AZƏRBAYCAN RESPUBLİKASI TƏHSİL NAZİRLİYİ
AZƏRBAYCAN DÖVLƏT İQTİSAD UNİVERSİTETİ

MAGİSTRATURA MƏRKƏZİ

Əlyazması hüququnda

Quluzadə Sona Fuad qızı

“İNFORMASİYA SİSTEMLƏRİNİN ETİBARLILIĞININ ƏSAS KONSEPSİYASI” *mövzusunda*

MAGİSTR DİSSERTASİYASI

İstiqamətin şifri və adı: **060509 “Kompüter Elmləri”**
İxtisasın şifri və adı: **“İqtisadi informasiya sistemləri”**

Elmi rəhbər **t.e.n Mənsimov H. İ**
Magistr proqramının rəhbəri

Kafedra müdiri **dos. Bayramov H. M**

BAKI – 2018

Mündəricat

G i r i ş

İqtisadiyyatda və cəmiyyətdə son on il ərzində informasiya texnologiyalarının rolu və əhəmiyyəti artmağa başladı. İnformasiya və kommunikasiya texnologiyaları insanların həyat fəaliyyətində özünü daha qabarıq şəkildə biruzə verdi. İnformasiya sistemləri əksər müəssisələrin əsasını təşkil edir. Demək olar ki, hər sahədə - təhsil, maliyyə, hökümət, səhiyyə, böyük və kiçik biznes təşkilatlarında informasiya sistemləri əvəzedilməz rol oynayır. Bir çox şirkət və müəssisələrin iş strategiyaları məhz informasiya sistemləri əsasında qurulmuşdur. Sistemlər banklar, onlayn səyahət agentlikləri, vergi orqanları və elektron kitabxanaların fəaliyyətində əsas pay sahibidir.

Mövzunun aktuallığı: İnformasiyanın həyatın əvəzedilməz parçasına çevrilməsinə baxmayaraq informasiya sistemlərinin inkişafı bugün bir sıra problemlə üzləşir. Ən böyük problemlərdən biri informasiya sistemlərində tez-tez sıradan çıxma hallarının müşahidə olunmasıdır. Bəzən informasiya sistemlərindən gözlənilən nəticə əldə edilmir. Böyük miqyaslı informasiya sistemlərinin uğursuzluğu medya sahəsində də əhəmiyyətli dərəcədə diqqəti cəlb etmişdir. Buna səbəb hər il informasiya sistemlərinə xərclənən milyardlarla dollar vəsaitin israf edilməsi olmuşdur. İnformasiya sistemlərinin uğursuzluğunun bir sıra fərqli səbəbləri ola bilər: büdcə və plandan kənara çıxma kimi iqtisadi uyğunsuzluqlar, zəif keyfiyyətli məhsullardan istifadə, müştəri məmmuniyyətinin kifayət qədər olmaması və s. Aparılmış sorğuya əsasən plana əsasən nəzərdə tutulmuş75% informasiya sistemi həyata keçirilməmişdir və ya alınmış hazır məhsuldan heç vaxt istifadə olunmamışdır. Digər sorğuda isə vaxtında və verilmiş büdcə planına uyğun yalnız 16% proyekt ərsəyə gətirilmişdi. Bu sorğuda iştirak edən 365 sistemin 31% tamamlanmamış və ya öncədən müəyyən səbəblərə görə istehsalı dayandırılmışdır, 53% informasiya sistemi isə tamamlanmasına baxmayaraq mövcüd büdcə planından kənara çıxmışdır. 2004-cü ildə hazırlanmış sistemlərin yalnız 29%-i özünü doğrultmuşdu. İnformasiya sistemlərinin uğursuzluğunun səbəbləri isə müxtəlif ola bilər. Tədqiqatçıların fikrincə səbəb biznes liderlərinin öhdəçiliklərini düzgün yerinə yetirməməsi, qarşılıqlı

ünsiyyət probleminin yaşanması, səhmdarların düzgün olmayan strategiyalarının olması və s. ola bilər.

İnformasiya sistemlərində sabitlik istəksiz bir şəkildə əldə edilməyən, həmçinin, hər gün yerinə yetirilməli olan "dinamik bir hadisə" kimi qəbul edilə bilər. Bu baxımdan sıradan çıxma tək bir uğursuz komponent və ya maneə səbəbindən deyil, kontekstdə gözlənilməz dəyişikliklərin baş verməsi nəticəsində əmələ gəlir. Bu işin əsas məqsədi sistemlərin iş qabiliyyətini saxlamaqla etibarlılığını təmin edilməsinin yollarını araşdırmaqdan ibarətdir.

Qəbul edilmiş proqram mühitində etibarlılığa nail olmaq üçün müəyyən edilmiş stategiyalar formal strukturlar, planlaşdırma,prosedurlara və proseslərə standartlaşdırılmış risk idarəetmə metodologiyasının tətbiqindən ibarətdir.

Tədqiqatın məqsədi etibarlı informasiya sistemlərinin müəssisələrin, hökümət qurumlarının, kommersiya təşkilatlarının inkişafına təkan verəcək amillərinin araşdırılmasıdır.

Tədqiqatın predmeti informasiya sistemləri, sistemlərin təhlükəsizlik və etibarlılıq məsələlərinin geniş şəkildə öyrənilməsidir.

Tədqiqatın nəzəri əsasları və metodoloji bazasını bir sıra yerli və xarici mənbələrə əsaslanan əsərlər təşkil edir. Dissertasiya işinin tədqiqində mühüm rol oynayan bu mənbələrdə olan məlumatlar qruplaşdırılaraq mövzunun araşdırılmasında əvəzedilməz pay sahibidir.

Elmi yenilik: İnformasiya sistemlərinin təhlükəsizlik prinsiplərinə, siyasətinə, standartlarına uyğun olan müxtəlif tip etibarlılıq modellərini analiz edərək ən müvafiq modelin seçilməsinə kömək etməkdən ibarətdir.

Nəzəri və təcrübi əhəmiyyəti: araşdırmaya əsasən informasiya təhlükəsizlik məsələləri nəzərdən keçirilərək səmərəli, sıradan çıxma intensivliyi minimum olan informasiya sistemlərinin qurulması təmin edilir. Dissertasiya işi keyfiyyətə nəzarət sahəsində bəzi etibarlılıq konsepsiyaları dərindən araşdırılmış və informasiya sistemlərinə tətbiq edilmişdir.

İşin strukturu və həcmi: Dissertasiya işi giriş, 3 fəsil, nəticə və təkliflər və ədəbiyyat siyahısından ibarətdir.

İşinin birinci fəslində informasiya sistemlərinin təhlükəsizlik prinsipləri əsasında arxitekturanın qurulma üsulları qeyd olunmuşdur. Fəsildə informasiya sistemlərinin əsas təhlükəsizlik prinsipləri, səmərəli arxitekturaya malik sistemlər haqqında məlumat verilir.

Magistr dissertasiyasının ikinci fəslində təhlükəsizlik siyasəti və standartları haqqında məlumatlar verilir, yaradılmış təhlükəsizlik modellərinin bir-birindən fərqli əsas üstünlükləri qeyd edilir.

Sonuncu fəslində etibarlı informasiya sistemlərinin əsas konsepsiyaları araşdırılmış, müvafiq modeldən istifadə olunaraq səmərəli sistemlərin davamlılığının artırılması yolları öyrənilmişdir.

FƏSİL I. İNFORMASİYA SİSTEMLƏRİNİN TƏHLÜKƏSİZLİYİ

1.1 İnformasiya təhlükəsizliyinin prinsipləri

İlk öncə informasiya təhlükəsizliyinin nə olduğunu müəyyənləşdirək. Əgər 10 müxtəlif insandan informasiya təhlükəsinin nə olduğunu soruşsaq,10 müxtəlif cavab əldə edərik ki, bu müxtəlif cavabların hamısı da düz ola bilər. Bununla belə, ümumi olaraq informasiya təhlükəsizliyinin tərifi qısa, sadədir. "İnformasiya təhlükəsizliyi informasiyanın konfidensiallığı, tamlığı və əlyetənliyin əsas məcmusundan ibarətdir" [1].

Konfidensiallıq: İnformasiya gizli qalmalı, o, ancaq istifadə səlahiyyətinə malik insan tərəfindən istifadə olunmalıdır. Hələ qədim zamanlardan insanlar biliyin güc demək olduğunu, məlumata sahib olmağın hər şeydən mühüm olduğunu bilirdilər. Konfidensial informasiyaya icazəsiz daxil olmaq milli təhlükəsizlik proqramlarında, kommersiyada, sənayedə dağıdıcı nəticələrə səbəb ola bilər. İnformasiya sistemlərinin konfidensiallığının qorunmasının əsas mexanizmi kriptoqrafiya və giriş idarəetmələridir. Konfidensial təhlükələrə misal olaraq pis niyyətli yazıları, təhlükəli şəbəkələri, zəif idarəetməyə malik olan sistemləri göstərə bilərik.

Tamlıq informasiyanın etibarlı, orjinal, düzgün, təhrif olunmamış şəkildə saxlanılması, eləcə də yanlış və icazəsiz şəkildə dəyişdirilməməsi bacarığını özündə saxlayır. İnformasiya təhlükəsizliyi konteksində tamlıq təkcə informasiyanın tam olmasına deyil, həm də dəqiq və əsl olmasına istinad edir. Tamlığı qoruma mexanizminin 2 tipi vardır:

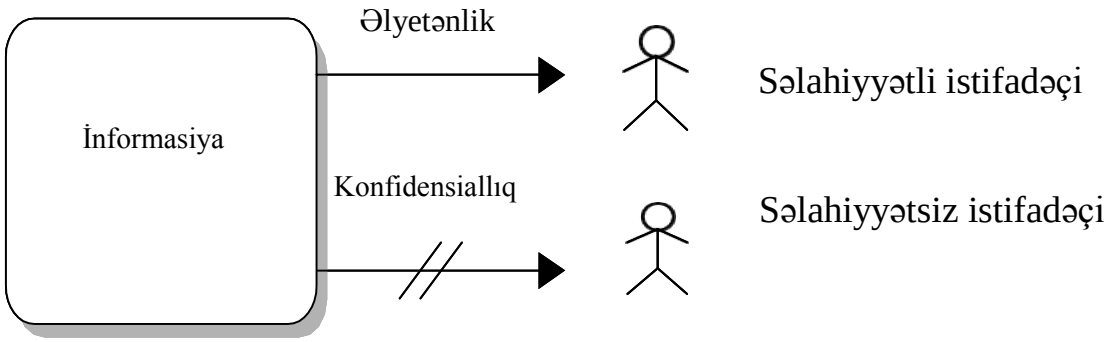
- icazəsiz informasiyanın dəyişdirilməsi qarşısını alan önləyici mexanizm;
- mexaniz önləyici mexanizmin çökməsinə səbəb olan icazəsiz dəyişmələri aşkar edən dedektiv mexanizmi.

Əlyetənlik informasiya təhlükəsizliyinin ən vacib sütunlarından biridir, konfidensiallıq və tamlıq kimi ən mühüm və lazımlı komponentidir. Əlyetənliyə qarşı

hücumlar DOS hücumları kimi tanınır. Təbii və insan tərəfindən həyata keçirilən süni hücumlar informasiya əlyetənliyinə təsir edir. Hər iki vəziyyət üçün isə hücum bərpa planları (daimi və etibarlı sürət çıxarma) itkilərin həcmini minumumlaşdırmağa yönəlmişdir [1].

Konfidensiallıq məlumatlardan icazəsiz istifadənin qarşısının alınmasıdır. İnformasiyanın tamlığında bütün diqqət icazəsiz və ya istəksiz dəyişdirilməyə, silinməyə yönəldilir.

Əlyetənliyin əsas məqsədi isə icazəli şəxslərin verilənlərdən rahatlıqla istifadəsini təmin etməkdir.



Tamlıq

Sxem. İnformasiya təhlükəsizliyinin 3 əsas prinsipinin qrafiki təsviri.

Konfidensiallıq, tamlıq və əlyetənlik ilə yanaşı identifikasiya, autentifikasiya, avtorizasiya əməliyyatları, metodları informasiya təhlükəsizliyinin təmin edilməsində mühüm rol oynayan konsepsiyalardır [3].

İdentifikasiya müəyyənləşdirmək-təsdiqləmək-icazə vermək(identify–authenticate –authorize) ardıcıllığının ilk addımı olub, hər gün informasiya və informasiya mənbələrinə hesabsız sayda insan və ya kompüterlərin girişini təmin edir. Bəzi identifikasiya sistemləri kimin və ya nəyin müəyyənləşdirilməsinin 3 fərqli xüsusiyyətinə: əhatə dairəsi, yeri və unikallığına görə bir-birindən fərqlənirlər.

İdentifikasiya əhatə dairəsinə görə lokal və qlobal ola bilər. Bu konseptin mahiyyətini internetdəki mail adresləri vasitəsilə izah edək. İnternetdə dünyanın

müxtəlif yerlərindən *jack* adında maillər ola bilər, lakin *jack* company.com şirkətində işləyən jack adlı istifadəçinin olduğunu müəyyən edir. Eyni sistemdə iki eyni adlı istifadəçi hesabı yaratmaq olmaz. Buna səbəb onların hansı icazələrə sahib olduqlarını ayırd edə bilməməklə yanaşı, həm də onlara qoyulan tələblərlə bağlıdır[3].

Təhlükəsizlik məqsədilə unikal ad tələb olunandır və əhatə dairəsindən asılı olaraq lokal unikal və mümkün qədər qlobal unikal olmalıdır ki, bu adlara əsaslanaraq hesablar yaratmak mümkün olsun.

İdentifikasiyadan sonra avtorizasiya mərhələsindən əvvəl həyata keçirilən autentifikasiya mərhələsində identifikasiya mərhələsində elan edilmiş kimlik yoxlanılaraq təsdiq edilir. Başqa sözlə, bu mərhələdə sistemə daxil olmaq istəyən şəxsin həqiqiliyi sübut olunur. Autentifikasiyanın 3 metodu vardır:

- What you know (nə bilirsən) metodu;
- what you have (nəyə sahibsən) metodu;
- what you are (kimsən) metodu.

İstifadə olunan metodlardan asılı olmayaraq əsas hədəf şəxsin kimliyinin təsdiq olunmasında məqbul əminlik əldə etməkdir. Müxtəlif autentifikasiya metodları xüsusiyyətlərinə və qiymətlərinə görə bir-birindən fərqlənirlər. Bu səbəbdən də bütün faktorları yaxşı araşdırıb lazımı modeli seçmək lazımdır.

What you know autentifikasiya metoduna parollar, açar ifadələr, gizli kodlar və şəxsi identifikasiya nömrələri (personal identification numbers-PİNs) daxildir. Ən çox istifadə edilən bu model həm ucuzdur, həm də informasiya sistemlərinə tətbiqi rahatdır. Lakin yüksək təhlükəsizlik tələb olunan sistemlərdə bu model təkcə istifadə olunmur.

Ən geniş yayılmış *What you have* autentifikasiya metodu tətbiq edilən informasiya sistemindən istifadə edən şəxs smart kartlar (smart cards), USB portları kimi bir sıra açarlara sahib olmalıdırlar. Şübhəsiz ki, eyni risklər bu metoddan istifadə zamanı da baş verə bilər, kartlar oğurlana, itirilə və ya korlana bilər. Bu

metoda hər bir istifadəçiyə xas əlavə dəyər də daxildir. Parolla müqayisədə bu metodun tətbiqi nəzərə çarpacaq qədər baha başa gəlir.

What you are metodu biometrik autentifikasiya metodlarına istinad edir. Biometrik metod istifadəçinin kimliyini müəyyən etmək üçün insanın fiziki və ya davranış xüsusiyyətlərinə əsaslanaraq şəxsin kimliyini təsdiq edən metodlardır. Biometrik metodlara barmaq izi, gözün tanınması, eləcə də səs, imza tanınması daxildir. Bu metodlar digər 2 metodla müqayisədə daha az istifadə olunur, lakin tətbiq edildiyi zaman isə yüksək səviyyəli təhlükəsizlik əldə olunur. Digər iki metoddan fərqli olaraq bu modelin qurulması, konfiqurasiyası, tətbiqi daha çox zəhmət tələb edir [5].

Güclü autentifikasiya əldə etmək üçün smart kart və PİN, parol və barmaq izi kimi 2 və daha artıq müxtəlif autentifikasiya modelini birlikdə tətbiq etmək daha məqsədə uyğundur.

Üçüncü avtorizasiya mərhələsində istifadəçinin sistemdə nə əldə edə biləcəyi müəyyənləşdirilir. Belə səlahiyyət vermə sistemin təhlükəsizlik siyasəti tərəfindən müəyyən edilir və sistem administratoru vasitəsilə qurulur. Bu səlahiyyətlərin miqyası "icazə yoxdur" və "hər şeyə icazəsi vardır" arasında dəyişə bilər.

İnformasiya təhlükəsizliyinin digər mühim prinsipi olan hesabatlılıq istifadəçilərin sistemdə həyata keçirilən hərəkətlərin, hadisələrin izlənilməsinə istinad edir. Hesabatlılıq təmin olunmayan sistemlər təhlükəsiz hesab edilmir.

Giriş hesabatların hazırlanması üçün nəzərdə tutulmuş sistemdə baş verən bütün əməliyyatların siyahısıdır. Belə ki, tamlıq təmin olunan sistemlərdə girişlər etibarlı hesab edilir. Başqa sözlə, əgər girişlərdə əlavə yazılma və ya silinmə hadisələri müşahidə olunubsa, bu zaman onlar hesabların hazırlanması üçün baza rolunu oynaya bilmir. Əlavə olaraq, şəbəkələrdə və telekommunikasiya sistemlərində girişlər dəqiq vaxtla işləməlidirlər, bir və ya bir neçə sistemin şəbəkədə qarşılıqlı münasibətini sinxron şəkildə qeyd etməlidir.

Audit izləri ilə girişlər arasındakı fərqlər aydın olaraq hələ də müəyyənləşdirilməyib. Buna baxmayaraq, qeyd etmək olar ki, girişlər mail

mesajlarının çatdırılması, veb səhifələrininn xidmətləri kimi yüksək səviyyəli prosesləri göstərdiyi halda, audit izlərində faylların açılması, fayla yazı yazmaq, şəbəkə vasitəsilə paketlərin göndərilməsi kimi aşağı səviyyəli əməlliyyatların siyahısı yadda saxlanılır. Audit izlərində sistemdə reallaşdırılan bütün əməliyyyatlar haqqında detallı şəkildə məlumatlar saxlanır, lakin bu məlumatların əksəriyyəti praktiki cəhətdən bir məna kəsb etmir. Detalların çoxluğu əməliyyatların yadda saxlanılması və analizinə daha çox vaxt sərf olunmasına səbəb olur. Bir digər tərəfdən audit izləri ilə girişlər arasındakı fərq onların mənbələri ilə bağlıdır: girişlər, adətən, sistemin proqram təminatında, audit izləri isə əməliyyat sistemlərində və ya audit modullarında saxlanılır.

Təhlükəsizliyin təmin olunmasının ən mühim prinsiplərdən biri də funksionallıq və əminlikdir. Bu prinsipi izah etməyin ən yaxşı yolu bir sıra suallar verməkdir: neçə dəfə kompüter çöküb?, neçə dəfə istənilməyən əməliyyatlat yerinə yetirilib? Bizim gözlədiyimizlə əslində olması gözlənilən hadisələr arasındakı fərq də məhz bu prinsipə istinad edir. Bu prinsipdə funksionallıq sisteminin nələr etməyə qadir olduğunu, əminlik isə sistemdə nələrin olmayacağını göstərir.

İnformasiya təhlükəsizliyi konteksində gizlilik istifadəçilərin şəxsi məlumatların gizlənilməsinə və qorunmasına istinad edir. Şəxsi informasiyalar, məsələn, ad və adreslər, sistemdən istifadə edən şəxslər haqqında gizli informasiyalardır.

Bir çox ölkələrdə şəxsi məlumatların gizliliyi qanunlar çərçivəsində təyin edilir, hər hansı bir uyğunsuzluq üçün müəyyən cəza tədbirləri həyata keçirilir. Avropa Birliyi (AB) təşkilatların şəxsi informasiyanın yerləşdirilməsi, istifadəsi haqqında çox ciddi qanunverciliyə malikdir.

Gizlilik təkcə insanların lazımı ehtiyacı olmadığından təşkilatlar şəxsi informasiyanın toplanması, saxlanması, emal edilməsində konfidensiallığı, tamlığı qorumaq məqsədilə müəyyən tədbirlər kompleksi həyata keçirməlidirlər. Bununla yanaşı, şirkətlər bu tip məlumatların necə toplanması və emal edilməsi barəsində informasiya təhlükəsizliyin siyasətini həyata keçirməlidirlər. informasiya təhlükəsizliyi konteksində imtina etməmə (non-repudiation) kriptoqrafik rəqəmsal

imzanın xüsusiyyətlərindən birinə istinad edir ki, bu da məlumatın rəqəmsal imza sahibi olan şəxsin əldə etməsinin təmin edilməsinin mümkünlüyünü təklif edir [5].

İmtina edilməmənin aşağıdakı xidmətləri İSO 14516:2002 beynəlxalq standartı tərəfindən müəyyənləşdirilmişdir.

- Təsdiqetmə: Məlumatın məzmununun təsdiqindən məsul olan şəxsin həqiqiliyini yoxlayır.
- Göndərmə: Məlumatın göndərilməsi reallaşdırılır.
- Mənbə: Təsdiqetmə və göndərmə xidmətlərinin kombinasiyasıdır.
- Asılılıq: Göndərən şəxs transmissiya qəbulu haqqında məlumat əldə edilməsini tələb edir.
- Nəqliyyat: Göndərən şəxsin məlumatı nəzərdə tutulan alıcıya çatdırılma prosesidir.
- Alıcı: Məlumatı qəbul edən şəxsdir.
- Bilik: Qəbul edilən məlumatın məzmununu alıcıya təqdim edilməsini təmin edir.
- Çatdırılma: Alıcı və biliyin kombinasiyasıdır, alıcının məlumatı qəbul etməsi və məzmunu ilə tanış olmasını reallaşdırır.

İmtina etməmənin qanuni məzmunu ilə informasiya təhlükəsizliyinin/ kriptoqrafiyanın məzmunu arasında bir sıra fərqlər vardır. Qanuni olaraq, təsdiq olunmuş imza sahibi aşağıda qeyd olunmuş hallarda imtina etmək hüququna malikdir:

- İmza düzgün olmadığı halda;
- İmza üçüncü şəxs tərəfindən saxtalaşdırıldığında;
- İmza başqa istifadəçilər tərəfindən ələ keçirildiyi halda.

İnformasiya təhlükəsizliyində istifadəçi yadda saxlamalıdır ki, sahib olduğu imza öz həmkarlarından fərqlənir. Bundan əlavə, bəzi ölkələrdə imza sahibinin hər hansı bir vərəqi özünün imzalayıb imzalamadığını sübuta yetirə biləcəyi yeni proqramlar mövcuddur.

Az səlahiyyət vermə: Bu prinsipin əsas şərti “lazımı miqdardan daha çox səlahiyyət vermə” ilə bağlıdır. Həmin prinsip təkcə kompüter sisteminin istifadəçilərinə deyil, həm də qeyri-informasiya sistemlərinin təşkilati idarə heyətinə də tətbiq edilir. Az səlahiyyət vermə prinsipi profilaktik nəzarətdir, çünki səlahiyyətlərin sayının azaldılması sistemdən sui-istifadə olunmasının qarşısını alır, nəticədə dəymiş ziyanları məhdudlaşdırır. Digər prinsiplər kimi bütün sistem mühitlərində tətbiq oluna bilər. Prinsipə daxil olan bəzi nümunələr aşağıda qeyd olunmuşdur:

- Yazı icazəsi olmayan istifadəçilər paylaşılmış faylı yalnız oxuya bilər;
- Proqram təminatı yaradıcılarına proqram təminatını istehsal serverindən istehlak serverinə köçürməyə icazə verilmir;
- Köməkçi heyət işçilərinin parol tələb edən istifadəçi hesabları yarada yaxud silə bilməz.

Dərin müdafiə prinsipinin əsas mahiyyəti birdən çox müdafiə qatının, tipinin olması ilə əlaqədardır. Nə qədər güclü, eləcə də etibarlı olmasına baxmayaraq, müdafiə qatının birinci təbəqəsi qırılsa da ondan aşağıda yerləşən qatların sıradan çıxarılması xeyli zəhmət tələb edir. İnternet və LAN arasında qoruyucu divar (firewall) istifadə olunması ilə yanaşı həm də İPSec protokolunun (İnternet Protocol Security-İnternet Protokolu Təhlükəsizliyi) tətbiqi kimi 2 və ondan artıq müxtəlif tip müdafiə mexanizmlərinin birləşdirilməsi zamanı adı qeyd olunan prinsip özünü daha yaxşı göstərir. Belə olan hallarda qoruyucu divar zədələnsədə, pis niyyətli şəxsin qorunan faylı ələ keçirməsi üçün İPSec protokolunu sındırmaq məcburiyyətindədir [1].

Ümumi olaraq, müxtəlif tip nəzarətlər birlikdə işlədilməsi daha məqsədə uyğundur: ilk öncə qoruyucu nəzarət ola biləcək bütün zərərli hücumların qarşısını alır; daha sonra aşkarlayıcı nəzarət sistemi qoruyucu mexanizmin işinə nəzarət edir; sonuncu mərhələdə isə düzəliş edici mexanizm vasitəsilə vurulmuş zərərlər aradan qaldırılır. Lakin, dərininə müdafiə prinsipi nəzarət mexanizmlərininə ayrılıqda tətbiq

edilməməlidir, təhlükəsizlik tədbirləri haqqında bəzi məlumatları öncədən bilmək lazımdır: müdafiə dərinliyi ilə təmin edilən təhlükəsizlik arasında balans müəyyən edilməlidir; daha sonra isə lazımı maliyyə, insan, məlumat qaynaqlarını qeyd olunmuş balansa uyğun şəkildə istifadə etmək lazımdır. Yuxarıda bildirilən balans gəlir-xərc analizinə əsaslanır [4].

Minimnallaşdırma prinsipi mahiyyət etibarı ilə az səlahiyyət vermə prinsipinə oxşayır və daha çox sistem konfiqurasiyasına tətbiq edilir. Bu prinsipə görə həvalə edilmiş işi yerinə yetirmək üçün tələb olunmayan proqramların, xidmətlərin istifadəsi məhdudlaşdırılmalıdır. Məsələn, e-mail xidməti üçün nəzərdə tutulmuş kompüterə yalnız e-mail proqramı yüklənməli və aktiv edilməlidir. Digər bütün xidmətlərdən istifadənin mümkünlüyü isə aradan qaldırılmalı, ya da heç kompüterə yüklənməməlidir. Minimallaşdırma prinsipinin möhkəmliyi təkcə təhlükəsizliyi artırmır, həm də iş qabiliyyətini yaxşılaşdırır, yaddaşa qənaət edir, ümumiyyətlə, sistemin işini kifayət qədər rahatlaşdırır.

Hər hansı təhlükəsizlik tədbirlərinin həyata keçirilməsi zamanı gəlir-xərc təhlili prinsipi nəzərdən keçirilməsi zəruridir. Prinsipə görə tətbiq edilən təhlükəsizlik nəzarətinə və ya mexanizminə sərf olunan xərc ümumi xərclərdən çox olmalıdır, əks təqdirdə bu tədbirlərin reallaşdırılması heç bir məna daşımır. Gəlir-xərc analizi birbaşa olaraq investisiyaların qaytarılmasına (ROİ-Return on İnvestment) təsir edir. Sadə səslənməsinə baxmayaraq ən vacib və tez-tez nəzərdən keçirilən problemlərdən biridir. Gəlir-xərc analizi zamanı müəyyən zaman çərçivəsindəki (məsələn, bir ildən beş ilə qədər) bütün xərclər və gəlirlər nəzərə alınmalıdır.

Bölmələndirmə və ya bölmədən (virtual sahələrdən) istifadə zədələnmiş bölmənin sistem üçün təhlükə yaratmasına mane olur, eləcə də digər bölmələrə ziyan vurulmasının qarşısını alır. İnformasiya təhlükəsizliyi konteksində bölmələndirmə müxtəlif bölmələri bir-birindən ayırır. Güclü təhlükəsizlik mexanizminə malik olan Solaris 10 əməliyyat sistemində də məhz bu prinsipdən istifadə edilir.

Sadələşdirmək: Mürəkkəblik təhlükəsizliyin ən pis düşmənidir. Mürəkkəb sistemlər təbii olaraq daha təhlükəlidir, çünki onları layihələndirmək, reallaşdırmaq,

test etmək daha çətindir. Əksər hallarda mürəkkəb sistemlər gözlənilən nəticəni vermir. Baxmayaraq ki, informasiya sistemlərinin, mürəkkəbliyi onun funksionallığını artirsa da, əvvəlcədən qaçınılan və qaçınılmayan mürəkkəblikdən xəbərdar olmaq lazımdır. Mürəkkəb sistemlə müqayisədə sadə sistemlə daha az iş görülməsinə baxmayaraq, istifadəçilər hər zaman sadə sistemə üstünlük verirlər.

Təhlükəsizliyin pozulması: Əgər hər hansı bir səbəbdən təhlükəsizlik nəzarəti pozulubsa, sistem təhlükəli vəziyyətdə olduğu göstərilmir. Məsələn, qoruyucu divar zədələnibsə, bu zaman "hər şeyə icazə ver" əmri əvəzinə "hər şeyi ləğv et" əmrindən istifadə edilir.

Zəif nöqtənin təhlükəsizliyi. İnformasiya sistemlərindən yeni istifadə etməyə başlayanlar üçün təhlükəsizlik prinsipi eyni cür səslənə bilər. Bəzən sistemin vəziyyətinin yaxşı olmasına baxmayaraq, biz ondan uğurla istifadə edə bilmirik. Bu səbəbdən də zəif nöqtə tapılaraq onun təhlükəsizliyi təmin edilir.

Yoxlanma nöqtələri: Təhlükəsizlik şəbəkə və sistemlərin daxili, xarici bütün yolların effektiv, səmərəli idarə edilməsi ilə bağlıdır. Yoxlama nöqtələri rahatlıqla izlənilən və idarə edilən məntiqi "dar kanallardır". Yoxlanma nöqtəsinə nəqliyyat funksiyasını həyata keçirən qoruyucu divar misal göstərmək olar. Qoruyucu divarları binaların, təsislərin girişlərini idarə edən hasar kimi də düşünmək olar.

Vəzifələrin ayrılması prinsipinin əsas məqsədi təşkilat daxilində bir şəxsin müxtəlif funksiyaların yerinə yetirməsindən azad edilməsidir. Bu prinsip təhlükəsizlik pozuntularının aradan qaldırılmasında uğurla tətbiq edilir. Faktiki təşkilatların iyearxiyası fərqli olsa da, bu prinsipin arxasında dayanan ideya dəyişməz olaraq qalır: "heç bir şəxs təhlükəsizliyi poza bilməz". Bu prinsip vasitəsilə şirkətlər rahatlıqla pozuntuları əvvəlcədən müəyyən etmək imkanına sahib olurlar [7].

1.2 İnformasiya təhlükəsizliyinin arxitekturası

İnformasiya təhlükəsizliyi (İT) təkcə texniki vasitələrdən deyil, eləcə də ilkin olaraq insan amilindən asılıdır. Başlıca olaraq effektsiz, səmərəsiz İT-nə səbəb ola biləcək bütün nöqsanlar, çatışmamazlıqlar müəyyən edilməli və onların təsiri minimum həddə çatdırılmalıdır.

Birinci informasiya sisteminin (İS) idarə edilməsi prosesinə və yaxşı idarəetmə üçün İS-nin planlaşdırılması, layihələndirilməsi, istifadəsi, emal edilməsi mərhələlərinə diqqət yetirmək lazımdır.

İS-nin idarə edilməsi. İT-i İS-nin idarə edilməsinin bir hissəsidir. İnsan həyatının bütün sahələrində İS-dən asılılıq gün keçdikcə daha da artır. İS-ləri milli təhlükəsizliyə, rəqabət qabiliyyətinə, iqtisadiyyata güclü təsir göstərir. İS-nin idarə edilməsi dedikdə obyektlərin və onların xidmət keyfiyyətinin müəyyənləşdirilməsi başa düşülür. Həmin səbəbdən yaxşı idarə edilməyə malik İS-i hər bir təşkilat üçün mühüm əhəmiyyət kəsb edir və onun yoxluğu birbaşa İS-nin təhlükəsizliyinə təsir edir [24].

İnformasiya sistemlərinin idarə olunması (İSİ) 2 əsas məsələnin həllinə şamil olunur: daha çox İS-nin resurslarına malik olmaq və eyni zamanda da sistemlə bağlı olan bütün riskləri idarə edə bilmək. İSİ prosesi təşkilatın yüksək səviyyəli idarə heyəti tərəfindən həyata keçirilir. İdarə heyətinin əsas vəzifəsi İS-nin təşkilatdakı rolunu və təsirini anlamaq, yüksək səviyyəli siyasəti müəyyənləşdirmək, İS-nin iş qabiliyyətini ölçmək və meydana gələcək risklərə qarşı bir sıra tədbirlər planı hazırlamaqdan ibarətdir.

Təəssüf ki, İT-ni tez-tez texnoloji məsələ ilə səhv salırlar, lakin araşdırmalar nəticəsində məlum olmuşdur ki, bu, ilk növbədə bir iş məsələsidir. İT inkişafın idarə olunması informasiya texnologiyalarının idarə heyəti tərəfindən məhdudlaşdırılır. İT-nin düzgün qurulması üçün işçi heyətin, məsul şəxslərin seçiminə diqqət yetirilməlidir. İşçi heyəti aşağıdakı xüsusiyyətlərə malik olmalıdır:

- İT barəsində anlayışa sahib olmalıdır;

- Strategiya və siyasət planını yarada bilməlidir;
- Sistemi resurslarla təmin etməlidir;
- İdarəetmə məsuliyyətini daşımalı və prioteritləri təyin etmək bacarığına malik olmalıdır.

İcra heyəti isə öz növbəsində İSİ-nin aspektlərinin həyata keçirmək üçün aşağıda adı çəkilən məsələləri həll etməlidir:

- İT siyasətini təyin etməlidir;
- İşçi heyətin öhdəliklərini müəyyənləşdirməlidir;
- İS ilə bağlı riskləri qiymətləndirməli, onların təhlili və idarə edilməsi ilə məşğul olmalıdır;
- İT idarəetmə çərçivəsinin sərhədlərini təyin etməlidir;
- Bütün əməkdaşları təhlükəsizlik haqqında maarifləndirilməsi təlimini həyata keçirtməlidir.

Təşkilat daxilində İSİ-nin effektivliyinin qiymətləndirilməsi İT-nin idarəetmə obyektlərinin tərkib hissəsi olan İnformasiya Texnologiyalarının İdarə Təşkilatı (Control Objectives for Information Technology-COBİT) tərəfindən həyata keçirilir. COBİT tərəfindən aşağıdakı idarəetmə kriteriyaları müəyyənləşdirilmişdir[25]:

- Effektivlik;
- Səmərəlilik;
- Məxfilik;
- Tamlıq;
- Əlyetənlilik;
- Uyğunluq;
- Etibarlılıq.

İnformasiya texnologiyalarına proqramlar, qurğular, texnologiyalar və təşkilatın verilənləri daxildir. Bu model vasitəsilə İSİ-nin 6 səviyyəsi müəyyənləşdirilir [25]:

- 0-cı səviyyə: mövcud olmayan;
- 1-ci səviyyə: ilkin;
- 2-ci səviyyə: təkrarlana bilən;
- 3-cü səviyyə: müəyyən edilmiş;
- 4-cü səviyyə: idarə edilən;
- 5-ci səviyyə: optimallaşdırılmış.

Mövcud olmayan: İSİ və təhlükəsizlik sisteminin idarə edilməsi prosesləri mövcud deyil. İcra və işçi heyəti müəssisə səhmdarları tərəfindən verilmiş məlumat sistemlərinin idarə edilməsi, qorunması ilə bağlı vəzifələrdən sui-istifadə edirlər.

Birinci səviyyə: İSİ və təhlükəsizliyinin mövcud olmasına baxmayaraq, yaxşı təşkil olunmamışdır. Təhlükəsizlik siyasəti, stamdartları, prosedurları mövcud deyil yaxud düzgün tətbiq edilməmişdir.

İkinci səviyyə: İS və təhlükəsizliyin müəssisə üçün əhəmiyyəti başa düşülür, lakin aktual İSİ-nin tətbiq olunmağı üçün müvafiq şərait yoxdur. Təhlükəsizlik effektiv və səmərəli deyildir. Bu səviyyəyə müəssisələrdə rast gəlmək olar.

Üçüncü səviyyə: Bütün proseslər sənədləşdirilir və müvafiq heyətə yönləndirilir. Risklərin idarə edilməsi, İT siyasəti mövcuddur və lazımı işçilərlə əlaqələndirilmişdir.

Dördüncü səviyyə: Burada sənədləşdirmə və yönəltmə prosesləri ilə yanaşı bütün proseslərin həqiqiliyindən, doğruluğundan əmin olmaq olar. Risklərin analizi prosesi ardıcıl olaraq icra edilir. Təhlükəsizlik siyasəti, prosedurları xüsusi təhlükəsizlik əsasları ilə tamamlanır. Standartlardan istifadə olunmağa başlanılır.

Optimallaşdırılmış: İS və İT-nin idarə olunmasının bütün aspektlərini əhatə edir. Strukturlaşdırılmış bir prosesin tətbiq olunduğu mərhələdə risklərin qiymətləndirilməsi yüksək səviyyədə inkişaf etmişdir və təşkil olunmuşdur.

Təhlükəsizlik funksiyaları layihələndirmə mərhələsindən başlayaraq proqramlara inteqrasiya olunur.

Göründüyü kimi hər bir səviyyə modeli əvvəlkindən fərqlənir, səmərəli və effektiv İSİ daha çox xərc tələb edir.

Ekspertlərin fikrincə İT zəncirinin ən zəif nöqtəsi insandır. Dayanılmadan edilən səhvlər nəticəsində risklərin sayı da artır, mövcüd vəziyyəti əvvəlki vəziyyətinə qaytarmaq məsələsi də çətinləşir. Sahibkarlar, menecerlər, layihə rəhbərləri, adminstratorlar, bunlarla yanaşı istifadəçilər informasiya cəmiyyətinin bir hissəsidir. Sahibkarlar, menecerlər İSİ prosesinin bütün məsuliyyətini öz üzərilərinə götürməli, layihə rəhbərləri, administratorlar təhlükəsizlik prinsiplərinə sadiq qalmalı, istifadəçilər bir dəqiqəlik rahatlıq üçün sistemi təhlükə altına atmamalıdırlar [26].

Dünyanın tanınmış ekspertlərindən biri olan Brus Sneirin fikrinə görə "təhlükəsizlik məhsul deyil, prosesdir". Həqiqətəndə, meydana çıxan müxtəlif növ yeni təhlükələrə qarşı yaradılmış müdafiə sistemləri təhlükəsizliyin heç vaxt bitməyən təkamül prosesi olduğunu açıq-aydın göstərir. Bu da bir müddətdən sonra təhlükəsizliyi rəfdən satın ala bilinməyəcəyini göstərir. Bütün əməliyyat mühitləri təhlükəsizlik texnologiyaları ilə təmin olunmuşdur, təhlükəli proses zamanı yarana biləcək zədələrin qarşısını almağa çalışır, düzəldici nəzarəti tətbiq etməklə sistemi əvvəlki vəziyyətinə gətirir.

Risklərdən qorunma prosesi lazımı resurslardan istifadə edərək yüksək kvalifikasiyalı ekspertlər tərəfindən onların aradan qaldırılmasından ibarətdir.

Əvvəlki mövzuda gəlir-xərc analizinə və risklərin idarə olunmasına toxunuldu. Bu prinsipləri daha dərindən araşdırmaqla sistem düşmənlərini tanımaq olar. Müdafiə sistemi qurulan zaman ən azından kimlərin hücum edə biləcəyi haqqında ümumi də olsa bir fikir formalaşır və bunun qarşısını almaq məqsədilə mühəndis bir sıra tədbirlər planı həyata keçirir. Hücum edən şəxsləri tanımadan və onların niyyətindən xəbərdar olmadan gəlir-xərc, risklərin analizini etmək çox çətindir.

İnformasiya sisteminin arxitekturası xüsusi konfiqurasiya prinsiplərinə əsaslanan komponentlərin və onların qarşılıqlı əlaqəsi ilə müəyyənləşdirilir. İS-nin arxitekturası aşağıdakı kimi təsvir edilə bilər [24]:

- Sintaksis – arxitekturanın strukturu. Eyni təbəqədə bir neçə sistem modulu yerləşir;
- Semantik – komponentlərin qarşılıqlı əlaqəsi. Eyni abstraksiya səviyyəsində bir-birinin funksionallığından istifadə edən çoxsaylı altsistemlər yerləşir;
- Praqmatik – strukturunun arxasında dayanan səbəblər vasitəsilə.

İnformasiya sistemlərinin 5 əsas aspekti vardır:

1. Verilən – sistem tərəfindən idarə olunan verilənlərin arxitekturası.
2. Sistem – diaqramlar vasitəsilə proqram təminatının arxitekturasının göstərilməsi.
3. Konfiqurasiya – aparat vasitələrinin və aşağı səviyyəli proqram təminatının (əməliyyat sistemləri, verilənlər bazasının idarəetmə sistemləri) arxitekturası.
4. Kommunikasiya – topologiya diaqramları ilə kommunikasiya infrastrukturunun (şəbəkələrin) təsviri.
5. Təşkilat – müəssisənin strukturu və administrasiya və sistem idarəsi ilə bağlı proseslərin arxitekturası.

1.3 Parolun köməyi ilə informasiya sistemlərinin təhlükəsizliyinin təmin edilməsi

Parol istifadəçilər üçün kompüter sistemlərinə və ya veb saytlarına girərkən özlərini doğrulamaq üçün ən çox istifadə edilən üsuldur. Şifrə icazəsiz girişlərdən qoruyan ilk müdafiə xətti kimi çıxış edir və bu səbəbdən də yaxşı parol idarəetmə siyasətini tətbiq edərək müdafiə xəttinin effektivliyini təmin etmək vacibdir.

Gündəlik həyatda informasiya texnologiyalarından getdikcə daha çox istifadə olunması yadda saxlamalı və idarə edilməsi lazım olan bir çox istifadəçi hesabının və parolunun yaranmasına səbəb olur. Müxtəlif informasiya sistemlərində istifadə olunan parolların seçimi isə ən çətin məsələlərdən biridir. Bir tərəfdən eyni paroldan istifadə bütün sistemlərə rahatlıqla daxil ola bilməklə nəticələnə bilər. Digər tərəfdən isə müxtəlif sistemlər üçün fərqli şifrələrdən istifadə edildikdə istifadəçilər əksər hallarda asan yadda qalan, zəif parol seçməklə sistemin təhlükəsizliyini təhlükə altına ata bilərlər. İstifadəçilərin parolu unutması isə şifrəni sıfırlamaq üçün əlaqəli istifadəçi dəstəyi tələb edərək əməliyyat xərclərini artırır [10].

Parol kompüter sisteminə daxil olan istifadəçilər üçün asan, rahat autentifikasiya üsuludur. Sistem sadəcə istifadəçinin həqiqiliyini müəyyən etmək üçün giriş zamanı parol tələb edir. Asanlıqla reallaşdırılmasına baxmayaraq parol yanaşması bir sıra hədələrə məruz qalır. Qanuni istifadəçilərin parolu itirməsi ümumi sistemi təhlükəli vəziyyətlə qarşı-qarşıya qoyur:

1. Şəxs öz şifrəsini yazdıqda kimsə onun yazdıqlarını müşahidə edərək görə bilər və ya kameradan istifadə edərək parolu oğurlaya bilər.
2. Kobud hücum. Parolun uzunluğu adəətən, 8 simvoldan ibarət olduğundan pis niyyətli şəxs parol yaradan proqramlardan istifadə edərək düzgün şifrəni tapana qədər bütün mümkün kombinasiyaları yoxlayır. Hesablama sahələrindəki son inkişaflar nəticəsində uğurlu kobud hücumları reallaşdırmaq üçün lazım olan vaxt xeyli azaldılmışdır.

3. Şəbəkə üzərində bir parol yazılan zaman şəbəkə kanalı düzgün şifrələnmədikdə parol asanlıqla oğurlana bilər. Əlavə olaraq, zərərli vasitələrlə autentifikasiya prosesi zamanı parolu müəyyən etmək olar.

4. Fişinq vasitəsilə bəzən pis niyyətli şəxs giriş ekranını xatırladan saxta ekran qurur. Bu zaman istifadəçi saxta ekrana parolu daxil etdikdə hücum edən şəxs asanlıqla şifrəni əldə edə bilir.

Bütün bu hücumlar müvəfəqiyyətli olsa, icazəsiz şəxslər qanuni istifadəçilərin parolunu asanlıqla oğurlayır. Sistem parolu daxil edənin həqiqi istifadəçi olub-olmadığını müəyyənləşdirə bilmir.

İstifadəçi baxımından parol çətin olsa belə, onu unutmamaq bir neçə parolu yadda saxlamaqdan asandır. Əlavə olaraq, əgər bütün sistemlərə daxil olmaq üçün bir parol kifayətdirsə, həmin parolu qorumaq daha çox diqqət tələb edir. Bəzən tək paroldan istifadə müxtəlif əməliyyat platformalarında texniki olaraq mümkün olmur [12].

İstifadəçilər nadir hallarda daxil olduqları sistemlərin parollarını unuda bilir. Bu da şifrələri sıfırlamaq üçün dəstək işçilərinə artan iş yükü yaradır. Bundan əlavə, istifadəçilər parolları vərəqə yazaraq və ya yadda qalan şifrə seçmə kimi təhlükəli addım atırlar.

Pis niyyətli şəxs tək parollu yanaşmalı zəif qorunan sistemləri avtomatik olaraq sındıra bilirlər. Buna görə də belə müəssisələrdə bütün sistemin təhlükəsizliyi eyni səviyyədə qorunmalıdır. Hər bir informasiya sistemi funksional xarakteristikadan və verilənlərin təsnifləşdirilməsindən asılı olaraq müxtəlif təhlükəsizlik tələblərinə malikdir. Ümumi qaydaya görə, autentifikasiya mexanizmləri müxtəlif səviyyələrdə tətbiq edilməli, qorunması lazım olan informasiya dəyərinə uyğun olmalıdır. Məsələn, gizli məlumatları idarə edən proqramı sıx giriş nəzarəti tələb edir, ümumi axtarışda internet proqramı isə anonim girişlərə icazə verə bilər.

Yuxarıda qeyd edilənlərə görə müxtəlif təhlükəsizlik tələblərinə cavab verən və müdafiə edilməli məlumatları fərqliliyinə görə hər sistem üçün müxtəlif parollardan

istifadə edilməlidir. Birdən çox sistemə daxil olmaq üçün bir paroldan istifadə edildikdə, istifadəçi hesabları ən yüksək təhlükəsizlik tələblərinə cavab verməlidir.

Yaxşı bir parol idarəetməsini təmin etmək üçün təhlükəsizlik siyasəti və təlimatlarının həyata ilə yanaşı aşağıda qeyd olunan bəzi effektiv texnologiyalardan istifadə etmək olar.

Açıq açar texnologiyası (Public Key İnfrastucture – PKİ) məlumatın gizliliyini, tamlığını, identifikasiyasını təmin edən təhlükəsizlik əməliyyatlarını asanlaşdırmaq üçün riyazi alqoritmlərdən və prosedurlardan istifadə edən texnologiyadır. PKİ fərdin həqiqiliyini yoxlamaq üçün rəqəmsal sertifikatlardan istifadə edir. Rəqəmsal sertifikat şəxsiyyat vəsiqəsi kimi istifadəçinin doğruluğunu müəyyən edən rəqəmsal sənəddir. Etibarlı sertifikat Sertifikat İdarəsi (Sİ) tərəfindən yaradılır və xüsusi açarlardan istifadə edilərək rəqəmsal şəkildə imzalanır. Şəxs müxtəlif platformalarda bu sertifikatdan istifadə edə bilər və rəqəmsal imza vasitəsilə fərdin həqiqiliyi yoxlanılır[10].

PKİ əvvəlcədən qeydiyyat keçmə prosesi olmayan onlayn əməliyyatlarda və proqramlarda istifadəçi identifik identifikasiyası üçün xüsusilə faydalıdır. İstifadəçilər etibarlı sertifat əldə etmək üçün özlərini doğrulamaq məqsədilə müxtəlif proqramlara müraciət etməlidirlər.

PKİ-nın istifadəsi bəzi təhlükəsizlik məsələlərinin həllini tələb edir:

1. Şəxsi açar PİN kod ilə qorunan smart kartlar kimi təhlükəsiz yerdə saxlanmalıdır.
2. İcazəsiz girişlərin qarşısını almaq məqsədilə PİN kimi müvafiq parol məhdudiyyətləri tətbiq edilməlidir.
3. Sertifikatların verilməsi, alınması, saxlanması, ləğv edilməsi üçün əsas prosedurlar olmalıdır.
4. Gizli açarın sürəti çıxarılmalı və şifrələnmiş şəkildə saxlanmalıdır.

Müqayisəli siqnal texnologiyasından (Single Sigh On – SSO) istifadə edərək daxili və xarici sistemlərə giriş üçün istifadəçi yalnız bir dəfə identifikasiya serverinə müraciət edərək öz həqiqiliyini yoxlamaq imkanı əldə edir. Texniki texnologiya

vasitəsilə bir sira fərqli parollardan istifadə etmək əvəzinə müxtəlif sistemlərə eyni parol ilə təhlükəsiz şəkildə daxil olmaq olar. SSO-nun tətbiqi ilə aşağıda qeyd olunan bir sıra təhlükəsizlik tədbirlərinə diqqət yetirmək lazımdır:

1. Tək identifikasiya nəzarəti ilə bütün resurlara giriş əldə edildiyindən həmin resurslar kifayət qədər təhlükəsiz olmalıdır. Belə qoruma ən kritik proqram tələblərinə cavab verməlidir. Tək identifikasiya prosesi əsl metodlardan zəif olmamalıdır, əks halda nəticədə təhlükəsizlik səviyyəsi aşağı olar.
2. İdentifikasiya prosesini gücləndirmək məqsədilə smart kart kimi ikinci dərəcəli faktorlardan istifadə oluna bilər.
3. Minimum parol uzunluğu, parol mürəkkəbliyi, giriş cəhdlərinin maksimum sayı və yenilənmə üçün minimum vaxt kimi müvafiq parol məhdudiyyətləri tətbiq edilməlidir.
4. Serverin hər zaman hücumların hədəfi olduğunu nəzərə alaraq, pis niyyətli şəxslərin identifikasiya məlumatlarını ələ keçirməməsi üçün çox yaxşı qorunmalıdır.
5. Şübhəli uğursuz giriş cəhdlərinin aşkarlanmasını və izlənməsi üçün təhlükəsizliyin audit və qeydiyyat prinsiplərindən istifadə edilməlidir.
6. Şəbəkə üzərində ötürülən şəxsi məlumatlar şifrələnərək qorunmalıdır.

Şifrələri idarə etmək üçün istifadə edilən digər texnologiya bir dəfəlik istifadə parollarıdır. İstifadəçilər iki unikal amil ilə özlərini təsdiqləyir. Texnologiyanın üstün cəhətlərindən biri parolu seçmək və ya yadda saxlamağın məcburi olmamasıdır. Kartlar həqiqiliyi doğrulamaq prosesi üçün PİN-lərə əsaslanaraq qorunan resurslara çıxış imkanı yaradan unikal, bir dəfəlik istifadə olunan parol yaradılır. Texnologiyanı tətbiq edərkən aşağıdakılar nəzərə alınır:

1. İdentifikasiya prosesi üçün nəzərdə tutulan kartlar əlavə vəsait tələb edir.

2. İstifadəçilər hər zaman kartları üzərilərində daşımalıdırlar. Kartlar unudulduqda və ya itirildikdə sistemə daxil olmaq cəhdləri uğursuzluqla nəticələnəcəkdir. Parol sıfırlanması tələb edən proqram əsaslı giriş nəzarət sistemlərindən fərqli olaraq, itirilmiş kart istifadəçilərin saatlarla, hətta günlərlə sistemə daxil olmasına mane olacaq.

3. İstifadəçilər kartların fiziki təhlükəsizliyinə diqqət yetirməli və kartların hər zaman düzgün şəkildə qorunmasını təmin etməlidir.

4. Cari bir dəfəlik parol identifikasiyası sxemlərin yalnız ilk əlaqəni təsdiqləyir.

5. Təhlükəsizlik kartlarını bütün proqramlar və serverlər tərəfindən dəstəklənməyə bilər.

Aşağıda bəzi əməliyyat və proqram sistemləri üçün nəzərdə tutulmuş yaxşı parol seçimi ilə əlaqədar kriteriyalar qeyd edilmişdir:

a) Yalnış giriş cəhdləri müəyyən edilmiş bir saydan sonra istifadəçi hesabı avtomatik olaraq dondurulur.

b) Məhdudlaşdırılmış hesab yalnız sistem və ya təhlükəsizlik administratoru tərəfindən əl ilə aktivləşdirilə bilər.

c) Sistem parolların əvvəlcədən müəyyən edilmiş uzunluqdan daha qısa olmasına və ya köhnə parolların yenidən istifadəsinə mane olur.

Parollar hesablama resurlarına daxil olmaq üçün ən çox istifadəı edilən identifikasiya formasıdır. Asan parolların, parol sındırma proqramlarının istifadəsi təhlükəsizlik halqasının ən zəif nöqtəsidir. Bu səbəbdən də siyasət prinsipləri əsasında parollar təyin edilməlidir. Ümumilikdə, parolun gücü onun uzunluğundan, mürəkkəblik dərəcəsindən asılıdır [2].

Böyük risklər yüksək səviyyəli müdafiə mexanizmi tələb edir. Belə olan hallarda çox funksiyalı identifikasiya kimi alternativ təhlükəszilik tədbirləri tətbiq edilməlidir. Yüksək riskli sistemlərə daxildir: kritik və ya həssas informasiyaya giriş təmin edən, paylanmış verilənlərə nəzarət, zəif təhlükəsizlik tədbirləri həyata

keçirilən, digər hesablara və təhlükəsizlik infrastrukturuna giriş əldə etmək imkanına malik sistemlər. Mərkəzi və şöbə müdirlərindən təhlükəsizlik və ya sistem administratorlarından səs vasitəsilə təhlükəsizliyin təmin edilməsini mümkün edən nümunə yaradıldı.

a. Bütün parollar müəyyən qaydalara uyğun olmalıdır:

- Ən azı 8 simvoldan ibarət olmalıdır;
- Ən az iki simvol və üç hərf olmalıdır;
- Hərflərdən ən az biri böyük və digəri isə kiçik olmalıdır;
- Şifrələr hər hansı bir dilin, dialektin, arqonun, lüğətdən olmamalıdır;
- Parollar asan təxmin edilən, şəxsi informasiyadan, ailə üzvlərinin adına uyğun qoyulmamalıdır;
- İfadə parolları 2 və daha artıq sözün simvollarla birləşməsi ilə yaradıla bilər. İfadələr istifadəçi üçün xatırlanması rahat olan sözlər olmalıdır.

b. Oğurluğun qarşısını almaq məqsədilə parol kimi kredit kartın nömrələrindən, şəxsiyyət vəsiqəsinin PİN kodundan istifadə olunmamalıdır.

c. Parollar email mesajları və ya digər elektron kommunikasiya formaları ilə göndərilməməlidir.

d. Müxtəlif platformalarda eyni şifrədən istifadə edilməməlidir.

e. Parolların hər 6 aydan bir dəyişilməsi tövsiyyə olunandır.

f. Parollar administrasiya işçiləri və İT administratorları da daxil olmaqla heç kimlə paylaşılmamalıdır.

g. Yalnız İnformasiya Texnologiyaları şöbəsinin yazılı icazəsi ilə bəzi istisnalara icazə verilə bilər və bütün məsuliyyət əlaqələndirici şəxsin üzərinə düşür. Şəbəkə qurğularını qorumaq üçün istifadə olunan parolların təhlükəsizliyindən istifadəçi məsuliyyət daşıyır və fərd yalnız müvafiq səlahiyyətli işçilərin həmin parollardan istifadəsinə şərait yaradır.

h. Şifrə təhlükəsizliyi şübhə altındadırsa, bu zaman parol dərhal dəyişdirilməlidir.

i. Şifrələrin oğurlanmasına və ya sındırılmasına nəzarət İT təhlükəsizliyi nümayəndələri tərəfindən müvafiq sistem administrasiyanın əməkdaşlığı və dəstəyi ilə dövri və ya təsadüfi olaraq həyata keçirilir. Belə hal aşkarlandığı zaman istifadəçidən parolu dərhal dəyişdirilməsi tələb olunur.

Yuxarıda qeyd olunan ümumi parol qaydalarına əlavə olaraq, texniki və ya administrativ cəhətdən mümkün olan hallar istisna olmaqla kliyent serverlərə bir sıra tələblər qoyulur. Birinci olaraq, hər bir kliyent qurğunun şifrəsi altı aydan bir yenilənməlidir. İkinci tələb parolu daxil etmək üçün cəhdlər avtomatik olaraq on yalnış təxmin ilə məhdudlaşdırılmalıdır. Yalnış cəhdlərdən sonra sistem minimum 10 dəqiqə kilitlənməlidir. Kliyent server qurğularına qoyulan sonuncu tələb isə uğursuz cəhdlərin sistemdə qeyd olunması ilə bağlıdır. Belə yazılar təxminən 30 gün ərzində sistemdə saxlanılır. Administratorlar mütəmadi olaraq bu qeydləri və onların yol açdığı üsulsuzluqları nəzərdən keçirməlidirlər [15].

Ümumi parol tələblərinə əlavə olaraq server administrasiyasına da bir sıra tələblər qoyulur:

1. İşçi heyətində baş verən dəyişikliklər ilə əlaqədar olaraq serverlərin parolları da dəyişilməlidir.

2. Hesabın və ya parolun təhlükə altında olduğundan şübhə edilərsə, bu barədə ilk İT təhlükəsizlik şöbəsinə bildirilir və daha sonra parolların dəyişdirilməsi zəruriləşir.

3. Kliyent server qurğularında olduğu kimi yalnız cəhdlərin sayı məhdud olur. Uğursuz cəhdlər üçün "Giriş ləğv edildi" kimi standart mesajlardan istifadə olunur. Standart cavab xaker hücumlarından yarana biləcək ipuclarını minimuma endirir.

4. Departament serverləri başçıları mərkəzi İT şəbəkələrinə qoşularaq administrator şifrəsi və müəyyən səlahiyyətlərlə təmin olunmalıdır. Administrativ səlahiyyətlərə və öhdəçiliklərə sahid olan şəxs

server sistemindəki qurğuları təhlükə altına atacaq hər hansı bir fəaliyyəti reallaşdırmaq məqsədilə öz şəxsi parollarından istifadə etməməlidir.

FƏSİL II. İNFORMASİYA TƏHLÜKƏSİZLİYİNİN ƏSAS KONSEPSİYASI

2.1 Beynəlxalq təhlükəsizlik standartları

Təhlükəsizlik standartlarının əsas məqsədi informasiya texnologiyaları sistemlərində, şəbəkələrində, kritik infrastrukturlarda təhlükəsizliyin təmin olunmasına xidmət etməkdir. Bir məhsulun və ya sistemin müəyyən bir standartlara uyğun olması onun bütün standartların xüsusiyyətlərini yerinə yetirməsinə işarədir. Hal-hazırda informasiya təhlükəsizliyini tənzimləyən bəzi əsas standartlar mövcuddur. Bunlardan birincisi ISO/IEC 27000 standartlarıdır.

1995-ci ildə Britaniya Standartlaşdırma Universiteti tərəfindən yaradılan və daha sonra ISO tərəfindən alınan bu standartlar ISO/IEC 27000 seriyası ilə satışa çıxarıldı. İkinci yerdə Amerikada Milli Standartlar və Texnologiyalar Universiteti tərəfindən yaradılan NİST SP 800 standartlar qrupu dayanır. Digər informasiya təhlükəsizlik standartlarına isə COBİT və BSI alman standartlarını misal göstərmək olar [18].

Standartların yekdilliklə istifadəsi qəbul olunmuşdur və fərdi təhlükəsizlik sistemini beynəlxalq səviyyədə qəbul edilmiş, müəyyənləşdirilmiş çərçivə ilə müqayisə etmək imkanı verir. Buna ən yaxşı nümunə müəyyən müəssisənin fəaliyyətində keyfiyyətin idarə olunmasına xidmət göstərən ISO 9000 standartlarıdır.

ISO müxtəlif milli standartlar təşkilatlarının nümayəndələrindən ibarət beynəlxalq standartlara cavab verən bir orqandır. 23 fevral 1947-ci ildə qurulan təşkilat dünya səviyyəsində xüsusi sənaye və ticarət standartlarını açıqlayır. Mərkəzi İsveçrənin ikinci böyük şəhəri olan Cenevrədə yerləşən ISO qeyri-hökümət təşkilatıdır, lakin buna baxmayaraq müqavilələr və ya milli standartlar vasitəsilə tez-tez qanunlara çevrilən standartları müəyyən etmək qabiliyyətinə malik olması onu əksər təşkilatlardan daha güclü edir [21].

Dünya üzərindəki 195 ölkənin 157-si ISO təşkilatının milli üzvüdür. Təşkilatda 3 əsas üzvlük kateqoriyası vardır:

- Əsas üzvlər hər bir ölkənin təməl standartlarını təmsil edən milli üzvlərdir. ISO-nun tək səsvermə hüququna malik üzvləridir, standartların qəbul edilməsində əsas söz sahibidirlər;
- Müxbir üzvlər öz şəxsi standartları olmayan ölkələrdir. Belə üzvlər ISO-nun işlərindən xəbərdardılar, lakin standartların qəbulunda iştirak etmirlər;
- İzləyici üzvlər kiçik iqtisadiyyata malik ölkələrdir. Onlar az miqdarda üzvlük haqqı ödəyərək standartların qəbul prosesini izləmək imkanı qazanırlar.

ISO/IEC 27000 seriyalı standartları ISO (The International Organization for Standardization) və IEC tərəfindən birlikdə qəbul edilmişdir. Seriya ümumi informasiya təhlükəsizliyini İdarəetmə Sistemi konteksində təhlükəsizliyin, risklərin idarə edilməsini və nəzarətin həyata keçirilməsini təmin edir. Keyfiyyət idarə olunmasını (ISO 9000 seriyalı) və mühitin qorunmasını (ISO 14000 seriyalı) təmin edən standartlar öz quruluşuna görə ISO 27000 standartlarını xatırladır. Bu seriya bütün formalı və ölçülü təşkilatlarda uğurla tətbiq edilir [19].

İlk 27000 seriyalı standartın sələfi olan ISO/IEC 17799 standartı 2000-ci ildə, ISO/IEC 27001 standartı isə 2005-ci ildə qəbul edildi. Hal-hazırda seriyanın 4 əsas standartı vardır: 27001, 27002, 27005 və 27006. Ondan çox standart isə hələki layihə mərhələsindədir. 27001 standartı təşkilatın təhlükəsizliyinin idarəetmə sistemlərini də sertifikatın əldə olunması üçün lazımı addımları müəyyənləşdirir.

Standart İTİS serfikatlaşdırılmasının yaradılması üçün 7 əsas element müəyyənləşdirir: sistemi qurmaq, həyata keçirtmək, idarə etmək, nəzərdən keçirtmək, saxlamaq və təkmilləşdirmək. İdarəetmə standartı kimi xüsusi nəzarət vasitələrinin istifadəsinə icazə vermir, belə ki, təşkilat üçün uyğun olan idarəetməni müəyyən etmək məqsədilə xüsusi prosesləri dəqiqləşdirir. Standart nəzarət obyektlərini siyahılaşdıran və xüsusi təhlükəsizlik nəzarəti tövsiyyə edən ISO/IEC 27002 standartı ilə birlikdə istifadə olunur.

ISO/IEC 27002 standartı ISO və IEC tərəfindən ISO/IEC 17799:2005 kimi tanıdıldı, daha sonra 2007-ci ildə yenidən ISO/IEC 27002:2005 adlandırılaraq 27000 seriyalı standartlar arasına daxil edildi. Standart informasiya texnologiyalarında informasiyanın təhlükəsizliyinin idarə edilməsi hüququna malikdir. Cari standart İngiltərə Standartı 7799-1:1999 sözbəsöz nüsxəsi olan 2000-ci ildə nəşr edilmiş ISO/IEC standartının bir seriyasıdır [19].

27002 standartının məqsədi 27001 standartına uyğunlaşaraq yüzlərlə informasiya təhlükəsizlik nəzarətlərini həyata keçirtməkdən ibarətdir. Məcburi standartlar siyahısına daxil olmayan 27002 müəssisələr tərəfindən istəyə uyğun olaraq azad şəkildə tətbiq edilir.

ISO/IEC 27002 İnformasiya Təhlükəsizliyi İdarəetmə Sistemlərinin (İTİS) təşkili, həyata keçirilməsi və aparılması üçün cavabdeh olan şəxslər tərəfindən istifadə üçün ən yaxşı təcrübə təklifləri təqdim edir. Məlumdur ki, təhlükəsizlik C-İ-A üçlüyü əsasında müəyyən olunur: konfidensiallığın (informasiyadan yalnız icazəli şəxslərin istifadəsinin təmin olunması), tamlığın (informasiyanın emal metodlarının düzgünlüyü, dəqiqliyini, tamlığının mühafizəsi) və əlyetənliyin (zəruri hallarda səlahiyyətli istifadəçilərə məlumat və əlaqəli fəaliyyətlərə giriş imkanının təmin edilməsi) qorunması.

ISO/IEC 27002 standartı informasiya təhlükəsizliyinin idarə edilməsinin müxtəlif sahələri üzrə təhlükəsizlik nəzarətləri təklif edir:

- Təhlükəsizlik siyasəti, informasiya təhlükəsizliyinin təşkili;
- İnsan resurslarının təhlükəsizliyi;
- Kommunikasiya və əməliyyatların idarəsi;
- İnformasiya sisteminin əldə edilməsi;
- İnformasiya təhlükəsizliyində pis niyyətli hadisələrin idarə olunması.

ISO/IEC 27005:2008 standartı təhlükəsizlik sahəsi üzrə risklərin idarə olunmasını təmin edir. Standart ümumiləşdirilmiş ISO/IEC 27001 standartının konsepsiyasına və risklərin menecmenti yanaşmasına əsaslanaraq təhlükəsizlik

proqramının həyata keçirilməsi üçün layihələndirilmişdir. ISO/IEC 27001 və ISO/IEC 27002 standartlarını da təsvir edilən terminalogiyanı və konsepsiyanı anlamaq ISO/IEC 27005:2008 standartını başa düşmək üçün vacibdir. ISO/IEC 27005:2008 bütün növ təşkilatlarda (kommersiya müəssisələrində, dövlət agentliklərində, qeyri-hökümət təşkilatlarında) pis niyyətli risklərin qarşısını almaq məqsədilə uğurla tətbiq edilir [21].

ISO/IEC 27006 standartı sertifikatlaşdırma orqanları tərəfindən izlənməli olan sertifikatlaşdırma və qeydiyyat proseslərini əks etdirir. Standartın əsas məqsədi məlumat təhlükəsizliyini idarəetmə sistemlərinin sertifikatlaşdırılması və ya qeydiyyat kimi formal proseslərə akkredite olunmuş sertifikatlaşdırılma orqanları tərəfindən rəhbərlik etməkdir.

ISO/IEC 27006 standartının əhatə dairəsi "İTİS üçün sertifikatlaşdırma və qeydiyyat əməliyyatları zamanı lazımı ümumi tələbləri müəyyənləşdirməkdən" ibarətdir [18].

Aşağıda qeyd olunmuş standartlar ISO/IEC JTC1 tərəfindən hazırlanır [21]:

ISO/IEC 27000 – informasiya təhlükəsizliyinin idarəetmə sistemlərinin standartlar ailəsinə giriş və ümumi baxış, əalvə olaraq ümumi terminlər lüğəti.

ISO/IEC 27003 – İTİS-nin icra təlimatları;

ISO/IEC 27004 – informasiya təhlükəsizliyinin idarəetmə ölçmələri üçün standart;

ISO/IEC 27007 – İTİS-nin auditi üçün nəzərdə tutulmuş təlimatlar (bütün diqqət idarəetmə sisteminə yönəlir);

ISO/IEC 27008 – informasiya təhlükəsizliyinin idarəetmə auditi üçün məlumatlar toplusu (diqqət təhlükəsizlik nəzarətində cəmləşir);

ISO/IEC 27011 – telekommunikasiya sahəsi üzrə İTİS-nin reallaşdırma təlimatları toplusu (X.1051 kimi tanınır);

ISO/IEC 27031 – biznes davamlılığına aid İKT sahəsi üzrə bəyannamə;

ISO/IEC 27032 – kiber təhlükəsizlik barədə təlimatlar toplusu (xüsusəndə internetdə "yaxşı qonşu olma");

ISO/IEC 27033 – informasiya texnologiyalarında şəbəkə təhlükəsizliyi, hal-hazırda ISO/IEC 18028:2006 kimi tanınan çox hissəli standart;

ISO/IEC 27034 – tətbiqetmə təhlükəsizliyi üçün təlimatlar.

1901-ci ildə Amerika Kommersiya Departamentinin daxilində yaradılan NİST (National İnistitute of Standarts and Texnology – Milli Standartlar və Texnologiyalar İnistitutu) qeyri-tənzimləyici federal agentlikdir. NİST-in əsas missiyası iqtisadi təhlükəsizliyi artıran və yaşayış tərzinin yüksəltmə üsulları ilə ölçmə elmini, standartlarını və texnologiyalarını inkişaf etdirməkdə Amerikanın innovasiya və sənaye rəqabətliliyinə dəstək verməkdir. İnistitutun ümumi büdcəsi 931.5 milyon dollardır və burada 2900-a yaxın alim, mühəndis, texnoloq, dəstəkləyici və administrativ işçi heyəti çalışır [21].

Amerika sənayesini 2 NİST laboratoriyası müəyyən növ ölçmələr və standartlarla təmin edir: elektron və elektrik mühəndisliyi, informasiya texnologiyaları, texnoloji xidmətlər, neytron tədqiqatı, fizika, nanotexnologiya elmi, istehsalat mühəndisliyi, materialşünaslıq, bina və yanğın araşdırmaları, kimya elmləri və texnologiyaları.

1990-cı ildə yaranan NİST Special Publications 800 (Xüsusi Nəşrlər – SP800) sənədlər toplusu bütün təhlükəsizlik standartlarının ən qocamanıdır. SP800 informasiya təhlükəsizliyinin demək olar ki, bütün aspektlərini əhatə edən yüzlərlə sənəddən ibarətdir. Bütün bu sənədlər içərisində NİST-in ideyasını ən yaxşı şəkildə ifadə edən SP800-12 standartıdır. SP800-12 informasiya təhlükəsizliyinin prinsipləri ətraflı şəkildə qeyd olunmuş kitabçadır. NİST-in mövzuya yanaşması aşağıdakı 8 əsas yol göstəricisini müəyyənləşdirir:

1. Kompüter təhlükəsizliyi təşkilatın missiyasını dəstəkləməlidir.
2. Kompüter təhlükəsizliyi idarəetmənin əsas elementidir.
3. Kompüter təhlükəsizliyi effektiv təşkil olunmalıdır.
4. Təhlükəsizlikdə səlahiyyətlər və öhdəçiliklər açıq qeyd olunmalıdır.

5. Sistem sahibləri öz təşkilatlarından kənarda da təhlükəsizlik məsuliyyətinə malik olmalıdır.

6. Kompüter təhlükəsizliyi hərtərəfli və vahid bir yanaşma tələb edir.

7. O, mütəmadi olaraq yenidən nəzərdən keçirilməlidir.

8. Kompüter təhlükəsizliyi ictimai amillərlə məhdudlaşır.

Seriyanın digər standartları da təhlükəsizlik prinsiplərinin bu prinsiplərə uyğun olaraq həll oluna biləcək xüsusi strategiyaları, prosedurları və tənzimləmələri detallı şəkildə izah etməyə davam edir. Vacib konsepsiyaları, xərclərin qiymətləndirilməsi və təhlükəsizlik nəzarətlərinin əlaqələndirilərək kompüter əsaslı qaynaqların (proqram, aparat təminatı və informasiya da daxil olmaqla) təhlükəsizliyinin təmin olunmasında köməkçi rol oynayır. NİST özü sertifikat proqramına istinad etməsə də, məlumatlandırma, təlim və təhsil sahələrində bir sıra təşəbbüslərə nail olmuşdur [20].

SP800 standartları bir sıra sahələri əhatə edir:

Elektron mail təhlükəsizliyi haqqında təlimatlar toplusu (SP800-45);

İnformasiya texnologiyalarının təhlükəsizliyində təlim proqramının inkişafına nail olma (SP800-50);

Elektronik icazələr barəsində təlimatlar toplusu (SP800-63);

Veb xidmətlərinin təhlükəsizliyinin təmin edilməsi (SP800-95).

Beynəlxalq qeyri-hökümət təşkilatı olan İnformasiya Təhlükəsizlik Formu (İnformation Security Form - İST) təhlükəsizlik sahəsi üzrə benchmarketingə (bir müəssisənin rəqabət gücünü artırmaq üçün müvəfəqiyyətli performansa malik digər müəssisələrin iş texnikalarını öz texnikaları ilə müqayisə etmək və müqayisədən alınan nəticələri tətbiq etmək) həsr olunub. 1989-cu ildə Avropa Təhlükəsizlik Formu adı altında yaranmış təşkilat 1990-cı illərdə öz missiyasını və üzvlərinin sayını artırmağa başlamışdı, belə ki, hal-hazırda Şimali Amerikadan, Asiyadan və dünyanın dörd bir yanından olan Fotune 500 jurnalında adı qeyd olunmuş yüzlərlə üzv daxildir. Üzvlər Avropa, Afrika, Asiya, Yaxın Şərq və Şimali Amerikada qruplar halında bölünüblər. ISF formunun baş qərargahı Londonda yerləşir, həm də müəssisənin Nyu-York şəhərində əməkdaşları vardır. ISF-nın üzvlüyü beynəlxalq səviyyədədir və

nəqliyyat, maliyyə xidmətləri, kimya, əzcaçılıq istehsalı, hökümət, pərakəndə satış, medya, telekommunikasiya, peşəkar xidmətlər və digər sahələr üzrə böyük şirkətlər daxildir.

Good Practice Standartı (SoGP) ilk olaraq 1996-cı ildə informasiya təhlükəsizliyi formu tərəfindən hazırlandı və təhlükəsizlik üçün ən yaxşı təcrübələri ətraflı sənədlər toplusu kimi əks etdirir. Standart hazırlandıqdan sonra onun üzərində iki dəfə dəyişikliklər edildi [19].

Pulsuz versiyaları mövcüd olan SoGP standartı ISO/IEC 27002 və COBIT v4.1 standartları əsasında hazırlanmışdır. Standart həm tədqiqat və real dünya təcrübəsinə əsaslanan funksional informasiya təhlükəsizliyi metodologiyasına əsaslanır. O, 6 əsas aspekt əsasında cəmləşdirilib:

1. Kompüter yükləmələri. Bu aspekt əsasən informasiya texnologiyaları mütəxəssislərinə yönəldilir və kritik biznes proqramlarını dəstəkləyən avadanlıq və proqramlara ünvanlanır.
2. Kritik biznes proqramları. Belə proqramlar müəssisənin fəaliyyətindən asılıdır. Bu baxımdan əsasən Mərkəzi Bankın sahibləri, biznes prosesləri və sistem inteqratorlarından məsul şəxsləri hədəf alınır.
3. Təhlükəsizliyin idarə edilməsi. Təhlükəsizlik idarəçiliyi aspektləri təhlükəsizlik qərarları verənlərə və auditorlara yönəldilir. Təşkilatın daxilində təhlükəsizlik proqramları ilə idarəetmə səviyyəsində qərar qəbul edir.
4. Şəbəkələr. Şəbəkələr unikal təhlükəsizlik zəifliklərı ilə əlaqədar xüsusi bir kateqoriya əmələ gətirir. Şəbəkə aspekti müəyyən bir təşkilatın şəbəkə tələblərinin təbiəti və tətbiqi ilə bağlıdır. Onun hədəfi şəbəkə menecerləri, şəbəkə xidməti mütəxəssisləri və şəbəkə xidməti təminatçılarıdır.
5. Sistemlərin inkişafı. Bu aspekt sistemin inkişaf etdiricilərinə ünvanlanır və sistem tələblərinin müəyyən edilməsi, tərtib edilməsi və tətbiqi ilə məşğul olur.

6. Son istifadəçi mühiti. Son istifadəçi mühiti şəxslərin təşkilatın sistemlərini və tətbiqlərini iş proseslərini dəstəkləmək üçün istifadə edilən mühitdir. Bu baxımdan belə son istifadəçi mühitlərində işləyən biznes menecerləri və şəxsləri hədəfə alır.

Kompüter qurğuları və şəbəkələri kritik biznes proqramlarının tətbiq edildiyi əsas informasiya təhlükəsizliyi infrastrukturuna müraciət edir. Son istifadəçi mühiti fərdi şəxslərin istifadəsində son nöqtədə korporativ və işçi stansiya proqramlarının qorunması ilə bağlı tənzimləmələri əhatə edir. Sistem inkişafı yeni proqramların və sistemlərin yaradılması ilə məşğul olur, təhlükəsizliyin idarəçiliyi isə yüksək səviyyəli nəzarətə ünvanlanır. Standartın özü tətbiqi tövsiyyələri əhatə edən geniş sənədlərlə tamamlanmış prinsip və məqsədlərdən ibarətdir.

Sürətlə dəyişən informasiya təhlükəsizliyində dünya valyutasının saxlanması üçün standart iki il ərzində nəzərdən keçirilir və yenilənir. SoGP standartına əlavə olaraq, İSF həmçinin İnformasiya Təhlükəsizliyi Status Sorğusu kimi tanınan iki illik qiymətləndirmə proqramını hazırlayır. İştirakçı təşkilatlar təhlükəsizlik sistemlərinin effektivliyi araşdırılır və nəticələr bir-birilə müqayisə edilir [21].

İSACA (İnformation System Audit and Control Association – İnformasiya Sistemlərinə Audit və Nəzarət Assosiasiyası) 1967-ci ildə Amerikada kompüter sistemlərində audit yoxlamaları ilə məşğul olan bir qrup şəxs tərəfindən bu sahə üzrə standarta ehtiyyac olduğunu hiss etdikləri zaman yaradılıb. 1969-cu ildə Stuart Tyrnaer EDP Auditorlar Assosiasiyası adlı bir təşkilat yaratdı. 1976-cı ildə assosiasiya informasiya texnologiyası idarəetmə və nəzarət sahəsinin bilik və dəyərini genişləndirilməsi sahəsindəki təhsil bazası kimi inkişaf etmişdir.

Bugün İSACA-nin 75000-dən çox üzvü vardır. İnformasiya texnologiyaları ilə əlaqəli müxtəlif mövqeləri əhatə edən üzvlər 160-dan çox ölkədə yaşayır və işləyirlər.

İnformasiya və əlaqəli texnologiyanın nəzarət məqsədləri (The Control Objectives for İnformation and related Texnology – COBİT) İSACA və İTGİ (İnformasiya Texnologiyalarının İdarəetmə İnistitutu) tərəfindən yaradılmış standartlar qrupudur.

COBİT ilk dəfə 1996-cı ildə hazırlandı. Onun missiyası "biznes menecerləri və auditorlar tərəfindən gündəlik istifadə olunan müasir, beynəlxalq, hamı tərəfindən qəbul edilmiş nəzarət obyektlərinin araşdırılması, inkişafı, ictimailəşdirilməsi ilə əlaqədardır". COBİT rəhbərliyə, auditorlara və digər istifadəçilərə İT sisteminin, təhlükəsizlik səviyyəsinin qərarlaşdırılmasını, eləcə də müəssisənin idarə etmək üçün hansı İT idarəetmə modelinin istifadə edilməsinin uyğun olduğunu anlamaqla kömək edir [29].

COBİT rəhbərliyə nəzarət tələbatları, texniki məsələlərdə və biznes riskləri problemlərindəki boşluqları doldurmağa icazə verir. COBİT 4.1-in sonuncu versiyası müəssisələrə İT sahəsində edilən dəyəri artırmağa və biznes proseslərini İT məqsədləri ilə əlaqələndirməyə, COBİT-in sadə şəkildə istifadə edilməsinə şərait yaradır. COBİT 4.1 ən yaxşı tənzimləmədir və COBİT-in daha əvvəlki versiyalarına əsasən işin effektivliyini artırmaq üçün istifadə edilir. COBİT 4.1 dörd bölmə üzrə təsnif edilən 210 nəzarət məqsədini əhatə edən 34 yüksək səviyyəli proseslərə malikdir: planlaşdırma və təşkilat; əhatə edilmə və həyata keçirilmə; çatdırılma və dəstək; monitorinq və qiymətləndirmə [21].

1. Plan və təşkiletmə. Bu kateqoriyada şirkətin öz hədəflərinə və məqsədlərinə çatmaq üçün informasiya texnologiyalarından necə istifadə edəcəyi təsvir olunur.
2. Əldə etmə və reallaşdırma. Bu bölmədə İT tələbatlarına uyğun texnologiya ilə əldə edilərək müəssisənin cari biznes proseslərində reallaşdırılır.
3. Çatdırılma və dəstək. Burada İT sistemi daxilində proqramların, eləcə də sistemin səmərəli icrasına imkan verən proseslərin mövcudluğunu əhatəliyir.
4. Monitorinq və qiymətləndirmə. Bu sahəyə şirkətin ehtiyyaclarını qiymətləndirmək strategiyası daxildir və hazırkı İT sisteminin müəssisə məqsədlərinə uyğun olub-olmaması müəyyənləşdirilir.

COBİT ISO/IEC 27002 standartları bir-birilə rəqabət aparır və bir-birini tamamlayır. COBİT standartı ISO/IEC 27002 standartından daha geniş sahəni əhatə edir.

The Bundesamt für Sicherheit in der Informationstechnik Almaniya hökümətinin kompüter və kommunikasiya təhlükəsizliyini idarə edən alman agentliyidir. Buraya kompüter proqramlarının təhlükəsizliyi, kritik qoruma infrastrukturu, internet təhlükəsizliyi, kriptoqrafiya, təhlükəsizlik mıəhsullarının sertifikatlaşdırılması, təhlükəsizlik test laboratoriyalarının akkreditasiyası sahələri daxildir. Mərkəzi Bonn şəhərində yerləşən agentliyin 400-dən çox işçisi vardır [20].

BSİ-nin ilk sələfi Almaniyanın xarici kəşfiyyat agentliyinin kriptoqrafik bölməsi idi. Agentlik hələ də Liberle şifrələnməsi kimi kriptoqrafik alqoritmlərin hazırlanması ilə məşğul olur.

BSİ alman standartı informasiya təhlükəsizliyi üçün nəzərdə tutulmuş metodların, əməliyyatların, prosedurların və yanaşmaların məcmusundan ibarətdir. Bu standart dövlət orqanlarının və müəsisələrin informasiya təhlükəsizliyi ilə əlaqədar bütün praktiki yanaşmaları əhatələyir.

BSİ alman standartı 100-1 seriyanın ilk standartı olub, İTİS üçün lazım olan ümumi tələbləri müəyyənləşdirir. Standart tamamilə ISO/IEC 27001 standartına uyğundur və ISO/IEC 13335 və 27002 standartlarına uyğun tövsiyyələri nəzərə alır.

Həmçinin alman metodologiyası kimi tanınan BSİ 100-2 standartı informasiya təhlükəsizliyinin necə qurulması və tətbiq edilməsinin sxemini müəyyənləşdirir. İT alman metodologiyası uyğun İT təhlükəsizlik ölçüsünün necə seçilməsi, təhlükəsizlik konsepsiyasının necə reallaşdırılmasını ətraflı şəkildə təsvir edir. Standart ISO/IEC 27001, 27002, 13335 standartlarının ümumi tələbləri şərh edilir və istifadəçilərə praktikada tətbiq etmələrinə kömək etmək üçün bir sıra nümunələr təqdim edir. İT alman kataloqları yalnız nə edilməli olduğunu izah etməklə yanaşı, tətbiqin necə görünəcəyinə dair xüsusi məlumatlar verir [20].

Seriyanın üçüncü standartı olan BSİ 100-3 risklərin analiznə əsaslanan metodlar ilə məşğul olur. Bu yanaşmadan hər birindən uğurla istifadə edərək risklərin təhlili xeyli asanlaşdırılır.

Bir təşkilat tələblərinə cavab verən informasiya təhlükəsizliyi standartlarına ehtiyac vardır. Bu səbəbdən də informasiya təhlükəsizliyini idarə etmək üçün yuxarıda qeyd olunan standartların birindən istifadə etmək lazımdır. Standartlardan hər hansı birinin tətbiqi müəssisəyə beynəlxalq səviyyəli faydalar verir və biznes ehtiyaclarını təmin etmək üçün biznes proseslərinin və fəaliyyətlərinin qorunmasını təmin edir. Yeganə problem təşkilatın təbiətinə və fəaliyyət sahəsinə uyğun standartın seçimi ilə bağlıdır. Çoxlu sayda fərqli informasiya təhlükəsizliyi standartları mövcud olsa da, onlar yalnız düzgün tətbiq edildiyi təqdirdə müəssisəyə fayda verə bilər.

Təhlükəsizlik bütün tərəflərin iştirak etməsi lazım olan sahədir. Rəhbərlik, praktiklər, İT mütəxəssisləri və istifadəçilər təşkilatın təhlükəsizliyinin təmin edilməsində əvəzedilməz rol oynayır. Təhlükəsizliyin müvəfəqiyyəti təşkilatın daxili və xarici bütün səviyyələrindəki tam əməkdaşlıq yolu ilə əldə edilə bilər.

2.2 Təhlükəsizlik siyasəti

İnformasiya təhlükəsizlik siyasəti təşkilatın idarə olunması, müdafiəsi, məlumat paylanması haqqında mövcud olan əmrlər, tənzimləmələr, qaydalar məcmusudur. Resursların ayrılması, rəqib hədəflər, təşkilatın strategiyası, texniki və informasiya resurslarının qorunması ilə bağlı olan qərarların qəbulunda menecerlər bir sıra çətinliklərlə üzləşir. Menecerlərin bütün səviyyələrdəki qərarları siyasətə təsir edir və siyasətin tətbiq etmə sahəsi rəhbərin səlahiyyətlərinə uyğun olaraq dəyişir. İnformasiya təhlükəsizliyi məsələləri üzrə idarəetmə qərarları bir-birindən fərqlənir. Siyasətin müxtəlif növlərini fərqləndirmək məqsədilə onları 3 əsas kateqoriyaya bölürlər: proqram siyasəti, xüsusiləşdirilmiş təhlükəsizlik siyasəti, baza təhlükəsizlik siyasəti.

Siyasət geniş səviyyədə yazıldığından təşkilatlar bir sıra standartlar, qayda və prosedurlar təklif edirlər ki, onlarda öz növbəsində istifadəçilərin, menecerlərin, sistem administratorlarının və işçi heyətin siyasəti tətbiq etməsinə, təşkilatın hədəflərinə çatmasında əvəzedilməz rol oynayır. Standartlar və qaydalar təhlükəsizlik sistemlərində istifadə olunan xüsusi texnologiyalar, metodlar çoxluğudur. Prosedurlar isə təhlükəsizliklə bağlı məsələlərin həllində istifadə edilən daha detallı addımlardır. Standartlar, qaydalar, prosedurlar tənzimləmələr kitabçasında qeyd edilir.

Təşkilat standartları məqsədə çatmaq üçün istifadə olunan xüsusi texnologiyalar, parametrlər, prosedurlardır. Təşkilatın geniş identifikasiyası nişanların standartlaşdırılması işçilərin rahatlığını, giriş-çıxış sistemlərinin avtomatlaşdırılmasını təmin edir. Standartların müəyyən edilməsi məcburi prosesdir.

Təlimatlar istifadəçilərin, sistem işçilərinin və digər şəxslərin təhlükəsizliyini təmin edir. Sistemin hansı dərəcədə əhəmiyyətli olması təlimatlar vasitəsilə müəyyən edilir. Məsələn, təşkilat təlimatları sistemin xüsusi standart prosedurlarının inkişafına kömək etmək məqsədilə istifadə edilə bilər. Məlumatların düzgün istifadəsinin birdən çox yolu ola bilər.

Prosedurların köməyi ilə müvafiq təhlükəsizlik siyasətinin, standartlarının və təlimatların necə tətbiq ediləcəyi təsvir olunur. Onlar müəyyən bir vəzifəni yerinə

yetirmək üçün istifadəçilər, sistem işçiləri tərəfindən atılan addımların məcmusudur (məsələn, yeni istifadəçi hesabları yaratmaq və müvafiq səlahiyyətlərin verilməsi).

Proqram siyasəti təşkilatın informasiya təhlükəsizlik proqramını yaratmaq üçün istifadə olunur. Bu siyasət vasitəsilə təhlükəsizlik strategiyaları qurulur və təşkilat daxilində reallaşdırılması üçün resurslar təyin edilir. Bu yüksək səviyyəli siyasət təşkilatın məqsədini müəyyənləşdirir, uyğun məsələləri əlaqələndirir, işçilərin, istifadəçilərin müəssisə daxilində rollarını təyin edir [12].

Proqram siyasətinin bir neçə əsas komponenti vardır:

Məqsəd. Siyasətin şərhində proqramın məqsədi və hədəfləri təsvir olunur. Yaradılmış siyasət planında tamlıq, əlyetənlik, konfidensiallıq kimi təhlükəsizlik ilə bağlı olan prinsipləri təmin edilməlidir. Buna misal olaraq, böyük müəssisələrdə səhvlərin sayının azaldılması, məlumat itkisi və bərpası kimi proseslərin idarə edilməsini xüsusilə vurğulamaq olar. Bu səbəbdən də belə şirkətlərin əsas məqsədi konfidensial şəxsi məlumatların qorunması və icazəsiz daxilolmalara qarşı güclü müdafiə sistemi yaratmaqdır.

Əhatə sahəsi. Aydındır ki, proqram siyasətinə təhlükəsizliyi təmin edilən resurslar (qurğular, aparat və proqram təminatı) daxildir. Əksər hallarda proqram bütün sistemləri əhatə edir, lakin bəzən isə təşkilatın informasiya təhlükəsizliyi proqramının əhatə dairəsi daha məhdud ola bilər. Məlumdur ki, gizli və ya yüksək təsirli sistemdə saxlanan məlumatları qorumaq üçün nəzərdə tutulan aşağı səviyyəli bir sistemin təmin edilməsi üçün nəzərdə tutulan bir siyasətdən daha sərt olacaqdır.

Cavabdehlik. İnformasiya təhlükəsizliyi proqramı qurulduqdan sonra onun rəhbərliyi adətən, yeni yaradılmış və ya mövcüd olan ofisə verilir. Təşkilatdakı vəzifəli şəxslərin öhdəçilikləri müəssisə daxilində müəyyən edilməlidir. Siyasət bəyannaməsinin bu hissəsi, məsələn, göstərilən xidmətlərdən istifadə edən informasiya xidmətləri göstəricilərinin və ərizələrin idarəçiləri arasında olan məsuliyyətləri fərqləndirəcəkdir. Bu cür siyasətdən həm də yüksək riskli və ya təşkilati əməliyyatlar üçün çox vacib təhlükəsizlik ofislərinin yaradılmasında istifadə edilir. Siyasət həmçinin işçi heyətin rollarını və öhdəçiliklərini müəyyənləşdirir [5].

Uyğunluq. Proqram siyasəti adətən, 2 uyğunluq məsələsini həll edir:

1. Ümumi uyğunluğa proqramın qurulmasına aid tələblər və təşkilat komponentlərinə verilmiş öhdəçiliklər daxil edilir. Nəzarət qurumları təşkilatın rəhbərlərinin öz səlahiyyətlərindən necə istifadə etməsidə daxil olmaqla uyğunluğu izləmək məsuliyyəti daşıyır.

2. Müəyyən edilmiş cərimələrin və intizam tədbirlərinin istifadəsi. Təhlükəsizlik siyasəti yüksək səviyyəli bir sənəd olduğundan normal olaraq müxtəlif pozuntulara görə olan xüsusi cəzalar burada detallı şəkildə qeyd olunur. Onun əvəzinə siyasət bəyannaməsində xüsusi intizam tədbirləri daxil edilmiş uyğunluq strukturu yaradılır.

Uyğunluq siyasətini tətbiq edən zaman xatırlamaq lazımdır ki, işçi səlahiyyətlərinin pozulması bəzən qərəzsiz ola bilər. Uyğunsuzluq bəzən bilik və ya iş təcrübəsinin çatışmamazlığının nəticəsi ola bilər. Bəzi hallarda şəxslərə cəza tədbirləri tətbiq edilməzdən əvvəl mütləq müvafiq hüquq məsləhətçilərindən təlimat almaq lazımdır. Qanunla qeyd olunmuş cəza tədbirləri siyasət planında təkrarlanmağa ehtiyyac duyulmur.

Təhlükəsizliyin baza siyasəti cari narahatlıq sahələrinin aradan qaldırılmasına yönəlmişdir. Təşkilat daxilində işçilərin xüsusi təlimatlara, əmrlərə uyğun şəkildə sistemdən istifadəsinin təmin edir. Baza siyasəti müəssisə tərkibinə daxil olan texnologiyaya aid edilir və aydın şəkildə istifadə qaydaları qeyd olunur. Proqram siyasətindən fərqli olaraq müəssisə daxilində baş verən texnoloji dəyişiklikləri də nəzərə alır.

Baza siyasətinin uyğun olduğu bəzi sferalar vardır. Hər yeni texnologiya və yeni hədələrin aşkar edilməsi tez-tez baza siyasətinin yaradılmasını təmin edir. Siyasətə daxildir:

İnternətə çıxış. İnternətə qoşulmaq bir çox uğura səbəb olsa da bəzən problemlərin yaranmasına da səbəb olur. İnternetə çıxış siyasəti vasitəsilə kimin giriş imkanı əldə etdiyi, şəbəkəyə daxil olan sistemlərin növləri, şəbəkə üzərində ötürülən informasiya haqqında məlumat, internətə qoşulu olan sistemlər üçün mövcud istifadəçi identifikasiya tələbləri müəyyən edilir.

Mail gizliliyi. Bu siyasət ilə toplanmış, saxlanmış informasiyadan istifadə yolları aydınlaşdırılır. Rəhbərlik işçilərin sistemdən yalnız iş məqsədləri üçün istifadə etdiyinə, təhlükəli obyektlər göndərməyinə, məxfi informasiyanın paylanmamasına nəzarət edir. İstifadəçilər email ilə əlaqədar müəyyən bir təhlükəsizlik səviyyəsi yarada bilər və bu siyasət məxfilik səviyyəsinin nə dərəcədə gözlənildiyini, həmçinin, hansı şərtlər daxilində mailin məzmununun oxuna biləcəyini təyin edir.

Şəxsi kompüterdən iş yerində istifadə siyasəti fərdlərə öz qurğularından istifadə imkanı yaradır. Siyasət məhsuldarlığın artmasına, təşkilat xərclərinin azalmasına nəzarət edir. Müxtəlif əməliyyat sistemlərində işləmə nəinki təşkilatın informasiya təhlükəsizliyini, həm də işçi məxfiliyini təmin etməkdə şirkət şəbəkəsində problemlərə yol açа bilər. Belə hər tərəfli siyasət qurğulara və istifadəçi davranışlarına xüsusi qaydalar şəklində tətbiq edilir.

Sosial medya. Şirkətin öz hesabı olmasa belə, istifadəçilərin var. Sosial medya hesabı siyasətinin olması təşkilatı və işçiləri qorumaq üçün vacib hesab olunur. Siyasətdə istifadəçilər üçün müxtəlif sosial medya platformalarından istifadə qaydaları öz əksini tapmışdır. Müəssisələrdən asılı olaraq siyasət çox ciddi (heç bir istifadəçiyə sosial medyadan istifadəyə icazə verilmir) və ya yumşaq (müəyyən qaydalar çərçivəsində icazə verilir) ola bilər.

Siyasətə digər mövzularda daxil edilir: risklərin idarə edilməsi və fövqəladə planlaşdırma yanaşması, konfidensial informasiyanın qorunması, icazəsiz avadanlıqların istifadəsi, siyasətin pozulması, daxili yaddaşda istifadədən gizlilik hüquqları, fiziki fəsadlar.

Baza siyasəti bir neçə komponentdən ibarətdir:

Problemin şərhi. İnformasiya sahibi siyasəti formalaşdırmaq üçün məsələ ilə bağlı terminləri, şərtləri müəyyənləşdirməlidir. Bu, adətən, uyğunluğu asanlaşdırmaq üçün siyasətin əsaslandırılması və hədəfi dəqiqləşdirmək üçün faydalı hesab edilir. Məsələn, müəssisə şirkət tərəfindən təsdiq edilməyən, satın alınmayan, nümayiş etdirilən, idarə olunmayan sıradan "qeyri-rəsmi proqramdan" istifadəsinə qarşı xüsusi siyasət hazırlamaq istəyir. Əlavə olaraq, bəzən yalnız iş mühitində istifadəsinə icazə

verilən və ya başqa bir müəssisə ilə razılıq əsasında həmin şirkətin proqramları tətbiq oluna bilər.

Təşkilatın mövqeyinin müəyyənləşdirilməsi probleminin aydınlaşdırılması əsas komponentlərdən biridir. Əvvəlki hissədəki nümunəyə əsaslanaraq qeyri-rəsmi proqramın bəzi və ya bütün hallarda qadağasını, təsdiq, istifadə üçün əlavə qaydaların, kimə, nəyə əsaslanaraq istisnaların olub-olmamısını müəyyənləşdirmək bu komponent vasitəsi ilə aydınlaşdırılır.

Tətbiq oluna bilmə. Hər bir siyasətin tərkibinə daxil olan bu komponent siyasətin harda, necə, nə zaman, kim tərəfindən və niyə tətbiq olduğunu aydınlaşdırır. Qeyri-rəsmi proqram təminatında tətbiq edilən hipotetik siyasət yalnız müəssisənin daxili resurslarına və işçilərinə aid edilir. Əlavə olaraq, siyasətin mümkünlüyü müxtəlif yerlərə səyahət edən işçilər arasında evdə çalışan müxtəlif yerlərə disklər vasitəsi ilə ötürülmədə özünü doğrultmalıdır.

Rolların və öhdəçiliklərin təyini də bəzən baza siyasətinə daxil edilir. Əgər müəssisə daxilində işçilər öz şəxsi sistemlərindən istifadə edirsə, bu zaman bir sıra icazə şərtləri qoyulur. Əks təqdirdə təsdiqlənmiş proqramdan istifadə edən şəxslərin hansı resurslara əlçatan olduqları müəyyən edilməlidir.

Müvafiqlik. Bəzi tip siyasətlərdə pozuntuların və pis niyyətli hərəkətlərin nəticələri daha ətraflı şəkildə təsvir edilməsi qəbul edilməzdir. Cəza tədbirləri açıq şəkildə göstərilir və təşkilatın işçi siyasətinə uyğunlaşdırılır. İstifadə zamanı siyasət müvafiq rəhbərliklə, hətta işçilərin müvaqilələri ilə belə əlaqələndirilir. Həmçinin xüsusi vəzifəni yerinə yetirən zaman monitorinq uyğunluğunada ehtiyac yaranır.

Əlaqə nöqtələri və tamamlayıcı informasiya. Hər bir baza siyasətində işçi şəxslərin təşkilat ilə olan əlaqəsi aydın şəkildə göstərilir. Heyətin mövqesinin, vəzifəsinin gec-gec dəyişməsi siyasətdə əlaqə nöqtələri kimi qeyd olunur. Müxtəlif növ məsələlərin həlli üçün nəzərdə tutulan əlaqə nöqtələrinə misal olaraq təsis müdiri, sistem administratorunu, texniki qurğuları dəstəkləyən şəxs və ya təhlükəsizlik proqramı təmsilçisini göstərmək olar.

Daha geniş olan yüksək səviyyəli proqram və baza siyasəti müəssisə daxilində cari sistemdə icazə verilən hərəkətləri müəyyənləşdirərək informasiya ilə təmin edən xüsusiləşdirilmiş təhlükəsizlik siyasəti əsasında yazılır. Bu siyasət müəssisə tərkibindəki xüsusi texnologiyalar ilə bağlı olduğundan baza siyasəti ilə oxşardır. Bununla yanaşı, xüsusiləşdirilmiş siyasət təşkilatın informasiya təhlükəsizliyi ehtiyaclarını ödəmək üçün lazım olan təhlükəsizlik nəzarətinin həyata keçirilməsinə cavabdeh olan kadrlara uyğun təklükəsizlik konfiqurasiyası hazırlayır [14].

Qarşılıqlı və hərtərəfli təhlükəsizlik siyasəti yaratmaq üçün müəssisə rəhbərliyi təhlükəsizlik qaydalarından istifadə edir. Sistemin təhlükəsizlik siyasəti üçün 2 səviyyəli model irəli sürülür: təhlükəsizlik obyektləri və təhlükəsizlik qaydaları. Qarşılıqlı sıx əlaqədə olan və tez-tez çətinliklə ayırd edilən texnologiyalar vasitəsi ilə siyasətin həyata keçirilməsidir. Xüsusiləşdirilmiş siyasətdə müəyyən edimiş zaman çərçivəsində cari təhlükəsizlik prosedurları ilə uyğunluğun təmin edilməsinə baxış tövsiyyə olunandır.

İdarə proseslərində ilk addım təhlükəsizlik obyektlərini müəyyənləşdirməkdən ibarətdir. Hər kəsə məludur ki, bu proses tamlığın, konfidensiallığın, əlyetənliyin analizi ilə başlanır. Təhlükəsizlik obyektləri xüsusi, dəqiq, yaxşı təyin edilmiş və aydın təsvir edilmiş olmalıdır. Səhmdarlar praktiki, ətraflı siyasətin yaradılmasında əhəmiyyətli rol oynayırlar. Bu səbəbdən də siyasətin təkcə rəhbərlik işçiləri üçün yaradılmadığını unutmamaq vacibdir.

Obyektlər müəyyənləşdirildikdə isə müəssisənin idarə edilməsi və fəaliyyəti üçün qaydalar toplusu tərtib edilməli və sənədləşdirilməlidir. Qaydalar əsasında icazəli dəyişikliklər (səlahiyyətlərə uyğun olaraq informasiyanın yazılması, sinifləşdirilməsi) müəyyənləşdirilir. Spesifikliyin dərəcəsi təhlükəsizliyinin fəaliyyətindən asılı olaraq sistemdən sistemə dəyişir. Daha detallı şəkildə təsvir edilmiş qaydalar administratorlar üçün istifadəsi daha rahatdır. Detallı təsvir həm də avtomatik mühafizəni səmərələşdirir.

Əlavə olaraq detalların səviyyəsinin qərarlaşdırılması ilə rəhbərliyin xüsusiləşdirilmiş siyasətin formallıq dərəcəsi müəyyənləşdirilir. Bir daha qeyd etmək

olar ki, daha formal sənəd vasitəsi ilə mühafizə və siyasət planını izləmək daha sadədir. Sistemdən istifadə qaydaları və uyğunsuzluğun nəticələri qeyd olunmalıdır. Girişə nəzarət siyasətinin sənədləşdirilməsi əhəmiyyətli dərəcədə sistemin təhlükəsizliyini təmin edir [7].

İnformasiya təhlükəsizliyinin digər sahələrindəki qaydalar risklərin analizi, akkreditasiya hesabatları və ya prosedur təlimatları şəklində sənədləşdirilir. Mübahisəli, qeyri-adi siyasətlərdə də formal bəyannamələr tərtib etmək lazımdır. Xüsusi siyasətlər yaradılan zaman standart müəssisə siyasətində mövcud olan yayınmaların səbəbi izah edilir.

Təhlükəsizlik siyasəti bir neçə mövzu ilə qarşılıqlı əlaqədədir:

Proqramların idarə edilməsi. Siyasət təşkilatın informasiya təhlükəsizlik proqramını yaratmaq məqsədilə yaradılır və proqram idarəetməsi, administrasiyası ilə sıx əlaqəlidir. Bu səbəbdən də müəssisə üçün həm proqram, həm də baza siyasəti yaratmaq olar. Siyasət planının hazırlanması şirkətin məqsədlərindən, yanaşmalarından asılıdır. Digər tərəfdən sistemin hissələri bir-birindən kifayət qədər ayrı olduğundan sistem sahibləri baş vermiş problemləri öz individual bazaları əsasında aradan qaldıra bilərlər.

Girişlərə nəzarət. Xüsusiləşdirilmiş sistem siyasəti adətən, giriş nəzarətlərini həyata keçirir. Məsələn, müəssisədə yalnız 2 işçi printerdən istifadə etmək icazəsinə malikdir. Sistemdəki giriş nəzarəti digər şəxslərin printerdən istifadəsinə şərait yaratmır.

Genişləndirilmiş təşkilat siyasətləri ilə əlaqə. Anlamaq vacibdir ki,. informasiya təhlükəsizlik siyasəti digər müəssisə siyasətlərinin davamıdır. Çaşqınlığı minimuma endirmək üçün informasiya təhlükəsizliyi ilə müəssisə siyasəti arasındakı dəstək və koordinasiya qarşılıqlı olmalıdır.

Bir sıra potensial xərclər informasiya təhlükəsizlik siyasətinin reallaşdırılması ilə əlaqədardır. Ən əlamətdar xərclər siyasətin həyata keçirilməsinə və onun müəssisəyə resurslar və kadr heyətinə sərf olunur. Təhlükəsizlik proqramının yaradılmasına külli miqdarda vəsait tələb olunur.

Digər xərclər siyasət tətbiq olunan zaman meydana çıxır. Layihələndirmə, koordinasiya, siyasətin yayılması və ictimailəşdirilməsi çəkilən xərclər administrativ xərclər siyahısına aid edilir. Əksər müəsisələrdə uğurlu siyasət planının reallaşdırılması zamanı əlavə işçi heyətinə və kadr hazırlığına ehtiyyac duyulur. Ümumilikdə, çəkilən xərclərin miqdarı təşkilatın hansı səviyyədə risklərin aradan qaldırılmasını planlaşdırması ilə bağlı olur.

İnformasiya və sistem təhlükəsizliyinə sərf olunan xərclər hər bir təşkilat üçün qaçınılmazdır. Obyektlərin mühafizəsinin təmin edilməsi tələb olunan təhlükəsizlik ilə onun dəyəri arasındakı balans mütənasibdir.

2.3 Təhlükəsizlik modelləri

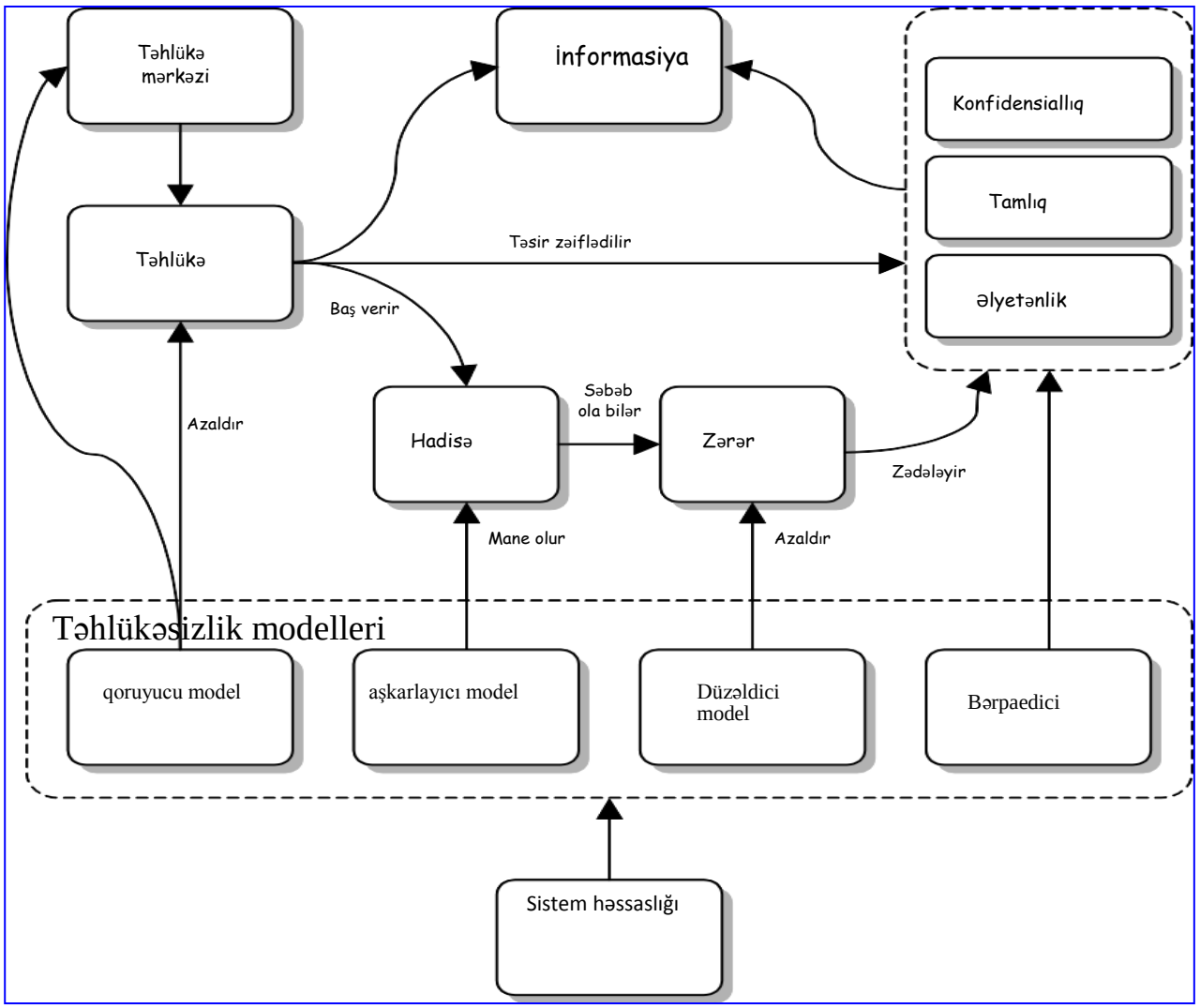
İnformasiya təhlükəsizliyi nəzarət funksiyasına (qoruyucu, aşkarlayıcı, düzəldici, əngəlləyici, tarazlaşdırıcı) və tətbiq edilmə sahəsinə (fiziki, inzibati, texniki) görə təsnifləşdirilə bilər. Fiziki nəzarətə qapılar, müdafiə qurğuları, yanğın çıxışları, havalandırma daxildir. İnzibati nəzarətə təşkilatın informasiya təhlükəsizliyi siyasəti, prosedurları daxil edilir. Texniki nəzarətə isə qoruyucu divar, identifikasiya sistemləri, zorla müdaxiləni aşkarlayan sistemlər, fayl şifrələnməsi kimi müxtəlif texniki vasitələri göstərmək olar [10].

Qoruyucu nəzarət modeli: Pis niyyətli şəxs ilk olaraq bu nəzarət sistemi ilə qarşılaşır. Bu nəzarət sistem təhlükəsizlik pozuntularının qarşısının alınması məqsədilə istifadə edilir. Digər nəzarət sistemləri kimi bu sistem də 3 cür ola bilir:

- Fiziki (yanğın çıxışları);
- İnzibati (təhlükəsizlik prosedurları);
- Texniki (zorla müdaxiləni aşkarlayan sistemlər).

Aşkarlayıcı nəzarət pozuntuları müəyyən etmək və bu haqda xəbər vermək funksiyasını yerinə yetirir. Belə model qoruyucu nəzarət sistemi sıradan çıxan zaman işləməyə başlayır. Aşkarlayıcı idarəetmə sistemlərinə kriptoqrafik sistemlər, faylın tamlığına nəzarət sistemləri, audit yazıları daxildir.

Düzəldici nəzarət modeli baş vermiş pozuntuları əmələ gətirdiyi vəziyyəti düzəltmək məqsədilə tətbiq edilir. Pozuntu zamanı əgər hər şey zədələnməyibsə, bu nəzarət modeli sistemi əvvəlki vəziyyətinə qaytarmağa çalışır. Tətbiq edildiyi sahəyə görə düzəldici təhlükəsizlik modeli dəyişə bilər və təbii olaraq, texniki, inzibati növləri vardır.



Sxem. Təhlükəsizlik modellərinin işləmə mexanizminin qrafiki təsviri

Əngəlləyici nəzarət sisteminə hücum olunmasının qarşısını alan idarəetmədir. Buraya informasiya təhlükəsizliyinin idarəedilməsində meydana gələn pozuntuların monitorinqi, yazılışı daxildir.

Bərpaedici nəzarət düzəldici modelə oxşayır, lakin onlar daha ciddi pozuntuları aradan qaldırmaqda, məlumat qaynaqlarını yenidən qurmaq məqsədilə istifadə edilir. Buraya iş davamlılığı mexanizmləri, ehtiyyat sistemləri, fövqəladə idarəetmə qaydaları daxildir.

Kompensasiya edici nəzarət dedikdə əsas idarəetmələr sıradan çıxdığı hallarda onu digər alternativlərlə əvəz olunması başa düşülür. Bu zaman eyni

hədələrin həllinə digər ikinci bir qrup nəzarət dəstəsi yönəldilir. Yeni yönəldilmiş dəstə kompensasiya edici nəzarət dəstəsi adlanır.

Giriş nəzarət modelləri:Aktual giriş nəzarət mexanizmlərinin və sistemlərinin qurulmasında məntiqi giriş nəzarət modelləri abstrakt rolunu oynayır. Giriş nəzarəti kompüter təhlükəsizliyinin ən vacib konsepsiyalarından biridir. Bu model vasitəsi ilə subyektlərin (istifadəçilərin, digər kompüterlərin, proqramların) obyektlərə (kompüterlərə, fayllara, serverlərə, qurğulara) girişi həyata keçirilir. 3 əsas giriş nəzarət modeli vardır:

- İxtiyari giriş nəzarət modeli (Discretionary Access Control-DAC);
- Mandat idarəetmə modeli (Mandatory Access Control-MAC);
- Əlyetənliyə nəzarətin rol modeli (Role-Based Access Control-RBAC).

İxtiyari giriş nəzarət modeli mövcud olan 3 modeldən ən çox istifadə olunan modeldir. DAC modelində məlumat (fayl, kataloq) sahibi (yaradıcısı) həmin obyektə girişə müəyyən məhdudiyyətlər qoyur. Bu modelin üstünlüyü onun istifadə rahatlığıdır: istifadəçi məlumatdan kimin necə istifadəsinə-oxumasına, yazma, silmə, adını dəyişməsinə qərar verə bilər. Belə rahatlıq həm də DAC modellərinin çatşmamazlığıdır, çünki hər hansı yalnış qərar təklükəli, uyğunsuz vəziyyətlərin yaranmasına səbəb ola bilər. Bütün bunlara baxmayaraq, DAC modeli bugün əksər əməliyyat sistemləri üçün ilkin model seçim olaraq qalır.

Mandat idarəetmə modeli adından göründüyü kimi girişlərə nəzarət üçün daha sərt yanaşma tələb edir. MAC modeli tətbiq edilən sistemlərdə istifadəçi öz məlumatlarına giriş icazəsi qoya bilmir. Düzgün istifadə zamanı ixtisaslaşdırılmış təhlükəsizlik siyasətinə malik olan MAC əsaslı sistemlər DAC modelli sistemlərdən daha etibarlıdır və əlavə məhdudiyyətlər yalnız əməliyyat sistemi tərəfindən müəyyən edildiyi üçün istifadəsi daha mürəkkəbdir. MAC nəzarət modelinə əsaslanan sistemlər yüksək təhlükəsizlik tələb edən hökümət, hərbi, maliyyə sahələrində istifadə

edildiyi üçün mürəkkəbdir, ona görə də qiyməti bahadır. Bu modeldən yüksək səviyyəli təhlükəsizliyi təmin etmək məqsədi ilə Solaris əməliyyat sisteminin Frusted Solaris versiyasında uğurla tətbiq edilir.

Əlyetənliyə nəzarətin rol modelində icazələr və hüquqlar fərdi istifadəçinin roluna əsaslanaraq təyin edilir. Əlavə edilmiş icazə təbəqəsi girişlərə nəzarət edilməsini daha rahat və asan hala gətirir. Bu sistemin ən üstün cəhətlərindən biri istifadəçi rolunun asanlıqla ləğv edilməsidir. Belə yanaşmanın tətbiqi ilə minlərlə işçisi olan təşkilatların təhlükəsizliyinin, etibarlılığının qorunması prosesi həyata keçirilir. Solaris əməliyyat sistemi 8-ci versiyadan başlayaraq RBAC modelini dəstəkləyir [10].

Əlyetənliyə nəzarətin rol modeli ilk dəfə 70-ci illərdə çox istifadəçili və çox tətbiqetməli sistemlərdə istifadə olunmağa başlandı. RBAC modelinin əsas xüsusiyyəti sistem istifadəçilərinin icazələrini onların rolları ilə əlaqələndirilir və onlara uyğun rollar təyin etməkdir. Rollar təşkilatda müxtəlif iş funksiyaları əsasında yaradılır və istifadəçilərinin sistemdə fəaliyyəti ilə bağlı olan öhdəçiliklərinə əsaslanır. İstifadəçilər asanlıqla müəssisədə öz rollarını dəyişə bilirlər.

Rollar adətən, stabil olur, buna səbəb isə təşkilat məqsədlərinin və ya funksiyaların gec-gec dəyişməsidir. Rol əlyetənliyə nəzarət siyasəti formallaşdırılan zaman semantik şəkildə təsvir edilir. Bu siyasətdə rolların icazəsi, istifadəçi rolu, rollar arasındakı əlaqə kimi RBAC modelinin müxtəlif komponentləri təcəssüm etdirilir[20].

RBAC modelinin siyasəti neytraldır və 3 əsas təhlükəsizlik prinsipini dəstəkləyir: az səlahiyyət vermə, vəzifələrin bölgüsü və məlumatın mücərrədliyi. Az səlahiyyət vermə prinsipinin dəstəklənməsinin səbəbi modeldə yalnız istifadəçi vəzifələrinin yerinə yetirilməsi üçün tələb olunan icazələr konfiqurasiya edilir. Vəzifə bölgüsü həssas bir tapşırığı yerinə yetirmək üçün xüsusi rolların təyin edilməsini təmin edir. Məlumat mücərrədliyi prinsipi ilə bank hesabları, kredit kimi şəxsi icazələr müəyyən edilir.

Artıq məlumdur ki, RBAC modelinin bütün komponentləri tək bir şəxsin nəzarəti altındadır. Böyük sistemlərdə yüzlərlə, hətta minlərlə rol ola bilər. Bütün rollar və onlar arasındakı əlaqələr təhlükəsizlik administratorları tərəfindən müəyyənləşdirilir.

RBAC modeli aşağıdakı komponentlərə malikdir[10]:

U, R, P və S (uyğun olaraq istifadəçilər, rollar, icazələr, sesiyalar göstərir)

PA $\subseteq$ P x R – "çoxluğun-çoxluğa" münasibəti vasitəsilə icazələrin təyini

UA$\subseteq$U x R – "çoxluğun-çoxluğa" münasibəti ilə istifadəçilərin təyini

RH $\subseteq$ R x R – iyearxix qoşulmaya malik rolların hissə-hissə düzülməsi.

Mərkəzləşdirilmiş və paylanmış giriş nəzarətləri arasında bir sıra fərqliliklər vardır. Paylanmış giriş nəzarətində qərar qəbul edilir və paylanmış qaydada tətbiq edilir, mərkəzləşdirilmiş giriş nəzarəti sistemlərində isə qərarların, sistemlərin idarə edilməsində istifadə edilir. Hər iki yanaşmanın üstünlüıləri və çatışmamazlıqları vardır, ümumilikdə hansı birinin daha yaxşı olduğunu demək çətindir. Lazımı giriş nəzarət yanaşmasının seçimi təşkilatın tələblərindən və hədəflərindən asılıdır.

Bell La Padula 1973-cü ildə David Elliot Bell və Leonard J. La Padula tərəfindən yaranmış informasiyanın konfidensiallığını qorumağa xidmət edən ən tanınmış modellərdən biridir. 70-ci illərdə ABŞ-ın hərbi sahəsində meynfreymlərlə paylaşılan informasiyanın təhlükəsizliyini təmin etmək əsas məsələlərdən biri idi, məhz bu səbəbdəndə Bell La Padula modeli yarandı. Eyni meynfreymlərdən istifadə edən çox saylı istifadəçilər mövcüd informasiyanı qorumağa diqqət yetirdi. Belə qoruma sistemi çox səviyyəli təhlükəsizlik sistemi adlanır. Model vasitəsilə sistemdə müxtəlif təsnifat səviyyələrinə uyğun informasiyalar müdafiə olunur. Riyazi cəhətdən özünü təsdiqləmiş model bugün hələ də uğurla tətbiq edilir. Təsnifat mərhələləri aşağıdan ən yuxarıya doğru qiymətləndirilir: qeyri-konfidensial, konfidensial, məxfi, tamamilə məxfi fayllar [10].

Obyekt sistemdə yerləşən hər hansı bir fayl və ya məlumat, subyekt isə həmin obyektlərdən istifadə edən istifadəçidir. Modeldə obyekt və subyekt arasında fərqli səviyyələrdə təhlükəsizlik əldə olunur. Hər bir subyekt obyektdən yalnız əvvəlcədən

müəyyən olunmuş səviyyədə istifadə edə bilər. Ümumilikdə, 2 tip əsas giriş xüsusiyyəti vardır:

1. Qeyri-konfidensial şəxs konfidensial məlumatı oxuya bilməz.

2. Tam məxfi məlumat qeyri-məxfi səviyyədə yazıla bilməz.

Bell La Padula modeli əlyetənliyin mandat idarəetmə modellərindən biridir. Bu modelinin bir sıra çatışmamazlıqları vardır:

- Təkcə konfidensiallığa yönəlməsi;
- Həddindən artıq mürəkkəb olması;
- Vaxtaşırı verilənlərin təsnifatlaşdırılmasında bir sıra problemlərin yaranması;
- Məlumatların "yüksək" təhlükəsizlik təsnifatlarına uyğun yazılmasına baxmayaraq daim istifadəçi tərəfindən nəzarətdə saxlanılmalıdır.

Modelin 3 əsas konfidensial siyasəti vardır:

1. Sadə təhlükəsizlik siyasəti – məxfi və qeyri-məxfi istifadəçi faylları oxuya bilməz.

2. Ulduz siyasəti – subyektin qeyri-məxfi fayllara yazmağa icazəsi yoxdur;

3. Güclü ulduz siyasəti – subyekt məxfi və ya qeyri-məxfi obyektləri oxuya və ya yaza bilməz.

Biba tamlıq modeli 1977-ci ildə Mitre Korporasiyası tərəfindən hazırlandı. Yuxarıda qeyd olunduğu kimi Bell La Padula modeli məlumatın təkcə konfidensiallığını təmin edirdi. Nəticədə hazırlanmış Biba modeli kompüter sistemlərində informasiyanın tamlığının qorunmasına yönəlmişdi. Modeldə müxtəlif tip tamlıq siyasətlərindən istifadə edilərək fərqli şərtlər altında informasiya tamlığı qorunurdu.

Biba modelində hər bir subyektə və obyektə tamlıq nişanı verilir. Nişanlar təklikdə informasiyanı qoruya bilmir, onlar təhlükəsizlik mexanizmləri ilə birlikdə tətbiq edilir. Adətən, təhlükəsizlik nişanları sabit olur, lakin bəzən dinamik nişanları

dəstəkləyən Biba modelində dəyişə bilirlər. Modeldə həm statik, həm də dinamik nişanlardan istifadə oluna bilər. Dinamik nişanlar tamlıq səviyyəsinə uyğun dəyişikliklərə icazə verir.

Tamlıq nişanı 2 hissədən ibarətdir: təsnifat və kateqoriyalar qrupu. Tamlığın təsviri iyearxiya şəklindədir və 3 səviyyədədir: kritik, vacib və az əhəmiyyətli. Kritik ən yüksək, az əhəmiyyətli isə ən aşağı təsnifat səviyyəsidir. Bu halda kritik > vacib > az əhəmiyyətli. Nişanın ikinci hissəsi bütöv sistemdəki kateqoriyalar çoxluğunun alt çoxluğudur. Hər bir tamlıq səviyyəsi L=(C,S) kimi təsvir edilir. Burada L tamlıq səviyyəsi, C təsnifat, S kateqoriyalar çoxluğudur [7].

Biba modelində digər modellərdə də olduğu kimi oxşar giriş rejimləri mövcuddur:

Dəyişdirmək rejimi – Subyektə obyekti yazmağa icazə verir.

Müşahidə rejimi – Subyektə faylı yalnız oxumağa icazə verir.

Əlaqə rejimi – Subyektin digər subyektlərlə əlaqə yaratmasına təmin edir.

İcra rejimi – Subyektin obyekti (proqramı) icra etməsinə icazə verir.

Bell La Padula modeli ilə müqayisədə daha rahat tətbiq edilən bu modelin bir sıra çatışmamazlıqları vardır. İlk problem mövcud siyasətlər içərisində düzgün siyasətin seçimi ilə bağlıdır. Digər çatışmamazlıq isə məlumatın konfidensiallılığının təmin olunmamasıdır. Bu səbəbdən də model digər modellərlə birləşdirilərək istifadə olunur. Lipner modeli Bell La Padula və Biba modellərinin birləşdirilməsindən yaranan modeldir. Modelin digər mənfi xüsusiyyəti isə icazələrin verilməsi və ləğvinin dəstəklənməməsidir.

Bella La Padula modelində əsas məqsəd yüksək təhlükəszilik səviyyəsindən aşağı təhlükəszilik səviyyəsinə informasiya axınını təmin etməkdir. Biba modelində əsas məqsəd isə yüksək tamlıq səviyyəsindən aşağı tamlıq səviyyəsinə doğru informasiyanın hərəkətini reallaşdırmaqdan ibarətdir. Hər iki modeldə informasiya axın modelidir. İnformasiya axın modeli təkcə informasiyanın axını ilə deyil, həm də müxtəlif növ verilənlərlə əlaqəlidir. Belə tip modellər vasitəsilə eyni və ya fərqli səviyyələr arasındakı axınlarla birlikdə müxtəlif obyektlər arasında baş verə biləcək

bütün təhlükəli proseslər izah olunur. İnformasiya axın modeli istifadə olunan hər sistemdə heç bir qanunsuz məlumat axınlarına icazə verilmir.

Əsasən, informasiya bir təhlükəsizlik səviyyəsindən digərinə və ya bir obyektdən o biri obyektə ötürülməsi məhdud əməliyyatlar çərçivəsində reallaşdırılır. Əksər sistemlərdə, məhdudlaşdırılmış bir əməliyyat tətbiq edildikdən sonra sistem bu əməliyyatın konkret mövzuya və ya bu obyektə xüsusi icazə verildiyini görmək üçün giriş nəzarət matrislərinə nəzər salınır.

Clark Wilson modeli kompüter sistemləri üçün tamlıq siyasətinin təhlili və müəyyənləşdirilməsində təməl rolunu oynayır. Model ilkin olaraq informasiya tamlıq anlayışının formalaşdırılmasına şamil olunur. Tamlıq siyasətində sistem verilənlərin vahid şəkildə saxlanmasını təsvir edir və sistemin müxtəlif prinsipləri müəyyənləşdirilir. Model vasitəsilə tətbiq və sertifikatlaşdırma qaydaları təyin edilir.

Model ilk dəfə 1987-ci ildə David D. Clark və David R. Wilson tərəfindən hazırlanmışdı. Kağızda Narıncı kitabda təsvir edilmiş çoxsəviyyəli təhlükəsizlik tələbləri əsasında tamlığın əldə edilməsini müəyyənləşdirir. Clark və Wilsonun fikrincə mövcud Biba modulu informasiya konfidensiallığından daha çox tamlığın təminə yönəlmişdir. Məlum olduğu kimi Biba modeli yüksək təsnifləşdirmə səviyyələrində etibarsız informasiya dəyişikliklərinin qarşısını alır. Clark Wilson modelində əksinə olaraq biznes və sənaye proseslərinin istənilən səviyyələrində ali dərəcəli informasiyanın tamlıq konteksindən istifadə edilir.

Modelin əsas prinsiplərindən biri çoxyönlü yanaşmalardan istifadə edilir. Burada hər bir məlumat elementi müəyyənləşdirilir və dəyişikliklər yalnız kiçik proqramlar vasitəsilə həyata keçirilir. Modeldə üçlü giriş nəzarətindən (subyekt – – obyekt – proqram əlaqəsindən) istifadə olunur. Bu əlaqə çərçivəsində subyektin obyektə birbaşa girişi olmur, ona yalnız proqram vasitəsilə daxil olmaq olar. Modelin əsası tranzaksiya ideyasına əsaslanır:

- Yaxşı formallaşdırılmış tranzaksiya sistemə giriş zamanı bir vəziyyətdən digərinə keçidi reallaşdıran əməliyyatlar ardıcıllığıdır;
- Modeldə tamlıq siyasəti tranzaksiyaların tamlığına ünvanlanır;

- Vəzifələrin bölgüsü prinsipi tranzaksiyaların sertifikatlaşdırılmasını tələb edir.

Model verilənlərin üzərində iş icrası üçün müxtəlif tip məlumatları və prosesləri özündə saxlayan bir sıra əsas layihələrdən ibarətdir. Clark Wilson modelindəki əsas məlumat növü Məhdudlaşdırılmış Məlumat Elementidir (Constrained Data İtem – CDİ). Tamlığın Təsdiqləmə Proseduru (İntegrity Verification Procedure – İVP) sistem cari vəziyyətindəki bütün CDİ-ləri təmin edir.

Clark Wilson modelində tamlığın qorunmasında 3 əsas hədəf vardır:

- İcazəsiz istifadəçilərin dəyişikliklər etməsinin qarşısını alır;
- Səlahiyyətli istifadəçilərin yalnış dəyişiklik etməsinə maneə törədir;
- Daxili və xarici uyğunluğu qoruyur.

Model vasitəsilə yuxarıda qeyd edilən bütün hədəfləri yerinə yetirmək olar. Biba modeli isə yalnız birinci problemin həllinə yönəlmişdir. Clark Wilson modelinin 3 əsas xüsusiyyəti vardır:

- subyektlər obyektlərə yalnız icazəli proqram vasitəsilə daxil ola bilər;
- vəzifə bölgüsü prosesi həyata keçirilir;
- ən əsas tələblərədn biri də auditdir.

1975-ci ildə Michael A. Harrison, Walter L. Ruzzo və Jeffrey D. Ullman tərəfindən yaradılmış HRU təhlükəsizlik modeli ilə kompüter sisteminə giriş hüdudlarının tamlığı qorunur. Model Graham Denming modelinin genişləndirilmiş forması olub, *s* subyektinin *o* obyektinə giriş icazələrini redaktə etmək üçün sonlu çoxluq prosedurlarının ideyasına əsaslanır.

Təqdim edilən HRU modelindən alqoritmlərdən istifadə edərək sistemin təhlükəsizliyini təmin etmək üçün onun imkanları və məhdudiyyətləri müzakirə edilir.

HRU modelində sistemin mühafizəsi ümumi hüquq (R) və əmrlər çoxluğu (C) vasitəsilə təmin edilir. Sistemin konfiqurasiyası (S, O, P) üçlüyü vasitəsilə təmin edilir: S – cari subyekt, O – cari obyekt, P isə giriş matrisidir. Sistemdə sadə sorğular vasitəsilə subyekt və obyektləri silmək və ya əlavə etmək olar, eləcə də mövcud subyekt və obyekt cütlüyünə giriş hüquqlarını müəyyən etmək olar. Subyekt və obyektlərin yaradılması sistemin cari konfiqurasiyasında həmin adda verilənlərin olmaması ilkin tələbdir. Mürəkkəb əmrlərdə əməliyyat sırası bir bütün olaraq reallaşdırılır.

Model vasitəsilə ümumi hallar üçün bütün sistemlərin təhlükəsizliyinin təmin etmək üçün ümumi alqoritm olmadığı sübut olundu. Eyni zamanda problemi həlledici hala gətirilməsi üçün yerinə yetiriləcək əmrlərə məhdudiyyətlərin qoyulması ilə əlaqədar olduğu dəqiqləşdirildi.

Həmçinin Çin divarı modeli kimi də tanınan Brever və Nash modeli istifadəçinin əvvəlki fəaliyyətlərinə görə dinamik şəkildə dəyişə biləcək giriş nəzarətini təmin etmək üçün yaradılmışdır. Modelin əsas məqsədi pis niyyətli şəxslərin gizli məlumatlara çıxışına maneə törətməsindən ibarətdir.

Çoxsəviyyəli təhlükəsizlik xüsusiyyətləri müxtəlif yollara ifadə edilə bilər. Bu konsepsiyaya əsasən yuxarı təhlükəsizlik səviyyələrində baş verən proseslər aşağı səviyyəli proseslərə təsir edir. Bu tip modeldə əsas narahatlıq informasiya axınları ilə deyil, subyektin sistemin vəziyyəti haqqında nə bildiyi ilə əlaqədardır. Bu səbəbdən də yüksək təhlükəsizlik səviyyəsində yerinə yetirilən proseslər aşağı səviyyəli proseslərin vəziyyətini dəyişə bilmir.

Modelin əsas xüsusiyyəti hər hansı səviyyədə müəyyən funksiyaları icra edən istifadəçiyə digər səviyyələrdə baş verən proseslərin təsir etməməsidir.

FƏSİL III. SİSTEMİN ETİBARLILIĞININ ƏSAS ELEMENTLƏRİ

3.1 Etibarlılıq blok diaqramı modelinin ardıcıl sistemlərə tətbiqi

Sistem arzuolunan tapşırıqları yüksək etibarlılıq və səmərə ilə yerinə yetirmək üçün xüsusi şəkildə dizayn edilmiş komponentlərin, alt sistemlərin toplusudur. Komponentlərin növü, kəmiyyəti, keyfiyyəti, onların yerləşməsi sistemin etibarlılığına birbaşa təsir edən amillərdəndir. Komponentlər arasındakı yalnış funksional əlaqə bütöv bir sistemin sıradan çıxmasına səbəb ola bilər.

Sistemin komponentlərinin və avadanlıqlarının sıradan çıxmasının müxtəlif səbəbləri ola bilər. Sistemin mühitindən və mürəkkəbliyindən asılı olaraq bu səbəblərin bəziləri məlum, bəziləri isə naməlum olaraq qalır. Məlum səbəblərin bəziləri aşağıda qeyd olunmuşdur:

- Sistemin və ya komponentlərin zəif qurulması;
- İstehsal texnikasının yalnış üsulu;
- Bilik və bacarıqların tam mütəşəkkil olmaması;
- Avadanlıqların hədsiz dərəcədə mürəkkəbliyi;
- Aşağı xidmət səviyyəsi;
- Təşkilati sərtlik və mürəkkəblik;
- İnsan səhvləri;
- Sıradan çıxma ilə nəticələnən ətraf mühit faktorları, proqram elementləri və insan faktorları.

Etirbarlılıq xüsusi $t = [0, t_M]$ zaman intervalında elementin (sistemin və ya altsistemin komponenti) verilmiş məsələni həll etmə ehtimalı ilə əlaqəlidir. Sistemi təşkil edən elementlər 2 vəziyyətdə ola bilər: element işləyir (1 ilə işarə olunur) və ya element işləmir (0 ilə işarə edilir). Bu bölmə aşağıdakı xarakteristikalara malik olan əlaqəli sistemlər üçün nəzərdə tutulmuşdur[31]:

- Komponentlərin etibarlılığının artırılması sistemə təsir edir;
- Sistemi təşkil edən bütün komponentlər bir-birilə sıx bağlıdır.

Əlaqəli sistemlərdə bir və ya bir qrup komponentlərin işdən imtinası etibarlılığa təsir edir, çünki hər bir komponent bütöv sistemə kiçik də olsa təsir edir [9].

Əgər sistemin *i*-ci elementinin işləmə ehtimalı p_i, imtina etmə ehtimalı isə q_i olarsa, onda

$$p_i = 1 - q_i \qquad (1)$$

$$q_i = 1 - p_i \,. \qquad (2)$$

Həmçinin, komponent həmişə 2 mümkün vəziyyətdə olur:

$$q_i + p_i = 1 \qquad (3)$$

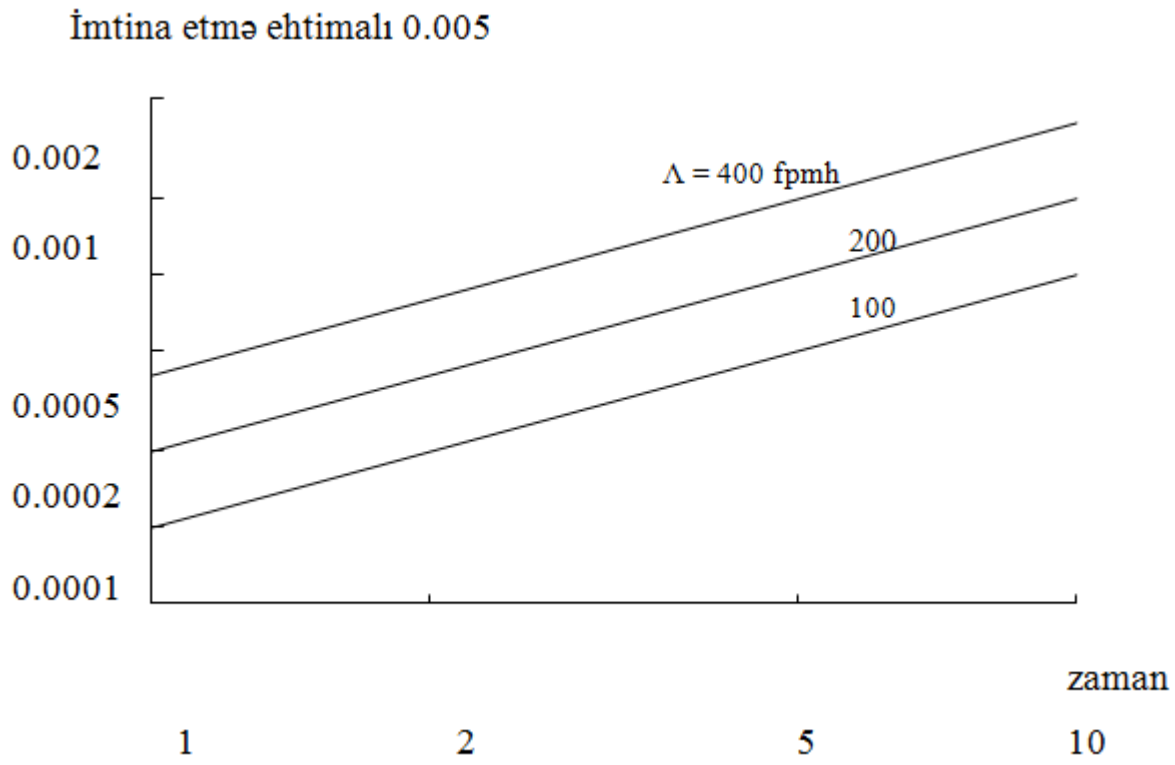
Sistem etibarlılığının kəmiyyət analizi zamanı hər bir individual komponentin vəziyyətini mütləq təsvir etmək lazımdır. Etibarlılıq funksiyası vasitəsi ilə komponentin işi icra etmə ehtimalı hesablanır. Elementin performans periodu dövrü məsafədən, zamandan asılı olur. Etibarlılıq funksiyası da məhz bu 3 parametrdən asılı olur. Ehtimalı xarakterizə etmək məqsədilə bəzi paylanma funksiyalarından istifadə olunur. Daha geniş yayılmış etibarlılıq funksiyalarına eksponensial, normal, Veibull paylanmaları daxil etmək olar.

Bu bölmədə daha çox eksponensial ehtimal paylanmasından istifadə edilmişdir. Bu paylanma vasitəsilə istənilən zaman kəsiyində elementlərin imtina etmə intensivliyini ölçmək olar. Tək komponentli sistemlərdə etibarlılıq funksiyası belə hesablanır:

$$r(\lambda, t) = e^{-\lambda t} \qquad (4)$$

Burada *t* zaman; λ isə imtina etmə intensivliyidir.

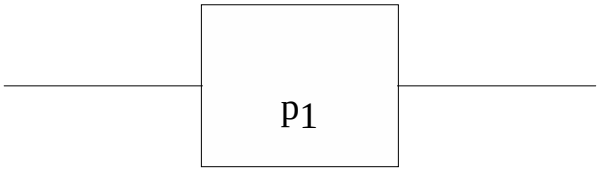
İmtina etmə intensivliyi λ=100,200,400 olan komponentlərin imtina olunma ehtimalı qrafik 1-də göstərilmişdir. Qrafikdə loqarifmik funksiya ikiölçülü müstəvidə düz xətlərlə təsvir olunduğundan qrafikdəki əyriliklər göstərilməmişdir. Göründüyü kimi işləmə ehtimalı zamandan və λ-dan asılı olaraq artır [31].



Qrafik1. Müxtəlif imtina etmə intensivliyi olan komponentlərin ehtimalı.

Sistemin etibarlılığının analizi üçün analitiklər birinci olaraq bütöv sistemi funksional blok diaqramlar vasitəsilə təsir etməlidirlər. Blok diaqramlarının məqsədi vacib altsistemləri və komponentləri saxlamaqla sistemi sadə şəkildə xarakterizə etmək, eləcə də elementlərin sistemə göstərdiyi təsiri təsvir etməkdir. Ümumilikdə, blok diaqramlar vasitəsilə sistem "qara qutuların" toplusu kimi göstərilir. Beləliklə, hər bir blok giriş-çıxışlara malik, bir-birilə qarşılıqlı əlaqədə olan elementdir. Hər bir blok imtina intensivliyi λ_i olan p elementindən ibarətdir.

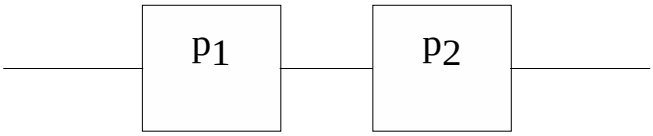
Qrafik 2-də daha böyük bir sistemin tərkib hissəsi ola bilən tək komponentli sistem qeyd olunmuşdur. Bu tək girişi və çıxışı olan blokdur. Qaydaya görə blokun girişi sol tərəfdən və ya yuxarıdan, çıxışı isə sağ tərəfdən və ya blokun aşağısından olur.



Qrafik 2. Tək komponentli blok diaqram

Bütöv bir sistem çoxlu bloklardan ibarət olur. Bu elementlər, elementlər qrupu bir-birinə ya ardıcıl, ya da paralel qoşula bilər.

Ən sadə sistem bir bloku giriş, digər bloku isə çıxış üçün nəzərdə tutulmuş 2 elementdən ibarət olan sistemdir. Nəticədə, sistem hər 2 blokun işlək vəziyyətdə olmasını tələb edir. Belə təsnifat ardıcıl birləşdirilmiş elementlər adlanır.



Qrafik 3. Ardıcıl birləşdirilmiş elementlərin blok diaqramı

Qrafik 3-də təsvir edilmiş p_1 və p_2 elementlərinin etibarlılığını müvafiq olaraq p_1 və p_2 ilə, sistemin ümumi etibarlılığını isə R_S ilə işarələsək, o zaman

$$R_S = p_1 p_2$$

olar. Düsturu ardıcıl birləşdirilmiş n sayda elementlər üçün ümumiləşdirsək, bu zaman aşağıdakı bərabərliyi almaq olar:

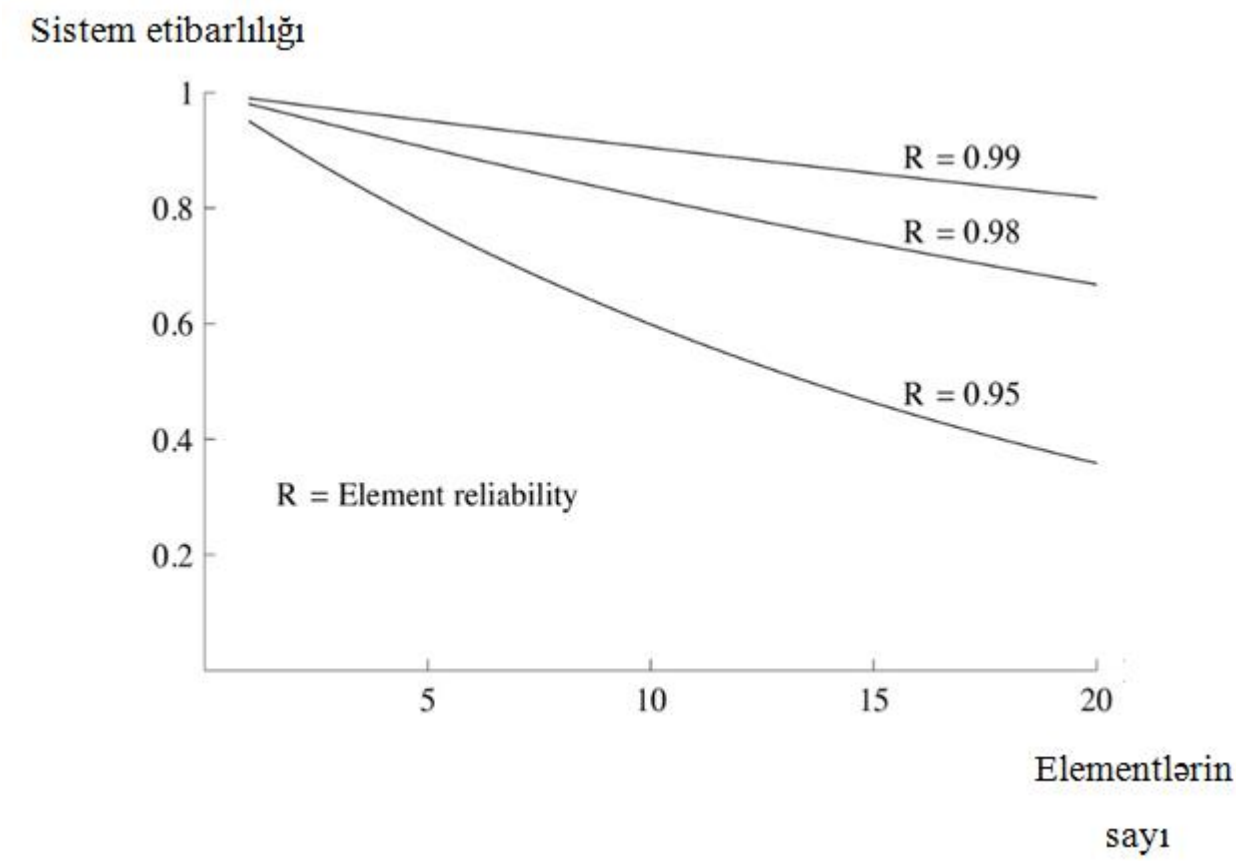
$$R_S = \prod_{i=1}^{n} p_i \qquad (5)$$

Belə sistemlərdə imtina etmə intensivliyini hesablama düsturu belədir:

$$\lambda = \sum_{i=1}^{n} \lambda \qquad (6)$$

Ardıcıl sistemlərin etibarlılığı individual element etibarlılığı funksiyasından, ardıcıl birləşdirilmiş elementlərin sayından asılıdır. Qrafik 4-də hər birinin etibarlılığı

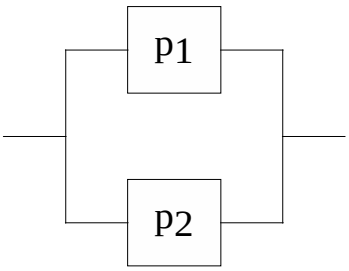
0,99; 0,98; 0,95 olan 20-ə yaxın elementli sistem təsvir edilmişdir. Aydındır ki, elementlərin sayının artması sistem etibarlılığının azalmasına səbəb olur [15].



Qrafik 4. Ardıcıl birləşdirilmiş sistemin etibarlılığı

3.2 Paralel birləşdirilmiş sistemlərin etibarlılığının müəyyən edilməsi

İkinci təməl sistem komponentlərinin quruluşu qrafik 5-də göstərilmişdir. Sistemi təşkil edən p_1 və p_2 elementlərinin biri və ya hər ikisi işlək vəziyyətdədir.



Qrafik 5. Paralel birləşdirilmiş elementlərin blok diaqramı.

p_1 və p_2 elementlərinin etibarlılığı uyğun olaraq p_1 və p_2, 2 elementdən ibarət olan sistemin etibarlılığını isə R_P ilə işarə etsək, onda

$$R_P = 1 - (1 - p_1)(1 - p_2)$$

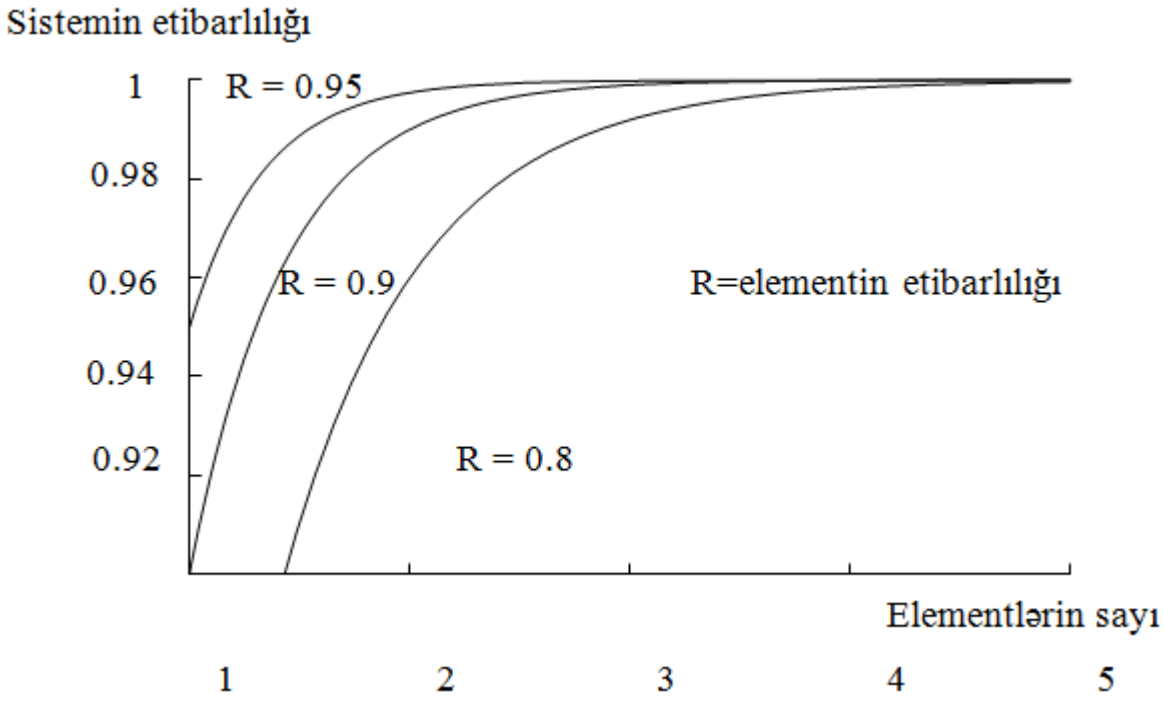
n komponentli sistemlər üçün bu formulu ümumiləşdirsək, aşağıdakı düstur alınar:

$$R_P = 1 - \prod_{i=1}^{n}(1 - p_i) \qquad (7)$$

Bərabərliyini dizyunksiya əməli ilə aşağıdakı kimi yazmaq olar:

- - rOR[p1, p2]:=1 − (1 − p1)(1 − p2)

Qrafik 6-da paralel elementlərin sayının artması sistem etibarlılığına təsiri əks olunmuşdur. Elementlər 0,95; 0,9; 0,8 etibarlılığa malikdirlər.



Qrafik 6. Paralel sistemlərin etibarlılığı

Qarışıq şəkildə birləşdirilmiş elementlər

Qrafik 7-də həm ardıcıl, həm də paralel şəkildə birləşdirilmiş yeddi elementdən ibarət sistem təsvir olunmuşdur. Hər bir elementin etibarlılığı p_i, bütöv sisteminki isə R_{sis} ilə işarə edilərsə, o zaman məntiqi əməllərin köməyi ilə R_{sis} aşağıdakı kimi müəyyən edilə bilər:

p12 = rAND[p1, p2]

$p1p2$

p345 = rOR[p3, rOR[p4, p5]]

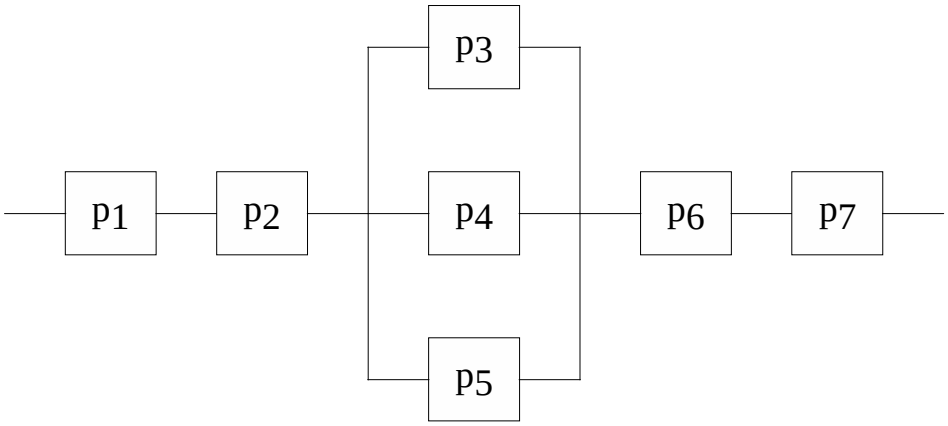
$1 - (1 - p3)(1 - p4)(1 - p5)$

p67 = rAND[p6, p7]

$p6p7$

Rsis = rAND[p12, rAND[p345, p67]]

$$p1p2(1 - (1 - p3)(1 - p4)(1 - p5))p6p7$$



Qrafik 7. Ardıcıl və paralel birləşdirilmiş sistem.

Belə sadələşdirmə texnikası ardıcıl, paralel birləşdirilmiş elementlər sistemini bütün elementləri sadə qarşılıqlı əlaqədə olan tək blok sistemlə ekvivalentləşdirir [15].

Hesab edək ki, qrafik 8-də təsvir olunduğu kimi 2 alternativ paralel birləşdirilmiş sistem mövcuddur. Hər iki sistem eyni komponentlərdən təşkil olunsa da, onların etibarlılığı eyni deyildir. A sistemində p1;p2 və p3 p4 elementlərinin hər ikisi işlək vəziyyətdə olmalıdır. B sistemində isə $p1$ və $p2$, $p1$ və $p4$, $p3$ və $p2$, və ya $p3$ və $p4$ element cütlərindən hər hansı birinin işlək vəziyyətdə olması kifayətdir. A sistemi yüksək səviyyəli, B sistemi isə aşağı səviyyəli səmərəlilik göstərir. Hər iki sistemin etibarlıllığı aşağıda göstərilən qayda ilə hesablanmışdır:

$$rSysA = rOR[rAND[p1, p2], rAND[p3, p4]]$$

$$p1p2 + p3p4 - p1p2p3p4$$

$$rSysB = rAND[rOR[p1, p3], rOR[p2, p4]$$

$$p1p2p3 + p1p4\ p1p2p4 + p3p4\ p1p3p4\ p2p3p4 + p1p2p3p4$$

Aydındır ki, iki sistem ekvivalent etibarlılığa malik deyil. Mövcüd 4 elementə qiymətlər versək, o zaman sistemlərin etibarlılığı aşağıdakı kimi olar:

$$p1 = 0.95;\quad p2 = 0.95;\quad p3 = 0.9;\quad p4 = 0.9;$$

$$rSysA = 0.981475$$

rSysB=0.990025

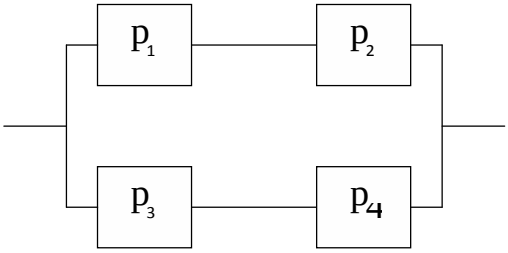
A və B sistemlərinin etibarsızlığı isə

qSysA = 1 – rSysA= 0.018525

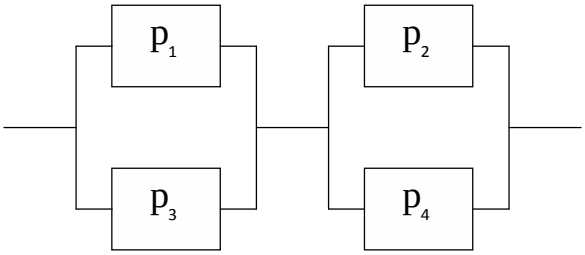
qSysB = 1 – rSysB=0.009975

qSysA/qSysB=1.85714

bərabərliklərdir. Hesablamalar nəticəsində aydın oldu ki, A sistemi B sistemindən 1,86 dəfə çox imtina etməyə meyillidir.



A sistemi

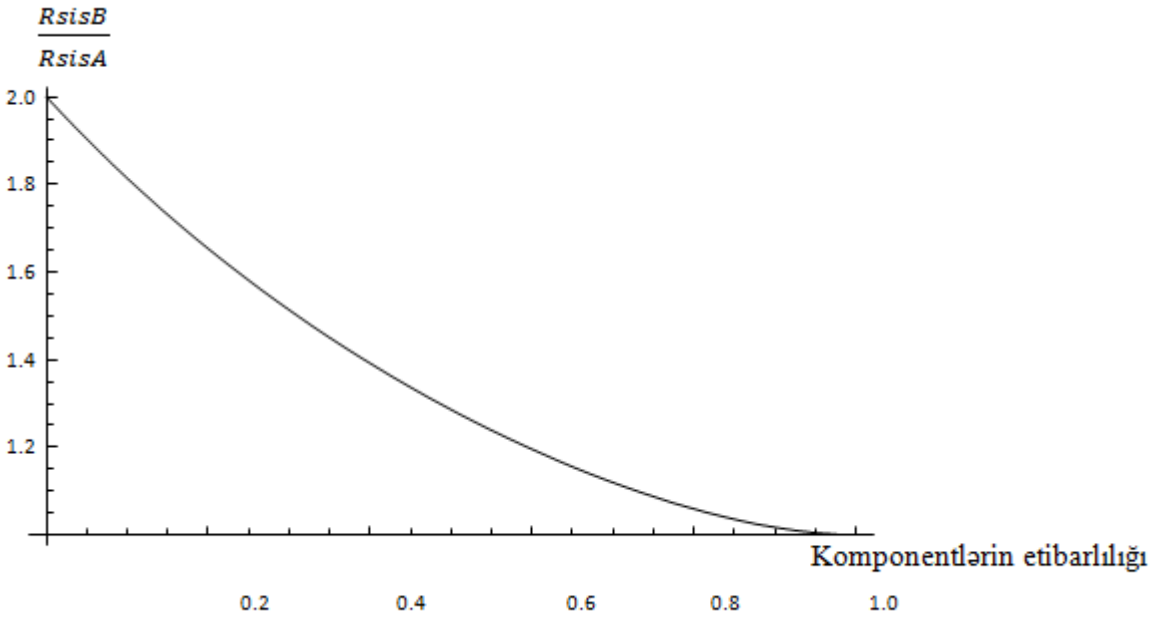


B sistemi

Qrafik 8. A və B sistemləri

3.3 Blok diaqram modeli vasitəsilə ehtiyyat sistemlərinin etibarlılığının əldə edilməsi

Hesab edək ki, A və B sistemlərinin komponentləri eynidir və nəticədə onların etibarlılığı da bərabərdir. Qrafik 9-da elementlərinin etibarlılığı [0 + z, 1] intervalında dəyişən B sisteminin A sisteminə olan nisbəti göstərilmişdir. Aşağı səviyyəli komponent etibarlılığına malik sistemlər üçün aşağı səviyyəli ehtiyyat sistemləri xarakterikdir. A və B sistemlərinin komponentlərinin eyni olmasına baxmayaraq, B sisteminin daha mürəkkəb quruluşa malik olduğundan bu nəticəni əldə etmək olar.



Qrafik 9. B sisteminin A sisteminə olan nisbətinin etibarlılıqdan asılılığı

Məlum olduğu kimi ehtiyyat nüsxələrə malik sistemlər tək, ardıcıl, birləşdirilmiş sistemlərdən daha etibarlıdır. Hər bir əlavə ehtiyyat sistemi sistemin sıradan çıxma riskini azaldır. Bir, iki, üç, dörd ehtiyyat sisteminə malik sistemlərin ümumi etibarlılığı aşağıdakı kimi hesablanılır:

$$rSis1 = p1$$

$$p1$$

rSis2 = r0R [p1,p2]

$1 - (1 - p1)(1 - p2)$

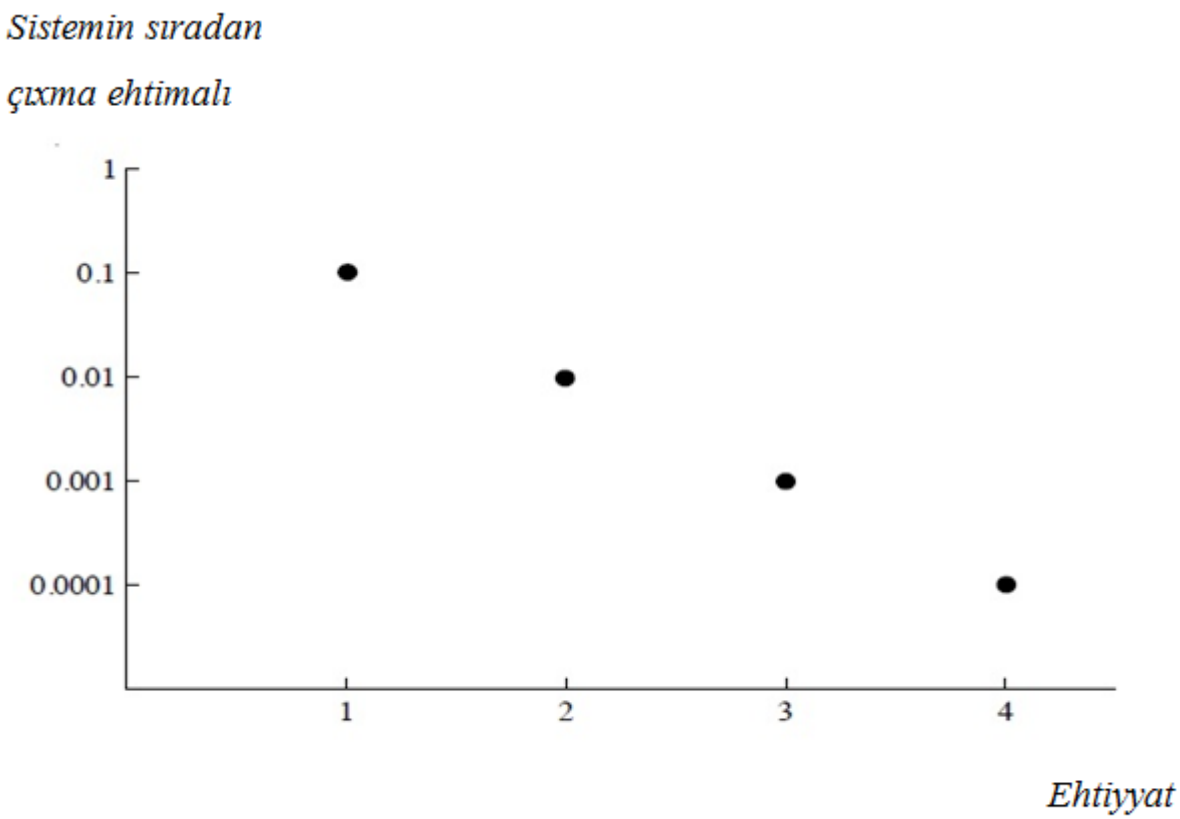
rSis3 = r0R [p1, r0R[p2, p3]]

$1 - (1 - p1)(1 - p2)(1 - p3)$

rSis4 = r0R [p1, r0R[p2, r0R[p3, p4]]]

$1 - (1 - p1)(1 - p2)(1 - p3)(1 - p4)$

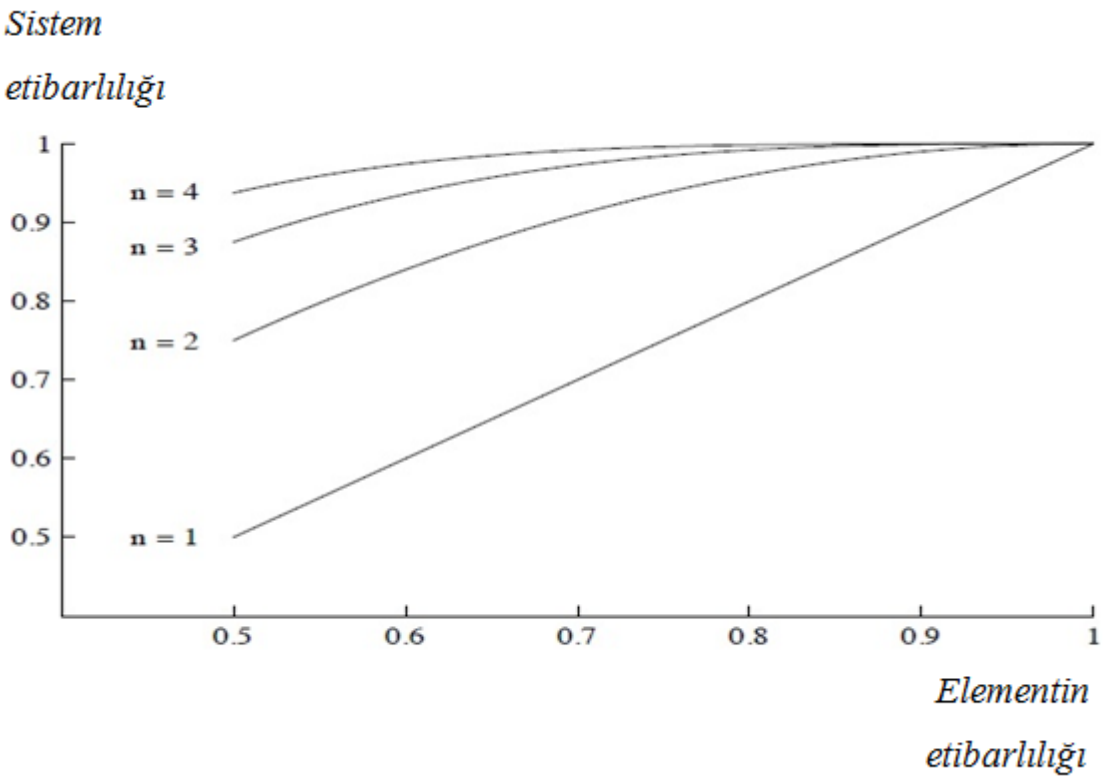
Qrafik 10-da elementlərinin etibarlılığı 0.9 olan ($p1 = p2 = p3 = p4 = 0.9$) sistemlərin sıradan çıxma ehtimalı qeyd olunmuşdur. Nümunədən göründüyü kimi sadə sistemlər dörd qat sistemə nəzərən 1000 dəfə çox sıradan çıxmaya meyillidir.



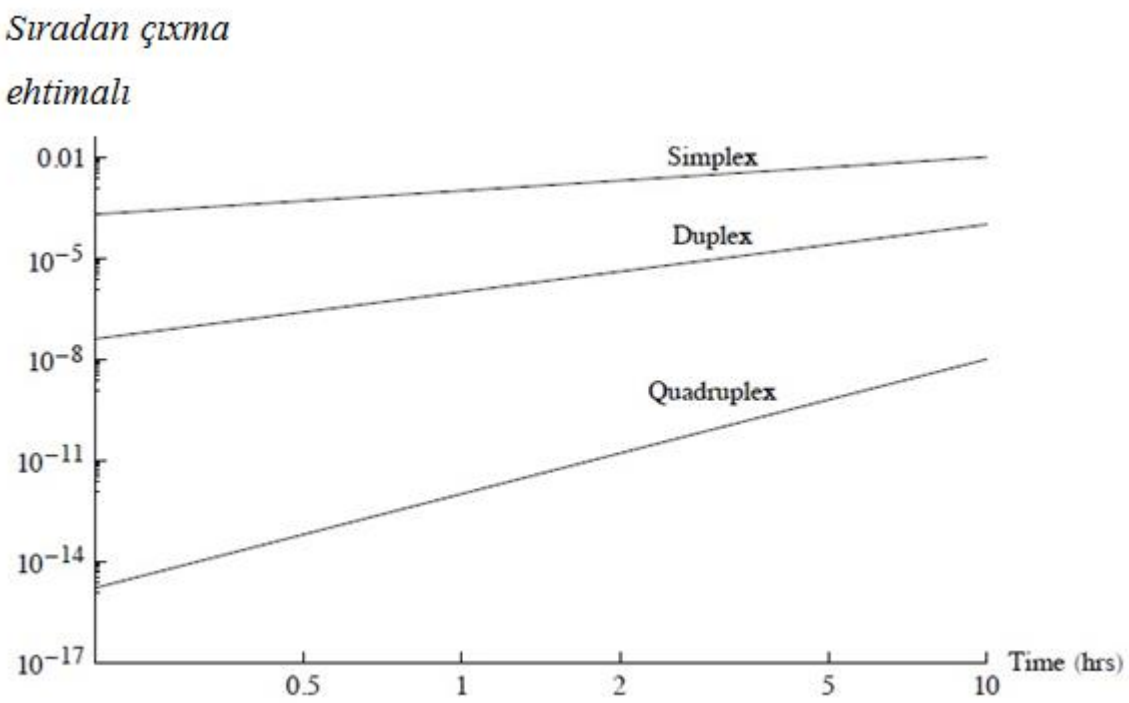
Qrafik 10. Ehtiyyat sistemlərinin sayından asılı olaraq sıradan çıxma.

Qrafik 11-də element etibarlılığı ilə ehtiyyat nüsxələri arasındakı əlaqə əks olunmuşdur. p=0.5 olan elementli sistemdə paralel birləşdirmə vasitəsilə yüksək

səviyyəli etibarlılıq (təxminən 0.94) əldə etmək olar. Həmçinin onu da qeyd etmək lazımdır ki, paralel birləşdirilmiş elementlərin sayının artması etibarlılılğın da artmasına səbəb olar.



Qrafik 11. Ehtiyyat sistemlərin elementlərdən asılılığı



Qrafik 12. λ=1000 olan sistemlərin sıradan çıxmasının zamandan asılılığı.

K-n sistemlərinin etibarlılığı

Yuxarıda qeyd edilən sistemlərlə yanaşı k-n (n sayda komponenti olan sistemin k sayda elementi işlək vəziyyətdədir) sistemlər mövcuddur. Ardıcıl sistemlər n sayda elementin hamısı, qarışıq sistemlər isə ən az k sayda işlək komponentə malikdirlər. k-n eyni komponentli sistemlərinin etibarlılığı aşağıda qeyd edilən bərabərlilik vasitəsilə hesablanır:

$$R(k,n) = \sum_{i=k}^{n} \binom{n}{i} p^i (1-p)^{n-i} \qquad 8)$$

$$= \sum_{i=k}^{n} \binom{n}{i} p^i q^{n-i}$$

(8) bərabərliyində $q=1-p$ düsturundan istifadə olunmuşdur. Ümumi halda, müxtəlif komponentli sistemlərin etibarlılığını hesablamaq isə bir qədər mürəkkəbdir. Tutaq ki, $p=\{p_1,....,p_n\}$ komponentin etibarlılıq vektoru, $q=\{1-p_1,....,1-p_n\}$ isə komponentlərin etibarsızlığı vektorudur. İndi isə aşağıdakı funksiyaları müəyyənləşdirək:

pT(i,p) – i sayda elementi olan p etibarlılıq çoxluğunun k alt çoxluğudur;

qT(i,q) – (n – i) sayda elementi olan q çoxluğunun k alt çoxluğudur.

K alt çoxluğu işlək elementlər çoxluğudur. K-n sisteminin etibarlılığı

$$R(k,n,\mathbf{p}) = \sum_{i=k}^{n} \sum_{j=1}^{\binom{n}{i}} \mathbf{qT}(i,\mathbf{p})_j \mathbf{pT}(i,\mathbf{p})_{\binom{n}{i}-j+1} . \qquad 9)$$

düsturu vasitəsilə hesablanır.

Məsələn: p={p_1, p_2, p_3} verilmişdir. Belə ki, n = |p|=3 olduqda

$$pT(1, p) = \{p_1, p_2, p_3\}$$

$$pT(2, p) = \{p_1 p_2, p_1 p_3, p_2 p_3\}$$

$$pT(3, p) = \{p_1 p_2 p_3\}$$

$$qT(1, q) = \{(1 - p_1)(1 - p_2), (1 - p_1)(1 - p_3), (1 - p_2)(1 - p_3)\}$$

$$qT(2, q) = \{(1 - p_1), (1 - p_2), (1 - p_3)\}$$

$$qT(3, q) = 1.$$

bərabərliklərinə nəzərə alaraq,

$$\begin{aligned} R(1,3,p) = {} & p_1(1 - p_1)(1 - p_2) + (1 - p_1)p_2(1 - p_3) + \\ & + p_1 p_2(1 - p_3) + (1 - p_1)(1 - p_2)p_3 + \\ & + p_1(1 - p_2)p_3 + (1 - p_1)p_2 p_3 + p_1 p_2 p_3 = \\ & = p_1 + p_2 - p_1 p_2 + p_3 - p_1 p_3 - p_2 p_3 + p_1 p_2 p_3 \end{aligned} \qquad (10)$$

Ümumi n sayda komponentdən dəqiq k sayda elementin işlək vəziyyətdə olarsa, etibarlılıq aşağıdakı düstur vasitəsilə hesablanılır:

$$R_e(k,n,\mathbf{p}) = \sum_{j=1}^{\binom{n}{k}} \mathbf{qT}(k,\mathbf{p})_j \mathbf{pT}(k,\mathbf{p})_{\binom{n}{k}-j+1} . \qquad 11)$$

Alınmış ifadəni sadələşdirək:

$$\begin{aligned} R_e(k,n) &= \binom{n}{k} p^k (1-p)^{n-k} \qquad 12) \\ &= \binom{n}{k} p^k q^{n-k} . \end{aligned}$$

3.4 Etibarlılığın təmin edilməsində Markov prosesinin rolu və əhəmiyyəti

Əvvəlki bölmələrdə sistem komponentlərinin yalnız 2 vəziyyətdə ola biləcəyi fərziyyəsindən danışılır: işlək və ya sıradan çıxmış vəziyyətdə. İndi isə statik və bərpa olunan sistemlərin analizi üçün uyğun olan modellərə baxaq.

Stoxastik proseslərin xüsusi növü olan Markov zənciri modelində sistem komponentləri bir neçə vəziyyətdə, eləcə də vəziyyətlər arasında keçid formasında ola bilər. Prosesin t zamanında vəziyyəti ixtiyari X(t) dəyişəni ilə işarə edilir. Bütün mümkün vəziyyətlər vəziyyət toplusu adlandırılır və X ilə işarə olunur. X{0,1,2,...,*r*} vəziyyətlər toplusu *r*+1 sayda müxtəlif vəziyyətdən ibarətdir. Zaman {0,1,2,..} qiymətlərini alaraq diskret və ya sonsuz ola bilər. Zaman diskret olarsa, zəncir diskret zamanlı Markov zənciri, sonsuz olarsa, fasiləsiz Markov zənciri və ya Markov prosesi adlanır. Diskret zamanlı olarsa, zaman n, Markov zənciri isə $\{X_n, n=0,1,2,..\}$ kimi işarə edilir.

Birinci dərəcəli diferensial Kolmoqorov tənliklərindən t zamanında Markov proseslərinin paylanma ehtimalını müəyyən etmək üçün istifadə edilir:

$$P(t)=[P_0(t), P_1(t),...,P_r(t)]$$

Burada P_i (t) t zamanında *i* vəziyyətinin ehtimalıdır. $t\to\infty$ olduqda müəyyən şərtlər altında P(t)-nin limiti P-ə yaxınlaşır. Limit prosesin sabit vəziyyətli paylanması adlanır. Sabit vəziyyətli paylanma və sistemin iş qabiliyyəti vasitəsilə ardıcıl və paralel birləşdirilmiş sistem, asılı komponentli sistemlər, müxtəlif tip dəstək sistemləri müəyyənləşdirilir. Sistemin iş qabiliyyəti dedikdə vəziyyət tezliyi, sistem əlyetənliyi, sistemin sıradan çıxma tezliyi başa düşülür [31].

Hesab edək ki, vəziyyət toplusu X={0,1,2,...,r} olan və stasionar keçid ehtimalı olan Markov prosesi {X(t), $t \geq 0$} kimi işarə edilib. Markov prosesinin keçid ehtimalının

$$P_{ij}(t)=P_r(X(t) = j \mid X(0)=i) \quad (i,j \in X)$$

matrisi şəklində göstərilib:

$$\mathbb{P}(t) = \begin{pmatrix} P_{00}(t) & P_{01}(t) & \cdots & P_{0r}(t) \\ P_{10}(t) & P_{11}(t) & \cdots & P_{1r}(t) \\ \vdots & \vdots & \ddots & \vdots \\ P_{r0}(t) & P_{r1}(t) & \cdots & P_{rr}(t) \end{pmatrix} \quad (1)$$

Girişlərin ehtimalı aşağıdakı bərabərsizliyi ödəyir:

$$0 \leq P_{ij} \leq 1 \quad (t \geq 0 \text{ olduqda bütün } i, j \in X)$$

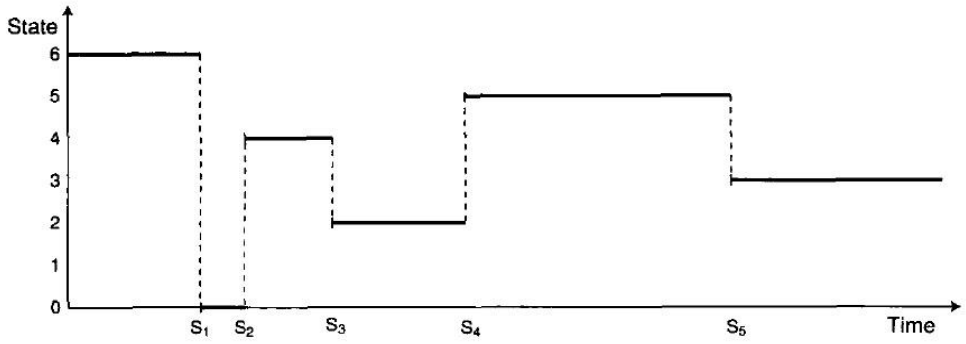
Əgər *a* prosesi 0 anında *i* vəziyyətindədirsə, onda *t* zamanında *i* vəziyyətində olmalı, ya da müxtəlif vəziyyətə keçid etməlidir. Bu zaman aşağıdakı bərabərlik alınır:

$$\sum_{j=0}^{r} P_{ij}(t) = 1 \quad (2)$$

Matrisin hər bir sırasında P ehtimallarının cəmi 1-ə bərabər olmalıdır [9].

Qeyd: Matrisin *i* sırası *i* vəziyyətlərindəki keçidləri ($j \neq i$), j sütunu isə vəziyyətlərin keçidlərini ($i \neq j$) göstərir.

Tutaq ki, $0 = S_0 \leq S_1 \leq S_2 \leq \ldots$ keçidlərin baş vermə anıdır. $T_i = S_{i+1} - S_i$ isə (i=1,2...) *i*-ci keçidin baş vermə müddətidir. Markov prosesinin "yolu" (trayektoriyası) qrafik 1-də göstərilmişdir. Markov prosesi t=0 anında 6-cı vəziyyətdə başlayır və sağa doğru hərəkət edir [16].



Qrafik 1. Markov prosesinin trayektoriyası

Hesab edək ki, Markov prosesinə giriş 0 anında *i* vəziyyətindədir ($X(0)=i$). $\dot{T}_i$ isə *i* vəziyyətinin baş vermə müddətidir (Qeyd: T_i keçidin baş vermə anı, $\dot{T}_i$ isə keçidə sərf olunan zamanı göstərir). İndi isə *s* zamanında *i* vəziyyətində olan ($\dot{T}_i > s$)

prosesin ehtimalını tapaq. Bunun üçün ilk öncə $\Pr(\dot{T}_i > t+s \mid \dot{T}_i > s)$ ehtimalını tapmaq lazımdır. Məlumdur ki, s zamanında sistemin hissələri bir-birilə əlaqəli deyil. Bu səbəbdən

$$\Pr(\dot{T}_i > t+s \mid \dot{T}_i > s) = \Pr(\dot{T}_i > t) \qquad s, t \geq 0$$

$\dot{T}_i$ ixtiyari dəyişəni mütləq ekponensial şəkildə paylanmalıdır.

İndi isə müxtəlif vəziyyətlərə sərf olunan zamanı nəzərə almadan $S_1, S_2, \ldots$ anında baş vermiş keçidlərə diqqət yetirək. $X_n = X(S_n)$ ilə n keçidindən dərhal sonrakı vəziyyət göstərilir. $\{X_n, n=1,2,..\}$ Markov prosesinin gedişatını əks etdirir. Keçidlər $n=1,2,...$ diskret zamanında baş verir və onların baş vermə müddəti deterministikdir və bərabər uzunluqdadır.

Stoxastik proses kimi Markov prosesi hər zaman anında i vəziyyətindəki girişi a-dır:

1. Müxtəlif vəziyyətlərə keçid üçün i vəziyyətinə sərf olunan $\dot{T}_i$ zamanlarını intensivliyi α_i –dir.
2. Proses i vəziyyətini tərk edən zaman, j vəziyyətinə daxil olanda ehtimalı belə hesablanılır:

$$\sum_{\substack{j=0 \\ j \neq i}}^{r} P_{ij} = 1.$$

Bu səbəbdən i vəziyyətində keçidin baş vermə müddəti

$$E(\tilde{T}_i) = \frac{1}{\alpha_i}$$

kimi hesablanılır. Əgər $\alpha_i = \infty$ olarsa, i vəziyyəti ani vəziyyət adlanır və a vəziyyətindən keçid müddəti 0-a bərabərdir. Markov prosesi a vəziyyətinə daxil olduqda ani vəziyyətdən çıxır. İndi isə fərz edək ki, bu prosesdə ani vəziyyət yoxdur və bütün i vəziyyəti üçün $0 \leq \alpha_i < \infty$ bərabərsizliyi ödənilir. $\alpha_i = 0$ olarsa, udma vəziyyəti baş verir (bir vəziyyətə girərkən digərindən çıxılır) [31].

Stoxastik Markov prosesi vəziyyətdən vəziyyətə dəyişən diskret zamanlı Markov zənciridir. a_{ij} aşağıda qeyd olunmuş şəkildə müəyyən edilir:

$$a_{ij} = \alpha_{ij} \cdot P_{ij} \quad (i \neq j) \qquad (3)$$

Burada α_i prosesin i vəziyyətini tərk etmə intensivliyi, P_{ij} vəziyyətinə keçmə ehtimalı a_{ij} isə i vəziyyətindən j vəziyyətinə a keçidinin intensivliyidir. a_{ij} başqa cür keçid intensivliyi kimi adlandırmaq olar.

$\sum_{j \neq i} P_{ij} = 1$ olarsa,

$$\alpha_i = \sum_{\substack{j=0 \\ j \neq i}}^{r} a_{ij} \qquad (4)$$

olar. T_{ij} i vəziyyətindən j vəziyyətinə keçmə müddətidir.

Tutaq ki, Δt qısa zaman intervalıdır.

$$\begin{aligned} P_{ii}(\Delta t) &= \Pr(\tilde{T}_i > \Delta t) = e^{-\alpha_i \Delta t} \approx 1 - \alpha_i \Delta t \\ P_{ij}(\Delta t) &= \Pr(T_{ij} \leq \Delta t) = 1 - e^{-a_{ij} \Delta t} \approx a_{ij} \Delta t \end{aligned}$$

Delta t zaman intervalı çox kiçik olduqda aşağıdakı bərabərliklər alınır:

$$\begin{aligned} \lim_{\Delta t \to 0} \frac{1 - P_{ii}(\Delta t)}{\Delta t} = \lim_{\Delta t \to 0} \frac{\Pr(\tilde{T}_i < \Delta t)}{\Delta t} &= \alpha_i \\ \lim_{\Delta t \to 0} \frac{P_{ij}(\Delta t)}{\Delta t} = \lim_{\Delta t \to 0} \frac{\Pr(T_{ij} < \Delta t)}{\Delta t} &= a_{ij} \end{aligned} \qquad (6)$$

X-ə daxil olan bütün i, j üçün a_{ij} taparaq (1) xüsusi vəziyyətində və (2) bütün $i \neq j$ özünü doğruldan keçid intensivliyi ilə Markov prosesini müəyyən etmək olar. İkinci daha məqsədəuyğun yanaşmadır. a_{ij} keçid intensivliyini matris şəklində də göstərmək olar:

$$\mathbb{A} = \begin{pmatrix} a_{00} & a_{01} & \cdots & a_{0r} \\ a_{10} & a_{11} & \cdots & a_{1r} \\ \vdots & \vdots & \ddots & \vdots \\ a_{r0} & a_{r1} & \cdots & a_{rr} \end{pmatrix} \qquad (7)$$

Burada bütün dioqnal elementlər üçün aşağıdakı bərabərlik doğrudur:

$$a_{ii} = -\alpha_i = -\sum_{\substack{j=0 \\ j \neq i}}^{r} a_{ij} \qquad (8)$$

A matrisi Markov prosesinin keçid intensivliyi matrisi adlanır. Bəzi müəlliflər onu prosesin sonsuz kiçik matrisi kimi qələmə alırlar.

Müşahidələrə görə *i* sətrindəki girişlər *i* vəziyyətindən keçmə intensivliyidir ($j \neq i$ üçün). Bunu bəzən *i* vəziyyətindən gediş intensivliyi də adlandırırlar. *i* sütünlarındakı girişlər *i* vəziyyətinə keçid intensivliyidir. *i* sətirlərində girişlərin cəmi 0-a bərabərdir[31].

Sistemin keçid intensivliyi matrisini yaratmaq üçün aşağıdakı qaydalara əməl etmək lazımdır:

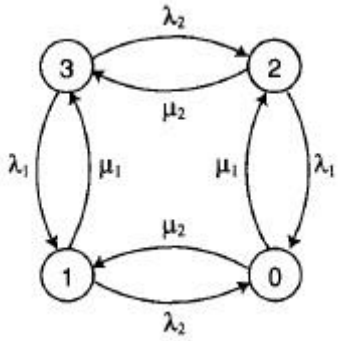
1. Bütün əlaqəli sistem vəziyyətləri təsvir edilməlidir. Qeyri-münasib vəziyyətlər silinməli və eyni, oxşar vəziyyətlər birləşdirilməlidir. Mövcud vəziyyətlərin hər biri unikal olmalıdır. Matrisdə 0-dan *r*-ə qədər bütün tam ədədlərdən istifadə olunur. *r* ilə sistemin ən yaxşı, 0 ilə isə ən pis vəziyyəti işarələnir. Sistemin vəziyyət toplusu X=[0,1,...,*r*] – dir.
2. Bütün $i \neq j$, $i, j \in X$ üçün a_{ij} keçid intensivliyi müəyyənləşdirilir. Keçid intensivliyi ilə sıradan çıxma intensivliyi və bərpa intensivliyi müəyyən edilir.
3. (7) matrisinə uyğun a_{ij} keçid matrisi tərtib edilir.
4. Bütün a_{ii} dioqnal elementləri 0 ilə və ya (8) düsturu vasitəsilə doldurulur.

Markov prosesi mümkün a_{ij} keçidləri vasitəsilə keçid vəziyyətlərin diaqramını qrafik şəkildə göstərmək olar. Keçid vəziyyət diaqramı həmçinin, Markov diaqramı da adlandırılır. Diaqramdakı çevrələrlə vəziyyəti, istiqamətlənmiş qövslər vasitəsilə vəziyyətlər arasındakı keçidlər təsvir edilir [14].

Hesab edək ki, 2 komponentli paralel sistem təsvir edilmişdir. Sistem üçün aşağıdakı xüsusi idarəetmə stategiyası qəbul edilmişdir. Komponent sıradan çıxan zaman bərpaetmə funksiyasının köməyi ilə komponent ilkin funksional vəziyyətinə

qaytarılır. Bərpa prosesi bitdikdən sonra komponent əvvəlki vəziyyətinə qayıdır. Hər bir komponentin özünəməxsus bərpa xüsusiyyəti vardır.

Hesab edək ki, komponentlərin sıradan çıxma intensivliyi λ_i bərpaetmə intensivliyi isə μ_i -dir (i =1,2). Dörd sistem vəziyyəti arasındakı keçidlər (1) sxemində əks olunmuşdur.



Sxem 1. Paralel strukturlu sistemin keçid vəziyyət diaqramı.

Sistem 0 anında 3 vəziyyətindədir. İlk keçid prosesi isə vəziyyət 2 və ya 1-də baş verir. 2 vəziyyətinin keçid intensivliyi $a_{32} = \lambda_2$, 1 vəziyyətinin isə $a_{31} = \lambda_1$ -dir. Keçidin baş vermə müddəti vəziyyət 3-də $\dot{T}_3 = \min[T_{31}, T_{32}]$ ilə hesablanılır. $\dot{T}_3$ üçün $a_{32} + a_{31} = \lambda_1 + \lambda_2$ bərabərliyi doğrudur və keçidin baş vermə müddəti isə $1/(\lambda_1 + \lambda_2)$ düsturu vasitəsilə tapılır [31].

Sistem vəziyyət 2-də növbəti keçid 3 ($a_{32} = \mu_2$) və ya 0 ($a_{20} = \lambda_1$) vəziyyətinə ola bilər. 3 vəziyyətinə keçmə ehtimalı $\mu_2 / (\mu_2 + \lambda_1)$, 0 vəziyyətinə keçmə ehtimalı isə $\lambda_1 / (\mu_2 + \lambda_1)$ düsturu vasitəsilə hesablanılır. Sistemin keçid intensivliyi matrisi aşağıdakı şəkildədir:

$$\mathbb{A} = \begin{pmatrix} -(\mu_1+\mu_2) & \mu_2 & \mu_1 & 0 \\ \lambda_2 & -(\lambda_2+\mu_1) & 0 & \mu_1 \\ \lambda_1 & 0 & -(\lambda_1+\mu_2) & \mu_2 \\ 0 & \lambda_1 & \lambda_2 & -(\lambda_1+\lambda_2) \end{pmatrix}$$

NƏTİCƏ VƏ TƏKLİFLƏR

Sadədən ən mürəkkəb sistemə qədər etibarlılıq modelini qurmaq və istifadə etmək müəssisə daxilindəki hər kəsin daha yaxşı qərarlar qəbul etməsinə imkan verir. Sistemin etibarlılığını anlamaq və izləmək üçün aşağıda qeyd olunanlardan hər ikisini də bilmək vacibdir:

- Sistem daxilindəki elementlərin etibarlılığını;
- Elementlərin bir-birilə qarşılıqlı əlaqəsi.

Etibarlılıq modellərindən istifadə zəif nöqtənin müəyyənləşdirilməsinə, resursların səmərəli istifadəsinə kömək edir. Təşkilatların hədəfini nəzərə alaraq, şirkətin ehtiyyaclarını yaxşı qarşılamaq üçün doğru modeli qurmaq ən vacib məsələlərdən biridir.

Etibarlı blok diaqram modellər sistemin daxilindəki elementlərin etibarlılığını və onların əlaqəsini nəzərə almaqla sistemin etibarlılığının qrafik və riyazi modelini təmin edir. Diaqram komponentlər və ya alt sistemlər arasında etibarlılıq əlaqələrinə diqqət yetirdiyindən sistemin funksional diaqramını özündə əks etdirmir. Məsələn, ardıcıl birləşdirilmiş sistemlərdə hər hansı blokun sıradan çıxması sistemin işinin dayandırılmasına səbəb olur. Digər nümunə kimi iki elementli paralel sistemə baxmaq olar. Belə birləşdirilmiş sistemdə bir komponentin işlək vəziyyətdə olmaması sistemin işinin dayandırılması ilə nəticələnmir. Paralel struktura ikidən daha artıq element daxil ola bilər. Belə olan halda sistem k-n sistemi (n sayda paralel birləşdirilmiş elementdən ibarət sistemin k sayda işlək elementinin olması) adlanır.

Problem ağacı sistemin istənməyən, arzuolunmaz və ya anormal vəziyyətlə qarşılaşdığında istifadə edilən məntiqi, qrafiki diaqramdır. Diaqram vasitəsilə sistemin tərkib hissələrinin, komponentlərinin, proqram təminatının və ya alt sistemlərində arzuolunmaz vəziyyətə gətirib çıxaran çoxsaylı problemlərin təsviri üçün istifadə edilir. Modelin ən üstün cəhətlərindən biri ən mühüm səhvləri, sıradan çıxma səbəblərini asanlıqla müəyyən etməkdir. Modelin qurulması çox çətin proses

deyildir, bunun üçün yalnız sıradan çıxmağa səbəb ola biləcək bütün yollar aydınlaşdırılmalıdır.

İnformasiya sistemlərinin strukturu blok diaqramlar vasitəsilə təsvir edilir. Etibarlı blok diaqram sistemin funksiyalarını təsvir edən uğurlu şəbəkədir. Onlar vasitəsilə müəyyən bir funksiyanı yerinə yetirən sistemin lazımı komponentləri arasındakı əlaqələr göstərilir. Əgər sistem birdən çox funksiyanı yerinə yetirirsə, hər bir funksiya tək-tək nəzərdən keçirilməli və onlar üçün ayrıca blok diaqramlar yaradılmalıdır.

Blok diaqramlar sistemin sıradan çıxma halında bərpa olunmayan komponentlər üçün uyğundur. Bərpa olunan sistemlərdə əsasən, Markov metodundan istifadə edilir.

Əksər praktiki proqramlarda etibarlı blok diaqramların əvəzinə problem ağacının qurulması daha məqsədə uyğundur. Problem ağacı vasitəsilə sıradan çıxma hallarında mövcud ola biləcək bütün səbəblər araşdırılır. Onun sayəsində analitik potensial səbəbləri daha yaxşı anlaya bilir. Layihələndirmədə edilən analiz zamanı analitik layihəni yenidən düşünür və potensial problemlərin aradan qaldırılması məqsədilə bir sıra tədbirlər görür.

Etibarlılıq blok diaqramı qurulan zaman yalnız informasiya sistemini təşkil edən komponentin funksiyası düşünülür və onun ətraf mühit və insan faktorlarından qorunması haqqında düşünülmür.

Əlavə qiymətləndirmə üçün əsasən, blok diaqramlara istinad edilir. Kəmiyyət və keyfiyyət analizi üçün problem ağacının əvəzinə blok diaqramlardan istifadə edilir. Bu səbəbdən də sistemin etibarlılığını analiz etmək üçün məhz blok diaqramlara üstünlük verilir və problem ağacı isə alternativ yanaşma olaraq qalır.

Uğur ağacı modeli mahiyyətinə görə problem ağacına oxşayır. Onun vasitəsilə elementlərin sistemlə əlaqəsi aydınlaşdırılaraq sistemin müvəfəqiyyət dərəcəsi müəyyənləşdirilir.

Bəzən sistemin etibarlılıq dərəcəsi onun cari vəziyyəti ilə müəyyənləşdirilir. Bu zaman Markov modellərindən istifadə edilir. Markov modelləri uzun müddətli

etibarlılıq və əlyetenlik dəyərlərini əldə etmək məqsədilə mürəkkəb bərpa olunan sistemlərdə tətbiq edilir.

Petri net modeli sistemi simvolik dildən istifadə edərək təsvir edir. Model mürəkkəb sistemlərin və ya sistem şəbəkələrinin analizinə icazə verir. Petri net funksional olmayan və ya sıradan çıxmış elementləri də daxil etməklə sistemin modelini qurmağa şərait yaradır. Başqa sözlə, model bir və ya daha çox pozulmuş və bərpa altında olan elementlər olduğu zaman sistemin layihələndirilməsinə icazə verir. Petri net modeli təmir/ bərpa müddətləri nisbətən uzun olduqda istifadə edilir, çünki blok diaqramlar və problem ağacı əksər hallarda qısa təmir müddətləri üçün nəzərdə tutulub.

Elementlər, xüsusilə də komponentlərin sıradan çıxmasının birdən çox yolu ola bilər və bəzən bunun əsasında fövqəladə hallar modeli qurulur. Belə mexanizmlərədn istifadə sistemdəki şəraitindəki dəyişiklikləri, layihədəki fərqlilikləri qiymətləndirməyə icazə verir. Modellər müəyyən bir uğursuzluq mexanizmi və istifadə şərtləri üçün analitik olaraq əldə edilmiş və təcrübəli şəkildə təsdiqlənmiş empirik məlumatlardan istifadə edir. Model mexanizmin uğursuzluğunu detallı şəkildə modelləşdirməyə icazə verir. Əgər məhsul müştərilər tərəfindən müxtəlif yollarla istifadə edilərsə, bu zaman model vasitəsilə sıradan çıxma intensivliyi rahatlıqla hesablanılır.

Sadə sistemlərdə fövqəladə hallar modeli ilə tamamlanmış etibarlılıq blok diaqramlarından istifadə olunur. Mürəkkəb və ya yüksək əlyetənlik sistemləri Markov və ya Petri net modellərindən istifadəni və eləcə də sistemin etibarlılıq modellərini yaratmaq və qorumaq üçün xüsusi resurslar tələb edir.

Modellər qərar qəbul etmək məqsədilə istifadə edilmədiyi hallarda faydalı hesab edilmir. Yaradılan model müəssisənin iş qabiliyyətini dəstəkləməli, layihə qərarlarını qəbul etməli və riskləri qiymətləndirməlidir.

Ədəbiyyat siyahısı

1. John Wylder: “Strategic Information Security”, New-york
2. Karl de Leeuw, Jan Bergstra: “The history of Information security”
3. V. S. Bagad, I. A. Dhotre: “Information Security”
4. L. Jean Camp, Stephen Lewis: “Economics of Information Security”
5. John R. Vacca : “Computer and Information Security”
6. Neal Koblitz : “Algebraic aspects of Cryptography”
7. Keith M. Martin : “Everyday Cryptography: Fundamental Principles and Applicatons ” , 2017.
8. Randal K. Nichols, Panos Lekkas : “Wireless Security : Models, Threats and Solutions”
9. Way Kuo, Ming J. Zuo : “Optimal Reliability Modeling : Principles and Applications”
10. M.N.Əlizadə, H.M.Bayramov, Ə.S.Məmmədov : “İnformasiya Təhlükəsizliyi”.
11. Александр Васильевич Васильков : “Безопасность и управление доступом в информационных системах”
12. В. Шаньгин : “Информационная безопасность
13. “Научно-техническая информация: Организация и методика информационной работы” , 1995
14. Александр Молдовян, Михаил Вус, Владимир Гусев, Дмитрий Долгирев: “ Информатика: введение в информационную безопасность”
15. В. Шаньгин : “Защита информации в компьютерных системах и сетях”
16. В. Г. Сергеевич : “Экономическая безопасность: Учебник для вузов”

17. Виктор Каштанов, Алексей Медведев: “Теория надежности сложных систем”

18. Jeroen Guinée : “Handbook on Life Cycle Assessment: Operational Guide to the ISO Standards”

19. David Clifford : “ISO/IEC 20000: An Introduction to the global standard for service management”

20. C. Douglas Woodward : “BSI-the story of standards”

21. Henk J. de Vries : “Standardization: A Business Approach to the Role of National Standardization Organizations”

22. Пирогов Владислав Юрьевич : “Информационные системы и базы данных: организация и проектирование”

23. Rajeev Kaula : “An Open Intelligent Information Systems Architecture” , 1999

24. William H. Inmon : “Information Systems Architecture: A System Developer's Primer”

25. David Eliot Dreyfus : “Digital Cement: Information System Architecture, Complexity, and Flexibility” , Boston University, 2009

26. A. Sevilla Gamio : “Modular Information System Architecture as Part of an Implementation Plan for a National Centre for Remote Sensing Operations” , ITC, 2007

27. Joseph Migga Kizza : “Guide to Computer Network Security”

28. Naganand Doraswamy, Dan Harkins : “IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks”

29. Betty Biringer, Eric Vugrin, Drake Warren : “Critical Infrastructure System Security and Resiliency”

30. Issues in Information Science: Information Technology, Systems, and Security: 2011 Edition

31.https://notendur.hi.is/hthb1/%C3%81rei%C3%B0anleiki%20kerfa/System%20Reliability%20Theory%20Models%20and%20Statistical%20Methods.pdf

32. Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition, ISACA, 2006.

33. "Организация и технология защиты информации", "Комплексная защита объектов информации"

34. Alessandro Aldini, Roberto Gorrieri: “Foundations of Security Analysis and Design”

35. I. M Alsmadi, G. Karabatis, A. Aleroud : “Information Fusion for Cyber-Security Analytic