Azərbaycan Respublikası Təhsil Nazirliyi
Azərbaycan Dövlət İqtisad Universiteti

MAGİSTRATURA MƏRKƏZİ

Əl yazması hüququnda

Mahmudzadə Süleyman Camaləddin oğlu

"*İnformasiya sistemlərinin fəaliyyətinin təhlükəsizliyinin və etibarliliğinin təmini*" mözusunda

MAGİSTR DİSSERTASİYASI

İxtisasın şifri və adı:	060632- "İnformasiya texnologiyaları və sistemləri mühəndisliyi"
İxtisaslaşma:	"İnformasiya mühəfizəsi və təhlükəsizliyi"
Elmi rəhbər:	f.-r.e.n.,dos. K. K. Məmtiyev
Magistr proqramının rəhbəri:	akademik Ə. M. Abbasov
Kafedra müdiri:	akademik Ə. M. Abbasov

Bakı-2020

MÜNDƏRİCAT

GİRİŞ

İnformasiya artıq çoxdan maddi məhsulların istehsalı üçün köməkçi resurs olmuşdur .O, istifadə edildikdə informasiya sahibinə gətirə biəcəyi real gəlir və yaxud informasiya sahibinə vurulan zərərin miqdarı ilə müəyyən edilən dəyərə malikdir. Şübhə yoxdur ki, informasiyanın toplanması, işlənməsi, analizi və son istifadəçiyə çatdırılması *texnologiyalarının* və *sənayesinin* yaradılması bir sıra mürəkkəb problemlər yaratmışdır. *Bu problemlərdən* biri informasiya – hesablama sistemlərində və şəbəkələrində dövr edən və emal olunan informasiyanın *etibarlı qorunması* və *statusunun saxlanılması* (aktuallıq, tamlıq, məxfilik), həmçinin həmin sistem və texnologiyaların özlərinin *təhlükəsizliyidir*.

İnformasiya təhlükəsizliyi, informasiya resurslarının saxlanılması və müxtəlif növ sirlərin qorunmasını təmin etmək problemləri və məsələləri kompüter dövründən xeyli əvvəl yaranmış və həll edilmişdir. Bununla birlikdə, həyatın bütün sahələrinin kütləvi kompüterləşməsi, istehsal və idarəetmə sahəsindəki əsas informasiya axınlarının kompüter formasına və kompüter texnologiyalarına tədricən tərcümə edilməsi *təhlükəsizlik* və *məlumatın qorunmasında* oynanılan rolda keyfiyyətcə dəyişikliklərə səbəb olmuşdur.

Kompüter dövrünün ilk günlərindən etibarən informasiya texnologiyalarını və informasiya sistemlərini yaradanların əsas vəzifələrindən biri *təhlüksizliyin təmin edilməsi* məsələsi olmuşdur. Heç bir mövcur kommersiya və ya dövlət elektron sistemi öz məlumatlarını icazəsiz girişdən qorunmaq vasitələri olmadan fəaliyyət göstərə bilməz. Ötən yüzilliyin 70-ci illərindən başlayaraq dünyada informasiya qorunmasının müxtəlif konsepsiyaları və metodları işlənməyə başlandı ki, bu da qısa müddətdə bu problemə vahid yanaşmanın yaranmasına səbəb oldu – *ilk təhlükəsizlik siyasəti* işlənib hazırlandı. Bu gün informasiya texnologiyalarının və sistemlərininin təhlükəsizliyini təmin etmək sahəsində qanun və qanunverici aktların müddəaları avtomatlaşdırılmış sistemlərdə qorunma mexanizmlərinə bir sıra tələbləri artıq müəyyənləşdirmişdir.

İnformasiya texnologiyalarının və informasiya sistemlərin təhlükəsizliyi təşkilatın iqtisadi təhlükəsizliyinin təmini probleminin ən vacib komponentlərindən biridir. Hüquqi bazanın çatışmamazlığı və uyğunsuzluğu şəraitində iqtisadiyyatın yeni dövlət və iqtisadi idarəetmə formalarına keçməsilə əlaqədar olaraq verilən, informasiya, bilik və informasiya kommunikasiya texnologiyalarının özünün qorunması sahəsində *bütöv problemlər kompleksi* əmələ gəlmişdir. Bu problemlərin kəskinləşməsi *milli*, *sosial* və *korporativ təhlükəsizliyin*, o cümlədən informasiya sahəsindəki təhlükəsizliyin təmin olunması məsələlərini ön plana çəkmişdir.

Sistemin, xüsulilə də iqtisadi sistemin təhlükəsizliyi anlayışı intuitiv olaraq kifayət qədər aydındır. Müəyyən bir biznes prosesinin, konkret bir obyektin və ya şəxsin təhlükəsizliyinin təmin edilməsi ilə bağlı problemlər mütəmadi olaraq ortaya çıxır və ən azı ağıllı düşüncə səviyyəsində həll olunur. Bununla belə, müəyyən bir sistemin təhlükəsizlik anlayışını dəqiq ifadə etmək o qədər də asan deyil. Təhlükəsizlik anlayışının özünü müəyyənləşdirmədən hər hansı bir sistemin fəaliyyətinin təhlükəsizliyinin təmin edilməsi məsələsini qoymaq düzgün deyil, çünki layihənin məqsədini dəqiq başa düşülməməsi resurslardan rasional istifadə olunmamağa gətitirir və bütün layihənin pozulmasına səbəb olur. Ona görə, dövlət səviyyəsində milli təhlükəsizlik anlayışını və dövlətin iqtisadi təhlükəsizliyi konsepsiyasını müəyyən edən sənədlər formalaşdırılır və qanuni şəkildə tərtib edilir. Bu sənədlərdə, eləcə də bir çox elmi sənədlərdə təhlükəsizlik müəyyən aktivlərin təhdidlərdən qorunması ilə əlaqələndirilir.

Təhdidlər qorunan aktivlərə zərər vermə ehtimalına görə təsnifatlandırılır. İnsanların *qəsdən* və ya *bilmədən* hərəkətləri ilə əlaqəli olan *təhdidlər* əsas hesab olunur. İnsan fəaliyyəti ilə əlaqəli təhdidlərlə yanaşı olaraq, təbiətdə baş verən obyektiv proseslərlə – təbii fəlakətlər, radio dalğalarının yayılmasına təsir edən fiziki proseslər və buna oxşar proseslərlə bağlı təhdidlər də mövcuddur və nəzərə alınırlar.

İnformasiya sisteminin *təhlükəsizliyini* İS-nin normal fəaliyyətinə *təhdiddən qoruma vəziyyəti kimi* müəyyən etmək olar. *Təhlükəsizlik* – informasiya siste-

minin *təhdidlərlə* bağlı mənfi nəticələrin azaldılmasını və ya aradan qaldırılmasını təmin edən *alətlərinin* və onların *tətbiqi metodlarının* mövcudluğu kimi başa düşülür.“***İS-nin təhlükəsizliyi***” anlayışının tərifinə izah olunan yanaşma həm təhdidlərin *siyahısının* və həm də onların zamana görə *sabit olmasını* əsas götürür. İqtisadi fəaliyyətin bəzi sahələri, məsələn, ***elektron biznes***, yüksək dinamika ilə xarakterizə olunur. Proqram təminatı, o cümlədən İS-nin proqram təminatı tez-tez yenilənir, yeni aparat vasitələrinin tətbiqi və biznes portnyorlar və sonuncu istifadəçilərlə qarşılıqlı əlaqə metodlarının davamlı axtarışı davam edir. Bu halda təhlükəsizliyin təyininə bir az *fərqli bir yanaşma* mümkündür.

Müasir texniki, texnoloji və təşkilati sistemlər, eləcə də insanlar, insan qrupları və bütövlükdə cəmiyyət xarici informasiya təsirlərinə çox həssasdırlar. Silahlı qüvvələrin və texniki komplekslərin bütün idarəetmə vasitələri elektron hesablama texnikasının köməyi ilə təmin olunur. Bununla birlikdə, onlar xarici məlumat təsirlərinə – girov proqramlarına, proqramlarda sabitlərin məqsədyönlü dəyişməsinə, viruslara çox həssasdırlar. Faktların məqsədyönlü olaraq qəsdən şişirdilməsi və medialarının metodik təqdimatı tələb olunan məzmunda kifayət qədər sabit ictimai rəy formalaşdıra bilər. İnsanın zehni və təfəkkürü xarici informasiya təsirlərinə yüksək dərəcədə həssasdır, bunlar təşkil edilərkən, insan davranışını dünyagörüşü və inanc dəyişikliyinə qədər proqramlaşdırmaq üçün istifadə edilə bilər. *Aktual* təkcə məlumatların təhlükəsizliyinin qorunması problemi deyil, həm də beynəlxalq və strateji xarakter daşıyan məlumatların qorunmasıdır.

Bu dissertasiya işində mütəxəssisə bütün tələb və faktları nəzərə alaraq informasiya sistemlərinin təhlükəsizliyini modelləşdirməyə və təhlil etməyə imkan verən məsələlər tədqiq olunur.

Mövzunun aktuallığı.İnformasiya sistemlərinin təhlükəsizliyi və etibarlılığı ilə əlaqəli problemləri araşdırarkən, informasiya sistemlərinin işlənməsi, tətbiq olunması və istismarının başlıca tərkib hissəsi olan informasiya təhlükəsizliyin mövcud aspektlərinin nəzərə alınması maraq doğurur və olduqca vacibdir.

Tədqiqat işinin məqsədi: Bu tədqiat işinin məqsədi informasiya sistemlərinin fəaliyyətinin təhlükəsizliyinin və etibarlılığının qorunması ilə bağlı məsələlərin, xüsusilə təhlükəsizliyin baza modellərinin – diskresion və mandat modellərinin araşdırılmasından ibarətdir.

Tədqiqatın predmeti: Tədqiaqt işinin predmeti informasiya sistemlərinin təhlükəsizliyinqorunması ilə bağlı məsələlərdir.

Tədqiqatın metodoloji bazası: Tədqiq olunan mövzunun obyektini öyrənmək üçün mövcud vəziyyəti araşdıraraq müqayisəli təhlil aparmaq metodikasından istifadə olunmuş, eyni zamanda bu sahədə tədqiat aparam nüfuzlu alim və mütəxəssislərin elmi nəticələri və praktiki təklifləri əsas götürülmüşdür.

Tədqiqatın mənbəyi: Tədqiqat işində təhlükəsizlik siyasəti ilə bağlı yazılmış elmi məqalələrdən, İnternet saytlarındakı məlumatlarından, xaric və rus dilli ədəbiyyatdan, həmçinin, təhsilin inkişafının "Ali təhsil müəssisələrində sosial iqtisadi fənnlərin tədrisinin təkmilləşdirilməsi" innovasiya layihəsi proqramı çərçivəsində "Kadrların hazırlanmasının milli fondu "nun tövsiyyəsilə yazılmış dərsliklərdən geniş istifadə edilmişdir.

Elmi yenilik: Tədqiqat işində informasiya sistemlərinin fəaliyyətinin təhlükəsizliyinin qorunması ilə bağlı praktiki əhəmiyyət kəsb edən təkliflər və nəticələr müəyyən edilmişdir ki, bunlar işin sonunda gətirilmişdir.

İşin praktiki əhəmiyyəti: Tədqiqat işində İnformasiya sistemlərinin təhlükəsizliyiini təmin olunmasını müəyyən faktorların təyin olunması ilə bağlı praktiki təkliflərin tapılması istiqamətində araşdırmalar aparılmışdır.

İşin strukturu və həcmi: Tədqiqat işi girişdən, üç fəsildən, nətisə və təkliflərdən ibarətdir. Birinci fəsil istisna olmaqla ikinci və üçüncü fəsillərin hər biri dörd paraqrafdan ibarəttdir. İşin sonunda istifadə olunan elmi mənbələrin siyahısı verilmişdir.

İşin girişində mövzunun aktuallığı, problem haqqında qısa məlumat, tədqiqat işinin məqsədi və qarşıya çıxan problemlər müəyyənləşdirilib.

Dissertasiya işinin birinci fəslində informasiya sistemlərinin təhlükəsizliyilə bağlı bəzi məsələlər analiz edilir. Bu fəsil iki paraqrafdan ibarətdir. *Birinci paraqrafda* təhlükəsizlik anlayışı verilir və zəif qorunan verilənlərə *təcavüzkarların hərəkətləri*, *personal tərəfindən buraxılmış səhvlər*, *qurğuların və proqramların işində dayandırma* və *qasırğa, yanğın və ya zəlzələ* kimi təbii fəlakətlərin təsirinin olması göstərilir. Qeyd edilir ki, informasiya sistemlərindən alınan informasiya *məxfilik*, *tamlıq* və *əl çatanlıq* tələblərini ödəməlidir və bu sistemlərin təhlükəsizliyinin analizində *hücum*, *təcavüzkar* və *təhdid mənbəyi* kimi anlayışlardan istifadə olunur. *İkinci paraqrafda* təhdidlərin *mənbəyinə*, *reallaşdırılma məqsədinə* və informasiya sistemlərinə *təsir xarakterinə* görə təsnifatı verilir. Göstərilir ki, informasiya sistemlərinin *təhlükəsizliyinin təminatı problemi* mürəkkəb bir problemdir və özündə *fiziki*, *texnoloji, məntiqi* və *insan ölçmələri* kimi müstəqil ölçmələri özündə cəmləşdirir.

Dissertasiya işinin ikinci fəslində təhlükəsizliyin əsas mənbələrinin və xarakteristikalarının araşdırılmasına baxılımışdır. Bu fəsil dörd paraqrafdan ibarətdir. Onun *birinci paraqrafında* ilk olaraq təhlükəsizlik siyasəti və onun formal model şəklində təsvir edilməsinin əsas məqsədi açıqlanır. Təhlükəsizlik siyasəti modellərinin üç əsas tipi – *diskresion*, *mandat* və *rol* modelləri, onlara aid nümunələr, onların üstün cəhərləri və şatışmamazlıqları sadalanır. Göstərilir ki, təhlükəsizliyin *rol* modelindən fərqli olaraq *diskresion* və *mandat* kimi klassik baza modellərində təhlükəsizlik siyasəti əvvəlcədən təyin olunur. Təhlükəsizliyin diskresion ***Harisson-Ruzzo-Ulman*** modelinin *troyan atları* proqramına həssas olduğu halda hərbi sənayedə tətbiq olunan mandatlı ***Bela-LaPadull*** modelində bu problemin olmadığı açkar edilmişdir. İkinci paraqrafda informasiya sitemlərinin *təhlükəsizliyinin* və *etibarlılığının təmini* üçün proqram kompleksləri sistemlərinin yaradılmasının zəruri olması və bu sistemlərin *məxfilik*, *tamlıq* və *əl çatanlıq* kimi komponentlərinin vacibliy, həmçinin təhlükəsizliyin təmnatı kompleksi sisteminin dörd səviyyəsi üçün xarakterik olan *metod* və *vasitələr* qeyd olunur. *Üçüncü paraqrafda* təhlükəsizliyin təminatının *təşkilatı*, *texniki* və *proqram* aspektləri araş-

dırılır, verilənlərin təhlükəsizliyi problemlərilə bağlı elmi tədqiqatların aparılmasının xüsusi rolu, o cümlədən, ABŞ Müdafiə Nazirliyi tərəfində tərtib olunan "*Narınci kitab*" in, qonşu Rusiya Federasiyasında hazırlanan sənədlərin və ***BS 7799*** britaniya standartının bu sahədə ilk metodiki baza olması qeyd olunmuşdur. Qorunma səviyyəsinə görə təhlükəsizlik siniflərinin *dörd qrupa*, avtomatlaşdırılmış sistemlərin informasiya emal proseslərinin təhlükəsizliyinə görə *üç qrupa* bölünməsi aşkar edilmişdir. İnformasiya sistemlərinin ***CRAMM*** adlanan tam tədqiqat metodikası sistemin analizi verilmişdir. Bu fəslin *sonuncu paraqrafında* informasiya sistemlərinin bərpası və nüsxələşdirilməsinin metod və vasitələri araşdırılmış, verilənlərin məhv edilməsinin bəzi tipik obyektiv və qəsdən edilə bilən səbəbləri açıqlanmış, verilənlərin bərpası məsələsinin üçün məlumat bazasının surətinin əldə edilməsinin *iki yolu* göstərilmiş, həmçinin, nüsxələşdirmə texnologiyasının rellaşmasına baxilmışdır.

Disertasiya işinin üçüncü fəslində nəzarətedici alt sistemlərin yaradılması ilə əlaqəli məsələlər araşdirılır. Bu fəsil də ikinci fəsil kimi dörd paraqrafdan ibarətdir. Onun *birinci paraqrafında* ABŞ Milli Standartlar və Texnologiyalar İnstitutu tərəfindən hazırlanmış kompüter təhlükəsizliyi təlimatının bölmələri, o cümlədən *təhlükəsizlik siyasətinin predmeti*, *təşkilatın mövqeyinin təsviri*, *tətbi-qi*, *rol və vəzifələr* və s. göstərilir. Təhlükəsizlik siyasətinin müvəffəqiyyətinin onu həyata keçirən insanların təcrübəsindən daha çox asılı olması qeyd olunur. *İkinci pqraqrafda* identifiksiya və audentifikasiya məsələlərinə baxılır, qeyd olunur ki, informasiya sistemi resurslarına çıxış əldə etmək *identifikasiya*, *au-dentifikasiya* və *avtorizasiya* kimi üç prosedurun yerinə yerinə yetirilməsinə əsaslanır. Konkret autentifikasiya prosedurlarının əsasını qoyan *prinsiplər* göstərilir. *Üçüncü paraqrafda* informasiya sistemlərinin ştat rejimini pozulmaları-nın tipləri tədqiq olunur. Qeyd olunur ki, qorunan informasiya sistemləri üçün xarakterik xüsusiyyətlərin itirilməsi üç böyük siniflə təqdim oluna bilər. Nəhyət, *sonuncu paraqrafda* müdaxilənin aşkarlanması və onun mənfi nəticələrinin aradan qaldırılması ilə bağlı problemlər araşdırılır, informasiya sistemlərinə müdaxilənin

aşkarlanmasını dörd üsulu göstərilir.

Disertasiya işi 76 səhifədən ibarətdir. İşdə 10 şəkil vardır, ədəbiyyat siyahısı 26 addan ibarətdir. Disertasiya üzərində işləyərkən çöxsaylı İnternet resurslarına baxılmış, yerli və xarıci, ocümlədən rus alimlərinin tədqiqat işlərindən geniş istifadə edilmişdir.

Fəsil I. İnformasiya sistemlərinin təhlükəsizliyi

1.1.Təhlükəsizlik anlayışı

İnformasiya təhlükəsizliyi anlayışı informasiyanın və müxtəlif növ verilənlərin qanunsuz öyrənilməsindən, istifadəsindən, məhv edilməsindən qorunması kimi müəyyən edilir. Bundan əlavə, informasiya təhlükəsizliyi informasiyanın icazəsiz yayılmasına səbəb olan hərəkətlərdən qorunmağı da əhatə edir. Zəif qorunan verilənlərə təsirlər çox fərqli ola bilər. Bu təsirlərə aşağıdakılar aiddir:

- təcavüzkarların hərəkətləri;
- personal tərəfindən buraxılmış səhvlər;
- qurğuların və proqramların işində dayandırma;
- qasırğa, yanğın və ya zəlzələ kimi təbii fəlakətlər.

Verilənlərin məxfiliyinə, tamlığına və etibarlılığının qorunmasına zəmanət verən tədbirlər görülsə, informasiya təhlükəsizliyinə həqiqətən nail olmaq olar. Verilənlərin qorunması informasiyaya tez əlçatanlığın əldə edilməsini təmin etmək üçün nəzərdə tutulmuşdur. İnformasiya təhlükəsizliyi mümkün təhdidləri görməlidir və saxlanılan və ya ötürülən məlumatın hüquqi əhəmiyyətini təsdiqləməlidir. Lazım gələrsə, informasiya və onun resursları müvafiq girişə açıq olmalıdır. Bunlar verilənlərin əsas xüsusiyyətləridir ki, onların nəzərə alınmaması verilənlərin effektivliyini əhəmiyyətli dərəcədə azaldır.

Geniş mənada *informasiya təhlükəsizliyi* informasiyanın təsadüfi və ya qəsdən pozulmadan qorumaq üçün müdafiə vasitələrinin yığımıdır. Zərbənin əsasının təbii amillər və ya süni səbəblərdən ibarət olmasından asılı olmayaraq informasiya sahibi itkilərə məruz qalır.

İnformasiya sistemlərinin təhlükəsizliyi geniş problemin – *kompüter sisteminin təhlükəsizliyi* və ya *informasiya təhlükəsizliyi* kimi daha geniş problemin hissəsidir. Bununla bağlı olaraq əhəmiyyətli dərəcədə informsiya sistemlərinə də tətbiq edilə bilən təhlükəsizliyə bəzi ümumi yanaşmaların müzakirəsi əhəmiy-

yətlidir. İnformasiya sistemlərindən alınan informasiya müəyyən tələbləri ödəməlidir. Təqdimat formasından asılı olmayaraq "*informsiya*" anlayışının məzmunlu analizi, onun toplanma, saxlanma, emal olunma, təqdim edlmə və verilmə prosesinin və texnologiyasının xüsusiyyətləri göstərir ki, informasiya ilə işləməyin funksional məzmunundan asılı olmayaraq "*İnformasiya təhlükəsizliyi*" anlayışı üç komponentdən ibarətdir:

1. *informasiyanın* ***məxfiliyi****;*

2. *informasiyanın* ***tamlğının*** *təmin edilməsi;*

3. *informasiyaya* ***əlçatanlığın*** *təmin edilməsi.*

Məxfilik – informasiyanın yalnız icazəsi olan insanların və proseslərin oxuya və şərh edə bilməsinə zəmanətdir. Məxfilik, icazəsiz istifadəçilər tərəfindən informasiyaların açıqlanmasının qarşısını alan prosedurları və tədbirləri əhatə edir. Buna misal olaraq məlumat alandan başqa hər kəs tərəfindən oxumaqdan qorunan bir poçt məlumatını göstərmək olar.

İnformasiyanın tamlığı – informasiyanın dəyişməz, korrekt və həqiqi olmasının təminatıdır. Tamlığın təmin edilməsi, informasiyanın icazəsiz yaradılmasının, dəyişdirilməsinin və ya silinməsinin qarşısının alınmasını nəzərdə tutur. Buna nümunə olaraq poçt məlumatlarının göndərilməsi zamanı onların dəyişdirilməməsinə zəmanət verən tədbirləri göstərmək olar.

Əl çatanlıq – icazəsi olan istifadəçilərin informasiya aktivlərinə, resurslarına və sistemlərinə daxil olmaq və işləmək zəmanətidir. Bu halda tələb olunan məhsuldarlıq təmin edilir. Əlçatanlığın təmin edilməsi, sistemin imtina etməsi və informasiya əlşatanlığının pozmaq üçün qəsdən edilən cəhdlər də daxil olmaqla, maneənin yaranması imkanının olmasına baxmayaraq informasiyaya çıxışı dəstəkləyən tədbirləri əhatə edir. Əlçatanlığı təmin etmək, sistem çatışmazlığı və əlçatanlığı pozmaq üçün qəsdən cəhdlər də daxil olmaqla, maneənin yaranması imkanına baxmayaraq məlumatların əldə edilməsini təmin etmək üçün tədbirləri əhatə edir. Buna misal olaraq poçt serverlərinin buraxılış imkanının təmin edilməsini göstərmək olar.

İnformasiya təhlükəsizliyinin məqsədi bu üç ən vacib təhlükəsizlik xidmətini təmin etməkdir. Demək olar ki, *informasiya sistemlərinin təhlükəsizliyi* informasiyanın və infrastrukturun təbii və ya süni xarkterli təsadüfi və ya qəsdən nəzərdə tutulmuş təsirlərdən qorunmasıdır. *İnformasiyanın qorunması* dedikdə informasiya təhlükəsizliyinin təmin olunmasına yönəldilmiş tədbirlər kompleksi nəzərdə tutulur.

Qeyd edək ki, informasiyanın *əlçatanlığı, tamlığı* və *məxfiliyi* əsasında qurulmuş informasiya təhlükəsizliyi bəzən ***CİA*** modeli adlanır. Bu qısa ad ***C****onfidentiality* (məxfilik), ***I****ntegrity* (tamlıq), ***A****vailability* (əl çatanlıq) ingilis sözlərindən yaranmışdır . İnformasiya təhlükəsizliyinin təhdidi dedikdə saxlanılan, ötürülən və ya emal olunan informasiyanın yəqinliyinin, tamlığının və məxfiliyinin pozulmasına səbəb olan hərəkətlər və ya hadisə başa düşülür. İnformasiya sistemlərinin analizində ***hücum*** (*təhdidi reallaşdırmaq cəhdi*), ***təcavüzkar*** (*hücumu həyata keçirən*), ***təhdid mənbəyi*** (*potensial təsavüzkar*) kimi anlayışlardan istifadə edilir.

İS-nin təhlükəsizliyini sistemin fəaliyyət göstərdiyi mühitin təcavüzkar təzahürlərə uyğunlaşmaq xassəsi kimi təyin etmək olar. Formalaşdırılmış tərifdə əsas diqqət neytrallaşdırılması təmin olunan təhdidlərin *siyahısı* və *məzmununa* deyil, sistemin keyfiyyətinin xüsusi xarakteristikasına yönəldilmişdir. Bu halda İS-nin əsas keyfiyyət əlaməti *səmərəlilikdir*, yəni təhlükəsizliyin *metod* və *vasitələrinin qiymətləndirilməsi* təhlükəsizlik mexanizminin reallaşmasına sərf olunan ***xərclərin*** və mühitin qəsdən və ya təsadüfən təcavüzkar təzahürü ilə bağlı zərərin qarşısının alınması hesabına alınan ***potensial gəlirlərin*** uçotu əsasında həyata keçirilir. İS-nin *təhlükəsizliyinə inam* qiymətləndirmə obyektinin istismarı və qiymətləndirilməsi prosesində razılaşdırılmış fəaliyyət nəticəsində əldə edilə bilər.

İS-nin təhlükəsizliyinin qiymətləndirilməsinin funksional məqsədi – sistemin onun üçün tələblərə nə dərəcədə cavab verdiyinə müəyyən dərəcədə inam əldə etməkdir. *Qiymətləndirmənin nəticələri* istehlakçıya sistemin təhlükəsizlik

səviyyəsinin sistemin nəzərdə tutulmuş tətbiqi üçün kifayət olub olmadığını və qalıq risklərin məqbul olub olmadığını müəyyənləşdirməyə kömək etməlidir. İS-nin təhlükəsizlik səviyyəsini təmin etmək üçün ortaya çıxan təhdidlərin xarakterini, sistemin və ya texnologiyanın zəifliyi səviyyəsini azaltmağın əsas üsullarını anlamaq vacibdir.

Qərar qəbul edənlər tərəfindən *təhdidlərin xarakteri* və təhlükəsizlik metodlarının məqsədi və xüsusiyyətləri barədə kifayət qədər məlumatlı olmaması müxtəlif səhv anlayışların geniş yayılmasına səbəb olur.

1.2.Təhdidlərin reallaşdırılması məqsədinə və informasiya sisteminə təsir xarakterinə görə təsnifat

Təhlükəsizliyin təyini üçün qəbul edilmiş yanaşmadan asılı olmayaraq ***təhdidlərin*** və onların ***mənbələrinin*** təsnifatı maraq doğurur. Bütün təhdidlərin onların xarakterinə görə bölünməsi, informasiya təhlükəsizliyinin təhdidlərinin *təsadüfüfi* və *qəsdən* olmaqla iki yerə bölünməsinə gətirir. *Təsadüfi təhdidlər* insanların iradəsindən və istəklərindən asılı olmayaraq ortaya çıxır, baxmayaraq ki, insanlar bu təhdidlərin mənbəyi ola bilərlər. *Qəsdən təhdidlər* həmişə insanlar tərəfindən və qəsdən hərəkətləri ilə yaradılır. Təhdidlərin müxtəlif əlamətlərə görə təsnifatı şəkil 1-də sxematik olaraq təsvir edilmişdir.

Qeyd edək ki, təhlükəsizlik təhdidlərini onların ***mənbəyinə görə*** üç sinfə ayırmaq olar:

- ***Təbii təhdidlər***. Təbii təhdidlər təsadüfi olur və ilk növbədə kompüter sisteminə və ya onun həyat təminetmə sisteminə birbaşa fiziki təsir ilə əlaqəlidir. Bu cür təhdidlərin mənbəyi təbii fəlakətlərdir. Bu cür hadisələrin qarşısını almaq mümkün deyil, lakin bunları qabaqcadan görməkk və mənfi nəticələrini minimuma endirmək olar.
- ***Texniki təhdidlər.*** Texniki təhdidlər – texniki vasitələrin nasazlığı (*kompüterlər, rabitə vasitələri və s*.) və proqram təminatının işi ilə bağlı problem-

lərin yaratdığı təhdidlərdir. Sonuncu halda, informasiya sisteminin bir hissəsi olan *proqram təminatındakı* nasazlıqlar və *sistemin proqram təminatındakı* nasazlıqları (*əməliyyat sistemləri, drayverlər, şəbəkə proqramı*) fərqləndirmək lazımdır. Texniki təhdidlərə həyat təminetmə sistemlərindəki (*binalar, istilik-, su təchizatı və s*.) nasazlıqlar da əlavə edilməlidir. Texniki təhdidlər nəinki qabaqcadan görünə bilər, bəzilərinin həyata keçirilməsi mümkün olmaya da bilər. Həyat təminatı sistemlərin vaxtında təmiri, fasiləsiz enerji təchizatı və hətta daha yaxşı alternativ mənbələr - bunların hamısı informasiya təhlükəsizliyinin bir hissəsidir.

- ***İnsanların yaratdığı təhdidlər***. Bu təhdidləri iki yerə ayırmaq olar – bilavasitə sistemlə işlyən adamların (xidməti heyət, proqramçılar, administratorlar, operatorlar, idarəedici aparat və s.) təhdidləri və xarici təcavüzkarın yaratdığı təhdid, o cümlədən xaker hücumları, kompüter virusları və s.

Təhdidin reallaşdırılması məqsədi ilə təsnifat İS-lərin, xüsusilə açıq sistemləridə, o cümlədən İnternetdə istifadə təcrübəsini əks etdirir. Bunlar aşağıdakılardır:

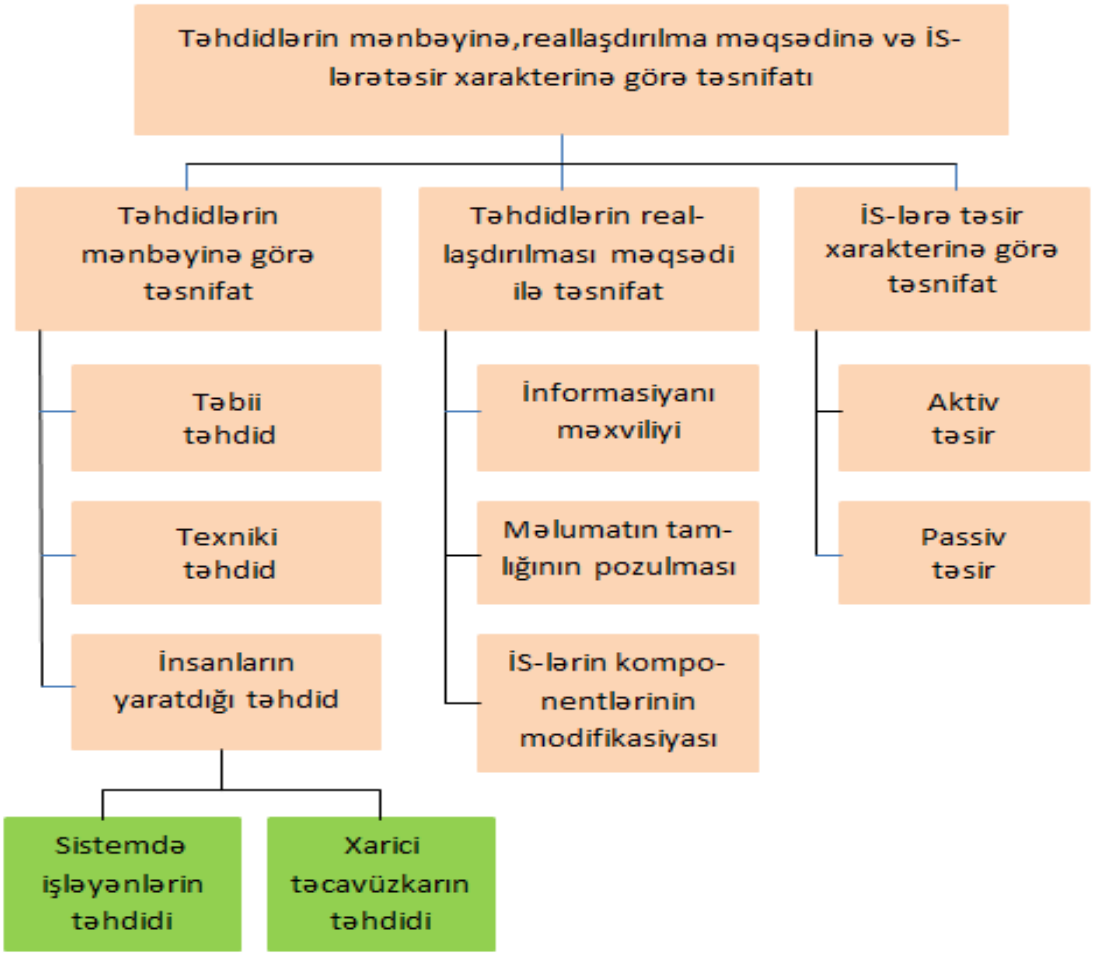
- informasiyaların *məxfiliyinin pozulması;* yəni İS - lərdə saxlanılan və informasiyanın sahibi olmayan şəxslərin və yaxud proseslərin informasiyadan istifadə etməsi;
- məlumatın *tamlığının pozulması*; yəni informasiyanın modifikasiya və ya məhv edilməsi;
- İS-lərin, onların komponentlərinin modifikasiyası və yaxud dəyişdirilməsi daxil olmaqla, komponentlərinin sıradan çıxması və yaxud qeyri korrekt dəyişməsilə hesabına *İS-nin işinin tam və ya qismən pozulması*.

İS-lərə təsir xarakterinə görə aşağıdakı iki təsirin seçilməsi xarakterikdir:

- ***aktiv təsir***, yəni İS-nin istifadəçisinin onun səlahiyyətlərindən kənara çıxan hər hansı hərəkəti, və yaxud İS-lə münasibətdə kənar istifadəçinin və ya prosesin yuxarıda göstərilən məqsədlərdən birinə və ya bir neçəsinə

çatmaq üçün nəzərdə tutulan hərəkəti;

- ***passiv təsir***, yəni istifadəçinin İS-nin hər hansı bir paramertini və yaxud toplanmış məlumatların analizi əsasında informasiyanın məxfiliyinin alınması məqsədilə əks effekləri müşahidə etməsi.



Şəkil 1. Təhdidlərin mənbəyinə,reallaşdırılma məqsədinə və İS-lərə təsir xarakterinə görə təsnifatı

Statistika göstərir ki, informasiya təhlükəsizliyi pozuntularının əsas səbəbləri təbii fəlakətlər və qəzalar, avadanlıqların qəzaları və nasazlıqları, dizayn səhvlərinin nəticələri, əməliyyat səhvləri, pozucuların və təcavüzkarların qəsdən etdikləri hərəkətlər. İnformasiya təhlükəsizliyinin təhdidlərini yuxarıda sadalanan əlamətlərdən başqa ***birbaşa*** və ***dolayı*** olaraq bölmək olar. Dolayı təhdidlər birbaşa kompüter sistemindəki istənilən arzuolunmaz hadisələrə səbəb olmur, lakin onlar yeni

dolayı və ya birbaşa təhdid mənbəyi ola bilər. Məsələn, kompüter virusu ilə yoluxmuş diskə bir fayl yazmaq yalnız müəyyən ehtimalla əməliyyat sisteminin işində nasazlıqlara səbəb ola bilər. Öz növbəsində əməliyyat sistemindəki nasazlıq da müəyyən ehtimalla informasiya sisteminin nasazlığına gətirir. Odur ki, mümkün olan *dolayı təhdidləri* bilmək bilavasitə informasiya sisteminə *təhdidləri hesablamaqda* və *təhlükəsizlik səviyyəsini artırmaqda* kömək edir.

"***İnformasiya təhlükəsizliyi***" təhdidi, bir qayda olaraq, informasiya təhlükəsizliyi rejiminin potensial pozulmasıdır. Təhdidin qəsdən həyata keçirilməsinə informasiya sisteminə ***hücum*** deyilir. Təhdidləri qəsdən həyata keçirən şəxslər ***təcavüzkarlardır***. Çox vaxt təhdid, informasiya sistemlərinin qorunmasında zəif yerlərin olmasının , məsələn, fərdi kompüterlərə və ya sənədsiz proqramlara nəzarətsiz girişin (təəssüf ki, hətta lisenziyalı proqram zəifsiz deyil) nəticəsidir.

İnformasiya təhlükəsizliyinin analizi və təhdidinin aşkar edilməsi administrativ səviyyədə informasiya təhlükəsizliyinin *ikinci vacib* funksiyasıdır. Bir çox cəhətdən işlənən müdafiə sistemi və onun reallaşdırılma mexanizmlərinin tərkibi bu mərhələdə aşkar olunan potensial təhdidlərlə müəyyən edilir. Məsələn, əgər təşkilatın hesablama şəbəkəsinin iştirakçılarının İnternetə çıxışı varsa, onda informasiya təhlükəsizliyi təhdidlərinin sayı kəskin olaraq artır və bu müdafiənin, uyğun olaraq, metod və vasitələrində əks olunur.

İnformasiya sistemlərinin inkişaf tarixi göstərir ki, yeni zəif yerlər həmişə əmələ gəlir. Eyni müntəzəmliklə, lakin bir az geriləmə ilə, qorunma vasitələri də yaranır. Bir çox müdafiə vasitələri ortaya çıxan təhdidlərə cavab olaraq meydana çıxır, məsələn, *Microsoft* şirkətinin proqram təminatında daima, onun zəif yerlərini aradan qaldıran düzəldilmələr edilir. Təhlükəsizliyin təminatı üçün belə yanaşma *az effektlidir,* belə ki, təhdidin aşkarlandığı və onun aradan qaldırılması arasında müəyyən zaman tələb olunur. Məhz bu zaman dövründə təcavüzkar informasiyaya düzəldilməsi mümkün olmayan zərər vura bilər.

Qeyd edək ki, İS-nin *təhlükəsizliyinin təminatı problemi* mürəkkəbdir və aşağıdakı kimi bir neçə müstəqil ölçmənin xüsusiyyətlərini özündə cəmləşdirir:

- fiziki ölşmə;
- texnoloji ölçmə;
- məntiqi (prosedur) ölşmə;
- insanın ölçməsi.

Fiziki ölçmənin xarakteristikası elektron biznesin informasiya mühitinin texniki əsasını təşkil edən *elementlərin fiziki müdafiəsinin* nə qədər səmərəli şəkildə təmin olunduğunu göstərir. Kompüterlər, marşrutlaşdırıcılar, rabitə xətləri *dağıdıcı təsirlərin* potensial daşıyıcıları üçün fiziki olaraq *əlçatmaz olmalıdır*. Monitor ekranları, avadanlıqların elektromaqnit şüalanması məxfi məlumat mənbəyi olmamalıdır.

Texnoloji ölçmənin xarakteristikası, tələb olunan təhlükəsizlik səviyyəsini (*istifadəçi identifikasiyası, girişə nəzarət, informasiya infrastrukturunun bütövlüyünü təmin etmək* və s.) təmin edən prosedurların *aparat-proqram realizasiyasının* nə qədər səmərəli şəkildə təmin olunduğunu göstərir. Disertasiya işində İS-lərin məhz bu ölçmələr üçün xarakterik olan *metod* və *vasitələr* araşdırılır.

Məntiqi (prosedur) ölçmənin xarakteristikası sistemin təhlükəsizlik mexanizmlərinin məntiqi əsaslarının nə qədər adekvat olduğunu göstərir. Əgər *kritik vacib məlumat blokları* səhv təyin olunmuşdursa, onda o, proqram və aparat kompleksindəki çatışmamazlıqlara görə deyil, sistemin layihələndirmə səhvlərinə görə həsas olur.

Dördüncü ölçmənin xarakteristikası sistemin təhlükəsizliyinə cavabdeh insanların davranışlarının nə qədər adekvat olduğunu göstərir. Bu xarakteristikanı ölçmək üsulları humanitar elmlər arsenalından götürülməlidir. Hər bir avtomatlaşdırılmış sistemdə, o cümlədən də iqtisadi fəaliyyətin təmin edilməsi üçün hazırlanmış İS-də, *kritik vacib məlumatlara sahib* və sistemin təhlükəsizliyinə cavabdeh olan adamlar var. Müxtəlif səbəblər, məsələn, *xəsislik, nədənsə narazılıq, boş şey* və s. bu məlumatın *təcavüzkara* könüllü ötürülməsinə və ya sistemdəki dağıdıcı təsirlərə qarşı effektiv mübarizə üçün *lazımi tədbirlərin görülməməsinə* səbəb ola bilər.

Təqdim olunan bu dörd ölçü müəyyən mənada bir birinə ortoqonaldır. Müəyyən bir ölçmənin xüsusiyyətlərini yaxşılaşdıran tədbirlər heç də həmişə bütövlükdə sistemin təhlükəsizliyinin artmasına səbəb olmur. Müxtəlif ölçmələrin xüsusiyyətləri balanslı olmalıdır.

FƏSIL II. Təhlükəsizliyin əsas mənbələri və xarakteristikalari

2.1. Verilənlərin təhlükəsizliyi və proqram-texniki elementlər

Məlumatların İS-lər üçün xarakterik olan *avtomatlaşdırılmış işlənməsi texnologiyaları* məlumatların və proqram və aparat elementlərinin təhlükəsizliyini təmin etmək üçün əsas yanaşmaları müəyyənləşdirir. İlkin olaraq, insanın həll etməli olduğu məsələ seçilməlidir. Bu vəziyyətdə şəxs (*təşkilatın ən yüksək səviyyəli idarəetmə meneceri*) ***təhlükəsizlik siyasətinin*** əsas xüsusiyyətlərini müəyyənləşdirməlidir.

İnformasiya sistemlərinin təhlükəsizliyi sahəsində fundamental anlayış təhlükəsizlik siyasətidir.

Təhlükəsizlik siyasəti dedikdə informasiyanın emalı prosesini tənzimləyən bir sıra *norma* və *qaydalar* yığımı başa düşülür, ki onların yerinə yetirilməsi müəyyən təhdidlərdən qorunmanı təmin edir və sistemin təhlükəsizliyinin zəruri şərtini təşkil edir.Təhlükəsizlik siyasətinin formal ifadəsinə ***təhlükəsizlik modeli*** (*giriş nəzarəti modeli, təhlükəsizlik siyasəti modeli*) deyilir. Təhlükəsizlik modeli sistemin formal işlənmə metodunda əsas rol oynayır. Bu modelin məqsədi, bir qayda olaraq, müəyyən bir sistem üçün təhlükəsizlik tələblərinin mahiyyətini ifadə etməkdir. Təhlükəsizlik modeli sistemdə icazə verilən məlumat axınını və məlumata çıxışın əldə edilməsi qaydalarını müəyyənləşdirir.

Model sistemin xüsusiyyətlərini analiz etməyə imkan verir, lakin bu və ya digər qorunma mexanizmlərinin reaizə olunmasına heç bir məhdudiyyət qoymur. Model formal olduğundan, sistemin müxtəlif təhlükəsizlik xüsusiy-yətlərini sübut etmək mümkündür. Yaxşı təhlükəsizlik modeli, modelləşdirilən sistemin mücərrədlik, sadəlik və adekvatlıq xüsusiyyətlərinə malikdir.

Sistemin təhlükəsizlik siyasətinin yaradılmasının və onun formal model şəklində təsvir edilməsinin ***əsas məqsədi*** sistemin vəziyyətinin tabe olduğu müəy-

yən şərtlərin müəyyən edilməsi, təhlükəsizlik meyarının tərtib edilməsi və təsis edilmiş qaydaları və məhdudiyyətləri gözləməklə sistemin bu meyarlara uyğunluğunun formal sübutunun aparılmasıdır. Bundan əlavə, ***formal təhlükəsizlik modelləri*** qorunan sistemlərin *layihələndirilməsi, işlənilməsi* və *sertifikatlaşdırılması* prosesində meydana çıxan bir sıra məsələləri həll etməyə imkan verir. Ona görə onlardan yalnız informasiya təhlükəsizliyinin nəzəriyyəçiləri deyil, həm də qorunan informasiya sistemlərinin yaradılması və istismarı prosesində iştirak edən digər kateqoriya mütəxəssislər (istehsalçılar, istehlakçılar, mütəxəssislər) də istifadə edir.

Qeyd edək ki,yalnız təşkilatın məqsədlərini və fəaliyyət şərtlərini aydın şəkildə bilən bir şəxs, hansı məlumatın qorunmasının lazım olduğunu və məlumatın icazəsiz yayılması, təhrif edilməsi və ya məhv edilməsinin nə qədər *əhəmiyyətli itki ola biləcəyini* müəyyən edə bilər.

Təhlükəsizlik siyasəti müəyyən edildikdən sonra, avtomatlaşdırılmış konturlarla onun realizə olunması texnologiyası məsələsinin həll olinması zəruridir. Təbii dil baxımından formalaşdırılan təhlükəsizlik siyasətinin *qaydaları* və *normalarını* həyata keçirmək üçün hər hansı bir formal dildə effektiv proqramlaşdırmaya imkanı verən müəyyən *fopmal modeldən* istifadə etmək (və işləmək) lazımdır.

Təhlükəsizlik modelləri qorunan informasiya sistemlərinin inkişafında və araşdırılmasında mühüm rol oynayır. Əslində təhlükəsizlik modelləri "*Müştəri (İstehlakçı) – Dizayner (İstehsalçı) – Ekspertt (Auditor)"* üçlüyündəki ilkin birləşdirici elementdir. Təhlükəsizlik modelləri əsasında ***müştərilər***, *təhlükəsizlik siyasətinə,* təşkilatlarında və müəssisələrində qəbul edilən məlumatların emalı proseslərinə uyğun qorunan informasiya sistemləri üçün tələblər formalaşdıra bilərlər. Təhlükəsizlik modelləri əsasında ***tərtibatçılar***, işlənən sistemlərə görə texniki – texnoloji tələblər və proqram – aparat həllini formalaşdırırlar.

Əvvəlcə təhlükəsizlik modelinin nə üçün zəruri olduğunu qeyd edək. Onun məqsədi baxılan sistemin təhlükəsizlik tələblərini formalaşdırmaqdır. Təhlükə-

sizlik modeli sistemin xüsusiyyətlərini təhlil edir və daxilində icazə verilən məlumat axınlarını müəyyənləşdirir. Təhlükəsizlik modeli nəzərdən keçirilərkən aşağıdakı anlayışlardan istifadə edilir:

1. **məlumat əldə etmək;**
2. **girişə nəzarət qaydaları;**
3. **giriş obyekti;**
4. **giriş subyekti.**

Onların hər birinin dəqiq tərifləri nə baxaq:.

İnformasiya çıxışın əldə edilməsi dedikdə informasiya ilə tanış olmaq və informasiya üzərində onun emalı, köçürülməsi, dəyişdirilməsi və məhv edilməsi kimi əməliyyatların aparılmasını nəzərdə tutulur.

Girişə nəzarət qaydaları – subyektlərin obyektlərə giriş hüquqlarını tənzimləyən qaydalar yığımıdır.

Giriş obyekti – girişə nəzarət qaydaları ilə tənzimlənən avtomatlaşdırılmış sistemin informasiya resursu vahididir.

Giriş subyekti – hərəkətləri girişə nəzarət qaydaları ilə tənzimlənən bir şəxs və ya prosesdir.

Təhlükəsizlik modelləri öz aralarında təhlükəsizlik siyasəti ilə fərqlənirlər. Təhlükəsizlik siyasəti informasiya emalının konkret texnologiyasından, istifadə olunan aparat və proqram təminatından və bu təhlükəsizlik siyasətinin təsvir olunduğu təşkilatın yerindən asılı ola bilər.

Bütün mövcud təhlükəsizlik modelləri aşağıdakı əsas anlayışlara əsaslanır.

1. Kompüter sistemi bir-biri ilə əlaqə quran mövcudluqların - *subyektlərin* və *obyektlərin* toplusudur. *Obyektləri* intuitiv olaraq informasiyaları özündə saxlayan *konteyner* şəklində təsəvvür etmək olar, *subyektlər* isə müxtəlif yollarla obyektlərə təsir edən işləyən *proqramlar* hesab edilə bilər. İnformasiya emalının təhlükəsizliyinin bu cür təsviri təhlükəsizlik siyasətini müəyyən edən qaydalar və məhdudiyyətlər yığımına uyğun olaraq subyektin obyektə çıxışının idarə olunması məsələsini həll et-

məklə təmin edilir. Hesab olunur subyektlərin təhlükəsizlik siyasətinin qaydalarını poza bilməməsi halında sistem etibarlıdır. Beləliklə, bütün modellər üçün ümumi kod, sistemi təşkil edən varlıqlar dəstinin məhz çoxlu sayda *obyekt* və *subyektlərə* bölünməsindən ibarətdir.

2. Sistemdəki bütün qarşılıqlı əlaqə subyektlər və obyektlər arasında müəyyən bir tip əlaqələrin qurulması ilə modelləşdirilir. Bu cür əlaqələrin bir çox növü subyektlərin obyektlər üzərində edə biləcəyi əməliyyatlar toplusu olaraq təyin olunur.
3. Subyektlər və obyektlər arasındakı bütün əməliyyatlar təhlükəsizlik siyasətinin qaydalarına uyğun olaraq *qadağan edilir* və ya *icazə verilir*. Bu əməliyyatlara qarşılıqlı əlaqə monitoru tərəfindən nəzarət edilir.
4. Təhlükəsizlik siyasəti *subyektlər* və *obyektlər* arasında bütün qarşılıqlı əlaqələri müəyyən edən qaydalar şəklində verilir. Bu qaydaların pozulmasına səbəb olan qarşılıqlı əlaqə giriş nəzarəti vasitəsi ilə bağlanır və həyata keçirilə bilməz.
5. Subyektlər, obyektlər və onların arasındakı münasibətlər (qurulmuş qarşılıqlı əlaqələr) yığımı *sistemin vəziyyətini* müəyyənləşdirir. Bu vəziyyətlər fəzasında sistemin hər bir vəziyyəti modeldə qəbul edilmiş təhlükəsizlik kriteriyalarına uyğun olaraq ya təhlükəsizdir, ya da təhlükəlidir.
6. Təhlükəsizlik modelinin əsas elementi, bütün qurulmuş qaydalara və məhdudiyyətlərə əməl olunarsa, təhlükəsiz vəziyyətdə olan sistemin təhlükəli vəziyyətə gələ bilməyəcəyinin sübutudur.

Təhlükəsizlik siyasəti modelləri arasında üç əsas tipi seçmək olar:

1. ***Diskresion*** (*ixtiyari*);
2. ***Mandat*** (*normativ*);
3. ***Rol***.

Bu modellərin əsasında,uyğun olaraq girişin diskresion idarəsi (*Discretionary Access Control – **DAC***), girişin mandat idarəsi (*Mandatory Access Control – **MAC***), girişin pol idrəsi (*Role-Based Access Control – **RAC***) durur.

Qeyd edək ki***,*** *diskresion giriş siyasəti* əksər qorunan İS-lərdə tətbiq olunan ən geniş *girişə nəzarət modellərini* əhatə edir və tarixən nəzəri və praktik baxımdan ilk olaraq hazırlananımışdır. İS-də informasiyaya çıxışın diskresion modellərinə aid ilk işlər hələ ötən əsrin 60-cı illərdə yaranmışdır və ədbiyyatda ətraflı təqdim edilmişdir. Bunlardan ən məşhurları ***ADEPT-50*** modeli (*60-cı illərin sonu*), ***beşölçülü Hartson*** fəzası (*70-ci illərin əvvəlləri*), ***Harrison-Ruzzo-Ulman*** modeli (*70-ci illərin ortaları*), ***Take-Grant*** modelidir (*1976*). Bu modellərin müəllifləri və tədqiqatçıları informasiya sisteminin təhlükəsizlik nəzəriyyəsinə mühüm töhfələr vermiş və onların işləri qorunan informasiya sisteminin sonrakı inkişafının əsasını qoymuşdur.

Təhlükəsizliyin diskresion modellərinə nümunə olaraq **ADEPT-50**,beşölçülü **Hartson** fəzası, giriş matrisinə əsaslanan, **Harison-Ruzzo-Ullman** modellərini, həmçinin **Take-grant** modelini və onun modifikasiyasını göstərə bilərik (şəkil 2).

Qeyd edək ki, diskresion model çərçivəsində subyektlərin (istifadəçilər və ya əlavələr) obyektlərə (müxtəlif informasiya resurslarını: sənədlər, əlavələr, çıxış qurğuları və s.) əlçatanlığı idarə olunur.

Hər bir obyekt üçün obyekt sahibi olanlar mövcuddur ki, obyektə kimlərin əlçatan olmalarını və icazə verilən çıxış əməliyyatlarını onların özləri müəyyən edır. Əsas giriş əməliyyatları READ (*oxumaq*), WRITE (*yazmaq*) və EXECUTE (icra etmək , bu yalnız proqramlar üçün məna daşıyır). Beləliklə, diskresion giriş modelində hər bir *subyekt-obyekt* cütlüyü üçün icazə verilən giriş əməliyyatları dəsti qurulur. Xatırladaq k, diskresion model çərçivəsində obyektə çıxış sorğusuna cavab olaraq, sistem obyektin giriş hüquqlarının siyahısında subyekt axtarır və sorğu verən subyekt siyahıda olduqda daxil olmağa imkan verir. Əks təqdirdə, subyektin obyektə əlşatanlığına icazə verilmir.

Klassik disresion (*ixtiyari giriş nəzarəti*) sistemi, obyektin əvvəlcə heç kim üçün əlçatan olmaması mənasında "*bağlı*" hesab olunur və icazələrin toplu-su giriş hüquqlarının siyahısında təsvir edilir. Həmçinin "*açıq*" sistemlər də var-dır ki, burada susma prinsipinə görə hər kəsin obyektə tam əlçatanlıq hüququ vardır, çıxış hüquqları siyahısında isə məhdudiyyətlər toplusu təsvir edilir. Belə model Windows və Linix əməliyyat sistemlərində realizə olunur.

Xüsusilə, Linix əməliyyat sistemində hər bir fayl üçün (bu əməliyyat sistemində bütün resurslar giriş - çıxış qurğuları da daxil olmaqla *fayllar* şəklində təmsil olunur), üç kateqoriya subyekt üçün giriş icazələri qurulur: faylın sahibi, onun kimi eyni qrupun üzvləri və bütüb digər istifadəçilər. Bu üç kateqoriya subyektin hər biri üçün oxumaq (**r**), yazmaq (**w**) və yerinə yetirmək (**x**) hüququ qurulur. Məsələn, " **rwxr-xr--** " yazısı onu bildirir ki, faylın sahibi faylla nə lazımdırsa edə bilər, onun qrupunun üzvləri faylı oxuya və yerinə yetirə bilər, lakin yaza bilməzlər, digər istifadəçilər isə yalnız oxuya bilərlər.

Qeyd etmək vacibdir ki, diskresion modellin çatışmamazlığı ondan ibarətdir ki, informasiyanı oxumaq hüququ olan *subyekt*, obyekt sahibinin *razılığı olmadan* informasiyanı onu oxumaq hüququ olmayan başqa bir *subyektə* verə bilər. Odur ki, informasiyanın ona əlçatanlığı olmayan subyekt üçün əlçatan ola bilməyəcəyinə zəmanət yoxdur. Bundan başqa, heç də bütün avtomatlaşdırılmış informasiya sistemlərində hər bir obyek üçün obyekt sahibini təyin etmək olmur-(əksər hallarda verilənlər ayrıca subyektlərə deyil, bütün sistemə məxsus olur).

1. Təhlükəsizliyin ilk *diskresion* modellərindən olan ***ADEPT-50*** modelində təhlükəsizliyə aid olan dörd tip obyektə baxılır: istifadəçi (***U***), tapşırıq (***J***), terminal (***T***) və fayl (***F***) . Bu yanaşma, bircins olmayan bir sıra proqramlar və məlumatlar, fayllar, istifadəçilər və terminallar üzərində giriş hüquqlarına vahid nəzarəti təmin edir [24]. Modeldə təhlükəsizlik obyektlərinin hər biri təhlükəsizlik vektoru ilə təsvir edilir. Vektora 4 komponent daxildir:

- əvvəlcədən göstərilən *sərişt*ə*lik*;
- *kateqoriya* fayllar üçün istifadə olunur;

- icazələr;
- giriş növlərinin yığımı.

Bu yanaşma, bircins olmayan bir sıra proqramlar və məlumatlar, fayllar, istifadəçilər və terminallar üzərində giriş hüquqlarına vahid nəzarəti təmin edir. ***ADEPT-50*** modeli ilk *mülahizəli təhlükəsizlik siyasəti* modellərindən biridir.

Modeldə aşağıdakılara baxılır:

- kompüter sisteminin $\boldsymbol{O = [o_j], j = 1,\dots n}$ obyektlər çoxluğu;
- kompüter sisteminin $\boldsymbol{S = [s_j], i = 1,\dots m}$ subyektlər çoxluğu;
- subyektlərin obyektlərə $\boldsymbol{R = [r_g], g = 1,\dots k}$ giriş hüquqları çoxluğu;
- kompüter sistemində yerinə yetirilən $\boldsymbol{E = [e_l], l = 1,\dots q}$ proseslərinin aid olduqları predmet sahələrinin siyahısından ibarət çoxluq;
- subyektlərin və obyektlərin təhlükəsizlik kateqoriyalarından ibarət $\boldsymbol{D = [d_x], x = 1,\dots v}$ çoxluğu.

Kompüter sisteminin subyektləri aşağıdakılarla xarakterizə olunur:

- aid olduqları mövzu sahəsi
- onlara verilmiş hüquqlar
- onlara verilən təhlükəsizlik kateqoriyası.

Kompüter sisteminin obyektləri aşağıdakılarla xarakterizə olunur:

- aid olduqları mövzu sahəsi
- onlara verilən təhlükəsizlik kateqoriyası.

2.*Hartsonun* beşölçülü fəzasının adı əsas yığmların – *qərarlaşmış səlahiyyətlər* (***A***), *istifadəçilər* (***U***), *əməliyyatlar* (***E***), *resurslar* (***R***), *sistemin vəziyyəti* (***S***) sayına uyğun olaraq adlandırılmışdır (bax.[18], səh. 50-53). ***Hartson*** tərəfindən təklif olunan *diskresion giriş modeli*, ehtimal ki, ən aydın şəkildə formal olaraq, relasyon cəbr dilində ifadə olunan *girişə nəzarətinin diskresiyon prinsipini* göstərir.

Bu modeldəki təhlükəsizlik oblastı həmin yığımların

$$\boldsymbol{A \times U \times E \times R \times S}$$

Dekart[1]hasili kimi təqdim olunur. Bu halda giriş olaraq istifadəçilər tərəfindən sistem resursları üzərində hər hansı bir əməliyyatı yerinə yetirən üçün daxil olan müraciətlər sayılır.

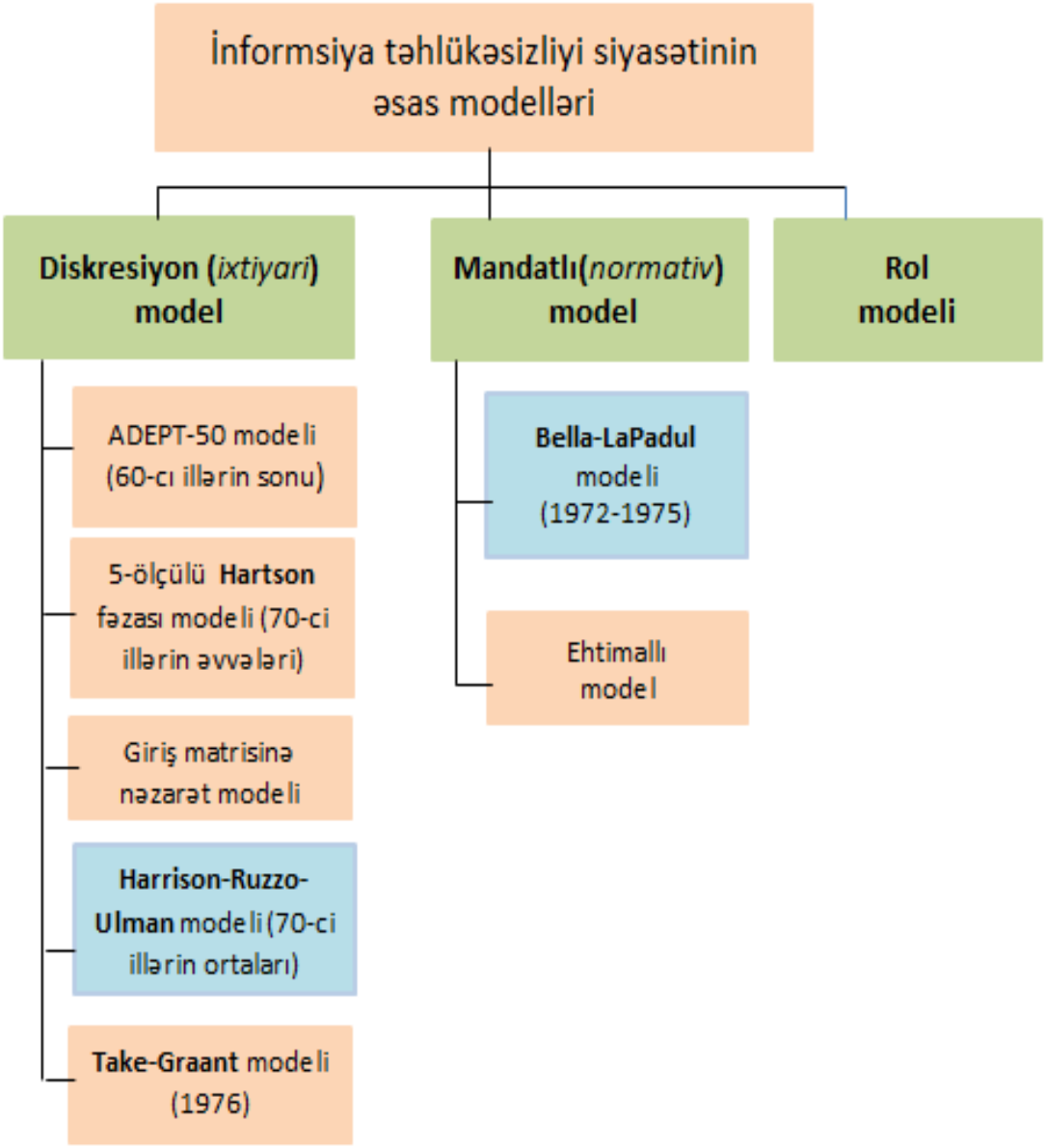
İstifadəçilər, resursa çıxış əldə etmələri üçün sorğu göndərirlər ki, bunun yerinə yetirilməsi nəticəsində sistem yeni vəziyyətə keçir. Giriş üçün sorğu

$$\boldsymbol{q = (u, e, R^1, s)}$$

dördlüyü ilə təqdim olunur, burada $\boldsymbol{u \in U,\ e \in E, s \in S, R^1 \subseteq R,}$ ($\boldsymbol{R^1 -}$ tələb olunan resurslar yığımıdır). Göründüyü kimi, girişə sorğu tələbi, təhlükəsizlik sahəsinin dörd ölçülü proyeksiyasının alt fəzasıdır. Sorğu, təhlükəsizlik oblastında olarsa yerinə yetirilir.

Girişin təşkili prosesinin alqoritmik olaraq təsvir [18] - də verilmişdir. Alqoritminin çox vaxt aparması səbəbindən, **Hartson** təhlükəsizlik modeli, giriş matrisinə əsaslanan modeldən fərqli olaraq praktikada geniş tətbiq olunmur.

Qeyd edək ki, bütün əyaniliyinə baxmayaraq ***Hartson*** modeli bir əhəmiyətli çatışmamazlığfa malikdir – bu model əsasında sitemin təhlükəsizliyi sübuta yetirilməyib. İstifadəçilər resurslara qanuni çıxış etməklə sistemin vəziyyətini, o cümlədən $\boldsymbol{R}$ resurlar çoxluğunu dəyişə bilər. Beləliklə, təhlükəsizlik oblastının özü də dəyişə bilər. Bu halda sistemin təhlükəsizliyi saxlanılırmı? Modelin bu suala cavabı yoxdur.



Şəkil 2. İS-nin əsas təhlükəsizik modelləri.

3.*Giriş matrisinə əsaslanan diskresyon modellər* nəzəri və praktiki olaraq ən böyük inkişaf və tətbiq əldə etmişdir. Bu modellərdə təhlükəsiz çıxış oblastı düzbucaqlı matris (cədvəl) kimi qurulur, ki onun sətirləri giriş subyektinə, sütunları isə giriş obyektinə uyğundur.

Şəkil 3-də təsvir olunmuş cədvəldə w – obyekti qeyd olunmasını, r – obyektin oxunmasını, e –isə obyektə buraxılmanı ifadə edir. Cədvəlin oyuqlarında göstərilən yazılanlar uyğun subyektin uyğun obyektə təhlükəsiz girişini müəy-

yən edir. Giriş hüququnun bü cür əks olnması beşölçülü Hartson fəzasından fərqli olaraq daha çox münasibdir. Cədvəl baxılan kompüter sistemində girişə nəzarət qaydaları siyasəti barədə bütün zəruri informasiyaları özünə daxil edir.

	O_1	O_2	...	O_j	...	O_N
S_1		w				
S_2	r					
...						
S_i				r,w		
...						
S_M						e

Şəkil 3. Giriş matrisi cədvəli

4.Harison-Ruzzo-Ullman modeli yüksək qorunan avtomatlaşdırılmış sistemlərdə rəsmi yoxlama üçün istifadə olunur. Onun, giriş matrisinin nəzarət metodunda olduğu kimi, bir çox giriş obyektləri və subyektləri vardır. Bu halda, subyektin hüququ varsa, o, obyektlər üzərində aşağıdakı əməliyyatları həyata keçirə bilər:

1. obyekt üzərində subyektə yeni bir hüququn əlavə edilməsi;
2. obyekt üzərində subyektin hüquqlarının aradan qaldırılması;
3. yeni bir subyektin yaradılması;
4. yeni bir obyektin yaradılması;
5. subyektin çıxarılması;

6. obyekti silmək.

Bu modelin üstünlükləri onun sadəliyində, səmərəliliyində və yüksək səviyyədə təhlükəsiz olmasındadır. Yəni, bu alqoritmin reallaşdırılması üçün subyektlərin obyektlər üzərində mürəkkəb əməliyyat mexanizlmərini bilməsi vacib deyil, belə ki, istifadəçi hüquqlarının idarə olunması bilavasitə subyektlərin hüquqlarının təsvir olunduğu giriş matrisində həyata keçirilir. Bu hüquqlar çox çevik ola bilər.

Belə sistemlərin çatışmamazlığı onların hər birinin təhlükəsizliyin yoxlanılması üçün öz alqoritmini tələb etməsidir. Bundan əlavə, bu model trojan atları[1] üçün olduqca həssas hesab olunur, çünki subyektlər arasında verilənlər axınının yoxlanılması yoxdur.

5.**Take-Grant** modelinin əsası olaraq qraf anlayışından istifadə edir. Bu mo-del 1976-cı ildə Conson, Lipton və Şnayder tərəfindən təklif olunmuşdur. Xa-tırladaq ki, qraf, təpələri və tilləri olan bir obyektdir. Bu modeldə təpələr olaraq ya obyektlərdən, ya da subyektlərdən istifadə olunur. Qeyd edək ki, kompüter sistemlərinin take-grant təhlükəsizlik modelindən istifadə etməklə, subyektlərin hüquqları dəyişdikdə sistemin vəziyyətinin necə dəyişdiyini müəyyənləşdirmək olur. Bu modeldən ixtiyari girişə nəzarət sistemlərini təhlil etmək üçün, ilk növbədə bu sistemlərdə giriş hüquqlarının paylanması yollarını təhlil etmək üçün istifadə olunur.

Modelin əsas elementləri olaraq *əlçatanlıq qrafından* və onun *çevrilməsi qaydalarından* istifadə olunur. ***Take-Grant*** modelinin məqsədi sitemin subyektinin vəziyyəti əlçatanlıq qrafı ilə təsvir olunan obyektə əlçatanlıq hüququnun alınmasının mümükünlüyü ilə bağlı *suala cavab verməkdən* ibarətdir.

---

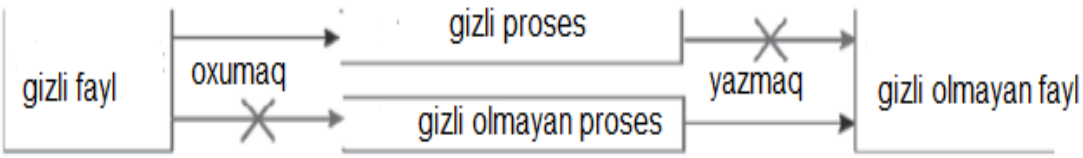
[1] ***Trojan atı*** - icrası təhlükəsizlik sisteminin fəaliyyətini pozan gizli və ya açıq proqram kodu olan bir proqram. Trojan atları məlumatları və ya faylları açmaq, dəyişdirmək və ya məhv etmək qabiliyyətinə malikdir. Bunlar geniş istifadə olunan proqramlarda, məsələn, şəbəkə xidməti proqramlarında, elektron poçtlarda quraşdırılmışdır.

Modelin formal təsvirinndə onun müəllifləri aşağıdakı işarələmələrdən istifdə etmişdir:

1. $\boldsymbol{O}$ – obyektlər çoxluğu (məsələn, fayl və ya yaddaşın seqmenti);
2. $\boldsymbol{S} \subseteq \boldsymbol{O}$ –aktiv obyekt-subyektlər çoxluğu (məsələn, istifadəçi və ya proses);
3. $\boldsymbol{R} = \{\boldsymbol{r_1}, \boldsymbol{r_2}, \dots, \boldsymbol{r_m}\} \cup \{\boldsymbol{t}, \boldsymbol{g}\}$ –giriş hüquqları çoxluğu, burada $\boldsymbol{t}$ (take)-çıxış almaq hüququ, $\boldsymbol{g}$ (grant)- çıxış vermək hüququdur;
4. $\boldsymbol{G} = (\boldsymbol{S}, \boldsymbol{O}, \boldsymbol{E})$ –... sonlu qrafdır ki, sistemə çarı əlçatanlığı təsvir edir;
5. $\boldsymbol{S}, \boldsymbol{O}$ –qrafın təpələrinə uyğun çoxluqlardır,$\boldsymbol{E} \subseteq \boldsymbol{O} \times \boldsymbol{O} \times \boldsymbol{R}$ –çoxluğu-nun elementləri qraf qövsüdür ki, $\boldsymbol{R}$ giriş hüquqları çoxluğunun boş ol-mayan hissəsilə işarə ounur.

Sistemin vəziyyəti giriş qrafı ilə təsvir olunur. Sistemin bir vəziyyətdən digər vəziyyətə keçidi, giriş qrafını dəyişdirilməsi əməliyyatları və ya qaydaları ilə müəyyən edilir.

6.Yuxarıda adları çəkilən bu moellərdən başqa təhlükəsizliyin ***Bella-LaPadul*** *mandatlı* modeli də vardır. Bu model hələ 1972-1975-ci illərdə amerikalı mütəxəssislər – ***Devid Bell*** və ***Leonard LaPadul*** (D. Elliott Bell, Leonard J. LaPadula**)** tərəfindən işlənmışdir və kompüter təhlükəsizliyi nəzəriyyəsinin inkişafında böyük motodoloji rol oynamışdır. Təhlükəsizliyin bu modelində girişə nəzarətlə bağlı bir çox anlayışların – subyektlərin, obyektlərin və giriş əməliyyatının tərifləri, həmçinin onların təsviri üçün riyazi aparat verilmişdir. Bu model əsasən iki əsas təhlükəsizlik qaydaları ilə tanınır: biri *oxumağa*, digəri isə məlumat *yazmağa* aiddir (şəkil 4).



Şəkil 4. Bella-LaPadul modeli

Tutaq ki, sistemin iki növdə verilənləri (fayllara) vardır: *gizli* və *gizlədilməmiş* və bu sistemin istifadəçiləri də iki kateqoriyaya mənsubdur: gizlədilməmış verilənlərə giriş səviyyəli (*gizlədilməmiş*) və gizli verilənlərə giriş səviyyəli (*gizli*). Model,şəkil 4-dən də göründüyü kimi, aşağıdakıqaydalara əsaslanır:

1. *Sadə təhlükəsizliyin xassəsi*: gizli olmayan istifadəçi (və ya onun adından başlanan bir əməliyyat) gizli fayldan verilənləri oxuya bilməz.
2. *Mürəkkəb təhlükəsizliyin xassəsi*: gizli məlumatlara girmə səviyyəsi olan istifadəçi məlumatları dizlədilməmış fayla yaza bilməz.

Bu təsvir edilən xassələrə görə, əgər gizli məlumatlara girmə səviyyəsi olan bir istifadəçi bu məlumatları adi bir sənədə (səhvən və ya zərərli məqsədlə) kopyalayarsa, istənilən "*gizli olmayan*" istifadəçi üçün əlçatan olacaqdır. Bun-dan başqa, sistemdə gizli fayllarla aparılan əməliyyatlara məhdudiyyətlər qoyula bilər (*məsələn, bu faylların başqa bir kompüterə köçürülməsi, elektron poçtla göndərilməsi və s*.). İkinci təhlükəsizlik qaydası, bu faylların (və ya sadəcə onların içindəki məlumatların) heç vaxt təsnif olunmayacağına və bu məhdudiyyətləri "*aşmayacağına*" zəmanət verir. Bu səbəbdən, bir virus, məsələn, həssas məlumatları oğurlaya bilməz.

Baxılan bu qaydalar sistemdə məlumatlara ikidən çox girmə səviyyəsi zərurəyi yaranan hallar üçün, məsələn, *gizli olmayan, konfidensial, gizli* və *tamamilə gizli* halları üçün ümumiləşdirmək asandır. Bu halda gizli məlumatlara girmə səviyyəsi olan bir istifadəçi *gizli olmayan, konfidensial* və *gizli* sənədləri ***oxuya*** , *gizli* və *tamamilə gizli* sənədləri isə yalnız ***yarada*** bilər. Beləliklə, yuxarıda təsvir edilən qaydalar bunu deməyə əsas verir ki, nəzəri olaraq istifadəçilər oxumaq hüququ olmayan sənədlər yarada bilərlər.

Bella-LaPadula modeli kompüterlərə tətbiq olunan ilk əhəmiyyətli təhlükəsizlik siyasət modeli olmuşdur və hələ də *hərbi sənayedə* dəyişdirilmiş formada tətbiq edilir. Model tam riyazi şəkildə rəsmiləşdirilib.

Bella-La Padull modeli kompüter təhlükəsizliyi nəzəriyyəsinin inkişafında böyük rol oynamışdır, və onun müddəaları təhlükəsizliyi təmin edən kompüter sistemlərinin standartlarında, xüsusən də məşhur "Narıncı Kitab" da (1983), dövlət sirri olan məlumatları emal edən sistemlərdə məcburi tələb kimi təqdim edilmişdir. *Bella-La Padull* modelinin bir güclü tərəfi ”***troyan***” proqramı probleminin avtomatik olaraq həll edilməsindən ibarətdir. Giriş matrisinə görə girişinə icazə olmayan obyektə ”*troyan*” proqramının köməyilə informasiyanın ötürülməsi prosesi, bütün digər informasiya axınlarında olduğu kimi, xüsusi prinsipilə həyata keçirilir. Beləliklə, informasiyanın belə ötürülməsi baş verməzsə, sistem təhlükəsiz vəziyyətdə qalır.

Hal hazırda məlumatların təhlükəsizliyinin ən çox yayılan iki klassik baza modelindən – ***mülahizəli*** (diskresion) və ***etimadnamə*** (mandatlı) modellərindən istifadə olunur. Yuxarıda qeyd olunduğu kimi, bu modellərin əsasını, uyğun olaraq, girişin *diskresiyon* (ixtiyari) idarə olunması və girişin *mandatlı* (normativ) idərə olunması təşkil edir.

Qeyd edək ki, ***diskresion model,*** *çərçivəsində* ***subyektin*** (məsələn, istifadəçinin) ***obyektə*** (fayllar, əlavələr, daxil etmə qurğuları və s. kimi informasiya resursları) çıxışına nəzarət edilir.

Hər bir *obyekt üçün* obyektə çıxışının olmasını, həmçinin icazə verilən çıxış əməliyyatlarını müəyyən edən *sahibkar-subyekt* var. Əsas giriş əməliyyatları bunlardır: *READ* (oxumq), *WRITE* (запись) и *EXECUTE* (yalnız proqram üçün əhəmiyyətli olan yerinə yetirilmə). Beləliklə, diskresion giriş modelində hər bir *subyekt-obyekt* cütü üçün icazə verilən giriş əməliyyatları yığımı qurulur.

Subyektin obyektə giriş sorğusuna cavab olaraq, sistem *subyekti* obyektin giriş hüquqları siyahısında axtarır və subyekt siyahıda olduqda girişə icazə verir. Əks təqdirdə, girişə icazə verilmir.

Girişə nəzarətin klassik diskresion sistemi, obyektin əvvəlcə heç kim üçün əlçatan olmaması mənasında “*qapalıdır*”, və *icazələrin yığımı* giriş hüquqları-nın siyahısında təsvir edilmişdir. Bununla yanaşı, hamıya obyektlərə tam giriş imkanı

olan, və giriş siyahısında isə məhdudiyyətlər toplusu təsvir olunan "*açıq*" sistemlər də mövcuddur. Belə model *Windows* və *Linux* əməliyyat sistemlərində realizə olunmuşdur.

Qeyd edək ki, giriş modelinin çatışmamağlığı informasiyanı oxumaq hüququ olan subyektin obyekt sahibi bilmədən onu oxumaq hüququ olmayan başqa subyektə verə bilməsidir. Beləliklə, informasiyaya əl çatanlığı olmayan subyektin informasiyaya çıxışının olmamasına zəmanət yoxdur.

Mandatlı siyasətinin inkişafına ilkin təkan, ehtimal ki, giriş hüquqlarınına nəzarət ilə bağlı problemlər, və xüsusən ixtiyari diskresion giriş sistemlərindəki "***troyan***" proqramları problemi ilə əlaqədardır. Diskresional modellərin əsas probleminin *informasiya axını üzərində nəzarətin olmamasında olduğunu* dərk edən *tədqiqatçılar* və diskresion siyasət *tənqidçiləri* bu problemlərin gizli uçotda necə həll edildiyini analiz etmişdilər.

Qeyd edək ki, bu təhlükəsizlik meyarı əslində təhlükəli və qəbuledilməz kimi izah olunan müəyyən informasiya axınının qadağan olunması deməkdir. Bundan əlavə, işçilərin gizli sənədlərlə işləmək icazələrinin təyin edilməsi, dəyişdirilməsi, məhrumiyyətlər və s., sənədlərin yaradılması, məhv edilməsi, gizlilik möhürlərinin verilməsi və ya dəyişdirilməsi qaydaları, həmçinin gizli sənədlərlə işin digər xüsusiyyətləri araşdırılmışdır. Xüsusilə qeyd edildi ki, sənədlərə giriş əldə etmək qaydaları onlarla işləmək xarakterindən asılı olaraq dəyişir – öyrənmək (oxumaq) və ya dəyişdirmək (yaratmaq, silmək, əlavələr etmək, redaktə etmək, yəni onlara yazmaq).

Diskresion və *mandatlı* modellər aşağıdakılara əsaslanır:

1. Avtomatlaşdırılmış sistem qarşılıqlı fəaliyyət göstərən qurumlar – ***subyektlər*** və ***obyektlər*** yığımıdır. *Obyektlər*, məlumatları özündə cəmləşdirən qurumlar şəklində təqdim edilə bilər, *subyektlər* isə müxtəlif yollarla *obyektlərə* təsir edən proseslər və ya şəxs hesab oluna bilər.
2. Məlumatların emalının təhlükəsizliyi verilmiş qaydalar və məhdudiyyətlər yığımına uyğun olaraq subyektlərin obyektlərə çıxışının idarə

olunması məsələsini həll etməklə təmin olunur. Bu halda müxtəlif modellərdə "*obyekt*" və "*subyekt*" anlayışlarının tərifləri əhəmiyyətli dərəcədə fərqlənir.

3. Sistemdəki bütün qarşılıqlı əlaqələr subyekt və obyektlər arasında müəyyən tip mühasibətlərin bərqərar olunmasıyla modelləşir. Münasibətlər tipindən ibarət olan çoxluq subyektlərin obyektlər üzərində apara biləcəyi əməliyyatlar toplusu kimi təyin olunur.
4. *Subyekt, obyekt* və onlar arasındakı *münasibətlər* yığımı (müəyyən olunmuş əlaqə) sistemin *vəziyyətini* təyin edir.

Təhlükəsizliyin ***Harrison-Ruzzo-Ulman*** (***HRU***) modeli klassik *diskresion* model hesab olunur. ***HRU modeli*** ilk dəfə 1971-ci ildə təklif olunmuşdur və formal olaraq 1976-cı ildə yaranmışdır. Bu model subyektlərin obyektə çıxışının ***istənilən*** idarəsini reallaşdırır və çıxış hüququnun yayılmasına nəzarəti realizə edir. Bu model çərçivəsində informasiyanın emalı informasiyaya çıxışı təmin edən aktib qurumun – *subyektlərin* (***S*** çoxluğu), qorunan informasiyadan ibarət olan passiv qurumun – *obyektlərin* (***O*** çoxluğu) və uyğun əməliyyatların (məsələn, *oxuma, yazma, yerinə yetirilmə*) yerinə yetirilməsinə səlahiyyəti ifadə edən *çıxış hüququnun* sonlu

$$\boldsymbol{R = \{r_1, r_2, \dots, r_n\}}$$

çoxluğu kimi təsvir edilir.

Modelin və subyektlər arasında münasibətin işə salınması üçün fərz olunur ki, bütün subyektlər eyni zamanda həm də obyektdirlər. Sistemin özünü necə aparması "*vəziyyət*" anlayışına əsasən modelləşir. Sistemin vəziyyətlər fəzası sistemin obyektlərinin, subyektlərinin və çıxış hüququnun çoxluqlarının dekart hasili ilə yaradılır: $\boldsymbol{O \times S \times R}$. Bu fəzada $\boldsymbol{Q}$ sisteminin cari vəziyyəti *subyektlər* çoxluğundan, *obyektlər* çoxluğundan və subyektlərin obyektə cari çıxış hüququnu təsvir eən ***M*** *çıxış hüququ matrisindən* ibarət olan $\boldsymbol{Q = (S, O, M)}$ üçlüyü ilə ilə təyin olunur. Adətən matrisin *sətirlərinin* subyektlərə, *sütunlarının* isə obyektlərə

uyğun olması qəbul edilir. Obyektlər çoxluğu özünə həm də subyektlər çoxluğunu daxil etdiyindən matris düzbucaqlı farmasındadır. $\boldsymbol{M[s,o]}$ matrisinin elementi $\boldsymbol{s}$ subyektin $\boldsymbol{o}$ obyektinə çıxış hüququ yığımından ibarətdir ki, $\boldsymbol{R}$ çıxış hüqüqları çoxluğuna daxildir. Sistemin zamana görə vəziyyəti müxtəlif vəziyyətlərə keçidlə modelləşir.

Real İS-nin təhlükəsizlik sistemlərində klassik mülahizə modelinin tətbiqini məhdudlaşdıran əsas problem *"**troyan**"* proqramının təsirindən *formal müdafiənin mümükün olmamasından* ibarətdir. *"**Troyan**"* proqramı dedikdə istifadəçidən gizli olaraq *sənədləşməmiş* və adətən *destruktiv funksiyaların* yerinə yetirilməsini həyata keçirən proqram başa düşülür. Təcavüzkar *"**troyan**"* proqramını hər hansı bir istifadəçinin proqram təminatına tətbiq edərkən informasiya ***həmin istifadəçinin çıxışı olan obyektdən təcavüzkarın çıxışı olan obyektə keçir*** və formal olaraq mülahizə siyasətinin heç bir qaydası *pozulmur*, amma məlumatın *icazəsiz ötürülməsi baş verir*.

Qeyd edək ki,nəzarətin *diskresion* olması kimlərin obyektə girişinin olmasını və onların giriş növlərini obyekt sahibinin özü tərəfindən müəyyən olmasını bildirir. Diskresion modelin çevikliyionun onun çoxsaylı sistem və əlavələrdə istifadə olunmasına imkan verir. Bunun sayəsində bu metod, xüsusilə də kommersiya əlavələrində, geniş yayaılmışdır. Diskresion nəzarətin istifadəsinin *Windows NT/2k/XP* sistemləridir.

Diskresion modelin, yuxarıda qeyd olunduğu kimi, əhəmiyyətli çatışmamazlığı vardır. Bu, onun informasiya əldə etmək imkanı olmayan *subyektiə* informasiya verilməyəcəyinə *tam zəmanət verməməsilə* əlaqədardır.

Diskresion modelə aid edilən digər bir şatışmamazlıq da sistemdəki bütün obyektlərin, başqalarının bu obyektlərin əl çatanlığına imkan verən subyektlərə aid olmasıdından ibarətdir. Praktikada məlum olur ki, əksər hallarda sistemdəki verilnlər ayrı-ayrı şəxslərə deyil, bütün sistemə aiddir. Belə sistemlərin ən ümumi nümunəsi informasiya sistemidir.

Qeyd etmək lazımdır ki, qorunan sistemlərin qurulması praktikası baxımından, ***Harrison - Ruzzo - Ullman*** modeli idarə etmək üçün ən asan və səmərəlidir, çünki heç bir mürəkkəb alqoritm tələb etmir ki, bu da müasir sistemlər arasında onun yayılması izah olunur. Bundan əlavə, bu modeldə təklif olunan təhlükəsizlik meyarı praktik cəhətdən çox güclüdür, çünki əvvəlcə müvafiq səlahiyyət verilməmiş istifadəçilər üçün müəyyən məlumatların əlçatmazlığına zəmanət verir. Bununla belə, ***Harrison, Ruzzo*** və ***Ulman*** sübut etmişdirlər ki, ümumi halda ixtiyari bir sistem üçün, onun ilkin $\boldsymbol{Q_0 = (S_0, O_0, M_0}$)vəziyyətinin və ümumi $\boldsymbol{r}$ hüquqlarının bu konfiqurasiyanın təhlükəsiz olub-olmamasına qərar verə biləcək bir alqoritmi yoxdur.

Bundan əlavə, bütün girişə nəzarətin ixtiyarı modelları, bir qayda olaraq, "***Trojan atı***"nının hücumlarına həssasdırlar, çünki diskresion modellər sub-yektlər arasında informasiya axınlarına deyil, yalnız subyektlərin obyektlərə da-xil olma əməliyyatlara nəzarət edir. Başqa sözlə, təcavüzkar "troyan″proqra-mını hər hansı bir istfvadəçinin proqram təminatında xəlvəti olaraq yerləşdir-dikdə bu proqram informasiyanı istifadəçi üçün əlçatan obyekdən təçavüzkar üçün əl çatan olduğu obyektə keçirir və formal olaraq təhlükəsizliyin diskresion siyasətinin heç bir qaydası pozulmur, bununla belə informasiya itkisi baş verir.

Çıxışın idarə olunmasının ***mandat modeli*** bir çox ölkələrin dövlət müəssisələrində *gizli sənəd dövriyyəsi* qaydalarına əsaslanır. Real praktikadan götürülən modelin əsas cəhəti qorunan ***məlumatın*** və *təhlükəsizlik səviyyəsi* adlanan "*məxfi*", "*gizli*" və s. kimi xüsusi nişanlar daxil edilmiş ***sənədlərin*** işlənməsi prosesinə bütün iştirakçıların cəlb olunmasıdır. Bütün təhlükəsizlik səviyyələri müəyyən olunmuş dominantlıq münasibətinin köməyilə nizamlanır. Məsələn, "*gizli*" səviyyəsi "*məxfi*" səviyyədən yüksək hesab olunur və onun üzərində dominantlıq edir. Çıxışa nəzarət, qarşılıqlı əlaqədə olan tərəflərin təhlükəsizlik səviyyəsindən asılı olaqar aşağıda təsvir edilən iki sadə qayda əsasında həyata keçirilir:

1. *səlahiyyətli subyek* yalnız o sənədləri oxumaq hüququn malikdir ki, hə-

min sənədlərin təhlükəsizliyi onun şəxsi təhlüksizliyindən böyük olmasın;

2. *səlahiyyətli subyek* yalnız məlumatları o sənədlərə daxil edə bilərki, həmin sənədlərin təhlükəsizliyi onun şəxsi təhlüksizliyindən kiçik olmasın.

Birinci qayda daha etibarlı (*yüksək səviyyəli*) qurumlar tərəfindən işlənmiş məlumatların az etibarlı (*aşağı səviyyəli*) qurumlar tərəfindən əldə edilməsindən qoruyur. İkinci qayda, məlumatların işlənməsi prosesinin yüksək səviyyəli iştirakçılarından *informasiyanın* aşağı səviyyəli iştirakçılara ötürülməsinin (*şüurlu və ya şüursuz*) qarşısını alır.

Beləliklə, əgər *mülahizəli modellərdə* giriş nəzarəti subyektlərə müəyyən obyektlər üzərində müəyyən əməliyyatlar aparmaq səlahiyyətini verməklə baş verirsə, *mandat modelləri* daxil olmaları bütün icazə verilən qarşılıqlı əlaqələri müəyyən edən sistem təhlükəsizlik səviyyələrinin bütün subyektlərinə həvalə edərək həyata keçirilir. Odur ki, çıxışın *mandatlı idarəi* təhlükəsizlik səviyyələri eyni olan və qarşılıqlı əlaqələrinə heç bir məhdudiyyət qoyulmayan qurumları fərqləndirmir. Ona görə çıxışın idarəsi *daha çevik yanaşma* tələb etdikdə *mandatlı model* hansısa *mülafizəli modellə* birgə tətbiq edilir. Bu halda *mülahizəli modeldən* eyni səviyyəli qurumlar arasındakı qarşılıqlı əlaqələrə nəzarət etmək və *mandatlı modeli gücləndirən* əlavə məhdudiyyətlər qoymaq üçün istifadə olunur.

Təhlükəsizliyin ***mandat modelində*** sistem $\boldsymbol{S}$ subyektlər, $\boldsymbol{O}$ (*obyektlər çoxluğu subyektlər çoxluğunu özünə daxil edir* $\boldsymbol{S} \subset \boldsymbol{O}$) obyektlər və çıxış hüququ *read* (*oxumaq*) və *write* (*yazmaq*) çoxluqları şəklində təsvir olunur. Mandat modelində, adətən yalnız *iki növ* çıxış nəzərə alınır. Çevik çıxışa nəzarət etməyə imkan verməyən belə sərt bir yanaşmanın istifadə olunması, *mandat modelinin* subyektın obyekt üzərində həyata keçirdiyi əməliyyatlara nəzarət etməməsi, məlumat axınının isə ancaq iki növ - ya subyektdən obyektə (*yazı*), ya da obyektdən obyekt (*oxu*) olmas ilə izah olunur.

Subyekt və obyektlərin təhlükəsizlik səviyyəsi $\boldsymbol{F}: \boldsymbol{S} \cup \boldsymbol{O} \rightarrow \boldsymbol{L}$ *təhlükəsizlik səviyyəsi funksiyasının* köməyilə verilir. Bu funksiya uyğun olaraq hər bir *ob-*

yekt və *subyektə* qarşı ***L*** təhlükəsizlik səviyyəsi çoxluğuna daxil olan *təhlükəsizlik səviyyəsini* qoyur.

Mandatlı modelin əsası məxfilikdir. Model təsnifatı dəyişdirmək probleminə məhəl qoymur: dəyişməz olaraq qalan bütün məlumatların gizliliyin müvafiq səviyyəsinə aid olduğu güman edilir. Lakin istifadəçilərin görmək hüququ olmayan verilənlərlə işləməli olduqları hallar olur.

Qeyd edək ki, yuxarıda adları çəkilən təhlükəsizlik siyasətinin əsasını ya *xarici faktorlarla* (diskresion giriş), ya *təhlükəsizlik səviyyəsiylə* (mandatlı giriş), ya da *informasiyanın mövzusuyla* (tematik giriş) təyin olunan münasibətlər təşkil edir.

Bununla belə, müxtəlif təşkilati-idarəedici və təşkilati-texniki sxemlərin analizi göstərir ki, real həyatda müəssisənin və təşkilatın əməkdaşı müəyyən funksional vəzifələri öz adından deyil, müəyyən bir vəzifə daxilində yerinə yetirirlər. Xüsusi pol kimi şərh olunan bir vəzifə, müəyyən bir fəaliyyət növü və işçi mövqeyinin növünü (tabeçilik, hüquq və səlahiyyət) ifadə edən bir mücərrəd, daha doğrusu ümumiləşmiş bir qurumu təmsil edir. Beləliklə, real həyatda, əksər təşkilati və texnoloji sxemlərdə, hüquqlar və səlahiyyətlər müəyyən bir işçiyə şəxsən (birbaşa) verilmir, lakin müəyyən bir vəzifəyə (rola) təyin olunmaqla müəyyən bir hüquq və səlahiyyət dəsti alır.

Həqiqi təşkilati-texnoloji və idarəetmə sxemlərinin *başqa bir istiqaməti*, hüquq və səlahiyyət anlayışlarının, informasiya sistemlərinin fəaliyyət sahəsinin təşkilati - texnoloji proseslərini əks etdirən sistem resursları üzərində müəyyən prosedurlar kimi istifadəsidir. Başqa sözlə, öz vəzifələrində çalışan əməkdaşlara hüquq və səlahiyyətlər resurslar *üzərində elementar əməliyyatlar aparmaq səviyyəsində* (oxumaq, dəyişdirmək, əlavə etmək, silmək, yaratmaq) deyil, məntiqi ümumiləşdirilmiş informasiya emalı prosedurlarının (məsələn, kredit və ya müəyyən büdcələr üzrə debet əməliyyatları) *qruplaşdırlmış elementar əməliyyatları səviyyəsində* verilir.

Beləliklə, müəyyən təşkilati-texnoloji və ya təşkilati-idarəetmə proseslərini avtomatlaşdıran informasiya sistemlərində *giriş nəzarəti siyasəti* informasiya sistemlərinin predmet sahəsində formalaşan ***fəaliyyət-rol münasibətləri*** əsasında qurulmalıdır.

İlk dəfə belə bir yanaşmaya 70-ci illərin sonu - 80-ci illərin əvvəllərində IBM korporasiyasının *giriş nəzarəti* proseslərinin araşdırılmasında baxılmış və ***rol əsaslı*** giriş nəzarəti adlandırılmışdır. 80-ci illərin əvvəllərində ədəbiyyatda həm də **MMS** modeli adı ilə rast gəlinən ***Landver-MakLina*** modeli təqdim edilmişdir. Bu model ***anlayış*** və ***rol*** mexanizmindən istifadə etməklə giriş nəzarətinin *diskresion* və *mandat* prinsiplərini özündə birləşdirmişdir. Bir qədər sonra ***rol əsaslı*** giriş nəzarətinin (*Role-Based Access Control*- **RBAC**) formal ifadələri yarandı.

Rol modellərinin əsasını, qeyd olunduğu kimi, əlavə aktiv kateqoriyaların - *rolların* informasiya sistemlərinin *subyekt - obyekt* modelinə daxil edilməsi təşkil edir. Xatırladaq ki, ***rol dedikdə*** informasiya sistemlərində sistem istifadəçiləri tərəfindən müəyyən funksional vəzifələri yerinə yetirmək üçün zəruri məntiqi əlaqəli səlahiyyətlərə malik aktiv fəaliyyət göstərən *bir qurum* başa düşülür. Rollara nümunə olaraq sistem administratorunu, söbə müdirirni, operatoru, mühasibi, meneceri və s. göstərmək olar.

Diskresion nəzarəti və *mandat* nəzarəti modelləri rol modelindən bir əsaslı fərqə malikdir. Bu fərq ondan ibarətdir ki, bu iki model sistemin *təhlükəsizlik siyasətini* əvvəlcədən müəyyənləşdirir və hər bir konkret vəziyyət üçün konfiqurasiya edir. Bununla belə, *rol* modeli heç bir şəkildə təhlükəsizlik siyasətini əvvəlcədən müəyyənləşdirmir, lakin təşkilatın tələb etdiyi formada onun konfiqurasiya olunmasına imkan verir. Beləliklə, giriş nəzarətinin *rol* modelinə əsaslanan sistemin təhlükəsizlik sisteminin qurulması iki mərhələdə həyata keçirilir:

1. Sistem *təhlükəsizlik siyasətinin* konfiqurasiya edilməsi;
2. Sistemdəki subyektlərə və obyektlərə giriş hüquqlarının müəyyən edilməsi.

Onu da qeyd etmək lazımdır ki, *Rol modeli* əhəmiyyətli dərəcədə yaxşılaşdırılmış *diskresion* modeldir, lakin onu nə ***diskresoin***, nə də ***mandat*** modellərinə aid etmək olmaz, çünki burada girişə nəzarət həm rollar üçün giriş hüquqları *matrisı əsasında*, həm də istifadəçilərin rollarına təyinatı tənzimləyən *qaydalardan* istifadə etməklə həyata keçirilir. Rol modelində klassik subyekt anlayışı *istifadəçi* və *rol* anlayışları ilə əvəz olunur.

Rol modelinin əsas üstünlükləri bunlardır:

1. *İdarəetmənin asanlığı*. diskresion modelindən fərqli olaraq hər bir "obyekt - istifadəçisi" cütü üçün icazələrin təyin edilməsinə ehtiyac yoxdur. Bu-nun əvəzinə, "obyekt - rol" cütləri üçün icazələr qeydiyyata alınır və hər bir isti-fadəçinin rolları müəyyən edilir. İstifadəçinin məsuliyyət sahəsi dəyişdirilərkən sadəcə olaraq onun rolu dəyişir. Rolların iyerarxiyası da həmçinin idarəetmə prosesini də asanlaşdırır.
2. *Ən az imtiyaz prinsipi*. Rol modeli istifadəçiyə sistemdə tələb olunan və-zifələri yerinə yetirmək üçün ən az zəruri olan rolu ilə qeydiyyatdan keçməyə imkan verir. Cari vəzifəni yerinə yetirmək üçün tələb olunmayan səlahiyyətlərin qadağan edilməsi sistemin təhlükəsizlik siyasətini aşmağa imkan vermir.
3. *Vəzifə bölgüsü*. Girişə nəzarətin rol modeli sistem və ya əlavə çərçivəsində istifadəçi imtiyazlarını idarə etmək üçün geniş istifadə olunur. Belə sistemlərin siyahısının tərkibinə Microsoft Active Directory, SELinux, FreeBSD, Solaris, СУБД Oracle, PostgreSQL 8.1, SAP R/3 və digər effektli tətbiq olunan rol modellərini daxil edir.

Sonda qeyd etmək lazımdır ki, girişə nəzarətin rol modeli ilə əlçatanlığın idarə olunmasının diskresion və mandat sistemləri modelləşdirilə bilər.

2.2.İnformasiya sistemlərin təhlükəsizliyinin və etibarliliğinin təmini sisteminin strukturu

İnformasiya sistemləri üçün xarakterik olan proqram həllinin əsasını əməliyyat sistemlərində üst qurum kimi işləyən *verilənlər bazsının idarə etmə sistemləri* (VBİS) təşkil edir. Əlavələrin ixtisaslaşdırılmış serverlərinin yaradıl-ması ilə yanaşı biznes - məntiqin həyata keçirilməsi vasitələri VBİS - də qurulmuşdur. Universal müştərinin (brauzerin) korporativ informasiya infrastrukturuna çıxış üçün vahid bir interfeys kimi istifadəsinə yönəldilmiş diqqət ümumi qəbul edilmişdir.

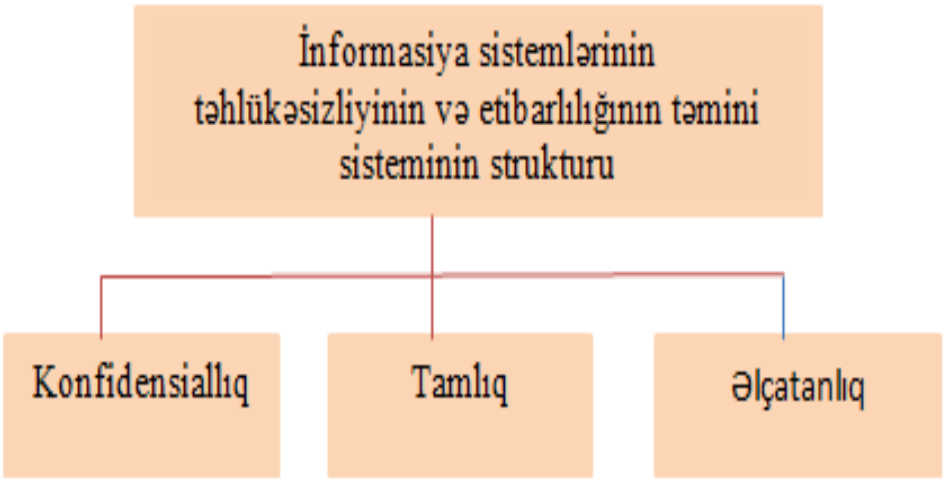
Baza proqram texnologiyalarının inteqrasiyanın *zəruriliyi* və *məqsədəuyğunluğu* ***keyfiyyətin***, ***sürətin*** və korporativ informasiya sistemlərinin komponentlərinin realizəsinin proqram vasitələrinin yüksək etibarlı fəaliyyətini təmin edən ***proqram komplekslərinin*** təhlükəsizliyinin artırılması ilə bağlı yeni tələblərin yaranmasına səbəb olmuşdur. Proqram istehsalçıları və İnternet xidməti təminatçıları istifadəçilərə birbaşa giriş sxemlərini yaratmaq üçün səy göstərdilər.

İnformasiya emalının proqram vasitələrinin və onun çatdırılma vasitələrinin inteqrasiyası İS-nin *təhlükəsizliyini* və *etibarlılığını* təmin etmək üçün proqram kompleksləri sistemlərinin yaradılmasını zəruri etmişdir. İnformasiya təhlükəsizliyi təminatının kompleks sistemi *iqtisadi informasiya sistemlərinin* aşağıda təsvir olunan dörd səviyyəsi üçün xarakterik olan *metod* və *vasitələr* nəzərə alınmaqla qurulmalıdır.

- istifadəçi ilə qarşılıqlı əlaqəyə cavabdeh *tətbiqi proqram təminatı səviyyəsi*;
- informasiya sisteminin verilənlərinin saxlanılmasına və emalına cavabdeh *verilənlər bazasının idarə edilməsi sistemi səviyyəsi*;
- verilənlər bazasının idarə edilməsi sisteminin və digər tətbiqi proqram təminatının fəaliyyətinə cavabeh *əməliyyat sistemləri səviyyəsi;*
- informasiya serverləri və informasiya istifadəçisinin qarşılıqı əlaqəsinə

cavabdeh olan *çatdırılma mühiti səviyyəsi*.

Bütün bu səviyyələrdə müdafiə sistemi effektli fəaliyyət göstərməlidir.



Şəkil 4. İnformasiya sistemlərin təhlükəsizliyinin və etibarlılığının təmini sisteminin strukturu

İS-lərin təhlükəsizliyinin və etibarlılığının təminatı problemi *üç qarşılıqlı əlaqəli məsələnin* həlli kimi təyin oluna bilər (şəkil 4):

1. ***konfidensiallıq*** – istifadəçinin yalnız aşkar və ya qeyri aşkar çıxışına *icazənin* təmin olunması;
2. ***tamlıq*** – informasiyanın və yaxud onun emalı prosesinin nəzərdə tutulmuş və ya tutulmamış dəyişikliklərdən *qorunmasının* təmin olunması;
3. ***əlçatanlıq*** – qəbul edilmiş texnologiyaya uyğun olaraq istifadəçinin avtomatlaşdırılmış formada informasiyaya *əlçatanlığının* təmin olunması.

Bu üç qarşılıqlı əlaqəli məsələnin həll metodu və vasitələri hər bir informasiya sistemi üçün xarakterikdir. Xüsusi halda, qərar qəbuletmə sistemləri üçün ***konfidensiallığın təmin olunması məsələsi*** icazəsi olmayan istifadəçilərin məxfi informasiyalara əlçatanlığının qarşısının alınması üçün kompleks tədbirləri nəzərdə tutur. ***Tamlığın təmin olunması məsələsi*** qəra r qəbuletmə sistemində istifadə olunan informasiyanı icazəsiz olaraq dəyişdirilməsinin və yaxud məhv edilməsinin qarşısının alınması üçün kompleks tədbirləri nəzərdə tutur.

Məlumatlara əlçatanlığın təmin olunması məsələsi, qəbul edilmiş texnologiyaya uyğun olaraq bütün qanuni istifadəçilərin sistem mənbələrinə daxil olmasını dəstəkləyən tədbirlər sistemini nəzərdə tutur.

Konfidensiallığın təmin olunması məsələsinin həlli sistemlə münasibətdə sistemlə qarşılıqlı əlaqədə oln *subyektlərdən* hansının və *hansı* informasiyaya əlçatanlığını müəyyən edən *xarici obyektin olmasına* əsaslanır. Avtomatlaşdırılmış sistemlər üçün xarakterik xüsusiyyətondan ibarətdir ki, müəyyən informasiyaya konkret subyektin əlçatanlığı və ya bunun mümükün olmaması yalnız sistemlə münasibətdə xarici obyekton olması ilə deyil, həm də uyğun tələblərin məntiqi ardıcıllığı ilə müəyyən edilir.

2.3. Təhlükəsizlik və etibarliliq təminatinin təşkilati, texniki və proqram aspekti

İnformasiy sistemlərində verilənlərin təhlükəsizliyinin təmininin *nəzəriyyəsi* və *praktikası* ilə bağlı ilk elmi təqdiqatları hər şeydən əvvəl bütövlükdə təhlükəsizlik probleminin və xüsusilə də informasiya təhlükəsizliyinin xüsusilə əhəmiyyətli olduğu *hərbi sahənin* ehtiyacalarından irəli gəlmişdir. Bu prosesin başlanğıcı XX əsrin 70-ci illərinin sonu və 80-cı illərinin əvvəllərində ABŞ Müdafiə Nazirliyinin kompüter təhlükəsizliyinin milli mərkəzində (*National Computer Securite Center – NCSC)* kompüter informasiyalarının qorunması tədqiqatları ilə qoyulmuşdur. Bu araşdırmaların nəticəsi 1983-cü ildə ABŞ Müdafiə Nazirliyi tərəfindən "**Etibarlı kompüter sistemlərini qiymətləndirmə meyarları**" [Trusted *Computer System Evaluation Criteria* (*TCSEC*). – USA, *Department of* Defense, 5200.28-STD, 1993] adlı sənədin dərc edilməsi oldu, sonradan həmin sənədin örtüyünün rənginə görə "**Narıncı Kitab"** adlandırıldı. Bu sənəd əslində etibarlı kompüter sistemlərinin yaradılması sahəsində *ilk standart* və son-radan məlumatların qorunması meyarlarına uyğun olaraq kompüter sistemləri üçün sertifikatlaşdırma sisteminin təşkili üçün əsas oldu.

1980-cı ilin ikinci yarısında təyinatına görə analoji sənədlər bir sıra avropa ölkələrində də nəşr olundu [*Information Technologe Securite Evaluation Griteria(ITSRC)* Harmonised *Criteria* of France-Germany-Netherlands-United Kingdom. – *Department* of Trade *and Industry*, London, 1991].

"**Narıncı Kitab**"da təqdim olunan qorunan sistemlərin qurulması və analizinə dair yanaşmalar bu sahədə gələcək tədqiqatların aparılması üçün metodoloji və metodik baza olmuşdur. 1991-ci ildə *NCSC* "**Verilənlər bazasının etibarlı idarəetmə sistemi anlayışına tətbiq olunan etibarlı kompüter sistemlərinin qiymətləndirmə meyarlarının şərhi***"* adlı bir sənəd nəşr etdi. Bu sənəd həm də "**Çəhrayı kitab**" adlanırdı. Kitab qorunan VBİS-nin yaradılması və inkişaf etdirilməsi üçün "**Narıncı Kitab**" ın əsas müddialarını konkretləşdirmiş və inkişaf etdirmişdir.

1980-ci illərin sonu - 1990-cı illərin əvvəllərində bir çox ölkələrdə kompüter təhlükəsizliyi problemilə bağlı analoji tədqiqatlar aparıldı və bu sahədə müvafiq milli standartlar yaradıldı. Qonşu Rusiya Federasiyasında Rusiya Federasiyasının Prezidenti yanında Dövlət Texniki Komissiyası (*Dövlət Texniki Komissiyası*) 1992-ci ildə hesablama texnikası vasitələrinin və avtomatlaşdırılmış sistemlərin qurulması tələblərini, metodlarını və standartlarını müəyyən edən "**İnformasiyaya icazəsiz daxil olmaqdan qorunmaq üçün rəhbər sənədlər**" hazırlayıb nəşr etdi.

2012-ci ildə ABŞ-da "**Kompüter cinayətkarlığı və təhlükəsizliyi: problemlər və tendensiyalar**" ("Issues *and* Trends: 2012 CSI/FBI *Computer Cri-me and Security* Survey") adlı illik hesabat nəşr olunmuşdur. Hesabatda kom-puter cinayətkarlığının sayının artması qeyd olunurdu. İnformasiya sistemlərinin işinin pozulmasını 28% xarıcı təcavüzkarlar etmişdir. İnternet vasitəsilə hücum 77% olmuşdur ki, bunun da 59%-ini şirkət işçilərinin özləri edilmişdir. Əksər şirkətlər (31%), ümumiyyətlə, kompüter proqramlarının və əlavələrinin müdafiə modullarının olmasınıa əsaslanaraq özlərinin komputer və şəbəkə sistemlərinin təhlükəsizlik vəziyyətini izləməmişdir. 2013- cü ilin aprelində nəşr olunmuş he-

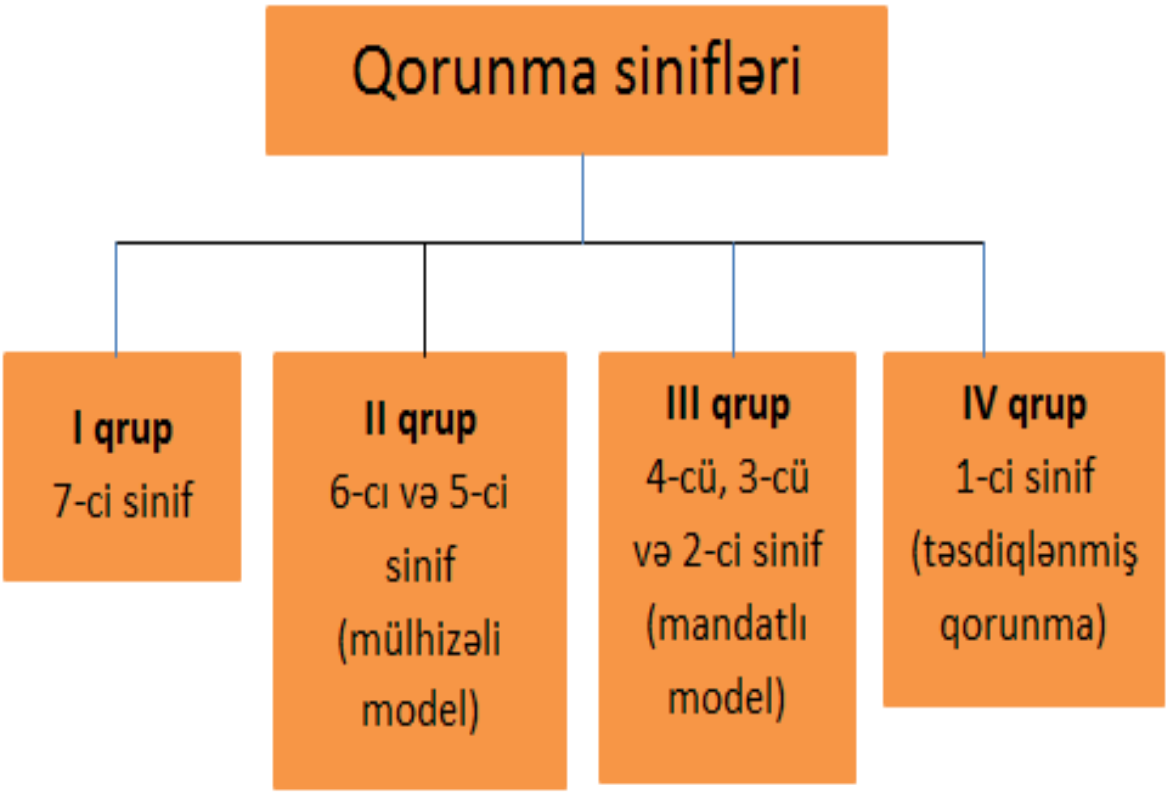
sabatda tendensiyanın əvvəlki kimi qalmışdır:

- sorğu edilənlərin 90%-i son 12 ildə onların təşkilatında informasiya təhlükəsizliyinin pozulmasını qeyd etmişdir;
- 78% bu pozuntulardan əhəmiyyətli maliyyə itkiləri olduğunu bildirdi;
- 49% zərərləri kəmiyyətcə qiymətləndirmişdir – onların ümumi məbləği 640 milyon dollardan çox olmuşdur.

Gartner Qrup təşkilatının məlumatına görə, ən böyük zərər daxili informasiya fəzasına çıxışın manipulyasiyası nəticəsində – korporativ şəbəkələrdən və verilənlər bazalarından verilənlərin və informasiyaların *oğurlanması*, informasiyanın *dəyişdirilməsi*, sənədlərin elektron formada *saxtalaşdırılması*, sənaye casusluğu baş verib. Son illərdə xarici hücumların sayının artması ilə yanaşı, virusların İnternet vasitəsilə yayılmasında da kəskin artım müşahidə olunmuşur.

Qeyd edək ki,"***Narıncı Kitab***"ın təlimatlarının tələblərinə uyğun olaraq, *kompüter texnikalarının təhlükəsizlik səviyyəsi* iyerarxik nizamlanmış yeddi sinifdən birinə aid olması ilə xarakterizə olunur. Təhlükəsizlik siniflərinin ierarxik nizamlanması – müəyyən bir sinif hesablama texnikası üçün icazəsiz girişdən qorunma vasitələrinin olması tələb olunduqda bu vasitələrin eyni zamanda daha yüksək sinif hesablama texnikası üçün də tələb ediləcəyini nəzərdə tutur. Baxılan vasitələrin üzərinə qoyulan tələblərin əhəmiyyətli tərəfi yalnız *daha yüksək təhlükəsizlik siniflərinə keçərkən* gücləndirilə bilər. Ən aşağı sinif yeddincidir, ən yüksək sininf icə birincidir. İcazəsiz girişdən qorunmanın müəyyən vasitələrinin olması yalnız bəzi (yüksək) təhlükəsizlik sinifləri üçün tələb oluna bilər.

Təhlükəsizlik sinifləri qoruma təminatının səviyyəsiniə görə fərqlənən dörd qrupda birləşmişdir: birinci qrupa yalnız bir *yeddinci sinif* daxildir; ikinci qrupa, ***seçmə təhlükəsizlik modelinin*** istifadəsi ilə xarakterizə olunur və *altıncı* və *beşinci* siniflər daxildirr; üçüncü qrup mandat təhlükəsizlik modelindən istifadə edir; bu qrupa *dördüncü, üçüncü* və *ikinci* siniflər daxildir; təsdiqlənmiş qorunma ilə xarakterizə olunan dördüncü qrupa yalnız *birinci* sinif daxildir (şəkil 5).



Şəkil 5. Müdafiənin təmini səviyyəsinə görə fərqlənən qorunma sinifləri

Verilənlərə icazəsiz daxil olmaqdan qorunmaq üçün bu və ya digər bir vasitənin olması və ya olmaması hesablama texnikası vasitələrinin təhlükəsizliyinin göstəricisidir. Təlimatlarda ümumilikdə 21 göstərici tərtib edilmişdir.

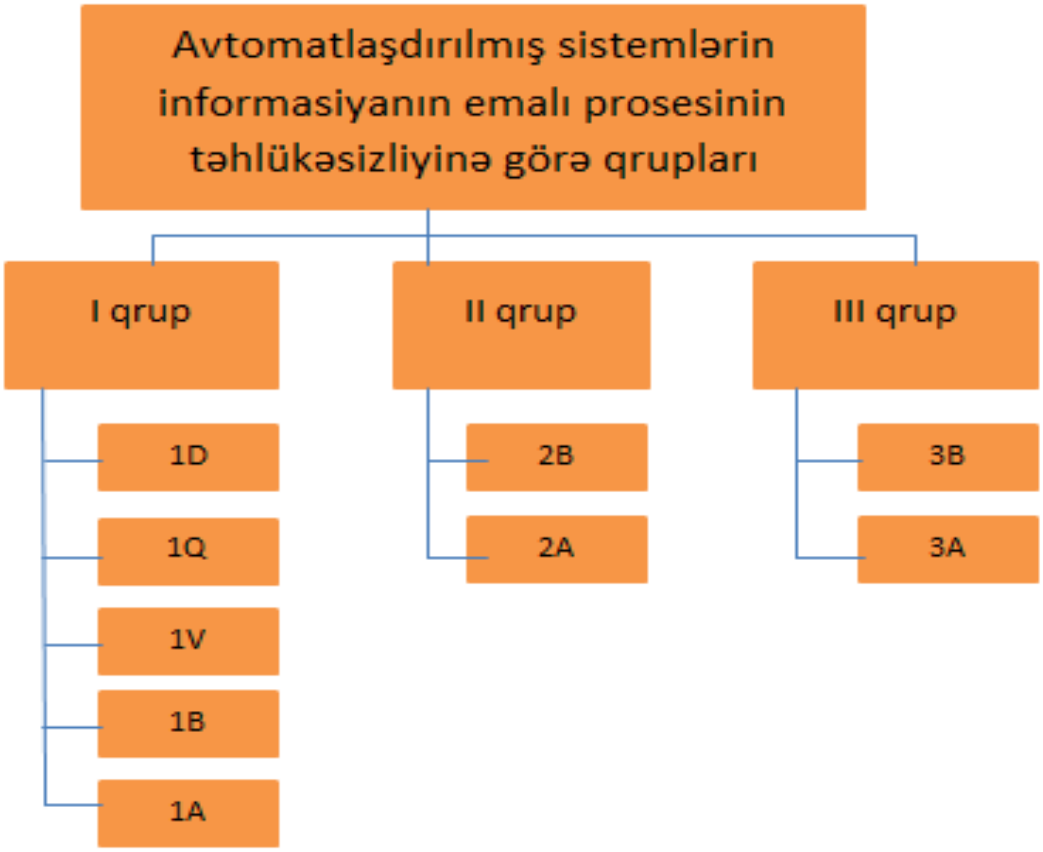
İnformasiya emal proseslərinin təhlükəsizliyinə görə, bütün avtomatlaşdırılmış sistemlər (AS) *üç qrupa* bölünür. *Üçüncü qrupa* bir istifadəçinin işlədiyi avtomatlaşdırılmış sistemlər daxildir. Onun bütün məlumatların *əl çatanlığı* və bu məlumatların *eyni məxfilik səviyyəsindəki daşıyıcılarda* yerləşdirildiyi qəbul edilir. İkinci və birinci qrupa məlumatların *müxtəlif məxfilik səviyyələrində* işləndiyi və saxlanıldığı çox istifadəçili avtomatlaşdırılmış sistemlər daxildir. Əgər istifadəçinin bütün işlənmiş və saxlanan məlumatlara eyni giriş hüququ varsa, onda avtomatlaşdırılmış sistem *ikinci qrupa* aiddir. Bütün istifadəçilərin heç də hamısının bütün məlumatları əldə etmək hüququ *olmadığı hallarda* sistem *birinci qrupa* aiddir (şəkil 6).

Emal olunan informasiyaların *məxfiliyindən* asılı olaraq, avtomatlaşdırılmış sistemlər hər qrupda siniflərə bölünür: üçüncü qrup iki sinifdən ibarətdir – 3B və 3A; ikinci qrupa da iki sinif daxildir - 2B və 2A; Birinci qrupa beş sinif daxildir - 1D, 1Q, 1V, 1B və 1A. Beləliklə, bütün avtomatlaşdırılmış sistemlər icazəsiz girişdən qorunma dərəcəsinə görə doqquz sinfə bölünür. Hər bir qrup daxilində qorunma tələblərinə görə siniflərin iyerarxiyası müşahidə olunur (tələbələrin siyahıları sırasına uyğun olaraq gücləndirilməklə).

İnformasiyanı icazəsiz daxil olmaqdan qorumaq üçün *proqram-texniki vasitələr sistemi* və *təşkilati tədbirlər* ***məlumatın qoruma sistemi*** tərəfindən həyata keçirilir. İnformasiya təhlükəsizliyi sistemi aşağıdakı dörd alt sistemdən ibarətdir:

- girişə nəzarət alt sistemi;
- uçot və mühasibat alt sistemi;
- kriptoqrafik alt sistem;
- bütövlük alt sistemi.

Konkret avtomatlaşdırılımış sistemin *atestasiya prosesi* sitemin müəyən sinfə daxil olması məqsədilə xüsusi ekspertzanın aparılmasından ibarətdir. Ekspertiza prosesi – siyahısı uyğun təlimatlarda göstərilən müəyyən xassələrin olmasını yoxlamaqdan ibaartədir.



Şəkil 6. Avtomatlaşdırılmış sistemlərin informasiya emal proseslərinin təhlükəsizliyinə görə qrupları

1999-cu ildə Beynəlxalq standartlaşdırma təşkilatı *İSO*. ”**İnformasiya texnologiyalarının təhlükəsizliyinin ümumi kriteriyaları**” adlı standart qəbul etdi. ”İSO/İES 15408:1999. İnformasiya texnologiyaları – informasiyanın mühafizəsinin metod və vasitələri – İT-lərin təhlükəsizliyinin qiymətləndirmə kriteriyaları". Bu standartd qəbul edilən qorunan sistemlərinin (o cüədən İS-lərin) qululma ideyasındakı dəyişikliyi əks etdirirdi. “Narıncı Kitab”dan və Dövət texniki komissiyanın təlimatından fərqli olaraq *yeni standartda* qeyd olunmuş qorunan siniflər yığımı konsepsiyası yoxdur. Yeni yanaşmanın əsas ideyası, təhlükəsizliyin bütün tələblərinin iki kateqoriyaya bölünmısindən ibarətdir: informasiya texnologiyasının təhlükəsizliyini təmin edən ***funksional*** kateqoriya, və funksional tələblərin düzgün və effektli reallaşmasını qiymətləndirən ***qiymətləndirməyə qarant tədbiri*** kateqoriyası.

İS-nin qorunmasının analizinə yaxın yanaşma ***BS 7799*** britaniya standartında təklif olunmuşdur. Standartın *qurulma ideyası* müxtəlif təyinatlı İS-lərin informasiyya təhlükəsizliyinin təmini təcrübəsinin ümumiləşdirilməsindən ibarətdir. Həmin standart 2000-ci ilin sonunda qəbul edilmiş ***İSO 17799*** standartının işlənməsi üçün əsas olmuşdur.

Standartın məzmunlu əsası təhlil olunan informasiya sistemindəki zəifliklərin müəyyənləşdirilməsi və qiymətləndirilməsindən, mövcud təhdidlərin səviyyəsinin qiymətləndirilməsindən və xərclərin təhlilinə əsasən təşkilat üçün risklərin məqbul səviyyəyə endirilməsi üçün tədbirlər toplusunun müəyyən edilməsindən ibarətdir.

Standart sistemin bütün həyat dövrü[2] mərhələlərində İS-nin təhlükəsizliyinin təmin olunmasının praktiki qaydalarından ibarətdir. Qaydalar kompleks metodlara inteqrasiya olunmuşdur və praktikada yoxlanan üsul və texnologiyalara əsaslanır. Məsələn, standart istifadəçilərin (və ya proseslərin) müəyyənləşdirilməsi və identifikasiyası, ehtiyat vasitələr, antivirus nəzarəti və s. vasitələrin istifadəsini tələb edir.

İnformasiya təhlükəsizliyinin təmini texnologiyasının təsvir olunan qaydalarının gözlənilməsi İS-nin bəzi baza səviyyəli təhlükəsizliyinə zəmanət verir. İS-nin təhlükəsizlik tələblərinin artması halında, mənbələrin dəyəri, informasiya risklərinin xüsusiyyətləri və sistem zəifliklərinin qiymətləndirilməsi aparılır ki, bunun əsasında informasiya resurslarını qorumaq sistemi seçilir.

İSO 17799 standartından istifadənin üştünlüyü – İS-nin təhlükəzizlik tələblərinə uyğunluğunun formal olaraq yoxlanılmasıdır. Sistemin atestasiyası uyğun spesifikasiya tələblərinin yerinə yetirilməsinin formal olaraq yoxlanılmasıdır. İS-nin təhlükəsizliyin baza səviyyəsinə uyğunluğu məsələsinin avtomatlaşdırılması üçün, spesifikasiyaların yerinə yetirilməsinin yoxlanılma proseduru ilə bağlı sualların siyahısını tərtib etməyə imkan verən proqram məhsulu işlən-

[2] *Sistemin həyat dövrü* – sistemin işlənməsinə başlanan andan onun istismardan çıxarılana qədər keçən zaman dövrüdür.

mişdir. Daxil edilmiş cavablara əsasən aşkar edilmiş çatışmazlıqların aradan qaldırılması üçün tövsiyələrlə birlikdə hesabat hazırlanır.

İS-nin *təhlükəsizliyin baza səviyyəsinə uyğunluğunun* atestasiyasının hazırlanmasının avtomatlaşdırılmış sisteminə nümunə olaraq *C&J Systems Security Ltd* (bax. [6]) firmasının ***COBRA*** proqram kompleksini göstərmək olar[3]. ***COBRA*** sisteminə bir neçə bilik bazası daxildir: ***ISO 17799*** standartının *ümumi tələblər bazası* və müxtəlif tətbiq sahələrinə yönəlmiş *ixtisaslaşmış baza*.

İS-nin təhlükəsizliyinin təmini səviyyəsinin daha tam araşdırılması aşağıdakıları təyin etməyə imkan verən tədqiqatların aparılmasını tələb edir:

- real olaraq IS üçün təhlükə yaradan bütün risklər müəyyənləşdirmək;
- IS resurslarındakı həssaslıqlar və onların səviyyələri qiymətləndirmək;
- təhdidləri müəyyənləşdirmək və səviyyələri qiymətləndirmək;
- İS-nin təhlükəsizliyinin təmin edilməsi ilə bağlı xərclərin qiyməylən-dirmək

İS-nin təhlükəsizliyinin ***CRAMM*** (bax. [7]) adlanan tam tədqiqat metodikası[4] sistemin analizinin ardıcıl *olaraq üç mərhələsinin aparılmasını* nəzərdə tutur.

1. ***Birinci mərhələdə*** İS-dən istifadənin təhlükəsizliyini əks etdirən İS modelinin qurulması və resursların identifikasiyası həyata keçirilir. Birinci mərhələ aşağıdakı məsələlərin həllilə bağlıdır:

- İS-nin tədqiqat sərhədlərinin təyini;
- resursların identifikasiyası (avadanlıq,verilənlər, proqram təminatı);
- İS-nin təhlükəsiz istifadəsini əksetdirə modelinin qurulması;
- resaursların dəyərinintəyini;
- hesabatın tərtibi və onun sifarışçitə təqdimi.

---

[3] ***COBRA*** – tanınmış proqram məhsuludur ki, ***İSO 17799*** standartının tələblərinin ödənilməsini yoxlamaq üçün nəzərdə tutulmuşdur.

[4] ***CRAMM metodu*** –Böyük Britaniyanın kompüter və telekommunikasiya agetliyi tərəfindən işlənmişdir və dövlər standartı kimi istifadə olunur.

2. ***İkinci mərhələdə*** İS-nin təhdid və həssaslığı təhlil edilir. Bu mərhələ aşağıdakı məsələlərin həllini əhatə edir:

- istifadəçi xidmətlərinin İS-nin müəyyən resurslarından asılılığının qiymətləndirilməsi;
- mövcud təhlükələrin səviyyəsini və İS-nin zəif cəhətlərini qiymətləndirmək;
- risk səviyyəsi hesablamalarının yerinə yetirilməsi.

3. ***Üçüncü mərhələdə*** əks tədbirlərin seçilməsi həyata keçirilir, avtomatlaşdırılmış rejimdə müəyyən edilmiş risklərə və onların səviyyələrinə uyğun olaraq IS-nin təhlükəsizliyi təhdidlərinə qarşı çıxmaq üçün bir neçə variant yaradılır. Adətən, informasiya riskləri üç kateqoriyada birləşir: *ümumi tövsiyələr*; *xüsusi tövsiyələr*; konkret bir vəziyyətdə İS-nin informasiya təhlükəsizliyini necə təmin etmək barədə *nümunələr*.

Bu mərhələdə İS-nin qorunmasının müxtəlif variantlarının və bu variantların dəyərinin effekliliyinin müqayisəli analizi aparılır.

2.4. İS-lərin bərpasinin və nüsxələşdirilməsinin metod və vasitələri

İS adminisratorunun həll etdiyi vacib məsələlərdən biri verilənərin iş nüsxəsi məhv etdikdən sonra sistemi bərpa etməsidir. Bu cür məhvin səbəbləri həm ***obyektiv***, həm də ***subyektiv*** ola bilər (şəkil 7).

İS-nin verilənlərinin məhv edilməsinin bəzi tipik *obyektiv səbəblərini* sadalayaq. Bunlar aşağıdakılardır:

- *aparat vasitələrinin normal işinin pozulması* (mexaniki hissələrin təbii aşınması və ya keyfiyyətə nəzarət zamanı aşkarlanmayan qüsurlar nəticəsində maqnit disk sürücüsünün sıradan çıxması);
- *təbii fəlakətlər nəticəsində hesablama sisteminin fiziki olaraq məhv edilməsi* (zəlzələlər, yanğınlar, daşqınlar);

- *proqram vasitələrinin normal işinin verilənlərin itkisilə nəticələnən pozulması* (yenidən yükləndikdən sonra operativ yaddaşdakı verilənlərin itirilməsi ilə əməliyyat sisteminin donması).

İS-dəki verilənlərin məhv edilməsinin səbəbi qəsdən və ya bilmədən *insan fəaliyyəti* ola bilər, məsələn:

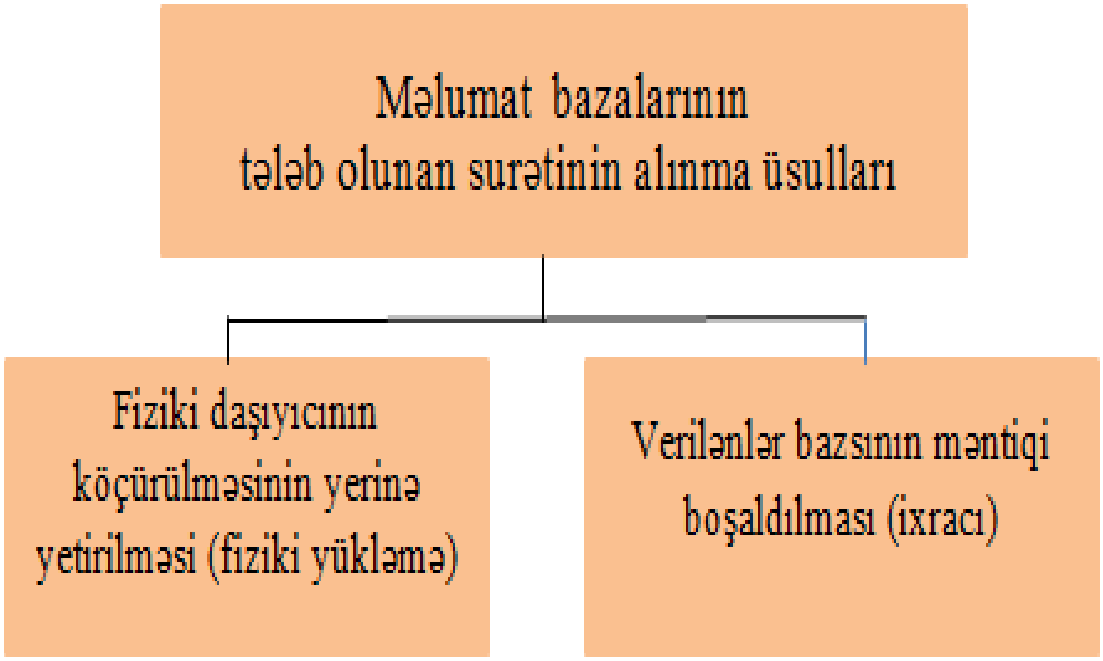
Şəkil 7. İS-nin verilənlərinin məhv edilməsinin səbəbləri

- *aparat vasitələrinin normal işinin bilərəkdən pozulması* (server rəfinə və ya soyutma sisteminə fiziki ziyan, zərərli niyyət və ya xidmət nümayəndəsinin qeyri sabit ruhi vəziyyəti nəticəsində qəfil elektrik kəsilməsi);
- *operatorun səhv hərəkətləri nəticəsində verilənlərin itirilməsinə səbəb olan proqram nasazlığı* (İS-nin işləməsi üçün vacib olan faylların səhv olarq məhv edilməsi, səhv əmrlərin icra edilməsi, kritik vacib proseslərin

məhv edilməsi və ya bloklanması);

- *virusların və digər dağıdıcı proqram təsirlərinin İS-ə daxil olduğu dağıdıcı hərəkətləri nəticəsində məlumatların itkisinə səbəb olan proqram vasitələrinin normal işinin pozulması* (informasiya daşıyıdıcılarının formatlaşdırmaq, İS sənədlərinin işləməsi üçün vacib olan sənədləri məhv etmək, məlumatları məhv edən əmrləri yerinə yetirmək).

Verilənlərin bərpası məsələsini həll etmək üçün IS verilənlərinin bir nüsxəsinə sahib olmaq zəruridir. Məlumat bazalarının tələb olunan surətini iki yolla əldə etmək olar (şəkil 8):



Şəkil 8. Məlumat bazalarının tələb olunan surətinin alınma üsulları

1. fiziki daşıyıcının köçürülməsinin yerinə yetirilməsi (fiziki yükləmə);
2. verilənlər bazasının məntiqi boşaldılması (ixracı).

Fiziki daşıyıcının köçürülməsinin yerinə yetirilməsi (maqnit disk daşıyıcıları), bir qayda olaraq, real verilənlər bazasının məntiqi yüklənməsilə müqayisədə daha tez həyata keçirilir. Əksər hallarda, bütün diskin bir nüsxəsini almaq əvəzinə, yalnız idarəedici informasiyaların və İS-nin verilənlərinin saxlanıldığı

fayllarının arxiv nüsxələrinin formalaşdırılması həyata keçirilir. İS fayllarının nüsxələrinin fiziki olaraq əldə etmək verilənlər bazası serverinin dayandırılmasını tələb edir və sistemə çıxışın müvəqqəti olaraq mümkün olmamasına səbəb olur.

Təcrübədə *verilənlər bazasından məntiqi boşaltma* daha çox tətbiq olunur. Bir nüsxədə xüsusi utilitlərdən istifadə etməklə bazada qeydə alınan məlumat bazasının tam və ya bir hissəsi haqqında məlumat ola bilər. Adətən, məntiqi boşaltma serverin bağlanmasını tələb etmir.Verilənlər bazasının məntiqi nüsxəsi, bir qayda olaraq, yüksək səviyyədə proqram-aparat sərbəstliyinə malikdir. Bir proqram-aparat platformasında yaradılan nüsxə, yalnız oxşar konfiqurasiyalı kompüterdə işləyən serverə deyil, həm də başqa əməliyyat sisteminin rəhbərliyi altında işləyən serverə yüklənə bilər.

İS-nin iş prosesində verilənlərdə baş verən dəyişikliklər yalnız verilənlər bazasının özündə deyil, həm də xüsusi jurnalda qeyd olunur. Sistemin etibarlılığının artırılması üçün verilənlər bazasının müasir serverləri adətən paralel olaraq jurnalın bir neçə nüsxəsini aparır.Verilənlər bazası pzulduqdan sonra onun vəziyyətinin bərpası həm də sistem jurnalının son nüsxəsinə əsasən həyata keçirilir.

Nümunə olaraq nüsxələşdirmə texnologiyasının rellaşmasına və ***Oracl*** verilənlər bazasının verilənlərinin bərpasına baxaq. Bu məqsədlə uyğun olaraq ***İMPORT*** və ***EXPORT*** utilitləri nəzərdə tutulmuşdur.Verilənlərin ixracının nəticəsi ***Oracl*** serverlərinin bütün realizasiyalarının dəstəklədiyi xüsusi formatlı fayllar yığımıdır.

Nüsxələşdirmə və bərpa utilitləri yalnız verilənlər bazsının rezerv nüsxəsinin yaradılması üçün deyil, həm də obyekt və verilənlərin sxemlər arası hərəkəti üçün istifadə oluna bilər. Bu utilitlərlə iki iş üsulu vardır – interaktiv və avtomatik. *Birinci üsulda* istifadəçi bilavasitə dialoq rejimində suallara cvab verərək *ixrac* və *idxal* parametrlərini verir. *İkinci üsulda* parametrlər əvvəlcə yaradılmış fayllardan oxunur. Qeyd etmək lazımdır ki,ikinci üsul daha çevikdir, belə ki, dialoq rejimində soruşulmayan parametrləri spesifikləşdirməyə imkan verir.

EXPORT utiliti verilənlərin nüsxələşdirilməsinin üç variantını dəstəkləyir: inkremental, komulyativ və ya tam. Tam ixracda bütün verilənlər bazasının boşaldılması baş verir. İnkrimental variantda verilənlər bazasının son inkremental ixrac anından başlayaraq dəyişən cədvəlləri boşaldılır. Belə ixrac aparılmadıqda son *komulyativ ixrac* anından başlayaraq dəyişən cədvəllər ixrac edilir. Komulyativ ixracda sonuncu tam ixrac anından başlayaraq dəyişən bütün cədvəllər emal olunur.

İdxal olunan verilənlər yalnız verilənlər bazasının bir və ya bir neçə cədvəlinin *məzmunu* deyil, həm də *istənilən sintaksis düzgün sorğunun* nəticəsi ola bilər.

İMPORT utiliti, verilənlər bazasının ***EXPORT*** utilitilə yaradılan rezerv nüsxəsinin köməyilə bərpa olunması üçün nəzərdə tutulmuşdur. Bərpanın üç variantı ola bilər: *konkret sahibkarın verilənləri*, *yalnız cədvəllər* və verilənlər bazasının *tam bərpası. Konkret sahibkarın verilənlərinin* ***bərpası variantından istifadə zamanı*** sahibi göstərilən istifadəçi olan *cədvəllər* yüklənir. ***Cədvəllərin bərpası rejimində*** parametrlərdə gösərilən *cədvəl utilitləri* ixrac olunur.

Verilənlərin idxalı prosesində bütün əməliyyatlar müəyyən bir ardıcıllıqla aparılır. Əvvəlcə *cədvəllər* yaradılır, sonra *veriləmlər* onlara yüklənir, sonra *indekslər* yaradılır. Bütün cədvəllər üçün bütövlük məhdudiyyətləri sonuncu olaraq daxil edilir. Verilənlər bazasının digər obyektləri (ardıcıllıqlar, təqdimatlar, saxlanılan prosedurlar və s.) dəyişdirilmədən ixrac edilir və idxal olunur.

FƏSIL III. Nəzarətedici sistemin yaradilmasi

3.1. Təhlükəsizlik siyasəti

İnformasiya təhlükəsizliyi sahəsindəki müasir lisenziyalaşdırma siyasəti informasiyanın qorunma vasitələrini hazırlayan və ya informasiyanın qorunması üzrə xidmətlər edən təşkilatlarda informasiya təhlükəsizliyinin konseptual və korporativ məsələləri təyin edən sənədlərin mövcudluğunu müəyyən edir. Dünya praktikasında ənənəvi olaraq belə bir sənəd təşkilatın ***təhlükəsizlik siyasəti*** adlanır.

İnformasiya təhlükəsizliyi siyasəti hər hansı bir təşkilatın fəaliyyətində istifadə etdiyi informasiya təhlükəsizliyi sahəsindəki qaydalar, prosedurlar, praktiki metodlar və qaydalar toplusudur. Başqa sözlə desək təkilatın informasiya təhlükəsizliyi dedikdə qiymətli məlumatların idarə edilməsi, onların qorunmasını və yayılmasını tənzimləyən sənədləşdirilmiş təhlükəsizlik qaydaları və prosedurları nəzərdə tutulur. İnformasiya siyasəti aşağıdakılardan asılıdır:

- informasiya emalının xüsusi texnologiyasından;
- istifadə olunan aparat və proqram təminatından;
- təşkilatın yerləşdiyi ərazidən.

Qeyd edək ki, qonşu Rusiya Federasiyasının ГОСТ Р ИСО/МЭК 17799-2005 standartına görə informasiya təhlükəsizliyi siyasəti rəhbərliyin məsuliyyətini müəyyənləşdirməlidir, həmçinin təşkilatın informasiya təhlükəsizliyinin idarəetmə yanaşmasını təsvir etməlidir. Göstərilən standarta uyğun olaraq, müəssisənin informasiya təhlükəsizliyi siyasətinə ən azı aşağıdakılar daxildir:

- informasiya təhlükəsizliyinin tərifi, ümumi məqsədləri və əhatə dairəsi, həmçinin məlumatın bölüşdürülməsi imkanını təmin edən bir vasitə kimi təhlükəsizliyin əhəmiyyətinin açıqlanması;
- rəhbərlik tərəfindən formalaşdırılmış informasiya təhlükəsizliyinin məqsəd və prinsiplərinin ifadəsi;

- təşkilat üçün ən vacib təhlükəsizlik siyasətinin xülasəsi, prinsiplər, qaydalar və tələblər, məsələn:
  - ✓ qanuni tələblərə və müqavilə öhdəliklərinə uyğunluq;
  - ✓ təhlükəsizlik təliminə tələblər;
  - ✓ virusların və digər zərərli proqramların yaranmasının və aşkarlanmasının qarşısının alınması;
  - ✓ işin davamlılığının idarə edilməsi;
  - ✓ təhlükəsizlik siyasətinin pozulmasına görə məsuliyyət.
- informasiya təhlükəsizliyinin idarə edilməsi çərçivəsində işçilərin ümumi və xüsusi vəzifələrinin müəyyənləşdirilməsi, o cümlədən informasiya təhlükəsizliyinin pozulması hadisələri barədə məlumat ve-rilməsi;
- informasiya təhlükəsizliyi siyasətini tamamlayan sənədlərə bağlantılar, məsələn, xüsusi məlumat sistemləri üçün daha ətraflı siyasət və prosedurlar, habelə istifadəçilərin riayət etməli olduğu təhlükəsizlik qaydaları.

Şirkətin informasiya təhlükəsizliyi siyasəti rəhbərlik tərəfindən təsdiqlənməlidir, dərc olunmalı və bütün işçilər üçün əlçatan və başa düşülən formada təqdim edilməlidir. İnformasiya təhlükəsizliyi siyasətinin yalnız "*kağız üzərində*" qalmaması üçün müəyyən tələblər ödənilməlidir.

İS üçün təhlükəsizlik siyasətinin *formalaşdırılmasında məqsəd* təşkilat rəhbərliyinin təşkilatın informasiya təhlükəsizliyi və texnologiyaları üçün təhdidlərin xarakteri barədə fikirlərini *açıq şəkildə ifadə* etməkdir. Təhlükəsizlik siyasəti ümumiyyətlə *iki hissədən* ibarətdir: ***ümumi prinsiplər*** və müxtəlif istifadəçilər üçün İS ilə işləmək üçün ***xüsusi qaydalar***. Təhlükəsizlik siyasəti həmişə İS resurslarının arzu olunan səviyyədə ***qorunması***, sistemlə işləmək ***rahatlığı*** və sistemin istismarı üçün ayrılan *vəsaitin* ***dəyəri*** arasında bir kompromisdir.

Təhlükəsizlik siyasəti bir neçə idarəetmə səviyyəsində sənədləşdirilməlidir. Yüksək rəhbərlik səviyyəsində təhlükəsizlik siyasətinin məqsədlərini, həll ediləcək vəzifələrin quruluşunu və siyahısını və siyasəti həyata keçirmək üçün mə-

suliyyəti müəyyən edən sənəd hazırlanıb təsdiq edilməlidir. Əsas sənəd təşkilatın fəaliyyət prinsipləri alaraq *məqsədlərin vacibliyi* və *resursların mövcudluğu* münasibətləri nəzərə alınmaqla İS-nin təhlükəsizlik administratorları (orta menecerlər) tərəfindən detallaşdırılmalıdır. Ətraflı qərarlar texniki və informasiya resurslarını necə qoru-maq *metodlarının aydın müəyyənləşdirilməsini*, həmçinin konkret vəziyyətlərdə işçilərin davranışlarını müəyyənləşdirən *təlimatları* daxil etməlidir.

ABŞ Milli Standartlar və Texnologiya İnstitutu (*National Institute of Standards and Technology — NIST*) tərəfindən hazırlanmış ***kompüter təhlükəsizliyi təlimatı***, aşağıdakı bölmələrin təhlükəsizlik siyasətinin təsvirinə daxil edilməsini tövsiyə edir.

Təhlükəsizlik siyasətinin predmeti. Bu bölmədə siyasətin *işlənməsinin məqsədləri* və *səbəbləri*, təşkilatın *sənəd dövriyyəsi sisteminin* müəyyən bir fraqmentində ***tətbiq sahəsi*** müəyyənləşdirilməlidir. Bu siyasətin toxunduğu İS - dən istifadə etməklə həll ediləcək məsələlər aydın əksini tapmalıdır. Zərurət yarandıqra sonrakı bölmələrdə istifadə olunan termin və təriflər tətib edilə bilər.

Təşkilatın mövqeyinin təsviri. Bu bölmədə İS resurslarının *xarakterini*, İS resurslarına icazə verilən *şəxslərin* və *proseslərin* siyahısını və İS resurslarına çıxış əldə etmə qaydasını dəqiq şəkildə təsvir etmək lazımdır.

Tətbiq. Bölmədə IS verilənlərinə giriş proseduru aydınlaşdırıla bilər, təhlükəsizlik siyasətinin həyata keçirilməsində tətbiq olunan məhdudiyyətlər və ya texnoloji zəncirləri təyin edilə bilər.

Rol və vəzifələr. Bu bölmədə *cavabdeh vəzifəli şəxslər* və təhlükəsizlik siyasətinin müxtəlif elementlərinin işlənməsi və tətbiilə bağlı *onların səlahiyyətləri* təyin olunur. Adətən verilənlərin təhlükəsizliyi administratorunun (o, IS resurslarına daxil olmağın təmin edilməsinin məsuliyyət daşıyır),verilənlər bazası administratorunun (girişə nəzarət mexanizmlərinin texniki realizasiyasını müəyyən edir), lokal şəbəkə administratorunun, operatorların səlahiyyətləri müəyyən edilir.

Siyasətə nəzarət. Bu bölmədə İS istifadəçisinin hüquq və səlahiyyətləri təs-

vir edilir. Təşkilatın informasiya mənbələrinə daxil olduqda və rejim tələblərinin pozulmasına görə cəzalandırılanda yolverilməz hərəkətlərin siyahısı ilə istifadəçilərin *aydın təsviri* və *sənədləşdirilmiş şəkildə* tanışlığı zəruridir. Təhlükəsizlik siyasətinin pozulması faktlarını qeyd etmək və pozuculara qarşı inzibati tədbirlərin tətbiqi texnologiyası dəqiq müəyyənləşdirilməlidir.

Effektiv həyata keçirmək üçün təhlükəsizlik siyasətini bütün IS istifadəçiləri başa düşməlidirlər. Təqdimatların hazırlamaq və seminarlarda təhlükəsizlik siyasətinin həyata keçirilməsinin əsas məqamlarını və praktik texnologiyalarını izah etmək mümkündür. Təşkilatın yeni əməkdaşları qəbul edilmiş təhlükəsizlik siyasətinə uyğun olaraq realizə olunan İS resurslarına çıxışın konkret qaydaları və texnologiyaları ilə tanış olmalı və ya öyrənməlidirlər. Nəticələrin müzakirəsi ilə birlikdə işçilərin hərəkətlərinə nəzarət yoxlamaları aparmaq məqsədəuyğundur.

Təhlükəsizlik siyasətini effektiv şəkildə həyata keçirmək yalnız o, mövcud sifarişlərə və təşkilatın ümumi məqsədlərinə uyğun olduqda mümkündür. Təhlükəsizlik siyasətini təşkilatın mövcud standartları ilə əlaqələndirməyin əsas üsulu, iş prosesi zamanı onun maraqlı şöbələrlə əlaqələndirilməsindən ibarətdir.

Təhlükəsizlik siyasətinin həyata keçirilməsi üçün *təşkilatın əsas qərarlarını təmsil edən sənədlər toplusuna* aşağıdakılar daxil edilməlidir:

- bütövlükdə təşkilat və zəruri hallarda konkret bölmələr üçün riskləri qiymətləndirmək və idarə etmək üçün istifadə olunan yanaşmaları müəyyən edən ***sənədləşdirmə;***
- baxılan İS qorunma vasitələrinin seçilməsində qəbul edilmiş ***qərarın əsaslandırılması;***
- qalıq riskinin mümkün səviyyəsinin təyini prosedurunun ***formal təsviri***;
- informasiya təhlükəsizliyi rejiminin *yoxlanılması qaydalarını* və yoxlamanın nəticələrinin qeyd olunduğu *jurnalları* müəyyən edən ***təlimat*** (informasiya təhlükəsizliyi vasitələrinin effektli realizəsinin yoxlanılmasını həyata keçirən üçün sənədlər zəruridir)
- IS-yə qulluq və idarəetmə proseslərini tənzimləyən sənədlər;

- risklərin qiymətləndirilməsi və idarə edilməsi üçün dövri auditlərin hazırlanması üçün sənədlər;
- informasiya təhlükəsizliyinin idarəetmə sisteminin təşkili və təhlükəsizliyin idarəetmə vasitələrinin qeydiyyatı haqqında məlumatların daxil olduğu "Uyğunluq Bəyannaməsi" sənədi;

Təhlükəsizlik siyasətinin müvəffəqiyyəti mürəkkəb proqram təminatı və aparat nəzarətindən daha çox təhlükəsizlik siyasətını həyata keçirən insanların səylərindən və təcrübələrindən asılıdır.

3.2. İdentifikasiya və autentifikasiya texnologiyalari

İnformasiya sistemi resurslarına çıxış əldə etmək üç prosedurun yerinə yetirilməsini nəzərdə tutur: ***identifikasiya***, ***audentifikasiya*** və ***avtorizasiya***.

İdentifikasiya prosedurunun mahiyyəti istifadəçi təyinatıdır, yəni verilənlər bazası serverinin tələbatçısı – obyektdir. İstifadəçi adı, qəbul edilmiş adlandırma konvensiyalarına uyğundur və nümayiş olunan obyektlərin məkanında bir real obyektin birmənalı identifikasiyasını təmin edən unikal bir etiketdir. IS baxımından identifikatoru təqdim edən mənbələr ayrılmazdır. Yəni istifadəçi həm terminalda oturan *real bir şəxs*, həm də tətbiqi *proses* olabilər ola bilər, lakin sistem üçün *hər iki obyekt* eynidır.

Daha sadə formada desək, ***identifikasiya*** – obyektə unikal adın verilməsi (müəyyən adla tanınması), və identifikatorun bütün digər identifikasiyalı adlarnan müqayisəsidir. İdentifikator obyekti birqiymətli olaraq xarakterizə etməlidir, yəni, iki müxtəlif obyektin eyni identifikatoru olmamalıdır.

İdentifikasiya birbaşa audentifikasiya ilə bağlıdır.

Audentifikasiya prosedurunun mahiyyəti identifikator təqdim edən istifadəçinin şəxsiyyətini təsdiqləməkdir. Başqa sözlə desək ***audentifikasiya*** – təqdim olunan identifikatorun orijinallığını yoxlanılması prosesidir, yəni müəyyən adla təqdin olunan obyektin iddia olunan obyekt olub olmadığının yoxlanılması prose-

sidir. Orijinallığını təsdiqləmək üçün obyekt başq heç nə ilə deyil, yalnız bu identifikatorla təqdim edilə bilər.

Avtorizasiya prosedurunun mahiyyəti, təsdir olunmuş istifadəçinin işləməsinə icazə verilən xüsusi məlumat mənbələrinin siyahısını müəyyənləşdirməkdir. Avtorizasiya prosesində istifadəçinin verilənlərlə həyata keçirə biləcəyi bir sıra mümkün əməliyyatlar da qurulur. Qeyd edək ki, İS-də *avtorizasiya* prosedurlarının həyata keçirilməsi üçün informasiyalar saxlanılmalıdır. Bu məlumat etibarlı şəkildə qorunmalıdır, çünki onun ilk növbədə ***təcavüzkarın*** hədəfi olduğu aydındır.

İdentifikasiya, *audentifikasiya* və *avtorizasiya* prosedurları hər bir qorunan İS-lər üçün vacibdir.

Təhlükəsiz sistemlərin qurulmasının *əsas prinsipi* odur ki, məlumat əldə etmək prosesi məlumat əldə etməyi tələb edən *subyektin* əvvəlcədən müəyyənləşdirilməsinə və tələb olunan obyektin təyin olunmasına əsaslanır. *İdentifikasiya* və *audentifikasiya* prosedurları, müəssisələrin İS-ləri də daxil olmaqla, hər bir avtomatlaşdırılmış sistem üçün *ilk müdafiə xəttini təmin* edən məcburi texnoloji prosedurlardır. Avtomatlaşdırılmış sistemlərdə əksər hallarda *identifikasiya* və *audentifikasiya* prosedurları ***Login***-prosedurları adlanır.

İdentifikasiya və *audentifikasiya* prosedurlarının effekliliyi bütövlükdə təhlükəsizlik sisteminin effektivliyinə əhəmiyyətli dərəcədə təsir göstərir. İdentifikasiya proseduru istifadəçinin sistemlə bağlantısının yaradılması ilə başlanır. İstifadəçi özünü tanımalı (identifikasiya etməli) və audentifikasiya prosedurunun bəzi parametrlərini təqdim etməlidir. Əgər audentifikasiya alt sistemi təqdim olunan parametri qəbul edərsə,onda ***Login***-ı proses müvəffəqiyyətlə başa çatır və istifadəçi ilə İS - nin qarşılıqlı təsir sessiyası yaranır.

Qorunan IS-lər üçün *audit alt sistemi* həm uğurlu, həm də uğursuz ***Login***-proseslərini qeyd etməlidir.

Konkret autentifikasiya prosedurlarının əsasını qoyan *üç növ prinsipi* seçmək olar - autentifikasiyaya aşağıdakılara əsaslanan:

- *bilik* (istifadəçinin bəzi məxfi bilikləri var);
- *mövcudluq* (istifadəçinin bəzi məxfi predmetləri var);
- *xüsusiyyətlərin yoxlanılması* (istifadəçi bəzi unikal xüsusiyyətləri təqdim edir).

Qorunan real informasiya sistemində müxtəlif prinsiplərə əsaslanan bir neçə *audentifikasiya* mexanizmindən istifadə etmək məsləhət görülür.

Biliə əsaslanan audentifikasiya prosedurlarının *üstünlüyü onun sadəliyidir*. Müvafiq prosedurlar uzun müddət avtomatlaşdırılmamış konurda istifadə edilmişdir. Məsələn, *parol* və *rəyin* köməyilə *hərbi* və *sərhəd* gözətçiliyində qarşılıqlı tanınma. Bu cür prosedurların əsas çatışmazlığı *çoxalma asanlığıdır* və parol yalnız *oğurlana, gizlədiliə* və *tutula* bilməkdən başqa, həm də *təxmin edilə* bilər.

Parol qoruma sistemlərində adətən, istifadəçi və sistemin ümumi sirri olaraq istifadəçinin yadda saxlaya biləcəyi əlifbanın 6 -dan 10-a qədər işarəsindən ibarət ardıcıllıq götürülür. İnformasiya sistemi resursuna (məsələn, verilənlər bazası, printer və s.) çıxışın əldə edilməsi üçün üçün istifadəçi *identifikatoru* və *parolu* təqdim edir və birbaşa və ya dolayı yolla lazımlı resurzu müəyyənləşdirir. Bu halda istifadəçi identifikatoru *identifikasiya üçün bir ərizə*, parol isə bu *ərizənin təsdiqi* kimi çıxış edir.

Sabit parolları olan sistemə *bir rəqibin ən sadə hücumu*, əsl parol tapana qədər *bütün mümkün variantları axtarmaqdır*. Bu hücum ***off-line*** rejimində xüsusilə təhlükəlidir. Belə ki, bu halda bilavasitə paroln yoxlanma cihazı ilə kontaktda olmaq tələb olunmur, və ona görə vahid zamanda parolun mənasız olaraq yoxlanımmasına cəhd edilmələrin sayı, adətən ***on-line*** rejimindəki yoxlamada olduöu kimi məhdudlaşdırıla bilməz. Bu hücumun effektivliyi birbaşa sistemə və ya onun resursuna girişi təmin edən *ilk parolu tapmaq cəhdlərinin sayından*, həmçinin bu cəhdlərin hər birinin vaxt mürəkkəbliyindən asılıdır.

Sistemə daxil olma ehtimalını təmin edən *bu identifikasiya sxeminin təhdidləri arasında* parolların açıqlanması və rabitə xətlərindən (sistemin daxilində) məlumatların tutulması da var. İstifadə olunan parolların qeyri-müəyyənliyini

artırmaq və eyni zamanda bir insanın yadda saxlama qabiliyyəti kimi vacib bir keyfiyyətin pozulmaması üçün çox vaxt ***parol cümləsindən*** istifadə olunur. Bu vəziyyətdə, *bütün cümlə* qısa bir söz əvəzinə parol kimi istifadə olunur. Açar sözlər sabit bir uzunluğa şifrələnir və adi parol ilə eyni rol oynayır. Bu metodun ideyası, bir adamın hərf və ya rəqəmlərin təsadüfi ardıcıllığından daha çox *bir ifadəni yadda saxlamasıdır*. Açar sözlər qısa paroldan daha çox təhlükəsizliyi təmin edir, lakin daxil edilməsi üçün daha çox vaxt tələb edir.

Birinci tip prosedurun *geniş istifadə olunması* həmçinin audentifikasiya (parol) parametrinin qiymətinin dəyişdirilməsinin sadə olmasındaan ibarət üstünlüklə bağlıdır. Parol onun bilinməsinə şübhə olduqda asanlıqla dəyişdirilə bilər.Əksər informasiya sistemlərində müntəzəm olaraq parolun dəyişdirilməsi vacib tələbdir.

Mövcudluğa əsaslanan *audentifikasiya,* hamıya gündəlik təcrübədən yaxşı məlumdur.Ən sadə seçim *kilid üçün* bir *metal açardır* (mənzil, avtomobil və s.). Bu cür audentifikasiya sistemlərinin ortaya çıxması zamanı onların etibarlılığı fiziki bir mövzunun çoxaldılmasının mürəkkəbliyinə əsaslanırdı. Fiziki obyektlərin reproduksiya texnologiyasının hazırda əhəmiyyətli dərəcədə inkişaf etmiş olmasına baxmayaraq, texnologiya yenə audentifikasiya üçün istifadə olunur. Sahibini audentifikasiya edən (eyniləşdirən) predmet olaraq, ***smart kartlar*** və ***elektron açarlar*** istifadə olunur.

Mülkiyyət əsaslı audentifikasiyadan istifadə edərkən yaranan əsas problem audentifikasiya elementinin *oğurlanması* və ya *itməsi* ola bilər. Buna görə adətən informasiya sistemlərində *iki mərhələdən ibarət olan* kompleks bir prosedur istifadə olunur. *İlk mərhələdə* sistem istifadəçisi bir element təqdim edir: *elektron açar, smart kart* və ya müvafiq oxuqurğusuna daxil edilən ixtisaslaşdırılmış mikrosxem (çip). *İkinci mərhələdə* istifadəçi, əşyanın həqiqi sahibi olduğunu və müəyyən informasiya resurslarına daxil olmaq hüququnu sübut etmək üçün şəxsi identifikasiya nömrəsini (PİN) daxil edir.

Tarixi şərait və istifadəçilərin rahatlığı üçün fərdi identifikasiya nömrəsi rəqəmsaldır və 4-dən 8 rəqəmə qədərdir. Onu total seçimdən qorumaq üçün əlavə

təşkilati tədbirlər istifadə olunur. Məsələn, ***əksər bankomatlar səhv nömrəni üç dəfə daxil etdikdə kredit kartını bloklayırlar***.

Xüsusiyyətlərin yoxlanılmasına əsaslanan audentifikasiya əksər hallarda insanın biometrik xüsusiyyətlərinə (barmaq izləri, gözün rəngbərəng şəkli və s.) əsaslanır.Bu texnologiyanın üstünlüyü odur ki, audentifikasiya elementi itirilə bilməz. Eyni zamanda, Pentaqonda və buna bənzər təşkilatlarda bu texnikanın geniş yayılması ilə bağlı çoxsaylı bəyanatlara baxmayaraq, audentifikasiyanın "*fəlsəfi daşı*" tapmaqla əlaqəli eyforiya əsassızdır.

Yapon kriptoqrafı ***Tsutomu Matsumoto*** və onun Yokohama Universitetindəki bir qrup tələbəsi 2002-ci ilin əvvəllərində *saxta barmaq izləri hazırlamaq üçün* iki çox təsirli texnologiya yaratdılar və nəşr etdilər. Birinci (*trivial*) üsulda, yaponlar "*qurban*" ın barmağından birbaşa tökmə düzəltdilər, bunun üçün təyyarə və gəmi modelçilərinin istifadə edilən *yeməli jelatin* və *qəlib plastiklərindən* istifadə etdilər. Jelatin zolaq barmaq izini səssizcə barmağa yapışdırmaq və girişin kompüter sistemini , hətta gözətçi olduqda belə aldatmaq olar. Bu sadə texnologiya, onlarla kommersiya biometrik qoruyucu cihazı sınaqdan keçirilərkən 80% hallarda uğurla tətbiq edilmişdir.

Bəzi təlimlərdən sonra *jelatin tökmə* ***həvəskar tədqiqatçılara*** nəm və ya elektrik müqavimətinə cavab verən "*canlı barmaq detektorları*" ilə təchiz olunmuş daha da inkişaf etmiş ***sistemləri aldatmağa imkan verdi.*** Bir qədər əvvəl, Hollandiyalı ***Ton van der Putte*** və ***Jeroen Koining***, bazardakı biometrik barmaq izi tanıma sistemlərinin 100% -ni aldadan öz texnologiyasını inkişaf etdirib İnternetdə yayımladılar. Kriptoqrafiya sahəsində tanınmış mütəxəssis ***Bruce Schneiern*** şərhindən istifadə etsək, alınan nəticələr oxşar sistemlərin tam etibardan salmaq üçün tamamilə kifayətdir.

İS istifadəçilərinin audentifikasiyası üçün *biometrik texnologiyaların istifadəsini tamamilə rədd edərək* digər yerə gedilməməlidir. IS istifadəçilərinin effektiv audentifikasiyası sistemi üç əsas sxemin səmərəli birləşməsinə əsaslanmalıdır.

İnformasiya sistemlərinin əhəmiyyətli bir hissəsi sənaye səviyyəli verilənlər bazasının idarəetmə sistemləri (VBİS) əsasında qurulmuşdur, buna görə praktik nümunə olaraq VBİS-də istifadə olunan *audentifikasiya texnologiyalarına* baxaq.

Sənaye səviyyəli VBİS-də audentifikasiya proseduru tamamilə xarici ola bilər, yəni *əməliyyat sistemi tərəfindən* həyata keçirilir (məsələn, *IBM DB2*-də), və ya daxili, yəni verilənlər bazası server alətləri ilə həyata keçirilir (məsələn, *Oracl*-da).

İstifadəçi *əməliyyat sistemi* (və ya ixtisaslaşdırılmış proqram) *tərəfindən müvəffəqiyyətlə təsdiqlənsə*, *IBM DB2* istifadəçini şəxsiyyəti ilə müəyyənləşdirir, bu adətən istifadəçinin əməliyyat sistemində qeyd olunduğu *adla eyni olur*, eyni zamanda istifadəçinin *DB2* korrekt adlar fəzasında adının əksi də ola bilər. Əməliyyat sisteminin *səlahiyyətli administratoru*, əməliyyat sistemininin vasitələrindən istifadə edərək istifadəçini qeydiyyata almaq üçün müvafiq əməliyyatları yerinə yetirərən yeni identifikator yaradır.

Oracle – da *standart təhlükəsizlik prinsipini* və ya *minimum imtiyazlar prinsipini* dəstəklənməsi reallaşmışdır. Bunun mahiyyəti ondan ibarətdir ki, istifadəçinin verilənlər bazası obyektinə (məsələn, *cədvəl* və ya *təqdimat*) daxil ola bilməsi və ya sistemdə müəyyən hərəkətlər edə bilməsi (məsələn, *yeni bir cədvəlin* və ya *yeni bir istifadəçinin* yaratması) yalnız buna açıq icazə verildiyi təqdirdə mümkündür. Ona görə, təsdiqini müvəffəqiyyətlə keçən istifadəçi, səlahiyyətli administrator bu istifadəçi üçün mümkün əməliyyatların siyahısını təyin etməyincə əslində heç bir şey edə bilməz. Xüsusilə, müvəffəqiyyətli identifikasiyadan sonra düzgün bir istifadəçi (düzgün parol) daxil olmaqla) verilənlər bazası serverinə qoşula bilməz, yəni, ***CONNECT*** əmrini uğurla icra edir.

DB2, əməliyyat sisteminin hər hansı bir istifadəçisinin müəyyən verilənlər bazası əməliyyatları aparmaq üçün minimum hüquqlarına sahib olduğu bir yanaşma tətbiq edir. Belə ki, *əməliyyat sisteminin istənilən istifadəçisi* verilənlər bazasının adını bilmək şərtilə ***CONNECT*** əmrindən istifadə edərək verilənlər bazası ilə əlaqə qura bilər. Verilənlər bazası yaratarkən, sistemin bütün istifa-

dəçilərinə səlahiyyətli administrator tərəfindən modifikasiya oluna bilən bir sıra standart imtiyazlar verilir. Bu yanaşmanın *üstünlüyü*, bəzi standart vəziyyətlərdə *təhlükəsizlik administratorunun* işinin sadələşdirilməsidir. *Çatışmamazlığı* – hər bir verilənlər bazası yaradıldıqdan sonra verilənlərin təhlükəsizliyini təmin etmək üçün artan tələbləri olan sistemlər üçün təhlükəsizlik administratorunun *zəruri hərəkətlərə* ehtiyacdır.

Audentifikasiya prosedurunu əməliyyat sistemi səviyyəsində aparan yanaşmanın *üstünlükləri* və *mənfi cəhətləri* vardır. Əsas üstünlük ondan ibarətdir ki, açıq kodlu əməliyyat sistemləri (məsələn, *Linux*) üçün audentifikasiya proseduru *daha şəffaf olu*r və buna görə təhlükəsizlik administratoru tərəfindən buna etibarlılıq səviyyəsi artır. Bu yanaşmanın *əsas çatışmazlığı*, əməliyyat sisteminin təhlükəsizlik sistemində aşkar edilmiş bir zəifliyin dərc edilməsi (*bu açıq kodlu sistemlər üçün standart bir prosedurdur*) verilənlər bazası serverinin *zəifliyinə* də səbəb olur.

3.3. İS-lərin fəaliyyətinin ştat rejiminin pozulmalarinin tipləri

İS-nin *ştat rejiminin pozulması*, qorunan İS-lər üçün üçün xarakterik xüsusiyyətlərin *tam* və ya *qismən* itirilməsi ilə bağlı olan *üç böyük sinif* ilə təqdim oluna bilər (şəkil 9):

- *saxlanılan* və *işlənmiş* məlumatların məxfiliyinin pozulması;
- məlumatın *bütövlüyünün* pozulması;
- sistemin mövcudluğunun *pisləşməsi* və ya *itirilməsi*.

Normal iş rejiminin pozuntularının *təsnifatı üçün əsas*, təcavüzkar tərəfindən məruz qalmış İS –nin təhlükəsizliyini təminatının *alt sistemi də* ola bilər. Oxşar təsnifat məlum *aktiv müdaxilələrin təcrübəsinin* analizi və ümumiləşdirilməsi əsasında qurulur və İS-nin *normal iş rejiminin pozulmasına əks təsir edən metod və vasitələri vəziyyətini diqət mərkəzində saxlayan* İS-nin təhlükəsizlik administratoru üçün nəzərdə tutulur.

Verilənlərin tutulması – verilənlərin paylanmış emal olunması üçün zəruri

olan serverlər arasında ötürülmə zamanı onların köşürülməsinin və ya dəyişdirilməsinin potensial imkanı. Sistemin ştat rejiminin pozulmasına səbəb olan aşağıdakı *hücum növlərini* ayırmaq olar:

- ötürülmə prosesində *verilənlərin dəyişdirilməsi*, məsələn, leqal tranzaksiya prosesində müəyyən hesaba köçürülən *pulun müqdarının* artırılması;
- məxfi məlumatları ayırmaq üçün ötürülmə zamanı verilənlərin köçürülməsi, məsələn, istifadəçi identifikatorlarını və bəzi şifrə sisteminin müvafiq şifrələrini və ya kredit kartı nömrələrini ayırmaq üçün *kanal* və ya *şəbəkə* səviyyəsindəki *paketlərin surətini çıxarmaq*;
- *leqal tranzaksiyanın təkrar yerinə yetirilməsi*, məsələn, leqal prosesin tutulmuş kopiyasının çoxsaylı təkrarlanmaı.

Şəlil 9. İS-lərin fəaliyyətinin ştat rejiminin pozulmalarinin tipləri

Bu növ pozuntu ilə mübarizənin əsas yolu onun ötürülməsi prosesində məlumatları qorumaq üçün *kriptoqrafik metodlardan* istifadə etməkdir.

Saxta identifikasiya – bu hər hansı bir üsulla əldə edilən digər şəxslərin audentifikasiya vasitələrindən istifadə etmək üçün bir fürsətdir. Sistemin ştat iş rejiminin pozulmasına gətirən *aşağıdakı hücum növləri* seçmək olar:

- *fərdi məlumatları toplamaq üçün saxta bir serverdən istifadə etmək*, məsələn, kredit kartı nömrələrini toplamaq üçün elektron bir mağaza serverini yaratmaq və ya başqasının adına imzalanmış elektron sənədləri yaratmaq üçün saxta açıq açar server yaratmaq;
- *audentifikasiya olunmuş informasiyadan icazəsiz istifadə*, məsələn, elektron sənədlərin icazəsiz imzalanması üçün klaviaturanın köməyilə köməyilə tutulmuş şəxsiyyət nişanları və parol və yaud gizli açarın nüsxəsi.

Bu növ pozuntu ilə ***mübarizənin əsas yolu*** istifadəçilər və proseslərin qarşılıqlı identifikasiyası və audentifikasiyası üçün lazımi prosedurların keyfiyyətini təmin edən ***audentifikasiya metodlarından*** istifadə etməkdir.

Şifrələrin istifadəsi üçün natamam üsul – insanların istifadə xüsusiyyətlərini bilməklə parolların kompensasiyasıdır. IS-nin nizamlı işinin pozulmasına səbəb olan *uğurlu hücumların* əsas növləri:

- *lüğətlə parolların avtomatik düşünülməsi*, məsələn, heyvan ləqəbləri və ev heyvanlarının adları və s. mövzularında dəyişiklik olan parollar;
- sistemin konkret istifadəçisi barədə informasiyanın analizi əsasında parolun düşünülməsi, məsələn, doğum tarixi temasının varyasıyası olan parol.

Bu növ pozuntu ilə ***mübarizənin əsas yolu*** budur – kifayət qədər uzun və mənalı olmayan parolun istifadəsi. Sistemdəki parolun müntəzəm olaraq dəyişdirilməsi. Qeyd edək ki, qabaqcıl nəsil texnikalarının tətbiqi, sistemin saxlanması üçün yerüstü xərclərin nəzərəçarpacaq dərəcədə artmasına səbəb olur (*xüsusən sistemin yararlılıq xüsusiyyətləri pisləşir və idarə olunması mürəkkəbləşir*).

Sistemin qeyr kafi auditi - bu istifadəçilərin sistem vasitəsi ilə *qeyd olunma yan* və *təsadüfən* və ya *məqsədyönlü şəkildə* sistem təhlükəsizliyinin pozulmasına səbəb olan hərəkətlər etməsi üçün potensial imkandır.

Bu növ pozuntu ilə mübarizənin əsas yolu – iqtisadi cəhətdən sağlam audit sistemindən istifadə etməkdir.

Çox səviyyəli çox istifadəçi sistemlərin təhlükəsizlik idarəetmə xüsusiy-

yətlərinin lazımi səviyyədə nəzərə alınmaması – bu on və ya yüz minlərlə istifadəçi üçün *audentifikasiya vasitələrinin*, həmçinin orta təbəqənin proqram təminatı ilə qarşılıqlı əlaqəsini təmin edən *agentlərin* dəstəyilə bağlı müdafiə sistemində səhvlərin əmələ glməsinin pitensial mümkünlüyüdür. Bir verilənlər bazası sistemi üçün kifayət qədər mürəkkəb olan problem bir neçə qarşılıqlı server və verilənlər bazası üçün əhəmiyyətli dərəcədə daha mürəkkəbdir.

Bu növ pozuntu ilə mübarizənin əsas yolu sistemdəki istifadəçi və ya proses üçün birdəfəlik audentifikasiya sxemindən istifadə etməkdir. Belə sxemlər, bir qayda olaraq, aşıq açarların müəyyən infrastrukturlara əsaslanır.

3.4. Müdaxilənin aşkarlanması və onun mənfi nəticələrə gətirməsinin qarşısının alınması

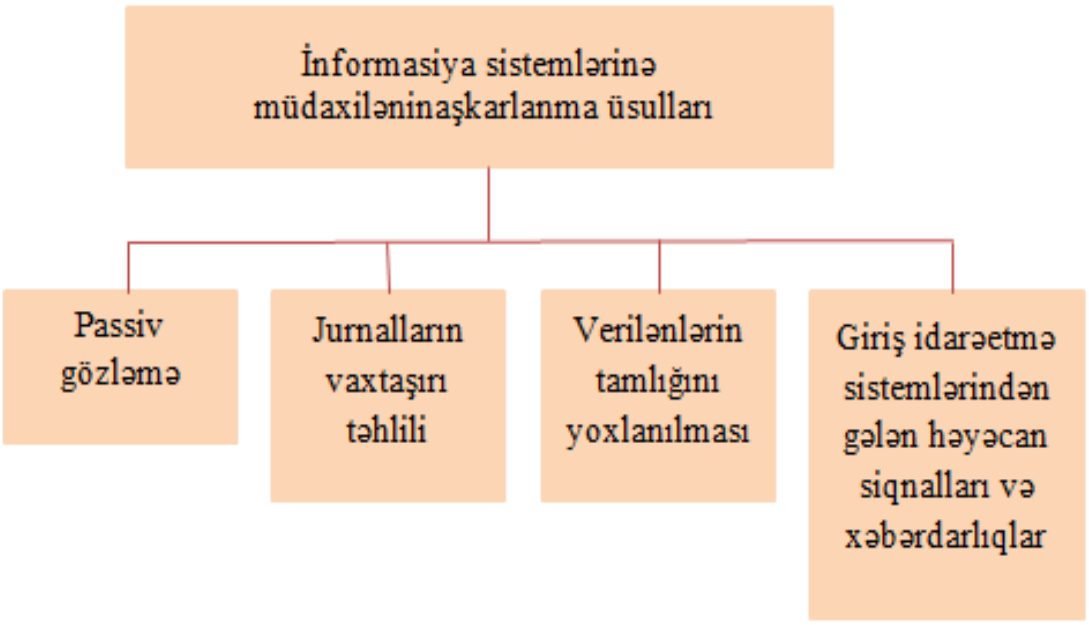
Müdaxilənin aşkarlanması sistemi (*intrusion detection*) təşkilatın təhlükəsizlik siyasətinin həyata keçirilməsi sisteminin *vacib hissəsidir*. Müdaxilənin istifadə olunan aşkarlanma sxemi təşkilatın İS-nin resurslarının qorunmasının ümumi probleminin həll mexanizminin iki vacib funksiyasını yerinə yetirir:

- ***əks əlaqə funksiyası.*** Aşkar edilmiş müdaxilələrin (həm *uğurlu*, həm də *uğursuz*) olması və ya olmaması barədə məlumatlar IS təhlükəsizlik alt sistemlərinin keyfiyyətini qiymətləndirmək üçün obyektiv əsasdır;
- ***sistemin registrasiya edici və qoruyucu mexanizmlərini yüklənməsi funksiyası***. Aşkar edilmiş müdaxilələrin olması barədə ***məlumat*** (müvəffəqiyyətli və uğursuz) müdaxilə parametrlərinin *qeydiyyatı funksiyasının* və *neytrallaşdırmanı* əlavə mexanizmlərinin inisalizsiyasını və ya *zərərin azaldılmasını* aktivləşdirən *bir şərtdir*.

İS-lərin göstərilən təhlükəsizliyi *proqram-texniki* və *təşkilati* metodların rasional birləşməsi ilə həyata keçirilir. Tədqiq olunan metoddan asılı olmayaraq təşkilat İS-yə müdaxilə ilə bağlı baş verən hadisənin araşdırılması üçün *əməkdaşların* ayrılmasını və ya *xüsusi qrupun* yaradılmasını təklif edir. İnformasiya

sistemlərinə *müdaxilənin aşkarlanma üsulları* sxematik olaraq şəkil 10-da təsvir edilmişdir.

Müdaxiləni aşkarlamasının ən sadə metodu şübhəli hadisələr və ya İS-nin qeyri adi davranışları barədə istifadəçi hesabatlarını ***passiv gözləməkdir***. Adətən hesabatlarda sistemin cavab vaxtının kəskin şəkildə artdığını, hansısa faylların silindiyini və yaxud verilənlər bazasının əlçatan mümkün sahəsinin olmaması səbəbindən verilənlərin yazılmasının mümkün olmaması barədə məlumatlar verilə bilər. Aydındır ki, belə metod, *yəni passiv gözləmə metodu*,təhlükəsizlik siyasətinin reallaşmasını təmin etmir. Peşəkar təlim görmüş təcavüzkar şübhəli simptomlara səbəb olacaq heç bir şey etməyəcəkdir. Bəlkə də bir müddətdən sonra İS-yə hücum edildiyi məlum olacaq, ancaq təşkilata dəyən zərərin qarşısını almaq və ya əhəmiyyətli dərəcədə azaltmaq çox gec olacaq. Ən pis vəziyyətdə, IS verilənlərinin təhlükəsizliyinin pozulduğuna dair bir siqnal, hüquq-mühafizə orqanları işçilərinin və ya mətbuat nümayəndələrinin təşkilatda görünməsi ola bilər.



Şəkil 10. İnformasiya sistemlərinə müdaxilənin aşkarlanma üsulları

Qeyd edək ki, daha təsirli, eyni zamanda daha bahalı bir üsul, IS-nin normal işləmə rejimi üçün xarakterik olmayan hadisələr barədə məlumatları aşkar

etmək üçün ***jurnalları vaxtaşırı təhlil*** etməkdir.

Belə hadisələ çox hallarda aşağıdakılardan ibarət olur:

- uğursuz audentifikasiya cəhdlərinin çox olması;
- informasiya resursuna daxil olmaq üçün çox sayda uğursuz cəhd (məsələn, VBİS cədvəli).

Bu üsul yoxlama prosedurlarına ciddi riayət etməyi tələb edir. Fəaliyyət qeydləri (audit) alətləri istənilən müasir sənaye səviyyəli VBİS-də qurulur. Ona görə monitorinq vasitələri standart və ya xüsusi prosedurlar əsasında yaradıla bilər. Monitorinq quruluşuna təsadüfi bir elementin daxil edilməsi məsləhət görülür. Təcavüzkarın IS resurslarına hücum etməzdən əvvəl standart yoxlamaların dövülüyünü müəyyənləşdirmək üçün sistemə bir müddət *nəzarət edəcəyini düşünmək* ağlabatandır.

Verilənlərin tamlığının yoxlaması vasitələri bəzi kritik cədvəllər üçün istinad yoxlamaları hesablanması üzərində qurula bilər. Bəzi qaydalara uyğun olaraq dəyişikliklər aşkar edilməsi üçün yoxlama cədvəlləri hesablanır və arayışlarla müqayisə edilir. Yoxlama sənədləri uyğun gəlmirsə, verilənin icazəsiz və ya təsadüfi dəyişikliyi barədə nəticə çıxarılır və müdaxilə qeydiyyatı proseduru başlayır. Bu vasitələr sinfi daha mürəkkəb sistem idarəçiliyini tələb edir. Verilənlərin icazəli dəyişikliyi yoxlamaların yeni hesablanması və onların fiksasiyası ilə müşayiət olunmalıdır. Bu vasitələr sinfi verilənlərin dəyişdirilməsi ilə əlaqəli hücumları aşkarlamaq üçün uğurla istifadə edilə bilər və verilənlərin icazəsiz oxunmasına nəzarət etmək üçün yararsızdır. Bundan başqa, tez-tez dəyişdirilən verilənləri üçün, yoxlama hesablarının hesablanması ilə əlaqəli xərclər qəbuledilməz dərəcədə yüksək ola bilər.

Giriş idarəetmə sistemlərindən gələn həyəcan siqnalları və xəbərdarlıqlar da hücumun başlanması əlamətidir. Girişin idarəetmə sistemi, şəbəkələr arası ekran və uzaqdan istifadəçi girişinə nəzarət sistemləri kimi adətən elə qurulur ki, müəyyən giriş qaydaları pozulduqda həyəcan siqnalları verə bilsin. Bu həyəcan siqnalları elektron poçt və peyjer vasitəsilə göndərilən səsli, vizual mesajlar ola

bilər. Bu mexanizm, tanınmış kanallar vasitəsi ilə həyata keçirilən xaricdən gələn müdaxilələrin qeydinə yönəldilmişdir. Təşkilatın işçiləri tərəfindən müəssisənin kritik informasiya resurslarına icazəsiz girişdə olduğu kimi, gizli və ya naməlum kanallar vasitəsilə xarici şəbəkələrdən daxilolmalar aşkarlanmayacaq.

Real vaxt rejimində *trafik təhlilini* aparan avtomatlaşdırılmış vasitələr dünya bazarında geniş şəkildə təmsil olunur. Bəzən belə sistemlər təşkilatın informasiya resurslarına hücumun əlaməti ola biləcək qeyri adi aktivliyi aşkar etmək üçün ekspert sistemlərilə təchiz olunur. Oxşar vasitələr həm xarici, həm də daxili müdaxilələri aşkar edə bilər. Bu sistemlərin müvəffəqiyyəti *nüfuz əlamətləri* olan hadisələr ardıcıllığının təsvirinin düzgünlüyündən asılıdır. Əgər sistemin parametrləri hadisələrin çox xüsusi bir ardıcıllığı üçün konfiqurasiya olunarsa, onda real hücum edən təcavüzkarın davranışı parametrlərin sazlanmasına uyğun olmaya bilər. Əgər sistemin parametrləri hadisələrin çox ümumi ardıcıllığı üçün konfiqurasiya edilərsə, onda sistem çox güman ki, sistemin rəsmi və ya qeyri-rəsmi bağlanmasına səbəb olacaq bir çox saxta həyəcan siqnalları yaradacaqdır.

Təhlükəsizlik siyasəti sistemə müdaxilə şübhəsi olduqda *hansı cavab tədbirlərini* və onları *kimlərin* qəbul etməli olduğunu dəqiq müəyyənləşdirməlidir. Belə situasiyalarda ediləcək hərəkət qaydasını əvvəlcədən müəyyənləşdirmək və müvafiq sənədlə tərtib etmək lazımdır. İnisializasiya sisteminin işə salınması ilə bağlı qərar verən şəxslərin siyahısı (günün istənilən vaxtı) müəyyənləşdirilməlidir. Həmçinin, əks tədbirlət və hücumun nəticəsinin ləğvi üçün personalların hərəkətlərinin müxtəlif variantların senarisini əvvəlcədən hazırlamaq və sənədləşdirmək də lazımdır. İdeal hal kimi, bu cür hərəkətləri həyata keçirmək üçün personalların məşq etdirilməsinini məsləhət görülür.

Mühüm bir məsələ, hücumun aşkarlandıqdan dərhal sonra təkrarlanacağını və ya sübut toplamaq üçün təcavüzkarın zərərli fəaliyyətini davam etdirib-etməməyini təyin etməkdən ibarətdir.

NƏTİCƏ VƏ TƏKLİFLƏR

Tədqiqat işinin nəticəsi olaraq müəyyən olundu ki, kompüter dövrünün ilk günlərindən etibarən informasiya texnologiyalarını və informasiya sistemlərini yaradanların əsas vəzifələrindən biri *təhlükəsizliyin təmin edilməsi* məsələsi olmuşdur. Heç bir mövcur kommersiya və ya dövlət elektron sistemi öz məlumatlarını icazəsiz girişdən qorunmaq vasitələri olmadan fəaliyyət göstərə bilməz. Artıq XX əsrin 70-ci illərindən başlayaraq dünyada informasiya qorunmasının müxtəlif konsepsiyaları və metodları işlənməyə başlanmışdır ki, bu da qısa müddətdə bu problemə vahid yanaşmanın yaranmasına səbəb olmuş – *ilk təhlükəsizlik siyasəti* işlənib hazırlanmışdır. Bu gün informasiya texnologiyalarının və sistemlərininin təhlükəsizliyinin və etibarlılığının təmin edilməsi sahəsində qanun və qanunverici aktların müddəaları avtomatlaşdırılmış sistemlərdə qorunma mexanizmlərinin üzərinə qoyulan bir sıra tələbləri, demək olar ki, artıq müəyyənləşdirmişdir.

Bununla belə İS-nin proqram təminatının tez-tez yenilənməsi, yeni aparat vasitələrinin tətbiqi və biznes portnyorlar və sonuncu istifadəçilərlə qarşılıqlı əlaqə metodlarının davamlı axtarışı təhlükəsizlik siyasətinin təyini ilə bağlı olaraq təhlükəsizlik modellərinin formalizə olunmasını zəruri etmişdir. Aparılan araşdırmalarin nəticəsi olaraq bu tədqiqat işinində aşağıdakılar müəyyən edilmişdir:

1. İnformasiya sistemlərindən alınan informasiya, təhlükəsizliyinin fundamenti olan *konfidensiallıq*, *tamlıq* və *əl çatanlıq* tələblərını ödəməlidir;

2. Aşkar edilmişdir ki, təflükəsizlik təhdidləri onların *mənbəyinə*, *reallaşma məqsədinə* və informasiya sistemlərinə *təsirinə* görə təsnifatlandırılır;

3. Araşdırmalar əsasında təhlükəsizliyin diskresion ***HRU*** modelinə əsaslanan sistemlərdə *giriş hüquqlarının paylanmasının* qeyri-müəyyənliyi ilə bağlı problemlər, o cümlədən *informasiya axınlarının yaranmasına nəzarətinin* olmaması müəyyən edilmişdir.

4. Müəyyən edilmişdir ki, təhlükəsizliyin ***HRU*** modelinə əsaslanan sistemlərdə daha bir ciddi problem“*Troyan*” proqramının təsiri nəticəsində *təcavüzkar subyektin* yaranmasına nəzarət etmək mümkün deyil.

5. Müəyyən edilmişdir ki, təhlükəsizliyin mandatlı ***Bella-LaPadul*** modeli məlumatların bir istifadəçidən digərinə ötürülməsinə məhdudiyyətlər qoyur ki, bu da “*Trojan atları”* problemini həll edir.

6. Aşkar olunmuşdur ki, təhlükəsizliyin *diskresion* və *mandat* modellərində *təhlükəsizlik siyasətini* əvvəlcədən müəyyənləşdirildiya halda, *rol* modelində təhlükəsizlik siyasəti əvvəlcədən müəyyənləşdirilmir, lakin təşkilatın tələb etdiyi formada konfiqurasiya olunur.

7. Müəyyən olunmuşdur ki, bütün təhlükəsizlik sinifləri icazəsiz girişdən qorunma dərəcəsinə görə dörd qrupda birləşir.

8. Müəyən edilmişdir ki, verilənərin iş nüsxəsi məhv etdikdən sonra sistemi bərpa edilməsi İS adminisratorunun həll etdiyi ən vacib məsələdir ki, bu da fiziki daşıyıcının köçürülməsinin yerinə yetirilməsi və verilənlər bazasının məntiqi boşaldılması yolu ilə həll edilir.

9. Təhlükəsizlik siyasətinin ümumi tərifi verilmiş və onun həyata keçirilməsi üçün təçkilatın qərarlarını təmsil edən sənədlər toplusu sadalanmışdır.

10. Müəyyən edilmişdir ki, İnformasiya sistemi resurslarına çıxış əldə etmək *identifikasiya, audentifikasiya* və *avtorizasiya* kimim üç prosedurun yerinə yetirilməsini əsaslanır.

11. İnformasiya sistemlərinə müdaxilənin aşkarlanmasının əsas üsulları müəyyən olunmuşdur.

İSTİFADƏ OLUNAN ƏDƏBİYYAT

1. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации: Руководящий документ / Гостехкомиссия России. М.: Военное издательство, 1992.

2. Герасименко В. А., Малюк А. А. Основы защиты информации. М.: Инкобук, 1997.

3. Грушо А. А., Тимонина Е. Е. Теоретические основы защиты информации. М.: Яхтсмен, 1996.–192 с.

4. Симонов С. В. Анализ рисков в информационных системах. Практические аспекты // Защита информации. Конфидент 2001,№ 2. С. 48-53.

5. Симонов С. В. Технология аудита информационной безопасности // Защита информации. Конфидент 2002,№ 2. С. 36-41.

6. www.securityauditor.net

7. www.crammusergroup.org.uk

8. Лукацкий А. В. Обнаружение атак. СПб: БХВ - Петербург, 2001.

9. Жилин В. В., Дроздова И. И. Модели безопасности на основе дискреционной политики // Технические науки в России и за рубежом: материалы VII Междунар. науч. конф. (г. Москва, ноябрь 2017 г.). – М.: Буки-Веди, 2017- С. 21-23.

10. Девянин П. Н. Элементы теории ХРУ // Модели безопасности компьютерных систем. – М.: Академия, 2005. –144 с.

11. Девянин П. Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах. Учебное пособие для вузов. – М.: Радио и связь, 2006. – 176 с.

12. Гаценко О. Ю. Защита информации. Основы организационного управления– СПб: Сентябрь, 2001. – 228 с.

13. https://moluch.ru/conf/tech/archive/286/13234/

14. http://csaa.ru/ponjatie-bezopasnosti-informacionnyh-sistem/

15. http://ssofta.narod.ru/admis/1.htm

16. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей. Учебное пособие – М.: ИД «ФОРУМ»: ИНФРА-М, 2009. – 416 с.

17. Гайдамакин Н. А. Теоретические основы компьютерной безопасности. Учебное пособие – Екатеринбург: изд-во Уральского университета, 2008. – 212 с.

18. Куликов С. С. Модели безопасности компьютерных систем. Учебное пособие для вузов. Воронеж: ФГБОУ ВПО «Воронежский государственный технический университет», 2015.- 179с.

19. https://studfile.net/preview/2880350/page:5/

20. Девянин П. Н. Элементы теории ХРУ // Модели безопасности компьютерных систем. – М.: Академия, 2005. –144 с.

21. Прокопьев И. В., Введение в теоретические основы компьютерной безопасности: учебное пособие – М.: МИЭМ, 1998. –184 с.

22. https://www.intuit.ru/studies/courses/14250/1286/lecture/24236

23. Креопалов В. В. Технические средства и методы защиты информации: учеб. – практ. пособие. – М.: Евразийский открытый институт, 2011. – 278 с.

24. http://db4.sbras.ru/elbib/data/show page.phtml?13+1736

25. Ravi S. Sandhu, Pierangela Samarati: Access Control: Principles and Practice. IEEE Comunication Magazine 1994.

26. Osborn, S., Sandhu, R., and Nunawer, Q. Configuring Role-Based Access Control To Enforce Mandatory And Discretionary Access Control Policies. ACM Trans. Info. Syst. Security, 3, 2, 2000.

РЕЗЮМЕ

Диссертация состоит из 68 страниц, содержит 10 рисунков и список литературы, состоящий из 26 наименований.

Во введение работы определяется актуальность темы, дается краткое информация о проблеме, целях исследовательской работы и основных задачах.

В первой главе диссертации анализируются некоторые проблемы информационной безопасности. Эта глава состоит из двух параграфов. В первом параграфе представлена концепция безопасности и, среди прочих факторов, показано влияние стихийных бедствий на плохо защищенные данные. Во втором параграфе показывается необходимость создания программных средств для обеспечения безопасности данных и важность свойств *конфиденциальности*, *полноты* и *доступности* информации.

Во второй главе работы рассматриваются основные источники и характеристики безопасности. Эта глава состоит из четырех параграфов. В первом параграфе изложено основное назначение политики безопасности и ее описание в форме формальной модели. Оказалось, что, в отличие от ролевых моделей в классических базовых моделях безопасности данных, политика безопасности определяется заранее, хотя дискреционная модель Харрисона - Руззо - Ульмана чувствительна к программе «троянский конь» в модели учетных данных Белла-ЛаПадуллы., которая используется в военной промышленности, не имеет этой проблемы. В третьем параграфе этой главы рассматриваются организационные, технические и программные аспекты безопасности данных, в частности, требования, изложенные в «Оранжевой книге», и другие методологические стандарты безопасности. Наконец, в последнем параграфе рассматриваются основные методы и средства восстановления и тиражирования информационных систем.

Эта глава также состоит из четырех параграфов, как и вторая глава. В первом параграфе изложены основные разделы руководящих принципов

компьютерной безопасности, разрабо-танных Национальным институтом стандартов и технологий США, включая тему политики безопасности, описание позиции организации, ее реали-зации, ролей и обязанностей. Во втором параграфе обсуждаются технологии *идентификации* и *аутентификации*. Отмечено, что доступ к ресурсам ин-формационной системы основан на трех процедурах, таких как иденти-фикация, аутентификация и авторизация. В третьем параграфе рассматри-ваются виды нарушений штатного режима информационных систем. Наконец, в последнем параграфе обсуждаются проблемы, связанные с вы-явлением вмешательства и устранением его негативных последствий.

SUMMARY

The dissertation consists of 68 pages, contains 10 figures and a list of references, consisting of 26 items.

The introduction of the work defines the relevance of the topic, gives brief information about the problem, the objectives of the research work and the main tasks that arose**.**

The first chapter of the dissertation analyzes some problems of information security. This chapter consists of two sections. The first paragraph presents the concept of security and, among other factors, shows the impact of natural disasters on poorly protected data. The second paragraph shows the need to create software tools for data security and the importance of the properties of confidentiality, completeness and accessibility of information.

The second chapter of the work discusses the main sources and characteristics of safety. This chapter is divided into four sections. The first paragraph sets out the main purpose of the security policy and its description in the form of a formal model. It turned out that, in contrast to the role models in the classic basic data security models, the security policy is determined in advance, although the Harrison-Ruzzo-Ullman discretionary model is sensitive to the Trojan horse program in the Bell-LaPadulla credential model used in the military industry does not have this problem. The third paragraph of this chapter discusses the organizational, technical and programmatic aspects of data security, in parti-cular, the requirements set forth in the Orange Book and other methodological security standards. Finally, the last paragraph discusses the basic methods and means of restoring and replicating information systems.

The third chapter of the dissertation discusses issues related to the creation of a controlling environment. This chapter also has four chapters, as does the second chapter. The first paragraph outlines the main sections on the computer security guidelines developed by the US National Institute of Standards and Technology, including the topic of security policy, a description of the

organizations position, implementation, roles and responsibilities. The second paragraph discusses identification and authentication technologies. It is noted that access to information system resources is based on three procedures, such as identification, authentication and authorization. The third paragraph discusses the types of violations of the regular regime of information systems. Finally, the last paragraph discusses the problems associated with identifying an intervention and eliminating its negative effects.