. Uçebnik pod red.N.B.Makarovoy. M., 1999.

18. İnformatika – Praktikum po texnoloqii rabotı na kompyutere. Pod. red. N.V.Makarovoy. M., 2000.
19. Marçenko A.İ., Marçenko L.M. Proqrammirovanie v serede TURBO PAS-CAL 7.0. Kiev – Moskva, 1998.
20. Potemkin V.Q. Vvedenie v MATLAB. Moskva, 2000.

İstifadə olunan saytların siyahısı

1. www.info.press.ru
2. www.İKT.az
3. www.mincom.gov.az
4. www.science.gov.az
5. www.ict.az
6. www.elm.az
7. www.rabitadunyasi.info.az
8. www.mincom.gov.az
9. www.csl-az.com
1 0. www.kitab.rabita.az
11. www.microsoft.com

Резюме

Современный этап развития науки и техники во всем мире одной из наиболее динамично развивающихся информационных систем и технологий. День за днем, меняется очень быстро развивающиеся технологии и развитие компьютерных сетей для использования приводит к более из них. Управление персоналом для современного общества и глобальной экономики является ее необыкновенные функции таких систем НАДЕЖНОСТИ, эффективность очень актуальной проблемой. Нарушение любого из этих систем факторов: отказ технических средств, обслуживающего персонала, неправильных движений, изменений условий окружающей среды и так далее затрагиваются.

В настоящее время с помощью компьютерных сетей и быстрого осуществления человеческой деятельности в отдельных областях обмена информацией, электронного бизнеса, электронной коммерции, электронных платежей и т.д. осуществляется и в ущерб пользователям, меры безопасности приняты для устранения причин.

Представленные диссертационной работы являются причинами важности и актуальности проблемы информационной безопасности, возникающие угрозы, характер опасных признаках типов вопросов, функций безопасности и защиты.

Summary

The present stage of development of science and technology all over the world one of the most dynamically developing information systems and technologies. Day after day, changing very rapidly developing technologies and the development of computer networks for use leads to more of them.HR management to modern society and the global economy is its extraordinary functions of such systems RELIABILITY, efficiency is very topical issue. Violation of any of these systems factors: the failure of technical facilities, service personnel, incorrect movements, changes in environmental conditions and so on affect.

Currently, with the help of computer networks and the rapid implementation of human activity in separate areas of exchange of information, e-business, e-commerce, electronic payments, etc. carried out and to the prejudice of users, security measures are taken to eliminate the causes.

Presented dissertation work are the reasons for the importance and urgency of the problem of information security, emerging threats, the nature of the danger signs of the types of issues of security and protection functions.