X.İ.Abdullayev N.T.Nağıyev R.M.Muxtarov

Müəssisənin informasiya təhlükəsizliyi

AZƏRBAYCAN RESPUBLİKASI TƏHSİL NAZİRLİYİ
"AZƏRBAYCAN HAVA YOLLARI" QSC
MİLLİ AVİASİYA AKADEMİYASI

MÜƏSSİSƏNİN İNFORMASİYA TƏHLÜKƏSİZLİYİ

Dərslik

Milli Aviasiya Akademiyası
Elmi-Metodiki Şurasının
19.12.2018-ci il tarixli iclasının
qərarı ilə (protokol 11/18)
çapına icazə verilmişdir.

Bakı – 2019

Müəlliflər: **X.İ.Abdullayev, N.T.Nağıyev, R.M.Muxtarov**

Rəy verənlər: **H.B. Babayev**Milli Aviasiya Akademiyasının Aeronaviqasiya kafedrasının müdiri, t.f.d., dosent

M.H. Həsənov Azərbaycan Texniki Universitetinin Telekommunikasiya sistemləri və informasiya təhlükəsizliyi kafedrasının müdiri, t.f.d., dosent

Elmi redaktor: **İ.M. İsmayılov**Milli Aviasiya Akademiyasının Aerokosmik informasiya sistemləri kafedrasının professoru, t.e.d., AMEA-nın müxbir üzvü

X.İ.Abdullayev, N.T.Nağıyev, R.M.Muxtarov. Müəssisənin informasiya təhlükəsizliyi /Dərslik. – Bakı, MAA-nın Poliqrafiya Mərkəzi. 2019, – 270 səh.

Dərslik Milli Aviaisya Akademiyasında bakalavriat səviyyəsində Hava nəqliyyatında texnoloji proseslərin və istehsalatın təhlükəsizliyi mühəndisliyi ixtisasının tədris planında yer alan Mülki aviasiyada informasiya təhlükəsizliyi fənninin proqramı əsasında tərtib edilmişdir.

Kitabda sistem yanaşma əsasında müəssisənin informasiya təhlükəsizliyi məsələlərinə, informasiya təhlükəsizliyinin təmini prinsiplərinə baxılmış, informasiyaya olan təhlükələrin təsnifatı, xarakteristikaları, onlarla mübarizə üsulları təqdim edilmişdir.

Dərslik ilk növbədə ali təhsil müəssisələrinin tələbələri üçün nəzərdə tutulsa da, ondan müəssisələrdə informasiya proseslərinin təhlükəsizliyinin təmini ilə məşğul olan mütəxəssislər də istifadə edə bilər.

MÜNDƏRİCAT

GİRİŞ

Hal hazırda müasir cəmiyyətdə informasiya strateji resurs hesab olunur. İnformasiyalaşdırmanın təsiri altında cəmiyyətin bütün sahələri genişmiqyaslılıq, çeviklik, müntəzəmlik kimi yeni keyfiyyətlər əldə edirlər. Lakin eyni zamanda ictimai proseslərin informasiya təsirindən potensial asılılığı da artmağa başlayır, bu da informasiyaya ünvanlanan hədələrin, təhlükələrin sayının artmasına səbəb olur.

Müəssisənin təhlükəsizliyinin təmin olunması sisteminin tərkib hissəsi olan informasiya təhlükəsizliyi son zamanlar mövcud problemlərə görə daha prioritet məsələyə çevrilmişdir.

Müəssisənin informasiya təhlükəsizliyi – zəruri informasiyaların əldə edilməsi, emalı, istifadəsi və digər proseslərdə onların icazəsiz girişdən, dağıdılmadan, həmçinin dəyişdirilmədən qorunması üçün mühafizəsinin təmin olunmasıdır. İnformasiyanın kompleks təhlükəsizliyinin təmin edilməsinin əsas məqsədi müəssisənin informasiya sisteminin tamlığının və bütövlüyünün saxlanması, informasiyanın dəyişdirilməsi və dağıdılmasının minimallaşdırılması, informasiyanın açıqlanması və sızması hallarının qarşısının alınmasıdır.

Beynəlxalq Mülki Aviasiya Təşkilatı (İCAO) artıq tez-tez mülki aviasiya obyektlərinin informasiya təhlükəsizliyi məsələlərinin həllinə yönəldilmiş müəyyən təşəbbüslərlə çıxış edir.

Hesablamalara əsasən söyləyə bilərik ki, mülki aviasiyanın da informasiya təhlükəsizliyinə ünvanlanmış hədələrin sayı artma tendensiyasına malikdir.

Bu göstərilənlər informasiya təhlükəsizliyinin təmin edilməsi sisteminin təkmilləşdirilməsinə və möhkəmləndirilməsinə ehtiyac olduğunu təsdiq edir. Belə ki, yarana biləcək problemləri həll etmək və informasiyanın

mühafizəsində maksimal səmərəliliyə nail olmaq imkanına malik, etibarlı prinsiplərə söykənmək vacibdir.

Müəssisənin təhlükəsizliyinin təmin olunmasının əsas prinsiplərindən biri obyektlərin informasiya təhlükəsizliyi sisteminin fasiləsiz olaraq təkmilləşdirilməsi və inkişaf etdirilməsi prinsipidir. Bu prinsipin əsas mahiyyəti informasiyaların mühafizə edilməsi sistemindəki zəif nöqtələrin, o cümlədən potensial sızma kanallarının üzə çıxarılmasına, hədə və risklərin dərəcələri və xarakterlərindən asılı olaraq informasiyanın qorunması mexanizmlərinin işlənməsi və yenilənməsinə əsaslanır. Faktiki olaraq, bu prinsip uzunmüddətli olmaqla, informasiya təhlükəsizliyinin təmin edilməsinə yönəlmiş bu və ya digər fəaliyyətin daimiliyini nəzərdə tutur.

Kompleks yanaşma prinsipi istehsalat prosesinin müxtəlif mərhələlərində müəssisədə informasiyanın qorunmasının bütün üsullarından, vasitələrindən və qüvvələrindən istifadəsini nəzərdə tutur.

Həmçinin qeyd etmək lazımdır ki, informasiya təhlükəsizliyinin səmərəli təmin edilməsi informasiya təhlükəsizliyinin təşkilinin vahid mexaniki sistemi mövcud olduğu halda reallaşa bilər. Bundan başqa, belə sistemin mövcudluğu bütün qüvvə və vasitələrin səmərəli idarə edilməsi informasiyanın və informasiya resurslarının mühafizəsini daha etibarlı təmin etməyə imkan verir.

Müəssisə obyektlərinin informasiya təhlükəsizliyi sistemi informasiyanın qeyri-qanuni girişdən etibarlı qorunmasını təmin edən orqanların, vasitələrin, üsulların və tədbirlərin mütəşəkkil məcmusudur.

Bundan başqa qanunilik prinsipinə ciddi əməl olunması, inzibati idarəetmə funksiyalarının tamlığı, şəxslərin, cəmiyyətin və dövlətin maraqlarının qorunması, informasiya təhlükəsizliyinə cavabdeh olan əməkdaşların peşəkarlığı

informasiya təhlükəsizliyinin təmin edilməsinin əsas istiqamətlərindəndir.

Bütün bu şərtlərə əməl olunmadan informasiya təhlükəsizliyi sisteminin potensial və real təhlükələrdən qorunmasını təmin etmək olduqca çətindir.

Bununla bərabər, qeyd olunan prinsiplərin reallaşdırılması üçün sistemli yanaşma mövqeyindən informasiyanın mühafizə edilməsi müəyyən tələblərə cavab verməlidir.

İnformasiya təhlükəsizliyi tədbirlərinin planlaşdırılması müəssisənin fəaliyyətini təmin edən bütün səlahiyyətli orqanların qarşılıqlı əlaqəsinin təşkili üçün vacibdir. İnformasiya resurslarının mühafizəsi konkret və məqsədyönlü olmalıdır. İnformasiya təhlükəsizliyinin təmin edilməsi tədbirləri informasiya sızmasının mümkün kanallarının və icazəsiz girişin müxtəlif cəhdlərini qabaqlamalıdır.

Bununla yanaşı mülki aviasiya obyektlərinin informasiya təhlükəsizliyinin təmin edilməsi sistemi iqtisadi baxımdan səmərəli olmalıdır.

Mülki aviasiya obyektlərinin informasiya təhlükəsizliyinin əsas tələbləri ilə yanaşı mühafizə vasitələrinin texniki cəhətdən sadə, istifadəçilər üçün aydın olması, istifadəçinin minimal imtiyazlara malik olması, informasiya təhlükəsizliyi sisteminin daimi fəaliyyətdə olması, mühafizə tədbirlərinin konfidensiallığının təmin olunması tövsiyə edilir.

1. İnformasiya təhlükəsizliyinin nəzəri məsələləri

1.1. İnformasiya anlayışı və onun növləri

İnsan hər gün müxtəlif tipli yeni informasiya əldə edir və emal edir, hər saat, hər dəqiqə, hər saniyə məlumat qəbul edib ötürür, hər an informasiya ilə işləyir. Beynəlxalq sistemin hər bir subyekti öz fəaliyyətində çoxsaylı informasiyalar toplusundan istifadə edir. "İnformasiya" - latın sözü olan "informatio" sözündən yaranmış, tərcümədə "məlumatlandırma, izah etmə" mənasını verir.

Əvvəllər informasiya dedikdə insanlar tərəfindən şifahi, yazılı və ya digər üsullarla (əyani siqnallar, texniki vasitələr və s.) ötürülən obyektiv reallıq haqqında istənilən məlumatlar başa düşülürdü.

XX əsrin ortalarından başlayaraq informasiya ümumi elmi anlayış kimi qəbul edilir: buraya – insanlar arasında, insanla texniki vasitə arasında, texniki vasitələrin qarşılıqlı əlaqələrində məlumat mübadiləsi, heyvanlar və bitkilər aləmində siqnallar mübadiləsi; hüceyrədən hüceyrəyə, orqanizmdən orqanizmə əlaqələrin ötürülməsi və s. daxildir.

Hal-hazırda "informasiya" sözünün vahid bir tərifi mövcud deyil. Ədəbiyyatlarda "informasiya" terminini əks etdirən, həmin anlayışı müxtəlif yanaşmalarla izah edən fərqli fikirlər çoxdur. "İnformasiya, informasiyalaşdırma vəinformasiyanın mühafizəsi haqqında" Azərbaycan Respublikasinin Qanununda bu termin aşağıdakı kimi təyin edilir: informasiya - yaranma tarixindən, təqdimat formasından və təsnifatından asılı olmayaraq istənilən fəaliyyət nəticəsində yaradılan, yaxud əldə olunan faktlar, rəylər, bilgilər, xəbərlər və ya digər xarakterli məlumatlardır.

İnformasiya və onun xüsusiyyətləri bir sıra elm sahələrinin tədqiqat obyektidir, onların arasında məlumat nəzəriyyəsi (informasiyanın ötürülməsinin riyazi nəzəriyyəsi),

kibernetika (maşınlarda və heyvanlarda, həmçinin cəmiyyətdə və insan varlıqlarında əlaqə və idarə etmə haqqında elm), semiotika (nişanlar və nişan sistemləri haqqında elm), kütləvi əlaqə nəzəriyyəsi (kütləvi informasiya vasitələrinin və onların cəmiyyətə təsirinin tədqiqi), informatika (bütün növ informasiyanın yığılması, dəyişdirilməsi, saxlanması, mühafizəsi, axtarışı, ötürülməsi və emalı proseslərinin öyrənilməsi) və başqalarını göstərmək olar.

İnformasiyanı müxtəlif cür təsnif etmək mümkündür. Ümumi olaraq, qəbul edilmə üsuluna görə məlumatlar aşağıdakı kimi təsnif olunur:

- Vizual – görmə orqanları ilə qəbul edilir;
- Audio – eşitmə orqanları ilə qəbul edilir;
- Təmaslı – toxunma (təmas) reseptorları ilə qəbul edilir;
- Qoxulu – iybilmə orqanları ilə qəbul edilir;
- Dadlı – dadbilmə orqanları ilə qəbul edilir.

Təqdim etmə formasına görə informasiyanın əsas növləri aşağıdakılardır:

- Mətn – insan nitqinin xüsusi simvollarla – hərflərlə kodlaşdırılması üsulu, müxtəlif xalqlar nitqi ifadə etmək üçün fərqli dillərdən və hərf toplularından istifadə edirlər;
- Rəqəmli – riyazi əməliyyatlar üçün nəzərdə tutulan rəqəm və işarələrdir, ticarətin, iqtisadiyyatın və pul dövriyyəsinin inkişafı ilə daha da əhəmiyyət kəsb edir; mətn informasiyasına uyğun olaraq onu ifadə etmək üçün xüsusi simvollarla – rəqəmlərlə kodlaşdırma üsullarından istifadə olunur;
- Qrafik – real dünyanın şəkillərini təsvir edən kağızda, kətanda, mərmərdə və digər materiallar üzərində çəkilən şəkil, qrafik, foto, sxem şəklində ötürülür;
- Səsli – şifahi və səs yazısı şəklində ötürülür; bizim ətrafımızda çoxlu səslər var, onların saxlanılması və yayılması

üsulu 1877-ci ildə səsyazan qurğunun kəşfi ilə həll olundu. Hal-hazırda qrafik məlumatlarda olduğu kimi səsli informasiya xüsusi simvolların kodlaşdırılması üsulu ilə emal olunur.

- Video məlumat – video yazı formasında ötürülür; kinonun ixtira edilməsi ilə yaranan ətraf mühitin "canlı" şəkillərinin qorunması üsuludur.

Təyinatına görə də məlumatları qruplara bölmək mümkündür:

- Kütləvi – tərkibində ümumi anlayışlar olan və cəmiyyətin çox hissəsinə bəlli məlumatlar;
- Xüsusi – tərkibində səciyyəvi anlayışlar olan, cəmiyyətin çox hissəsinə bəlli olmayan, lakin müəyyən qrup insanlara zəruri məlumatlar;
- Gizli – müəyyən qrup insanlara aid olan, bağlı və mühafizə olunan kanallarla ötürülən məlumatlar;
- Şəxsi (fərdi) – hər hansı bir şəxsə aid olan məlumatlar.

1.2. İnformasiyanın xüsusiyyətləri

Hər bir obyekt kimi, informasiya da xarakterik xüsusiyyətlərə malikdir. İnformasiyanı təbiətin və cəmiyyətin digər obyektlərindən fərqləndirən xarakterik xüsusiyyətlər kimi aşağıda qeyd olunanları göstərə bilərik: obyektivlik, etibarlılıq, bütövlük, dəqiqlik, aktuallıq, faydalılıq, dəyərlilik, vaxtında olma, aydınlıq, mümkünlük, qısalıq və s.

1. *İnformasiyanın obyektivliyi.* İnformasiyanın obyektivliyi nisbi anlayışdır. Obyektivlik – hər hansı bir varlığı əks etdirən elə məlumatlardır ki, onun aid olduğu mövcud parametrlərə uyğunluq göstəricisi kimi çıxış edir. Eyni bir əşya, hadisə, incəsənət əsəri, təbii varlıq, elmi-təcrübi proseslər, və s. barədə müxtəlif insanların müxtəlif fərqli fikirləri ola bilər. Həqiqətlər bilərəkdən və ya bilməyərəkdən, təcrübəsizlikdən, savadsızlıqdan, hər-hansı bir mənafe xatirinə və digər

səbəblərdən düzgün qiymətləndirilməyə və ya təhrif oluna bilər. İnformasiya – xarici obyektiv dünyanın əks edilməsidir. İnformasiya – onun təsbiti üsullarından, kiminsə fikrindən asılı deyilsə – obyektivdir.

Məsələn, iki anlayışı - informasiya və enerjini (istiliyi) müqayisə edək. İki müxtəlif şəxsdən içəridəki havanın temperaturunu qiymətləndirməyi xahiş etsək, onlardan biri havanın isti olduğunu, digəri isə havanın onun üçün normal olduğunu və onu narahat etmədiyini deyə bilər. İçəridəki temperatur haqqında insanların fikirləri subyektivdir. Əgər cihazın köməyi ilə temperaturu ölçsək (bizim halda hərarəti ölçən cihaz ilə), bu zaman biz obyektiv qiymət alacağıq, bu qiymət heç kimin fikrindən asılı olmayacaqdır.

Obyektiv informasiyanı, məsələn, işlək, saz vəziyyətdə olan vericilərin, ölçü cihazlarının köməyi ilə almaq olar. Müəyyən insanın şüurunda əks olunaraq informasiya obyektivliyini itirir, artıq konkret subyektin fikrindən, təcrübəsindən, biliklərindən, mülahizəsindən (çox və ya az miqdarda) asılı olaraq dəyişir.

2. *İnformasiyanın etibarlılığı* - qarşıya qoyulan məqsədə nail olmaq üçün bilavasitə tələb olunan informasiyanın səhvlərdən və qərəzdən azad olma səviyyəsini müəyyənləşdirir. Əgər informasiya işlərin həqiqi vəziyyətini əks etdirirsə, o, etibarlıdır. Obyektiv informasiya həmişə etibarlıdır, amma etibarlı məlumat həm obyektiv, həm də subyektiv ola bilər. Etibarlı məlumat bizə düzgün qərarı qəbul etməyə kömək edir.

Etibarlı olmayan informasiya aşağıdakı səbəblərdən ola bilər:

- qəsdən təhrif edilmə (dezinformasiya) və ya bilməyərəkdən təhrif edilmə - subyektiv fikrin nəticəsi;
- maneələrin təsiri nəticəsində və ya kifayət qədər dəqiq olmayan qəbul vasitələri səbəbindən yaranan təhrif edilmə.

3. *İnformasiyanın əlyetənliyi* - bu və ya digər informasiyanı əldə etmək imkanının ölçüsüdür.İnformasiyanın əlyetənliyi dedikdə, həmçinin informasiya proseslərinin istənilən mərhələsində mühafizənin etibarlılığının təmin olunması ilə bərabər, istifadəsinin də sadə və geniş imkanlara malik olması başa düşülür.

4. *İnformasiyanın tamlığı*. Hər-hansı bir obyekti (varlığı) xarakterizə edən informasiyanın tamlığı obyektin (varlığın) malik olduğu parametrləri (və ya tərkibi) hərtərəfli əks etdirməsi deməkdir. Əgər informasiya başa düşülmək və qərar qəbul etmək üçün kifayət edirsə, informasiyanı tam adlandırmaq olar. Natamam informasiya səhv nəticəyə və ya qərara gətirib çıxara bilər.

5. *İnformasiyanın dəqiqliyi (adekvatlığı)* - obyektə (varlığa) məxsus olan və onu tam, düzgün xarakterizə edən parametrlərin, xüsusiyyətlərin istisnasız qiymətləndirilməsidir. Bu meyar obyektin, prosesin, hadisələrin və s. real vəziyyətinə yaxınlıq dərəcəsi ilə müəyyən edilir, real, obyektiv vəziyyətə uyğunluğun dərəcəsini xarakterizə edir. Qeyri-adekvat informasiya natamam və ya mötəbər (etibarlı) olmayan məlumatlar əsasında yeni informasiyanın yaradılması zamanı meydana çıxa bilər.

Etibarlı məlumatlar + qeyri-adekvat metodlar = qeyri-adekvat informasiya.

6. *İnformasiyanın aktuallığı* – onun mövcud zamanda əhəmiyyətliliyi, maraqlılığı, zəruriliyidir. Yalnız vaxtında əldə edilmiş informasiya faydalı ola bilər. Köhnəlmiş, qeyri-adekvat informasiya aktual deyildir.

7. *İnformasiyanın faydalılığı (dəyəri)* – konkret məqam üçün yararlı olma dərəcəsini göstərir. Faydalı informasiya - məqsədə çatmaq üçün istifadəsi zəruri olan, nəticələrin əldə olunmasında mühüm əhəmiyyət kəsb edən və əldə olunması mümkün olan informasiyadır.

Ən qiymətli informasiya – obyektiv, etibarlı, tam, dəqiq, məqsədə çatmaq üçün zəruri olmaqla bərabər, bu şərtləri ödəyən, əlçatan və aktual olandır. Bu halda nəzərə almaq lazımdır ki, qeyri-obyektiv, mötəbər olmayan informasiya da (məsələn, bədii ədəbiyyat), insan üçün böyük əhəmiyyətə malikdir.

Vaxt ötdükcə informasiyanın miqdarı artır, informasiya yığılır, onun sistemləşdirməsi, qiymətləndirilməsi və ümumiləşdirməsi baş verir. Bu növ xüsusiyyətləri informasiyanın artması və akkumulyasiyası adlandırmağa başladılar.

İnformasiyanın qocalması dedikdə, zaman ötdükcə onun dəyərinin azalması, aktuallığının itirilməsi kimi başa düşülür. Bu baxımdan informasiyanı zamanın deyil, əvvəlki məlumatları daha da dəqiqləşdirən, müasir tələblərə uyğunlaşdıran yeni üsullar, metodlar və vasitələrin tətbiqi ilə əldə olunan yeni informasiyanın meydana çıxması qocaldır. Məlumdur ki, elmi-texniki informasiya daha sürətli, estetik informasiyalar (incəsənət əsərləri) isə daha yavaş qocalır. Cəmiyyətdə müxtəlif sahələrdə mövcud olan informasiyalar -tarixi hadisələr, təbiət hadisələri, çoxsaylı elmlərə aid informasiyalar, incəsənət, bədii, dini və s. bu kimi informasiyalar heç vaxt qocalmır və aktuallığını itirmir.

1.3. İnformasiya təhlükəsizliyi sistemi

«İnformasiya» anlayışından müasir dövrdə geniş və hərtərəfli istifadə olunur. Bu anlayışdan istifadə edilməyən bilik sahəsini tapmaq qeyri-mümkündür. Elmi biliyin, informasiyanın həcmi, mütəxəssislərin hesablamalarına görə, hər 5 ildə 2 dəfə artır. Bu, XXI əsrin informasiya əsri olduğu deməkdir.

Əsaslı olaraq belə bir sual yaranır – informasiya nədir? İnformasiya – yaranma tarixindən, təqdimat formasından və təsnifatından asılı olmayaraq, istənilən fəaliyyət nəticəsində

yaradılan, yaxud əldə olunan faktlar, rəylər, bilgilər, xəbərlər və ya digər xarakterli məlumatlardır. Bu da məlumdur ki, informasiya – şəxslər, predmetlər, faktlar, hadisələr və proseslər haqqında məlumatdır. İnformasiya – kompüterə daxil edilmiş məlumatlar, məktublar və ya yaddaş qeydləri, düsturlar, rəsmlər, diaqramlar, modellər, dissertasiyalar, məhkəmə sənədləri və s. daxil olmaqla, müxtəlif formaya malik ola bilər.

İnformasiya hər bir kəsə, onun cəmiyyətdə mövcud olması, fəaliyyət göstərməsi, yaşaması, inkişaf etməsi üçün lazımdır. Bu səbəbdən, digər həyat fəaliyyəti üçün gərəkli olan elementlər kimi informasiya da mühafizə olunmalıdır.

Məxfi, konfidensial, şəxsi informasiyaların mühafizəsi istehsalat və xidmət sahələrində uğurla fəaliyyət göstərməyə, şəxsi həyatını təhlükəsiz və uğurla yaşamağa köməklik göstərir.

Vəziyyətin təhlili göstərir ki, informasiya təhlükəsizliyinin təmin edilməsi sahəsində mühafizənin formalaşmış konsepsiyası və strukturu mövcuddur. İnformasiyanın mühafizəsinin əsas şərti aşağıdakılardan ibarətdir:

- İnformasiyanın mühafizə edilməsi üçün texniki vasitələrin tətbiq edilməsi;
- İnformasiyanın mühafizə edilməsi məsələlərinin həllində ixtisaslaşmış təşkilat və ya qurumların yaradılması;
- İnformasiyanın mühafizə probleminin həllində müxtəlif sistemlərin mövcudluğu;
- İnformasiyaların mühafizə edilməsində qabaqcıl təcrübənin tətbiqi və təcrübənin müntəzəm olaraq artırılması və s.

Bütün növ informasiyaların mühafizə edilməsi sahəsində müxtəlif hüquqi, texniki, təşkilati, profilaktik

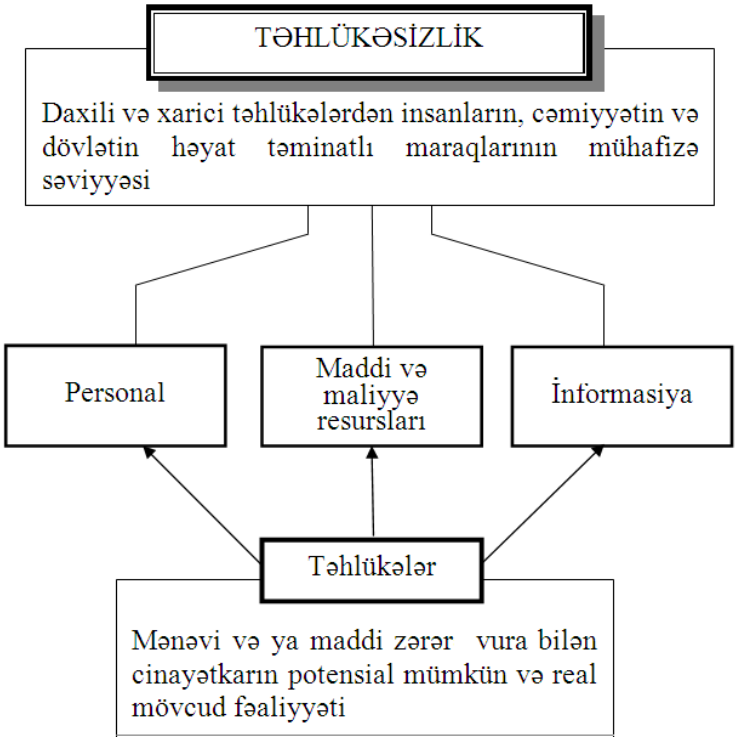
tədbirlərin görülməsinə baxmayaraq, informasiya ilə əlaqəli cinayət hadisələrinin sayı artır və onun əhatə etdiyi sahələr geniş-lənməkdə davam edir. Təcrübə göstərir ki, bu tendensiyanın qarşısının alınması üçün informasiya resurslarının müdafiəsi prosesini ciddi və məqsədyönlü formada təşkil etmək, real şəraitə uyğun praktiki, texniki və nəzarət tədbirlərini həyata keçirmək lazımdır. İnformasiyanın mühafizəsinin təmin olun-ması informasiya proseslərində iştirak edən hər bir hüquqi və fiziki şəxsin peşəkarlığından, məsuliyyətindən və bu sahədə texniki təminatın zəruri tələblərə uyğun olmasından çox asılıdır. İnformasiyaların mühafizəsi prosesinin səmərəli təmin edilməsi üçün informasiya proseslərinin ünvanına yönələn bütün növ hədələr, bu sahədəki cinayətkarlıq, o cümlədən, kibercinayət və kiberterrorçuluq aktlarının əhatəli təhlili əsa-sında zəruri normativ hüquqi sənədlərin, təşkilati və texniki normaların müəyyən edilməsi və bu prosesin bütün subyektlərinin məsuliyyəti müəyyənləşdirilməli, bu sahədə peşəkar kadrların hazırlanması təmin olunmalıdır.

Təcrübə həmçinin göstərir ki:

- İnformasiya təhlükəsizliyinin təmin edilməsinin təşkili məsələləri birdəfəlik akt olmayıb, informasiyaların mü-hafizəsi sisteminin inkişaf etdirilməsi üsullarının, yollarının tətbiqi, onun vəziyyətinə nəzarətin həyata keçirilməsini, həssas, zəif yerlərinin və qeyri-qanuni müdaxilələrin aşkar edilməsini özündə birləşdirən fasiləsiz prosesdir.
- İnformasiya təhlükəsizliyi istehsal sistemlərinin bütün struktur elementlərində və informasiyanın emalı üzrə texnoloji prosesin mərhələlərində, müdafiə vasitələrindən kompleks istifadə zamanı təmin oluna bilər. Təcrübə göstərir ki, yalnız istifadə olunan vasitələr, üsullar və tədbirlər bütöv bir mexanizmdə - İnformasiyanın Mühafizəsi Sisteminə

(İMS) birləşdikdə yüksək key-fiyyət almaq mümkündür. Bununla belə, daxili və xarici şərtlərin dəyişməsindən asılı olaraq fəaliyyətdə olan sistemlər nəzarətdə saxlanmalı, yenilənməli və inkişaf etdirilməlidir.

- İstifadəçilər hazırlığa malik olmadan və müdafiəyə yönəlmiş bütün təyin olunan qaydalara riayət etmədən heç bir İnformasiyanın Mühafizəsi Sistemi tələb olunan təhlükəsizlik səviyyəsini təmin edə bilməz (şəkil 1.1).



Şəkil 1.1. Müəssisənin fəaliyyətinə yönəlik hədə ünvanları

İnformasiyanın Mühafizəsi Sistemi - informasiyaların bütün növ daxili və xarici təhlükələrdən müdafiəsini təmin edən xüsusi orqanların, vasitələrin, üsulların və tədbirlərin mütəşəkkil birləşmiş kompleksi kimi qəbul edilir. İnformasiyanın mühafizəsinin sistem yanaşmasına xüsusi tələblər mövcuddur. İnformasiyanın mühafizəsi aşağıdakı prinsiplər əsasında qurulmalıdır.

- ***Fasiləsiz.*** Zamanın istənilən anında informasiyalar üsul və vasitələrlə daimi formada mühafizə edilməlidir. Bu onunla əlaqədardır ki, cinayətkarlar onları maraqlandıran informasiyanın müdafiəsini yarmağa daim imkan axtarırlar;
- ***Planlı.*** Müəssisənin (təşkilatın) ümumi məqsədini nəzərə alaraq, informasiyanın mühafizəsi hər bir xidmət tərəfindən hazırlanan plan üzrə həyata keçirilməlidir. Bu məqsədlərə informasiyaların növləri, onların məxfilik səviyyəsi, dövlətin və ya ayrı-ayrı subyektlərin təhlükəsizliyinin təmin edilməsi siyasəti, informasiyalara qarşı yönələn hədələrin səviyyəsi, mühafizə edən qüvvə və vasitələrin nəzərə alınması aid edilə bilər;
- ***Konkret (ünvanlı).*** Bütün informasiya deyil, yalnız itirilməsi təşkilata müəyyən zərər yetirə biləcək konkret informasiyalar mühafizə olunmalıdır. Dövlətin və dövlət əhəmiyyətli işlərin həyata keçirilməsində xüsusi maraq kəsb edən informasiyaların mühafizəsinin gücləndirilməsi prioritet məsələ olmalıdır;
- ***Aktiv.*** İnformasiyanı xüsusi fəallıqla mühafizə etmək lazımdır;
- ***Etibarlı.*** Mühafizənin üsul və növləri qorunan sirlərə mümkün qeyri-qanuni müdaxilə yollarının qarşısını etibarlı almalıdır;
- ***Universal.*** Hesab olunur ki, istənilən yerdə, istənilən vasitə ilə, informasiyanın xarakterindən, formasından və növündən asılı olmayaraq, qeyri-qanuni müdaxilələrdən qoruna biləndir.

➢ ***Kompleks.*** İnformasiyanın mühafizəsi üçün struktur elementlərin bütün növ mühafizə üsulları tam həcmdə tətbiq olunmalıdır. Texniki vasitələr və formalar ayrı-ayrılıqda tətbiq olunmamalıdır. Müdafiə kəsilməz, bir-biri ilə əlaqəli və bir-birindən asılı proseslərdən ibarət mürəkkəb sistem olduğu üçün bu sistem kompleks halda həyata keçirilməlidir.

Bu komplekstəhlükəsizlik tələblərini təmin etmək üçün İnformasiyanın Mühafizəsi Sistemi müəyyən şərtlərə cavab verməlidir, yəni:

- İnformasiya fəaliyyətinin bütün texnoloji kompleksini əhatə etməli;
- İstifadə edilən vasitələr müxtəlif növlü olmalı;
- İnformasiya təhlükəsizliyi üzrə tədbirlərin dəyişdirilməsi və əlavələr edilməsi üçün açıq olmalı;
- Qeyri-standart və müxtəlif tipli olmalı. Müdafiə vasitələrini seçərkən cinayətkarların imkanları haqqında məlumatlı olmalı;
- Texniki xidmət üçün sadə, istifadəçilərin yararlanması üçün isə rahat olmalı;
- Etibarlı olmalı. İnformasiyanın yayılma kanallarının yaranmasına səbəb ola bilən texniki vasitələrin istənilən qüsurlarının düzəldilməsi;
- Sistemin hər hansı bir hissəsinə xəbərsiz yaxınlaşmağın mümkün olmaması üçün bütöv, komplekssşəkildə olmalı.

İnformasiyanın Mühafizəsi Sisteminə həmçinin müəyyən tələblər irəli sürülə bilər:

- Müəyyən növ informasiyanı əldə etmək üçün istifadəçilərin hüquq və vəzifələri dəqiq müəyyən edilməli;
- İstifadəçiyə verilmiş tapşırığı yerinə yetirə bilməsi üçün minimal vəzifələr təyin edilməli;
- Bir neçə istifadəçi üçün ümumi olan mühafizə vasitələrinin sayı minimuma endirilməli;

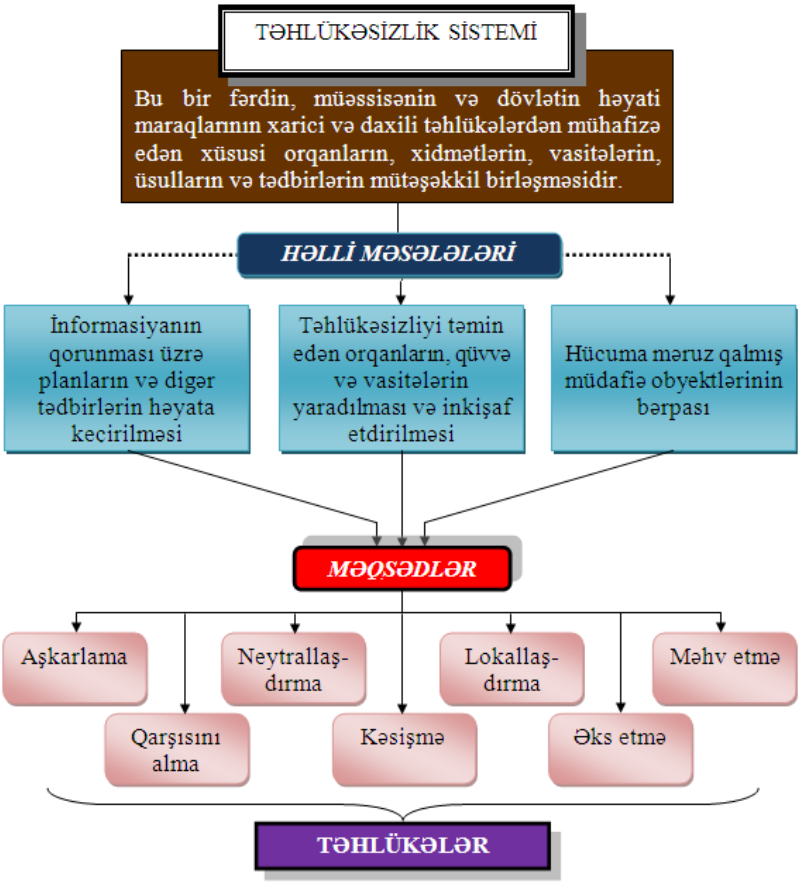
- Konfidensial informasiyaya qeyri-qanuni müdaxilə cəhdlərinin və hallarının hesabatı aparılmalı;
- Konfidensial informasiyanın vacibliyinin səviyyəsi qiymətləndirilməli;
- Texniki vasitələrin sazlığına nəzarət təmin edilməli və onların sıradan çıxması zamanı nasazlıqlar dərhal aradan qaldırılmalıdır.

İnformasiyanın Mühafizəsi Sistemi, digər sistemlər kimi, öz funksiyasını yerinə yetirmək üçün müəyyən növ təminata malik olmalıdır. İnformasiyanın mühafizəsi sistemi aşağıdakı təminatlara malikdir:

- ***Hüquqi təminat.*** Bura normativ hüquqi sənədlər, əsasnamələr, təlimatlar, rəhbər göstərişlər, Azərbaycanın qoşulduğu beynəlxalq normalar, fəaliyyət sahəsində vacib olan tələblər daxildir;
- ***Təşkilati təminat.*** Bu odeməkdir ki, informasiyanın mühafizəsinin təşkili müəyyən strukturlar (sənədlərin qorunması xidməti, rejim, girişə nəzarət, mühafizə xidməti, texniki vasitələrlə informasiyanın müdafiəsi xidməti, informasiya-analitik fəaliyyət və d.) tərəfindən həyata keçirilir;
- ***Aparat təminatı.*** İnformasiyanın mühafizəsi və İnformasiyanın Mühafizəsi Sisteminin fəaliyyətinin təmin edilməsi üçün texniki vasitələrdən geniş istifadə edilməsi nəzərdə tutulur;
- ***İnformasiya təminatı.*** Buraya sistemin fəaliyyətini təmin edən məsələlərin həllində gərəkli olan məlumatlar, verilənlər, göstəricilər, parametrlər daxildir;
- ***Proqram təminatı*** konfidensial informasiyaya qeyri-qanuni müdaxilə yollarının və yayılma kanallarının mövcudluğu, onların təhlükə səviyyəsinin qiymətləndirilməsini həyata keçirən müxtəlif informasiya, qeydiyyat, statistik və hesabat proqramlarından ibarətdir;

- ***Riyazi təminat.*** Burada cinayətkarların texniki vasitələrinin, müdafiə zonalarının təhlükə səviyyəsinin qiymətləndirilməsi ilə əlaqəli müxtəlif hesablamalar üçün riyazi metodlar nəzərdə tutulur;
- ***Linqvistik təminat.*** Buraya İnformasiyanın Mühafizəsi Sistemində mütəxəssislərin və istifadəçilərin xüsusi dilli (şifrli) əlaqə vasitələrinin birləşməsi aiddir;
- ***Normativ-metodiki təminat.*** Buraya informasiyanın mühafizəsi funksiyasını həyata keçirən orqanların, xidmətlərin, vasitələrin fəaliyyətinin normaları və qaydaları və informasiyanın mühafizəsi zamanı istifadəçilərin fəaliyyətini nizama salan müxtəlif növ metodikalar daxildir.

Təhlükəsizlik sistemini bir fərdin, müəssisənin və dövlətin həyati maraqlarını xarici və daxili təhlükələrdən mühafizə edən xüsusi orqanların, xidmətlərin, vasitələrin, üsulların və tədbirlərin mütəşəkkil birləşməsi kimi başa düşürük (şəkil 1.2). İnformasiya təhlükəsizlik sisteminin öz məqsədi, həlli məsələləri, üsulları və vasitələri vardır.



Şəkil 1. 2. Mühafizə sistemi

1.4. İnformasiya təhlükəsizliyinin konseptual modeli

İnformasiya təhlükəsizliyinə dair hədələri (təhdidləri), təhlükələri, bu təhlükələrin mənbələrini, onların icra üsullarını, məqsədlərini və, həmçinin, sabitliyi pozan digər şərtləri və fəaliyyətləri müəyyən etmək lazımdır. Bu zaman zərər yetirə bilən qeyri-qanuni müdaxilələrdən qoruyacaq müdafiə tədbirlərini də nəzərdən keçirmək lazımdır.

Təcrübə göstərir ki, bu qədər təhlükə mənbələrini, obyektlərini və fəaliyyətini analiz etmək üçün modelləşdirmə metodundan istifadə etmək daha uyğundur.

İnformasiya təhlükəsizliyinin konseptual modelinin komponentləri kimi aşağıdakıları göstərmək olar:

- Təhlükə hədəfləri;
- İnformasiya mənbələri;
- İnformasiyaya yönəlmiş təhlükə mənbələri;
- İnformasiyaya yönəlmiş təhdidlər;
- İnformasiya təhlükəsizliyinin kateqoriyaları;
- İnformasiyanınəldə edilmə üsulları;
- İnformasiya mühafizəsinin istiqamətləri;
- İnformasiya mühafizəsinin üsulları;
- İnformasiya mühafizəsinin vasitələri.

Təhlükə hədəfləri kimi müdafiə obyektinin (personal, maddi və maliyyə dəyərləri, informasiya resursları) heyəti, vəziyyəti və fəaliyyəti haqqında məlumatları göstərmək olar.

İnformasiya mənbələri kimi insanlar, sənədlər, texniki vasitələr, məhsul və tullantılar və s. çıxış edə bilər.

İnformasiyaya yönələn təhlükələr onun keyfiyyət meyarları hesab olunan bütövlüyünə, gizliliyinə, həqiqiliyinə, tamlığına və əlyetənliyinə qarşı hər hansı bir hədənin yarandığı zaman özünü büruzə verir.

Təhlükə mənbəyi (subyekti) kimi rəhbərlik, əməkdaşlar, texniki vasitələr, rəqiblər, cinayətkarlar və d. çıxış edirlər.

İnformasiyalara qarşı təhlükə yaradan hədələr aşağıdakılardan ibarətdir:

- Mühafizə olunan məlumatlarla, onların tərkibi ilə qanunsuz əməllər törətmək məqsədilə tanışlıq, informasiyanın dəyişdirilməsi və maddi ziyanın vurulması üçün onların dağıdılması (oğurlanması);

- Məlumatların açıqlanması, müxtəlif kanallara sızdırılması, qorunan məlumatlara qeyri-qanuni müdaxilələrlə onların əldə edilməsi.

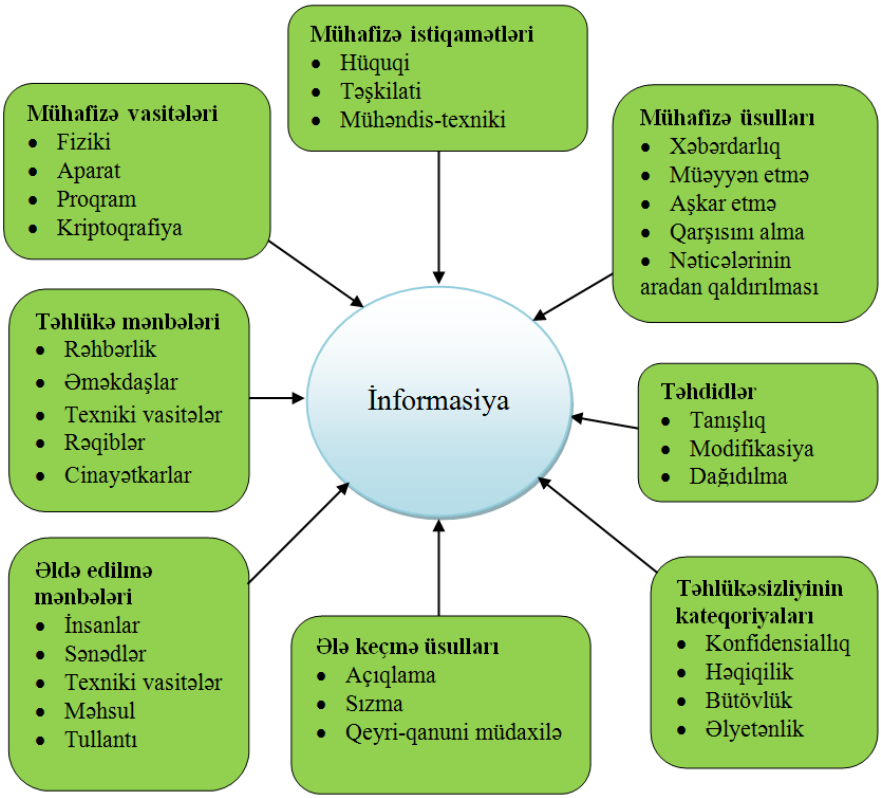
İnformasiyaların müdafiəsinin əsas istiqamətləri hüquqi, təşkilati və mühəndis-texniki tədbirlərdir.

İnformasiyanın mühafizəsi fiziki, aparat, proqram və kriptoqrafik vasitələrlə həyata keçirilir.

Mühafizə üsulları kimi təhlükələrin xəbərdarlığı, təhlükələrin müəyyən edilməsi və aşkar edilməsi, təhlükələrin qarşısının alınması, cinayət fəaliyyətinin nəticələrinin aradan qaldırılması üzrə bütün mümkün tədbirlər və fəaliyyətlər çıxış edə bilər.

Ümumi şəkildə, baxılan komponentlər informasiya təhlükəsizliyinin konseptual modeli kimi aşağıdakı cədvəldə verilmişdir (şəkil 1.3).

Təhlükəsizlik konsepsiyası müəssisəni daxili və xarici təhlükələrdən qoruyan əsas nəzəri modeldir.



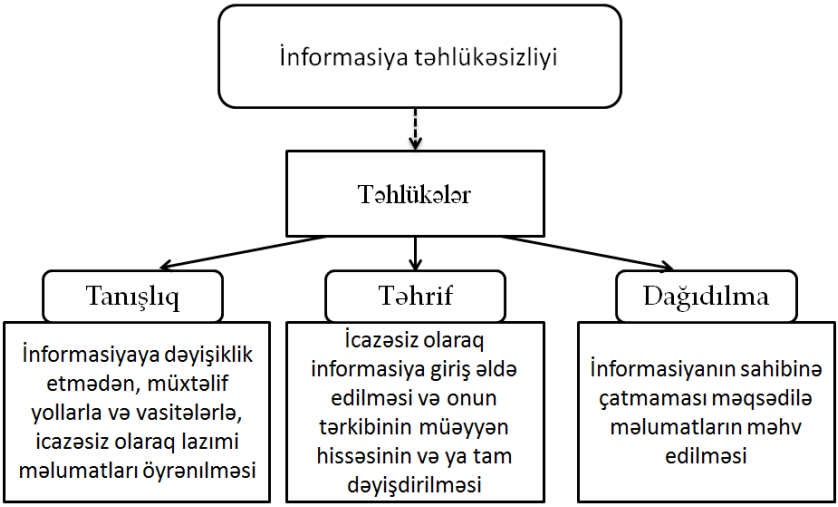
Şəkil 1.3. İnformasiya təhlükəsizliyinin konseptual modeli

1.5. İnformasiyaya qarşı yönəlmiş təhlükələr

Gizli informasiyaya qarşı yönəlmiş təhlükələr dedikdə qorunan məlumatları qeyri-qanuni əldə etməyə yönələn, informasiya resurslarına qarşı potensial və real mümkün fəaliyyət başa düşülür.

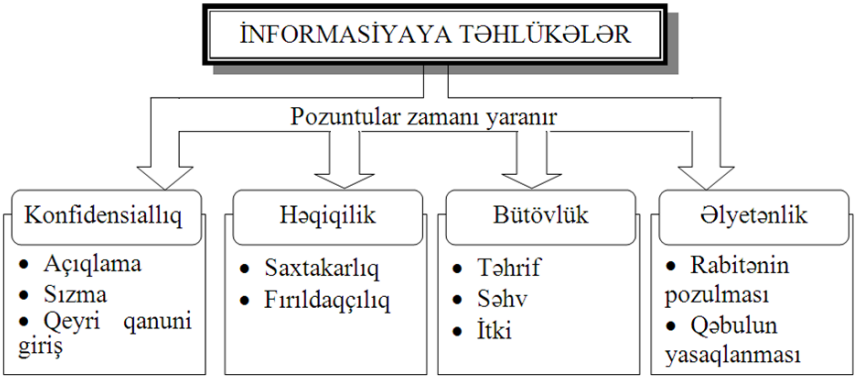
Belə fəaliyyətlər:

- bütövlüyünü və tamlığını saxlamaqla, müxtəlif yollarla və vasitələrlə, icazəsiz olaraq gizli informasiya ilə tanışlıq;
- cinayət məqsədi ilə məlumatların tərkibinin müəyyən hissəsinin və ya tam dəyişdirilməsi – informasiyanın modifikasiyası;
- birbaşa maddi zərər vurmaq məqsədi ilə vandalizm aktı kimi informasiyanın məhv edilməsidir (dağıdılmasıdır) (şəkil 1.4.).



Şəkil 1.4. İnformasiya təhlükəsizliyinə ünvanlanan təhdidlər

Son nəticədə, informasiyaya qarşı yönəlmiş qeyri-qanuni hərəkətlər (təhdidlər) onun konfidensiallığının, bütövlüyünün, həqiqiliyinin və əlyetənliyinin pozulmasına gətirib çıxara bilər (şəkil 1.5). Bu da öz növbəsində idarəetmə rejiminin sıradan çıxması ilə nəticələnir.



Şəkil 1.5. İnformasiya təhlükəsizliyinə qarşı olan təhdidlərin növləri

Hər bir təhlükə müəyyən zərərə – maddi və mənəvi – gətirib çıxara bilər. Mühafizə və əks tədbirlər isə bu zərərin qarşısını almağa və ya həcmini azaltmağa (idealda tam, realda isə çox və ya bir hissəsini) yönəlir.

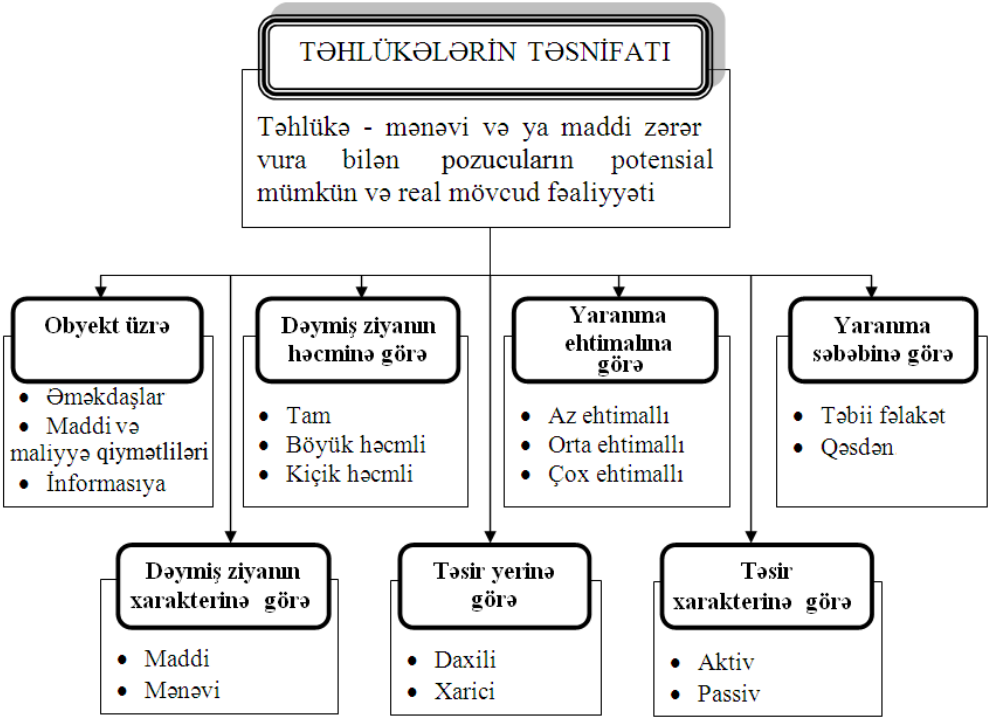
Bunları nəzərə alaraq, təhlükələri aşağıdakı qruplar üzrə təsnif etmək mümkündür (şəkil 1.6):

- Obyekt üzrə:

– Əməkdaşlar;
– Maddi və maliyyə dəyərləri;
– İnformasiya.

- Dəymiş ziyanın həcminə görə:

– Tam. Bunun nəticəsində şirkət müflis ola bilər;
– Böyük həcmli. Müflisləşməyə gətirib çıxarmır;
– Kiçik həcmli. Müəyyən vaxtdan sonra şirkət zərəri aradan qaldıra bilər.



Şəkil 1.6. Fərqli parametrlərinə görə təhlükələrin təsnifatı

- Yaranma ehtimalına görə:
– Az ehtimallı təhlükə;
– Orta ehtimallı təhlükə;
– Çox ehtimallı təhlükə.

- Yaranma səbəblərinə görə:
– Təbii fəlakət;
– Qəsdən.

- Dəymiş ziyanın xarakterinə görə:
– Maddi;
– Mənəvi.

- Təsir xarakterinə görə:
– Aktiv;
– Passiv.

- Təsir yerinə görə:
– Daxili;
– Xarici.

Daxili təhlükə mənbələri aşağıdakılardır:
- Müəssisənin rəhbərliyi;
- Əməkdaşlar;
- Fəaliyyəti təmin edən texniki vasitələr.

Xarici təhlükə mənbələri aşağıdakılardır:
- Rəqiblər;
- Cinayətkar qruplar və dəstələr;
- Rəhbər şirkətlər və onların əməkdaşları.

Ümumi hesablamalara görə daxili və xarici təhlükələrin nisbətini aşağıdakı qaydada səciyyələndirmək mümkündür: cinayətin böyük hissəsi şirkətin əməkdaşlarının birbaşa və ya dolayı yolla iştirakı ilə törədilir; cinayətin az hissəsixarici təhlükələrin nəticəsində yaranır; cüzi zərər təsadüfi şəxslər tərəfindən yetirilir.

1.6. Gizli informasiyanı qeyri-qanuni ələ keçirməyə yönəlmiş fəaliyyət

İnformasiya prosesindəki əks maraqlara malik obyektlə (şirkət, müəssisə, fərd və s.) subyekt (rəqib, cinayətkar və s.) arasındakı münasibətə gizli informasiyanın qeyri-qanuni ələ keçirilməsinə yönələn fəaliyyət kimi baxmaq olar. Bu zaman aşağıdakı vəziyyətlər ola bilər:

- İnformasiya sahibi (mənbə) gizli informasiyanın qorunması üçün heç bir tədbir görmür ki, bu da cinayətkara istədiyi məlumatı rahat şəkildə əldə etməyə imkan verir;
- İnformasiya sahibi informasiya təhlükəsizliyi tədbirlərinə ciddi nəzarət edir. Bu zaman cinayətkar qorunan məlumatlara giriş əldə etmək üçün kifayət qədər qüvvə sərf etməli olur və bu prosesdə bütün qeyri-qanuni müdaxilə üsullarından istifadə edir;
- Orta vəziyyət. Bu halda informasiya texniki kanallarla, mənbənin xəbəri olmadan (əks halda, hər hansı bir tədbir görmək mümkün olardı) sızmağa başlayır. Cinayətkar isə asan yolla, böyük qüvvə sərf etmədən bu vəziyyətdən öz maraqları üçün istifadə edir.

Ümumilikdə, qorunan informasiyanın cinayətkarlar və ya rəqiblər tərəfindən ələ keçirilməsi faktı sızma adlanır. Lakin bununla bərabər, bir çox qanunverici aktlarda, rəsmi məlumatlarda, ədəbiyyatlarda “məlumatın açıqlanması” və

“konfidensial informasiyaya icazəsiz giriş” anlayışlarından da istifadə olunur (şəkil 1.7).

1. Açıqlanma – kənar şəxslərin əlinə keçməsi ilə nəticələnən, gizli məlumatları qəsdən və ya ehtiyatsız, söyləmə, elan etmə və d. fəaliyyət. Bunun nəticəsində kənar şəxslər gizli məlumatlarla tanış olurlar.

Həm işgüzar, həm də elmi informasiyaların ötürülməsi, göndərilməsi, çap edilməsi, itirilməsi, paylanması, mübadilə edilməsi və digər fəaliyyət açıqlanma hesab olunur. Açıqlanma rəsmi və qeyri-rəsmi kanallarla yayıla bilər.

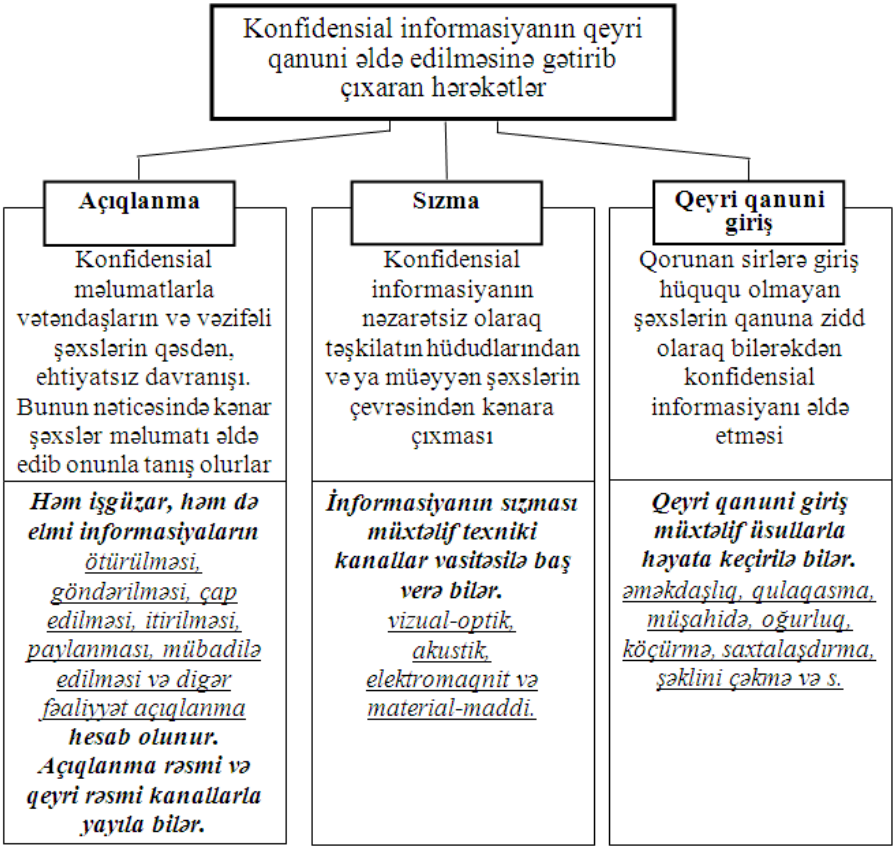
Rəsmi kanallara aşağıda qeyd olunanlar aiddir:

- işgüzar görüşlər, müşavirələr, rəsmi danışıqlar, sərgilər, seminarlar, konfranslar və digər kütləvi tədbirlər və digər rabitə formaları: rəsmi informasiyanın ötürülməsi vasitələri ilə (poçt, telefon, teleqraf və s.) rəsmi-işgüzar və elmi sənədlərin mübadiləsi, həmçinin kütləvi informasiya vasitələri (nəşr, qəzet, müsahibə, radio, televiziya)..

Qeyri-rəsmi kanallara aşağıda qeyd olunanlar aiddir:

- şəxsi danışıqlar (görüşlər, yazışma), söhbətlər

Bir qayda olaraq, gizli informasiyanın açıqlanmasının səbəbi əməkdaşların “kommersiya sirrinin qorunması qaydaları” haqqında az məlumatlı olmaları və bu qaydalara ciddi əməl etməmələridir. Bunun üçün əsas tədbirləri qorunan sirlərin sahibi (mənbə) görməlidir.



Şəkil 1.7. Gizli informasiyanın qanunsuz əldə olunması növləri

2. Sızma – gizli informasiyanın təhlili, ötürülməsi, işlənməsi, onlardan istifadə, onların tətbiqi zamanı nəzarətsiz olaraq təşkilatın hüdudlarından və ya müəyyən şəxslərin çevrəsindən kənara çıxmasıdır.

İnformasiyanın sızması müxtəlif texniki kanallar vasitəsilə baş verir. Məlumdur ki, informasiya enerji və ya maddə ilə ötürülə bilər. Bu, akustik dalğa (səs), elektromaqnit

şüalanma, kağız vərəqi (yazılmış mətn) və s. ola bilər. Bunu nəzərə alaraq deyə bilərik ki, təbiətdə informasiyanın müxtəlif daşınma yollarımövcuddur, məsələn, işıq şüaları, səs dalğaları, elektromaqnit dalğaları, materiallar və maddələr. Buna müvafiq olaraq informasiyanın sızma kanalları belə təsnif olunur:

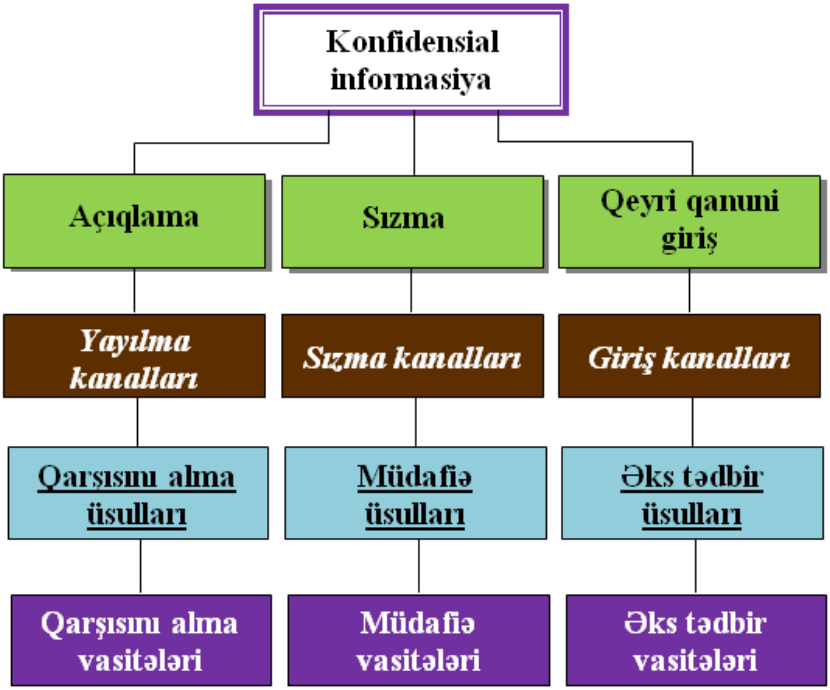
- ***vizual-optik,***
- ***akustik,***
- ***elektromaqnit***
- ***maddi-material.***

İnformasiyanın sızma kanalı dedikdə gizli informasiya mənbəyindən cinayətkara qədər olan fiziki yol başa düşülür. Bunun nəticəsində cinayətkar qorunan məlumatı əldə edə bilər. İnformasiyanın sızma kanalının yaranması üçün müəyyən məkan, enerji və zaman şərtlərinin olması və cinayətkarın informasiyanın müvafiq qəbul, emal və qeyd etmə qurğusuna malik olması zəruridir.

3. Qeyri-qanuni giriş – bu, qorunan sirlərə giriş hüququ olmayan şəxslərin qanuna zidd olaraq bilərəkdən gizli informasiyanı əldə etməsidir.

Gizli informasiyanın mənbəyinə qeyri-qanuni giriş müxtəlif üsullarla həyata keçirilir: sirləri satmaq istəyən şəxslə əməkdaşlıqdan başlayaraq kommersiya sirlərinə yiyələnmə vasitələrindən istifadəyə kimi. Bu işləri yerinə yetirmək üçün cinayətkara çox vaxt obyektə daxil olmaq və ya obyektin yaxınlığında müasir texniki vasitələrlə təchiz olunmuş stasionar və ya hərəkətli xüsusi nəzarət və baxış postunu yaratmaq lazım gəlir.

Gizli informasiyanın qeyri-qanuni əldə edilməsinin hər bir üsuluna müvafiq müəyyən kanallar, mühafizə tədbirləri, mühafizə və əks-tədbir vasitələri mövcuddur. Bu kanalların, üsulların və vasitələrin əlaqəsini növbəti şəkildəki kimi göstərmək olar (şəkil 1.8):



Şəkil 1.8. Konfidensial informasiyalara ünvanlanmış təhdidlərlə mühafizə tədbirlərinin əlaqəsi

1.7. İnformasiya mühafizəsinin üsulları

İnsanın istənilən fəaliyyəti hər hansı bir nəticənin əldə olunması üçündür və müəyyən üsullarla həyata keçirilir.

İnformasiyanın mühafizəsi üsulları – informasiyanın gizliliyini, bütövlüyünü, tamlığını və əlyetənliyini təmin edən qüvvələrin və vasitələrin birləşməsidir.

Əlbəttə ki, mühafizə üsulları, qüvvələri və vasitələri hər bir təhlükə növünə uyğun olaraq tətbiq olunur.

İnformasiya təhlükəsizliyinin təmin edilməsi müəyyən tədbirlər sistemi ilə yerinə yetirilir. Bu tədbirlər sistemi aşağıda qeyd olunan istiqamətdə olur:

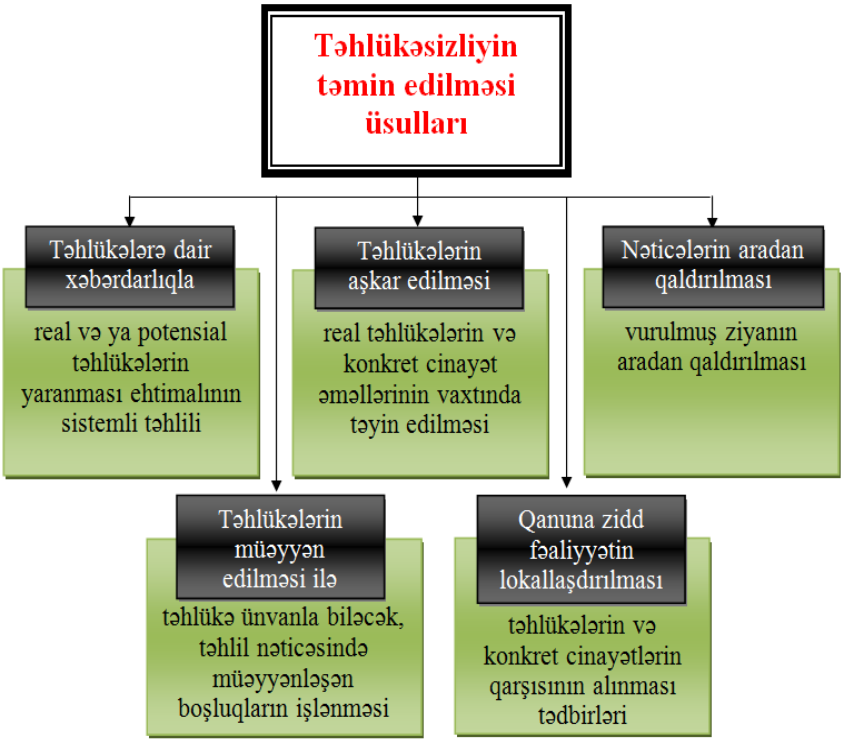
- Təhlükələrə dair **xəbərdarlıq,** onların yaranmasının qarşısının alınmasına yönəlmiş informasiya təhlükəsizliyinin təmin edilməsi baxımından ilkin təhlili və xəbərdarlıq üzrə tədbirlər;
- Təhlükələrin **müəyyən edilməsi,** real və ya potensial təhlükələrin yaranması ehtimalının sistemli təhlili və onların xəbərdarlığı üzrə tədbirlər;
- Təhlükələrin **aşkar edilməsi** – real təhlükələrin və konkret cinayət əməllərinin təyin edilməsi;
- Cinayət fəaliyyətinin **lokallaşdırılması** –təhlükələrin qarşısının alınması;
- Təhlükələrin və cinayət fəaliyyətinin nəticələrinin **aradan qaldırılması** və "status-kvo"nun bərpası (şəkil 1.9).

Mümkün təhlükələr və qeyri-qanuni fəaliyyət haqqında xəbərdarlıq müxtəlif tədbirlər və vasitələrlə təmin edilə bilər. Buraya əməkdaşların təhlükəsizlik və informasiya mühafizəsi problemlərini daha dərindən anlamasından başlayaraq fiziki, aparat, proqram və kriptoqrafik vasitələrlə mühafizə sisteminin yaradılmasına kimi tədbirlər aid ola bilər.

Qanunsuz hücumlar, planlaşdırılan oğurluqlar, hazırlıq işləri və digər cinayət tərkibli işlər haqqında məlumatlar əldə etməklə (qəbul etməklə) də təhlükələrə dair xəbərdarlıq etmək mümkündür. Bu məqsədlər üçün daxili və xarici informatorlarla təhlükəsizlik xidməti əməkdaşlarının birgə əlaqədə olması, fəaliyyəti (daxili kollektivin əməkdaşlarını, xarici rəqibləri və cinayətkar qruplaşmaları müşahidə etmək və obyektiv qiymətləndirmək) gərəklidir.

Təhlükələrin xəbərdar edilməsində kriminogen vəziyyətin, rəqiblərin və cinayətkarların fəaliyyətinin təhlili məsələləri

üzrə təhlükəsizlik xidmətinin informasiya-analitik fəaliyyəti baş rol oynayır.



Şəkil 1.9. İnformasiya mühafizəsinin üsulları

Təhlükələrin müəyyən edilməsi - məhsulların və malların istehsalı və satışı bazarındakı rəqiblərin, kriminal strukturların cinayət fəaliyyətinə hazırlanmasının mümkünlüyü haqqında məlumatların toplanması və analitik emalının nəticəsidir. Bu işdə öz əməkdaşlarının öyrənilməsinə, onların fəaliyyətinin müşahidə edilməsinə xüsusi önəm verilməlidir. Onların arasında narazılar, təcrübəsizlər, "daxil edilmişlər" (rəqib müəssisə tərəfindən sızdırılan işçilər) də ola bilər. Müəssisədəki bütün boşluqlar müəyyən edilməlidir.

Təhlükələrin aşkar edilməsi zərər yetirən təhlükələrin və onların mənbələrinin təyin edilməsidir. Bu növ fəaliyyətə oğurluq və dələduzluq faktlarının, həmçinin gizli informasiyanın açıqlanması faktları və ya kommersiya sirlərinin mənbələrinə qeyri-qanuni giriş hallarının aşkar-lanması aid edilə bilər. Təhlükələrin aşkarlanması tədbirlərində tək təhlükəsizlik xidmətinin əməkdaşları deyil, digər struktur bölmələrin əməkdaşları, həmçinin qanun pozuntularının müşahidə və aşkarlanmasının texniki vasitələri də əsas rolu oynaya bilər.

Təhlükələrin qarşısının alınması və ya lokallaşdırılması – mövcud təhlükənin və konkret cinayət fəaliyyətinin aradan qaldırılmasına yönəlmiş fəaliyyətdir. Məsələn, ventilyasiya sistemləri ilə informasiyanın sızmasının, akustik kanallar hesabına gizli danışıqlara qulaqasmanın qarşısının alınması.

Nəticələrin aradan qaldırılması – sistemin təhlükədən öncəki vəziyyətə gətirilməsi, bərpa edilməsidir. Buraya cinayətkarın oğurlanmış əmlak ilə birgə tutulması, partlayışdan dağılmış binanın bərpası və s. ola bilər.

Bütün bu üsullar qeyri-qanuni müdaxilədən aşağıda qeyd olunan tədbirlərlə informasiya resurslarının qorunması məqsədini güdür:

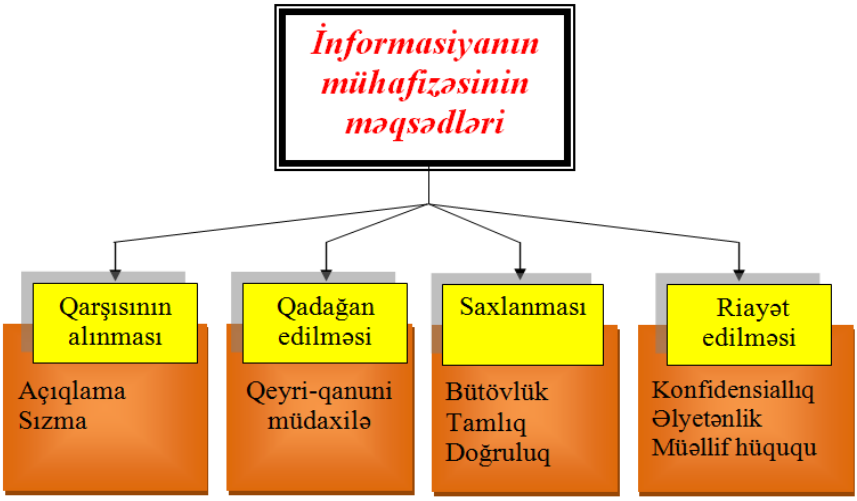
- Gizli informasiyanın açıqlanmasının və sızmasının qarşısını alır;
- Gizli informasiya mənbələrinə qeyri-qanuni girişi yasaqlayır;
- İnformasiyanın bütövlüyünü, tamlığını və əlyetənliyini saxlayır;
- İnformasiyanın konfidensiallığına riayət edir, müəllif hüquqlarını qoruyur (şəkil 1.10).

Beləliklə, açıqlamadan mühafizə olunmaq müəssisənin gizli məlumatlarının siyahısının hazırlanması ilə başlayır. Bu siyahı məlumatların gizliliyinin qorunması barədə öhdəlik

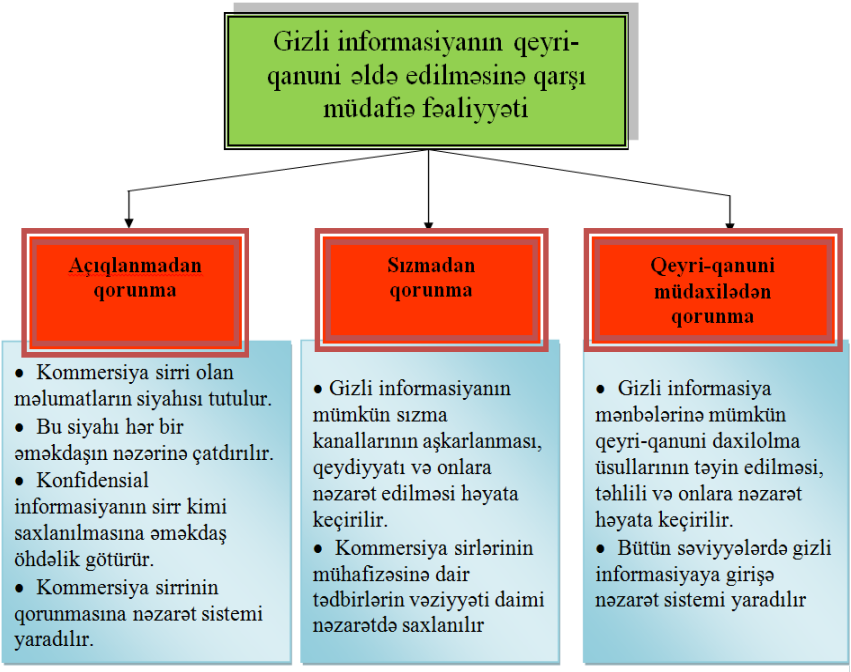
götürmüş və bu sirlərlə işləməyə buraxılmış hər bir əməkdaşın nəzərinə çatdırılmalıdır. Əsas tədbirlərdən biri də sirlərin qorunmasına nəzarət sisteminin yaradılmasıdır.

Gizli informasiyanın sızmasından mühafizə müəyyən şəraitdə mümkün sızma kanallarının müəyyən olunması, qeydiyyatı və onlara nəzarət, bu kanalların ləğvi üzrə təşkilati və texniki tədbirlərin həyata keçirilməsidir.

Gizli informasiyaya qeyri-qanuni müdaxilədən müdafiə qanunsuz girişin aşkarlanması, təhlili, onlara nəzarət edilməsi və qeyri-qanuni müdaxilələrə qarşı fəaliyyət üzrə təşkilati və texniki tədbirlərin həyata keçirilməsi ilə təmin olunur (şəkil 1.11).



Şəkil 1.10. İnformasiyanın mühafizəsi



Şəkil 1.11. Təhlükələrdən gizli informasiyanın mühafizə edilməsi tədbirləri

Fəsil üzrə yoxlama sualları

Qeyd olunan fikrin səhv və ya düz olduğunu müəyyənləşdirin

	Düz	Səhv
1. Tərkibində ümumi anlayışlar olan və cəmiyyətin çox hissəsinə bəlli məlumatlar xüsusi məlumatlar hesab olunur.	☐	☐
2. İnformasiyanın beynəlxalq vahid tərifi mövcuddur.	☐	☐
3.Təhlükələrə dair xəbərdarlıq təhlükələr müəyyən edildikdən sonra təşkil olunur.	☐	☐

Test suallarını cavablandırın:

1. Yaranma səbəblərinə görə təhlükələri necə təsnif etmək olar?

a) Təbii fəlakət
b) Texnogen
c) Ekoloji
d) Qəsdən

2. Açıqlanmanın rəsmi kanalı hansı bənddə göstərilmişdir?

a) Şəxsi danışıqlar
b) İşgüzar görüşlər
c) Sərgilər
d) Seminarlar

3. Daxili təhlükə mənbələrinə hansılar aid deyil?

a) Müəssisənin rəhbərliyi
b) Rəqiblər
c) Rəhbər şirkətlər və onların əməkdaşları
d) Əməkdaşlar

Açıq sualların cavablarını əhatəli qeyd edin:

1.Təqdim etmə formasına görə informasiyanın əsas növləri hansılardır?

_____
_____
_____
_____
_____

2. İnformasiyanın etibarlılığı dedikdə nə nəzərdə tutulur?

_____
_____
_____
_____
_____

2. İnformasiyanın mühafizəsi üsulları və vasitələri

2.1. İnformasiya təhlükəsizliyinin təmin edilməsi istiqamətləri

İnformasiyaların təhlükəsizliyinin təmin edilməsi məqsədi ilə onların mühafizə edilməsi üçün həyata keçirilən kompleks tədbirlər sistemi dövlət, müəssisə, təşkilat, həmçinin, fərdi şəxslər tərəfindən müəyyən edilir. İnformasiya təhlükəsizliyinin təmin edilməsi üzrə həyata keçirilən tədbirlər aşağıdakı istiqamətlər üzrə aparılır.

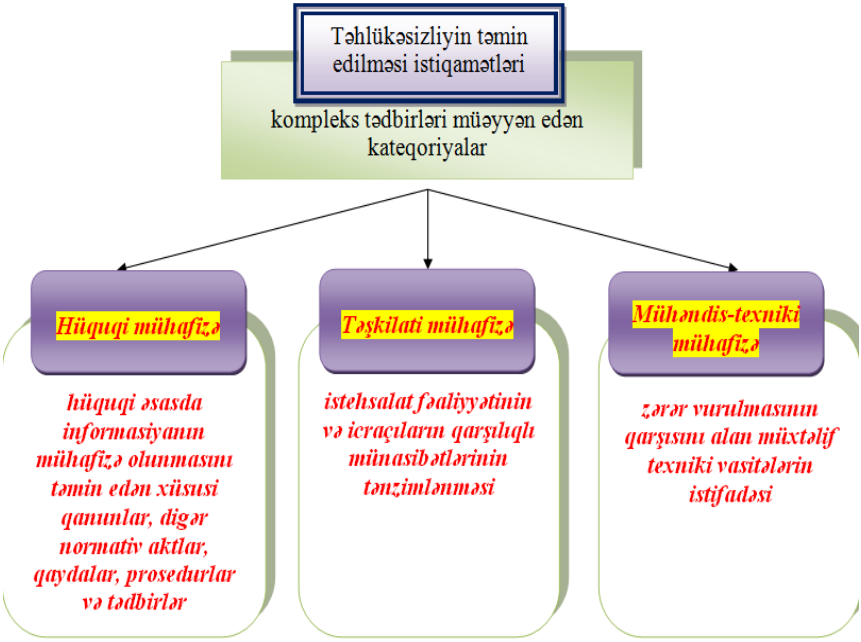
- **Hüquqi mühafizə** – informasiyaların mühafizə edilməsi məqsədi ilə həyata keçirilən tədbirlərin normativ-hüquqi əsaslarını müəyyən edir; intizam, inzibati, cinayət, idarəetmə tədbirləri üzrə hüquqi normaları əhatə edir.
- **Təşkilatimühafizə** – daxili və xarici təhdidlərin yaranmasının, gizli informasiyanın qanunsuz əldə edilməsinin qarşısını alan və ya çətinləşdirən istehsalat fəaliyyətinin və icraçıların qarşılıqlı münasibətlərinin tənzimlənməsidir.
- **Mühəndis-texnikimühafizə** – informasiya təhlükəsizliyinə zərər vurulmasının qarşısını alan müxtəlif texniki vasitələrdən, proqram təminatlarından istifadədir (şəkil 2.1).

2.1.1. İnformasiyanın hüquqi təhlükəsizliyi

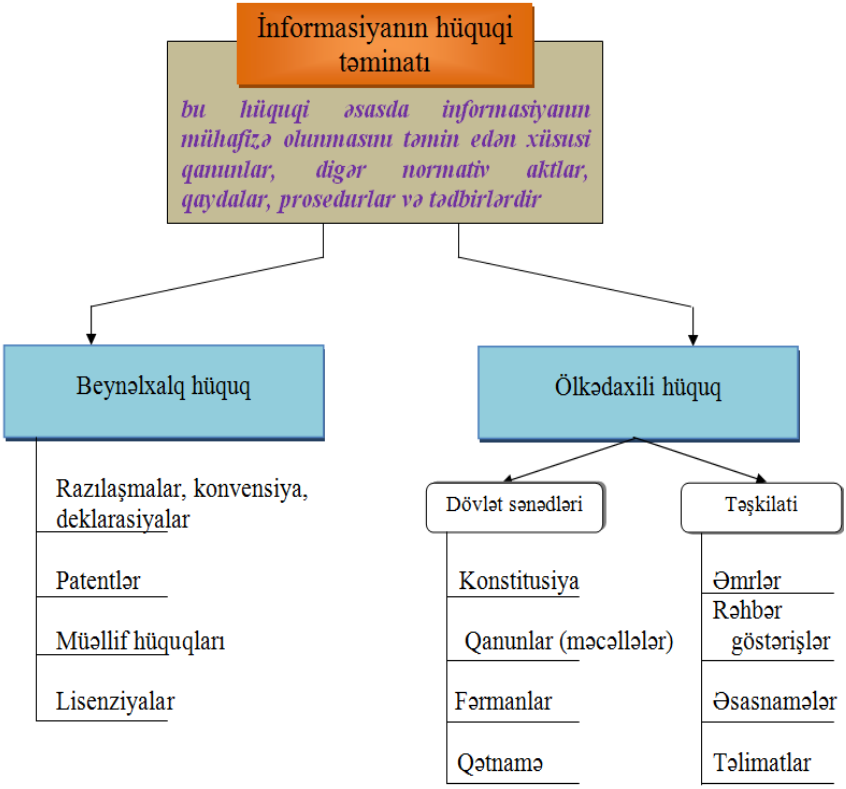
Məlumdur ki, hüquq – dövlət orqanlarının, müəssisələrin (təşkilatların) və əhalinin (fərdi şəxsin) müəyyən həyat sahəsi və fəaliyyəti ilə bağlı dövlət tərəfindən müəyyən olunan və ya icazə verilən davranış qaydalarının və normalarının məcmusundan ibarətdir.

Hüquq insan fəaliyyətinin ən müxtəlif sahələrində, habelə ən müxtəlif faktiki əsaslarda və ən müxtəlif situasiyalarda müxtəlif hüquq subyektlərinin iştirak etdiyi ictimai münasibətləri tənzimləyir.

Resurs kimi informasiyanın hüquqi müdafiə olunması beynəlxalq və dövlət səviyyəsində tanınır, dövlətlərarası razılaşmalar, konvensiyalar, deklarasiyalar ilə müəyyən edilir, onların müdafiəsi üçün patentlər, müəlliflik hüququ və lisenziyalar ilə reallaşdırılır. Dövlət səviyyəsində hüquqi müdafiə dövlət və idarə aktları ilə nizamlanır (şəkil 2.2).



Şəkil 2.1. İnformasiya təhlükəsizliyinin təmin edilməsi istiqamətləri



Şəkil 2.2. İnformasiyanın hüquqi mühafizəsi

İdarəetmə üzrə normativ-hüquqi aktlar dövlət idarəçiliyi üzrə, həmçinin idarə, təşkilat, müəssisədaxili inzibati hüquqi normalardan (təlimatlar, əsasnamələr, nizamnamələr, göstərişlər və s.) ibarətdir.

İnformasiya təhlükəsizliyinə dair tələblər qanunvericiliyin bütün mərhələlərinə (konstitusiya qanunvericiliyi, əsas ümumi qanunlar, dövlət idarəetmə sisteminin təşkili üzrə

qanunlar, xüsusi qanunlar, idarənin normativ aktları və d.) daxil olunmalıdır.

İnformasiyanın hüquqi müdafiəsinə yönəlmiş hüquqi aktların strukturunu bu cür vermək olar:

Birinci blok – Konstitusiya qanunvericiliyi Azərbaycan Respublikasının Konstitusiya normaları. İnformasiya prosesləri və informasiyanın mühafizəsi məsələlərinə dair normalar.

İkinci blok – İnformasiya prosesləri və informasiyanın mühafizəsi məsələlərinə dair normalar daxil olan konstitusiya qanunları, məcəllələr (mülkiyyət, mühit, torpaq, vətəndaş hüququ, vergilər və s. haqqında).

Üçüncü blok – təsərrüfat, maliyyə, dövlət sistemi orqanlarının ayrı-ayrı strukturlarına aid olan və onların statusunu müəyyən edən idarəetmənin təşkili haqqında qanunlar. Bura informasiyanın mühafizəsi üzrə ayrı-ayrı hüquqi-normativ aktlar və onların müəyyənləşdirdiyi qaydalar daxildir.

Dördüncü blok – konkret sahəyə aid xüsusi normativ-hüquqi aktlar. Buraya həmçinin "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının Qanunu, "Milli təhlükəsizlik haqqında" Azərbaycan Respublikasının Qanunu daxildir. Bu qanunlar blokunun tərkibi və məzmunu informasiya təhlükəsizliyinin hüquqi təmin edilməsinin əsası kimi xüsusi qanunvericiliyin mövcud olmasını nəzərdə tutur.

Beşinci blok – informasiya mühafizəsinə dair subyektlərin normativ aktları, təlimatları, əsasnamələri, göstərişləri və planlarından ibarətdir.

Altıncı blok – bu, tərkibində informasiyaların mühafizəsi sahəsində qanun pozuntuları üzrə məsuliyyətin müəyyən edilməsinə dair normativ-hüquqi aktları özündə birləşdirir. Belə normativ aktlara Azərbaycan Respublikasının Cinayət məcəlləsi və Azərbaycan Respublikasının İnzıbati xətalar məcəlləsi, Cinayət-prosessual məcəlləsi aid edilir.

İnformasiya təhlükəsizliyinin təmin edilməsi üzrə Azərbaycan Respublikasının qanunvericilik bazası

Azərbaycan Respublikasında informasiyaların mühafizə edilməsi üzrə normativ-hüquqi sənədlər aşağıdakılardır: Azərbaycan Respublikasının Konstitusiyası, bu sahədə Azərbaycan Respublikasının Qanunları, Azərbaycan Respublikası Prezidentinin fərman və sərəncamları, Nazirlər Kabinetinin qərarları, mərkəzi icra orqanlarının normativ sənədləri, Azərbaycan Respublikasının qoşulduğu beynəlxalq normalar, müqavilələr.

Azərbaycan Respublikasında informasiya və informasiya proseslərinin mühafizəsi Azərbaycan Respublikasının Konstitusiyası və qanunları ilə təmin olunur. İnformasiyalar əqli mülkiyyət formasında fiziki və ya hüquqi şəxslərə məxsusdur. Azərbaycan Respublikasının Konstitusiyasının 30-cu maddəsinə görə hər kəsin əqli mülkiyyət hüququ (xüsusi halda İnformasiyalara sahib olmaq) vardır və bu hüquq Konstitusiyanın 29-cu maddəsinə görə dövlət tərəfindən qorunur.

Azərbaycan Respublikası Konstitusiyasının 50.1-ci maddəsinə görə "Hər kəsin istədiyi məlumatı qanuni yolla axtarmaq, əldə etmək, ötürmək, hazırlamaq və yaymaq azadlığı vardır".

İnformasiya proseslərinin təhlükəsizliyinin hüquqi tənzimlənməsi "İnformasiya, informasiyalaşdırma və informasiyaların mühafizəsi", "Fərdi məlumatlar" və "Dövlət sirri haqqında" və d. qanunlarla, Azərbaycan Respublikasının Cinayət, İnzibati xətalar və Cinayət-prosessual məcəllələri ilə həyata keçirilir. İnformasiyaların təhlükəsizliyinin təmin edilməsinin ümumi məsələləri, qeyd edilən qanunlarla bərabər müəyyən obyektlərin və sistemlərin mühafizəsinin təşkili mərkəzi icra hakimiyyəti orqanlarının normativ-hüquqi aktları və təşkilatların qəbul etdikləri normativ-hüquqi aktların vasitəsi

ilə tənzimlənir. İnformasiyaların formalaşması və bu sahədə gedən proseslər, informasiya proseslərinin mühafizəsi elə inkişaf həddinə çatmışdır ki, bu sahədə ictimai münasibət formalarının səviyyəsi, həmçinin hüquq normalarının çoxluğu və beynəlxalq hüquq normalarının sayı bu sahənin fəaliyyətini və onun təhlükəsizliyini nizamlayan müstəqil bir hüquq institutunun yaradılmasına ehtiyac yaradır. Bu qanunvericilik aktı tamamilə informasiya təhlükəsizliyi məsələlərinə həsr olunmalı və aşağıdakı sahələri əhatə etməlidir:

- informasiya və informasiyanın mühafizəsinin təmin olunması üzrə hüquqi normalar;
- informasiya əldə etmək məsələlərini tənzimləyən hüquqi normalar;
- informasiya və məlumat azadlığı haqqında hüquqi norma;
- dövlət sirri və məlumatların dövlət sirrinə aid edilməsi haqqında qanunvericiliyin tələbi;
- fərdi və konfidensial məlumatlar, kommersiya sirri haqqında qanunvericilik aktı;
- biometrik informasiya, elektron imza və elektron sənəd haqqında qanunvericilik aktı;
- feldyeger rabitəsi haqqında qanunvericilik aktı;
- kibercinayətkarlıq, kompüter sistemlərinin təhlükəsizliyi haqqında qanunvericilik aktları;
- müəlliflik hüququ, patent və əlaqəli hüquqlar haqqında qanunvericilik aktları.

İnformasiyanın anlayışı, növü və mühafizəsi

İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında Azərbaycan Respublikası Qanununun 10-cu maddəsinə əsasən əldə olunma növünə görə informasiya ümumi istifadə üçün açıq və alınması məhdudlaşdırılan informasiyalara bölünür. Azərbaycan Respublikasının qanunu

ilə əldə olunması məhdudlaşdırılmayan informasiyalar açıq informasiyalar sayılır.

Əldə edilməsi qanunla məhdudlaşdırılan informasiyalar hüquqi rejiminə görə məxfi və gizli (konfidensial) olur. Dövlət sirri məxfi; vətəndaşların, mülkiyyət növündən asılı olmayaraq yaradılmış idarə, müəssisə və təşkilatların, digər hüquqi şəxslərin qanuni maraqlarının qorunması məqsədi ilə əldə olunmasına məhdudiyyət qoyulan peşə (həkim, vəkil, notariat), kommersiya, istintaq və məhkəmə sirləri konfidensial xarakter daşıyır. Bundan əlavə, fərdi məlumatlar də konfidensial ola bilər. *Fərdi məlumatlar haqqında Azərbaycan Respublikası qanununun 5-ci maddəsinə əsasən* fərdi məlumatlar daxil olma (əldə olunma) növünə görə konfidensial və açıq kateqoriyalara bölünür. Şəxsi və ailə həyatına dair məlumat (fərdi məlumat) - şəxsin kimliyini birbaşa və ya dolayısı ilə müəyyənləşdirməyə imkan verən istənilən məlumatdır.

İnformasiya əldə etmək haqqında Azərbaycan Respublikası Qanununun 2-ci maddəsinə əsasən Azərbaycan Respublikasında informasiyanın əldə olunması azaddır. Hər kəs özü birbaşa və ya nümayəndəsi vasitəsilə informasiya sahibinə müraciət etmək, informasiyanın növünü və əldə etmə formasını seçmək hüququna malikdir. İnformasiya sahibinə müraciət edən hər kəs:

- sorğu edilən informasiyanın informasiya sahibində olub-olmadığını öyrənmək, bu informasiya olmadıqda onu əldə etmək üçün yardımçı məlumatlar almaq;
- informasiya sahibi sorğu edilən informasiyaya malik olduqda, onu sərbəst, maneəsiz və hamı üçün bərabər şərtlərlə əldə etmək hüququna malikdir.

Fiziki şəxslərin özləri barəsindəki sənədləşdirilmiş informasiya ilə maneəsiz tanış olmaq, onu əldə etmək, bu informasiyada dəqiqləşdirmələr aparılmasını tələb etmək, informasiyadan kimlərin və hansı məqsədlə istifadə etdiyini öyrənmək hüququ vardır.

İnformasiya sahiblərindən bu qanunun tələblərinə uyğun olaraq əldə edilmiş sənədləşdirilmiş informasiyadan digər məqsədlər, o cümlədən kommersiya məqsədləri üçün törəmə informasiya məhsulunun yaradılmasına bu şərtlə icazə verilir ki, törəmə informasiya yaradılarkən ilkin mənbəyə istinad edilsin.

İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında Azərbaycan Respublikası Qanununun 12-ci maddəsinə əsasən fiziki və hüquqi şəxslər barəsində sənədləşdirilmiş informasiyanın siyahısı və onların informasiya sistemlərində istifadə edilməsi qaydası Azərbaycan Respublikasının qanunvericiliyi ilə müəyyən edilir.

Fiziki və hüquqi şəxslərin özləri barəsindəki sənədləşdirilmiş informasiyaya, Azərbaycan Respublikasının qanunvericiliyi ilə müəyyən edilmiş hallar istisna edilməklə, maneəsiz olaraq buraxılmaq, bu informasiyada dəqiqləşdirmələr aparılmasını tələb etmək, informasiyadan kimlərin və hansı məqsədilə istifadə etdiyini bilmək hüququ vardır.

Həmin qanunun 17-ci maddəsinə əsasən informasiyanın mühafizəsinin məqsədləri aşağıdakılardan ibarətdir:

- informasiyanın məhvinin, itməsinin, saxtalaşdırılmasının qarşısının alınması;
- dövlətin, ictimaiyyətin, vətəndaşların təhlükəsizliyinin təmin edilməsi;
- informasiyanın məhvi, modifikasiyası, surətinin çıxarılması, təcrid edilməsi ilə bağlı sanksiyalaşdırılmamış hərəkətlərin qarşısının alınması;
- konfidensial və dövlət sirri təşkil edən informasiyanın qorunması;
- informasiya proseslərində və informasiya sistemlərinin, texnologiyalarının və onların təminat vasitələrinin işlənməsi, istehsalı, tətbiqi zamanı fiziki və hüquqi şəxslərin hüquqlarının təmin olunması.

Fərdi məlumatlar, onların mühafizəsi

İnformasiya əldə etmək haqqında Azərbaycan Respublikası Qanununun 38-ci maddəsinə əsasən əldə olunmasına məhdudiyyətlər qoymaqla fərdi məlumatları xidməti istifadə üçün nəzərdə tutulmuş hesab etmək olar. Fərdi məlumatlar şəxsi və ailə həyatına dair məlumatların məcmusudur. Əldə olunmasına məhdudiyyətlər qoyulan şəxsi həyata dair məlumatlar aşağıdakılardır:

- qanunla müəyyənləşdirilmiş qaydada qeydə alınan özəl hüquqi şəxslərdə, üzvlüyə dair məlumatlar istisna olmaqla, siyasi baxışları, dini etiqadları və dünya görüşlərini əks etdirən məlumatlar;
- etnik mənşə və ya irqi mənsubiyyət haqqında məlumatlar;
- cinayət işləri və ya digər hüquq pozuntularına dair işlər üzrə icraatın gedişində toplanmış informasiyalar açıq məhkəmə iclasınadək və ya hüquq pozuntusuna dair məhkəmə qərarı çıxarılanadək, yaxud insanların mənəviyyatı, şəxsi və ailə həyatının müdafiəsi, yetkinlik yaşına çatmayanın, zərərçəkənin və ya şahidin mənafeyi, yaxud ədalət mühakiməsinin həyata keçirilməsi üçün tələb edilən hallarda;
- sağlamlıq vəziyyəti haqqında məlumatlar;
- şəxslərin özəl xüsusiyyətləri, qabiliyyətləri və xarakterlərinin digər cizgiləri haqqında məlumatlar;
- sosial yardım və sosial xidmətlər göstərilməsinə dair vəsatətlər barəsində məlumatlar;
- ruhi və fiziki əzablara dair məlumatlar;
- vergi ödənişləri üzrə borclar istisna olmaqla, vergitutma ilə əlaqədar məlumatlar.

Əldə olunmasına məhdudiyyətlər qoyulan ailə həyatına dair məlumatlar aşağıdakılardır:

- cinsi həyat haqqında məlumatlar;
- vətəndaşlıq vəziyyəti aktlarının qeydiyyatı haqqında məlumatlar;

- ailə həyatının ayrı-ayrı məqamları haqqında məlumatlar;
- övladlığa götürmə ilə bağlı məlumatlar.

Fərdi məlumatlar alındığı və ya sənədləşdirildiyi gündən etibarən onların əldə olunmasına məhdudiyyətlər qoyulur.

İnformasiya sahibi aşağıdakı hallar istisna olmaqla, fiziki şəxslərin sorğuları əsasında özləri barəsindəki fərdi məlumatla onları tanış etməyə borcludur:

- yetkinlik yaşına çatmayan şəxsin informasiya ilə tanış olması onun mənşəyi haqqında sirri pozursa;
- informasiyanın əldə olunması cinayətin qarşısını almağa, cinayətkarı tutmağa və ya cinayət işində həqiqəti müəyyənləşdirməyə mane olarsa;
- digər insanların hüquq və azadlıqlarının müdafiəsi informasiyanın açıqlanmamasını tələb edirsə;
- informasiya dövlət təhlükəsizliyi naminə toplanıbsa.

Aşağıdakı şəxslər bu maddədə göstərilən fərdi məlumatlarla tanış olmaq və ya onu əldə etmək hüququna malikdir:

- valideynlər və ya qəyyumlar - yetkinlik yaşına çatmayanlar haqqında məlumatlarla;
- qəyyumlar - fiziki cəhətdən qüsurlu şəxslər barədə məlumatlarla;
- dövlət və bələdiyyə qulluqçuları - xidməti vəzifələrinin yerinə yetirilməsi ilə bağlı məlumatlarla;
- fərdi məlumatlarla işləməyə icazə alanlar - yalnız bu icazədə göstərilən məlumatlarla;
- normativ-hüquqi aktlarla və ya müqavilə əsasında təhsil, mədəniyyət, səhiyyə və sosial sahələrdə xidmət göstərən özəl hüquqi şəxslərin işçiləri və sahibkarlar - yalnız bu xidmətlərin göstərilməsi üçün zəruri olan həddə informasiyalarla;
- fiziki şəxslər - özləri barəsindəki informasiyalarla;

İnformasiya sahibi fərdi məlumatları əldə edən şəxslərin qeydiyyatını aparmalı, həmin qeydiyyatda informasiya ilə tanışlığın və ya onu əldə etmənin məqsədi, vaxtı və üsulu göstərilməlidir.

Dövlət sirri təşkil edən məlumatlara dair Azərbaycan Respublikasının qanunvericiliyi

Dövlət sirri haqqında Azərbaycan Respublikası Qanununun 5-ci maddəsinə əsasən dövlət sirri təşkil edən məlumatların siyahısına müəyyən olunmuş məlumatlar - hərbi sahədə, iqtisadi sahədə, xarici siyasət sahəsində və kəşfiyyat, əks-kəşfiyyat və əməliyyat-axtarış fəaliyyəti sahəsindəki məlumatlar aid edilir.

Hərbi sahədə aşağıdakı məlumatlar dövlət sirrini təşkil edir:

Azərbaycan Respublikasının Silahlı Qüvvələrinin, başqa silahlı birləşmələrinin, qanunvericiliklə nəzərdə tutulmuş digər qoşunlarının strateji, operativ və səfərbərlik üzrə yerləşdirilməsinə dair əməliyyatların hazırlanması və keçirilməsi üzrə strateji və əməliyyat planlarının, döyüşü idarəetməyə dair sənədlərin məzmunu, onların döyüş və səfərbərlik hazırlığı, səfərbərlik ehtiyatlarının yaradılması və istifadəsi haqqında;

- Azərbaycan Respublikası Silahlı Qüvvələrinin və Azərbaycan Respublikasının qanunvericiliyinə uyğun olaraq yaradılmış digər silahlı birləşmələrinin quruculuq planları, silahların və hərbi texnikanın inkişafının istiqamətləri, silah və hərbi texnika nümunələrinin yaradılması və modernləşdirilməsi üzrə məqsədli proqramların, elmi-tədqiqat və təcrübi-konstruktor işlərinin məzmunu və yerinə yetirilməsinin nəticələri haqqında;
- silah və hərbi texnika nümunələrinin taktiki-texniki xarakteristikaları və döyüşdə tətbiqi imkanları, hərbi təyinatlı

yeni növ maddələrin xüsusiyyətləri, resepturaları və ya texnologiyaları haqqında;

- milli təhlükəsizlik və müdafiə mülahizələrinə görə xüsusi əhəmiyyət kəsb edən obyektlərin dislokasiyası, təyinatı, hazırlıq və müdafiə olunma dərəcəsi, tikintisi və istismarı, habelə bu obyektlər üçün torpaq, yer təki və akvatoriyalar ayrılması haqqında;
- qoşunların dislokasiyası, həqiqi adları, təşkilati strukturu, şəxsi heyətin sayı və onların döyüş təminatı haqqında, həmçinin hərbi-siyasi və ya əməliyyat şəraiti haqqında;
- Azərbaycan Respublikası ərazisinin müdafiə və mühüm iqtisadi əhəmiyyətli geodeziya məntəqələrinin və coğrafi obyektlərinin koordinatları haqqında.

İqtisadi sahədə aşağıdakı məlumatlar dövlət sirrini təşkil edir:

- Azərbaycan Respublikasının və onun ayrı-ayrı bölgələrinin mümkün hərbi əməliyyatlara hazırlıq planlarının məzmunu, silah və hərbi texnikanın istehsalı və təmiri üzrə sənayenin səfərbərlik gücü, hərbi sahədə istifadə edilən xammal və materialların strateji növlərinin göndərilməsi həcmi, ehtiyatları, həmçinin dövlət material ehtiyatlarının yerləşdirilməsi, faktiki həcmi və istifadəsi haqqında;
- Azərbaycan Respublikasının müdafiə qabiliyyətinin və təhlükəsizliyinin təmin olunması məqsədi ilə onun infrastrukturundan istifadə olunması haqqında;
- mülki müdafiə qüvvələri və vasitələri, inzibati idarəetmə obyektlərinin dislokasiyası, təyinatı və müdafiə olunma dərəcəsi, əhalinin təhlükəsizliyinin təmin olunma dərəcəsi, dövlətin təhlükəsizliyinin təmin olunması üçün nəzərdə tutulan nəqliyyat və rabitənin fəaliyyəti haqqında;
- dövlət müdafiə sifarişlərinin həcmləri, planları (tapşırıqları), silah, hərbi texnika və digər hərbi məhsulların buraxılması və göndərilməsi (pul və ya natura ifadəsində),

onların buraxılışı üzrə mövcud güc və bu gücün artırılması haqqında, göstərilən silah, hərbi texnika və digər hərbi məhsulları işləyib hazırlayan və ya istehsal edən müəssisələr, onların kooperasiya üzrə əlaqələri haqqında;

- dövlətin təhlükəsizliyinə təsir edən mühüm müdafiə və ya iqtisadi əhəmiyyəti olan elmi və texniki nailiyyətlər, elmi-tədqiqat, təcrübi-konstruktor, layihə işləri və texnologiyaları haqqında;
- siyahısı qanunvericiliklə müəyyənləşdirilən strateji növlü faydalı qazıntıların ehtiyatlarının, istehsalının, idxalı və ixracının, satışının həcmi, dövlət ehtiyatları haqqında, pul əsginaslarının, qiymətli kağızların hazırlanması, saxtalaşdırmadan qorunması, həmçinin dövlətin maliyyə fəaliyyətinin digər xüsusi tədbirləri haqqında.

Xarici siyasət sahəsində aşağıdakı məlumatlar dövlət sirrini təşkil edir:

- Azərbaycan Respublikasının xarici-siyasi və xarici-iqtisadi fəaliyyəti haqqında, əgər onların vaxtından əvvəl açıqlanması dövlətin təhlükəsizliyinə ziyan vura bilərsə;
- Azərbaycan Respublikasının digər dövlətlərlə hərbi, elmi-texniki və başqa sahələrdə əməkdaşlığı haqqında, əgər onların vaxtından əvvəl açıqlanması tərəflərdən heç olmasa biri üçün diplomatik fəaliyyətinin həyata keçirilməsində çətinlik yaranmasına səbəb ola bilərsə.

Kəşfiyyat, əks-kəşfiyyat və əməliyyat-axtarış fəaliyyəti sahəsində məlumatlar:

- kəşfiyyat, əks-kəşfiyyat və əməliyyat-axtarış fəaliyyətinin qüvvə və vasitələri, mənbələri, metodları, planları və nəticələri haqqında, habelə bu fəaliyyətin maliyyələşdirilməsinin göstəriciləri haqqında, əgər bu göstəricilər sadalanan məlumatları açıqlayırsa;
- kəşfiyyat, əks-kəşfiyyat və əməliyyat-axtarış fəaliyyətini həyata keçirən orqanlarla konfidensial əsaslarla əməkdaşlıq edən və əməkdaşlıq etmiş şəxslər haqqında;

- dövlət mühafizəsi obyektlərinin təhlükəsizliyinin təmin olunmasının təşkili, qüvvə və vasitələri, metodları haqqında, habelə bu fəaliyyətin maliyyələşdirilməsinin göstəriciləri haqqında, əgər bu göstəricilər sadalanan məlumatları açıqlayırsa;
- şifrlənmiş, o cümlədən kodlaşdırılmış və məxfiləşdirilmiş rabitə sistemləri haqqında, şifrlər, şifrlərin işlənməsi və hazırlanması, onlarla təminat, şifrləmə və xüsusi mühafizə vasitələri haqqında, xüsusi təyinatlı informasiya-analitik sistemləri haqqında;
- məxfi məlumatların mühafizəsi metodları və vasitələri haqqında;
- dövlət sirrinin mühafizəsinin təşkili və faktiki vəziyyəti haqqında;
- Azərbaycan Respublikasının dövlət sərhədinin mühafizəsi haqqında;
- Azərbaycan Respublikasında dövlətin müdafiəsinin, təhlükəsizliyinin və hüquq-mühafizə fəaliyyətinin təmin olunması ilə əlaqədar dövlət büdcəsinin xərcləri haqqında;
- dövlətin təhlükəsizliyinin təmin olunması məqsədi ilə keçirilən tədbirləri açıqlayan kadr hazırlığı haqqında.

Dövlət sirri haqqında Azərbaycan Respublikası Qanununun 7-ci maddəsinə əsasən dövlət sirrinə aid edilməyən və məxfiləşdirilməyən məlumatlar aşağıdakılardır:

- insanların həyat və sağlamlığı üçün təhlükə törədən fövqəladə hadisələr və qəzalar, onların nəticələri, habelə təbii fəlakətlər, onların rəsmi proqnozları və nəticələri haqqında;
- ekologiya, səhiyyə, sanitariya, demoqrafiya, təhsil, mədəniyyət və kənd təsərrüfatının, habelə cinayətkarlığın vəziyyəti haqqında;
- dövlətin vətəndaşlara, vəzifəli şəxslərə, müəssisə, idarə və təşkilatlara verdiyi imtiyazlar, güzəştlər və kompensasiyalar haqqında;

- insan və vətəndaş hüquqlarının və azadlıqlarının pozulması faktları haqqında;
- Azərbaycan Respublikasının ali vəzifəli şəxslərinin səhhəti haqqında;
- dövlət hakimiyyəti orqanları və onların vəzifəli şəxsləri tərəfindən qanunvericiliyin pozulması faktları haqqında.

Məlumatların dövlət sirrinə aid edilməsi qaydalarına uyğun olaraq, məlumatların dövlət sirrinə aid edilməsi və məxfiləşdirilməsi məqsədi ilə dövlət sirrinə aid edilən məlumatların siyahısı hazırlanır. Həmin siyahı qanunilik, əsaslılıq və vaxtında həyata keçirilməsi prinsipləri əsasında, onların sahə, idarə və ya məqsədli proqram mənsubiyyətinə uyğun olaraq, habelə dövlət hakimiyyəti orqanlarının təklifləri nəzərə alınmaqla Azərbaycan Respublikasının Prezidenti yanında Dövlət Sirrinin Mühafizəsi üzrə İdarələrarası Komissiya tərəfindən hazırlanır. Siyahı Azərbaycan Respublikasının Prezidenti tərəfindən təsdiq edilir.

Zəruri hallarda siyahıya yenidən baxıla bilər. Siyahıya yenidən baxılması onun hazırlandığı qaydada həyata keçirilir. Geniş siyahıya daxil edilən məlumatlara aşağıdakı məxfilik dərəcələri verilə bilər:

"Xüsusi əhəmiyyətli" – dövlətin hərbi, xarici-siyasi, iqtisadi, kəşfiyyat, əks-kəşfiyyat və əməliyyat-axtarış fəaliyyəti sahələrinə aid olan və yayılması həmin sahələrdən birində və ya bir neçəsində Azərbaycan Respublikasının mənafeyinə ziyan vura bilən məlumatlara verilən məxfilik dərəcəsi;

"Tam məxfi" – dövlətin hərbi, xarici-siyasi, iqtisadi, kəşfiyyat, əks-kəşfiyyat və əməliyyat-axtarış fəaliyyəti sahələrinə aid olan və yayılması həmin sahələrdən birində və ya bir neçəsində Azərbaycan Respublikasının mərkəzi icra hakimiyyəti orqanının mənafeyinə ziyan vura bilən məlumatlara verilən məxfilik dərəcəsi;

“Məxfi” – dövlətin hərbi, xarici-siyasi, iqtisadi, kəşfiyyat, əks-kəşfiyyat və əməliyyat-axtarış fəaliyyəti sahələrinə aid olan və yayılması həmin sahələrdən birində və ya bir neçəsində ayrı-ayrı dövlət müəssisə, idarə və təşkilatlarının mənafeyinə ziyan vura bilən məlumatlara verilən məxfilik dərəcəsi.

Dövlət sirri haqqında Azərbaycan Respublikası Qanununun 12-ci və 13-cü maddələrinə əsasən dövlət sirri təşkil edən məlumat daşıyıcılarına rekvizitlər verilir. Rekvizitlərdə aşağıdakılar göstərilir:

- müvafiq dövlət hakimiyyəti orqanında, müəssisə, idarə və ya təşkilatda qüvvədə olan məxfiləşdirilməli məlumatlar siyahısının müvafiq bəndinə istinadla daşıyıcıdakı məlumatların məxfilik dərəcəsi;
- daşıyıcını məxfiləşdirən dövlət hakimiyyəti orqanı, müəssisə, idarə, təşkilatın adı;
- qeydiyyat nömrəsi;
- məlumatların məxfiliyinin açılması tarixi və ya şərti, yaxud buna səbəb ola biləcək hadisə.

Bu rekvizitləri məlumat daşıyıcısında əks etdirmək mümkün olmadıqda, onlar daşıyıcıya qoşulan sənədlərdə göstərilir.

Daşıyıcı məxfilik dərəcəsi müxtəlif olan tərkib hissələrindən ibarətdirsə, onların hər birinə müvafiq məxfilik qrifi, bütövlükdə daşıyıcıya isə bu daşıyıcıda ən yüksək məxfilik dərəcəsi olan tərkib hissəsinin məxfilik qrifi verilir.

Məlumatların və məlumat daşıyıcılarının məxfiliyinin açılması dövlət sirri təşkil edən məlumatların yayılmasına və onların daşıyıcıları ilə tanışlıq üçün buraxılmağa bu qanunla nəzərdə tutulmuş qaydada qoyulmuş məhdudiyyətlərin götürülməsidir. Məlumatların məxfiliyinin açılması üçün əsaslar aşağıdakılardır:

- məxfilik müddətinin bitməsi;

- Azərbaycan Respublikasında dövlət sirri təşkil edən məlumatların açıq mübadiləsi sahəsində Azərbaycan Respublikasının beynəlxalq öhdəliklər götürməsi;
- obyektiv halların dəyişməsi nəticəsində dövlət sirri təşkil edən məlumatların mühafizəsinin məqsədəuyğunluğunun aradan qalxması.

Məlumatın məxfilik müddəti onun məxfiləşdirildiyi gündən hesablanır. Bu müddət məxfi məlumatlar üçün 10 ildən, tam məxfi məlumatlar üçün 20 ildən, xüsusi əhəmiyyətli məlumatlar üçün 30 ildən, məxfilik dərəcəsindən asılı olmayaraq şəxsin kəşfiyyat, əks-kəşfiyyat, əməliyyat-axtarış fəaliyyətini həyata keçirən orqanların əməkdaşı olmasını və ya bu orqanlarla konfidensial əsaslarla əməkdaşlıq edən, yaxud əməkdaşlıq etmiş şəxslərin şəxsiyyətini müəyyən etməyə imkan verən məlumatlar üçün 75 ildən çox olmamalıdır. Həmin müddətlər müvafiq icra hakimiyyəti orqanının rəyi ilə uzadıla bilər.

Həmin qanunun 20-ci maddəsinə əsasən dövlət sirrinin mühafizə orqanlarına aşağıdakılar aiddir:

- müvafiq mərkəzi icra hakimiyyəti orqanları;
- dövlət hakimiyyəti orqanları, müəssisə, idarə, təşkilatlar və onların dövlət sirrinin mühafizəsi üzrə struktur bölmələri.

Dövlət sirrinin və konfidensial məlumatların yayılması üzrə cəzalar.

Dövlət sirri və kommersiya sirri təşkil edən məlumatları qeyri-qanuni yolla əldə edən və ya yayan şəxslər Azərbaycan Respublikasının müvafiq qanunvericiliyində nəzərdə tutulmuş qaydada məsuliyyət daşıyırlar.

Cinayət məcəlləsinə müvafiq olaraq, Dövlətə xəyanət, yəni Azərbaycan Respublikasının suverenliyi, ərazi toxunulmazlığı, dövlət təhlükəsizliyi və ya müdafiə qabiliyyəti zərərinə olaraq Azərbaycan Respublikasının vətəndaşı qəsdən

dövlət sirrini xarici dövlətə verərsə, on iki ildən iyirmi ilədək müddətə azadlıqdan məhrum etmə və ya ömürlük azadlıqdan məhrum etmə ilə cəzalandırılır.

Şəxs tərəfindən ona etibar edilmiş və ya xidməti vəzifəsinə və yaxud işinə görə ona məlum olan dövlət sirrini təşkil edən məlumatların yayılması, dövlətə xəyanət əlamətləri olmadıqda - üç ilədək müddətə müəyyən vəzifə tutma və ya müəyyən fəaliyyətlə məşğul olma hüququndan məhrum edilməklə üç ildən altı ilədək müddətə azadlıqdan məhrum etmə ilə cəzalandırılır.

Eyni əməllər ağır nəticələrə səbəb olduqda - üç ilədək müddətə müəyyən vəzifə tutma və ya müəyyən fəaliyyətlə məşğul olma hüququndan məhrum edilməklə dörd ildən səkkiz ilədək müddətə azadlıqdan məhrum etmə ilə cəzalandırılır.

Dövlət sirri təşkil edən məlumatların, məzmununda dövlət sirri olan sənədlərin, habelə barəsindəki məlumatlar dövlət sirri olan əşyaların zor tətbiq etmək hədəsi ilə və ya zor tətbiq etməklə, hədə-qorxu və ya digər məcburetmə vasitələri ilə, talama, aldatma yolu ilə, yaxud məxfi məlumatların gizli əldə edilməsi üçün nəzərdə tutulmuş xüsusi və ya digər texniki vasitələrdən istifadə etməklə qanunsuz əldə edilməsi, dövlətə xəyanət və ya casusluq əlamətləri olmadıqda - iki ildən beş ilədək müddətə azadlıqdan məhrum etmə ilə cəzalandırılır.

Məzmununda dövlət sirri olan sənədlərin, habelə barəsindəki məlumatlar dövlət sirri olan əşyaların, etibar olunan şəxs tərəfindən göstərilən sənədlərlə və ya əşyalarla Azərbaycan Respublikasının qanunvericiliyi ilə müəyyən edilmiş davranış qaydalarının pozulması nəticəsində onların ehtiyatsızlıqdan itirilməsi ağır nəticələrə səbəb olduqda - iki ildən beş ilədək müddətə azadlığın məhdudlaşdırılması və ya üç ilədək müddətə müəyyən vəzifə tutma və ya müəyyən fəaliyyətlə məşğul olma hüququndan məhrum edilməklə beş ilədək müddətə azadlıqdan məhrum etmə ilə cəzalandırılır.

Kommersiya və ya bank sirlərini təşkil edən məlumatların toplanması həmin məlumatları yaymaq və ya onlardan qanunsuz istifadə etmək məqsədi ilə sənədləri oğurlamaqla, satın almaqla və ya hədələməklə, habelə digər qanunsuz üsulla törədildikdə - min beş yüz manatdan iki min beş yüz manatadək miqdarda cərimə və ya bir ilədək müddətə islah işləri və ya iki ilədək müddətə azadlıqdan məhrum etmə ilə cəzalandırılır.

Sahibkarın razılığı olmadan kommersiya və ya bank sirri olan məlumatların tamah və ya başqa şəxsi niyyətlə qanunsuz yolla istifadə edilməsi və ya yayılması külli miqdarda ziyan vurmaqla törədildikdə - cinayət nəticəsində vurulmuş ziyanın üç mislindən beş mislinədək miqdarda cərimə və ya iki ilədək müddətə islah işləri və ya altı ayadək müddətə azadlıqdan məhrum etmə ilə cəzalandırılır.

2.1.2. İnformasiyanın təşkilati təhlükəsizliyi

Təşkilati mühafizə – gizli informasiyanın ələ keçirilməsini, daxili və xarici təhlükələrin yaranmasına maneə yaradan və ya ümumiyyətlə qarşısını alan istehsalat fəaliyyətinin və icraçıların ayrılıqda və birgə qarşılıqlı münasibətlərinin nizamlanmasıdır.

Təşkilati mühafizə aşağıda qeyd olunanları təmin edir:

- obyektin mühafizəsi, rejim tədbirləri, kadrlarla və sənədlərlə işin təşkilii;
- təhlükəsizlik üzrə texniki vasitələrin və sahibkar fəaliyyətinə qarşı yönələn daxili və xarici təhlükələrin aşkarlanması üzrə informasiya-analitik fəaliyyətin istifadəsini;

Təşkilati tədbirlər informasiyanın mühafizəsinin etibarlı mexanizminin yaradılmasında mühüm rol oynayır, belə ki, gizli məlumatların qeyri-qanuni istifadəsinin mümkünlüyü

texniki amillərlə deyil, cinayət fəaliyyəti ilə, istifadəçilərin və ya mühafizə personalının etinasızlığı, məsuliyyətsizliyi və səhlənkarlığı və bəzi hallarda qəsdi ilə şərtlənir. Təkcə texniki vasitələrdən istifadə etməklə bu amillərin təsirindən yayınmaq praktiki olaraq qeyri-mümkündür. Bunun üçün təşkilati-hüquqi və təşkilati-texniki tədbirlərin məcmusu lazımdır.

Əsas təşkilati tədbirlərə aid edilir:

- mühafizə və rejimin təşkili. Bunun məqsədi əraziyə və obyektə kənar şəxslərin gizli daxil olması ehtimalının yaranmasına imkan verməmək; əməkdaşların, qonaqların içəri daxil olmasına və hərəkətinə nəzarəti təmin etmək; gizli işlərin tipinə görə müstəqil giriş sistemi olan ayrı-ayrı istehsalat zonaları yaratmaq; müəssisənin iş rejiminə əməkdaşların əməl etməsinə nəzarət etmək; etibarlı buraxılış rejimini təşkil etmək və s.
- Əməkdaşların işə qəbulu və işə təyin olunmasını nəzərdə tutan fəaliyyəti təşkil etmək. Buraya əməkdaşlarla tanışlıq, onların öyrənilməsi, gizli məlumatlarla işləmə qaydalarına dair təlimatlandırmaq, informasiya təhlükəsizliyinin təmin edilməsi qaydalarının pozulduğu hallarda məsuliyyət tədbirləri ilə tanış edilməsi daxildir.
- sənədlərlə və sənədləşdirilmiş informasiya ilə işi təşkil etmək. Buraya gizli informasiya sənədlərinin və daşıyıcılarının işlənməsi və istifadəsi, onların qeydiyyatı, icrası, qaytarılması, saxlanılması və məhv edilməsi daxildir.
- gizli informasiyanın yığılması, emalı, toplanması və saxlanması üçün nəzərdə tutulan texniki vasitələrin istifadəsini təşkil etmək;
- gizli informasiyaya ünvanlanan daxili və xarici təhlükələrin təhlili və onların təhlükəsizliyinə dair tədbirlərin hazırlanması üzrə işin təşkili;
- gizli informasiya ilə əlaqəli olan əməkdaşların işinə, sənədlərin və texniki daşıyıcıların qeydiyyatı, saxlanması və

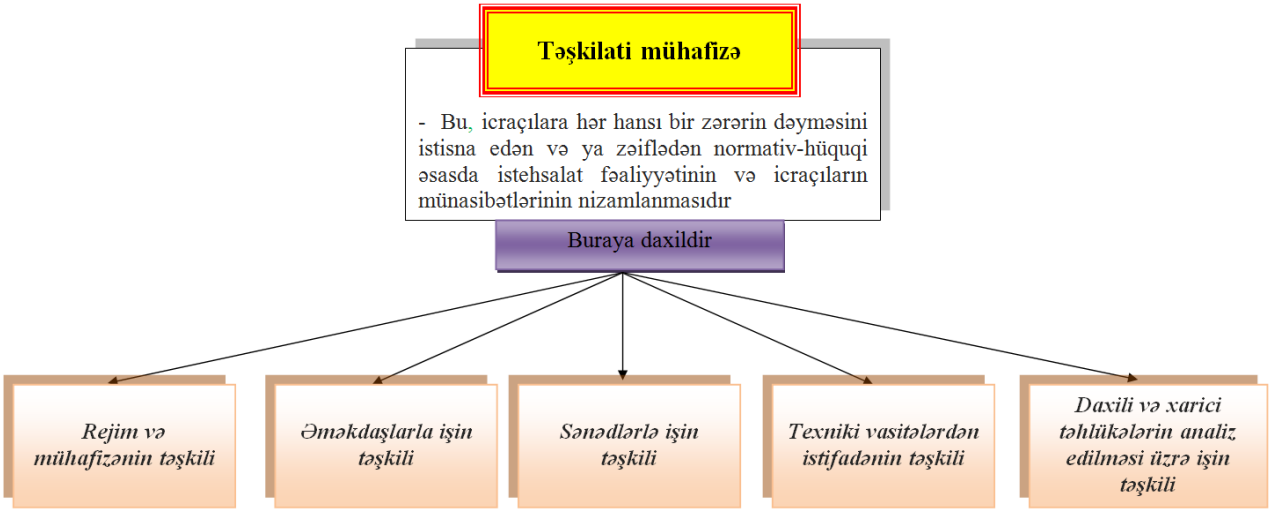
məhv edilməsi qaydalarına sistemli nəzarətin həyata keçirilməsi üzrə işlərin təşkili (şəkil 2.3).

Hər bir müəssisənin bu təşkilati tədbirləri həyata keçirilməsi üzrə öz səciyyəvi istiqaməti vardır.

Təşkilati tədbirlərin səciyyəvi xüsusiyyəti personal kompüterlərin, informasiya sistemlərinin və şəbəkələrin mühafizəsinin təşkilidir.

Personal kompüterlərin və informasiya sistemlərinin təşkilati mühafizə tədbirləri aşağıda qeyd olunan hallarda tətbiq olunur:

- binaların, şəbəkə qovşaqlarının və digər informasiya sistemi obyektlərinin layihələndirilməsi, tikilməsi və avadanlıqla təchiz olunması zamanı;
- personalın seçilməsi və hazırlığı zamanı. Bu halda işə götürülənlərin yoxlanılması, məxfi informasiya ilə işləmə qaydalarının öyrədilməsi, mühafizə qaydalarının pozulmasına cavabdehlik tədbirləri ilə tanışlıq nəzərdə tutulur;
- sənədlərin və digər daşıyıcıların qorunması və istifadəsi zamanı (nişanlama, qeydiyyat, verilmə və alınma qaydalarının müəyyən olunması, sənədləşmənin aparılması və s.);



Şəkil 2.3. Təşkilati tədbirlərin strukturu

- növbəli iş rejimi olarkən texniki vasitələrə, kompüterlərə və informasiya sistemlərinə etibarlı buraxılış rejiminin tətbiq olunması zamanı (növbələrdə informasiyanın mühafizəsi üzrə məsul şəxslərin müəyyən olunması, əməkdaşların işinə nəzarət, iş jurnallarının tutulması, müəyyən olunmuş qaydada gizli istehsalat sənədlərinin məhv edilməsi);
- proqram təminatına dəyişikliklər edilən zaman (dəyişikliklər layihəsinə dəqiq baxılması və təsdiq olunması, mühafizə tədbirlərinin tələblərinə cavab verməsi, dəyişikliklərinrəsmiləşdirilməsi və s.);
- istifadəçilərin işinə nəzarət zamanı.

Əsas təşkilati tədbirlərdən biri də gizli informasiya sistemlərində informasiya mühafizəsinin xüsusi ştat xidmətlərinin yaradılmasıdır.

Aydındır ki, təşkilati tədbirlər dəqiq planlaşdırılmalı, istiqamətləndirilməli və hər hansı bir təşkilati strukturla həyata keçirilməlidir. Bu strukturda sahibkar fəaliyyətinin təhlükəsizliyi və informasiyanın mühafizəsi üzrə müvafiq mütəxəssislər çalışmalıdır.

Belə struktur işini əsasən müəssisənin (firma, təşkilat) təhlükəsizlik xidməti yerinə yetirir. Bu xidmət də aşağıdakı funksiyaları yerinə yetirməlidir:

- əməkdaşların, maddi və material dəyərlərin, gizli informasiyanın mühafizəsinin təşkili və təmin edilməsini;
- əraziyə, binalara buraxılış və obyektdaxili rejimin təşkili, əməkdaşların, qonaqların rejimin tələblərinə riayət etməsinə nəzarəti;
- informasiyanın mühafizəsi üzrə əlaqələrin hüquqi və təşkilati nizamlanması üzrə işlərə rəhbərliyi;
- informasiyanın mühafizəsi və təhlükəsizliyi üzrə əsas sənədlərin, xidmətlərin əsasnamələrinin, əmək müqavilələrinin, rəhbər təlimatların və əməkdaşların vəzifə təlimatlarının işlənməsində iştirakı;

- digər bölmələr ilə gizli məlumatlarla fəaliyyətə dair tədbirlərin işlənməsi və həyata keçirilməsi;
- istənilən təhlükəni aşkar etmək və onlara qarşı əks tədbirlər görmək üçün istehsalat, kommersiya, maliyyə və digər fəaliyyət sahələrinin öyrənilməsi, təhlükəsizlik rejiminin pozulması hallarının qeydiyyatının və təhlilinin aparılması, rəqib və digər təşkilatların pis niyyətli məqsədləri, müəssisənin, onun müştərilərinin fəaliyyəti haqqında məlumatların toplanması və analizi;
- məlumatların açıqlanması, sənədlərin itirilməsi, gizli informasiyanın sızması və s. hallar üzrə xidməti təhqiqatın təşkili və aparılması;
- "Konfidensial xarakterli məlumatların siyahısı"nın və digər normativ aktların işlənilməsi, yenilənməsi, siyahı üzrə işləmə və siyahıya əlavələrin edilməsi;
- müəssisənin istehsalat sirlərinin mühafizəsi üzrə normativ sənədlərin tələblərinin dəqiqliklə yerinə yetirilməsinin təmin edilməsi;
- informasiyanın mühafizəsinin və istehsalat fəaliyyətinin təhlükəsizliyinin bütün istiqamətləri üzrə müəssisənin və təhlükəsizlik xidməti əməkdaşlarının qeydiyyatının aparılmasının təşkili və həyata keçirilməsi;
- gizli iş üçün ayrılmış yerlərin, texniki vasitələrin, onlarda ola biləcək informasiyanın mümkün sızma kanallarının və qorunan sirlərin mənbələrinə daxilolma kanallarının qeydiyyatını aparmaq və onlara ciddi nəzarət etmək;
- daxili və xarici təhlükələr nəticəsində maddi və mənəvi ziyanın vurulması cəhdlərinin qarşısının alınması üzrə bütün lazımi tədbirlərin görülməsini təmin etmək;
- rayonun (ərazinin) kriminogen vəziyyətinin öyrənilməsi və böhran şəraitində yardımın göstərilməsi məqsədi ilə hüquq-mühafizə orqanları və qonşu müəssisələrin təhlükəsizlik xidmətləri ilə əlaqələri qoruyub-saxlamaq;

Təhlükəsizlik xidməti birbaşa müəssisənin rəhbərinə tabe olan müstəqil təşkilatdır. Təhlükəsizlik xidmətinə müəssisənin direktorunun təhlükəsizlik üzrə müavini rəhbərlik edir.

Təhlükəsizlik xidməti təşkilati olaraq aşağıdakı strukturlardan ibarət olmalıdır:

- rejim və mühafizə dəstəsi;
- gizli xarakterli sənədləri emal edən xüsusi dəstə;
- mühəndis-texniki dəstə;
- informasiya-analitik dəstə.

Bu heyətlə təhlükəsizlik xidməti gizli informasiyanın istənilən təhlükədən mühafizəsini təmin etmək iqtidarına malikdir.

Müəssisənin təhlükəsizlik xidmətinin həlli məsələləri aşağıdakılardan ibarət olmalıdır:

- vəzifəsindən asılı olaraq gizli xarakterli məlumatlara giriş hüququ olan şəxslərin müəyyən edilməsi;
- gizli məlumatların toplanması sahələrinin müəyyən edilməsi;
- müəssisə ilə kooperativ əlaqələri olan tərəfdaş müəssisələrin müəyyən edilməsi (istehsalat münasibətləri nəticəsində gizli xarakterli məlumatlarnəzarətdən çıxa bilər);
- gizli informasiya ilə işləməyə buraxılmayan, lakin belə məlumatlara həddən artıq maraq göstərən şəxslərin müəyyən edilməsi;
- təşkilata maddi ziyanın vurulması, iqtisadi rəqibin sıradan çıxarılması və ya nüfuzdan salınması məqsədi ilə qorunan informasiyaları əldə etməkdə maraqlı olan təşkilatların, həmçinin kənar müəssisələrin casuslarının aşkara çıxarılması;
- gizli xarakterli məlumatlar olan sənədlərin mühafizə sisteminin işlənməsi;

- sıradan çıxması müəssisəyə maddi zərər vura biləcək, qəza baxımından zəif sahələrin müəyyən edilməsi;
- sıradan çıxması böyük iqtisadi itkilərə yol açа biləcək müəssisənin texnoloji avadanlıqlarının müəyyən edilməsi;
- qanunsuz dəyişikliklər edildikdə buraxılan məhsulun keyfiyyətini itirməsinə gətirib çıxaran, müəssisəyə maddi və ya mənəvi zərər vura bilən istehsalat dövriyyəsi texnologiyalarında zəif yerlərin aşkar edilməsi;
- qanunsuz müdaxilə edildikdə hazır məhsulun və ya yarımfabrikatların götürülməsinə, oğurlanmasına səbəb olan müəssisənin zəif yerlərinin müəyyən edilməsi və onların fiziki müdafiə və mühafizə olunması;
- müəssisənin, personalın, məhsulun və informasiyanın hüquqi, təşkilati və mühəndis-texniki mühafizəsi tədbirlərinin təyin edilməsi və əsaslandırılması;
- müəssisənin iqtisadi, sosial və informasiya təhlükəsizliyi sisteminin mükəmməlləşdirilməsinə yönəldilmiş lazımi tədbirlərin işlənməsi;
- elmin və texnikanın yeni nailiyyətlərinin, iqtisadi və informasiya təhlükəsizliyinin təmin edilməsi sahəsində qabaqcıl təcrübələrin müəssisənin fəaliyyətinə tətbiq edilməsi;
- təhlükəsizlik xidməti əməkdaşlarının funksional vəzifələrinin yerinə yetirilməsi üzrə müvafiq tədrisin və ya hazırlıq kurslarının təşkili;
- müəssisənin iqtisadi və informasiya təhlükəsizliyinin təmin edilməsinin vəziyyətinin öyrənilməsi, analizi və qiymətləndirilməsi və onların təkmilləşdirilməsi üzrə təkliflərin və tövsiyələrin işlənməsi;
- iqtisadi və informasiya təhlükəsizliyinin təmin edilməsi üzrə tədbirlər sisteminin təkmilləşdirilməsi məqsədi

ilə texniki vasitələrin əldə olunması istiqamətində texniki-iqtisadi əsaslandırmanın işlənməsi, mütəxəssislərdən məsləhətlərin alınması, lazımi sənədləşmənin hazırlanması.

Təşkilati tədbirlər informasiyanın kompleks mühafizəsinin formalaşdırılması, həyata keçirilməsi və müəssisənin təhlükəsizlik sisteminin yaradılmasında həlledici rol oynayır.

2.2. İnformasiya mühafizəsini təmin edən xidmətlər

Hər bir dövlətin təhlükəsizliyini təmin etmək məqsədilə kəşfiyyat fəaliyyətini həyata keçirən xüsusi xidmət orqanları vardır. Bu xidmətlər öz dövlətlərinin qanunvericiliyinə uyğun olaraq, kəşfiyyatdan əlavə, əks-kəşfiyyat, kriptoanaliz, məlumatların əldə edilməsi, təhlili, emalı, ötürülməsi, təhlükəsizliyinin təmin edilməsi və d. funksiyaları icra edir.

Bundan əlavə, hər bir dövlətin bəzi xüsusi xidmət orqanları bilavasitə mülki aviasiya fəaliyyətinin təhlükəsizliyinin təmin edilməsində, qanunsuz müdaxilə aktlarının qarşısının alınmasında iştirak edir.

2.2.1. Keçmiş Sovet İttifaqının xüsusi xidmət orqanları

İlk öncə keçmiş SSRİ-nin 2 xüsusi xidmət orqanının - XX əsrdə dünya tarixinə öz təsirini göstərmiş Dövlət Təhlükəsizlik Komitəsinin (DTK-nın) (rusca - КГБ – Комитет Государственной Безопасности) və Baş Kəşfiyyat İdarəsinin (BKİ-nin) (rusca ГРУ – Главное Разведывательное Управление) fəaliyyətini nəzərdən keçirmək gərəkdir. Əlbəttə ki, bu 2 qurumun siyasi məqsədi və maraqları indiki dövlətlərin kəşfiyyat xidmətlərinin məqsədlərindən tamam fərqlənirdi. Lakin DTK və BKİ-nin strukturunun və iş prinsipinin analizi XXI əsrin demokratik dövlətlərinin xüsusi xidmət orqanlarının inkişaf nəzəriyyəsini daha yaxşı anlamağa imkan verir.

SSRİ-nin Dövlət Təhlükəsizlik Komitəsi

SSRİ-nin Nazirlər Şurasının nəzdindəki Dövlət Təhlükəsizlik Komitəsi 13 mart 1954-cü ildə dövlət təhlükəsizliyi ilə əlaqəli olan idarələrin, xidmətlərin və bölmələrin Daxili İşlər Nazirliyindən ayrılması yolu ilə yaradılmışdı, 1991-ci ilin 3 dekabrında isə o, fəaliyyətini dayandırmışdır.

Dövlət Təhlükəsizlik Komitəsinin əsas funksiyaları - xarici kəşfiyyat, əks-kəşfiyyat, əməliyyat-axtarış fəaliyyəti, SSRİ-nin sərhədlərinin qorunması, Sovet İttifaqı Kommunist Partiyasının rəhbərlərinin və SSRİ hökumətinin mühafizəsi, hökumət rabitəsinin təşkili, həmçinin millətçiliklə, fərqli düşüncəylə, cinayətkarlıqla və antisovet fəaliyyətinə qarşı mübarizə idi. Bundan əlavə, Sovet İttifaqı Kommunist Partiyasının Mərkəzi Komitəsinin dövlət təhlükəsizliyi və ölkənin müdafiəsi, Sovet İttifaqındakı sosial-iqtisadi vəziyyət, xarici siyasət məsələləri ilə bağlı məlumatlarla təmin etmək DTK-nın əsas vəzifələrinə daxil idi.

Şəkil 2.4. DTK-nın emblemi

DTK sisteminə dövlət təhlükəsizliyinin orqanları, sərhəd qoşunları və hökumət rabitəsi qoşunları, hərbi əks-kəşfiyyat orqanları, təhsil və elmi-tədqiqat müəssisələri daxil idi.

DTK-nın strukturu:

Baş idarələr:

- Birinci baş idarə (xarici kəşfiyyat, əks kəşfiyyat və informasiyaların analizi);
- İkinci baş idarə (daxili təhlükəsizlik, əks kəşfiyyat);
- Sərhəd qoşunları baş idarəsi (SQBİ);
- Səkkizinci baş idarə (rabitə kəşfiyyatı, rabitə vasitələrinin təhlükəsizliyi, şifrləmə xidməti).

Baş idarələrdən əlavə, DTK-nin strukturuna aşağıdakı idarələr və bölmələr daxil idi:

- Üçüncü idarə (orduda kəşfiyyat);
- Dördüncü idarə (səfirliklərin mühafizəsi və daxili təhlükəsizliyi);
- Beşinci idarə (konstitusiya quruluşunun qorunması (kənar düşüncələrin aradan qaldırılması, ideoloji məsələlər));
- Altıncı idarə (iqtisadi təhlükəsizlik);
- Yeddinci idarə (kənar müşahidə);
- Doqquzuncu idarə (Hökumətin mühafizəsi)
- On beşinci idarə (Dövlət obyektlərinin mühafizəsi);
- On altıncı idarə (Radioələkeçirmə və elektron kəşfiyyat);
- Hərbi obyektlərin tikintisi idarəsi.

Bölmələr və xidmətlər:

- İstintaq bölməsi
- Hökumət rabitəsi
- DTK-nın ali məktəbi
- Altıncı bölmə (ələ keçirmə və korrespondensiyanın yoxlanılması)
- On ikinci bölmə (qulaqasma)

1954-cü ilin əvvəllərində DTK-nın əməliyyat-kəşfiyyat bölmələrinin sayı təxminən 80000 nəfərdən ibarət idisə, 1991-ci ildə DTK orqanlarının əməkdaşlarının sayı təxminən 480 000 nəfər təşkil edirdi.

DTK-nın mərkəzi aparatının əsas hissəsi Moskvada, Dzerjinski meydanında yerləşirdi (şəkil 2.5) (1990-cı ildən – Lublyansk meydanı) (hal-hazırda həmin binada Federal Təhlükəsizlik Xidmətinin qərargahı yerləşir).

Şəkil 2.5. Dzerjinski meydanında yerləşən DTK-nın mərkəzi aparatı

2.2.2. Ümummilli Lider Heydər Əliyevin təhlükəsizlik orqanlarında fəaliyyəti

Ümummilli lider Heydər Əliyevin çox gənc yaşlarından dövlət hakimiyyətinin mühüm strukturlarından birində - 1944-cü ilin may ayında təhlükəsizlik orqanında xidmətə başlaması, burada çalışdığı uzun illər ərzində yüksək peşəkarlığa və təşkilatçılıq bacarığına yiyələnməsi onun həyat yolunu müəyyənləşdirən başlıca amil idi. Sovet hakimiyyəti dövründə özünün nadir istedadı və fenomenal xüsusiyyətləri sayəsində bu orqanda sıravi əməkdaşdan komitə sədri və general-mayor rütbəsinədək yüksəlmiş ilk azərbaycanlı kimi adını tarixə yazdıran Heydər Əliyev, həm də müstəqil Azərbaycanın milli təhlükəsizlik konsepsiyasının müəllifi və onun gerçəkləşməsini təmin edən səmərəli idarəçilik sisteminin yaradıcısı oldu.

Şəkil 2.6. Heydər Əliyev Azərbaycan SSR Dövlət Təhlükəsizliyi Komitəsinin sədri vəzifəsində

Müasir dövrdə təhlükəsizlik orqanlarının vəzifəsi şəxsiyyətin, cəmiyyətin və dövlətin ən ümdə maraqlarını müdafiə etmək, ölkənin sabit inkişafına nail olmaq, xarici və daxili təhlükələrə qarşı mübarizə aparmaqdır. Lakin sovet hakimiyyəti illərində bu orqanların fəaliyyəti tamamilə siyasiləşdirilmiş, hakim kommunist ideologiyasının tələb və prinsiplərinə tabe edilmişdi. Bu tələbləri yerinə yetirməklə yanaşı, həm də milli düşüncəyə, doğma xalqına məxsus mənəvi-əxlaqi dəyərlərə sadiq qalmaq xüsusi xidmət orqanı əməkdaşından böyük hünər və cəsarət tələb edirdi. Ulu Öndər Heydər Əliyev yalnız özünün fenomenal şəxsi keyfiyyətləri sayəsində bu çətin missiyanın öhdəsindən gəlməyi bacarmışdır.

Məlum olduğu kimi, Heydər Əliyev 1949-1950-ci illərdə Leninqradda (indiki Sankt-Peterburqda) Dövlət Təhlükəsizlik Komitəsinin Ali Məktəbində təhsil almışdır. Məktəbi bitirərkən verilən xidməti xasiyyətnamədə baş leytenant Heydər Əliyevin özünü yalnız nümunəvi tərəfdən göstərdiyi, öyrənilən fənlər üzrə imtahan və məqbullardan əla qiymətlər aldığı, adının məktəbin "Şərəf lövhəsi"nə salındığı qeyd edilməklə yanaşı, bildirilirdi ki, o, operativ məsələlərin həllində ən mühüm olanı bacarıqla tapır, əməliyyat şəraitində həll yolunu sərbəst və

düzgün seçir, doğru qərarlar qəbul edərək əməliyyat sənədlərini hərtərəfli və əsaslandırılmış şəkildə tərtib edir.

O, 1950-ci ildə Azərbaycan SSR Dövlət Təhlükəsizliyi Komitəsində bölmə rəisi təyin edilib.

Azərbaycan Respublikasının Dövlət Təhlükəsizliyi Xidmətinin arxivində Heydər Əliyevin əks-kəşfiyyat sahəsindəki peşəkarlığını əyani olaraq təsdiqləyən çoxsaylı sənədlər saxlanılır. Vaxtilə xarici xüsusi xidmət orqanlarının respublikamızda planlaşdırdığı və həyata keçirməyə çalışdığı kəşfiyyat-pozuculuq tədbirlərinin qarşısının alınması, agentura və casusluq fəaliyyətinin aşkar edilməsi məqsədilə onun iştirakı və rəhbərliyi ilə bır sıra uğurlu və mükəmməl əməliyyatlar həyata keçirilmiş, bu əməliyyatlarda əldə edilən təcrübə SSRİ-nin digər təhlükəsizlik orqanlarında öyrənilmiş və geniş tətbiq edilmişdir.

Heydər Əliyev 1958-ci ildə Azərbaycan SSR Dövlət Təhlükəsizliyi Komitəsinin əks-kəşfiyyat şöbəsinin rəisi, 1964-cü ildə DTK-nın sədr müavini təyin edilib.

1966-cı ildə Moskvada DTK-nın F.E. Dzerjinski adına Ali Məktəbinin rəhbər heyətin təkmilləşdirilməsi kurslarını müvəffəqiyyətlə bitirib. 1967-ci ildə Azərbaycan SSR Nazirlər Soveti yanında Dövlət Təhlükəsizliyi Komitəsinin sədri vəzifəsinə təyin edilib və həmin ildə də ona general-mayor rütbəsi verilib.

Bununla belə, Heydər Əliyevin 1950-1960-cı illərdə dövlət təhlükəsizliyi orqanlarında xidməti uğurları və milli mənafeləri qorumaq təşəbbüsləri ona heç də asanlıqla başa gəlməmiş, bəzən çox ciddi sınaqlara məruz qoymuşdur. Ulu Öndər xatırlayırdı ki, həmin dövrdə dövlət təhlükəsizliyi sistemində əsas rəhbər vəzifələrdə başqa millətlərə mənsub olan kadrlar işləyirdi, yerli kadrlar isə nəinki az idi, üstəlik də, onların bir çoxu yüksək savada, biliyə, yaxud keyfiyyətə malik deyildilər. Repressiya illərindən sistemdə qalmış, milli mənafelərə xilaf çıxmış belə kadrlar Heydər Əliyevin yerli kadr

potensialını yeniləmək və gücləndirmək, say tərkibini yüksək mənəviyyatlı, millətini sevən gənclərin hesabına artırmaq təşəbbüslərinə hər vəchlə mane olmağa çalışıb, müəyyən fitnə-fəsadlara əl atsalar da, onun dəmir iradəsi və peşəkarlığı qarşısında aciz qalırdılar. Sonralar bu hadisələri xatırlayarkən Ulu Öndər demişdir: *"Ancaq 1950-ci illərin ikinci yarısında, 1960-cı illərdə, sonra 1970-ci illərdə Azərbaycanın təhlükəsizlik təşkilatında ciddi dəyişikliklər həyata keçirmək mümkün oldu"*. Heydər Əliyevin Azərbaycan SSR Dövlət Təhlükəsizlik Komitəsində əks-kəşfiyyat idarəsinə rəhbərlik etdiyi 1956-65-ci illər ərzində, xüsusilə də komitə rəhbərliyinə irəli çəkildiyi 1965-ci ildən sonra bu orqana milli kadrların cəlb edilməsi, onların yetişdirilib, həlledici iş sahələrində rəhbər vəzifələrə irəli çəkilməsi bu istiqamətdə mühüm addım olmuşdur. Məhz Ulu Öndərin səyi və birbaşa iştirakı ilə həmin dövrdən təhlükəsizlik orqanlarında azərbaycanlıların xüsusi çəkisi sürətlə artaraq, 1980-ci illərdə 70 faizə çatmış, bu proses dinamik, dönməz xarakter almışdır. Bu dövrdə Azərbaycan təhlükəsizlik orqanlarında formalaşmış yeni nəsil sonralar müstəqil Azərbaycanın milli təhlükəsizlik orqanlarının kadr potensialının özəyini təşkil etmişdir. Həmin dövrdə respublikanın təhlükəsizlik təşkilatının milliləşdirilməsini ən böyük nailiyyət kimi dəyərləndirən Heydər Əliyev bu addımın təşkilatın fəaliyyətini milli mənafelərə daha çox uyğunlaşdırmaq imkanı yaratdığını da vurğulayırdı.

Azərbaycan Kommunist Partiyası Mərkəzi Komitəsinin 1969-cu il iyulun 14-də keçirilmiş plenumunda Heydər Əliyev Azərbaycan Kommunist Partiyası Mərkəzi Komitəsinin birinci katibi seçilmişdir.

Ümummilli Lider sovet hakimiyyəti illərində Dövlət Təhlükəsizliyi Komitəsində çalışdığı və ona rəhbərlik etdiyi dövrdə bu orqanın milli kadr potensialını artırmaqla, milliləşdirmə siyasəti aparmaqla yanaşı, həm də respublikada milli oyanışın, bu prosesin fəal iştirakçısı olan vətənpərvər

ziyalıların siyasi-ideoloji təqiblərdən qorunması, öz yaradıcılıqlarında xalqımızın tarixi-mənəvi dəyərlərini təbliğ etməsi üçün hətta əfsanələşmiş, yaddaşlarda əbədi yaşayan misilsiz fədakarlıqlar göstərmişdir. Azərbaycanın bir çox görkəmli ziyalılarını - akademik Ziya Bünyadovu, Xəlil Rza Ulutürkü, Bəxtiyar Vahabzadəni, Anarı və digər ədiblərimizi milli düşüncələrinə görə təqibdən məhz Heydər Əliyev qorumuş, əslində, özünün yüksək karyerasını təhlükə altına atmaqla milli mənafelərin açıq-aşkar müdafiəsinə qalxmışdır. Sonralar Azərbaycana rəhbərlik etdiyi illərdə respublikada yaradıcı ziyalılar arasında siyasi dissidentlərin olmaması barədə danışarkən Ulu Öndər demişdir: *"...Əgər axtarsaydıq, çox dissident çıxarmaq olardı. Amma biz axtarmırdıq. Bu nə deməkdir? Bu o deməkdir ki, həmin dissident sayılanların əsərlərini biz qəlbən qəbul edirdik və onların özünə yol tapması üçün imkanlar yaradırdıq. Beləliklə, həmin müəlliflərə öz həmrəyliyimizi bildirirdik".*

Göründüyü kimi, mövzu və məzmunca mövcud ideoloji-siyasi istiqamətə zidd əsərləri qəlbən qəbul etmək, onları qələmə alan müəlliflərlə həmrəy olmaq sovet təhlükəsizlik orqanı rəhbərinin təkcə hünər və cəsarətindən, milli ideyalara sədaqətindən deyil, həm də özünün mənəvi gücünə və xarizmasına inamından, milliyyətçiliyi dövlət mənafeyinə xəyanət hesab edən Mərkəzin qarşısında öz mövqeyini qoruya bilmək bacarığından xəbər verir. Məhz Ümummilli Lider Heydər Əliyevin sayəsində Azərbaycan cəmiyyətinə aşılanan özgürlük və milli dirçəliş ideyaları, ötən əsrin 80-90-cı illərinin qovuşuğunda xalqımızın yenidən baş qaldıran azadlıq və müstəqillik mübarizəsinin rüşeymini təşkil etmişdir. Ulu öndər Heydər Əliyev istər dövlət təhlükəsizliyi sistemində çalışdığı, istərsə də respublikaya birinci dəfə rəhbərlik etdiyi dövrdə erməni millətçilərinin Azərbaycana qarşı torpaq iddialarının qarşısının alınması üçün əksər hallarda təkbaşına, yalnız öz təcrübəsi, siyasi bəsirəti və geniş intellektual

imkanları hesabına davamlı olaraq qətiyyətlə mübarizə aparmışdır. Bu bir tarixi həqiqətdir ki, "Böyük Ermənistan" xülyası ilə yaşayan erməni millətçiləri, onların hərbi-terrorçu təşkilatları və siyasi ideoloqları ərazilərimizi ələ keçirmək üçün xalqmızın əleyhinə fasiləsiz şəkildə fitnəkar planlar qurur, açıq düşmənçilik fəaliyyəti göstərirlər. Ötən əsrin əvvəllərində Azərbaycan torpaqlarında erməni dövlətinin qurulmasından, sonrakı illərdə kommunist rejiminin himayəsi ilə yenidən respublikamızdan qoparılan ərazilər hesabına bu dövlətin sərhədlərinin genişlənməsindən başlamış, yüz minlərlə soydaşımızın müxtəlif illərdə həmin sərhədlərin hüdudlarından, öz ata-baba yurdlarından qovulub çıxarılmasına, nəhayət, Dağlıq Qarabağın Ermənistana birləşdirilməsi üçün başlanan və bu gün də davam edən işğalçı hərbi təcavüzədək saysız-hesabsız erməni fitnəkarlığı tarixin yaddaşına əbədi yazılmışdır.

Bu tarixdə bir unudulmaz dövr var: Heydər Əliyevin şəxsi və siyasi iradəsi sayəsində ermənilərin çirkin niyyətlərinin puça çıxarılması dövrü. Ötən əsrin 60-cı illərində daşnak-millətçi ünsürlər torpaq iddialarını gerçəkləşdirmək üçün Dağlıq Qarabağda fəallaşmağa başladılar. Xüsusi xidmət orqanları bu bölgəni daim diqqətdə saxlasa da, təxribatçılar imkan tapıb 1967-ci ilin yayında indiki Xankəndi şəhərində milli zəmində qarşıdurma yarada, burada yaşayan azərbaycanlılar və ermənilər arasına ədavət sala bildilər. Nəticədə bir neçə azərbaycanlı vəhşicəsinə qətlə yetirildi. Baş vermiş hadisənin təfərrüatına varmadan deyək ki, məhz respublika Dövlət Təhlükəsizlik Komitəsinin sədri kimi Heydər Əliyev birbaşa Xankəndinə gəlib, burada qalaraq hadisələrin əsl günahkarlarının - azğınlaşmış ermənilərin ifşa edilməsinə və öz haqlı cəzalarını almasına, eləcə də bu hadisələrə laqeydlik göstərmiş vilayət rəhbərləri haqqında sərt tədbirlər görülməsinə nail oldu.

Çox təəssüf ki, keçmiş ittifaq dövlətinin rəhbərliyi Ermənistanın haqsız və ədalətsiz torpaq iddialarının qarşısını almağa cəhd göstərmir, Azərbaycanın o vaxtkı siyasi rəhbərliyinin isə, sadəcə, bu iddialara tutarlı cavablar verməyə gücü çatmırdı. Sonralar Ulu Öndər 1968-1969-cu illərdə bununla bağlı baş vermiş hadisələr barədə tarixi faktlara istinadən demişdir: *"...Mənim xatirimdədir, o vaxt mən respublikanın rəhbəri deyildim, amma rəhbər vəzifə tuturdum. Respublikanın o vaxtkı rəhbərləri Ermənistanın rəhbərləri ilə bir neçə dəfə görüşlər keçirdilər. 1968-ci ildə protokol da imzalanmışdı... 1969-cu ilin iyul ayında mən Azərbaycanın o vaxtkı Mərkəzi Komitəsinin birinci katibi seçildim. Bir neçə gün idi ki, işləyirdim, bu məsələni gətirib mənim qarşıma çıxardılar. Moskvadan da çox böyük təzyiq edirdilər ki, qərar qəbul olunub, tez edin, icrasına sərəncam verin. Dedim, bilirsiniz, bu qərar mayda qəbul olunub, əgər iyul ayına qədər icra edilməyibsə, imkan verin, mən onu bir araşdırım. Şübhəsiz ki, mən araşdırandan sonra gördüm ki, buna razılıq verə bilmərəm. Mən razılıq vermədim. Bu da məlumdur. Nə qədər ki, mən Azərbaycanda işlədim, o qərar həyata keçmədi..."*.

Sovet Azərbaycanının rəhbəri vəzifəsində olarkən torpaqlarımızın işğalına yönələn erməni fitnəkarlığını ifşa etmək və bu torpaqların əzəli Azərbaycan torpaqları olduğunu sübut etmək məqsədi ilə hələ 1978-ci ildə böyük cəsarət və siyasi iradə nümayiş etdirərək, Moskvadan və İrəvandan olan böyük nümayəndə heyətinin iştirakı ilə ermənilərin Qarabağ ərazisinə köçməsinin 150 illiyini təntənəli qeyd etmiş və bu hadisənin 150 illiyi şərəfinə Dağlıq Qarabağın Ağdərə rayonu ərazisində abidə ucaldılmışdı. Hansı ki, erməni vandalları Dağlıq Qarabağı işğal etdikdən sonra ilk olaraq həmin abidəni tamamilə məhv etmişdilər.

Təəssüf ki, Ulu Öndər Heydər Əliyevin, öz iradəsindən asılı olmayaraq Azərbaycana rəhbərlikdən uzaq qaldığı bir zamanda erməni millətçiləri və separatçıları öz istəklərini

gerçəkləşdirməyə, xalqımıza və dövlətimizə sağalması hələ də mümkün olmayan yaralar vurmağa imkan tapırdılar. Tarixin və taleyin hökmü ilə yenidən Azərbaycana rəhbərliyə qayıtdıqdan, müstəqil dövlətiçiliyi real olaraq bərpa etməyə, yeni, müasir dövlət idarəçiliyi sistemi qurmağa başladıqdan sonra Heydər Əliyev həm də Ermənistanın hərbi təcavüzkarlığının qarşısını almaq üçün zəruri addımlar atmalı oldu. 1993-cü ilin iyununda xalqın israrlı və təkidli tələbi ilə siyasi hakimiyyətə qayıdan Ulu Öndərin qətiyyəti və uzaqgörən siyasəti nəticəsində müstəqil dövlətçiliyimiz məhv olmaq təhlükəsindən qurtuldu, müstəqilliyimizin əbədiliyi və dönməzliyi təmin edildi.

Heydər Əliyevin hələ sovetlər dövründə Azərbaycanın gələcək müstəqilliyini düşünərək respublika həyatının bütün sahələrində misilsiz işlər gördüyü əbədi olaraq tarixin yaddaşına yazılmışdır və bugünki güclü Azərbaycan Respublikasının təməli də məhz Ulu Öndərimizin dövlət təhlükəsizlik orqanlarına və davamlı olaraq ölkəmizə rəhbərlik etdiyi vaxtlardan qoyulmuşdur. Həmin dövrdə yüzlərlə gənc keçmiş SSRİ-nin nüfuzlu ali məktəblərinə göndərilmiş, milli hərbi kadrların hazırlanması məqsədi ilə Bakıda Cəmşid Naxçıvanski adına Hərbi Məktəb açılmışdır. Bunun nəticəsidir ki, hazırda dövlətçiliyimizin möhkəmləndirilməsinə uğurla xidmət edən böyük ziyalı, alim, mühəndis, hərbçi və digər mütəxəssis nəsli vardır. Ulu Öndər Heydər Əliyev SSRİ-nin rəhbərlərindən olduğu vaxtda da gələcək müstəqil Azərbaycanın iqtisadi, elmi, texniki və hərbi imkanlarının formalaşdırılmasına böyük töhfələr vermişdir.

Ulu Öndər yeni ictimai-siyasi və hərbi situasiyada milli təhlükəsizlik orqanlarının səmərəli fəaliyyətinin təşkili məsələlərini də diqqətdə saxlayırdı. Sovet İttifaqının süqutu ərəfəsində və Azərbaycanda müstəqilliyin bərpasının ilk illərində bu orqanın üzləşdiyi çətin sınaqlar, xüsusən, kadr potensialının zəifləməsi və peşəkarlıq səviyyəsinin aşağı

düşməsi kimi hallar baş vermişdi. Heydər Əliyev bu orqanlardakı mövcud nöqsanlarla, qüsurlarla yanaşı, vətənpərvər insanların, xüsusən azərbaycanlıların əksəriyyətinin öz xalqına, millətinə sədaqətlə xidmətinin də unudulmaz olduğunu bildirmişdir.

Azərbaycan Respublikasının Prezidenti kimi Heydər Əliyev özünün 23 mart 1997-ci il tarixli sərəncamı ilə ölkəmizdə təhlükəsizlik orqanlarının peşə bayramı gününü təsis etmiş, bu orqanların Azərbaycan Xalq Cümhuriyyəti ilə bağlı tarixi varisliyinin təmin edilməsinə qərar vermişdir. Ulu Öndər deyirdi: "...Dövlətimizin, xalqımızın təhlükəsizliyini təmin etmək peşəsinə sahib olmaq hər bir vətəndaş üçün şərəfli vəzifədir. Çünki təhlükəsizlik təşkilatının əməkdaşları cəmiyyətdə yüksək etimada, eyni zamanda yüksək səlahiyyətə malikdirlər. Gərək hər bir əməkdaş bunların müqabilində öz məsuliyyətini dərk edə bilsin və üzərinə düşən vəzifəni yerinə yetirə bilsin".

Dövlət Təhlükəsizliyi Xidmətinin əməkdaşı üçün Heydər Əliyev tərəfindən müəyyənləşdirilmiş peşə və mənəviyyat meyarları - yüksək biliyə malik olmaq, dövlətimizin daxili və xarici siyasətini, beynəlxalq vəziyyəti, qanunlarımızı yaxşı bilmək, xalqımıza və dövlətimizə sədaqətli olmaq, böyük şəxsi cəsarət, iradə, dönməzlik - bütün bunlar daim siqlətini və əhəmiyyətini saxlayır. Müstəqil Azərbaycan Respublikasının mühüm dövlətçilik təsisatlarından olan təhlükəsizlik orqanları üçün xalqına və dövlətinə ləyaqətlə xidmət edən, onun təhlükəsizliyinin keşiyində dayanan, sədaqətli və vətənpərvər, yeni nəsil peşəkar və ixtisaslı kadrların hazırlanmasını həyata keçirən Dövlət Təhlükəsizliyi Xidmətinin Heydər Əliyev adına Akademiyasının yaradılması da bilavasitə Ulu Öndərin adı ilə bağlıdır.

Ümummilli Lider Heydər Əliyevin milli inkişaf strategiyasını uğurla davam etdirən Azərbaycan Respublikasının Prezidenti möhtərəm İlham Əliyevin həyata keçirdiyi

ardıcıl və prinsipial daxili və xarici siyasət nəticəsində bu gün davamlı inkişafda olan Azərbaycan bölgənin lider dövləti kimi beynəlxalq münasibətlər və təhlükəsizlik sistemində öz layiqli yerini tutur, xalqımız rifah və sabitlik şəraitində yaşayır.

2.2.3. Müstəqil Azərbaycanın təhlükəsizlik orqanları

"Dövlətin təhlükəsizlik, yaxud kəşfiyyat orqanı o vaxt qalib gəlir, öz vəzifəsini layiqincə yerinə yetirir ki, orada peşəkar kadrlar və iş üslubu olsun."

Heydər Əliyev

Azərbaycan Respublikası 1991-ci ildə müstəqilliyini yenidən bərpa etdikdən sonra ona qarşı yönəlmiş təzyiqlər, daxili və xarici təhdidlər daha da gücləndi. Azərbaycan Respublikası Ali Sovetinin qərarı ilə 1991-ci il noyabr ayının 1-də Dövlət Təhlükəsizlik Komitəsinin əsasında Milli Təhlükəsizlik Nazirliyi təsis edildi. İlk növbədə bu qurumun qarşısında duran vəzifələrin məzmunu və mahiyyəti dəyişməli idi. Əgər respublikanın Dövlət Təhlükəsizlik Komitəsinin bütün imkanları və potensialı ümumilikdə Sovet imperiyasının mövcudluğunun və strateji maraqlarının təminatına yönəlmişdisə, Milli Təhlükəsizlik Nazirliyinin qarşısında duran başlıca vəzifə Azərbaycan Respublikasının suverenliyinə, konstitusiya quruluşuna, iqtisadi, müdafiə və elmi-texniki potensialına, həmçinin dövlət sirri təşkil edən məlumatların qorunmasına, xarici dövlətlərin xüsusi xidmətlərinin və təşkilatlarının, cinayətkar qrupların və ayrı-ayrı şəxslərin kəşfiyyat və digər təxribat-pozuculuq fəaliyyətinin qarşısının alınmasına, bir sözlə, xalqımızın milli mənafeyini və maraqlarını müdafiə və mühafizə etməyə yönəlmişdi.

Bu gün Ulu öndərin siyasi kursunu inamla və uğurla davam etdirən, müstəqilliyimizi əzmlə möhkəmləndirən, demokratik prinsiplərə söykənərək sivil, hüquqi dövlət

quruculuğu yolunda dönməzliyini sübuta yetirən Azərbaycan Respublikasının Prezidenti möhtərəm İlham Əliyevin rəhbərliyi ilə Azərbaycanın öz dövlətçilik ənənələrini daha da inkişaf etdirərək, etibarlı və təhlükəsiz gələcəyi, əbədiyaşarlığı üçün sarsılmaz təməl yaradılmışdır.

Məhz Silahlı Qüvvələrin Ali Baş Komandanı cənab İlham Əliyevin rəhbərliyi ilə mühüm təşkilati-əməli islahatların həyata keçirilməsi, zəruri hüquqi bazanın möhkəmləndirilməsi istiqamətində ardıcıl tədbirlər planı işlənib hazırlanmışdır. «Milli təhlükəsizlik haqqında», «Kəşfiyyat və əks-kəşfiyyat haqqında», «Dövlət sirri haqqında» Azərbaycan Respublikası qanunlarının, «Azərbaycan Respublikasının Milli Təhlükəsizlik Konsepsiyası»nın və sair qanunvericilik aktların, normativ-hüquqi sənədlərin qəbulu təhlükəsizlik orqanlarının fəaliyyət istiqamətlərinin qanunvericilik bazasının təkmilləşdirilməsinin göstəriciləridir.

Çağdaş dönəmdə qlobal təhlükəsizlik arxitekturasının, beynəlxalq nizamın ciddi təzyiq və təsirlərə məruz qaldığı, regional əmin-amanlığa təhdidlərin artdığı bir dövrdə dövlət müstəqilliyinin, ictimai-siyasi sabitliyin qorunması və möhkəmləndirilməsi işinin daha da yüksəldilməsi təhlükəsizlik orqanlarının da fəaliyyətinin daim təkmilləşdirilməsini, müasir çağırışlara cavab verən adekvat bir xüsusi xidmətə çevrilməsini zəruri edir.

Azərbaycan Respublikasının Prezidenti cənab İlham Əliyevin imzaladığı 14 dekabr 2015-ci il tarixli 706 nömrəli Fərman ilə xüsusi xidmət orqanlarının fəaliyyətinin səmərəliliyini artırmaq və dövlət idarəetmə strukturunu təkmilləşdirmək məqsədilə Azərbaycan Respublikası Milli Təhlükəsizlik Nazirliyinin əsasında Azərbaycan Respublikasının Dövlət Təhlükəsizliyi Xidməti və Azərbaycan Respublikasının Xarici Kəşfiyyat Xidməti yaradılmışdır. Azərbaycan xalqının ən böyük nailiyyəti olan dövlət müstəqilliyinin qorunub saxlanılmasında və daha da möhkəmləndirilməsində üzərinə

mühüm vəzifələr düşən Azərbaycan Respublikasının Dövlət Təhlükəsizliyi Xidmətində qarşıya qoyulmuş vəzifələri həyata keçirən şəxsi heyətin saflığına, Vətənə, xalqa və dövlətə sədaqətinə, eyni zamanda peşə, fiziki və döyüş hazırlığına xüsusi önəm verilir. Yüksək peşəkarlıq və intellektual səviyyə, ciddi xidmət və icra intizamı başlıca meyarlardır.

Şəkil 2.6. Azərbaycan Respublikasının Dövlət Təhlükəsizliyi Xidmətinin emblemi

Fəsil üzrə yoxlama sualları

Qeyd olunan fikrin səhv və ya düz olduğunu müəyyənləşdirin

	Düz	Səhv
1. Şəxsi və ailə həyatına dair məlumatlar konfidensial ola bilməz.	☐	☐
2. Dövlət sirlərinə 4 məxfilik dərəcəsi verilə bilər.	☐	☐
3. SSRİ-nin Dövlət Təhlükəsizlik Komitəsi fəaliyyətini dayandırıb.	☐	☐

Test suallarını cavablandırın:

1. Mühafizə xidməti təşkilati olaraq hansı strukturlardan ibarət olmalıdır?

a) Kargüzarlıq dəstəsi
b) Rejim və mühafizə dəstəsi
c) Konfidensial xarakterli sənədləri emal edən xüsusi dəstə
d) Mühəndis-texniki dəstə
e) İnformasiya-analitik dəstə
f) Kəşfiyyat dəstəsi

2. Məxfi informasiya hansıdır?

a) Kommersiya sirri
b) Fərdi məlumatlar
c) Konfidensial informasiya
d) Dövlət sirri

3. Ölkədaxili hüquq üzrə informasiyanın mühafizəsini təmin edən sənədlər hansı bənddə göstərilmişdir?

a) Konvensiya
b) Konstitusiya
c) Deklarasiya
d) Dövlətlərarası razılaşmalar

Açıq sualların cavablarını əhatəli qeyd edin:

1. Təşkilati mühafizə nədən ibarətdir ?

_____
_____
_____
_____
_____

2. Dövlət sirri haqqında Azərbaycan Respublikası Qanununun 7-ci maddəsinə əsasən dövlət sirrinə aid edilməyən və məxfiləşdirilməyən məlumatları qeyd edin

_____
_____
_____
_____
_____

3.İnformasiyanın mühəndis-texniki mühafizəsi

3.1. Mühəndis-texniki mühafizə

Sənaye casusları, rəqiblər və cinayətkarlar obyektlərə qanunsuz müdaxilə etmək və konfidensial informasiyaya yiyələnmək üçün ən müxtəlif texniki vasitələrə malik olurlar. Belə şəraitdə informasiya təhlükəsizliyinin təmin edilməsində səmərəlilik baxımından yüksək nəticələr əldə etmək məqsədi ilə qorunan sirlərin mühafizəsi üçün müxtəlif funksiyalı etibarlı, dözümlü texniki vasitələrdən və üsullardan istifadə etmək lazımdır.

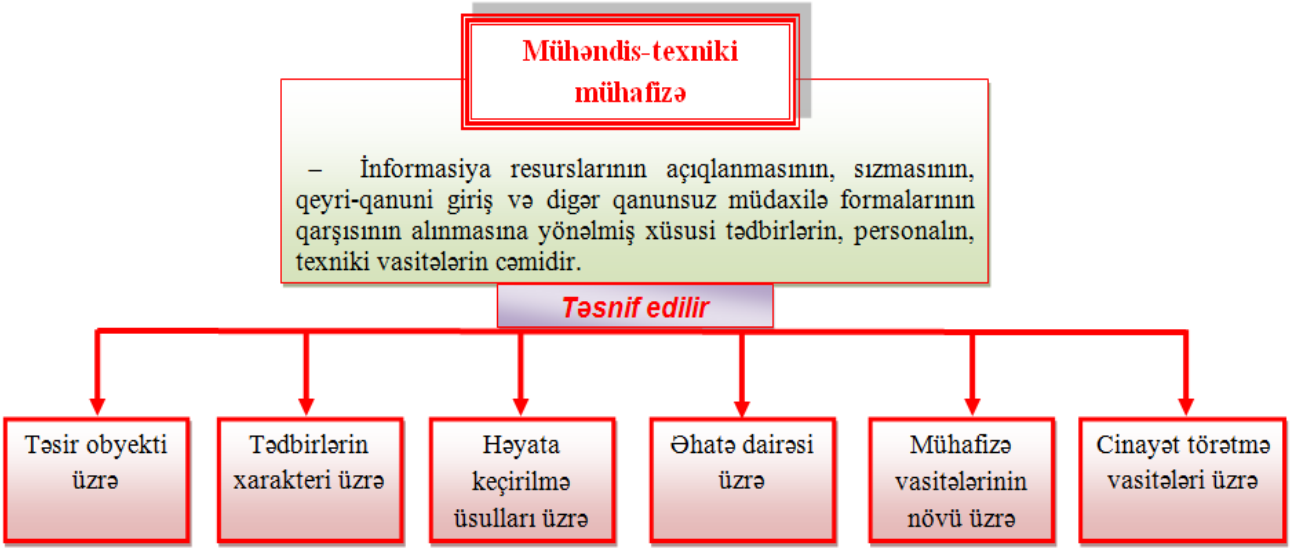
Mühəndis-texniki mühafizə (MTM) – informasiya təhlükəsizliyinə qarşı yönələn hədələrin qarşısının alınması üçün müxtəlif texniki vasitələrdən istifadə edilməklə həyata keçirilən tədbirlər sistemidir.

Mühafizə olunan obyektlərin xarakterinə və həyata keçirilən tədbirlərin növünə, istiqamətinə və digər xarakteristikalarına görə MTM sisteminin təsnifatını aparmaq zərurəti yaranır. Məsələn, mühəndis-texniki mühafizə vasitələrini onların təsir obyektlərinə görə təsnif etmək olar. Bu baxımdan onlar insanların, maddi vəsaitlərin, informasiya resurslarının mühafizəsi, mühafizə edilən obyektlərin növünə görə təsnif olunur.

Mühəndis-texniki mühafizənin təxmini təsnifat strukturu şəkil 3.1-də verilmişdir.

Təsnifat xarakteristikalarının müxtəlifliyi mühəndis-texniki vasitələrin təsir obyektlərinə, tədbirlərin xarakterinə, həyata keçirilmə üsuluna, əhatə dairəsinə, cinayətkarların xarakterinə, cinayət törətmə vasitələrinin növünə görə nəzərdən keçirməyə imkan verir.

Funksional təyinatına görə mühəndis-texniki mühafizə vasitələri aşağıdakı qruplara bölünür:



Şəkil 3.1. Mühəndis-texniki mühafizənin təsnifatı

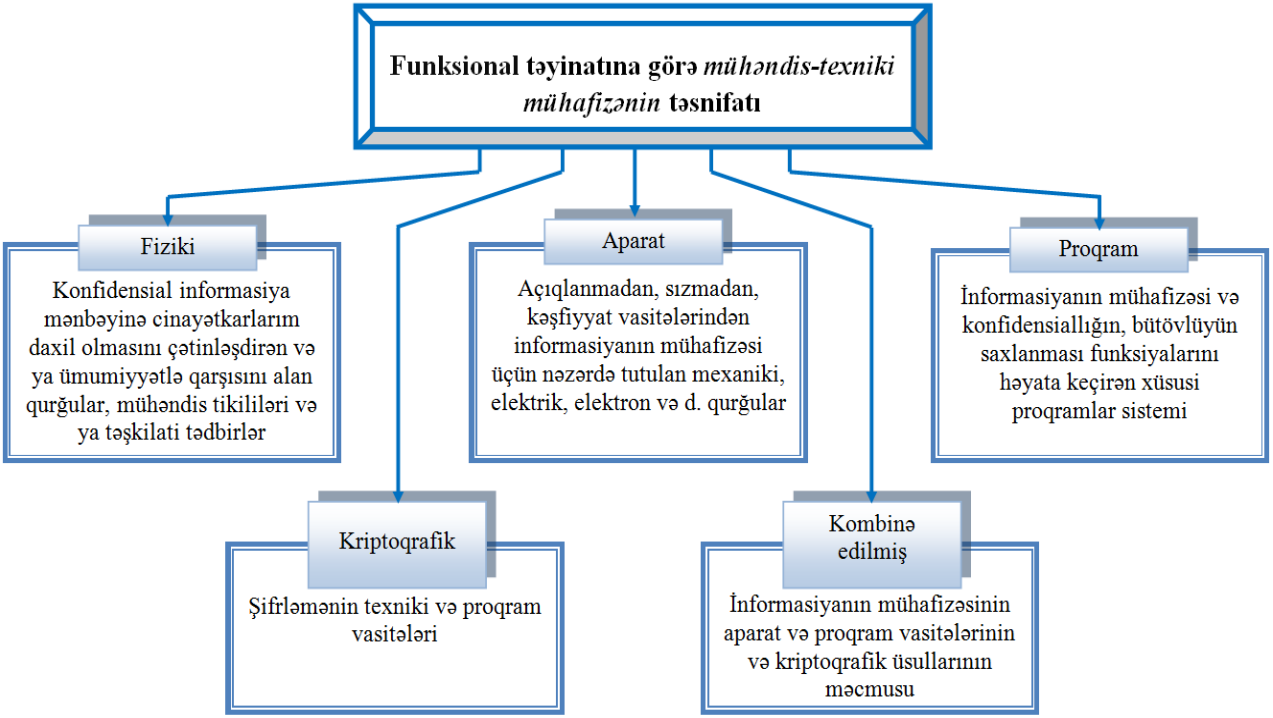
• **Fiziki mühafizə vasitələri (FMV)** - personalın, maddi vəsaitlərin, maliyyənin və informasiyanın qanunsuz müdaxilələrdən mühafizə olunması üçün istifadə edilir. Bu növ FMV-nə mühafizə olunan obyektlərə və konfidensial informasiyanın maddi daşıyıcılarına cinayətkar ünsürlərin daxil olmasının qarşısını alan müxtəlif vasitələr və tikililər daxildir (şəkil 3.2).

• **Aparat mühafizə vasitələri.** Buraya informasiyanın mühafizə olunması üçün cihazlar, qurğular, alətlər və digər texniki həllər daxildir. Müəssisənin fəaliyyətində telefon aparatından tutmuş istehsalat fəaliyyətini təmin edən mükəmməl avtomatlaşdırılmış sistemlərə kimi geniş çeşiddə müxtəlif vasitələrdən istifadə olunur. Aparat mühafizə vasitələrinin əsas vəzifəsi – açıqlanmadan, sızmadan və istehsalat fəaliyyətini təmin edən texniki vasitələr ilə qeyri-qanuni müdaxilədən informasiyanın davamlı və dayanıqlı mühafizəsini təmin etməkdən ibarətdir.

• **Proqram mühafizə vasitələri** – müxtəlif təyinatlı informasiya sistemlərində verilənlərin emalı (yığılması, toplanması, saxlanması, istifadəyə hazırlanması və ötürülməsi) vasitələrində xüsusi proqramları, proqram komplekslərini və informasiyanın mühafizə sistemlərini əhatə edir.

• **Kriptoqrafik mühafizə vasitələri** – informasiyanın mühafizəsinin xüsusi riyazi və alqoritmik vasitələridir. Bunlar müxtəlif şifrləmə üsullarından istifadə etməklə, kompüter sistemlərində olan və orada istifadə olunan sistemlər və rabitə şəbəkələri ilə ötürülür.

Mühafizənin aparat vasitələri və üsulları geniş yayılmışdır. Amma kifayət qədər uyğunlaşma qabiliyyəti (elastik) olmadığına görə iş prinsipi aşkar edildikdə, tez-tez öz mühafizə xüsusiyyətlərini itirir və gələcəkdə istifadə oluna bilmir.



Şəkil 3.2. Funksional təyinatına görə mühəndis-texniki mühafizənin təsnifatı

Mühafizənin proqram vasitələri və üsulları etibarlıdır və onların zəmanətli istifadə müddəti aparat vasitə və üsullarının zəmanət müddətindən kifayət qədər çoxdur.

Kriptoqrafik metodlar kompüter sistemlərinin proqram təminatının mühafizəsində də əsas yer tutur və informasiyanın mühafizəsinin dayanıqlığını etibarlı təmin edir. Aydındır ki, informasiyaların mühafizəsi vasitələrinin bu formada bölgüsü şərtidir, belə ki, təcrübədə onlar tez-tez ya qarşılıqlı əlaqə ilə işləyir, ya da alqoritmlərdən geniş istifadə olunmaqla, proqram-aparat modulları şəklində, kompleks halda həyata keçirilir.

3.2. Fiziki mühafizə vasitələri

Fiziki mühafizə vasitələri – konfidensial informasiya mənbəyinə cinayətkarların daxil olmasını çətinləşdirən və ya ümumiyyətlə qarşısını alan qurğular, mühəndis tikililəri və ya təşkilati tədbirlərdir.

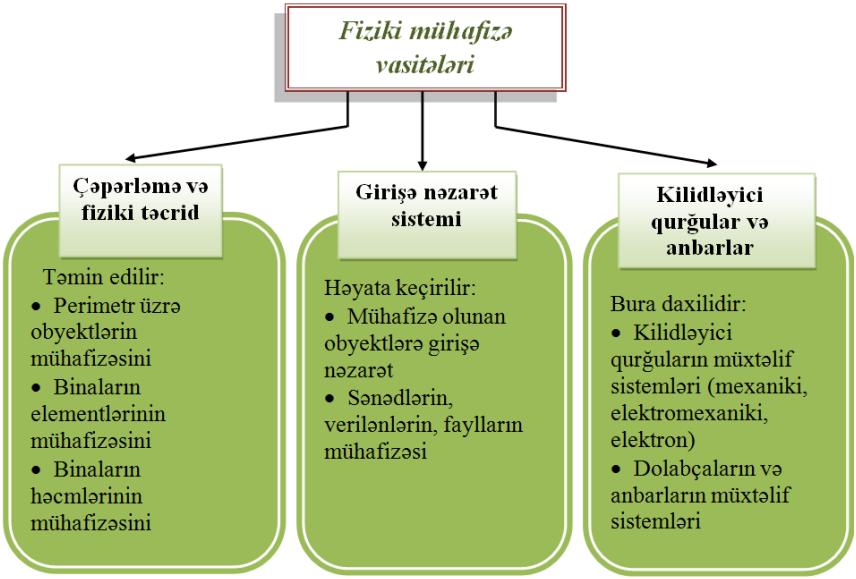
Fiziki mühafizə vasitələrinə aiddir: qanunsuz girişdən (çıxışdan), vasitələrin və materialların qanunsuz içəri daxil edilməsindən (kənara çıxarılmasından) və digər cinayət aktlarından qorunmaq üçün mexaniki, elektromexaniki, elektron, elektron-optik, radio və radiotexniki və digər qurğular (şəkil 3.3).

Bu vasitələr aşağıda qeyd olunan məsələləri həll etmək üçün lazımdır:

1. Ərazinin mühafizəsi və ona nəzarət edilməsi;
2. Binaların xarici və daxili hissələrinin qorunması və onlara nəzarət edilməsi;
3. Qurğuların, məhsulların, maliyyə ehtiyatlarının və informasiyanın mühafizəsi;
4. Obyektə girişə nəzarətin həyata keçirilməsi.

Funksional təyinatına görə bu kateqoriyalardan olan bütün vasitələri aşağıdakı qruplara bölmək olar:

- Mühafizə sistemləri və mühafizə siqnalizasiya vasitələri;
- Video-müşahidə vasitəsi ilə mühafizə;
- Mühafizə işıqlandırılması;
- Fiziki təcridetmə.



Şəkil 3.3. Fiziki mühafizə vasitələri

3.2.1. Mühafizə sistemləri və mühafizə siqnalizasiya vasitələri

Mühafizə sistemləri və mühafizə siqnalizasiya vasitələri müxtəlif növ təhlükələrin aşkar edilməsi üçün nəzərdə tutulmuşdur. Bu sistemlər və siqnalizasiya vasitələri mühafizə obyektlərinə, qorunan zonalara və obyektlərə daxil olmaq, silah, sənaye kəşfiyyatı vasitələrini keçirmək, maddi və

maliyyə qiymətlilərini oğurlamaq cəhdlərinin qarşısının alınması üçün istifadə edilir. Bundan əlavə, bu sistemlər obyektin mühafizə xidmətini və ya əməkdaşları təhlükə yaranmasına dair və obyektə, binalara nəzarəti gücləndirməyə dair xəbərdarlıq etmək üçün lazımdır.

Mühafizə sistemlərinin əsas elementləri təhlükəni aşkarlayan vericilərdir. Vericilərin xarakteristikaları və iş prinsipi mühafizə sistemlərinin əsas parametrlərini və praktiki imkanlarını müəyyən edir.

İndiki dövrdə çoxlu sayda müxtəlif vericilər (müxtəlif fiziki sahələrin aşkarlanma prinsiplərinə, taktiki istifadəsinə görə və s.) işlənib hazırlanmış və geniş istifadə olunur.

Mühafizə sistemləri və mühafizə siqnalizasiya vasitələrinin effektivliyi əsasən vericilərin parametrləri və iş prinsipləri ilə müəyyən olunur. Hal-hazırda müxtəlif növ vericilər məlumdur: mexaniki açarlar (yandırıb-söndürmək üçün), maqnit açarı, təzyiq xalçaları, civə açarı, şifrləmə vericisi, ultrasəs verici, akustik verici, infraqırmızı verici, fotoelektron verici, vibrasiyalı verici və s.

Vericinin hər bir tipi müəyyən növ mühafizəni həyata keçirir: nöqtəvi mühafizə, xətli mühafizə, sahəli mühafizə və ya həcmi mühafizə. Mexaniki vericilər xətli mühafizəyə, təzyiq xalçaları nöqtəvi aşkarlamaya hesablanmışdır, infraqırmızı vericilər isə sahə və həcm üzrə aşkarlamada geniş istifadə olunur.

Vericilər bu və ya digər əlaqə kanalları vasitəsilə mühafizə məntəqəsinin nəzarət-qəbul qurğusu və xəbərdarlıq vasitələri ilə birləşmişdir.

Mühafizə siqnalizasiyaları sistemində əlaqə kanalları xüsusi çəkilmiş məftilli xətlər, obyektin telefon xətləri, yayım rabitə xətləri, xəbərdarlıq sistemləri və radiokanallar ola bilər. Kanalların seçimi obyektin imkanları ilə təyin olunur.

Mühafizə sisteminin əsas obyekti həyəcan-xəbərdarlıq vasitələridir: təhlükənin yaranması barədə səslər, işıqlar, daimi və kəsilən işıq siqnalları.

Taktiki təyinatına görə mühafizə sistemlərini aşağıdakı qruplar üzrə təsnif etmək olar:

- obyektləri perimetr üzrə qoruyan mühafizə sistemləri;
- xidməti və anbar binaları, onların girişlərini qoruyan mühafizə sistemləri;
- seyfləri, avadanlıqları, əsas və yardımçı texniki vasitələri qoruyan mühafizə sistemləri;
- avtonəqliyyatı qoruyan mühafizə sistemləri;
- personalı, şəxsi heyəti və digər obyektləri qoruyan mühafizə sistemləri;

Fiziki mühafizə vasitələrinə aiddir:

- təbii və süni maneələr;
- perimetrlərin, keçidlərin, binaların, seyflərin, anbarların əsas konstruksiyaları;
- təhlükəsizlik zonaları.

Təbii və süni maneələr obyektin ərazisinə qanunsuz müdaxilələrə qarşı yönəlmişdir. Lakin əsas mühafizə yükü süni maneələrin – hasar və digər çəpərləmələrin üzərinə düşür. Təcrübə göstərir ki, mürəkkəb konfiqurasiyalı çəpərlər cinayətkarı kifayət qədər uzun müddətə tutub saxlaya bilər.

Perimetrlərin, keçidlərin, binaların, seyflərin, anbarların xüsusi konstruksiyaları istənilən müəssisə və təşkilat üçün təhlükəsizlik baxımından mütləq hesab olunur. Bu konstruksiyalar cinayətkar elementlərin istənilən fiziki təsir üsullarına tab gətirməlidir. Bu üsullara: mexaniki deformasiyalar, deşilmələr, dağıdılmalar, termiki və mexaniki kəsilmələr, partlayışlar, açarların saxtalaşdırılması, şifrin tapılması və s. daxildir. Keçidlərin, binaların, seyflərin və anbarların əsas texniki mühafizə vasitələrindən biri qıfıllardır. Onlar sadə

(açarlarla), mexaniki (şifrli) və proqram qurğularından ibarət (qapıları və seyfləri müəyyən hallarda açmaq üçün) olur.

Təhlükəsizlik zonaları. Fiziki mühafizə baxımından əsas iş obyektinin, onun binalarının təhlükəsizlik zonaları üzrə planlaşdırılmasıdır. Bu zonalar obyektin müxtəlif hissələrinin mühafizəsinin nə qədər vacib, dəyərli olmasından asılıdır. Təhlükəsizlik zonalarının optimal yerləşdirilməsi və bu zonalarda qanuna zidd fəaliyyətin aşkarlanması, onların qarşısının alınması və məhv edilməsi üzrə effektli texniki vasitələrin quraşdırılması obyektin mühəndis-texniki mühafizəsi konsepsiyasının əsasını təşkil edir. Mühafizə zonalarının digər bir əhəmiyyəti əməkdaşların müəssisə ərazisində vəzifə borclarını yerinə yetirmək üçün girişinə icazə verilən, yalnız müəyyən olunmuş zonalara daxil olmasına nəzarəti təmin etməkdir.

Təhlükəsizlik zonalarında obyektin ərazisinin perimetri boyunca hasardan informasiyanın saxlanıldığı yerə kimi ardıcıl olaraq zonalar üzrə keçidlər yerləşdirilə bilər. Bu mühafizə dövrəsi bir-birinin ardınca pozucunun keçməli olacağı ərazidə növbələşən maneələr (sərhədlər) zəncirini yaradacaqdır. Keçidlər nə qədər mürəkkəb və etibarlı olarsa, onda pozucu hər bir zonanı keçməyə daha çox vaxt sərf etməli olacaqdır. Bu zaman pozucunun aşkarlanması və həyəcan siqnalının verilməsi ehtimalı da artacaqdır.

Təhlükəsizlik zonalarının etibarlılıq səviyyəsi obyektin mühafizəsinin göstəricisi olacaqdır.

3.2.2. Mühafizə video-müşahidəsi

Mühafizə video-müşahidəsiən geniş yayılmış mühafizə vasitələrindən biridir. Mühafizə video-müşahidəsinin əsas xüsusiyyətlərindən biri təkcə mühafizə rejiminin pozulmasının aşkarlanması deyil, eləcə də hadisənin inkişaf prosesində vəziyyətə nəzarət etmək, fəaliyyətin təhlükəlilik səviyyəsini təyin etmək, gizli müşahidə aparmaq və görüntüləri yazmaq

(cinayətkarı məsuliyyətə cəlb etmək və qanun pozuntusunu analiz etmək üçün) imkanının olmasıdır.

Mühafizə video-müşahidəsində təsvirin mənbəyi (vericilər) kameralardır. Obyektivdən cinayətkarın təsviri kameranın işığa həssas elementinə düşür. Burada o, elektrik siqnalına çevrilir və xüsusi kabel ilə monitora, ehtiyac olduqda isə görüntü yazan qurğuya ötürülür.

Videokamera video-müşahidə vasitəsilə olan mühafizənin əsas elementi hesab olunur, belə ki, bütün nəzarət və müşahidə sisteminin effektivliyi və nəticə göstərməsi onun xarakteristikalarından asılıdır. Hal-hazırda həcminə, imkanına və konstruksiyasına görə müxtəlif model kameralar (qaranlıqda işləyən, hərəkətə həssas, məsafədən idarə edilən, 180°-dən çox hərəkət etdirilə bilən və s.) işlənib istehsal olunur.

Video-müşahidə sisteminin ikinci əsas elementi onun monitorudur. O, xarakterinə görə videokamera ilə uyğunlaşdırılmalıdır. Adətən bir monitorda bir neçə kameradan qəbul edilən video çəkilişləri izləmək mümkün olur. Bu kameralar xüsusi təyin olunmuş qaydalara uyğun olaraq, monitora avtomatik çevrilmə vasitələri ilə ardıcıl qoşulur.

Bəzi video-müşahidə sistemlərində qayda pozuntusu, cinayət baş verən əraziyə baxan kameraya avtomatik olaraq qoşulma imkanı nəzərdə tutulmuşdur. Buraya bir neçə təsviri eyni zamanda ötürən qurğular, təsvirdə hər hansı bir dəyişikliyin aşkarlanması zamanı həyəcan siqnalının verilməsi üçün hərəkət detektorları aiddir.

Mühafizə işıqlandırılması.

İstənilən obyektin mühafizə sisteminin tərkib hissəsi mühafizə işıqlandırılmasıdır. Mühafizə işıqlandırılmasını iki qrupa bölmək olar – növbətçi və həyəcan.

Növbətçi işıqlandırma – qeyri-iş vaxtlarında, axşamlar və gecələr, obyektin ərazisində və binanın içində daimi istifadə üçün nəzərdə tutulmuşdur.

Həyəcan işıqlandırılması – mühafizə siqnalizasiyaları vasitələrindən həyəcan siqnalı daxil olduqda işə düşür. Bundan əlavə, həyəcan siqnalı üzrə işıqlandırmaya əlavə olaraq səs cihazları da işə düşə bilər (səslər, sirenalar və s.).

Siqnalizasiya və növbətçi işıqlandırmanın qəza və elektrik işıq şəbəkəsinin söndürülməsi halları üçün ehtiyat elektrik-qida mənbəyi olmalıdır.

3.2.3. Çəpərləmə və fiziki təcridetmə

Son illərdə həyəcan siqnalları sistemi ilə birləşdirilmiş fiziki mühafizə sistemlərinin yaradılmasına xüsusi diqqət ayrılır. Məftilli çəpərlərlə istifadə edilmək üçün elektron siqnalizasiya sistemi məlumdur. Sistem elektron vericilərdən və mikroprosessordan ibarətdir. 100 m uzunluqlu çəpərlər açıq sahələrdə və ya divarlarda, çardaqlarda və mövcud hasarlarda quraşdırıla bilər. Ətraf mühitin təsirinə davamlı vericilər dirəklərdə, kronşteynlərdə (dayaqlarda) montaj olunur. Məftilli çəpərlər üfüqi dartılmış polad tellərdən ibarətdir. Bu tellərin hər birinin orta hissəsinə deformasiya zamanı yaranan dəyişiklikləri elektrik siqnallarına çevirən elektromexaniki vericilər yerləşdirilir.

İdarəetmə və nəzarət mərkəzi (məntəqəsi) ilə sistemin əlaqəsi multipleksor ilə həyata keçirilir. Multipleksor avtomatik olaraq müəyyən vaxt intervalından sonra aparatın və proqram vasitələrinin komponentlərinin işini yoxlayır və normadan kənara çıxma hallarında müvafiq siqnal verir.

Fiziki mühafizənin digər oxşar, analoji sistemləri obyektin ərazisinə daxilolma hallarının aşkar edilməsi məqsədi ilə obyektlərin perimetr boyu mühafizəsi üçün istifadə olunur.

İnfraqırmızı diapazonda şifrlənmiş siqnalları ötürən 2 lifli, optik kabelli torlardan ibarət sistemdən də istifadə edilir. Əgər torda zədələnmə yoxdursa, siqnallar qəbuledici qurğuya təhrifsiz daxil olur. Toru zədələmə cəhdləri kabellərin

qırılmasına və ya deformasiyasına səbəb olur ki, bu da həyəcan xəbərdarlıq siqnalının yaranmasına gətirib çıxarır. Optik sistemlərdə yanlış həyəcan vermə ehtimalı aşağı, daxil olma cəhdlərinin aşkarlanması ehtimalı isə yüksəkdir. Yanlış həyəcan siqnalları kiçik heyvanların, quşların təsiri, hava şəraitinin dəyişməsi ilə əlaqədar yarana bilər.

Fiziki mühafizənin növbəti forması bina və tikililərin elementlərinin mühafizəsidir. Binaların pəncərə keçidlərinin fiziki mühafizəsini ənənəvi metal çərçivələr, həmçinin polad məftillə armaturlaşdırılmış plastik kütlə əsaslı xüsusi şüşələr təmin edir. Mühafizə olunan binanın qapı və pəncərələrinin sındırılması zamanı işə düşən, lakin digər səbəblərdən onların titrəməsinə reaksiya göstərməyən vericilər quraşdırılır. Vericilərin işə düşməsi həyəcan siqnalı yaradır.

Fiziki mühafizə vasitələri arasında personal kompüterləri oğurlanmaqdan və onlara icazəsiz girişdən qoruyan mühafizə vasitələrini qeyd etmək olar. Bunun üçün stolun səthinə bərkidilmiş (yapışmış) yapışqan altlıqlı metal konstruksiyalardan istifadə olunur. Stolu sındırmadan belə personal kompüterlərin götürülməsi və yerinin dəyişdirilməsi mümkün deyil. Kompüterlərin yerinin dəyişdirilməsi yalnız xüsusi açarlar və ya alətlər ilə mümkündür.

Kilidləyici qurğular.

Texniki vasitələrin qorunması üçün xüsusi metal dolablar istehsal olunur. Belə dolablar etibarlı ikili kilidləmə sisteminə - açar tipli kilidə və 3-5 nişanlı kombinə edilmiş qıfıla malik olur. Belə dolablar sənaye kəşfiyyatından mühafizə olunmaq üçün kifayət qədər möhkəmliyə və etibarlılığa malikdir.

Mexaniki və elektron saatların köməyi ilə açılma vaxtı proqramlaşdırılmış kilidlər də istehsal olunur.

3.2.4. Girişə nəzarət sistemi

Binaya girişə nəzarətin idarə edilməsi ilk öncə təhlükəsizlik xidməti (həmçinin aviasiya təhlükəsizlik xidməti) və texniki vasitələrlə həyata keçirilir.

Girişə nəzarət müəyyən mühafizə olunan zonalara, binalara məhdud sayda şəxslərin daxil olmasına və həmin şəxslərin orada hərəkətinə nəzarəti həyata keçirir.

Heydər Əliyev Beynəlxalq Hava Limanında tətbiq olunan təhlükəsizlik qurğularının təhlili aparılmışdır.

Stasionar metalaxtaran.

Stasionar metalaxtaraninsan bədənində və geyimində olan metal, odlu və soyuq silahların aşkarlanması üçündür.

Aviasiya təhlükəsizliyi sahəsində stasionar metalaxtaranın ilk dəfə tətbiqi 17 iyul 1970-ci ildə ABŞ-ın Nyu-Orlean ştatının Moisant Beynəlxalq Aeroportunda hava gəmisinin qaçırılmasına qarşı yoxlama sistemində həyata keçirilmişdir (şəkil 3.4). Bu sistemə əsasən bütün sərnişinlər stasionar metalaxtaran vasitəsilə üzərində silahın olub-olmamasına dair yoxlamadan keçirilirdilər.

Konstruksiyası: Stasionar metalaxtaranlar konstruksiyasına görə iki şəkildə hazırlanır: sütun və panelşəkilli. Sütunşəkilli metalaxtaranlar estetik baxımdan panel şəkilliləri qabaqlayır. Onlar yüngüldür, az yer tutur və nəzarət sahəsini tutmurlar, yəni növbədə duran sərnişinlər asan müşahidə olunurlar. Lakin xarakteristikalarına görə panel şəkillilər daha üstündürlər. Panelşəkilli stasionar metalaxtaran Пşəkilli keçiddən ibarətdir. Keçidlərdən birində elektromaqnit dalğaları generatoru, digərində isə qəbuledici yerləşir. Nəzarət keçidinin alt tərəfində idarəedici qurğu, ön panelində displey və ya elektron bloku yerləşir. Elektron bloku və ya displey köklənmiş parametrlərin indikatorudur. İndikatorlar köklənəcək proqramın nömrəsini, həssaslığı, xəbərdarlıq siqnalının

ucalığını, işçi tezliyi, səs siqnalının tonunu, davametmə müddətini və s. göstərir. O, parametrləri daxil etmək üçün klaviaturaya malikdir. Stasionar metalaxtaranların idarəedici qurğusu olur ki, bu idarə edici qurğu metalaxtaranda köklənəcək parametrləri tənzimləmək funksiyasını yerinə yetirir. Misal üçün deyə bilərik ki, idarəedici qurğu üzərində olan PG - proqramı, SENS - həssaslığı, VOL - səsin ucalığını tənzimləmək üçün nəzərdə tutulmuşdur. Stasionar metalaxtaranın idarəedici qurğusundan (idarəedici pult) istifadə edərkən operator 3m məsafədən uzaq durmamalıdır.

Şəkil 3.4. Moisant Beynəlxalq Aeroportunda təhlükəsizlik üzrə baxış məntəqəsi, 1970-ci il

İş prinsipi: Qurğunun işi nəzarət zonasında metal obyekt mövcud olduğu halda generator və qəbuledici antenalarında elektromaqnit induksiyasının dəyişməsinin qeyd edilməsi prinsipinə əsaslanır. Generator elektromaqnit dalğaları şüalandırır və bunlar qəbuledici tərəfindən qəbul olunur. Şəxsin üzərində metal əşya olduqda, yəni generatorla qəbuledici arasında metal əşya olduqda, elektromaqnit dalğaları deformasiya olunur, xəbərdarlıq siqnalı çalınır və qırmızı işıq yanır (şəkil 3.5). Əgər şəxs ürək xəstəliyi olduğunu bildirərsə

və buna müvafiq sənədi olarsa, onda o, fiziki yolla baxışdan keçirilir.

Şəkil 3.5. Üzərində metal əşya olan şəxsin metal detektordan keçməsi zamanı xəbərdarlıq siqnallarının yaranması

Stasionar metalaxtaranların əsas parametrləri: həssaslıq, ayırdetmə qabiliyyəti və maneəyə davamlılıqdır.

Həssaslıq qurğunun aşkar edə bildiyi metalın minimal çəkisi ilə təyin olunur. Müxtəlif növ metalları aşkar etmək üçün səkkiz növ proqram vardır. Məsələn: geniş diapazonlu silahı təyin etmək üçün ümumi proqram, dəmirdən hazırlanmış silahı təyin edən proqram, paslanmayan dəmirdən hazırlanmış silahı təyin edən proqram, kiçik əşyaları aşkar etmək üçün böyük həssaslığa malik proqram və s. Hər bir proqramın həssaslığı müxtəlifdir. Elə metalaxtaranlar vardır ki, onların həssaslığı 1 qramlıq metal əşyanı aşkar etməyə imkan verir.

Ayırdetmə qabiliyyəti (bircinslik) nəzarət zonasının bircinsliyindən asılıdır. Başqa sözlə desək, bircinslik - qurğunun ən kiçik kütləli əşyanı aşkar edə bilmə xassəsidir. Bircins zona almaq üçün çoxzonalı metalaxtaranlardan istifadə

olunur. Zona bircins olmadıqda, nəzarət zonasında «ölü» və «aktiv nöqtələr» yaranır ki, bu da bir sıra əşyaların nəzarətdən yayınmasına səbəb olur. Kifayət qədər bircinslik almaq üçün nəzarət zonasında kəsişən elektromaqnit sahələri yaradan xüsusi konfiqurasiyalı ötürücü və qəbuledici sistemlərindən istifadə olunur. Optimal həndəsi ölçülərin də seçilməsi çox vacibdir. İstehsalçılar aydınlaşdırmışlar ki, dayaqlar arasındakı məsafə 0,80 m-dən böyük olduqda, bircinslik pozulur. Yeni nəsil stasionar metalaxtaranlarda bir deyil, 8 generator - qəbuledici dəsti tətbiq edilir. Bu isə dayaqlar arasında bircins elektrik sahəsini yaradır.

Metalaxtaranlar yüksək ***maneəyədavamlılıq*** xassəsinə malikdirlər. Maneəyədavamlılıq xassəsinin effektiv olması stasionar metalaxtaranların düzgün yerləşdirilməsindən də asılıdır. Belə ki, hava limanlarında səhv işədüşmə halları mümkündür. Bu, metalaxtaranların yaxınlığında avtonəqliyyatın, metal qapının və liftlərin və digər metal birləşmələrinin olması ilə izah olunur. Odur ki, metalaxtaranlar düzgün yerləşdirilməlidir. Qurğuda maneəyədavamlılığı artırmaq üçün o, hərəkət etməyən metal birləşmələrdən (qapı, lift) 0,5 m, hərəkət edən metal birləşmələrdən 1-1,5 m aralı yerləşdirilir. Kənar şəxslər və xidmət göstərən heyət 0,5 m uzaqlıqda durmalıdır.

Stasionar metalaxtaranın üstünlükləri. Hal-hazırda Heydər Əliyev Beynəlxalq Hava Limanında istifadə olunan Metor-6M metalaxtaranında cəmləşən müasir funksiyalar tam olmasa da, yüksək təhlükəsizliyə təminat verir. Stasionar metalaxtaranın fərqləndirici xüsusiyyəti kimi böyük ayırdetmə qabiliyyətini, etibarlı aşkarlama, böyük işgörmə (buraxma) qabiliyyətinə malik olduğunu və davamlılığını göstərmək olar. Metor-6M beynəlxalq standartlara əsaslanan aşkarlama proqramları ilə təchiz olunmuş və bir çox funksiyaları özündə cəmləşdirir. Misal olaraq, təsadüfi həyəcan siqnalı funksiyasını deyə bilərik. Bu funksiya təhlükəsizlik xidmətinin əməkdaşına

seçim əsasında istənilən sərnişinin əlavə baxışını keçirməyə imkan verir.

Əl metalaxtaranları.

Əl metalaxtaranlarıstasionar metalaxtaranlarla qeydə alınmış metal əşyaların aşkar edilməsi məqsədi ilə təkrar baxış üçün, həmçinin stasionar metalaxtaran olmayan məntəqələrdə sərnişinlərin üstündə gizlədilmiş metal əşyaları aşkar etmək, hava gəmisinin bortunda və trapın yanında sərnişinlərə baxış keçirmək, eləcə də əl yüklərini və baqajı açmadan, yaxın məsafədən yoxlamaq üçün istifadə olunur. Başqa sözlə, əl metalaxtaranları daha dəqiq, daha konkret axtarış aparmaq üçün nəzərdə tutulmuşdur (şəkil 3.6).

Şəkil 3.6. Əl metalaxtaranı

Metalaxtaranların tarixi ABŞ-ın 20-ci prezidenti Ceyms Abraham Qarfildlə bağlıdır. Belə ki, Şotland fiziki Aleksandr Bell 1881-ci ildə sui-qəsd nəticəsində sinəsindən güllə yarası almış ABŞ prezidentinin bədənindən gülləni aşkar etməyə çalışmışdır. Lakin ixtira olunmuş cihazın lazımi həssaslığı olmadığına görə o, gülləni aşkar edə bilməmişdir. Həmən vaxtdan bəri əl metalaxtaranları daimi olaraq daha üstün funksiyalara malik olanları ilə yenilənmiş və özlərini gömrükdə, metrolarda, həbsxanalarda, sənaye obyektlərində, keyfiyyətə nəzarət xidmətlərində doğrultmuşdur. Əl metalax-

taranlarının tətbiqinə, həmçinin, mülki aviasiya sahəsində də çox rast gəlinir.

Aviasiyada əl metalaxtaranlarından daha çox şəxslərə operativ baxış tətbiq etmək üçün istifadə olunur. O, skanedici səthə malikdir. Metal obyektləri aşkarlamaq üçün onu elə hərəkət etdirmək lazımdır ki, metalaxtaranın skanerləyici səthi şəxsi daha çox əhatə edə bilsin. Metal obyektlərin aşkar olunması yaxın məsafədən aparılır. Keyfiyyətli aşkarlama üçün o, daim hərəkətdə olmalıdır. Əl metalaxtaranları ilə dərin baxış keçirmək çox vaxt tələb edir. Odur ki, kütləvi və daimi tədbirlərdə adətən stasionar metalaxtaranlardan istifadə olunur.

Adətən mülki aviasiyada əl və stasionar metalaxtaranlardan kompleks şəkildə istifadə olunur.

Cihazın iş prinsipi.

Əl metalaxtaranının iş prinsipi stasionar metalaxtaranların iş prinsipi ilə eynidir. O, qəbuledici və ötürücüdən ibarətdir. Ötürücü tərəfindən şüalandırılan elektromaqnit dalğaları qəbuledici tərəfindən qeydə alınır. Metal əşya aşkar olunduqda, elektromaqnit dalğaları deformasiyaya uğrayır və səs siqnalı işə düşür.

Metalaxtaranların əsas göstəriciləri:

- müəyyən etmə - bu avadanlığın sərnişin üzərində olan metal əşyaları fərqləndirmə qabiliyyətidir.
- həssaslıq - ən kiçik metal əşyanı (ülgüc, mikrosxem və s.) verilmiş ehtimalla aşkar edə bilmə qabiliyyətidir.

Maneəyədavamlılıq qəbuledici antenaların xüsusi seçilmiş konstruksiyası və elektron dövrələrin sxemotexniki həlləri ilə təmin edilir.

Hal-hazırda Heydər Əliyev Beynəlxalq Hava Limanında istifadə olunan əl metalaxtaranları arasında ən müasiri Adams Electronics AMR-11 əl metalaxtaranıdır. O, yüksək həssaslığa malik olub, 11 fərdi tənzimlənən proqram ehtiva edir. Bu metalaxtaran operatora konkret ölçülü metal əşyaları effektiv aşkar etmək üçün optimal həssaslıq səviyyəsi seçməyə imkan

verir. Səs və vizual işıq xəbərdarlıq siqnalına malikdir. Aşkar olunmuş metal obyektin ölçülərindən asılı olaraq, xəbərdarlıq sianalının intensivliyi müxtəlifdir: kiçik ölçülülər qısamüddətli siqnal, böyük ölçülülər uzunmüddətli siqnal ilə müşahidə olunur. Bunlardan başqa, aşkarlayıcı qurğu avtomatik rejimdə kalibrləmə və həssaslığın tənzimlənməsi funksiyalarına malikdir.

Rentgen introskopu.

Rentgen introskopu əl yüklərinə və baqaja baxış keçirmək üçün nəzərdə tutulmuşdur.

Hal-hazırki dövrdə isə rentgen texnologiyası hər bir beynəlxalq hava limanının təhlükəsizlik sisteminin ən vacib ünsürlərindən biridir. Bu texnologiyadan dünyanın əksər aeroportlarında istifadə olunur və kütləvi-informasiya vasitələri, həmçinin ictimaiyyət tərəfindən ilkin müdafiə xətti kimi qəbul edilir. Hal-hazırda bu texnologiya sabit inkişaf edir. İstehsalçılar tərəfindən elmi-texniki tərəqqinin son nailiyyətlərinə cavab verən qurğular istehsal olunmuşdur. Rentgen avadanlıqlarının istehsalçıları bu sistemləri bir və yaxud bir neçə sahələr üçün işləyib hazırlamışlar. Hər bir sahədə tətbiq edilən avadanlıqlar həndəsi ölçülərinə, erqonomik və təsvirlərin alınması xüsusiyyətlərinə görə digərindən fərqlənir.

Rentgen texnologiyasının bir neçə növü vardır:

- **Transmissiya** – rentgen şüalarının obyektlərdən keçən enerjisini istifadə edən ənənəvi texnologiya.
- **Əks yayılma** – rentgen şüalarının obyektlərdən əks istiqamətdə yayılan enerjisini istifadə edən texnologiya.
- **Difraksiya** – rentgen şüalarının obyektlərin kristal strukturunda bölünən enerjisini istifadə edən texnologiya.
- **Rentgen kompüter tomoqrafiyası** – şüa mənbəyinin obyektin ətrafında sürətlə fırlanmasından istifadə edən ənənəvi texnologiyadır.

Aviasiya sənayesində rentgen qurğusu vasitəsilə yoxlama 3 əsas istiqamət üzrə tətbiq edilir:

1. Əl yükünün yoxlanılması;
2. Qeydiyyatdan keçmiş baqajın yoxlanılması;
3. Yüklərin (poçt və müşayiət olunan yük də daxil olmaqla) yoxlanılması.

Rentgen introskoplarının bir çox növləri vardır. Bu qurğunun ən müasir növlərindən biri olan Rapiscan 620 DV-dən hal-hazırda Heydər Əliyev Beynəlxalq Hava Limanında istifadə edilir. Rapiscan 620 DV rentgen introskopu nümunəsindəki DV hərfləri qurğunun "DUAL View", yəni iki şüa mənbəyinə malik olduğunu bildirir. Qurğu ABŞ-ın AnOSI (Open Systems International, Inc.) *Systems Company Rapiscan* şirkətinin istehsalıdır.

İki rentgen şüa generatoruna malik olan təkmilləşdirilmiş introskopun monitorunda baqajın bir skanerlənməsi zamanı iki proyeksiyalı (yuxarıdan və yan tərəfdən) təsvirləri əks olunur. Alınan 2D ölçülü təsvir skanerlənən baqajdakı əşyaların tanınması prosesini yaxşılaşdırır və onun məzmunu haqqında tam məlumat verir (şəkil 3.7). Nəticədə baqajın təkrar skanerləməsinə ehtiyac qalmır. Bu isə operativ iş rejiminin təmin olunması ilə sistemin buraxma qabiliyyətinin artması deməkdir. Erqonomik dizayna malik introskopun istismar qaydalarını yaxşılaşdırmaq məqsədilə o, standart platformaya quraşdırılır.

Şəkil 3.7. Baqajın üfüqi və şaquli istiqamətlərdə skanerlənmiş təsvirləri

Bu qurğunun bir sıra özünəməxsus üstünlükləri vardır:

- OS 600 proqram təminatı - yüksək keyfiyyətli təsvir alınmasını və introskopun lokal şəbəkəyə qoşulma imkanını təmin edir.

- TİP sistemi - bu sistem X-Ray operatorları üçün məşq, yaxud təlim proqramı olub, monitorinq alətidir.

- TİPNET sistemi - təhlükəli əşyaların təsvirlərindən ibarət şəbəkə sistemidir.

- Target texnologiyası - real vaxt rejimində konveyeri saxlamadan, operatora potensial partlayıcı maddələri avtomatik rejimdə aşkar edən köməkçi proqramdır.

- DTA funksiyası - yüksək sıxlıq şəraitində xəbərdarlıq funksiyasıdır.

- OTP proqramı - tətbiqi proqram olub, istifadəçinin X-RAY sistemlərinin əsas funksiyalarını və imkanlarını öyrənməsinə kömək edir.

Ayaqqabı metaldetektoru.

Ayaqqabı metaldetektoru ayaqqabılara onları çıxarmadan baxış keçirmək üçündür (şəkil 3.8). Qurğuda ionlaşdırıcı dalğa olmayan və insan üçün tamamilə zərərsiz olan aşağı tezlikli elektromaqnit dalğalarından istifadə olunur. Baxış müddəti 2 saniyədir. Bu qurğuda həm vizual, həm də akustik siqnallar mövcuddur. Qabaqcıl texnologiyanın tətbiqi ilə yalan işləmələrin sayı minimuma çatdırılmış və yüksəksürətli baxış təmin olunmuşdur. Bu metaldetektor yüksək təhlükəsizlik tələb olunan aeroportlarda, təcridxanalarda, vağzallarda, stadionlarda, elektrik stansiyalarında tətbiq olunmaq üçün nəzərdə tutulmuşdur.

Şəkil 3.8. Ayaqqabı metaldetektoru

22 dekabr 2001-ci ildə Parisdən Mayamiyə uçan American Airlines aviaşirkətinə məxsus hava gəmisini partlatmağa cəhd edən Britaniya vətəndaşı Ricard Reyd Boston federal məhkəməsi tərəfindən ömürlük həbs cəzasına məhkum olunmuşdur.

Qərb kütləvi-informasiya vasitələri Reydi ayaqqabı terroristi adlandırmışdılar. Belə ki, təyyarəni partlatmağa cəhd edən Reyd partlayıcı maddəni ayaqqabının dabanında gizlətmişdi. Bir sıra qəzetlər bu hadisədən əvvəl Riçard Reydin "Əl-Qaidə" və "Əl-Mahadcirun" təşkilatlarında təlim keçdiyini yazırdı. Riçard Reyd partlayış həyata keçirən dövrəni işə salmağa cəhd edərkən, ekipaj üzvləri və sərnişinlər tərəfindən zərərsizləşdirilmiş, 183 sərnişin və 14 ekipaj üzvü olan təyyarə Bostonda məcburi enmə yerinə yetirmişdir. Bu hadisədən sonra TSA (Transportation Security Adminstration – Nəqliyyat Təhlükəsizliyi Administrasiyası) ayaq geyimlərinin çıxarılaraq, rentgen qurğusunda yoxlanılmasına dair qaydaları tətbiq etməyə başladı. 2005-ci ildən isə ayaqqabılara baxış üçün xüsusi texniki qurğular tətbiq olunmağa başlanmışdır.

Metaldetektorun üstünlükləri:

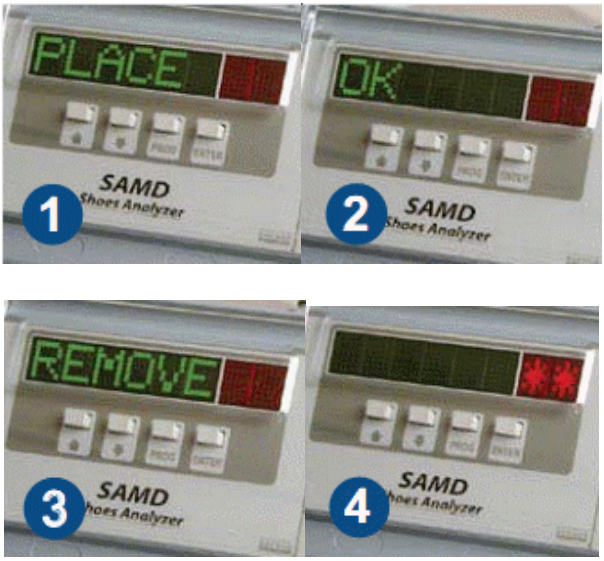
– ayaqqabıda gizlədilmiş istənilən təhlükəli əşyanı aşkar edir;
– cəld, rahat, effektlidir;
– yüksək buraxma qabiliyyətinə malikdir;
– Avropa standartlarının tələblərinə uyğundur.

Bütün bu sadaladığımız xüsusiyyətlərdən başqa, qurğunun digər üstünlükləri də vardır. Belə ki, ayaqqabı metaldetektoru operatorlar üçün, elektrostimulyatorlar üçün, hamilə qadınlar üçün zərərsizdir və maqnit daşıyıcılarına təsir etmir. Metaldetektor beynəlxalq elektrik təhlükəsizliyi və elektromaqnit uyğunluğu standartlarına cavab verir.

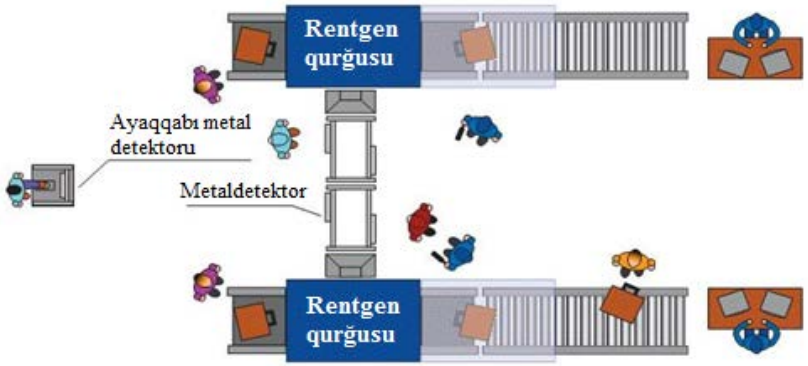
İstifadə qaydaları şəkil 3.9-da göstərilmişdir.

Qurğunun nəzarət zonasında yerləşdirilməsinin nümunəsi.

Ayaqqabı metaldetektoru nəzarət zonasında rentgen avadanlığı və stasionar metalaxtarandan qabaq yerləşdirilir. Burada məqsəd yoxlanılan şəxslərin çox əziyyət çəkməməsi və onların üzərində heç bir təhlükəli metal əşya qalmadan stasionar metalaxtarandan keçməsidir. Yoxlanılan şəxs birinci ayaqqabı metaldetektorunda yoxlanışdan keçir, əgər avadanlıq həyəcan siqnalı verərsə, sərnişinin ayaqqabısı onun üst geyimləri və əşyaları ilə birgə rentgen avadanlığında baxışdan keçirilir. Bu proses həmin şəxsin stasionar metalaxtarandan keçərkən, onun üzərində metal əşyanın qalmaması ehtimalını artırır və onun təkrar qayıdaraq stasionar metalaxtarandan keçməsinin qarşısını alır (şəkil 3.10).



Şəkil 3.9. Ayaqqabı metaldetektorunun istifadə qaydaları: 1 - SAMD elektron blokunda PLACE FOOT xəbərdarlığı əks olunur; 2 – OK - onu göstərir ki, baxış keçirilmiş, metal əşya aşkar olunmamışdır; 3 – REMOVE - sərnişinə baxışın başa çatdığını bildirir; 4 - Təhlükəli əşya aşkar olunduqda, səs və vizual həyəcan siqnalı verilir



Şəkil 3.10. Qurğunun nəzarət zonasında yerləşdirilməsinin nümunəsi

Bədən skaneri.

Bədən skaneri qurğusu nəzarət məntəqələrində yoxlanılan şəxslərin üzərində olan istənilən ölçüdə, istənilən materialdan hazırlanmış maddə və əşyaları aşkar etmək üçündür (şəkil 3.11).

İlk dəfə Hollandiyanın Shiphol hava limanında 17 may 2007-ci ildə metal detektorun əvəzedicisi kimi bədən skanerlərinin istifadəsinə başlanılmışdır. Bədən skanerlərinin tətbiqində məqsəd sərnişinlərin üzərində gizlətdikləri bütün əşyaları görmək və sərnişinlərin sıralarda gözləməsi, kəmər və digər metal əşyaların çıxarılması ilə narazılıqların aradan qaldırılması idi. Lakin 2013-cü il 18 yanvar tarixində bədən skaneri ilə yoxlanılmış müəyyən sərnişinlərin nisbi olaraq lüt bədən şəkillərinin mediaya sızmasından sonra bu, bir çox ölkələrdə narazılıqlara səbəb oldu. Bundan sonra həmin qurğuların tətbiqi ilə yoxlanılmada sadələşdirmə prosedurları tətbiq olunmağa başlanır.

Şəkil 3.11. Bədən skaneri

Baxış keçirən texniki vasitələrin əksəriyyəti rentgen şüalanması prinsipinə əsaslanır. Lakin bundan fərqli olaraq, bədən skaneri qurğularının işi aktiv millimetrlik dalğa şüalanması prinsipinə əsaslanmışdır.

Portativ qazanalizator.

Bir neçə saniyə ərzində yük bağlaması açılmadan, bağlamanın üstündən hava sormaqla buxarları analiz edir. Bu qurğu ion dreyfi spektrometriyası texnologiyası əsasında hazırlanmışdır.

Şəkil 3.12. Portativ qazanalizator

İonscan B portativ qazanalizatoru daxil olduğu qrupda ən universalıdır. O, partlayıcı və narkotik maddələri, eləcə də

kimyəvi maddələri təyin edir, kiçik qabaritlidir, yüksək həssaslığa malikdir.

Mina axtarışı işində, güc strukturlarında, gömrük sistemində və təhlükəsizlik xidmətində tətbiq olunmaq üçün nəzərdə tutulmuşdur.

Aviasiya sahəsində sahibsiz əşyalara baxış, həmçinin partlayıcı vasitələri təyin etmək üçün istifadə olunur. Hal-hazırda Heydər Əliyev Beynəlxalq Hava Limanında da bu qurğu təhlükəsizlik tədbirlərinin bir hissəsidir. Cihazın istifadəsinin asan olması - onun üstünlüyüdür. Cihazın çəkisinin az olması onu asanlıqla əldə daşımağa imkan verir. Bu isə aviasiya təhlükəsizliyi işçilərinin işini asanlaşdırır. Çünki bir çox hallarda hava limanında sahibsiz əşyalara rast gəlinir ki, belə əşyaların təhlükəli olub-olmamasını ayırd etmək üçün çətin daşınan, quraşdırılması çətin olan qurğuların istifadəsindənsə, bu cür portativ qazanalizatorlardan istifadə daha məqsədəuyğundur. Bu cihazın çatışmazlığı kimi isə qurğunun yaddaşında olan partlayıcıların növlərinin sayını az olmasını qeyd edə bilərik.

Tanıma üsulları. Girişdə tanıma (sistemə daxil olmağa icazə verən parametrlərlə müqayisə) üsulları əsas götürülür. Şəxslərin girişinə icazə verilməsi (əgər daxil olmaq hüququ varsa) və ya qadağan edilməsi (əgər daxil olmaq hüququ yoxdursa) tanıma əsasında yerinə yetirilir.

Məsul şəxslərin əraziyə, obyektə daxil olması üçün bir çox tanıma üsulları mövcuddur. Atribut və personal tanıma üsulları daha geniş yayılmışdır. Atribut üsullarına səlahiyyətlərin təsdiqi vasitələri – sənədlər (pasport, vəsiqə), kartlar (foto kartlar, maqnit, elektrik, mexaniki və identifikasiya kartlar və s.) və digər vasitələr (açarlar, siqnal elementləri və s.) aiddir. Qeyd edək ki, bu vasitələr kifayət qədər saxtakarlıqlara və hiyləgərliklərə məruz qalır.

Personal tanıma üsulu – bu, şəxslərin fərdi xarakteristikalarına görə onların tanınmasıdır. Müstəqil göstəricilərə

barmaq izləri, əlin forması, gözlərin xüsusiyyətləri aiddir. Personal xarakteristikalar statik və dinamik olur. Sonunculara nəbz, təzyiq, kardioqram, səs, yazı xətti və digər əlamətlər aiddir.

Personal tanıma üsulların istifadəsi daha cəlbedicidir. Birincisi, hər bir şəxs fərqli özəlliklərə malikdir, ikincisi isə fərdi xarakteristikaları saxtalaşdırmaq çox çətindir və ya ümumiyyətlə mümkün deyil.

Personal tanıma statik və dinamik özəlliklərə əsasən istifadə olunur.

Statik özəlliklərə fiziki xarakteristikaların analizi – barmaq izləri, əlin formasının özəllikləri, gözün xarakteris-tikaları və s. daxildir. Onlar həqiqidir və səhv olma ehtimalı azdır.

Dinamik özəlliklərə isə tanıma zamanı dəyişən xarakteris-tikalar aiddir. Buraya səsin xüsusiyyəti, yeriş, sifət və s. daxildir.

Təhlükəsizlik tələbləri aşağı səviyyədə olan hallarda yadda qalan bir parametrə (kod, şifr) əsaslanan tanıma üsulları tətbiq olunur. Belə ki, bu informasiya tez-tez istifadəçilər tərəfindən müxtəlif kağızlara, qeyd kitabçalarına və digər daşıyıcılara yazılır, bunlar da kənar şəxslərin əlinə keçdikdə bütün görülən təhlükəsizlik tədbirləri sıfra enir. Bundan əlavə, bu informasiyaya baxmaq, qulaq asmaq və ya digər yollarla (təcavüz, oğurluq və s.) əldə etmək kimi real imkanlar mövcud olur.

İnsan (qarovulçu, növbətçi) tərəfindən həyata keçirilən tanıma üsulu "insan amili" səbəbindən daim etibarlı deyil. Belə ki, insan bir çox kənar təsirlərə məruz qalır (yorğunluq, əhvalın pisləşməsi, stress, pulla ələ alınma). Tanınmanın texniki vasitələrində "insan amili"nin rolu az olduğu üçün onlar daha etibarlıdır, bu səbəbdən səs, yazı xətti, barmaqlar və s. tanıma üsulları, identifikasiya kartları daha geniş tətbiq olunur.

İdentifikasiyanın daha sadə və geniş yayılmış üsulu müxtəlif kartlardan istifadədir ki, bunların üzərinə kartın sahibi, onun səlahiyyətləri və s. haqqında şifrlənmiş və ya açıq informasiya yerləşdirilir. Adətən bu, plastik kartlar formasında buraxılış vəsiqələri və jetonlar olur. Belə kartlardan istifadə olunan tanıma üsullarının və şəxsin identifikasiya qurğularının müxtəlif növləri mövcuddur. Bəziləri optik yolla şəkilləri və başqa identifikasiya elementlərini, digərləri isə maqnit sahələrini tutuşdurur.

Ümumilikdə söyləsək, fiziki mühafizə vasitələri cinayətkarlar qarşısında duran ilk maneədir.

3.3. Aparat mühafizə vasitələri

İnformasiyanın aparat mühafizə vasitələrinə fəaliyyət prinsipinə, qurğularına və imkanlarına görə müxtəlif olan, açıqlanmanın qarşısının alınmasını, sızmadan mühafizə olunmasını və konfidensial informasiyanın mənbələrinə qeyri-qanuni müdaxilələrə əks tədbirləri təmin edən texniki qurğular aiddir.

Aparat mühafizə vasitələri aşağıda qeyd olunan məsələlərin həlli üçün istifadə olunur:

- mümkün sızma kanallarının olub-olmamasını müəyyən etmək üçün istehsalat fəaliyyətini təmin edən texniki vasitələrlə xüsusi nəzarət tədqiqatlarının aparılması;
- müxtəlif obyektlərdə və binalarda informasiyanın sızma kanallarının aşkarlanması;
- informasiyanın sızma kanallarının lokallaşdırılması;
- sənaye kəşfiyyatı vasitələrinin axtarışı və müəyyən edilməsi;
- konfidensial informasiya mənbələrinə qeyri-qanuni müdaxilələrə əks tədbirlərin həyata keçirilməsi.

Funksional təyinatına görə aparat mühafizə vasitələri aşkarlama vasitələrinə və axtarış vasitələrinə bölünür.

Aparat mühafizə vasitələri axtarış imkanlarına görə - ilkin (ümumi) qiymətləndirməni həyata keçirmək məqsədi ilə qeyri-peşəkarların istifadəsi üçün nəzərdə tutulan **ümumi təyinatlı;** və sənaye kəşfiyyatı vasitələrinin bütün xarakteristikalarını dəqiq axtarmağa, aşkarlamağa və dəqiq ölçmə aparmağa imkan verən **professional komplekslər** ola bilər.

Ümumi təyinatlı mühafizə vasitələrinə nümunə olaraq geniş spektrdə siqnal qəbul edən və çox kiçik həssaslığa malik olan elektromaqnit şüalanma indikatorlarını göstərmək olar.

Professional komplekslərə nümunə kimi isə radioötürücülərin, radiomikrofonların, telefona qoşulmaların və şəbəkə radioötürücülərinin avtomatik aşkarlanması və yerinin müəyyən edilməsi üçün nəzərdə tutulan radioqoşulmaların aşkarlanması və pelenqlənməsi üçün kompleksləri göstərmək olar. Bu, artıq mürəkkəb, müasir, peşəkar axtarış-aşkarlama kompleksidir.

Axtarış aparatlarını 2 qrupa bölmək olar: *informasiyanın ötürülməsi vasitələrinin axtarışı aparatı* və *informasiyanın sızma kanallarının tədqiq edilməsi aparatı*.

Birinci tip aparat cinayətkarlar tərəfindən tətbiq edilmiş qeyri-qanuni müdaxilə vasitələrinin axtarılmasına və həmin vasitələrin lokallaşdırılmasına yönəlmişdir. İkinci tip aparat informasiyanın sızma kanallarının aşkar edilməsi üçün nəzərdə tutulmuşdur. Bu növ sistemlər üçün əsas cəhət tədqiqatların operativliyi və əldə olunan nəticələrin etibarlılığıdır.

Peşəkar axtarış aparatından istifadə etmək üçün operatordan yüksək peşəkarlıq tələb olunur.

Fiziki təbiətinə görə informasiyanın müxtəlif sızma kanalları, həmçinin fiziki prinsiplərinə görə müxtəlif qeyri-qanuni müdaxilə sistemləri mövcuddur. Bu faktorlar axtarış aparatlarının müxtəlif növlü olmasına, bu müxtəliflik isə

aparatların qiymətlərinin yüksək olmasına gətirib çıxarır. Bu səbəbdən belə komplekslər yalnız daimi olaraq müvafiq tədqiqat işi aparan strukturlarda ola bilər. Belə strukturlar ya təhlükəsizlik xidmətləri, ya da kənar təşkilatlara xidmət göstərən xüsusi şirkətlərdir.

Əlbəttə ki, axtarış vasitələrindən müstəqil olaraq da istifadə etmək mümkündür. Bu vasitələr kifayət qədər sadədir və profilaktik tədbirlər görmək üçün əlverişlidir.

Xüsusi qrupa informasiya və kommunikasiya sistemlərinin aparat mühafizə vasitələri aid edilir.

Aparat mühafizə vasitələri həm personal kompüterlərdə, həm də şəbəkənin müxtəlif səviyyələrində və sahələrində: informasiya sistemlərinin mərkəzi prosessorlarında, əməli yaddaş qurğusunda (ƏYQ), xarici yaddaş qurğularında, terminallarda və s. tətbiq olunur.

3.4. Proqram mühafizə vasitələri

Kompüterin kənar müdaxilələrdən mühafizə olunması sistemləri müxtəlifdir, onlar aşağıdakı kimi təsnif olunur:

- ümumi proqram təminatı üçün nəzərdə tutulan fərdi mühafizə vasitələri;
- hesablama sisteminin tərkibində mühafizə vasitələri;
- informasiya sorğusu ilə mühafizə vasitələri;
- aktiv mühafizə vasitələri;
- passiv mühafizə vasitələri və s.

Bu mühafizə qrupları şəkil 3.13-də daha dəqiq təqdim olunmuşdur.

İnformasiyanın proqram mühafizəsinin əsas istiqamətləri.

Konfidensial informasiyanın təhlükəsizliyini təmin etmək üçün proqram mühafizəsinin aşağıda göstərilən istiqamətlərini qeyd etmək olar:

- qanunsuz müdaxilədən informasiyanın mühafizəsi;

- informasiyanın köçürülmədən mühafizəsi;
- proqramların köçürülmədən mühafizəsi;
- proqramların viruslardan mühafizəsi;
- informasiyanın viruslardan mühafizəsi;
- rabitə kanallarının proqram mühafizəsi.

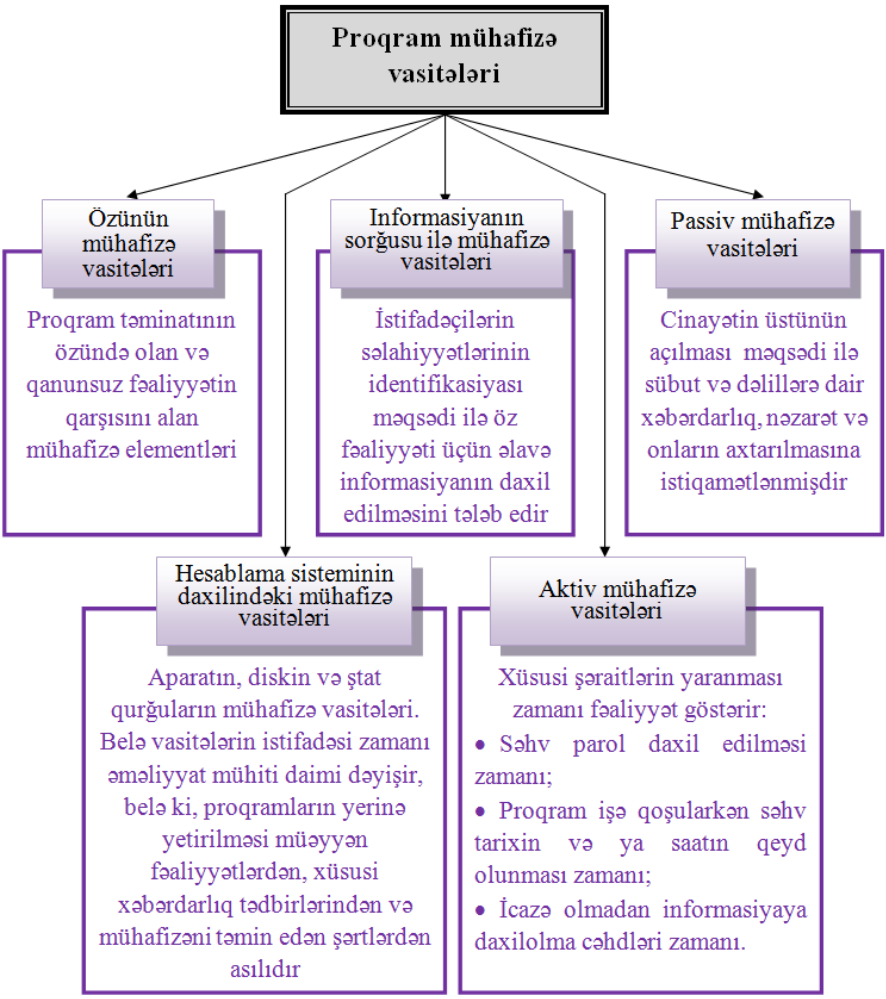
Göstərilən hər bir istiqamət üzrə kifayət sayda keyfiyyətli, nüfuzlu şirkətlər tərəfindən hazırlanıb satışa çıxarılmış proqram məhsulları vardır (şəkil 3.14).

Proqram mühafizə vasitələri müxtəlif xüsusi proqram növlərinə malikdir:

- texniki vasitələrin, faylların identifikasiyası və istifadəçilərin autentifikasiyası;
- texniki vasitələrin və istifadəçilərin işinin qeydiyyatı və onlara nəzarət;
- kompüterlərin əməli sistemlərinin və istifadəçilərin tətbiqi proqramlarının mühafizəsi;
- istifadədən sonra mühafizə qurğularındakı informasiyanın silinməsi;
- resurslardan istifadə hallarında pozuntular haqqında xəbərdarlıq;
- müxtəlif təyinatlı köməkçi proqramlardan istifadə (şəkil 3.15).

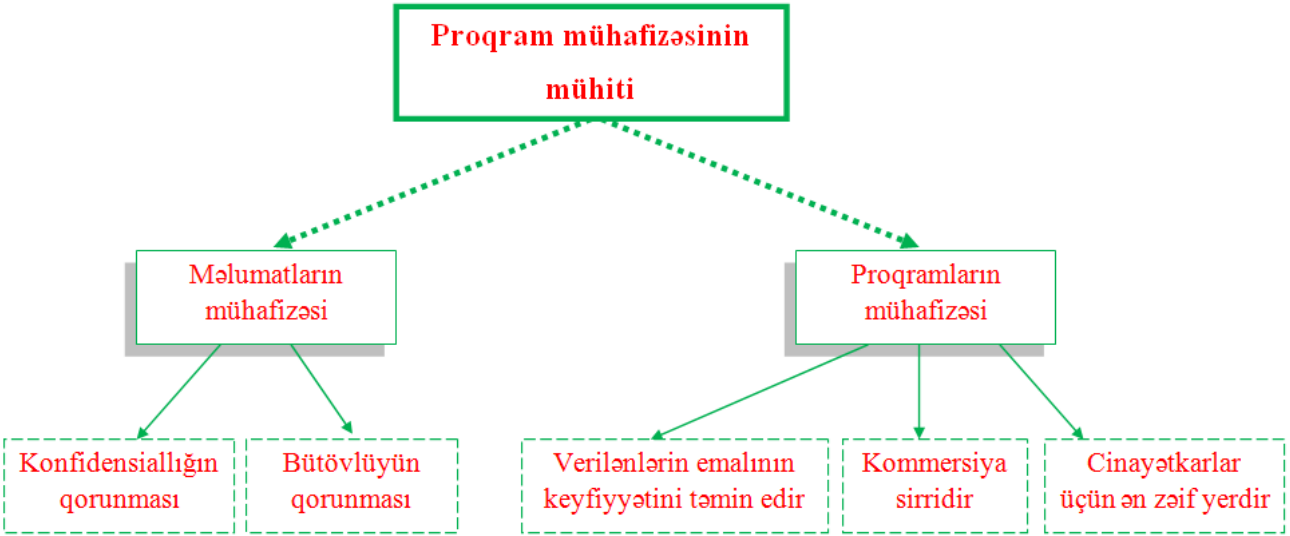
Texniki vasitələrin və faylların identifikasiyası üzrə proqramlar informasiya sisteminin müxtəlif komponentlərinin və obyektlərinin qeydiyyat nömrəsinin təhlili və onların idarəetmə sisteminin mühafizə qurğusunda saxlanılan ünvanlar və parollarla tutuşdurulması əsasında həyata keçirilir.

Mühafizənin etibarlılığının parolların köməyi ilə təmin edilməsi üçün mühafizə sisteminin işi elə təşkil olunur ki, məxfi parolun açılması ehtimalı az olsun.



Şəkil 3.13. Mühafizə qrupları

Şəkil 3.14. Proqram mühafizəsinin əsas istiqamətləri



Şəkil 3.15. Xüsusi proqram növləri

3.5. Autentifikasiyası prosesində şifrlərin tətbiqi

Şifrlərin təsnifatı. Şifrlərin yaradılması qaydaları.

Şifrlər, bir qayda olaraq, sistemə giriş açarları kimi qəbul edilir, lakin onlar müvafiq fəaliyyətin proqram təminatının qanuni sahibləri və istifadəçiləri tərəfindən həyata keçirilməsinə tam əmin olmaq üçün istifadə olunur.

Şifrlərin təsnifatı.

Şifrlər bir neçə əsas qrupa bölünür:

- sistem tərəfindən generasiya olunan şifrlər;
- yarımsözlər;
- əsas söz birləşmələri;
- "sual-cavab" tipli interaktiv ardıcıllıqlar;
- istifadəçi tərəfindən yaradılan şifrlər.

Sistem tərəfindən yaradılan *təsadüfi şifrlər* və kodlar müxtəlif növlü ola bilər. Sistemin proqram təminatı tamamilə təsadüfi simvol ardıcıllığını tətbiq edə bilər - registrlərə, rəqəmlərə, durğu işarələrinə, uzunluqlara qədər.

Yarımsözlər qismən istifadəçi, qismən də sistem tərəfindən yaradılır. Bu, o deməkdir ki, əgər istifadəçi hətta asanlıqla müəyyən edilə bilən şifr daxil etsə belə, məsələn, "sirr", kompüter onu tamamlayıb (məsələn, "sirr2rs87") daha mürəkkəb şifr yaradacaq.

Əsas *söz birləşmələrini* tapmaq çətin, yadda saxlamaq isə asandır.

Söz birləşmələri mənalı və ya heç bir məna kəsb etməyən ola bilər. Proqramlaşdırmada əsas söz birləşmələrinin daha geniş tətbiqinə keçid tendensiyası müşahidə olunur.

"Sual-cavab" tipli interaktiv ardıcıllıqlar istifadəçiyə bir neçə suala cavab verməyi təklif edir, bu suallar da, bir qayda olaraq, şəxsi məsələlərə dair olur. Bazada bir çox belə suallara cavablar toplanmışdır. İstifadəçinin sistemə girişi zamanı kompüter alınmış cavabları "düzgün" cavablarla müqayisə edir.

İstifadəçi tərəfindən yaradılan şifrlər. Şifrlərin əksəriyyəti "özün seç" tipinə aiddir. Adətən şifr ən azı dörd-beş simvoldan ibarət olur. Eləcə də, istifadəçiyə uğursuz şifr yaratmağa imkan verməyən başqa tədbirlər də mövcuddur. Məsələn, sistem təkid edə bilər ki, şifr böyük və kiçik hərflərdən, rəqəmlərdən ibarət olsun, adi şifrlər qəbul olunmur, məsələn, "user", "ana", "Azərbaycan" və s.

Şifrlərin yaradılması qaydaları.

Şifrlərin yaradılması üzrə bir sıra qaydalar mövcuddur, bu qaydalara riayət etmək gərəkdir.

Şifrlər aşağıda qeyd olunanlardan ibarət olmamalıdır:

– yalnız rəqəmlər və ya eyni hərflər;

– istənilən formada adınız, atanızın adı və ya soyadınız (yəni kiçik hərfli, böyük hərfli, qarışıq formada, sondan əvvələ yazılmış, iki dəfə təkrar olunan və s.);

– xanımınızın (yoldaşınızın) və ya uşağınızın adı;

– şəxsi informasiyalar – buraya telefon nömrələri, buraxılış vəsiqələrindəki (icazə vərəqələrindəki) və digər sənədlərdəki nömrələr, avtomobilin nömrəsi və ya markası, poçt ünvanı və s. daxildir;

– lüğətlərdə (istənilən, xarici lügətlər daxil olmaqla) qeyd olunan sözlər.

Şifrdə rahat tapılan simvollar yığımından istifadə etmək qadağan olunur.

Şifrlərin mürəkkəbliyinin yoxlanılması üçün xüsusi şifr kontrollerlərindən (nəzarətçi) istifadə edilir. Kontrollerlər müxtəlif üsullarla şifrin qırılması cəhdlərini həyata keçirir, məsələn:

1. İstifadəçinin adının, onun inisiallarının və onların kombinasiyalarının giriş şifri kimi istifadə edilməsinin yoxlanılması.

2. Müxtəlif lüğətlərdə qeyd olunmuş sözlərin şifr kimi istifadə edilməsinin yoxlanılması:

–kişi və qadın adları;

–ölkə və şəhər adları;

–cizgi film qəhrəmanlarının adları, filmlər, elmi-fantastik əsərlər və s.;

–idman terminləri (idman komandalarının adları, idmançıların adları, idman jarqonu və s.);

–saylar (rəqəmlərlə və yazı ilə);

–hərflərin və rəqəmlərin sətirləri (məsələn, AA, AAA, AAAA və s.);

–dini adlar;

–bioloji terminlər;

–jarqon sözlər və söyüşlər;

–simvolların klaviaturada yerləşməsi ardıcıllığı (məsələn, QWERTY, ASDF, ZXCVBN və s.);

–tez-tez istifadə edilən xarici sözlər.

3. İkinci bənddə qeyd olunan sözlərin müxtəlif yerdəyişmələrinin yoxlanılması, aşağıdakılar daxil olmaqla:

- sözün birinci hərfinin böyük yazılması;
- sözün bütün hərflərinin böyük yazılması;
- sözün bir hərfinin böyük yazılması;
- sözün iki hərfinin böyük yazılması (təxminən 1,500,000 sözdə);
- sözün üç hərfinin böyük yazılması;
- sözdə “O” hərfinin “0” rəqəmi ilə əvəz edilməsi və əksinə (1 rəqəmin I hərfi ilə əvəz edilməsi və s.);
- sözlərin cəmdə yazılması.

Yuxarıda göstərilən nümunələr şifrlərin zəifliyinin azaldılmasının bir sıra üsullarının yaradılmasına imkan verir. Şifr aşağıdakı tələblərə cavab verməlidir:

a) müəyyən qədər uzun olmalı;

b) böyük və kiçik hərflərdən istifadə edilməli;

c) bir və daha çox rəqəmdən istifadə edilməli;

d) ən azı bir rəqəm və hərf olmayan simvoldan istifadə edilməli.

O cümlədən şifrlər:

- elə təşkil olunmalıdır ki, onları klaviaturada tez yığmaq mümkün olsun. Bu, şifrə kənar adamların baxıb yadda saxlaması ehtimalını azaldacaq;
- asan yadda saxlanan olsun ki, onları qeyd etməyə ehtiyac olmasın;
- şifrin uzunluğu ən azı 8 simvol təşkil etməlidir;
- hərf olmayan simvollar olmalıdır (yəni rəqəmlər, durğu işarələri, xüsusi simvollar);
- şifri seçərkən kiçik və böyük hərflərdən, rəqəm və digər işarə kombinasiyalarından istifadə etmək tövsiyə edilir;
- hər bir şifr ən azı iki hərf (böyük və ya kiçik), bir rəqəm və ya simvoldan ibarət olmalıdır;
- yeni şifr köhnədən ən azı üç simvolla fərqlənməlidir;
- hər şifr istifadəçi adından fərqlənməlidir;
- istifadəçi ən azı ayda bir dəfə əsas şifri dəyişməlidir.

Şifrin ən əhəmiyyətli xüsusiyyəti onun uzunluğu və dəyişdirilməsi dövrüdür (həyat dövrü). Şifrin uzunluğu nə qədər çox olarsa, cinayətkar onu müəyyən etmək üçün daha çox güc sərf etməli olacaqdır. Şifrin həyat dövrü nə qədər uzun olarsa, onun qırılması ehtimalı bir o qədər çox olacaq.

3.6. Kriptoqrafik mühafizə vasitələri

İnformasiyanın kriptoqrafik mühafizə vasitələri kommersiya fəaliyyəti sahəsində getdikcə daha önəmli yer tutur.

Kriptoqrafiya kifayət qədər qədim tarixə malikdir. Əvvəllər o, daha çox hərb və diplomatiya sahələrində geniş istifadə olunurdu. İndi isə kriptoqrafiya istehsalat və kommersiya fəaliyyətində geniş yayılmışdır. Nəzərə alsaq ki,

indiki dövrdə şifrlənmiş rabitə kanalları ilə milyonlarla xəbər, telefon danışıqları, böyük həcmdə kompüter məlumatları göndərilir və bütün bu məlumatlar kənar şəxslərə aid olmadığı üçün belə məlumatların gizliliyinin qorunması çox vacibdir.

Kriptoqrafiya nədir? Bura müasir riyaziyyatın bir neçə bölməsi, həmçinin fizikanın, radioelektronikanın, rabitənin xüsusi sahələri daxildir.

«Kriptoqrafiya» sözü kryptos (“gizli”) və graphos (“yazı”) yunan sözlərindən yaranmışdır. Şifrləmə proseduru adətən müəyyən kriptoqrafik alqoritmdən və açardan istifadəni nəzərdə tutur.

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

Kriptoqrafiyanın əsas məqsədi rabitə kanalları ilə ötürülən məxfi məlumatların, telefon danışıqlarının və ya kompüter verilənlərinin riyazi metodlarla dəyişdirilməsidir ki, onlar kənar şəxslər üçün anlaşılmayan olsun. Yəni kriptoqrafiya gizli informasiyanın mühafizəsini elə təşkil etməlidir ki, əgər o, kənar şəxslərin əlinə keçsə də, ən qabaqcıl kompüterlərdə emal edilsə də, elmin və texnikanın sonuncu nailiyyətlərindən istifadə olunsa da, onun deşifrlənməsi (şifrinin açılması) növbəti illərdə də mümkün olmasın. Belə informasiya çevrilməsi üçün müxtəlif şifrləmə vasitələrindən – sənədlərin şifrlənməsi vasitələri, danışığın şifrlənmə vasitələri (telefon və radio-danışıqlar), teleqraf xəbərlərinin şifrlənmə vasitələri kimi – istifadə olunur.

Kriptoqrafik alqoritm – məlumatların çevrilməsinin müəyyən üsuludur. Açar isə çevirmə üsulunu konkretləşdirir. Müasir kriptoqrafiya o prinsipdən çıxış edir ki, kriptoqrafik çevirmənin məxfiliyi yalnız açarın məxfi saxlanması ilə təmin edilməlidir.

İlk kripto-sistemlər artıq bizim eranın əvvəlində meydana çıxmışdır. Məsələn, məşhur Roma sərkərdəsi Yuliy Sezar (e.ə. 100-44-cü illər) öz yazışmalarında indi onun adını daşıyan şifrdən istifadə edirdi. Müasir ingilis əlifbasına tətbiqdə bu şifr aşağıda qeyd olunan kimi yazılırdı. Yəni adi əlifba yazılırdı, sonra onun altında həmin əlifba, lakin sola üç hərf dövri sürüşmə ilə yazılırdı:

ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ

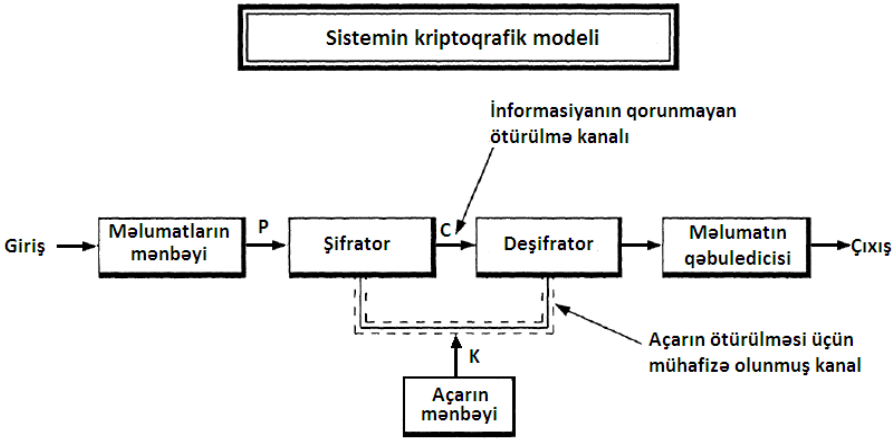
Şifrləmə zamanı A hərfi D hərfi ilə, B hərfi E ilə və beləcə əvəz olunurdu. Məsələn: VENI VIDI VICI ® YHQL YLGL YLFL. Şifrlənmiş məlumatı alan tərəf hərfləri ikinci sətirdə axtarırdı və onların üstündəki hərflərə görə ilkin mətni bərpa edirdi. Sezar şifrində açar əlifbanın ikinci sətrindəki sürüşmənin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

Şifrləmənin ümumi texnologiyası

Rabitə kanalları ilə ötürülən başlanğıc informasiya nitq, verilənlər, videosiqnallar ola bilər və P adlanır (şəkil 3.16).

Şifrləmə qurğusunda P məlumatı şifrlənir (C şifrinə çevrilir) və "qapalı" rabitə kanalı ilə ötürülür. Qəbul məntəqəsində C məlumatı başlanğıc P məlumatını bərpa etmək üçün deşifrə edir.

Müəyyən informasiyanın çıxarılması üçün tətbiq olunan parametr açar adlanır.



Şəkil 3.16. Şifrləmənin ümumi texnologiyası

Şifrləmənin simmetrik və asimmetrik adlanan iki əsas üsulu var. Simmetrik şifrləmə üsulunda eyni açar (gizli saxlanılan) həm məlumatı şifrləmək, həm də deşifrləmək üçün istifadə olunur. Olduqca effektiv (sürətli və etibarlı) simmetrik şifrləmə metodları vardır.

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

Asimmetrik kriptoqrafiyada iki açardan istifadə olunur. Onlardan biri açıq açar (sahibinin ünvanı ilə birlikdə nəşr oluna bilər) - şifrləmə üçün istifadə olunur, digəri gizli açar (yalnız alana məlumdur) - deşifrləmə üçün istifadə olunur. Rəqəmsal imza alqoritmlərində gizli açar şifrləmə, açıq açar isə deşifrləmə üçün istifadə edilir. Açıq açara görə uyğun gizli açarın tapılması çox böyük həcmdə hesablamalar tələb edir,

hesablama texnikasının hazırki inkişaf səviyyəsində bu məsələ qeyri-mümkün hesab edilir.

Asimmetrik kriptoqrafiyanın əsas çatışmayan cəhəti sürətin aşağı olmasıdır. Buna görə onlar simmetrik metodlarla birgə işlədilir. Məsələn, açarların göndərilməsi məsələsini həll etmək üçün əvvəlcə məlumat təsadüfi açarla simmetrik metodla şifrlənir, sonra qəbul edən tərəfin açıq asimmetrik açarı ilə təsadüfi açarı şifrləyirlər, bundan sonra məlumat və şifrlənmiş açar şəbəkə ilə ötürülür.

Asimmetrik metodlardan istifadə etdikdə (istifadəçi - açıq açar cütünün) həqiqiliyinə zəmanət tələb olunur. Bu məsələnin həlli üçün rəqəmsal sertifikatdan istifadə edilir. Rəqəmsal sertifikat xüsusi sertifikasiya mərkəzləri tərəfindən verilir. Rəqəmsal sertifikatda aşağıdakı verilənlər olur: sertifikatın seriya nömrəsi; sertifikatın sahibinin adı; sertifikatın sahibinin açıq açarı; sertifikatın fəaliyyət müddəti; elektron imza alqoritminin identifikatoru; sertifikasiya mərkəzinin adı və s. Sertifikat onu verən sertifikasiya mərkəzinin rəqəmsal imzası ilə təsdiq edilir.

Fəsil üzrə yoxlama sualları

Qeyd olunan fikrin səhv və ya düz olduğunu müəyyənləşdirin.

	Düz	Səhv
1. Şifrin həyat dövrü nə qədər uzun olarsa və şifrin uzunluğu nə qədər az olarsa, onun qırılması ehtimalı bir o qədər çox olacaq.	☐	☐
2. Təbii və süni maneələr aparat mühafizə vasitələrinə aiddir.	☐	☐
3. Asimmetrik kriptoqrafiyanın əsas çatışmayan cəhəti sürətin aşağı olmasıdır.	☐	☐

Test suallarını cavablandırın:

1. Funksional təyinatına görə mühəndis-texniki mühafizə vasitəsi hansı bəndlərdə göstərilmişdir?

a) təşkilati vasitələr
b) proqram vasitələri
c) kriptoqrafik vasitələr
d) hüquqi vasitələr

2. Hansı tanıma üsulları vardır?

a) kriptoqrafik
b) atribut
c) personal
d) təcrid

3. Şifrlər əsas hansı qruplara bölünür?

a) əsas söz birləşmələri

b) teqlər
c) “sual-cavab” tipli interaktiv ardıcıllıqlar
d) istifadəçi tərəfindən yaradılan şifrlər
e) IP-lər
f) sistem tərəfindən generasiya olunan şifrlər
g) yarımsözlər

Açıq sualların cavablarını əhatəli qeyd edin:

1.Stasionar metalaxtaranın üstünlükləri hansılardır?

_____
_____
_____
_____
_____

2. Şifrləmənin simmetrik üsulu nədir?

_____
_____
_____
_____
_____

4. Cəmiyyətə ünvanlanan informasiya təhlükələrinin təhlili

4.1. İnformasiya müharibəsi

Son vaxtlar "informasiya müharibəsi" anlayışlarından tez-tez istifadə olunur və həmin anlayış müxtəlif cür izah edilir.

Lakin bir "informasiya müharibəsini" informasiyadan istifadə edilən mübarizənin ali forması kimi izah etmək olar. İnformasiya müharibəsi rəqibin informasiya sistemlərinə, proseslərinə, kompüter şəbəkəsinə, əhalinin və hərbi qüvvələrin şəxsi heyətinin şüuruna təsir yolu ilə informasiya üstünlüyünün əldə edilməsi üçün istifadə edilən, eyni zamanda öz informasiya mühitini mühafizə edən tədbirlər kompleksidir. Belə anlayış ABŞ-ın Hərbi Qüvvə Qərargahlarının rəhbər komitəsi tərəfindən hazırlanan "İdarəetmə və rabitə sahəsində vahid rəqabət doktrinası"nda istifadə olunur.

Beləliklə, qeyd olunan doktrinada 2 növ informasiya mübarizə forması vardır: informasiya-texniki və informasiya-psixoloji. Tarix boyu hər iki növ informasiya mübarizə forması inkişaf etmiş və təkmilləşmişdir.

İnformasiya tarixi inkişafın bütün mərhələlərində mübarizə obyekti olmuşdur. İnformasiya mübarizəsi bütün müharibələrdə həyata keçirilirdi. Hələ qədimdə sərkərdələr, mütəfəkkirlər döyüşsüz qələbə qazanmağın vacibliyindən danışırdılar. O zamandan bəri düşmənə dezinformasiya, hədələr, qorxutma ilə təsir üsulları tətbiq edilirdi. Bu üsullar XV əsrlərdə daha da inkişaf etmişdi. XX əsrin kiçik və geniş miqyaslı müharibələrində kütləvi informasiya vasitələrinin rolu xüsusilə geniş olmuşdur.

Müasir elmi-texniki inqilab informasiya mübarizəsində çevriliş etdi. Aktiv olaraq psixoloji əməliyyatlar keçirilməyə, yeni informasiya texnologiyaları intensiv olaraq tətbiq edilməyə başlandı. Bu gün informasiya mübarizəsinə daha çox

qüvvə və vəsait cəlb edilir, onun nəticələri daha təsirli olur. ABŞ, Yaponiya, Almaniya, Fransa, Rusiya, İsrail və d. inkişaf etmiş ölkələrdə informasiya təhlükəsizliyinə geniş yer verilir, belə ki, bu sahə müasir dünyanı ələ almağın əsas amillərindən biri hesab olunur.

İnformasiya müharibəsi dedikdə, əsasən, qədim zamanlardan bizim dövrə kimi böyük müharibələrdə, lokal münaqişələrdə informasiya mübarizələrinin işıqlandırılması başa düşülür. Burada nəzər yetirilməli olan əsas məqamlar – ictimai rəyə təsir mexanizmləri, hərbi münaqişələrdə kütləvi informasiya vasitələrinin rolu, "Qaynar nöqtələrdə" mətbuat xidməti əməkdaşlarının, jurnalistlərin işi və dövlət sirrinin mühafizəsi problemləridir.

4.1.1. Qədim dövlətlərdə informasiya-psixoloji təsir

Psixoloji təsirli informasiya silahı qədim tarixə malikdir. Hərbi-tarixi ədəbiyyatda dezinformasiyadan istifadə etmə halları olmuşdur. Məsələn, e.ə. 1312-ci ildə xetlər yalan informasiya ilə firon II Ramzesin başçılığı altında Misir qoşunlarını yanılda bilmiş və Kadeş qalası yaxınlığındakı döyüşdə onlara qəfil zərbə endirə bilmişdilər. Bu hadisə II Ramzesi Kadeş qalasını ələ keçirmək niyyətindən yayındırır və Misirə qayıtmağa sövq edir.

B.e.ə. VI əsrin sonları-V əsrin əvvəllərində yaşamış qədim Çin sərkərdəsi Sun-tzı hesab edirdi ki, ən yaxşı qələbə - döyüşsüz əldə olunan qələbədir. Qədim Çin hərb tarixində dədüşmənlərini döyüşsüz məğlub edə bilən sərkərdələrə daha çox ehtiram olunurdu. Məsələn, Yuy Şun imperatorunun vaxtında (b.e.ə. 2255-2220-ci illər) San-Myao xalqı qiyam qaldırır. İmperator qiyamı yatırtmağa çalışır, lakin görür ki, həmin xalqın yaşadığı ərazi xarakterinə görə müdafiə üçün yaxşı uyğunlaşmışdır və onları silahla ram etməyi gərəksiz bilir. Öz ordusu ilə geri çəkilən Yuy öz ölkəsinin rifahının

qaldırılması, mədəniyyətinin inkişaf etdirilməsi, xalqının vəziyyətinin yaxşılaşdırılması ilə məşğul olmağa başlayır. Həmçinin Yuy çalışırdı ki, bunlar haqda məlumat San-myao xalqına da çatsın. Və o, öz istəyinə nail olur, həmin əhali özü itaətkarlıq göstərir.

B.e.ə. III əsrdə isə hökmdar Tsao Tsao Xandan şəhərini mühasirəyə almaqla ələ keçirir. Lakin kiçik qalalardan biri olan İyanı zəbt edə bilmirdi. Həmin qalanın sakinləri Xan Fanın başçılığı altında şücaətlə müdafiə olunurdular. Bu zaman Tsao Tsao öz əsas sərkərdələrindən biri olan Syu Xuanı bu qalanı fəth etmək üçün göndərir. Syu qalanı tutmaq üçün hücum etmək əvəzinə ox vasitəsilə Xan Fana məktub yollayır, həmin məktubda ona müqavimət göstərməyin tam faydasız olduğunu əsaslı şəkildə izah edir və təslim olmağı tövsiyə edir. Syu öz məktubunda izahatı elə yaxşı göstərə bilmişdi ki, öz istəyinə çatmışdı, Xan Fan müqavimət göstərməyi dayandırmışdı. Belə təsir üsullarına Qədim Çin hərb sənəti tarixində tez-tez əl atılırdı.

Bu nümunələrdən məlum olur ki, qədim hökmdarlar və sərkərdələr düşmənlərinə döyüşsüz, informasiya üsullarından istifadə etməklə qalib gəlmək üçün 3 metod tətbiq edirdilər: birinci üsul müdrik hakimiyyət formasını yaratmaq, dövlətin firavanlığını təmin etmək, xalqın rifahını yaxşılaşdırmaq; ikinci üsul rəqiblə münasibət qurmaq, onun istəklərinə, ehtiyaclarına diqqət göstərmək üçün müdrik siyasət; üçüncü üsul müqavimət göstərməyin faydasızlığını anlatmaq üçün hərbi-strateji xarakterli tədbirlər. Bütün qeyd olunan 3 üsulla hökmdarlar öz fəaliyyəti ilə düşmənin şüuruna təsir göstərməyə çalışırdılar və qan tökülmədən qələbə qazanmağa nail olurdular. Və bu qeyd olunan hər bir konsepsiyada informasiya elementi az rol oynamırdı.

Qədim Yunanıstanda, Romada müharibələrdə, döyüşlərdə informasiya-psixoloji təsirlərdən – əhalinin ictimai rəyi, təbliğat, şayiələr, divarüstü yazılardan istifadə edilirdi.

4.1.2. Orta əsrlərdə müharibənin informasiya-psixoloji təminatı

Qədim dövlətlərin müharibələri zamanı yaranan informasiya-psixoloji təsirin əsas istiqamətləri və formaları orta əsrlərdə daha da inkişaf etməyə başlayır. Bu, əsasən orta əsr dünyasının demək olar ki, əsas regionlarını ələ keçirən monqolların hücumlarında özünü daha çox büruzə verirdi. Bu hücumlar zamanı monqollar məharətlə psixoloji müharibə aparır, düşmənin iradəsini qırmaq üçün xüsusi təbliğat kampaniyaları təşkil edirdilər. Məsələn, Çingizxan öz istilaları zamanı zəbt etmək istədiyi ərazilərə ordusundan qabaq öz casuslarını göndərirdi. Casuslar tacir qiyafəsində əhali arasında daxil olur, onlara monqolların ordusunun gücü və qüvvəsi, sayı, döyüşləri, qələbələri, viran qoyduğu, talan etdiyi ərazilər, amansızlığı, qəddarlığı haqqında danışır, əhalini mənəvi cəhətdən zəiflədir, onlarda ruh düşkünlüyü yaradırdılar.

Orta əsrlərdə müharibələrin informasiya-psixoloji təminatında dini ideyalar aktiv rol oynayırdı. Bu dövrdə İslam ölkələrində və Avropa ölkələrində psixoloji-dini fikirləri yaymaqla, vahid bir ideya altında müharibələrdə qələbə əldə daha asan mümkün olurdu.

XV əsrin ortalarında İohan Quttenberqin kəşfi olan kitab çapı informasiya-təbliğat müharibələri tarixində dönüş nöqtəsi olmuşdu. Alman ixtiraçısının kəşfinin mühümlüyünü ilk olaraq dini zümrə anlamış və dini yazıların çapında tətbiq etməyə başlamışdı. Bu kəşfdən 50 il sonra kitablar informasiya-psixoloji müharibələrdə istifadə olunan silaha çevrilmişdi. 1500-cü ildə artıq 200-dən çox ölkədə 110 nəşriyyat 12 milyon nüsxəli 36000 müxtəlif adda kitab buraxılmışdı.

XVI əsrdə təbliğat ədəbiyyatı daha da artmış, türklərin istilaları haqqında çoxlu sayda kitabçalar nəşr olunmuşdu. Həmçinin genişmiqyaslı münaqişələr zamanı Almaniyada

reformasiya və kəndli müharibəsi, Fransada dini müharibələr, Niderlandda burjua inqilabı zamanı kitab buraxılışının sayında sıçrayışlar müşahidə olunurdu. Dini və elmi ədəbiyyatla yanaşı, "uçan" broşürlər və kağızlar çoxlu sayda çap olunurdu. Almaniyada çap olunan broşürlərin çox hissəsi reformasiyaya həsr olunurdu.

XVII əsrdən başlayaraq, ictimai rəyin formalaşmasında dövri nəşrlərin – qəzetlərin təsiri daha geniş rol almağa başlamışdı.

Napoleon Bonapart da istilalarında təbliğatdan istifadə edirdi. Rusiyanı ələ keçirmək üçün öz işğalı altında olan ölkələrin iqtisadi və hərbi resurslarından əlavə, onların qəzetlərindən də istifadə edirdi. Mahir sərkərdə, lider və təşkilatçılıq xüsusiyyətləri ona ictimai rəyə təsir etmək bacarığını inkişaf etdirməkdə yardımçı olmuşdu. Rusiyaya hücumdan öncə Napoleona Fransada və digər Avropa ölkələrində öz hərbi səfərinə bəraət qazandırmaq lazım idi. Napoleonun göstərişi ilə mətbuatda Rusiyanın işğalçı, Avropa sivilizasiyasını məhv etmək istəyən ölkə kimi göstərilməsinə çalışılırdı. Hətta "yalandan" "I Pyotrun vəsiyyəti" adlı sənəd çapdan buraxılmışdı ki, orada Rusiyanın XIX əsrə kimi qonşu Avropa ölkələrini zəbtetmə planı göstərilirdi. Beləliklə, Napoleon öz hücumuna "mühafizə tədbiri" donu geyindirmək və Avropada özünə dəstək tapmaq istəyirdi. Napoleonun bir kəlamı da məşhur idi: "Dörd qəzet düşmənə 100 minlik ordudan çox zərər yetirə bilər".

Rəqibə say baxımından uduzan ordusunun döyüş ruhunu artırmaq məqsədi ilə Napoleonun əmri ilə həvəsləndirici əmrlər və hərbi bülletenlər buraxılırdı. Həmin bülletenlərdə Fransız döyüşçülər düzgün yolun davamçıları, qayda-qanun gətirənlər kimi göstərilirdi. Onun göstərişi ilə çap olunan həvəsləndirici manifestlər isə həm öz ordusu, həm də işğal olunan xalqa ünvanlanırdı (göndərilirdi), öz hücumlarına haqq qazandır-mağa, yerli nüfuzlu xadimlərlə əlaqə yaratmağa xidmət edirdi.

İmperator bütün böyük işğallarından sonra (İtaliyada, Misirdə, Hollandiyada, Almaniyada) həmin ərazilərdə hərbi qəzetlərin çapına başlayır, həmin ölkələrin mətbu şirkətlərini ələ alırdı.

4.1.3. XX əsrdə informasiya müharibələri

İnformasiya müharibələri daha çox XX əsrdən başlayaraq geniş vüsət almışdır. Müharibə aparan tərəflərdə radioəlaqə vasitələrindən istifadə edilməsi rəqiblərə tətbiq edilən yeni təsir üsullarının yaranmasına gətirib çıxardı. İnformasiyanın əldə edilməsi sahəsində ənənəvi kəşfiyyatla və rəqibin dezinformasiyası üzrə tədbirlərlə yanaşı, radiomaneələrlə radioəlaqənin yatırılması vasitələri tətbiq edilməyə başlandı. İlk dəfə bu üsullardan 1904-cü ildə rus-yapon müharibəsində istifadə edilmişdir. Növbəti mərhələlərdə bu tədbirlər Birinci və İkinci Dünya müharibələrində qələbələr əldə etməkdə böyük rol oynamışdır.

Birinci Dünya müharibəsi ərəfəsində Qərb ölkələrinin (İngiltərə, ABŞ, Fransa, Almaniya və s.) psixoloqları tərəfindən çoxsaylı xüsusi tədqiqatlar həyata keçirilirdi. Bu tədqiqatlarda hərbi qulluqçuların döyüş vəziyyətində adekvat və düzgün fəaliyyətə psixoloji hazırlığı yoxlanılır, onların təlaşa, qorxuya qarşı mübarizə aparması, uzunmüddətli əsəb-psixoloji yüklənmələrə tab gətirmək bacarığı öyrənilirdi. Müharibə zamanı bir çox ölkələrdə düşmən xalqa və rəqib qüvvələrə qarşı yönəlmiş, təbliğat aparmağı bacaran xüsusi dəstələr yaradılmışdı.

Çap materiallarının yayılması və şifahi təbliğat uzun illər bir ölkənin digər ölkəyə ideoloji təsirinin əsas kanalı idi. Radioyayımın inkişafı bu kanalları arxa plana çəkdi. XX əsrin 20-30-cu illərində bir çox ölkələrdə radioyayımdan xarici siyasətə və ideologiyaya qarşı ən kəskin silah kimi istifadə edilirdi.

İkinci Dünya müharibəsində informasiya silahı əhəmiyyətli dərəcədə inkişaf etdi. İnformasiya təsirinin əhəmiyyətini hamıdan öncə Almaniya dərk etmişdi. Hakimiyyətə gəlişindən dərhal sonra Hitler ilk dəfə olaraq digər ölkələrin əhalisinə qlobal informasiya-psixoloji təsir göstərməyə cəhd etdi. Belə ki, qəfil hücum həyata keçirmək üçün Almaniyanın hərbi-siyasi rəhbərliyi tərəfindən ümumdövlət planı hazırlanırdı. Bu plana əsasən hücuma məruz qalacaq dövlətlərin və onların müttəfiqlərinin rəhbərlərini aldatmaq, yanıltmaq əsas məqsəd daşıyırdı. 1941-ci ilin iyun ayında SSRİ-yə qarşı əvvəldən elan edilmədən, qəfləti hücum belə fəaliyyətin aşkar nümunəsi idi. Dezinformasiya planlarına vahid fikir altında birləşmə və öz aralarında siyasi, diplomatik, iqtisadi və hərbi tədbirləri razılaşdırma daxil idi. Bundan əlavə, Almaniya dövlətinin rəhbərliyi Versal müqaviləsinə əsasən qadağan edilmiş müdafiə sənayesi sahələrinin, hava qüvvələrinin, tank əleyhinə qoşunların yaradılması kimi tədbirlər həyata keçirirdi. Hazırlıq tədbirlərinin gizliliyi və hücumun aniliyi bu planın əsası hesab olunurdu.

Normandiyadakı genişmiqyaslı desant hücumunda (1944-cü ildə) informasiya sahəsində üstünlük əldə etmək üçün ABŞ və onun müttəfiqləri əməliyyatı müvəffəqiyyətlə həyata keçirdilər. Nəticədə müttəfiqlərin böyük gəmi armadası La-Manş boğazını praktiki olaraq maneəsiz ötüb keçdi, sahilin ələ keçirilməsi isə gözləniləndən daha asan oldu.

Bir çox əməliyyatlarda gizlilik və rəqibin dezinformasiya edilməsi uğurla həyata keçirilirdi. İnformasiya müharibəsi radioelektron vasitələrin tətbiqi ilə daha da inkişaf etməyə başlamışdı. Məsələn, 1940-cı ildə Almaniyanın Hərbi-Dəniz Qüvvələrinin radiokəşfiyyatı Britaniya Hərbi-Dəniz Qüvvələrinin radio-əlaqələrini yarmış və onların radioqramlarının 50%-ni ələ keçirmişdi.

İnformasiya-psixoloji əməliyyatların əsas məqsədlərindən biri də rəqib qoşunların və düşmən əhalinin təbliğat

vasitəsi ilə mənəvi sarsıdılması idi. Bunun üçün mübarizə aparan tərəflər radiotəbliğatdan və aviasiya vasitəsilə vərəqələrin yayılmasından istifadə edirdilər. Bir çox ölkələrin psixoloji müharibə vasitələri sərbəst xidmət göstərirdi.

Koreyada və Yaxın Şərqdə müharibələr zamanı efirlərdə əsl "informasiya döyüşləri" aparılırdı. Bu halda radiomaneələr vasitəsilə radioəlaqələrin kəsilməsi, qoşunlara rəhbərlik, Hava Hücumundan Müdafiə sistemlərinin çaşdırılması kimi işlər həyata keçirilirdi. Həmçinin rəqibin radioşəbəkəsinə daxil olmaqla, onun qoşunlarına yanlış göstərişlər və əmrlər verilirdi.

6 iyun 1967-ci il tarixində ərəb-İsrail müharibəsində ərəb qoşunlarının radioşəbəkəsinə daxil olmaqla, Misirin 4-cü tank diviziyasının həmləsinin qarşısı alınmışdı. İsrail dezinformatorları tərəfindən radio vasitəsi ilə diviziyanın komandirinə döyüşdən çıxmaq və Süveyş kanalından geri çəkilmək haqqında əmr verilmişdi.

İngilis desantları tərəfindən Folklend adalarının ələ keçirilməsi zamanı informasiya müharibəsinin elementləri əməliyyatların hazırlığı və həyata keçirilməsinin əsas hissəsi olmuşdu. ABŞ-ın kəşfiyyat peyklərindən alınmış informasiya ilə ingilis sualtı gəmisi Argentina donanmasının "General Belqrano" kreyserini batırmağa nail olmuş və bütövlükdə donanmanın fəaliyyətini iflic etməyi bacarmışdı.

Liviyada "Eldorado Kanyon" əməliyyatının (1986-cı il) gedişatında aviasiya zərbələrinin aniliyinin effektliliyini təmin etmək üçün maskalanma tədbirlərindən: dezinformasiya, radiosükut rejimi, radiomaskalanma və s. istifadə edilirdi. Liviyanın Hava Hücumundan Müdafiə sisteminin işini pozmaq məqsədi ilə kəşfiyyat vasitələrini söndürmək üçün yanlış komandalar verən agenturadan istifadə edilirdi.

XX əsrin ikinci yarısı informasiya-psixoloji mübarizə sahəsində dönüş mərhələsi oldu. Bir sıra ölkələrin silahlı qüvvələrində rəqibə və öz qoşunlarına mənəvi-psixoloji təsir göstərə bilən xüsusi orqanlar, güclər və vasitələr yaradılmağa

başlandı. Bütün hərbi münaqişələrdə, hücuma hazırlıqlarla bərabər, ictimai rəyə məqsədyönlü, qlobal xarakter daşıyan informasiya-psixoloji təsirlər başlayırdı. İnformasiya vasitələrinin və rəqiblə mübarizə üsullarının hazırlanmasında lider Amerika Birləşmiş Ştatları olmuşdu.

XX əsrin 2-ci yarısında tez-tez müharibə iştirakçısı olan ABŞ informasiya müharibələrinin təşkil edilməsində daha çox təcrübə qazanırdı, öz ordusunun hərbi fəaliyyətinin informasiya-psixoloji təminatını, öz vətəndaşlarının və beynəlxalq ictimaiyyətin psixoloji baxımdan təkmilləşdirilməsini həyata keçirirdi.

ABŞ ilk öncə Vyetnam müharibəsində ictimai rəyi nəzərə almadığına görə məğlubiyyətə düçar olmuşdu. Müharibə göstərdi ki, döyüşdə partizan metodlarını tətbiq edən daha zəif rəqiblə uğurla mübarizə aparmaq üçün yalnız hərbi və texnologiya üstünlüyü kifayət deyil, əlavə olaraq, informasiya-psixoloji üstünlük də qazanmaq lazımdır. Bu amillərin nəzərə alınmaması ABŞ ordusunda və ölkədə "Vyetnam sindromunun" yaranmasına gətirib çıxarmışdı.

Qrenadaya (1983-cü il), sonradan isə Panamaya (1989-cu il) müdaxilə zamanı ABŞ-ın siyasi və hərbi rəhbərliyi, Vyetnamın təcrübəsini nəzərə alıb, ictimai rəyi ələ almaq üçün, həmçinin döyüş fəaliyyətində informasiya təminatı üçün çoxlu əmək sərf etmişdi. Əməliyyatların bütün mərhələlərində mətbuat və televiziya ilə sıx əlaqələrin saxlanmasına böyük diqqət ayrılırdı. Belə ki, artıq 1988-ci ilin fevralından başlayaraq, Panamada amerikalı hərbi qulluqçuların və onların ailələrinin yerli hakimiyyət tərəfindən diskriminasiyası haqqında Amerika mətbuatında müntəzəm olaraq məqalələr çap olunurdu. Xüsusi olaraq seçilmiş və göstərişlər almış jurnalistlər və fotoreportyor qrupları döyüşə başlamazdan öncə Panamanın uyğun obyektlərinə göndərilirdilər. Döyüşlər gedən zonalara arzu edilməyən jurnalistlərin girişini məhdudlaşdırmaq üçün hər şey edilirdi. Beləliklə, ABŞ qüvvələrinin hərbi

fəaliyyətini vahid və yaxşı idarə edə biləcək informasiya-psixoloji təminat sistemi yaradılmışdı. Panamanın hərbi və siyasi sistemini yanıltmaq üçün tədbirlər həyata keçirilir, Panamanın milli müdafiə qüvvələri və mülki əhali arasında xüsusi təbliğat aparılırdı. Panamada toplanan təcrübələrdən daha sonra Fars körfəzində və Yuqoslaviyaya qarşı keçirilən hərbi əməliyyatlarda istifadə olunurdu.

SSRİ və sonrakı postsovet ölkələrinə qarşı ABŞ-ın informasiya-psixoloji müharibəsi onilliklərlə davam etmiş və demək olar ki, 90-cı illərdəki proseslərdə öz bəhrəsini vermişdir. Bu gün də bu proses davam edir, Rusiyada və postsovet ölkələrində "Azadlıq" və "Amerikanın Səsi" radiosu fəaliyyət göstərir. Səfirlik və konsulluqlar yanında xüsusi informasiya-resurs mərkəzləri vardır. Bu mərkəzlərdən hər biri Moskvadan başlayaraq Vladivostoka qədər Rusiyanın ərazisini öz nəzarətində saxlayır. Bundan əlavə, dezinformasiya sahəsində çoxsaylı fondlar, mətbuat orqanlarının filialları fəaliyyət göstərir.

Bir çox hallarda Rusiya Amerikanın informasiya üzrə təsir obyekti idi. Belə ki, Rusiya Çeçenistan müharibəsinin (1994-cü il) gedişatında, həmçinin Baltikyanı ölkələrlə münasibətlərdə, Ukrayna (2004 və 2014-cü ildə), Gürcüstan və hətta MDB ölkələrində informasiya sahəsində məğlubiyyətə düçar olurdu.

ABŞ-ın İraqa qarşı keçirtdiyi birinci əməliyyat (1991-1992-ci illər) informasiya mühitində pozitiv ictimai rəy uğrunda mübarizənin gözəl bir nümunəsidir. Məsələn, döyüşlərin başlanmasından 5 ay öncə start verilən tədbirlər nəticəsində Fars körfəzində müharibəni təqdir edən amerikalıların sayı 10%-dən 80%-ə qədər artmışdı. Döyüş əməliyyatlarından informasiyaların ötürülməsi də güclü nəzarətdə idi. Yalnız xüsusi seçilmiş hərbçilər müsahibə verirdilər. Həlak olmuşlar və yaralılar haqqında informasiyaların minimum səviyyədə olmasına xüsusi diqqət

yetirilirdi. Döyüş əməliyyatları haqqında informasiyanın yayılmasına sərt senzura tətbiq edilmişdi. Müharibənin əleyhdarlarına verilən efir vaxtı məhdudlaşdırılırdı.

Əməliyyatın başlama tarixini gizlətmək, Rusiya Federasiyasının rəhbərliyi və BMT Təhlükəsizlik şurası üçün müharibəni qəfildən təşkil etmək məqsədi ilə dövlət və hərbi səviyyədə dezinformasiyanın effektivliyini qeyd etmək lazımdır. Fars körfəzində müharibə ərəfəsində informasiya-psixoloji mübarizəyə dair tədqiqatlar göstərirdi ki, onun vasitələrindən bacarıqla istifadə edilməsi ABŞ qoşunlarının döyüş imkanlarını həyata keçirməyə və rəqibin döyüş imkanlarını əhəmiyyətli dərəcədə zəiflətməyə imkan verir.

İraqla ikinci müharibədə və Səddam Hüseynin devrilməsində informasiya təminatı ABŞ üçün daha az uğurlu olmuşdu. Amerikalıların düşərgəsində böyük itkilərin olmasını, İraq əhalisi ilə işğalçılar arasında artan mənfi münasibətləri gizlətmək mümkün olmadı. Ən əsası da İraq ərazisinə müdaxilənin əsas bəhanəsinin yalan çıxması oldu. Belə ki, İraqda kütləvi qırğın silahı tapılmadı, bu da o anlama gəlir ki, həmin silahların başqa ölkələrə, eləcə də ABŞ-a qarşı tətbiqi mümkün deyildi. Bundan sonra heç bir dezinformasiya İraqın işğalına bəraət qazandıra bilməzdi ki, bu da ABŞ prezidentinin mövqeyini əhəmiyyətli dərəcədə zəiflətdi.

ABŞ-ın başçılığı ilə NATO-nun 1999-cu ildə (mart-iyun aylarında) Yuqoslaviyaya qarşı həyata keçirtdiyi təcavüzdə informasiya təminatı kifayət qədər uğurla tətbiq olunurdu. Hərbi əməliyyatlar güclü təbliğatla həyata keçirilirdi. Bu təbliğatda əsas istiqamət Yuqoslaviya İttifaq Respublikasının rəhbərliyinin siyasi kursunu etibardan, hörmətdən salmaq, qərb ölkələrinin əhalisi arasında "düşmən obrazını" formalaşdırmaq və təcavüzə mənəvi dəstək idi. Bütün informasiya təminatı yalnız bir mənbədən – NATO-nun Brüsseldəki mətbuat xidmətindən həyata keçirilirdi. Başqa informasiyanın olmaması səbəbindən yüzlərlə akkreditə olunmuş jurnalist birtərəfli

olaraq NATO-nun məlumatlarını yaymağa məcbur idilər. Amerika aviasiya dəstələri Yuqoslaviyanın informasiya yayımı vasitələrini məhv edirdi. Oradakı radio və televiziya ötürücü aparatlarının 40%-dən çoxu sıradan çıxarılmış və ya məhv edilmişdi. Nəticədə amerikalılar özləri üçün Yuqoslaviyadakı müharibəyə dair uyğun informasiya-psixoloji mühitini yaratmağa nail olmuşdular. Hərbi əməliyyatlar bitdikdən sonra güclü informasiya təsiri və Qərbin iqtisadi təzyiqi ilə ABŞ öz istəyinə nail oldu: Yuqoslaviyada hakimiyyətə qərbyönümlü rəhbərlik gəldi, Miloşeviç isə hərbi cinayətkar kimi Haaqa tribunalına verildi. Beləliklə, "ölümcül olmayan" informasiya mübarizə vasitələri Miloşeviçə 1999-cu ildə 30 min hərbi təyyarənin vura bilmədiyi həlledici zərbəni vurdu.

"Ərəb baharı" hadisələrində də informasiya müharibələrinin rolu olmuşdur. Qeyd etmək lazımdır ki, hakimiyyətə qarşı yönəldilmiş vətəndaşların kütləvi etirazları iqtisadi artım yüksək olan, yoxsulluq səviyyəsi 10%-dən çox olmayan, rüşvətxorluğun nisbətən aşağı olduğu ölkələrdə baş verirdi. Bu ölkələrdə "inqilab" termini ənənəvi hal deyildi, dövlət əleyhinə etiraz üçün obyektiv səbəblər yox idi. Ancaq vəziyyətin destabilizasiyası praktiki olaraq dərhal baş verir və mövcud olan hökumətlərin devrilməsinə gətirib çıxarırdı. Bu halda etiraz edən camaatın idarə edilməsi üçün prinsipial olaraq yeni mexanizmlər tətbiq edilirdi. "Ərəb baharı" hadisələrində İnternetin və müxtəlif informasiya-rabitə texnologiyaların geniş istifadəsi vacib məqam oldu. Bu texnologiyalar etiraz edən kütlə üçün mühərrik və başlanğıc rolunu yerinə yetirirdilər.

Dönüş nöqtəsi kimi 2009-cu ildə Tunisdə cərəyan edən hadisələri hesab etmək olar. Kütləvi narazılıqların baş verməsindən sonra prezident Ben Əli sonra ölkəni tərk etmiş, keçid hökuməti qurulmuşdu. Burada silahlı qüvvələr cəlb edilməmiş, siyasi müzakirələr və seçkilər isə kənar qüvvələrin ssenarisi üzrə baş verirdi.

Analoji xətlə Misirdə, Liviyada və Suriyada da həmin tipli hadisələr, narazılıqlar inkişaf edirdi. Hər yerdə inqilabi-etiraz hadisələrinin birinci mərhələsində internet şəbəkələrindən fəal istifadə edən təhsilli gənclər başlıca rol oynayırdılar.

4.1.4. Terrorizmlə mübarizə

Hadisələrin inkişafına güclü təsir göstərə bilən informasiya vasitələri terrorizmlə mübarizədə mühüm yer tutur.

İnformasiya texnologiyalarının effektliliyinin artması ilə ayrı-ayrı şəxslərin və bir qrup insanların zərər vurma potensialı da çoxalır. Dünya Ticarət Mərkəzindəki partlayışdan (11 sentyabr 2001-ci il) sonra ABŞ bu terror aktının əsas təşkilatçısı olan Rəmzi Yusifin ələ keçirilməsi üçün bir sıra tədbirlər görmüşdü. Həmin terrorçu haqqında məlumatlar hər yerdə (qəzetdə, jurnalda, internetdə, hətta kibrit qutularında) yerləşdirilmişdi. Nəticədə məhz kibrit qutusu üzərindəki informasiyanı oxuyan şəxs Yusifi tutmaqda köməkçi olmuş və mükafatı almışdı (şəkil 4.1). Bu terror aktı bəşəriyyət tarixində misli görünməmiş, terrorçuluğa qarşı ən genişmiqyaslı və bahalı əməliyyatların başlanğıcını qoydu.

Şəkil 4.1. Kibrit qutusunun üzərindəki Rəmzinin şəkli

İnformasiya-psixoloji təsirin yüksək effektli vasitələrinin və üsullarının meydana çıxması təcavüz və müharibələr haqqında köhnə təsəvvürlərə yeni prizmadan baxılmasına gətirib çıxardı. XX əsrin sonlarında KİV və informasiya-kompüter sistemləri artıq müasir müharibənin əsas təsir vasitəsi hesab olunurdu. Keçən əsrin son onilliyi ərzində ABŞ-da informatikaya və informasiya müharibələrinə hazırlıq xərclərinin ümumi hissəsi üç dəfəyə qədər artırılmış və hərbi büdcənin 20%-nə çatmışdı. Mütəxəssislər hesab edirlər ki, informasiya texnikasının və rabitə texnologiyalarının inkişafı müddətində "qaynar müharibələr" (hərbi əməliyyatlı müharibələr) informasiya silahı üstünlük təşkil edən "soyuq müharibələr" tərəfindən sıxışdırılıb çıxarılacaqdır. Müharibədə uğurlu nəticə əldə etmək üçün XX əsrin birinci yarısında aviasiya və zirehli tank texnikası gərəkli idisə, XXI əsrdə informasiya baxımından üstünlük əldə edilməsi vacib olacaqdır.

ABŞ-ın keçmiş prezidenti R.Niksonun fikrinə görə informasiya vasitələrinə, informasiya təminatına 1 dollar yatırım etmək yeni növ silahların yaradılmasına 10 dollar yatırım etməkdən daha sərfəlidir. Silah tətbiq edilməsi ehtimalı çox deyil, lakin informasiya təbliğatı fasiləsiz olaraq gün ərzində 24 saat işləyir.

4.2. İnformasiya müharibəsinin xüsusiyyətləri

İnformasiyaya ətrafda baş verən və dünyada cərəyan edən proseslər haqqında məlumat kimi baxmaq olar. İnformasiya hər bir kəsə cəmiyyətdə mövcud olmaq üçün şərait və vasitədir. Bu səbəbdən də yaşayış mühiti qida və həyat fəaliyyətinin digər elementləri kimi mühafizə olunmalıdır.

İqtisadi, elmi-texniki, mədəni, siyasi, hərbi və digər informasiyaların operativ mübadiləsi imkanlarının sürətli artması cəmiyyətin böyük nailiyyətidir.

Üçüncü minillikdə bəşəriyyətin sənaye sivilizasiyasından informasiya sivilizasiyasına keçidi fonunda informasiya tarixi inkişafın əsas amillərindən birinə çevrildi. O, bütün ictimai və dövlət institutlarının uğurlu fəaliyyəti, hər bir insanın ayrı-ayrılıqda adekvat davranışı üçün əsas məna kəsb edir. Cəmiyyətin ətraf mühit ilə daimi informasiya əlaqəsi olmadan, insanların normal həyat fəaliyyəti prinsip etibarilə qeyri-mümkündür. Sosial mühitlə informasiya əlaqələrinin dayandırılması bir qayda olaraq, insanın şəxsi deqradasiyasına aparır, müxtəlif geriləmələrə, yayınmalara səbəb olur, hətta psixi sarsıntılara qədər gətirib çıxarır.

İstənilən sahədə inkişaf müəyyən həddə qədər pozitivdir və faydalı ola bilər, sonrakı mərhələlərdə onun zərər vermə ehtimalı vardır. Belə ki, informasiya texnologiyalarının inkişafı eyni zamanda kütləvi dezinformasiya imkanlarının genişlənməsinə – yalan xəbərlərin yayılması, faktların dəyişdirilməsi, gizlədilməsi, dəlillərin saxtalaşdırılması ilə çoxlu sayda insanın aldadılmasına və cəmiyyətin inkişafında ciddi problemlərin yaranmasna səbəb ola bilər. Nəticədə müasir cəmiyyətdə çox şeydən xəbəri olan, məlumatlı insanlarla yanaşı, dezinformasiya edilmiş, yalan məlumatla aldadılmış insanlar da meydana çıxır ki, onlar özləri də aldatmağa daha çox meylli olurlar.

İnformasiya müharibəsi – yeni tip müharibədir, onun əsas obyekti yalnız informasiya sistemləri deyil, insanların şüuru, onların davranışı və sağlamlığıdır.

İnformasiya müharibəsində dövlətlərarası ziddiyyətlərin və münaqişələrin həll olunması üçün dövlətlərin informasiya sahəsinə və cəmiyyətin şüuruna təsir üsullarından və vasitələrindən istifadə olunur. İnformasiya müharibələri ölkənin daxilində də ola bilər: məsələn, siyasi və iqtisadi rəqiblərin toqquşması zamanı, hakimiyyətin ələ keçirilməsi üzrə mübarizənin kəskinləşməsi vəziyyətlərində, seçki kampaniyalarının keçirilməsi vaxtı, məhkəmə proseslərində və s.

"İnformasiya müharibəsi" termini çoxdan məlumdur, lakin İraqla müharibənin tamamlanmasından sonra Amerika mütəxəssisləri tərəfindən geniş istifadə edilməyə başladı. Həmin ərəfədə informasiya silahı öz yüksək effektivliyini göstərmişdi.

1992-ci ildə Pentaqon "İnformasiya müharibəsi" direktivini çap etdi. Burada belə növ müharibələrə hazırlıq üzrə əsas görülməli işlər, metod və vasitələr öz əksini tapmışdır.

İnformasiya müharibəsinin əsas məqsəd və vəzifələri aşağıdakılardır:

- mübarizə aparan tərəfin idarəetmə sistemlərinin çökdürülməsi və məhv edilməsi;
- döyüş əməliyyatlarının, siyasətin, iqtisadiyyatın təsirlərinin informasiya təminatının əldə edilməsi;
- rəqibin elektron sistemlərinin çökdürülməsi;
- şəxsi heyətə və əhaliyə psixoloji təsir;
- rəqib informasiya sistemlərinə haker nüfuzetməsi.

İnformasiya müharibələrinin tərkib elementi informasiya əməliyyatlarıdır. Obyektlərin xarakterindən və təsir vasitələrindən asılı olaraq, informasiya əməliyyatları 2 yerə ayrılır: *informasiya-texniki və informasiya-psixoloji.*

Hücum xarakterli informasiya əməliyyatı informasiya həmlələri ilə təsir edir. Buraya aşağıda qeyd olunan tədbirlər daxildir:

- strateji maskalanma;
- rəqibin dezinformasiyalaşdırılması;
- psixoloji əməliyyatlar;
- radioelektron mübarizə;
- informasiya infrastrukturu obyektlərinin fiziki məhv edilməsi;
- rəqibin kompüter şəbəkələrinə hücumlar.

İnsanlara və cəmiyyətə qarşı məkrli fikirlərlə və hətta cinayət məqsədi ilə həyata keçirilən hücum xarakterli informasiya əməliyyatını informasiya təcavüzü adlandırmaq olar.

Müdafiə xarakterli informasiya əməliyyatı şəxsi informasiya resurslarının təhlükəsizliyinin təmin olunması üzrə tədbirləri əhatə edir. Bura aşağıdakılar aiddir:

- operativ və strateji maskalanma;
- sirlərin saxlanılması;
- əks-kəşfiyyat;
- informasiya infrastrukturu obyektlərinin fiziki mühafizəsi;
- səs batırma, rəqibin KİV-nin mühasirəyə alınması;
- əks-təbliğat;
- psixoterapiya;
- əks-dezinformasiya;
- radioelektron mübarizə.

İnformasiya müharibələrində müəyyən vasitələrdən və silahlardan istifadə olunur. İnformasiya silahı dedikdə, əhalinin davranışına və şüuruna, personala, hərbçilərə, dövlətin informasiya-texniki infrastrukturuna və cəmiyyətə dağıdıcı təsir göstərə bilən informasiya texnologiyalarının məcmusu başa düşülür.

İnsana təsir edən informasiya silahını mütəxəssislər bilavasitə iki növə bölürlər:

- informasiya-psixoloji silah hər şeydən əvvəl insanın şüuruna yönəldilir və oradan davranışa, baxışlara, cəmiyyətdə baş verən münasibətə təsir edir. Belə silah kimi bütün kütləvi informasiya vasitələrindən, internetdən, söhbətlərdən, hipnozdan və s. istifadə oluna bilər.

- enerji-informasiya silahı insanın fiziologiyasına və onun psixofiziologiyasına təsir edir. İnsan təsir faktını hiss etmir, lakin onun növündən asılı olaraq, ya özündə gümrahlıq,

əminlik və ya məyusluq, həyəcan, qorxu hiss etməyə başlayır və ya öz hərəkətlərinə nəzarət etmək qabiliyyətini itirir. Təbiətdə belə psixofiziki təsiri Günəş göstərə bilir, məsələn, beyinin bioelektrik fəallığına və insanın ümumi vəziyyətinə təsir edir.

Enerji-informasiya təsirinin mənbələri kimi radiolokasiya sistemləri, kosmik aparatlar, aşağı və yuxarı tezlikli generatorlar, biolokasiya qurğuları, kimyəvi və bioloji vasitələr və başqa qurğular tətbiq edilə bilər. Enerji-informasiya silahının köməyi ilə insanların davranışını dəyişdirmək olar, məsələn, nümayişlərin, iğtişaşların alovlanma dərəcəsini artırmaq və ya azaltmaq, bununla da cari sosial proseslərə təsir etmək mümkündür. Rəqibin və ya terrorçuların şəxsi heyətinin psixofiziki vəziyyətini pisləşdirərək onların döyüş bacarığını aşağı salmaq, hətta təslim olmağa belə razı salmaq olar. Belə silahın tətbiq edilməsinin əsas nəticəsi izahedilməz qorxudur. Qorxu isə insanı köklü şəkildə dəyişdirmək iqtidarındadır.

Qorxu haqqında qədim ibrətli hekayə mövcuddur. Səyyah taunla rastlaşıb ondan "Sən hara gedirsən?" deyə soruşur, taun isə «Bağdada gedirəm. Mənə orada beş min insan öldürmək lazımdır" deyə cavab verir. Bir müddətdən sonra həmin insan taunla yenidən qarşılaşır. "Bəs sən demişdin axı beş min adam öldürəcəksən, amma əlli min öldürdün" deyərək insan xəstəliyi qınayır. "Yox" deyib taun etiraz edir, "mən yalnız beş min nəfəri məhv etdim, qalanları qorxudan öldülər".

İnformasiya müharibələrinin və informasiya silahının tətbiq edilməsinin məqsədi rəqibin üzərində üstünlüyün əldə edilməsi və həm konkret mübarizədə və ya müəyyən əməliyyatda, həm də xarici və daxili siyasətdə, iqtisadiyyatda onu məğlub etməkdir.

İnformasiya silahının tətbiq edilməsinin məqsədləri:

- dövləti beynəlxalq nüfuzdan salmaq, başqa ölkələrlə əməkdaşlıqlarına təsir göstərmək;

- ölkə daxilində ictimai şüurla manipulyasiya etmə və inamsızlıq atmosferinin yaradılması, milli mirasa neqativ münasibətlər;
- ölkə daxilində siyasi gərginliyə və xaosun provokasiya edilməsinə, etnik və dini toqquşmalara, tətillərə, kütləvi qarışıqlıqlara və başqa etiraz aksiyalarına səbəb olmaq;
- ölkənin tarixi, dövlət orqanlarının işi haqqında əhaliyə yalan məlumatların verilməsi, onların nüfuzdan salınması, bütün idarəetmə sisteminin etibardan salınması;
- qoşunların, silahlanmanın və hərbi texnikanın idarəetmə sisteminin pozulması;
- dövlətin iqtisadi, sosial və digər fəaliyyət sahələrində mühüm maraqlarına ciddi zərərin vurulması.

Adi silahla müqayisədə informasiya mübarizə vasitələrinin üstünlükləri:

- nisbətən az xərclər;
- gizli tətbiq imkanı;
- təsirin ənənəvi sərhədlərinin olmaması;
- şəxsi məğlubiyyət riskinin az olması;
- ekoloji zərərin yoxluğu;
- maddi-iqtisadi infrastrukturun saxlanılması imkanı.

İnformasiya silahını tez-tez "ağıllı", daha humanist və "ölümcül olmayan" adlandırırlar. Bu, yanlış fikirdir. Bu silah adi silahdan fərqli olaraq, insanlar üçün daha təhlükəlidir. O, insanda ən çətin bərpa olunana – onun psixikasına qarşı yönəlmişdir. Buna görə də informasiya silahı insanların iç dünyasını zədələyərək, güllə və ya qəlpə yarasından daha dərin yaralayır.

İnsana uzunmüddətli, məqsədyönlü yalan məlumat verməklə, narkomaniyaya, psixi pozuntulara, intiharlara və cinayətkar davranışlara gətirib çıxarmaq mümkündür.

İstənilən müharibədən sonra sağlam uşaqlar doğulur, cəmiyyətin normal fəaliyyəti kifayət qədər tez bərpa olunur. İnformasiya silahı ilə zərər çəkmişlər psixi cəhətdən sağlam gələcək nəsil formalaşdırmaq bacarığına malik olmurlar. Sosial mirasın qanunlarına görə onlar yalnız oxşarlarını böyüdə bilərlər. Əsəbi, kompleksli, manqurtlaşdırılmış şəxsin yanında bir qayda olaraq, nevrotik və ya zombi böyüyür. Nəticədə informasiya müharibələrindən sonra uduzmuş dövlət bərpa oluna bilmir. Amma bu müharibələrin sonu olmur. İnformasiya silahı – yeni, qorxunc və hələ ki, qadağan edilməmiş kütləvi qırğın silahıdır. İnformasiya silahı öldürücü və qeyri-humanistdir.

İnformasiya amillərinin insan şüuruna təsirinin gücü və genişmiqyaslılığı informasiya-psixoloji təminatı qlobal problem səviyyəsinə qaldırmağa vadar edir. Bu səbəbdən də özünü informasiya təcavüzündən qorumaq, əhalinin informasiya təhlükəsizliyini təmin etmək qabiliyyəti hər bir dövlətin əsas məqsədinə çevrilir.

Fəsil üzrə yoxlama sualları

Qeyd olunan fikrin səhv və ya düz olduğunu müəyyənləşdirin.

	Düz	Səhv
1. 2 növ informasiya mübarizə forması vardır: informasiya-texniki və informasiya-psixoloji.	☐	☐
2. Adi silahla müqayisədə informasiya mübarizə vasitələri daha çox xərc tələb edir.	☐	☐
3.İnformasiya təsir üsulları XX əsrdən tətbiq olunmağa başlayıb.	☐	☐

Test suallarını cavablandırın:

1. Adi silahla müqayisədə informasiya mübarizə vasitələrinin üstünlükləri nədən ibarətdir?

a) nisbətən az xərclər;
b) gizli tətbiq üçün gözəl imkan;
c) təsirin ənənəvi sərhədlərinin olmaması;
e) təsiri daim qalır;

2. Radiomaneələrlə radioəlaqənin yatırılması vasitələri ilk dəfə hansı müharibədə tətbiq edilməyə başlanmışdır?

a) 1939-1945-ci illər - II Dünya Müharibəsi
b) 1967-ci il - ərəb-İsrail müharibəsi
c) 1904-cü il - rus-yapon müharibəsi
d) 1991-1992-ci illər - ABŞ-İraq müharibəsi

3. İnformasiya müharibələri neçənci əsrdən sonra daha çox vüsət almağa başlamışdır?

a) XX
b) XIX
c) XVIII
d) XVII

Açıq sualların cavablarını əhatəli qeyd edin:

1.İnformasiya müharibəsinin xüsusiyyətləri hansılardır?

_____
_____
_____
_____
_____

2. Terrorla mübarizənin hansı üsulları mövcuddur?

_____
_____
_____
_____
_____

5. İnformasiya sistemləri və onların təhlükəsizliyi

Bütün dünyada aviasiya təhlükəsizliyi və uçuşların təhlükəsizliyi sistemlərinin etibarlılıq səviyyəsinin artırılmasına, onların təkmilləşdirilməsinə baxmayaraq, bu sahə hələ də terrorçu qrupların, cinayətkarların diqqət mərkəzindədir.

Aviasiya təhlükəsizliyi sisteminə fərqli yanaşmaların dönüş nöqtəsi olan 11 sentyabr hadisələrindən sonra hava nəqliyyatına müxtəlif formalı hücumlar həyata keçirilməyə başladı. 2001-ci il – "partlayıcı yerləşdirilmiş çəkmə"dən istifadə etməklə hücum, 2006-cı il – maye partlayıcı maddələrdən istifadə hədələri, 2009-cu il – "alt paltarı bombası", 2010-cu il – printer kartricində yerləşdirilmiş əldə düzəldilən bombanın hava gəmisinin göyərtəsində partladılması cəhdi, 2011-ildən başlayaraq hava limanlarında (Moskva, Burqas, Brüssel, İstanbul və s.) intiharçı terrorçuların çantalarındakı partlayıcıların partladılması kimi terror dalğaları bu gün də davam etməkdədir.

Bu onu sübut edir ki, beynəlxalq mülki aviasiya haqqında konvensiyaya edilmiş 17 nömrəli əlavəyə əsasən həyata keçirilən yeni beynəlxalq standartların və tövsiyə olunan təcrübələrin, yeni təhlükəsizlik tədbirlərinin dövlətlər tərəfindən tətbiqinə baxmayaraq, öz məqsədlərinə nail olmaq üçün terrorçular hava nəqliyyatında yeni hücum yollarını axtarmağa davam edirlər.

Mülki aviasiyanın fəaliyyətinə yönəlmiş hədələr getdikcə daha çoxşaxəli, mürəkkəb, genişmiqyaslı olur. Hal-hazırda cəmiyyətin nəzər yetirməli olduğu sahə kiber-hücumların yarada biləcəyi hədələrdir.

Kiber-hücumlar aviasiya təhlükəsizliyinə ünvanlanmış yeni təhdid deyildir. Kompüter əsaslı sistemlərdən, biometrik vasitələrdən istifadə mülki aviasiyanın bütün sahələrinə aid edilə bilər: aeronaviqasiya sistemləri, uçan aparatların idarə edilməsi, hava gəmisinin göyərtəsindəki rabitə sistemləri,

sərnişinlərin və yüklərin qeydiyyatı sistemləri, təhlükəsizlik sistemləri, reyslər, əməkdaşlar, sərnişinlər barədə konfidensial informasiyanı özündə toplayan sistemlər və s. artıq uzun müddətdir ki, istifadə edilir. Analoji olaraq o da söylənilə bilər ki, kompüter sistemlərinə hakerlər tərəfindən kompüter virusları və digər ziyankar proqramlarla hücumlar artıq qeyri-adi hal deyil, sistemli xarakter daşıyır.

Mülki aviasiya sahəsinin davam edən inkişafı, daşınan aviasərnişinlərin sayının sürətlə artması, daha yeni, böyük və müasir hava limanlarının açılması, həmçinin yeni və daha yüksək göstəricilərə malik olan hava gəmilərinin istifadəyə verilməsi səbəbindən informasiya texnologiyalarından, daha təkmilləşmiş kompüter sistemlərindən, şəbəkələrindən aviasiya sahəsinin bütün istiqamətlərində geniş istifadə olunması labüdlüyünün göstəricisinə çevrilmişdir. Bu hal həmçinin daha yüksək nəticənin əldə edilməsinə, əmək resurslarının istifadə olunmasının ixtisarına təkan verir. Bir çox hava limanları sərnişinlərinin rahatlığı üçün daha müasir texnologiyaların, məsələn, elektron biletlərin sifarişi və alışı, gəlmə zamanı qeydiyyat, immiqrasiya qeydiyyatı üçün telefonların, kiçik kompüter vasitələrinin, sərnişinlərin tanınması üçün biometrik sistemlərin tətbiqinə nail olmuşdur.

Bu gün bir çox dövlətlərin mülki aviasiya məkanında müasir kompüter və informasiya sistemlərindən asılılıq mövcuddur və bu tip innovativ yeniliklərdən asılılıq getdikcə artmaqda davam edir.

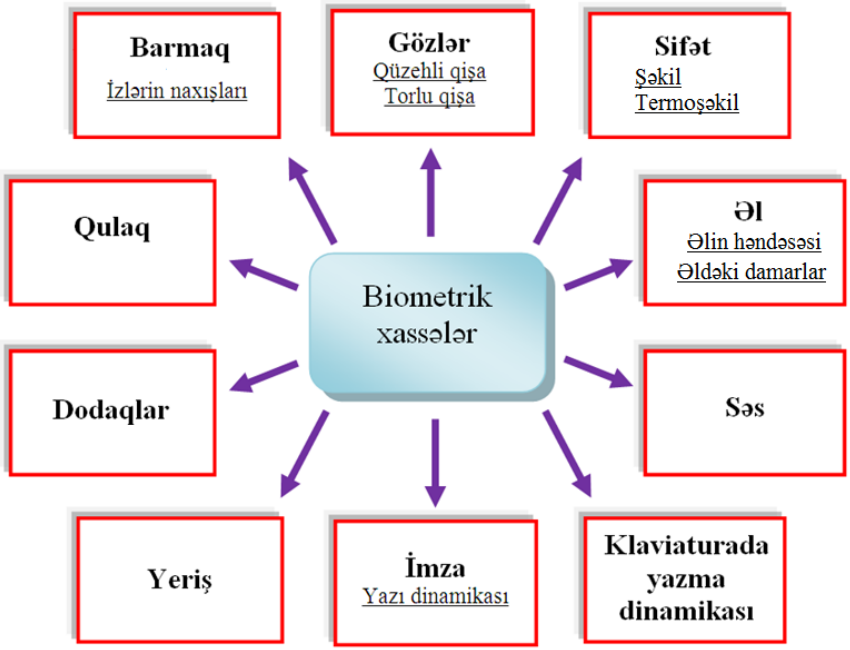
Lakin bu informasiya texnologiyaları sistemlərinin birinə ziyankar hücumlar nəinki aviasiyanın fəaliyyətini pozar, hətta günahsız sərnişinlərin, yerüstü personalın və heyət üzvlərinin, həmçinin digər insanların həyatına hədə yarada bilər.

5.1. Biometrik informasiya sistemləri

5.1.1. Biometriya anlayışı

Biometriya – şəxsin identifikasiyası və autentifikasiyası üçün insanın fiziki xarakteristikalarının və davranış əlamətlərinin ölçülməsi üsullarını öyrənən elm sahəsidir.

İnsanın biometrik xassələrinin əsas mənbələri – barmaq izləri, gözün qüzehli və torlu qişası, səs, üz, kompüter klaviaturasında işləmə tərzi, imza, yeriş və s.-dir (şəkil 5.1).



Şəkil 5.1. İnsanın biometrik xassələrinin əsas mənbələri

Hal-hazırda ən inkişaf etmiş biometrik sistem – barmaq izləri, gözün qüzehli qişası və sifətin iki ölçülü şəklidir. Barmaq izi üzrə identifikasiya tətbiqinə və maliyyə baxımından əlyetənliyinə görə bütün digər sistemləri üstələyir.

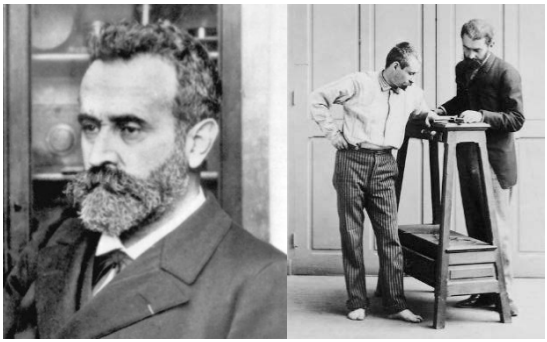
Biometrik xassələr əsasında identifikasiyanın və autentifikasiyanın üsulları və texniki vasitələri biometrik texnologiyalar adlanır. Autentifikasiyanın məqsədi əldə olunan biometrik məlumatın, bu məlumatların aidiyyəti olan əsli ilə uyğunluğunun müqayisə edilməsindən ibarətdir. Autentifikasiya (və ya 1-ə 1 müqayisə) subyektin əldə olunan məlumatlarla eyni olması və ya əldə olunan məlumatların subyektə aid olduğunun yoxlanması deməkdir.

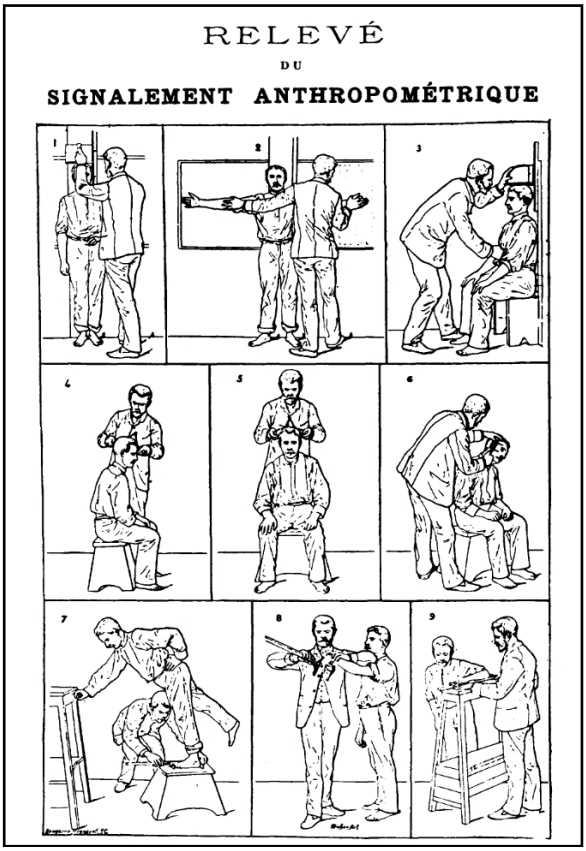
İdentifikasiya (və ya N-ə 1 müqayisə) əldə olunan biometrik məlumatın, mövcud olan subyektlərdən hansına daha çox uyğun gələninin müəyyənləşdirilməsi deməkdir. Yəni, daha sadə dillə desək, əldə edilən biometrik məlumatların mövcud subyektlərə aid olan analoji məlumatlarla müqayisəsinin davamlı olaraq təkrarlanmasıdır.

5.1.2. Biometriyanın tətbiqi tarixi

Tanınmanın biometrik sistemləri tarix boyu istifadə edilmişdir. Biz tanışları – onların sifət quruluşuna, səsinə və ya yerişinə görə tanıyırıq.

Biometriyanın kütləvi tətbiqini Alfons Bertilyonla əlaqələndirmək olar. O, XIX əsrin 90-cı illərində Paris polisinin kartotekasında işləyərkən qərara gəlir ki, 11 ölçü vahidi üzrə insanların oxşarlığı, eyniliyi ehtimalı çox aşağıdır və hər bir cinayətkarı ölçdükdən sonra alınan nəticələri şəxsi kitabçaya dəqiqliklə yığdıqda səhvsiz identifikasiya mümkün olacaqdır (şəkil 5.2). Bu ölçülər aşağıdakılar idi:





Şəkil 5.2. Alfons Bertilyon və onun ölçmələr aparması

1. İnsanın boyu (başın ən yuxarı hissəsindən yerə kimi)
2. Əllərin genişliyi (bir əlin ən uzun barmağının ucundan digər əlin ən uzun barmağının ucuna kimi)
3. Gövdə (başın yuxarı hissəsindən oturduğu stula kimi)
4. Başın uzunluğu (başın arxa nöqtəsindən qabağına kimi)
5. Başın eni (sol qulağın yuxarı hissəsindən sağ qulağın yuxarı hissəsinə kimi)
6. Sağ qulaq (qulağın yuxarı hissəsindən aşağı hissəsinə kimi)
7. Sol ayaq (ayağın arxa hissəsindən qabaq hissəsinə (ən uzun barmağa) kimi)
8. Sol orta barmaq (digər barmaqlara nisbətdə 90° əyilmiş sol orta barmağın ovuca birləşən hissəsindən ucuna kimi)
9. Sol qol (90° əyilmiş sol qolun ucundan dirsəyə kimi)
10. Sol kiçik barmaq (digər barmaqlara nisbətdə 90° əyilmiş sol kiçik barmağın ovuca birləşən hissəsindən ucuna kimi)
11. Sağ yanaq (burunun sağ dəliyindən sifətin yanına kimi)

Bir neçə genişmiqyaslı əməliyyatlardan sonra bu identifikasiya sistemi fransız polisi tərəfindən daha dəqiq öyrənilməyə başlanılmışdır.

Ölçmələrin cəmi üzrə identifikasiyanın əvəzinə XX əsrin əvvəllərindən daktiloskopiyadan (barmaq izləri üzrə insanın identifikasiyası) istifadə edilməyə başlandı. Barmaq izləri üzrə identifikasiya bir neçə dəqiqə çəkirdi. 10 ildən sonra bu sistem bütün Avropada tətbiq olunurdu.

Tarixi nümunələrdən görünür ki, biometrik texnologiyalar, xüsusən də daktiloskopiya, kriminalistikada çoxdan istifadə edilir, keçən əsrin axırlarından isə texnikanın inkişafı ilə insanların xarici görkəminə və davranış özəlliklərinə görə tanınması alqoritminin formalaşdırılması və bunun üçün avtomatlaşdırılmış sistemlərin tətbiqi mümkün oldu.

Biometriya hal-hazırda inkişaf dövrünü yaşayır. Bu inkişaf pasport-viza sənədlərində biometriyanın tətbiqi haqqında qabaqcıl dövlətlərin qərarları ilə bağlıdır ki, bununla da geniş maliyyə və material resursları bu sahəyə yönəlməyə başladı. Hal-hazırda cəmiyyətdə bu texnologiyalara böyük maraq vardır.

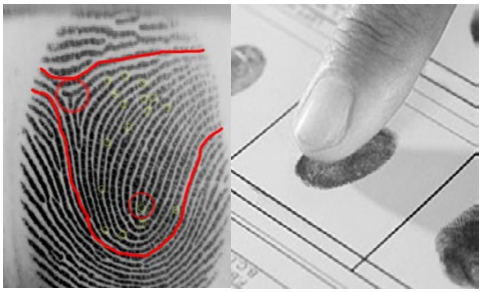
Aviasiyada biometrik sistemlərdən geniş istifadə olunur. Hər bir dövlət hava limanında şəxsiyyətin təsdiq edilməsinin etibarlılığının artırılması məqsədi ilə müxtəlif növ biometrik sistemlərdən istifadə edir. Aviasiyada tətbiqi üçün biometrik parametrlərin sistemli öyrənilməsinə 1998-ci ildən başlanılmışdır. İlk öncə uçuş sənədlərində istifadə üçün hansı biometrik parametrlərin qoyulan tələbləri ödədiyini müəyyənləşdirməyə çalışmışlar. Qiymətləndirmənin nəticəsində üzə görə identifikasiya aviasiyada daha yüksək reytinq əldə etmiş və əsas tanıma sistemi kimi istifadə olunur, barmaq izi və gözün qüzehli qişası ilə identifikasiya isə köməkçi identifikasiya kimi tətbiq olunur.

5.1.3. Tanıma sistemləri

Biometrik xassələrə uyğun olaraq, hər bir biometrik parametrin üstün və zəif cəhətləri var və seçim, adətən, tətbiqdən asılı olur. Aşağıda biometrik texnologiyaların qısa xülasəsi verilmişdir.

Barmaq izləri. Bu metodun əsası hər bir insanın bir və ya bir neçə barmağında papilyar naxışların fərdiliyi və təkrar olunmamasıdır (şəkil 5.3). 1877-ci ildə ingilis məmuru Uilyam Herşelin papilyar şəkillərin dəyişməzliyi fərziyyəsi əsasında ingilis antropoloqu Frensis Qalton 1895-ci ildə İngiltərədə cinayətkarların qeydiyyatı üsulu kimi daktiloskopiyanın tətbiqinə nail olmuşdur. 1902-ci il 18 apreldə isə Böyük Britaniyada cinayətkarın tanınması üçün daktiloskopiya ilk

dəfə tətbiq edilmişdir. Növbəti onilliklərdə bu metoddan bütün Avropa ölkələrində istifadə edilməyə başlanılmışdı.



Şəkil 5.3. Barmaq izləri ilə autentifikasiya

Adətən alqoritmlər barmaq izlərindəki özəl nöqtələri istifadə edirlər: xətlərin sonluğu, xətlərin şaxələnməsi, nöqtələri. Papilyar naxışların özəllikləri unikal şifrə çevrilir. Barmaq izlərinin şifrləri axtarış və müqayisə üçün istifadə edilən məlumat bazasında saxlanılır. Bazadan asılı olaraq, barmaq izi şəkillərinin şifrlərə çevrilməsi adətən 1 san-dən artıq vaxt çəkmir.

Üsulun üstün və mənfi cəhətləri.

Üsulun üstünlükləri:

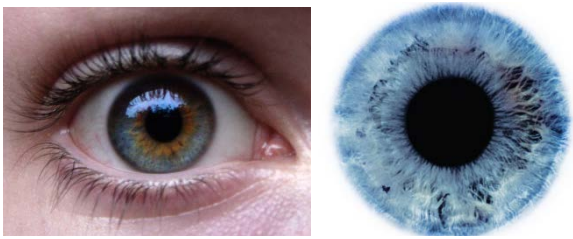
- yüksək dəqiqlik;
- ucuz qiymət;
- sadə texnologiya.

Mənfi cəhətləri:

- papilyar naxışların kəsiklər zamanı zədələnməsi;
- şəklin formasını dəyişmək imkanı;

Gözün qüzehli qişası. İnsan gözünün qüzehli qişası, barmaq izləri kimi, onun unikal biometrik xarakteristikasıdır. Qüzehli qişanın şəkli ana bətnindəki inkişafın 8-ci ayında formalaşmağa başlayır, uşaq 2 yaşında olarkən tamamilə dayanır, ömür boyu dəyişməz qalır (güclü zədələri və

patologiyaları çıxmaq şərti ilə) (şəkil 5.4). Qeyd edək ki, sağ və sol gözün qüzehli qişasının şəkli əhəmiyyətli dərəcədə fərqlənir. Bu ən dəqiq tanıma sistemlərindən biridir.



Şəkil 5.4. Gözün qüzehli qişası

Gözün qüzehli qişasına əsasən şəxsin identifikasiyası sistemi 2 hissəyə bölünür: şəkli götürən qurğu və məlumat bazasındakı şəkillərlə müqayisə aparan qurğu.

Gözün qüzehli qişasının identifikasiyası zamanı linza və eynəklər çıxarılmalıdır.

Gözün qüzehli qişasının identifikasiya sistemi kimi tətbiq edilməsi təklifi keçən əsrin 70-80-ci illərində verilmişdir.

Üsulun üstün və mənfi cəhətləri.

Üsulun üstünlükləri:

– identifikasiya zamanı toxunuşa ehtiyac yoxdur;

– identifikasiyanı 1 neçə sm-dən 1 m məsafədə aparmaq olar;

– zamanla gözün qüzehli qişası dəyişmir.;

– yüksək dəqiqlik.

Mənfi cəhətləri:

− sistemin qiymətinin bahalı olması.

Sifət. Sifətin həndəsəsinə görə müxtəlif tanıma üsulları mövcuddur. Onların hamısı insanın üz cizgilərinin və kəllə formasının fərdiliyinə əsaslanmışdır. Biometriyanın bu sahəsi hər kəs üçün cəlbedici olur, çünki biz hamımız bir-birimizi

sifətdən tanıyırıq. Bu sahə 2 istiqamətə bölünür: 2-D tanıma və 3-D tanıma. Onların hər birinin öz müsbət və mənfi cəhətləri vardır.

2-D aşkarlama biometriyanın ən statistik effektsiz üsullarından biridir, çoxdan mövcuddur və əsasən də kriminalistikada istifadə olunmuşdur.

Üsulun üstün və mənfi cəhətləri.

Üsulun üstünlükləri:

– identifikasiya zamanı toxunuşa ehtiyac yoxdur;
– bahalı qurğunun alınmasına ehtiyac yoxdur;
– müəyyən məsafədən istifadə edilə bilər.

Mənfi cəhətləri:

– aşağı statistik həqiqilik;
– işığa ehtiyac;
– sifətin neytral olmasına ehtiyac (müəyyən alqoritmlər sifətin mimikasının dəyişməsini nəzərə ala bilmir);
– kənar maneələrin alqoritmlər tərəfindən qəbul olunmaması (saqqal, eynək və s.).

Şəkil 5.5. Sifət 2-D şəkli

3-D tanıma üsulunun həyata keçirilməsi kifayət qədər mürəkkəb məsələdir. Buna baxmayaraq, hal-hazırda sifətin 3-D tanınması üzrə çoxlu sayda üsullarmövcuddur. 3-D şablonun alınmasında da bir kameradan istifadə edilir. Bazaya subyekti

daxil edərkən, subyekt başını çevirir və alqoritm şəkilləri birləşdirir və 3-D şablon alınır.

Üsulun üstün və mənfi cəhətləri.

Üsulun üstünlükləri:

– identifikasiya zamanı toxunuşa ehtiyac yoxdur;

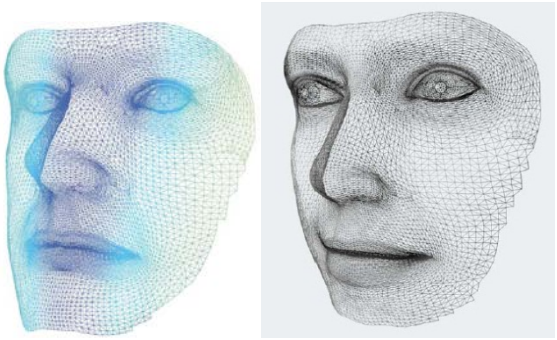
– kənar faktorlara az həssaslıq, yəni insanda (eynəyin, saqqalın olması, saç düzümünün dəyişdirilməsi) və ətrafda (işıqlılıq, başın çevrilməsi) dəyişikliklər;

– barmaq izləri üzrə identifikasiya üsulunda olduğu kimi yüksək dəqiqlik, etibarlılıq.

Mənfi cəhətləri:

− qurğunun baha olması;

− üsul hələ kifayət qədər yaxşı işlənməmişdir ki, bu da onun geniş tətbiqində problemlər yaradır.



Şəkil 5.6. Sifət 3-D şəkli

Əl venaları. Əldəki venaların yerləşməsinin analizi biometriyada yeni texnologiya olub, geniş tətbiqinə 2004-ci ildən başlanmışdır. İnfraqırmızı kamera ovucun arxa və qabaq hissəsindən şəkil çəkir. Qanda olan hemoqlobin infraqırmızı şüaları udduğuna görə əlin venalarının şəklini çəkmək mümkün olur. Xüsusi proqram vasitəsilə çəkilən şəkil emal olunur və venaların yerləşməsi sxem üzrə rəqəmsal formada yaddaşda saxlanılır. Tanıma prosesi yarım saniyə çəkir. Əldə olunan

məlumatın keyfiyyəti əl ilə qurğunun səthi arasındakı məsafədən asılı deyildir.

Şəkil 5.7. Əlin venaları

Texnologiyanı etibarlılığına görə gözün qüzehli qişası ilə müqayisə etmək olar. Əlin venaları illər keçdikcə də, dəyişməz qalır. Bu, kifayət qədər yeni texnologiya olduğu üçün dünya miqyasında çox tətbiq olunmur, lakin hal-hazırda bu üsula dünyada daha çox maraq yaranmağa başlayıb. Məsələ burasındadır ki, bu üsul gözün qüzehli qişası və ya sifət üzrə tanıma vasitələri kimi bahalı deyil, kifayət qədər də dəqiqdir.

Üsulun üstün və mənfi cəhətləri.

Üsulun üstünlükləri:

– identifikasiya zamanı toxunuşa ehtiyac olmaması;

– yüksək dəqiqlik;

– bahalı qurğuya ehtiyac yoxdur;

– xarakteristikaların gizliliyi – bu xarakteristikanı saxtalaşdırmaq çox çətindir.

Mənfi cəhətləri:

− günəş şüaları və halogen lampalarla işıqlanmağa icazə verilmir;

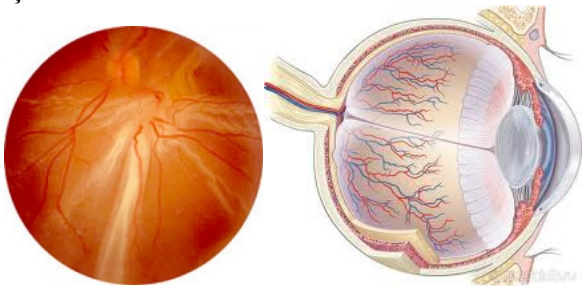
− üsul hələ kifayət qədər yaxşı işlənməmişdir.

Gözün torlu qişası. Gözün torlu qişasına əsaslanan tanıma üsulu XX əsrin 50-ci illərindən tətbiq olunmağa başlamışdır. Son vaxtlara kimi hesab olunurdu ki, bu üsul şəxsin biometrik identifikasiyası və autentifikasiyasının ən etibarlı üsuludur. O, özündə gözün qüzehli qişası və əlin venaları üzrə identifikasiyanın ən yaxşı cəhətlərini toplamışdır. Skaner gözün torlu qişasındakı kapilyarların şəklini çəkir. Torlu qişa zamanla dəyişməyən, hərəkətsiz struktura malikdir. Yalnız gözün katarakta xəstəliyi nəticəsində dəyişə bilər.

Gözün torlu qişasının şəklinin çəkilməsi zamanı aşağı intensivlikli infraqırmızı şüalar göz bəbəyindən keçərək, gözün arxa divarındakı qan damarlarına yönəlir. Alınmış siqnaldan yüzlərlə ilkin xarakterik nöqtə seçilir, onlar haqqında orta informasiya hesablanır və kodlanmış faylda saxlanılır.

Gözün torlu qişasını çəkən skanerlər xüsusi strateji obyektlərin girişinə nəzarət sistemlərində geniş istifadə olunur. Belə ki, bu üsulda səhvlər praktiki olaraq mümkün deyil.

Lakin bir çox müəssisələrdə bu üsulun tətbiqi artıq əlverişli deyil. Skaner mürəkkəb optik sistemdən ibarətdir, subyekt müəyyən vaxt (1 dəqiqəyə yaxın) tərpənməməli, bir nöqtəyə baxmalıdır. Belə ki, şəklin çəkilməsi zamanı işıq seli bir nöqtəyə yönəlməlidir və bu sistemlər torlu qişanın qeyri-düzgün yerləşməsinə həssasdır.



Şəkil 5.8. Gözün torlu qişası

Üsulun üstün və mənfi cəhətləri.

Üsulun üstünlükləri:

–yüksək etibarlılıq.

Mənfi cəhətləri:

–uzun müddət tələb olunması;

–sistemin bahalı olması.

İnsanın identifikasiya sistemlərinin hamısı ya ayrı-ayrı, yaxud da kompleks şəkildə işləyə bilər. Kompleks şəkildə fəaliyyət daristiqamətli və ya çoxməqsədli ola bilər. Mühafizə, nəzarət, qeydiyyat və xəbərdarlıq funksiyalarını həyata keçirən sistemlər kompleks hesab olunur.

Kompleks sistemlər aşağıda qeyd olunanları təmin edir:

- müəssisənin ərazisinə xüsusi kodlaşdırılmış kartlarla (buraxılış vəsiqələri) girişi;
- icazəsiz girişə cəhdlər zamanı (buraxılış vəsiqəsi olmadan keçmə, girişə icazəsi olmayan xüsusi yerlərə keçmə) keçidlərin qapanmasını;
- iş qrafikini pozan şəxslər üçün girişin qapanmasını (gecikmə, işdən vaxtından əvvəl çıxma və s.);
- operatorun göstərişi ilə müəyyən şəxsləri tutmaq üçün Nəzarət Buraxılış Məntəqəsində (NBM-də) buraxılış vəsiqələrinin kodlarının yoxlanılmasını;
- NBM-dən keçmə vaxtının qeyd olunması və bu məlumatların personal kompüterin verilənlər bazasında saxlanılmasını;
- alınan məlumatların emalı və müxtəlif sənədlərin hazırlanmasını (iş vaxtının tabeli, gündəlik raport, əmək intizamını pozanların siyahısı və s.). Bu, müəyyən vaxt ərzində əmək intizamını pozanlar haqqında operativ informasiyaya malik olmağa imkan verir;
- şifr üzrə verilənlər bazasının informasiyasının təshih (korrektə) edilməsini;

- sərbəst qrup üzrə əməkdaşların (bütövlükdə müəssisənin əməkdaşlarının, struktur bölmə əməkdaşlarının, ayrı-ayrı əməkdaşların) iş vaxtı cədvəllərinin çapını;
- qayda pozuntuları haqqında konkret məlumatlarla iş vaxtı qrafikini pozanların siyahılarının çapını;
- müəyyən seçilmiş vaxt üzrə müəssisəyə daxil olanların və oradan çıxan əməkdaşların, qonaqların təhlilini.

5.2. Kompüter sistemlərində və şəbəkələrində informasiya təhlükəsizliyi

Qlobal internet şəbəkəsinin və informasiya texnologiyalarının sürətli inkişafı insan fəaliyyətinin bütün sahələrinə təsir edən informasiya mühitinin formalaşmasına gətirib çıxardı. Yeni texnoloji imkanlar informasiyanın yayılmasını asanlaşdırır, istehsal proseslərinin effektliliyini artırır, işçi münasibətlərin genişlənməsinə şərait yaradır. Lakin kompüter vasitələrinin və informasiya texnologiyalarının intensiv inkişafına baxmayaraq, müasir informasiya sistemlərinin və kompüter şəbəkələrinin zəif nöqtələri azalmır. Bu səbəbdən informasiya təhlükəsizliyinin təmini problemləri həm mütəxəssislərin, həm çoxsaylı istifadəçilərin, həm də elektron ticarət sahəsində çalışan şirkətlərin diqqət mərkəzindədir.

İnformasiyanın mühafizəsinin müasir texnologiyalarına, standartlarına və proqram vasitələrinə yönəlmiş təhdidlər ilə tanış olmadan və onlarla peşəkarcasına mübarizə aparmadan kompüter sistemlərinin və şəbəkələrinin informasiya təhlükəsizliyini etibarlı mühafizə etmək mümkün deyil. Bu səbəbdən müasir təhlükələri və onlarla mübarizə üsullarını təhlil etmək lazımdır.

- 2006-cı ildə internetdən hücum nəticəsində ABŞ Federal Aviasiya Administrasiyasi (FAA) Alyaskada havada hərəkəti idarə edən sistemlərdən bəzilərini söndürməyə məcbur olmuşdu;

- 20 avqust 2008-ci ildə Madrid-Baraxas marşrutu üzrə hərəkət edən Spanair aviaşirkətinin McDonnell Douglas təyyarəsi havaya qalxdıqdan sonra qəzaya uğrayır, onun göyərtəsində olan 154 nəfər həlak olur. Qəzanı araşdıran tədqiqat komissiyasının yekun qərarına əsasən hava gəmisinin göyərtəsində texniki problemləri yerdən monitorinq edən mərkəzi kompüter sisteminin ziyanverici proqram ilə yoluxması qəzaya səbəb olmuşdur;
- 2009-cu ilin fevral ayında FAA-nın kompüter sisteminə hücum zamanı hakerlər FAA-nın 48000 nəfər keçmiş və indiki əməkdaşlarının məlumatlarına giriş əldə etmişdilər;
- 2013-cü ilin iyul ayında İstanbulun Atatürk və Sabiha Gökçən hava limanında kiber hücum zamanı uçma terminallarında pasport nəzarəti sistemlərinin söndürülməsi çoxlu uçuşların yubanmasına və terminallarda xaosun yaranmasına səbəb olmuşdur və s.

Bu və bu hadisələrdən sonra baş vermiş kiber hücumlar təhlükə riskinin artmasından xəbər verir.

5.2.1. Ziyanverici proqramlar

Kompüter sistemlərində informasiya təhlükəsizliyinə yönəlmiş təhdidlərin əsas mənbələrindən biri "ziyanverici proqramlar" kimi ümumi ad almış xüsusi proqramların istifadəsidir. "Ziyanverici proqramlar" (ing. malware) anlayışı icazəsiz və əksər hallarda ziyankar əməllərin həyata keçirilməsi üçün yaradılan və istifadə edilən bütün proqramları birləşdirir.

Təsir mexanizmindən asılı olaraq ziyanverici proqramlar kompüter viruslarına, soxulcanlara, troya atlarına və s. bölünür.

Soxulcanlar − müstəqil, yəni başqa proqramlara yeridilmədən, öz surətlərini kompüter sistemlərində yaymağa və onları işə salmağa qadir olan proqramlardır (virusun aktivləşməsi üçün yoluxmuş proqramın işə salınması tələb olunur). Soxulcanların axın kimi yayılması rabitə kanallarının,

yaddaşın həddən artıq yüklənməsinə və son nəticədə sistemin iflic olmasına gətirib çıxarır.

Troya atları – "yaxşı fayl" adı ilə maskalanıb, funksional cəhətdən faydalı proqram kimi görünən ziyanverici proqramlardır. İşə düşdükdə, troya atları elan edilmiş faydalı funksiyalarla yanaşı, digər elan olunmamış funksiyaları da yerinə yetirir, yaradıcısına həmin kompüterə daxil olmaq imkanı verir.

Nə vaxtsa bütün ziyanverici proqramları təsvir etmək üçün "virus" və "troya atı" anlayışları kifayət edirdi. Lakin həmin vaxtlardan kompüterlərin yoluxdurulması üsulları və texnologiyaları xeyli inkişaf etmişdir və hal-hazırda bu iki anlayış ziyanverici proqramların bütün rəngarəngliyini təsvir etmək üçün kifayət etmir.

Son vaxtlar ziyanverici proqram təminatının yeni növləri meydana çıxmışdır:

Spyware – xəbərsiz olaraq kompüter istifadəçisini izləyən təhlükəli proqramdır. Fərdi məlumatların toplanması ilə məşğul olur: maliyyə məlumatları, kompüterin IP-ünvanı, əməliyyat sisteminin və İnternet-brauzerin versiyası, ən çox baş vurulan İnternet-resursların siyahısı, axtarış sorğuları və sonrakı reklam kampaniyalarında istifadə edilə bilən digər verilənlər. Proqram təminatının yaradıcısı bu məlumatların istifadəsindən pul qazana bilir.

Adware – adətən spyware ilə birlikdə gəlir. İstifadəçinin kompüterində reklam göstərilməsi proqramlarıdır. Çox vaxt belə proqramlar rəsmi satılan məhsulların tərkibinə daxil olur, onların istehsalçıları öz proqram təminatlarının şərti pulsuz versiyalarını təklif edirlər.

Rutkit (rootkit) – kompüterin dərinliklərində yerləşən, təhlükəsizlik proqramları və istifadəçidən gizlənən proqram və ya proqramlar toplusudur. Sistemdə quraşdırılan rutkitlər elə maskalanır ki, nəinki istifadəçilər onu görmür, çox vaxt onları heç antivirus proqram təminatı da aşkarlaya bilmir. Məsələn,

rutkit Windows-un yüklənməsindən öncə işə düşə və əməliyyat sisteminin funksiyalarını dəyişdirə bilər.

Keylogger – fon rejimdə işləyən və hər bir düymənin basılmasını qeyd edən ziyanverici proqramdır. Buraya istifadəçi adları, şifrlər, kredit kartlarının nömrəsi və digər konfidensial məlumatların qeyd edilməsi aiddir. Keylogger bu düymələrin basılmasını öz serverinə ötürür.

Botnet – istehsalçının nəzarəti altında olan böyük kompüter şəbəkəsidir. Hər bir kompüter "bot" (avtomatik olaraq və ya müəyyən olunmuş cədvəl üzrə hər hansı bir fəaliyyət göstərən xüsusi proqramdır) kimi fəaliyyət göstərir, belə ki, xüsusi ziyanverici proqram ilə yoluxmuşdur. "Botla" yoluxmuş kompüter hər hansı bir nəzarət serverinə qoşulur və botnetin yaradıcısından təlimatlar gözləyir. Məsələn, bütün kompüterlər bir sayta və ya serverə qoşulur, sorğu göndərir və belə çoxlu qoşulmalar və sorğular serverin işinin dondurulmasına gətirib çıxara bilər. Botnetlərin yaradıcıları bot şəbəkəsinə girişi cinayət əməli törətmək üçün digər hakerlərə sata bilərlər.

Şantajçılar – kompüteri və ya faylları girov saxlayan və əvəzində pul istəyən proqramlardır. Bu proqramlar vasitəsilə onların yaradıcıları faylları ya dağıtmaq, ya da köçürməklə hədələyərək, pul tələb edirlər.

Kompüter virusları – digər proqramlara yeridilmə yolu ilə müstəqil yayılan, müəyyən şərtlər yerinə yetirildikdə kompüter sisteminə mənfi təsir göstərən kiçik proqramlardır.

5.2.2. Kompüter virusları və onların təsnifatı

Bu gün fərdi kompüterlərin kütləvi tətbiqi təəssüf ki, kompüterin normal işinə mane olan, disklərin fayl strukturunu dağıdan və kompüterdə saxlanılan informasiyaya zərər vuran proqram-virusların da geniş yayılmasına səbəb olur.

Bir çox ölkələrdə kompüter cinayətləri ilə mübarizə haqqında qanunların qəbul edilməsinə və viruslardan mühafizə üzrə xüsusi proqram vasitələrinin hazırlanmasına baxmayaraq, yeni virus proqramlarının miqdarı daim artır. Bu hallar fərdi kompüter istifadəçilərindən virusların təbiəti, viruslara yoluxma və onlardan müdafiə üsulları haqqında biliklərə yiyələnməyi tələb edir.

Yayılma, təsir və inkişaf mexanizmi bioloji viruslarla oxşarlığına görə kompüterdəki bu tip ziyanverici proqramlar kompüter virusları adlandırılmışdır. Virus – özü-özünə inkişaf etmək, fəaliyyət göstərmək qabiliyyətinə malik olan proqramdır. Belə qabiliyyət virusların bütün tiplərinə məxsus olan tək vasitədir. Özü-özünə çoxalmaq yalnız viruslara məxsus deyil. İstənilən əməliyyat sistemi və bir çox proqramlar şəxsi surətlərini yaratmaq bacarığına malikdir. Lakin virusların surətləri nəinki orijinalla uyğun olmaya, hətta tamamilə fərqli ola bilər!

Virus "tam təcriddə" mövcud ola bilmir: bu gün proqramların kodundan (fayl strukturu haqqında məlumat və ya sadəcə digər proqramların adları) istifadə etməyən virusu təsəvvür etmək mümkün deyil. Səbəb aydındır: virus hər hansı bir üsulla idarəetməni ələ almağa məcburdur.

Virusların təsnifatı

Hal-hazırda 50000-dən çox proqram virusları məlumdur. Onları aşağıdakı qruplar üzrə təsnif etmək olar:

- Yaşayış mühiti üzrə (zədələmə obyektləri üzrə);
- Yoluxma üsulu üzrə;
- Təsir dərəcəsi üzrə;
- Təsir edilən əməliyyat sistemləri və platformalar üzrə.

Yaşama mühitindən asılı olaraq, virusları şəbəkə, fayl, yükləmə və fayl-yükləmə viruslarına bölmək olar. Şəbəkə virusları müxtəlif kompüter şəbəkələrinə yayılır. Fayl virusları

əsasən icra edilən modullara kök salır, yəni COM və EXE genişlənmələrinə malik olan fayllara, dinamik kitabxana fayllarına (DLL), drayverlərə (SYS), komanda faylları-na (BAT, CMD) və digər fayllara təsir edir. Onlar icra olunan faylların kökünə öz kodlarını daxil etməklə, yayılırlar. Yoluxmuş belə faylları işə salarkən, əvvəlcə virusun kodu, bundan sonra isə proqramın öz kodu yerinə yetirilir. Fayl virusları başqa tip viruslarda da kök sala bilər, amma bir qayda olaraq, belə fayllara yazılmış viruslar heç vaxt idarəetməni ələ ala bilmir və, beləliklə, artma qabiliyyətini itirir. ***Yükləmə virusları*** (boot-virus) diskin yükləmə sektorunun (Boot-sektor) və ya sistem diskinin (Master BootRe-cord) yüklənməsi proqramını özündə saxlayan sektorda kök salır və kompüterin işə salınması zamanı yüklənir. Kompüterin qoşulması və yenidən yüklənməsi zamanı boot-virus yükləmə kodu ilə əvəzlənir və, beləliklə, əməliyyat sisteminin yüklənməsindən bilavasitə öncə idarəetməni ələ keçirir. ***Fayl-yükləmə virusları*** faylları, həmçinin disklərin yükləmə sektorlarını da yoluxdurur.

Yoluxmanın üsulu üzrə viruslar rezidentlərə və qeyri-rezidentlərə bölünür. Yoluxma vaxtı ***rezident virusu*** kompü-terin əməli yaddaşında öz rezident hissəsini qoyur, bu hissə daha sonra əməliyyat sisteminin yoluxma obyektlərinə (fayllara, disklərin yükləmə sektorlarına və s.) müraciətini yaxalayır və onlarda kök salır. Rezident virusları yaddaşda yerləşir və kompüterin söndürülməsinə və ya yenidən yüklənməsinə qədər aktiv qalır. ***Qeyri-rezidentvirusları*** kompüterin yaddaşını yoluxdurmur və məhdud vaxtda aktiv olur.

Təsir dərəcəsi üzrə virusları aşağıdakı kimi təsnif etmək olar:

• təhlükəsiz olanlar - kompüterin işinə mane olmayan, amma disklərdə azad (boş) əməli yaddaşın və yaddaşın həcmini azaldanlar. Belə virusların təsirləri hər hansı qrafik və ya səsli effektlərdə hiss olunur;

• təhlükəli viruslar - kompüterin işində müxtəlif narahatçılıqlara gətirib çıxara bilər;

• çox təhlükəlilər - proqramların itməsinə, məlumatların məhv olmasına, diskin sistem sahələrində (ərazilərində) informasiyanın silinməsinə gətirib çıxara bilər.

Virusların təsir etdiyi əməliyyat sistemləri və platformalar aşağıdakılardır (DOS, Microsoft Windows, Unix, Linux).

5.2.3. Virusların yaranması və yayılması

1949-cu ildə macar mənşəli Amerika alimi Con Nauman (John von Naumann) özü-özünə hasil olan proqramların yaradılmasının riyazi nəzəriyyəsini hazırladı. Bu, elmi cəmiyyətdə olduqca az maraq doğuran, kompüter viruslarının yaradılmasının birinci nəzəriyyəsi idi (şəkil 5.9).

Şəkil 5.9. Con Nauman

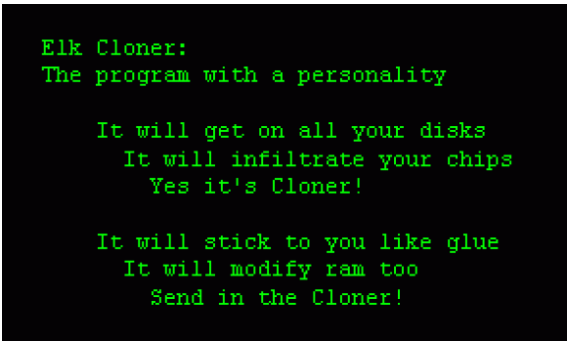
60-cı illərin əvvəllərində Amerika şirkəti olan "Bell Telephone Laboratories"in mühəndisləri - V.A.Vısotskiy, Q.D. Makilroy və Robert Morris - "Darvin" oyununu yaratdılar. Oyun hesablayıcı maşının yaddaşında oyunçular tərəfindən yaradılan rəqib-proqramlar arasında mübarizə qaydalarını

müəyyən edən nəzarətçinin olmasını nəzərdə tuturdu. Proqramlar məkanın tədqiqi, çoxalma və məhvetmə kimi funksiyalara malik idi. Oyunun məqsədi rəqib proqramının bütün surətlərini dağıtmaq və döyüş sahəsini tutmaqdan ibarət idi.

Birinci virusların yaranması 60-cı illərin sonu, 70-ci illərin əvvəllərinə təsadüf edir. Bəzi hallarda bu proqramlarda səhvlər var idi, belə ki, proqramlar öz-özünü köçürür, surətini çıxarır, kompüterlərin sərt diskini zibilləyərək, onların məhsuldarlığını aşağı salırdı. Lakin çox zaman şüurlu olaraq dağıtmaq məqsədi ilə viruslar yaradılmırdı.

Ehtimal edilir ki, əyləncə üçün proqramçı tərəfindən yazılmış virusun birinci qurbanı Univax 1108 kompüteri olmuşdur. Virus "Pervading Animal" adlanırdı və yalnız bir kompüteri - öz kompüterini yoluxdurmuşdu.

İlk geniş məlum olan viruslar Virus 1,2,3 и Elk Cloner Apple II kompüteri üçün 1981-ci ildə hazırlanmışdır. Richard Screnta tərəfindən hazırlanmış Elk Cloner virusu şeir formasında aşkar olunurdu (şəkil 5.10).



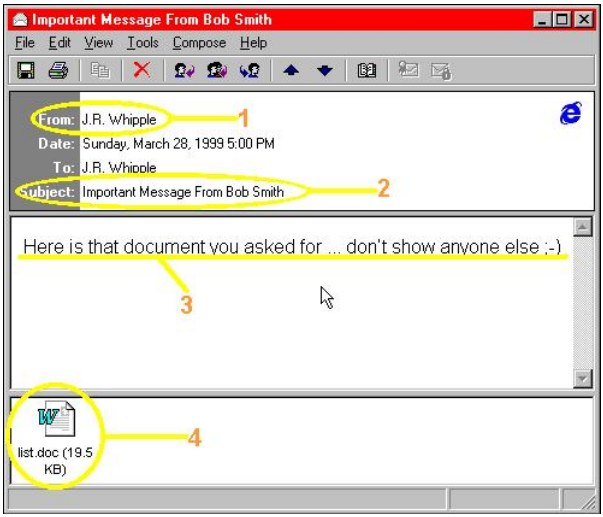
Şəkil 5.10. Elk Cloner virusu

Birinci virus epidemiyası 1987-ci il Brain virusu (həmçinin Pakistan virusu kimi məlumdur) ilə baş vermişdi. O, 1986-cı ildə Amdjat və Basit Faroog Alvi qardaşları tərəfindən hazırlanmış və 1987-ci ilin yayında aşkar edilmişdi.

Məlumatlara görə virus yalnız ABŞ-da 18 mindən çox kompüteri yoluxdurmuşdu. Proqram onların firmasında proqram təminatını oğurlayan yerli cinayətkarları cəzalandırmalı idi. Proqramda qardaşların adları, ünvanları və telefonları qeyd olunmuşdu. Ancaq gözlənilmədən "The Brain" Pakistan sərhədindən çıxaraq, bütün dünyada minlərlə kompüteri yoluxdurmuşdu.

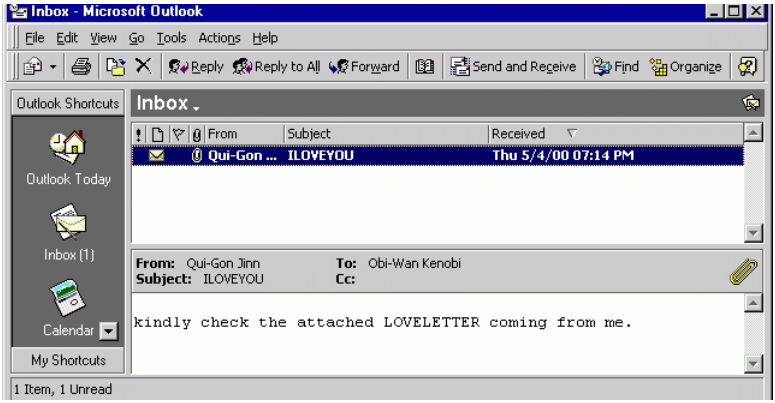
Dünyanın ən məşhur viruslarından biri CIH, "Win95.CIH" və ya "Çernobıl" hesab olunur. Bu virusa yoluxdurulmuş kompüter "işə düşmür", belə ki, bu virus BIOS-u tamamilə məhv edirdi. CIH 1998-ci ildə Tayvan tələbəsi tərəfindən yaradılmış, onun öz inisialları ilə adlandırılmışdı. Virus kompüterə internet, elektron poçt və disklər vasitəsilə düşür, başqa proqramların daxilində gizlənir və müəyyən bir vaxtda isə (26 apreldə, Çernobıl Atom Elektrik Stansiyasında qəzanın tarixi ilə uyğun gəlir) aktivləşib, sərt diskin tərkibini silərək, kompüterin aparat hissəsinə zərər verirdi. "Çernobıl" epidemiyası 1999-cu ilin aprelində baş verdi. Bu zaman xüsusilə Şərqi Asiyada, 300 mindən çox kompüter sıradan çıxmışdı. Növbəti illərdə də 26 aprel tarixində virus öz fəaliyyətini davam etdirir. Müxtəlif ekspertlərin hesablamalarına görə "Çernobıl" virusu bütün dünya üzrə yarım milyon kompüterə ziyan vurmuşdur.

26 mart 1999-cu ildə yaradılmış "Melissa" virusu on minlərlə kompüteri yoluxdurmuş və 100 milyon dollar ziyan vurmuşdu. Bu insidentdən sonra dünyada antivirus proqramlarına böyük tələb yarandı. "Melissa"ya görə böyük İT-şirkətlər, həmçinin Microsoft və Intel kütləvi şəkildə korporativ elektron poçt xidmətlərini söndürürdü (şəkil 5.11).



Şəkil 5.11. Melissa virusu

Ən təhlükəli kompüter viruslarının siyahısında 2000-ci ildə meydana çıxmış "I Love You" virusu ilk yerləri tutur. O, həmçinin "Loveletter", "The Love Bug" adları ilə də tanınır. Bir çox ekspertlər onu internetin tarixində ən zərərverici hesab edirlər. "I Love You" elektron poçtla yayılırdı, Windows-un sistem kanalında Love-Letter-For-You.Htm faylı yaradır, kompüterə ziyan vururdu. Məktubun mövzusunda bu sözlər idi: "mən səni sevirəm". Bu məktuba qoşma əlavə edilirdi, əlavədə yoluxmuş maşınlardan parolları oğurlayan ziyanverici proqram olurdu (şəkil 5.12). Loveletter yayılmasının mexanizmi - Outlook-da ünvanlar axtarır və öz surətini həmin ünvanlara göndərirdi. Loveletter bütün dünyada milyonlarla kompüteri yoluxdurmuşdu. Bu virus ümumilikdə bütün dünyada mövcud olan kompüterlərin 10%-ni bu virusa yoluxdurmuş və 10-15 milyard dollar həcmində ziyan vurmuşdu.



Şəkil 5.12. "I Love You" virusu

"Conficker" virusu ən məşhur kompüter ziyanverici proqramı adını almışdır. O, Microsoft Windows ailəsinin əməliyyat sistemlərinə hücum edirdi. Virus 2008-ci ildə bütün dünyada 12 milyondan çox kompüteri yoluxdurmuşdur. Confickerin iş prinsipi: buferin dolması ilə bağlı Windows-da zəif nöqtələri tapır, sonra servis xidmətlərini söndürür və Windows-un yenilənməsini dayandırır, həmçinin bir sıra antivirusların istehsalçılarının saytlarına girişi bloklayırdı.

Yayılma kanalları

1980-90-cı ildə yoluxmanın ən yayılmış kanalı floppi disklər (disketlər) idi. Hal-hazırda USB flashlar disketləri əvəz etmiş və onların taleyini yaşayır. Çoxlu sayda virus rəqəmsal fotoaparatların, videokameraların, pleyerlərin (MP3-player), mobil telefonların yaddaş qurğuları vasitəsilə yayılır. Bu kanaldan istifadə autorun.inf-in xüsusi faylının yaddaş qurğusunda yaradılması ilə şərtlənir ki, bu proqram autorun soxulcanlarının işə salınması üçün vasitəçi ola bilər. İnternet şəbəkəsinə qoşulmayan kompüterlər üçün yoluxmanın əsas mənbəyi USB flash-lardır.

Elektron poçt virusların yayılmasının əsas kanallarından biridir. Adətən viruslar elektron poçtun məktublarında zərərsiz qoşmaların altında maskalanır: şəkillər, sənədlər, musiqi, sayta

keçidlər (linklər) və s. Bəzi məktublarda həqiqətən da yalnız sayta keçidlər ola bilər. Lakin belə keçidlərdən istifadə etdikdə, virus kodlar olan xüsusi yaradılmış veb-sayta düşmək olar. Bir çox poçt virusları istifadəçinin kompüterinə düşdükdən sonra öz surətinin göndərilməsi üçün Outlook tipli poçt müştərilərinin ünvan kitabçalarından istifadə edir.

Viruslar həmçinin foto, musiqi və ya proqram saytlarına keçidlərdə ola bilər.

Həmçinin müxtəlif "aktiv" tərkibə (skriptlər, ActiveX-komponentlər, Java plaginlər) malik İnternet saytlarından yoluxma halları da baş verir. Bu halda istifadəçinin kompüterində və saytda yazılmış proqram təminatının zəifliyi səbəbindən heç nədən şübhələnməyən istifadəçilər belə sayta girib öz kompüterini yoluxdurmaq riskinə məruz qoyurlar.

Kompüterin ziyankar proqramlara yoluxması əlamətləri. Yoluxmanın aşkar edilməsi zamanı fəaliyyət.

Kompüterdə təhlükəli proqramların olmasını aşkar etmək çətindir, çünki onlar adi faylların arasında gizlənir (maskalanır).

Ziyankar proqramlara yoluxma əlamətləri:

- kompüterin işləmə sürətinin aşağı düşməsi;
- kompüterin öz-özünə sönməsi və yenidən işə başlaması;
- nəzərdə tutulmayan mesajların və ya təsvirlərin ekrana çıxarılması;
- nəzərdə tutulmayan səs siqnallarının verilməsi;
- gözlənilmədən DVD-ROM qurğusunun (CD və DVD-lərin oxudulması qurğusu) qapağının açılması və bağlanması;
- sərbəst, sizin iştirakınız olmadan, hər hansı proqramların kompüterdə işə salınması;
- hər hansı bir proqramın internetə qoşulması cəhdi barədə xəbərdaredici məlumatların ekrana çıxması (hərçənd bu barədə təşəbbüs göstərilməmişdir).
- əməliyyat sisteminin işə qoşulmaması;

- faylların və ya qovluqların itməsi və ya tərkibinin dəyişməsi;
- internet brauzerinin donması və ya normal işləməməsi.

Bundan başqa, elektron poçt vasitəsilə viruslara yoluxmanın xarakterik əlamətləri vardır:

- dostlara və ya tanışlara xəbərlər (mesajlar) göndərilir;
- poçt qutusunda əks ünvansız və başlıqsız olan çoxlu sayda xəbər (mesaj) olur.

Belə halların mövcudluğu 90% ehtimalla yoluxmanın simptomu hesab olunur. Bu zaman antivirus proqramı ilə kompüteri tam yoxlamaq tövsiyə edilir.

Yoluxmanın aşkar edilməsi zamanı fəaliyyət:

- kompüteri internetdən (lokal şəbəkədən) ayırmaq;
- hər hansı bir əməliyyat etməzdən əvvəl xarici yaddaş daşıyıcısında (DVD-disk, USB flash və s.) məlumatları saxlamaq;
- antivirus proqramını yazmaq (əgər kompüterdə heç bir antivirus proqramı yazılmayıbsa);
- antivirus bazasını yeniləmək (əgər bu mümkündürsə, həmin kompüterdən deyil, başqa kompüterdən).

5.2.4. Antivirus proqramları

Kompüter viruslarının geniş yayılması onları aşkarlayan və məhv edən, zədələnmiş mənbələri "müalicə" edən antivirus proqramlarının hazırlanmasına gətirib çıxardı.

Antivirus proqramlarının əksəriyyətinin əsas işi virusların siqnaturasının axtarışıdır. Virus siqnaturası - kompüter sistemində virusun olmasını aşkar edən virus proqramının bəzi unikal xarakteristikasıdır. Bəzən antivirus proqramlarına virusların siqnaturalarının vaxtaşırı yenilənən məlumat bazası qoşulur. Antivirus proqramı kompüter sistemini öyrənir və təhlil edir, həmçinin məlumat bazasında siqnaturalarla

uyğunluğu axtararaq, müqayisə aparır. Proqram uyğunluq tapdığı zaman o, aşkar edilmiş virusu təmizləməyə çalışır.

İşləmə prinsipinə görə antivirus proqramlarını aşağıdakı kimi təsnif etmək mümkündür:

- filtrlər;
- müfəttişlər;
- doktorlar;
- detektorlar;
- vaksinlər və s.

Proqram-filtrlər – daim kompüterin yaddaşında olan "gözətçilərdir". Onlar şübhəli əməliyyatları yerinə yetirmək üçün əməliyyat sisteminə ünvanlanan bütün sorğuları yaxalayır. Bu, artımı həyata keçirmək və kompüterdə informasiya və proqram resurslarını dağıtmaq üçün virusların istifadə etdiyi əməliyyatlardır. Buraya faylların atributunu dəyişmək cəhdi, COM və ya EXE faylların dəyişdirilməsi aiddir.

Bu növ əməliyyatların yerinə yetirilməsi üçün hər bir sorğu zamanı kompüterin ekranına belə fəaliyyət barədə mesaj çıxır (hansı fəaliyyət tələb olunur, hansı proqram onu yerinə yetirəcək). Bu halda istifadəçi onun icrasına ya icazə verir, ya da qadağan edir. Kompüterin yaddaşında "gözətçilər" proqramının daimi olması onun həcmini əhəmiyyətli dərəcədə azaldır, bu da proqramların əsas çatışmazlığı hesab olunur. Proqram-filtr faylları və ya disklər "müalicə etmək" bacarığına malik deyil. Bu funksiyanı başqa antivirus proqramları yerinə yetirir, məsələn, AVP, Norton Antivirus for Windows, Thunder Byte Professional, McAfee Virus Scan.

Müfəttiş-proqramlar viruslardan müdafiənin etibarlı vasitəsidir. Onlar virusa yoluxmamış kompüterin proqramlarının, kataloqların və diskin sistem sahələrinin ilkin vəziyyətini yadda saxlayır. Proqram vaxtaşırı ilk vəziyyətlə cari vəziyyəti müqayisə edir. Uyğunsuzluqlar (faylın

uzunluğuna, modifikasiyanın tarixinə, faylın dövri nəzarət koduna görə) aşkar edilərkən, bu barədə xəbər (mesaj) kompüterin ekranına çıxır. Müfəttiş-proqramlara Adinf və ona əlavə Adinf cure Module proqramını aid etmək olar.

Doktor-proqramlar yalnız ziyankar proqramları aşkar etmək deyil, həmçinin də yoluxdurulmuş proqramları və ya diskləri "müalicə etmək" bacarığına malikdir. Bununla belə virus yoluxdurulmuş proqramları da məhv edir. Bu tip proqramları faqlara və polifaqlara bölmək olar. Faqlar – müəyyən növ virusları axtaran proqramlardır. Polifaqlar – çoxlu sayda müxtəlif virusları aşkarlamaq və məhv etmək üçün nəzərdə tutulmuşdur. Tez-tez istifadə olunan polifaqlar arasında Doctor Web-in adını çəkmək olar. Onlar meydana çıxan yeni viruslarla mübarizə aparmaq üçün fasiləsiz olaraq yenilənir.

Detektor-proqramlar bir və ya bir neçə məşhur virus proqramları istehsalçıları tərəfindən yoluxdurulmuş faylları aşkar edə bilir.

Proqram-vaksinlər və ya immunizatorlar rezident proqramlar sinfinə aiddir. Onlar proqramları və diskləri elə dəyişdirir ki, bu, onların işinə təsir etmir. Lakin vaksini hazırlanan virus o proqramları artıq yoluxdurulmuş hesab edir və onlarda kök salmır. Hal-hazırda geniş yayılmış və viruslarla mübarizə üçün yeni yenilənmiş bir çox antivirus proqramı hazırlanmışdır.

Biz aşağıdakı proqram-texniki tədbirləri nəzərdən keçirəcəyik: ***identifikasiya*** və ***autentifikasiya***.

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

Autentifikasiya (ingilis dilində "authentication") vasitəsi ilə ikinci tərəf əmin olur ki, subyekt doğrudan da özünü qələmə verdiyi şəxsdir. Autentifikasiya sözünün sinonimi kimi çox

vaxt “həqiqiliyin yoxlanması” işlədilir. Subyekt aşağıdakı mənbələrdən ən azı birini təqdim etməklə, özünün həqiqiliyini təsdiq edə bilər:

- bildiyi nəyi isə (parol, şəxsi identifikasiya nömrəsi, kriptoqrafik açar);
- sahib olduğu nəyi isə (şəxsi kart və ya digər təyinatlı analoji qurğu);
- özünün tərkib hissəsi olan nəyi isə (səs, barmaq izləri və s., yəni özünün biometrik xarakteristikalarını).

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

Fəsil üzrə yoxlama sualları

Qeyd olunan fikrin səhv və ya düz olduğunu müəyyənləşdirin.

	Düz	Səhv
1. Barmaq izinə görə identifikasiya aviasiya sahəsində əsas tanıma sistemi kimi istifadə olunur.	☐	☐
2. Şantajçılar – kompüteri və ya faylları girov saxlayan və əvəzində pul istəyən proqramlardır.	☐	☐
3. Aviasiyaya kiber hücum cəhdləri qeydə alınmamışdır.	☐	☐

Test suallarını cavablandırın:

1. Biometriyanın kütləvi tətbiqini kiminlə əlaqələndirirlər?

a) Riçard Niksonla
b) Yuliy Sezarla
c) Edvard Quverlə
d) Alfons Bertilyonla

2. Antivirus proqram-vaksinlərin iş prinsipi nədən ibarətdir?

a) yalnız bir və ya bir neçə məşhur virus proqramlarının istehsalçıları tərəfindən yoluxdurulmuş faylları aşkar etmək
b) virusa yoluxmamış kompüterin proqramlarının, kataloqların və diskin sistem sahələrinin ilkin vəziyyətini yadda saxlamaq

c) həm ziyankar proqramları aşkar etmək, həmçinin də yoluxdurulmuş proqramları və ya diskləri "müalicə etmək"
d) proqramların və disklərin işinə təsir etmədən kod hissəsini dəyişmək

3. Gözün torlu qişası əsasında tanıma sisteminin mənfi cəhətləri nədən ibarətdir?

a) Toxunuşa ehtiyac
b) Uzun vaxtın tələb olunması
c) Sistemin bahalı olması
d) Üsul hələ kifayət qədər yaxşı işlənməmişdir

Açıq sualların cavablarını əhatəli qeyd edin:

1.Kompüter sistemlərində virusların yayılması tarixi necə inkişaf etmişdir?

_____
_____
_____
_____
_____

2. Gözün qüzehli qişası üzrə tanıma sistemi nədir?_____
_____
_____
_____
_____
_____

6. İnformasiyaya qeyri-qanuni müdaxilənin qarşısının alınması

6.1. İnformasiyanın sızmadan mühafizə olunması

Qorunan məlumatların təşkilatın və ya müəyyən şəxslərin çevrəsindən nəzarətsiz kənara çıxması informasiyanın sızması adlanır. Sızmaya gətirən səbəbləri və sızmanın hansı kanallarla baş verdiyini aydınlaşdıraq.

İnformasiyanın sızmasının səbəb və şərtlərində fərqliliklər olduğu kimi, oxşarlıqlar da vardır.

Səbəblərə bir qayda olaraq, informasiyanın saxlanması normalarının qeyri-mükəmməlliyi, bu normaların pozulması, konfidensial informasiya saxlanılan müvafiq sənədlərlə, texniki vasitələrlə və digər materiallarla işləmə qaydalarından kənara çıxmalar aid ola bilər.

Şərtlərə isə müəssisənin (təşkilatın) elmi, istehsalat, reklam, nəşriyyat, hesabat, məlumatlandırma və digər fəaliyyət nəticəsində yaranan və sızmaya zəmin yaradan müxtəlif amillər daxildir. Belə amilləri nəzərdən keçirək:

- Müəssisənin əməkdaşlarının informasiyanın mühafizəsi qanunlarını kifayət qədər bilməməsi və onlara riayət etmənin vacibliyini anlamaması;
- Konfidensial informasiyanın emalında testdən keçirilməmiş texniki vasitələrdən istifadə;
- İnformasiyanın hüquqi, təşkilati və mühəndis-texniki tədbirlərlə mühafizə qaydalarına riayət edilməsinə nəzarətin zəif olması;
- Konfidensial xarakterli məlumatlara sahib olan kadrların axını (işdən çıxması).

Beləliklə, konfidensial informasiyanın sızmasına zəmin yaradan səbəblərin və şərtlərin çox hissəsi müəssisənin rəhbərlərinin və işçilərinin nöqsanları səbəbindən baş verir.

Bundan əlavə, informasiyanın sızmasına şərait yaradan:

- Təbii fəlakət (tufan, qasırğa, zəlzələ, subasma və s.);
- Texnogen fövqəladə hallar (texniki vasitələrin və avadanlıqların nasazlığı, yanğın, partlayış, qəzalar) da ola bilər.

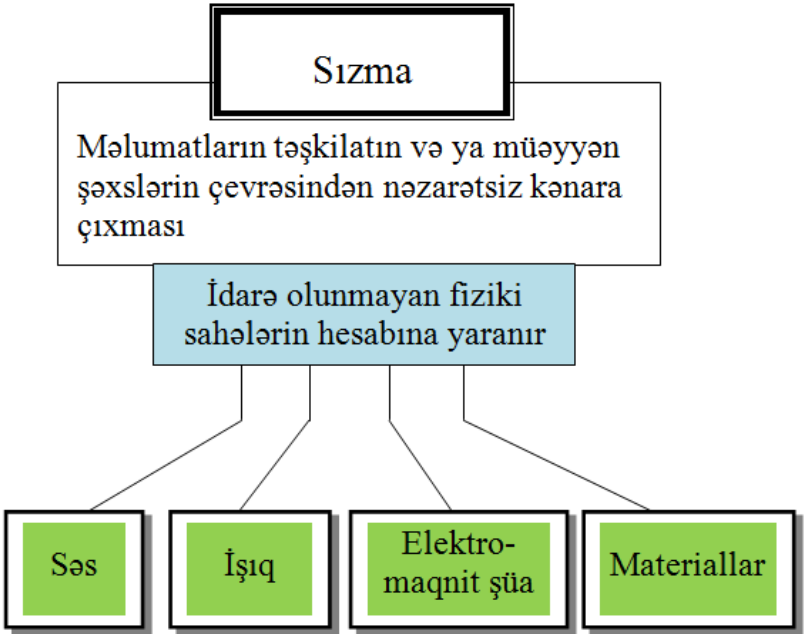
Məlumdur ki, informasiya ümumiyyətlə sahə və ya maddə ilə ötürülür. Bu ya akustik dalğa (səs), ya elektromaqnit şüalanma, ya da mətnli kağız vərəq ola bilər. Amma nə ötürülən enerji, nə göndərilən maddə özü-özlüyündə heç bir məna kəsb etmir. Bu prosesdə onlar yalnız informasiya daşıyıcısı kimi xidmət edir. İnsan informasiya daşıyıcısı kimi nəzərdən keçirilmir. O, ya münasibətlərin subyekti, ya da informasiya mənbəyi kimi çıxış edir.

Buna əsaslanaraq söyləmək mümkündür ki, fiziki mühitdə informasiyanın daşıyıcısı aşağıdakılar ola bilər:

- İşıq şüaları;
- Səs dalğaları;
- Elektromaqnit dalğaları;
- Materiallar (şəkil 6.1).

Təbiətdə digər informasiya daşıyıcısı mövcud deyildir.

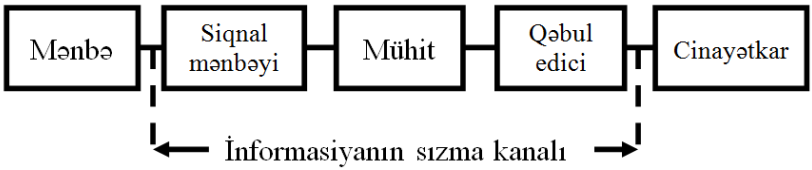
İnsanlar bu və ya digər fiziki sahələri öz maraqları çərçivəsində istifadə edərkən, informasiya ötürməsistemlərini yaradır. Belə sistemləri rabitə sistemləri adlandırmaq qəbul olunmuşdur. İstənilən rabitə sistemi (informasiya ötürmə sistemi) informasiya mənbəyindən və informasiya qəbuledicisindən ibarətdir. Bu sistemlər öz təyinatına uyğun olaraq gündəlik həyatda istifadə edilir və informasiyanın ötürülməsinin rəsmi vasitəsi hesab olunur.



Şəkil 6.1. İnformasiya daşıyıcıları

Lakin müəyyən hallar mövcuddur ki, obyektin və mənbənin istəyindən asılı olmayaraq informasiyanın bir nöqtədən digər nöqtəyə ötürülməsi sistemi yaranır. Əlbəttə ki, bu sistem açıq-aşkar özünü göstərmir. Belə informasiyanın ötürülmə kanalını informasiyanın sızma kanalı adlandırırlar. Bu da siqnal mənbəyindən, yayılma mühitindən və qəbul qurğusundan ibarətdir. Bu kanalda informasiyanın istiqaməti bir tərəfə - mənbədən qəbuledici tərəfə yönəlmiş olur (şəkil 6.2).

Aşağıdakı şəkildə informasiyanın sızma kanalının strukturu verilmişdir:



Şəkil 6.2. İnformasiyanın sızmasının sxemi

İnformasiyanın sızma kanalı dedikdə konfidensial informasiya mənbəyindən pozucuya kimi olan yol başa düşülür. İnformasiyanın sızma kanalının yaranması üçün müəyyən fəza, enerji və zaman şərtlərinin, həmçinin cinayətkar tərəfdən informasiyanın mənimsənilməsi və qeyd edilməsi üçün müvafiq vasitələrin olması gərəklidir.

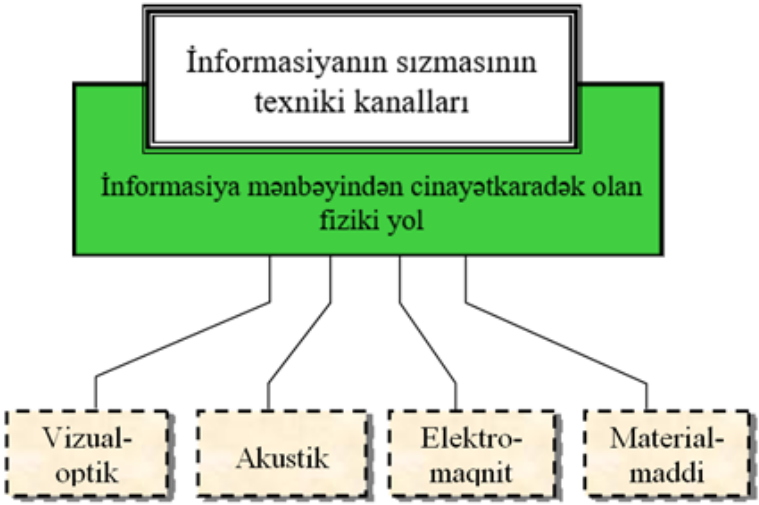
Fiziki təbiəti nəzərə alaraq praktikada tətbiq olunmaqla informasiyanın sızma kanalını aşağıdakı qruplara bölmək olar:

- Vizual-optik;
- Akustik;
- Elektromaqnit;
- Maddi-material (kağız, foto, maqnit daşıyıcıları, müxtəlif növ istehsalat tullantıları – bərk, maye, qaz) (şəkil 6.3).

Hər bir kanal növünün xüsusi özəllikləri vardır.

Vizual optik kanallar. Bu, bilavasitə və ya kənardan (həmçinin, televiziya) müşahidədir. Vizual optik qrupda gizli informasiya mənbəyinin buraxdığı və ya ondan əks olunan infraqırmızı, ultrabənövşəyi və görünən diapazonlarda işıq informasiya daşıyıcısı rolunu oynayır.

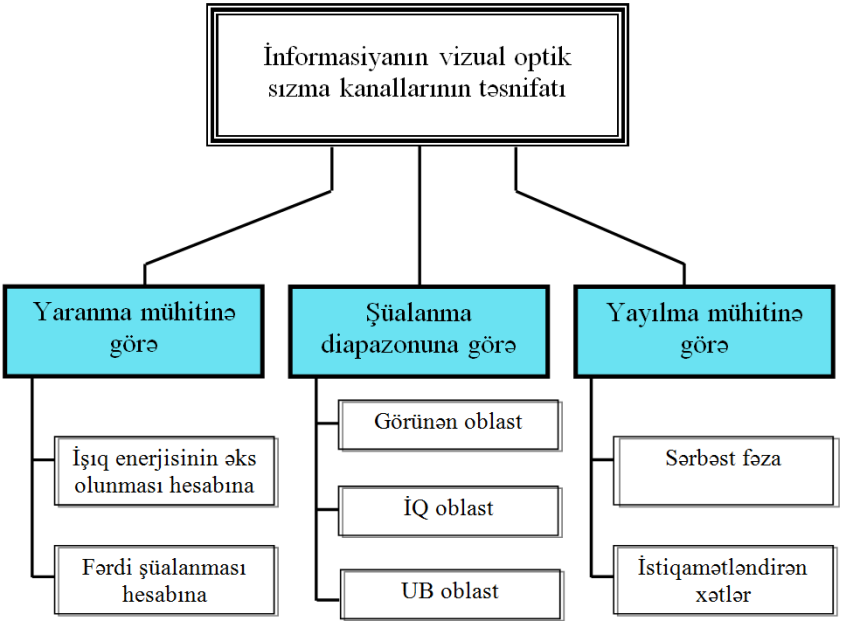
Vizual optik kanalların təsnifatı şəkil 6.4.-də verilmişdir .



Şəkil 6.3. Sızma kanalları

Akustik kanallar. İnsan üçün informativliyə (informasiyanın alınması, qəbulu, qavranması) görə eşitmə görmədən sonra ikinci yer tutur. Buna görə informasiyanın kifayət qədər yayılmış sızma kanallarından biri akustik kanaldır. Akustik kanalda informasiya daşıyıcısı infrasəs (20 Hs-dən aşağı), eşidilən (20 – 20000 Hs) və ultrasəs (20000 Hs-dən yuxarı) diapazonlarında olan səsdir. İnsan nitqinin tezliyi 100-6000 Hs aralığındadır.

Akustik dalğa havada yayılan zaman hava hissəcikləri rəqsi hərəkət etməyə, enerjini bir-birinə ötürməyə başlayırlar. Səsin qarşısında hər hansı bir maneə yoxdursa, o, bərabər şəkildə hər tərəfə yayılır. Əgər səs dalğasının qarşısında hər hansı bir maneə olarsa – arakəsmə, divar, pəncərə, qapı, tavan və s. – səs dalğaları onlara müvafiq təsir göstərir və onları da, həmçinin rəqsetmə rejiminə gətirir. Səs dalğalarının bu təsirləri informasiyanın sızma kanallarının yaranmasının əsas səbəbidir.



Şəkil 6.4. Vizual optik kanalların təsnifatı

Mühitdən asılı olaraq səs dalğalarının yayılmasının müəyyən xüsusiyyətlərini fərqləndirirlər: Bunlar – səsin hava məkanında maneəsiz yayılması, bərk mühitdə səsin yayılması, səsin texniki vasitələrlə yayılması və s. (şəkil 6.5).

Danışıqlar aparılan zaman otaqda sərbəst hava məkanında akustik kanallar qapıların, pəncərələrin, nəfəsliklərin açıq olması zamanı yaranır. Bundan əlavə, belə kanallar otağın hava ventilyasiya sistemi vasitəsilə də yaranır. Bu halda kanalların yaranması hava ötürücülərinin həndəsi ölçülərindən və formasından, rəzələrin, hava paylayıcılarının və s. elementlərin akustik xarakteristikalarından çox asılı olacaqdır.

Struktur səs dedikdə bərk cisimlərdə mexaniki rəqslər başa düşülür. Divarların, arakəsmələrin, boru kəmərlərinin mexaniki rəqsləri bir tərəfdə yaranıb, kifayət qədər uzaq

məsafələrə sönmədən yayıla bilər. Belə sızma kanalının təhlükəsi idarə edilməyən səsin yayılma məsafəsidir.

Şəkil 6.6-da informasiyanın akustik və vibrasiyalı sızma kanallarının sxemi göstərilmişdir. Burada akustik rəqslərin və struktur səsin bərk cisimlərdə, metal konstruksiyalarda, binaların və tikililərin digər elementlərində necə yayılması təqdim olunmuşdur.

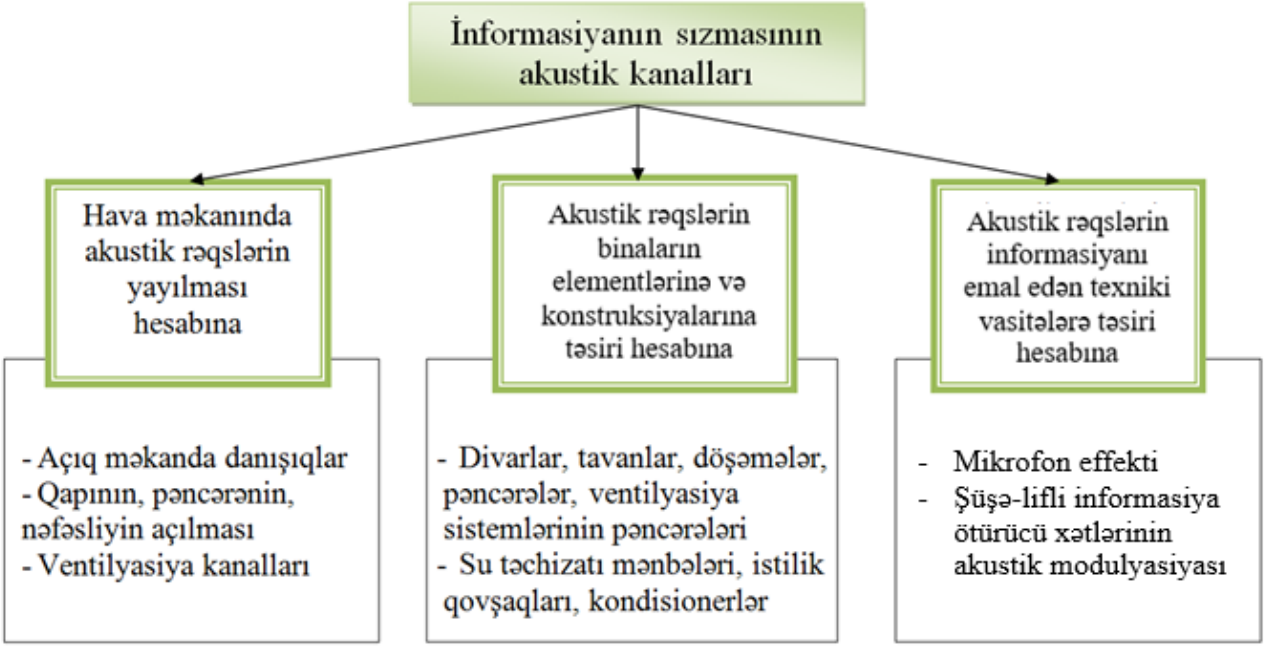
Çevirici, daha dəqiq desək, akustik-çevirici kanal – elektron sxemlərin bu və ya digər siqnallarının akustik sahələrin təsiri altında dəyişməsidir. Praktikada belə hal mikrofon effekti kimi qəbul olunur.

Elektromaqnit kanal. Burada informasiya daşıyıcısı 10km dalğa uzunluqlu (30 kHs-dən aşağı) ifrat uzun dalğalardan 1-0.1mm dalğa uzunluqlu (300 - 3000 QHs) submillimetrlik dalğa diapazonuna qədər olan elektromaqnit dalğalarıdır. Bu növ elektromaqnit dalğalarından hər biri özəl yayılma xüsusiyyətlərinə (uzunluğa, mühitə görə) malikdir.

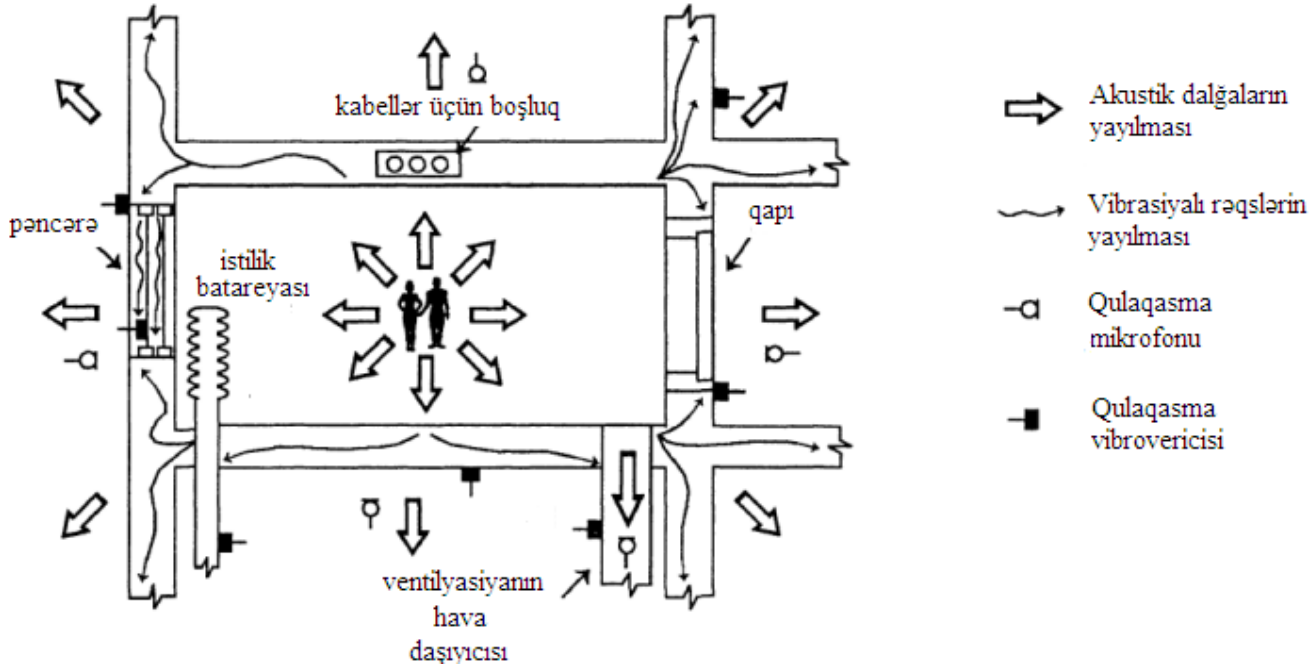
Məsələn, uzun dalğalar uzaq məsafələrə yayılır, millimetrlik dalğalar isə əksinə. Bundan əlavə, müxtəlif telefon xətləri və rabitə kabelləri öz ətraflarında elektrik və maqnit sahələri yaradır ki, bunlar da yaxınlıqda yerləşən digər xətlərə, aparatların elementlərinə yaxınlaşdırmanın hesabına informasiyanın sızma kanalına çevrilə bilər (şəkil 6.7).

Maddi-material kanallar. Belə kanallar kimi bərk, maye və qazabənzər və ya korpuskulyar (radioaktiv elementlər) şəkildə müxtəlif materiallar çıxış edə bilər. Bunlara istehsalat tullantıları, zədəli məmulatlar, köhnə materiallar və s. misal gətirə bilərik.

Aydındır ki, hər bir konfidensial informasiya mənbəyi bu və ya digər səviyyədə sızma kanallarının birləşməsi ola bilər.



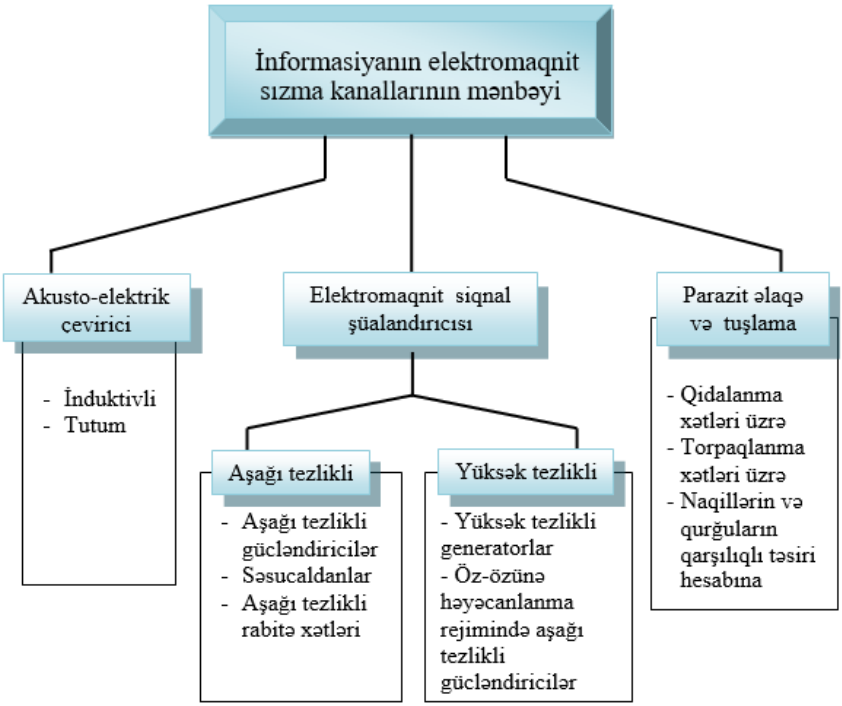
Şəkil 6.5. Səsin fərqli mühitlərdə yayılması



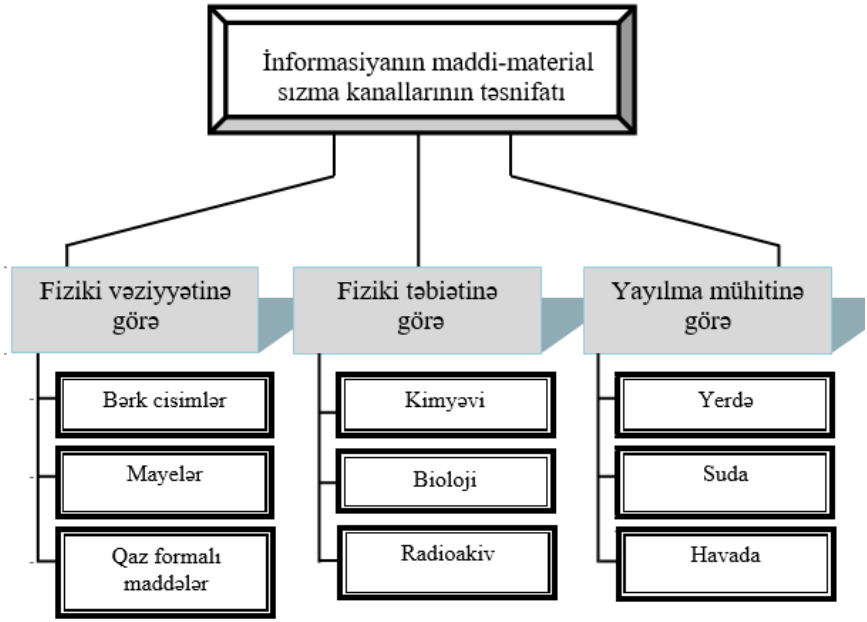
Şəkil 6.6. Akustik və vibrasiyalı sızma kanallarının sxemi

İstehsalatda və elmi fəaliyyətdə müxtəlif texniki vasitələrin istifadəsi texniki informasiyanın sızma kanalları qrupunun yaranmasına səbəb oldu. Texniki vasitələrdə sızma kanallarının yaranmasına səbəb onlar işləyən zaman ətraf fəzada akustik və elektromaqnit dalğaların yaranmasıdır. Bu dalğalar xəbərsiz olaraq informasiyanı daşıya bilər. Qeyd etmək lazımdır ki, texniki vasitələr və sistemlər fəzaya həm siqnal yaya, həm də öz mikrofon və antenaları hesabına akustik və elektromaqnit şüaları qəbul edə, onları elektrik siqnalına çevirib öz rabitə xətləri vasitəsilə ötürə bilər.

Şəkil 6.7. İnformasiyanın elektromaqnit sızma kanallarının təsnifatı



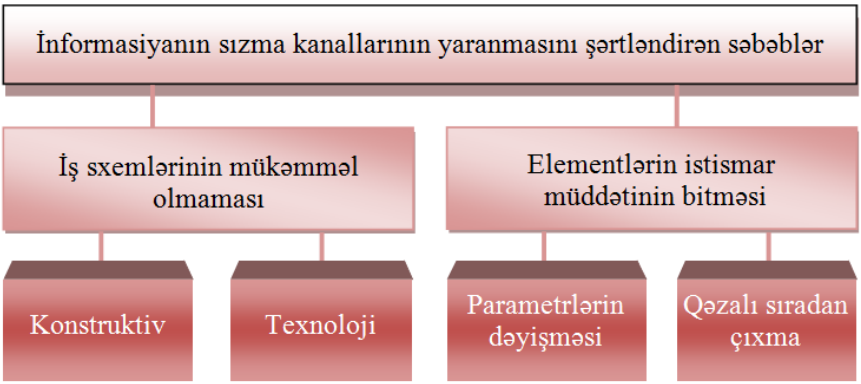
Şəkil 6.8. İnformasiyanın elektromaqnit sızma kanallarının mənbəyi



Şəkil 6.9. İnformasiyanın maddi-material sızma kanallarının təsnifatı

Təhlükəli "mikrofon effekti" (parazit elektrik siqnalının yaranması) bəzi telefon aparatlarının dəstəyi yerdə olduğu zaman da yarana bilər.

Kənar elektromaqnit şüalanma mənbələrinin yaranmasında bir çox amil öz təsirini göstərir. Buraya layihələndirmə zamanı iş sxemlərinin mükəmməl olmaması və qurğuların elementlərinin istismar müddətinin bitməsidir (şəkil 6.10).



Şəkil 6.10. İnformasiyanın sızma kanallarının yaranmasını şərtləndirən səbəblər

İnformasiyanı texniki kanallar vasitəsilə sızılmadan mühafizə etməklə aşağıdakılara nail olmaq mümkündür:

1. İnformasiyanın sızma kanallarını vaxtında müəyyən etmək;
2. Nəzarət olunan zonanın sərhədlərində sızma kanalının energetik xarakteristikalarını müəyyən etmək;
3. Bu kanallara nəzarət etmək üçün cinayətkarların vasitələrinin imkanlarını qiymətləndirmək;
4. Müvafiq təşkilati, təşkilati-texniki və texniki vasitələrlə sızma kanallarının enerjisinin zəiflətmək və ya ümumiyyətlə aradan qaldırmaq.

6.2. İnformasiyanın vizual optik kanallarla sızılmadan mühafizəsi

İnformasiyanın vizual optik kanallarla sızılmadan mühafizəsi – işıq enerjisinin yayılması hesabına konfidensial informasiyanın nəzarət olunan zonadan kənara çıxması ehtimalını azaldan və ya istisna edən kompleks tədbirlərdir.

İnsan ətraf mühiti və ya onun predmetlərini onlardan əks olunan işığın və ya onların özlərinin şüalanması hesabına görür.

İnsan üçün obyektlər haqqında informasiya daşıyıcısı insan gözü ilə görünən şüalardır. İnsan ən böyük həcmdə (90%) informasiyanı görmə sistemi vasitəsilə əldə edir. Görünən spektrin qonşu infraqırmızı və ultrabənövşəyi sahələri də həmçinin kifayət qədər informasiya daşıyır, amma onlar bilavasitə insan gözü ilə görünmür. Onlardan yararlanmaq, onları görmək üçün müxtəlif çeviricilərdən (görünməyən şəkli görünənə çevirən konvertorlardan) istifadə edilir.

Bizi əhatə edən dünya təbii (Günəş, Ay, ulduzlar) və süni yollarla işıqlanır. Obyektləri müşahidə etmək imkanı düşən işıq selinin (işıqlanma), obyektdən əks olunan işığın (əks etmə xüsusiyyətləri) böyüklüyü və onu əhatə edən əşyaların fonunda obyektin kontrastı ilə müəyyən olunur.

Gündüz vaxtı, işıqlanma Günəş şüaları vasitəsilə yaranan zaman insan gözü ən çox işıq və kontrast həssaslığına malik olur. Alatoranlıq vaxtı, Günəş batan zaman gün batmasından asılı olaraq işıqlanma azalır. İşıqlanmanın azalması görmə qabiliyyətinin azalmasına – uzaq məsafədən görmənin və rəng çalarlarının ayırd edilməsinin pisləşməsinə gətirib çıxarır. İnformasiyanın vizual optik kanallarla sızılmadan mühafizəsi zamanı işıqlanmanın bu fiziki xüsusiyyətlərini nəzərə almaq lazımdır.

Mühafizənin vasitə və metodları.

İnformasiyanın vizual optik kanallarla sızılmadan mühafizəsi məqsədi ilə aşağıda qeyd olunan tədbirləri görmək məsləhətdir:

- Cinayətkar tərəfə işığın yayılmasının qarşısı alınması məqsədilə obyektlərin uyğun yerləşdirilməsi (məkan maneələri);

- Mühafizə olunan obyektin əks olunma xüsusiyyətlərinin azaldılması;
- Mühafizə olunan obyektin işıqlandırılmasının azaldılması (energetik məhdudiyyət);
- Əks olunan işığın qarşısının alma və ya zəiflətmə vasitələrindən istifadə edilməsi: ekranlar, pəncərə pərdələri, tünd şüşələr və başqa əngəl törədən vasitələr, maneələr;
- Cinayətkarı çaşdırmaq və müdafiə məqsədi ilə maskalanma, imitasiya və s. vasitələrin tətbiq edilməsi;
- Aerozol pərdələr və maskalayan torlar kimi gizlətmə vasitələrdən istifadə edilməsi.

Gizlətmə vasitələri kimi aerozol pərdələrindən geniş istifadə olunur. Bu, ölçülərindən və aqreqat halından asılı olaraq tüstü, his, duman yaradan, qazaoxşar mühitdə birləşmiş müxtəlif maddələrin xırda hissəcikləridir. Onlar müdafiə olunan obyektdən işığın əks olunmasına əngəl yaradırlar. Tüstü yaradan maddələr yaxşı işıqudma xüsusiyyətlərinə malikdirlər.

6.3. İnformasiyanın akustik kanallarla sızmadan mühafizəsi

İnformasiyanın akustik kanallarla sızılmadan mühafizəsi – akustik sahələrin hesabına nəzarət edilən zonanın hüdudlarından məxfi informasiyanın çıxma ehtimalını azaldan və ya ümumiyyətlə istisna edən kompleks tədbirlərdir.

Bu növ mühafizədə əsas tədbirlər təşkilati və təşkilati-texnikidir.

Təşkilati tədbirlər - arxitektur-planlaşdırma, məkan və rejim tədbirlərindən, təşkilati-texniki isə passiv (səs izolyasiyası, səsin udulması) və aktiv (səsi boğma) tədbirlərdən ibarətdir. Konfidensial danışıqların aparılmasının xüsusi mühafizə vasitələrinin tətbiqi hesabına da texniki tədbirlərin həyata keçirilməsi istisna edilmir (şəkil 6.11).

Arxitektur-planlaşdırma tədbirləri binaların və otaqların layihələndirilməsi mərhələsində həyata keçirilir. Belə tədbirlər bilavasitə hava məkanında və ya tikinti konstruksiyalarında səs sahələrinin nəzarətsiz yayılmasını zəiflədən və ya ümumiyyətlə qarşısını alan müəyyən şərtlərin qoyulmasını və ya rekonstruksiyasını, avadanlıqlaşdırılmasını nəzərdə tutur. Bu məqsədlə qapılar tamburlarla təchiz edilir, pəncərələr kənar əraziləra baxan istiqamətdə deyil, qorunan (nəzarət olunan) tərəfdə tikilir.

Rejim tədbirləri əməkdaşların və qonaqların daxili zonada olmalarına ciddi nəzarəti nəzərdə tutur.

Təşkilati-texniki passiv tədbirlər səs udan vasitələrin istifadəsini nəzərdə tutur. Sadə və yumşaq materiallar – pambıq, xovlu xalça, penobeton (məsaməli beton), məsaməli quru suvaq yaxşı səs izoləedici və səsuducu material hesab olunur. Onlarda səthlər arasında hava qatları vardır ki, bu da səs rəqslərinin dəfələrlə əks olunmasına və udulmasına gətirib çıxarır.

Divarların və tavanların üzlənməsi üçün xüsusi hermetik akustik panellərdən geniş istifadə olunur. Bu panellər yüksək sıxlıqlı və müxtəlif qalınlıqlı (12-50 mm) şüşə-pambıq materialdan hazırlanır. Belə panellər səsin udulmasını təmin edir və divar konstruksiyalarında yayılmasını istisna edir. Səsin udulma səviyyəsi (A) maneələrdən səsin əksolunması və buraxılması, səs udulma, əksolunma, buraxılma əmsalları ilə xarakterizə edilir.

Səs enerjisinin əks olunması və udulması səviyyəsi səsin tezliyi və əks edən (udan) material ilə (məsaməlilik, konfiqurasiya, qalınlıq) müəyyən olunur.

Səs izolə edən örtüyün quraşdırılması həcmi kiçik olan otaqlarda məqsədəuyğundur. Belə ki, böyük otaqlarda səs enerjisi divarlara çatmamış maksimum udulur. Məlumdur ki, hava məkanı müəyyən səsudma qabiliyyətinə malikdir, səsin

gücü havada mənbədən divara kimi olan məsafənin kvadratına mütənasib olaraq azalır.

Otağın daxilində səsin gurluq səviyyəsi açıq havadakına nisbətən yüksək olur. Belə ki, qapalı otaqda səs müxtəlif səthlərdən əks olunur, səs mənbəyi işini dayandırdıqdan sonra da səsin qalması davam edir (reverberasiya). Reverberasiyanın səviyyəsi səsin udulma dərəcəsindən asılıdır.

Səsin udulma kəmiyyəti A səsin udulma əmsalından (α) və səthin səs udma ölçülərindən (S) asılıdır:

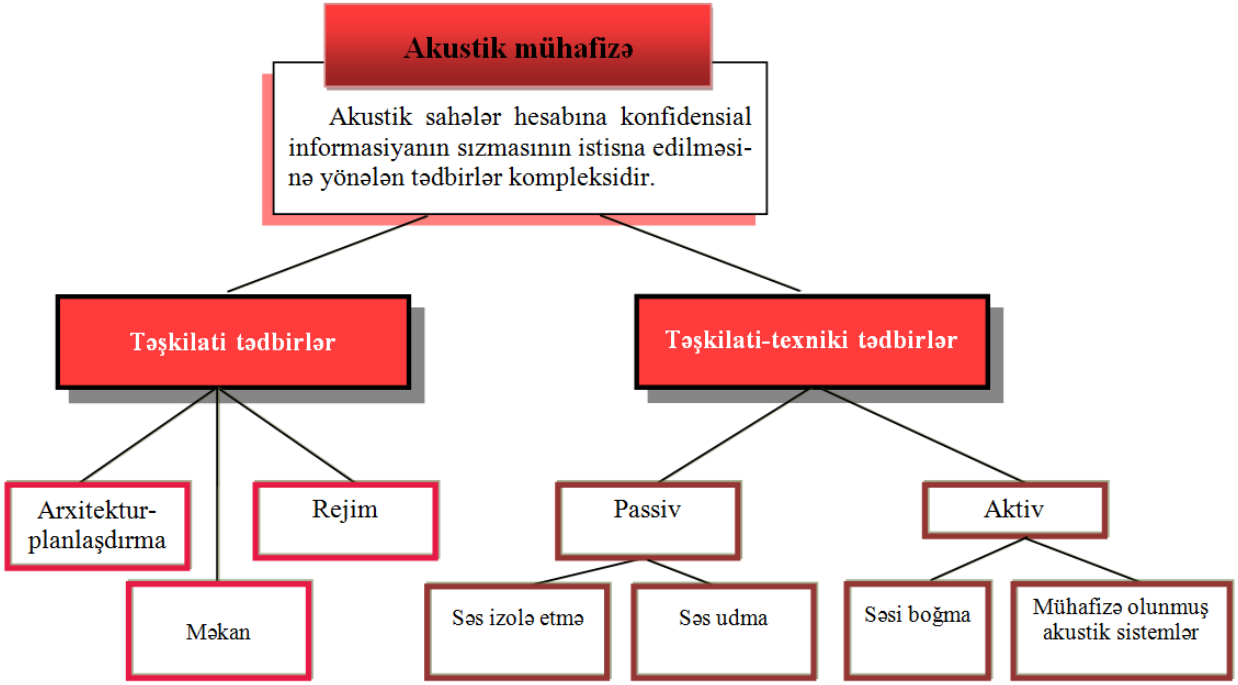
$$A = \sum \alpha \cdot S$$

Müxtəlif materialların udma əmsalları məlumdur. Adi məsaməli materiallar – keçə, pambıq, məsaməli suvaq üçün - 0,02 – 0,8-dir. Kərpic və beton demək olar ki, səsi udmur(α = 0,01 – 0,03).

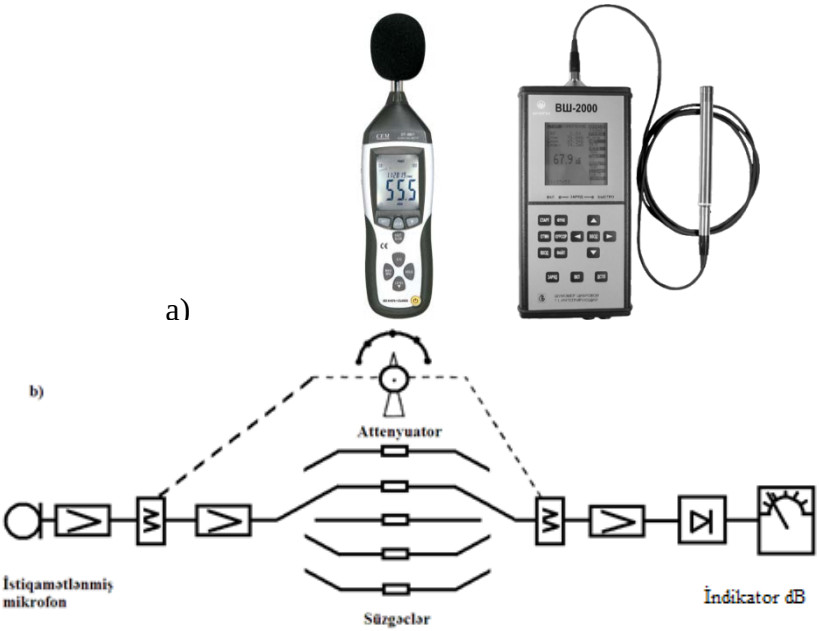
Səsuducu səthlərin tətbiqi zamanı səsin zəifləmə dərəcəsi desibellə (dB) ölçülür. Məsələn, kərpic divarların (α = 0,03) suvaq (α = 0,3) ilə emalı zamanı otaqda səsin təzyiqi 10 dB zəifləyir.

Mühafizənin vasitə və metodları.

Səs izolyasiyasının effektivliyini təyin etmək üçün küyölçənlərdən istifadə olunur. Küyölçən – səs təzyiqi rəqslərinin səviyyəsini göstərən ölçü cihazıdır. Səsin akustik mühafizə sahəsində analoq küyölçənlərdən istifadə olunur (şəkil 6.12).



Şəkil 6.11. Akustik sızmadan mühafizə tədbirləri

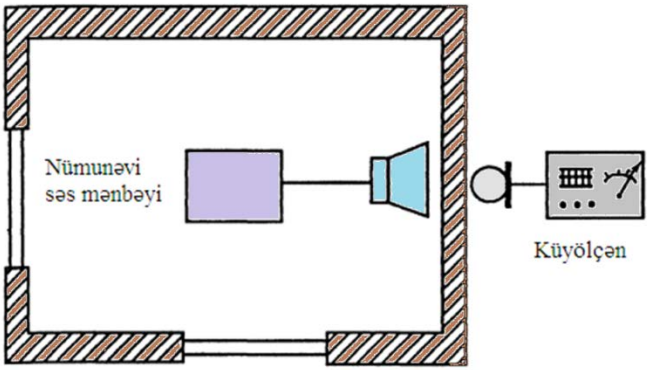


Şəkil 6.12. a) Küyölçənlər ; b) Analoq küyölçənin blok-sxemi.

Göstəricilərin dəqiqliyinə görə küyölçənlər 4 sinfə bölünür. 0 – sinfinə aid küyölçənlər laboratoriya ölçmələri üçün istifadə olunur. 1-ci sinfə aid olanlar havada ölçmələr, 2-ci sinfə aid olanlar ümumi məqsədli ölçmələr, 3-cü sinfə aid olanlar səmtləşdirilmiş ölçmələr üçündür. Praktikada akustik kanalların mühafizə olunma dərəcəsini qiymətləndirmək üçün 1-ci sinif küyölçənlərdən daha çox 2-ci sinif küyölçənlər istifadə olunur.

Akustik qorunmanın ölçülməsi nümunəvi səs mənbəyi metodu ilə həyata keçirilir. Nümunəvi səs mənbəyi olaraq, müəyyən tezlikdə məlum gücə malik mənbə hesab edilir. Belə mənbə kimi 500Hs və 1000Hs tezlikli siqnal yazılmış pleyer

götürülür. Nümunəvi səs mənbəyi və küyölçən vasitəsilə otağın səsudma qabiliyyətini ölçmək mümkündür (şəkil 6.13).



Şəkil 6.13. Küyölçənin işləmə sxemi

Nümunəvi səs mənbəyinin akustik təzyiqinin qiyməti məlumdursa, divarın əks tərəfindən qəbul olunan siqnal küyölçən tərəfindən ölçülmüşdürsə, alınan qiymətlər arasındakı fərq udulma əmsalını göstərir.

Verilən otağın kateqoriyasından asılı olaraq, səs izolyasiyasının effektivliyi müxtəlif olmalıdır. 500 və 1000 Hs tezliklərinə müvafiq aşağıda qeyd olunan udulma normativləri tövsiyə olunur:

Siqnalın tezliyi (Hs)	Udulma əmsalına görə otaqların kateqoriyaları (dB)		
	I	II	III
500	53	48	43
1000	56	51	46

Otaqların akustik və vibrasiya kanalları ilə sızmadan mühafizə olunma səviyyəsini ölçmək üçün elektron stetoskoplardan istifadə olunur. Bu qurğular divardan, döşəmədən, tavandan, qızdırıcı, su təchizatı, ventilyasiya

kommunikasiya sistemlərindən və digər metal konstruksiyalardan otaqda aparılan danışıqlara qulaq asmağa imkan verir.Onlarda həssas element kimi səsin mexaniki rəqslərini elektrik siqnalına çevirən vericilərdən istifadə olunur. Stetoskoplar nəzarət olunan obyektdə konstruksiyanın divarlarından və ya kommunikasiya xətlərindən informasiyanın vibrasiya-akustik sızma kanallarını aşkar etmək, həmçinin informasiyanın mühafizə vasitələrinin effektivliyinə nəzarət etmək üçün nəzərdə tutulmuşdur.

Passiv tədbirlə lazımi təhlükəsizlik səviyyəsini təmin etmək mümkün olmayan hallarda aktiv vasitələrdən istifadə olunur. Aktiv vasitələrə küy generatorları – küyəbənzər elektron siqnallar hasil edən texniki qurğular aiddir. Bu siqnallar müvafiq akustik və ya vibrasiya çevrilmə vericilərinə ötürülür. Akustik vericilər otaqda və ya ondan kənarda akustik küylərin yaradılması üçün nəzərdə tutulmuşdur. Vibrasiya vericiləri isə mühafizə konstruksiyalarında maskalama küylərinin yaradılması üçündür. Vibrasiya vericiləri mühafizə olunan konstruksiyalara yapışdırılır, səs rəqsləri yaradır (şəkil 6.14).

Şəkil 6.14. Küy generatoru

Praktikada istifadə olunan küy generatorları informasiyanı divardan, döşəmədən, tavandan, pəncərədən, qapıdan, borulardan, ventilyasiya kommunikasiyaları və s. konstruksiyalardan kifayət qədər yüksək etibarlıqla mühafizə etməyə imkan verir.

Beləliklə, akustik kanallarla sızmadan mühafizə aşağıda göstərilən tədbirlərlə həyata keçirilir:

- Səs uducu səthlərin, xüsusi əlavə qapı tamburlarının, iki birləşdirilmiş şüşəli pəncərələrin tətbiqi;
- Akustik səs yayan vasitələrin istifadəsi;
- Ventilyasiya kanallarının, qızdırıcı, elektrik təchizatı, telefon və radiokommunikasiya sistemlərinin bağlanması;
- İnformasiyanın sızma kanallarının yaranmasını istisna edən xüsusi yoxlanılmış otaqlardan istifadə.

6.4. İnformasiyanın elektromaqnit kanallarla sızmadan mühafizəsi

İnformasiyanın elektromaqnit kanallarla sızılmadan mühafizəsi – kənar elektromaqnit sahələrin və tuşlamaların hesabına nəzarət edilən zonanın hüdudlarından məxfi informasiyanın çıxma ehtimalını azaldan və ya ümumiyyətlə istisna edən kompleks tədbirlərdir.

Aşağıda qeyd olunan elektromaqnit sızma kanalları məlumdur:

- Elektron sxemlərin elementlərinin mikrofon effekti;
- Aşağı və yüksək tezlikli elektromaqnit şüalanma;
- Müxtəlif təyinatlı gücləndiricilərin parazit generasiyası;
- Elektron sistemlərin qidalanma dövrələri və torpaqlama dövrələri;
- Naqillərin və rabitə xətlərinin qarşılıqlı təsiri;
- Yüksəktezlikli bağlanma;
- Lifli-optik sistemlər.

Elektromaqnit kanallarla informasiyanı sızmadan mühafizə etmək üçün ümumi və xüsusi müdafiə metodları tətbiq olunur. Bundan əlavə, mühafizə fəaliyyətini konstruktor-texnoloji (kanalların yaranması ehtimalının qarşısını almağa yönəlik) və istismar (istehsalat və əmək fəaliyyəti şəraitlərində bu və ya digər texniki vasitələrin istifadəsini tənzimləməyə yönəlik) tədbirlərinə təsnif etmək olar.

İnformasiyanın sızma kanallarının yaranma ehtimalının qarşısının alınması üzrə ***konstruktor-texnoloji*** tədbirlərə aiddir:

- Aparatın elementlərinin və qovşaqlarının ekranlaşdırılması;
- Elementlər və cərəyan daşıyan naqillər arasında elektromaqnit, tutum, induktiv əlaqənin zəiflədilməsi;
- Qidalanma və torpaqlama dövrəsində siqnalların süzgəclənməsi və s. tədbirlər (şəkil 6.15).

Şəkil 6.15.İnformasiyanın konstruksiyalı mühafizə üsulu

Ekranlanma – arzu edilməyən akustik və elektromaqnit siqnalların öz elektromaqnit sahələrinin şüalarının təsirlərindən

qorumağa, həmçinin xarici şüalanmaların parazit təsirini zəiflətməyə imkan verir.

Avadanlığın və onun elementlərinin torpaqlanması və metallaşdırılması yerə tuşlanmış siqnalların yayındırılmasının, parazit əlaqələrin zəifləməsinin etibarlı vasitəsi hesab olunur.

Müxtəlif təyinatlı süzgəclər siqnalların yaranması və ya yayılması zamanı onların yatırılmasına və ya zəiflədilməsinə, həmçinin informasiyanı emal edən avadanlığın qida sisteminin mühafizəsinə xidmət göstərir.

İstismar tədbirlərinə əsasən texniki vasitələrin quraşdırılma yeri elə seçilməlidir ki, onların elektromaqnit sahələri nəzarət olunan zonanın hüdudlarından kənara çıxmasın. Bunun üçün də kənar elektromaqnit şüa səviyyəsi yüksək olan avadanlıqlar yerləşən otaqların ekranlanmasını həyata keçirmək mümkündür.

Mikrofon effekti səbəbindən baş verən sızmadan mühafizə.

Danışıq zamanı yaranan akustik enerji elektron aparatın elementlərində müvafiq rəqslər yaradır, onlar da öz növbəsində elektromaqnit şüalanmanın və ya elektrik cərəyanının yaranmasına səbəb olur. Elektron aparatın akustik təsirlərə ən həssas elementləri induktivlik sarğacları, dəyişən tutumlu kondensatorlar və pyezoelektrik çeviricilərdir.

Bu elementlər olan qurğuda mikrofon effektinin yaranması ehtimalı vardır. Məlumdur ki, mikrofon effektinə telefon aparatlarının müəyyən növləri, səsucaldanlar, istehsalat və əmək fəaliyyətini təmin edən digər növ texniki və elektron vasitələr malikdir.

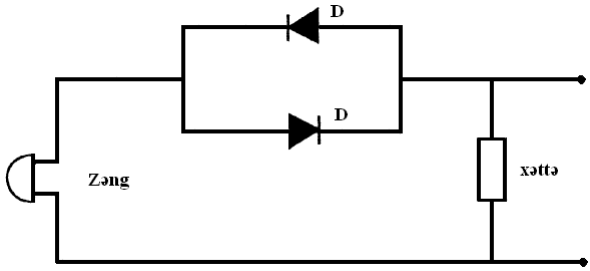
Mikrofon effekti səbəbindən baş verən sızmadan telefon aparatının mühafizəsi təşkilati və ya texniki tədbirlərlə təmin edilir.

Təşkilati tədbirlər aşağıdakılar ola bilər:

- Telefon aparatını yuvadan (rozetkadan) çıxarmaq. Bununla mikrofon effektinin yaranmasının tamamilə qarşısını almaq mümkündür;
- Telefonu daha etibarlı aparatla əvəz etmək.

Texniki tədbirlərə isə telefon xəttinə mikrofon effektinin qarşısını alan xüsusi qurğuların qoşulması aiddir.

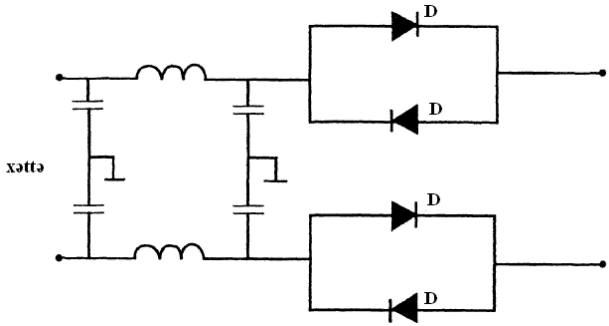
Telefon aparatında mikrofon effektinin yaranma mənbəyi elektromexaniki zəngdir. Onda akustik rəqslərin təsiri altında mikrofon effektinin elektrik hərəkət qüvvəsi (MEEHQ) yaranır. Mühafizə tədbirləri kimi bu elektrik hərəkət qüvvəsinin (EHQ) yatırılması sxemləri istifadə olunur. Şəkil 6.19-da MEEHQ-nin mümkün yatırılma sxemlərindən biri verilmişdir.



Şəkil 6.19. Mikrofon effektinin EHQ-sinin azaldılma sxemi

Zəng dövrəsinə MEEHQ-nin yatırılma sxemini təşkil edən 2 diod daxil edilir. MEEQ-nin kiçik hədlərində belə sxem böyük müqavimətə malik olur, danışıq siqnalında isə (kifayət qədər böyük həddə malik) sxem açılır və danışıq siqnalı azad şəkildə xəttə keçir. Bu sxem avtomatik klapan rolunu oynayır: kiçik EHQ-nin qarşısını alır, abonentin danışıq siqnalını buraxır.

Daha mürəkkəb sxemləri tətbiq etmək də mümkündür (şəkil 6.20).



Şəkil 6.20. EHQ-nin azaldılmasının fərqli sxemi

Bu sxemin əvvəlkindən əsas fərqi 2 cüt diodun və yüksək tezlikli süzgəcin istifadəsindən ibarətdir.

Hər iki sxem mikrofon effekti hesabına informasiyanın sızmasının yaranma ehtimalının qarşısını alır.

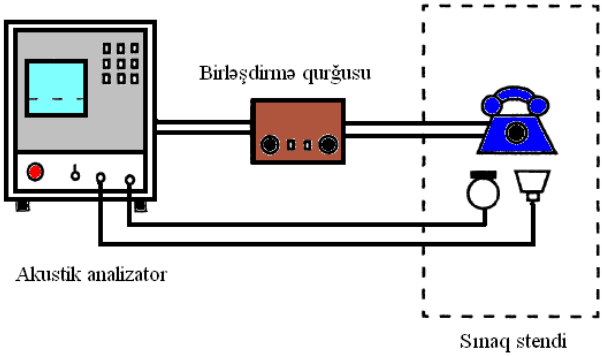
Mikrofon effektinin boğulması sxemləri konstruksiyalarına görə müxtəlif cür hazırlanır. Son vaxtlar belə sxemlər telefon yuvası (rozetkası) formasında düzəldilir ki, bu da onların gizli qalmasına imkan yaradır.

Texniki vasitələrdə mikrofon effektinin olub-olmamasını yoxlamaq və tədqiq etmək üçün yüksək keyfiyyətli sınaq aparatlarından istifadə etmək mümkündür. Nümunə kimi bir sınaq aparatını nəzərdən keçirək. Bu aparat komplekti elektroakustik və elektromexaniki çeviricilərin (telefon aparatları, səsucaldanlar, mikrofonlar, qulaqcıqlar, səs (qulaq) aparatları və s.) hazırlanması, sınaqları və keyfiyyətinə nəzarət zamanı istifadə olunur.

Xüsusi tədqiqatlar şəkil 6.21-də qeyd olunan sxem üzrə aparılır.

Aparat tədqiq olunan texniki vasitələrin ötürülmə xassələrini, onların ekvivalent sxemlərini, mikrofon effektinin xüsusiyyətlərini və digər parametrləri müəyyən etməyə imkan verir: qəbul, ötürülmə xarakteristikasının və telefonun özünün

eşidilmə imkanlarının, həmçinin, küy və təhriflərin ölçülməsini təmin edir.



Şəkil 6.21. Telefon aparatının sınaq sxeminin nümunəsi

Elektromaqnit şüalanma səbəbindən yaranan sızmadan mühafizə.

Elektron və radioelektron vasitələr, xüsusən də elektrik rabitə vasitələri informasiyanın ötürülməsi üçün yaradılan əsas elektromaqnit şüalanmaya və konstruktor texnoloji xarakterli bu və ya digər səbəblərdən yaranan arzuedilməz əlavə şüalanmalara malikdirlər.

Arzuedilməz şüalanmalar kənar elektromaqnit şüalanmalar (KEMŞ), xətdən kənar və küy şüalanmalarına bölünürlər. Bu şüalanmaların hamısı təhlükəlidir. Lakin KEMŞ daha təhlükəlidir. Məhz onlar informasiyanın elektromaqnit sızma kanallarının yaranmasına səbəb olur.

Hər bir elektron qurğu elektromaqnit sahə mənbəyi hesab olunur. Onların xarakteri, təyinatı və sxem həlləri, qurğunun gücü, hazırlanma materialları və onun konstruksiyası ilə fərqlənir.

Məlumdur ki, elektromaqnit sahənin xarakteri onun qəbul edilmə uzaqlığına (məsafəsinə) görə dəyişir. Bu məsafə 2 hissəyə bölünür: yaxın və uzaq.

Yaxın məsafə - sızmanın maqnitlənmə hesabına baş verdiyini, uzaq məsafə isə elektromaqnit şüaları hesabına baş verdiyini göstərir.

Otaqda elektromaqnit şəraitiniaşağıdakı amillər müəyyən edir:

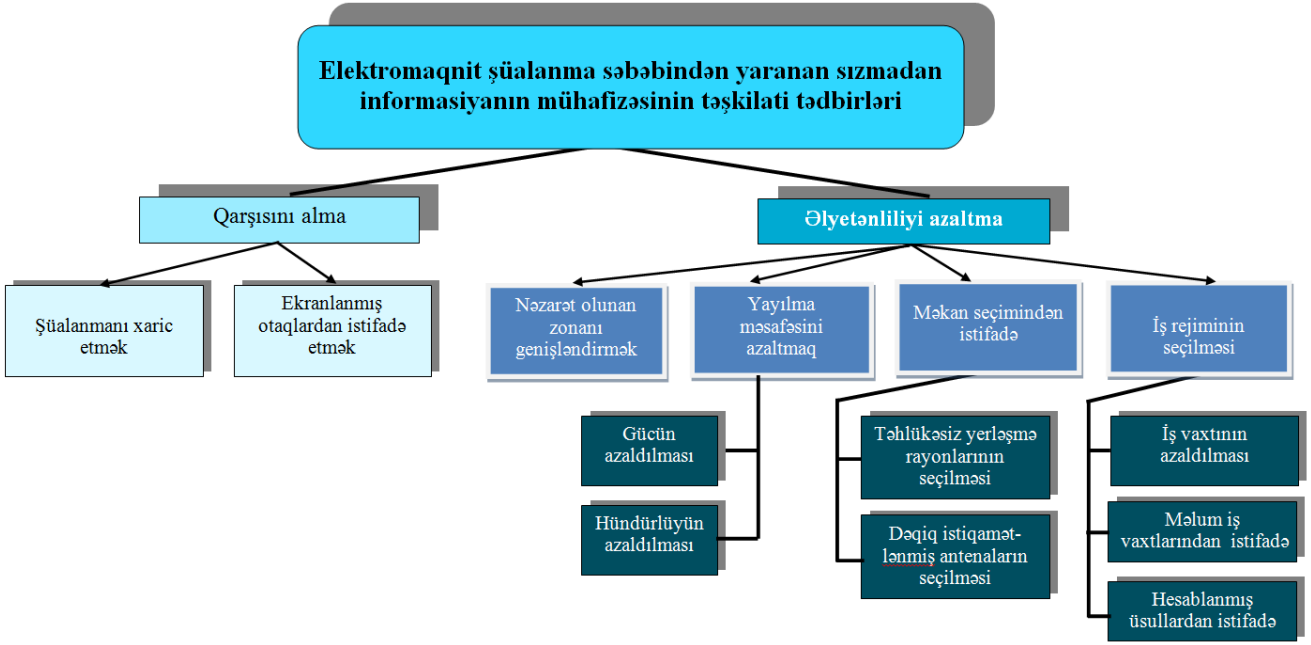
- Otağın həcmi və forması;
- İstifadə edilən avadanlıqların sayı, gücü, iş rejimi və onların eyni vaxtda işlədilməsi;
- Otaqların elementlərinin və texniki vasitələrin hazırlandığı materiallar.

Mühafizə və elektromaqnit sahələrin zəiflədilməsi üsulları kimi elektrik süzgəclərindən istifadə olunur, passiv və aktiv ekranlanma vasitələri və avadanlıqların, qurğuların xüsusi yerləşdirilməsi tətbiq olunur.

Ekranlanma vasitələri ya şüalanma mənbəyinin bilavasitə yaxınlığında, ya mənbənin özündə və yaxud da elektromaqnit siqnalları mənbələri yerləşən otaqda quraşdırılır.

Elektromaqnit şüalanması səbəbindən yaranan sızmadan mühafizəyə bu siqnalların zonanın hüdudlarından kənara çıxmasının qarşısını alan və onların əlçatanlığını azaldan tədbirlər daxildir. Bu tədbirlərin geniş sxemini şəkil 6.22-dəki kimi ifadə etmək mümkündür.

İnformasiyanın mühafizəsi üzrə tədbirləri həyata keçirərkən elektromaqnit şüaların təhlükəlilik səviyyəsini qeyd etmək lazımdır. Belə ki, onların məkanda yayılma xüsusiyyətləri (istiqaməti və məsafəsi üzrə) tezliklər diapazonu və şüalanma gücü ilə ölçülür. Şüalanmanın istiqaməti və məsafəsi elektromaqnit dalğaların müvafiq növünün yayılmasının fiziki təbiəti ilə, təhlükəli siqnalın mənbəyinin və qəbuledici vasitənin yerləşməsi ilə müəyyən olunur.



Şəkil 6.22. Elektromaqnit şüalanma səbəbindən yaranan sızmaya qarşı mühafizə tədbirləri

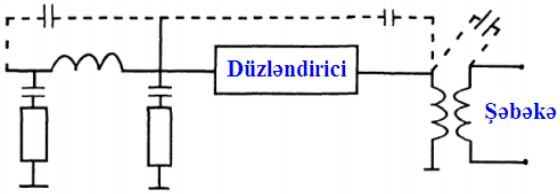
Parazit generasiya hesabına sızmadan mühafizə.

Gücləndiricilərin parazit generasiyası sxemin konstruktiv əsasları hesabına və ya elementlərin köhnəlməsi hesabına idarə olunmayan müsbət əks əlaqə səbəbindən yaranır.

Elektrik qida dövrəsində yaranan sızmadan mühafizə.

Bu və ya digər texniki vasitələrdə dövr edən konfidensial informasiya elektrik qida xəttinə və ya şəbəkəsinə düşə bilər və buradan da nəzarət olunan zonanın hüdudlarından kənara çıxa bilər. Məsələn, elektrik qida xəttinə yüksək tezlik transformatorlarının qida bloklarının parazit boşluqları vasitəsilə keçə bilər.

Mühafizə tədbirləri kimi ayrıca stabilizatorların, çeviricilərin, şəbəkə süzgəclərinin köməyi ilə ayırma üsulundan istifadə olunur (şəkil 6.23).



Şəkil 6.23. Elektrik qida dövrəsi ilə sızmanın sxemi

Torpaqlama dövrəsində yaranan sızmadan mühafizə.

Torpaqlama dövrəsi ilə informasiyanın sızmadan mühafizəsinin əsas şərtlərindən biri onun düzgün quraşdırılmasıdır.

Torpaqlama – torpaqlayan vasitəni elektrik qurğuları, cihazları, maşınları ilə birləşdirən keçiricidən ibarət qurğudur. Torpaqlayan müxtəlif formada – boru, ox, xətt, kağız formasında ola bilər. Torpaqlama vasitələri mühafizə funksiyasını yerinə yetirir və mühafizə cihazlarının yerlə birləşdirilməsi üçün nəzərdə tutulub. Torpaqlama vasitəsinin potensialı ilə ondan keçən cərəyanın asılılığı torpaqlama müqaviməti adlanır.

Torpaqlamanın qiyməti torpağın xüsusi müqavimətindən və torpaqlama vasitəsinin yer ilə birləşmə hissəsinin sahəsindən asılıdır.

Naqillərin və rabitə xətlərinin qarşılıqlı təsiri hesabına sızmadan mühafizə. İstənilən elektron sistemlərin və sxemlərin elementləri, dövrələri, birləşdirici naqilləri və rabitə xətləri daim müxtəlif mənşəli daxili və xarici elektromaqnit sahələrin təsiri altında olur. Bunlar dövrənin elementlərinə elektromaqnit təsirlər və ya sadəcə olaraq təsir adlanır. Bu təsirlər nəzərdə tutulmayan əlaqələr nəticəsində yarandığına görə onlara parazit əlaqələr və tuşlamalar da deyilir.

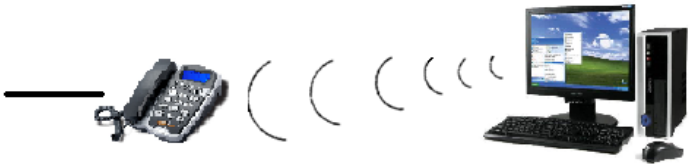
Elektron qurğuların sxemlərində parazit əlaqələrin əsas növləri tutum, induktiv, elektromaqnit, elektromexaniki əlaqələr və radioelektron vasitələrin qidalanma və torpaqlama mənbələri vasitəsilə keçən əlaqələrdir.

Yüksək tezlikli bağlanma hesabına sızmadan mühafizə

İstənilən elektron qurğu yüksək tezlikli elektromaqnit sahəsinin təsiri altında yüksək tezlikli rəqsləri ikinci şüalanma mənbəyinə - təkrar şüalandırcıya çevrilir. Belə siqnal intermodulyasiyalı şüalanma kimi qəbul olunmuşdur, praktikada isə mütəxəssislər onu "yüksək tezlikli bağlanma" adlandırırlar.

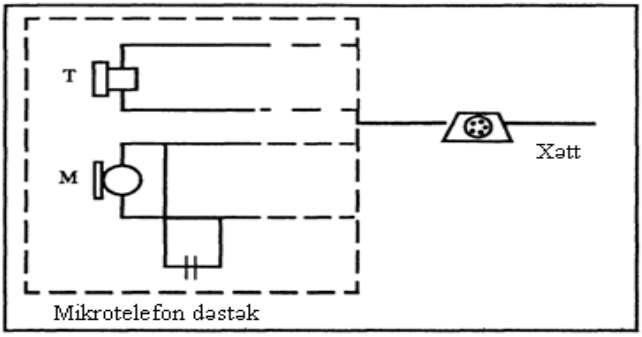
Aşağıdakılar yüksək tezlikli əlaqə mənbəyi ola bilər:

- Mühafizə obyektinin yaxınlığında yerləşən radioyayım stansiyaları;
- Elektromaqnit sahələri telefona və faks aparatlarına təsir göstərə bilən fərdi (personal) kompüterlər. Bundan sonra isə siqnal naqillərlə otaqdan və binadan kənara çıxa bilər (şəkil 6.24).



Şəkil 6.24. Yüksək tezlikli bağlanma

Yüksək tezlikli bağlanmanın telefon aparatına təsiri nəticəsində modulyasiya elementi kimi onun mikrofonu çıxış edir. Bu səbəbdən də yüksək tezlikli cərəyanın ondan keçməsinin qarşısını almaq lazımdır. Buna mikrofona paralel olaraq 0,01- 0,05 мкF tutumlu daimi kondensatorun qoşulması ilə nail olmaq olar. Bu halda yüksək tezlikli siqnal mikrofondan yan keçib, kondensatordan keçəcəkdir.



Şəkil 6.24. Yüksək tezlikli bağlanma zamanı telefonun sızmadan qorunması

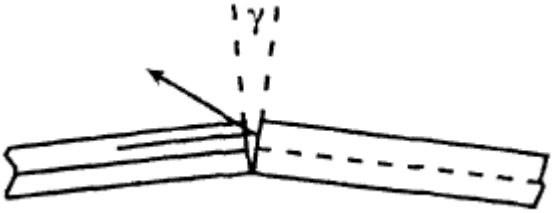
Lifli optik xətlərdə və rabitə sistemlərində sızmadan mühafizə

Lifli optik rabitə xətləri informasiyanın optik sızma kanalları və informasiyanın akustik sızma kanalını yaradan akustooptik effektə malikdir.

Lifli işıq ötürənlərin yığıla bilən birləşmələrində şüalanmanın yaranmasına səbəb (işıq informasiyasının sızması) birləşdirilən liflərin uyğunsuzluğudur (şəkil 6.25).

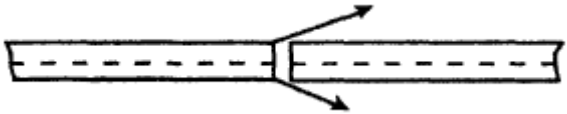
Şəkil 6.25. Liflərin uyğunsuzluğu

- İşıq ötürənlərin orta xəttinin bucaq uyğunsuzluğu (şəkil 6.26);



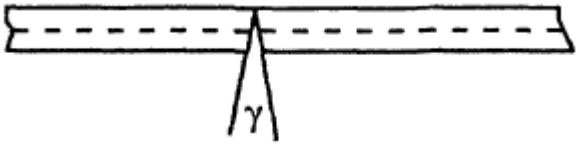
Şəkil 6.26. Bucaq uyğunsuzluğu

- İşıq ötürənin qıraqları arasında boşluqların qalması (şəkil 6.27);



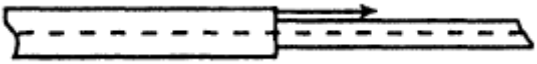
Şəkil 6.27. Boşluqlar

- İşıq ötürənlərin qıraqlarında qarşılıqlı qeyri-paralelliyin olması (şəkil 6.28);



Şəkil 6.28. Qeyri-paralellik

- Birləşdirilən liflərin diametrlərində fərqin olması (şəkil 6.29).



Şəkil 6.29. Liflərin diametrlərində fərq

Bütün bu səbəblər işıq siqnallarının ətraf mühitə şüalanmasına gətirib çıxarır.

6.5. İnformasiyanın maddi-material kanallarla sızmadan mühafizəsi

Maddi-material kanallarla sızmadan informasiyanın mühafizəsi – istehsal və ya sənaye tullantıları şəklində nəzarət edilən zonanın hüdudlarından məxfi informasiyanın çıxma ehtimalını azaldan və ya ümumiyyətlə istisna edən kompleks tədbirlərdir.

İşin istiqamətindən asılı olaraq müəssisənin tullantıları korlanmış fakturalar, icra edilən sənədlərin fraqmentləri, qaralamalar, yeni texnika və məmulatların ilkin hazırlanmış zay (zədəli) modelləri və s. ola bilər.

Tullantılar formaca bərk, maye və qazabənzər ola bilər. Bunlardan da hər biri nəzarətsiz olaraq mühafizə olunan zonadan kənara çıxa bilər. Mayelər kanalizasiyaya axır, qazlar atmosferə yayılır, bərk maddələr isə çox vaxt zibilliyə atılır. Bərk tullantılar xüsusilə təhlükəlidir. Bu həm sənədlər, həm

texnologiya, həm istifadə olunan materialdır. Bu kanalın mühafizəsi tədbirlərinə xüsusi şərh verməyə ehtiyac yoxdur.

İstənilən kanalla sızmadan mühafizə olunmaq üçün aşağıda qeyd olunan fəaliyyət ardıcıllığına fikir vermək lazımdır:

1. Mümkün sızma kanallarının aşkarlanması;
2. Real kanalların müəyyən edilməsi;
3. Real kanalların təhlükəsinin qiymətləndirilməsi;
4. İnformasiyanın sızma kanallarının qarşısının alınması;
5. Kanalların yaranmasına və onlardan mühafizənin keyfiyyətinə daimi nəzarət.

6.6. İnformasiya mənbəyinə qeyri-qanuni müdaxilələr

Gizli informasiya mənbəyinə qeyri-qanuni müdaxilə - qapalı informasiyanı əldə etmək hüququ olmayan şəxs tərəfindən qanuna zidd olaraq, bilərəkdən müxtəlif üsullar və vasitələr tətbiq etməklə həmin informasiyanı ələ keçirməsidir.

Bazar iqtisadiyyatı şəraitində rəqabətli mübarizə zamanı lazımi, vacib informasiyanı əldə etmək istəyənlərin sayı daima artır. Bunun üçün yeni məhsullar işləyib-hazırlamaq lazım gəlir. Lakin iqtisadi mahiyyət də ondan ibarətdir ki, çoxlu vəsait sərf edib yeni məhsulu işləmək və almaqdansa (bunun üçün adətən külli miqdarda pul tələb olunur), bu vəsaitin kiçik hissəsini xərcləməklə, qeyri-qanuni yollarla tələb olunan informasiyanı rəqibdən əldə etmək və bu üsulla böyük gəlir əldə etmək mümkündür. Bundan əlavə, digər məqsədlər də ola bilər: rəqibi aradan qaldırmaq, onu mənfəətli sazişdən, müqavilədən məhrum etmək, şirkətin nüfuzunu aşağı salmaq və s.

Kommersiya sirlərini əldə etmək üçün cinayətkarlar lazımi heyətə, texniki vasitələrə və işlənmiş fəaliyyət üsullarına malikdirlər.

Qeyri-qanuni müdaxilə üsulları

Həm qeyri-qanuni müdaxilələr, həm də onun növləri yerli və xarici ədəbiyyatda müxtəlif cür təfsir olunur. Bir çox ədəbiyyatlarda qeyd olunanları nəzərə alsaq, deyə bilərik ki, qeyri-qanuni müdaxilə üsulları cinayətkar tərəfindən konfidensial xarakterli, mühafizə olunan məlumatları əldə etməyə imkan verən qaydalar toplusudur. Həmçinin, qeyri-qanuni müdaxilə üsulları kimi aşağıdakıları qeyd etmək olar:

1. Əməkdaşlığa təşəbbüs göstərmə;
2. Əməkdaşlığa məcbur etmək;
3. Söz almaq;
4. Gizlicə qulaq asmaq;
5. Müşahidə etmək (güdmək);
6. Oğurluq;
7. Köçürmə;
8. Saxtalaşdırmaq;
9. Məhv etmək;
10. Qeyri-qanuni qoşulma;
11. Ələ keçirmək;
12. Gizli tanış olmaq;
13. Şəklini çəkmək;
14. İnformasiyanın yığılması və analitik emalı.

Əməkdaşlığa təşəbbüs göstərmək xüsusiyyəti adətən nədənsə narazı qalan və ya yaşamaq üçün müəyyən vəsaitə ehtiyacı olan əməkdaşlardan və ya sadəcə tamahkar, acgöz, asan qazanc əldə etmək üçün istənilən qeyri-qanuni fəaliyyətə hazır olan şəxslərin əməllərində özünü göstərir. Siyasi, əxlaqi və maddi düşüncələrlə, həmçinin müxtəlif səbəb və məqsədlərə görə kifayət qədər əməkdaşlığa təşəbbüs göstərmə halları məlumdur. Maliyyə çətinlikləri, qeyri-adi siyasi və ya elmi düşüncələr, işdəki vəziyyətdən, rəhbərlikdən və hakimiyyətdən, öz mövqeyindən narazılıq və digər səbəblər konfidensial

informasiyaya malik şəxsləri cinayətkar qruplaşmalarla və xarici kəşfiyyat orqanları ilə əməkdaşlığa sövq edir. Müəssisənin istehsalat və ya idarəetmə sahəsində belə şəxsin olması cinayətkarlara şirkətin fəaliyyəti haqqında məlumatlar əldə etməyə imkan yaradır. Bu, onlar üçün çox rahatdır, belə ki, məlumat əldə etmək istəyən öz agentini içəri daxil etmək üçün vaxta və xərclərə qənaət edir, adi üsullarla əldə edilməsi çətin olan informasiyanı dərhal və həqiqi mənbədən rahat almaq imkanına malik olur.

Əməkdaşlığa məcbur etmə - bu, bir qayda olaraq cinayətkarlar tərəfindən zorakı fəaliyyətdir. Məcburetmə və ya cəlbetmə halları satın almaq, qorxutmaq, şantaj yolu ilə həyata keçirilə bilər. Əməkdaşlığa məcburetmə real hədələr, təqib etmə və digər fəaliyyət forması ilə həyata keçirilir. Yaşamaq üçün vəsaitlər, imtiyazlar əldə etmək, hakimiyyət uğrunda mübarizədə siyasi fayda qazanmaq məqsədi ilə şantaj müasir dövrdə çox tez-tez və rahatlıqla həyata keçirilən tədbirlərdən biridir. Bəzi rəqiblər "reket" üsullarına da əl atmaqdan çəkinmirlər. Bundan əlavə, rəqib şirkətin mütəxəssislərinin biliklərindən yararlanmaq məqsədi ilə onların öz şirkətləri ilə əməkdaşlığa cəlb edilmək üsulları da mövcuddur.

Söz almaq – sadə və şübhə yaratmayan suallar altında müəyyən məlumatlar almaq cəhdidir. İnformasiyanı almaq üçün yalandan hər hansı bir işə cəlb edilmək barədə vədlər vermək və ya digər üsullardan istifadə etmək mümkündür.

Qulaq asmaq – agentlər, müşahidəçilər, informatorlar tərəfindən xüsusi qulaqasma nöqtələrindən istifadə etməklə tətbiq olunan kəşfiyyat və müəssisə casusluğunun aparılma üsuludur. Qulaqasma birbaşa və ya akustik cihazların istifadəsi ilə həyata keçirilir, bunun üçün isə cinayətkarlar ən müxtəlif hiylələrə əl atırlar, məsələn, xüsusi adamlardan, əməkdaşlardan, müasir texnikalardan istifadə edirlər.

Müşahidə - rəqibin vəziyyəti və fəaliyyəti haqqında kəşfiyyatın həyata keçirilməsi üsuludur. Müşahidə vizual

olaraq, həmçinin optik cihazların köməkliyi ilə həyata keçirilir. Müşahidə prosesi kifayət qədər mürəkkəbdir, belə ki, xeyli güc və vəsait sərfi tələb edir. Bu səbəbdən müşahidə xüsusi hazırlanmış şəxslər tərəfindən məqsədyönlü, müəyyən vaxtda və lazımi yerdə gizli aparılır. Texniki vasitələrə optik cihazlar (binokl, durbin, periskop), televiziya sistemləri, gecə vaxtı və məhdud görünmə zamanı müşahidə cihazları aiddir.

Oğurluq – bilərəkdən qeyri-qanuni olaraq başqasının əmlakını, vasitələrini, sənədlərini, materiallarını, informasiyasını əldə etməkdir. Açıqda qalan hər bir şey oğurlana bilər, məsələn, sənədlər, məhsullar, disketlər, açarlar, kodlar, parollar və şifrlər.

Surəti çıxarılma (köçürülmə) - Cinayət aləmində tərkibində cinayətkarı maraqlandıran məlumatlar olan sənədlərin, məlumatların avtomatlaşdırılmış işlənməsi sistemlərində emal olunan informasiyaların, məhsulların surəti çıxarılır.

Saxtalaşdırma (falsifikasiya, dəyişdirilmə) – rəqabət şəraitində geniş istifadə olunur. Müəyyən informasiyanı, məktubları, hesabları, mühasibat və maliyyə sənədlərini, açarları, buraxılış vəsiqələrini, şifrləri və s. əldə etməyə imkan verən gizli sənədlər saxtalaşdırılır.

Məhv etmək. Həm sənədlərin, həm informasiyanı emal edən vasitələrin, həm də məhsulların məhv edilməsi.

Qeyri-qanuni qoşulma dedikdə informasiyaya qanunsuz müdaxilə məqsədi ilə təmasla və ya təmassız müxtəlif xətlərə və naqillərə qoşulmalar nəzərdə tutulur. İnformasiyanı gizli əldə etmək üçün qanunsuz qoşulma üsulu çoxdan məlumdur. Qoşulma telefon və teleqraf xətləri, həmçinin digər informasiya təyinatlı digər rabitə xətləri ilə (dispetçer xətti, konfrans xətləri, qida və torpaqlanma xətləri və s.) mümkündür.

Ələ keçirmək – radioelektron kəşfiyyatda ələ keçirmə dedikdə passiv qəbul etmə vasitələri ilə elektromaqnit enerji siqnallarının qəbulu hesabına kəşfiyyat informasiyasının əldə olunması başa düşülür. Bu vasitələr bir qayda olaraq gizli

informasiya mənbəyindən uzaq məsafədə yerləşmiş olur. İstənilən radioəlaqə sistemi, mobil rabitə vasitələri ilə (radiotelefon) aparılan danışıqlar ələ keçirilə bilər.

Gizli tanış olma - qapalı informasiya ilə işləməyə buraxılmayan subyektin, lakin müəyyən şəraitdə həmin gizli məlumatı əldə etməsi (söhbət zamanı stolun üstündə gizli sənədin açıq olması, başqa bir adamın gizli informasiya ilə işləməsi zamanı onun kompüterinin ekranına baxma və s.) üsuludur. Gizli tanış olmaya, həmçinin müəssisə və şəxsi yazışmaların poçt göndərmələrinin yoxlanması da aiddir.

Şəklini çəkmək – lazımi obyektin şəklinin əldə edilməsi üsuludur. Üsulun özəlliyi - müşahidə obyekti haqqında qiymətli, detallı məlumatların sənədliliyidir (həqiqiliyidir).

İnformasiyanın yığılması və analitik emalı – informasiyanın öyrənilməsinin və nəticə çıxarılmasının son mərhələsidir. Bir üsulla rəqibin fəaliyyəti haqqında tam həcmli məlumat əldə etmək mümkün deyil. Cinayətkar nə qədər çox informasiya toplamaq imkanlarına malikdirsə, mübarizədə bir o qədər çox uğur əldə edə bilər. Tez bir zamanda və tam olaraq lazımi informasiyanı toplayıb, emal edib qərar verə bilən şəxs uğura ümid edə bilər.

Qeyri-qanuni müdaxiləni həyata keçirmək üçün istifadə olunan texniki vasitələr.

Akustik nəzarət. Akustik nəzarət sisteminə müxtəlif radiomikrofonlar aiddir ki, onların təyinatı informasiyanın alınması və radiokanal vasitəsilə ötürülməsidir.

Radiomikrofonlar – informasiya ələ keçirən xüsusi qurğudur. İstifadəsinə görə:

- Sadə - daimi şüalanan;
- Nəzarət olunan yerdə danışıq və ya küy əmələ gələrkən ötürülmə üçün işə düşən;

- Məsafədən idarə olunan – müəyyən məkana nəzarət etmək üçün lazım olan, vaxta görə söndürülüb-yandırılan.

İnformasiyanı ələ keçirən və radiokanal vasitəsilə ötürən xüsusi qurğuları aşağıdakı əlamətlərinə görə təsnif etmək olar:

- İstifadə olunan tezlik diapazonuna görə (27 MHs-dən 1.5 GHs-ə qədər və daha çox)
- İşləmə davamiyyətinə görə (5 saatdan 1 ilə qədər);
- Fəaliyyət radiusuna görə (15 m-dən 10 km-ə kimi);
- Modulyasiya növünə görə (AM, ÇM və s.).

Son vaxtlar akustik informasiyanı ötürmək üçün aşağıda bəhs ediləcək müxtəlif "qeyri-ənənəvi kanallardan" istifadə edən qurğular tətbiq olunur:

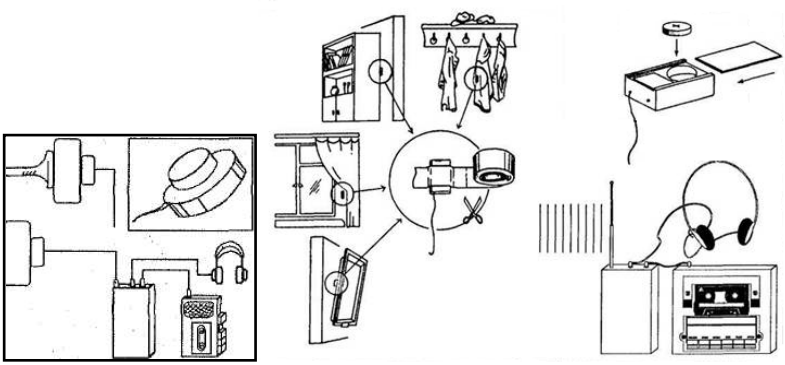
*İnfraqırmızı diapazonda informasiyanı ələ keçirmə qurğuları.*Belə qurğuları aşkar etmək çətin olur. Kəsilməz iş müddəti 1-3 gündür. Bu qurğulardan adətən informasiyanın ötürülmə məsafəsini artırmaq üçün istifadə olunur. Onlar adətən pəncərələr önündə, ventilyasiya dəliklərində yerləşdirilir. İnformasiyanı qəbul etmək üçün 10-15 m məsafədə etibarlı əlaqəni təmin edən İQ diapazonlu xüsusi qəbuledicidən istifadə edilir.

Məlumatların ötürülmə kanalı kimi 127/220/380 V elektrik şəbəkəsindən istifadə edən informasiyanın ələ keçirilməsi qurğuları. Belə qurğuları elektrik rozetkalarına, elektrik uzadıcılarına, məişət avadanlıqlarına, elektrik şəbəkəsinə birləşən və ya şəbəkə keçən istənilən yerə quraşdırılır. Bu qurğuların üstün cəhəti məhdudiyyətsiz işləmə vaxtıdır. Belə qurğulardan informasiyanın qəbulu 300 m radiusda elektrik şəbəkəsinə qoşulmuş xüsusi qəbuledicilərlə həyata keçirilir.

Lazer mikrofon əsaslı informasiyanı ələ keçirmə qurğuları. Belə qurğular 300 m məsafədə pəncərə şüşələrinin rəqslərini qeyd edə və onları səs siqnalına çevirə bilir.

Qeyri-ənənəvi kanallardan istifadə edən qurğular adətən çox baha olur və istifadəsi çətindir. Bu səbəbdən də onların fərdi şəxslər tərəfindən istifadə edilmə ehtimalı azdır.

İnformasiyanın ələ keçirmə qurğusunu birbaşa olaraq obyektdə quraşdırmaq mümkün olmayan hallarda stetoskop mikrofonlardan istifadə olunur (şəkil 6.30).Bu mikrofonlar möhkəm sədd (divar, şüşə, avtomobil korpusu və s.) arxasındakı danışıqlara qulaq asmaq imkanı verir. Bu sədd nə qədər möhkəm və bircinsli olarsa, bir o qədər stetoskoplar daha yaxşı işləyər. Stetoskop gücləndirici və telefon (və ya avtomatik səsyazıcı qurğu) ilə birləşmiş vibrovericidən ibarətdir.



Şəkil 6.30. Mikrofon stetoskop

Stetoskop mikrofonun köməyi ilə 1 m və daha qalın divarlardan danışıqlara qulaq asmaq mümkündür. Bu sistemin əsas üstün cəhəti onun aşkarlanmasının çətinliyidir, yəni stetoskop-mikrofonu qonşu otaqda quraşdırmaq olar. İnformasiyanı ələ keçirmə qurğusu məkan sahibinin icazəsi ilə və yaxud icazəsi olmadan xüsusi hazırlanmış yerdə gizlədilir,

yaxud məişət, interyer əşyalarına və ya otaqdakı dəliklərə qoyulur.

Rabitə vasitələrinə qeyri-qanuni müdaxilələr.

Son vaxtlar şəxsi və kommersiya xarakterli informasiyaya qanunsuz müdaxilənin əsas üsullarından biri telefon danışıqlarına qulaq asmaq olmuşdur. Telefon danışıqlarına qulaq asmaq üçün aşağıda qeyd olunan qoşulma üsullarından istifadə olunur:

- Telefon xəttinə paralel qoşulma. Bu halda telefon radioretranslyatorları aşkar etmək çətindir, lakin xarici qida mənbəyi tələb edir;
- Telefon xətlərinin kəsiyinə telefon radioretranslyatorlarının ardıcıl qoşulması. Bu halda telefon radiotranslyatorlarının qidalanması telefon xəttindən həyata keçirilir və telefon dəstəyi qaldırılan kimi ötürülməyə başlayır.

Telefon radiotranslyatorlarının qoşulması birbaşa olaraq telefona və ya telefon xəttindən telefon qovşağına qədər istənilən hissədə həyata keçirilə bilər. Hal-hazırda dəstəyi yerinə qoyulmuş telefonların mikrofonlarından otağa qulaq asmaq imkanı verən telefon radiotranslyatorları mövcuddur. Bunun üçün telefon xəttinin birinə yüksəktezlikli rəqslər generatorunun siqnalı verilir, digərinə isə gücləndirici ilə amplitud detektoru qoşulur. Bu halda yüksəktezlikli rəqslər mikrofondan və ya "mikrofon effektinə" malik telefon aparatının elementindən keçir və qulaq asılan otaqdakı akustik siqnallar modulyasiya edilir. Modulyasiya edilmiş yüksəktezlikli siqnal amplitud detektoru ilə demodulyasiya edilir və güclənmədən sonra qulaqasılmaya və yazılmaya hazır olur. İkiməftilli xətdə yüksək tezlikli siqnalın sönməsinə görə bu sistemin fəaliyyət məsafəsi bir neçə metrdən çox olmur. Telefon xəttinə birbaşa elektron birləşmə tələb etməyən telefon danışıqlarına qulaq asma sistemləri mövcuddur. Bu sistemlər informasiyanın ələ keçirilməsinin induktiv üsulundan istifadə

edir. Onlar müəyyən həcmə malikdir, belə ki, zəif yüksəktezlikli siqnalları gücləndirmək üçün bir neçə elementdən ibarətdir. Telefon radiotranslyatorlarından informasiyanı qəbul etmək üçün radiokanal ilə informasiyanı ələ keçirən akustik qurğularda olduğu kimi qəbuledicilərdən istifadə olunur. Halhazırda faks və modem rabitəsini ələ keçirmə sistemləri inkişaf edir.

Telefonlara və xətlərə birbaşa qoşulma.

Telefon xətlərinə birbaşa qoşulma – informasiyanın əldə edilməsinin ən sadə və etibarlı üsuludur. Ən sadə halda xətlər ayrılan, bölünən qutudakı xətlərə telefonçu ustanın telefon dəstəyi ilə qoşulması qeyd oluna bilər. Adətən peşəkar olmayan cinayətkarlar tez-tez bu üsullara əl atırlar. Peşəkar cinayətkarlar xüsusi xidmət orqanlarının avadanlıqlarından pis olmayan qurğularla təchiz olunurlar. Yadda saxlamaq lazımdır ki, telefon qovşağı 1 kOm gərginliklə təsir göstərməklə xətti danışığa qoşa bilir. Aşağı gərginlikli qulaqasma qurğusunun qoşulmasını kifayət qədər tez aşkarlamaq mümkündür. Əgər xətdəşıqqıltı (çıqqıltı) və ya səsin azalıb-güclənməsi eşidilərsə, bu zaman telefona qeyri-peşəkar olmayan üsulla qulaq asma cəhdlərinin olması ehtimalı vardır.

Telefon qovşağının əməkdaşlarının satın alınması.

Telefon qovşağında xidmət göstərən personalın satın alınması - sirlərin üstünün açılmasının olduqca yayılmış üsuludur. Bu, əsasən, indiyə qədər köhnə telefon qovşaqlarından istifadə olunan kiçik şəhərlərdə mümkündür. Böyük ehtimalla cinayətkar qruplar və ya rəqabət aparan firmalar bu üsuldan istifadə edə bilərlər.

Elektromaqnit zəng vasitəsilə qulaqasma.

Çağırış qurğusu kimi elektromaqnit zənglərdən istifadə olunan telefon aparatları bir çox ölkələrdə geniş yayılmışdır.

Zəng duallıq xüsusiyyətinə malikdir, yəni elektromaqnit zəngə səs dalğaları təsir göstərirsə, o, müvafiq formada modullanmış cərəyan yaradır. Onun amplitudu növbəti emal üçün kifayətdir.

Gizli foto və video çəkiliş.

Məlumat toplamaq üçün vizual müşahidənin ən qədim və çox effektli üsul olduğu məlumdur. Bunun üçün kəşfiyyatın tarixinə müraciət etməyə ehtiyac yoxdur. Hal-hazırda informasiya əldə etmək üçün miniatür gizli və xüsusi (adi əşyalar formasında) foto və video kameralar istifadə edilir (şəkil 6.31).

Şəkil 6.31. Gizli foto və video çəkiliş vasitələri

- Miniatür (gizli) kameralar məişət texnikasına qoşulur, video informasiya kabel və ya yüksək tezlikli kanal vasitəsilə televiziya ötürücüsünün köməyi ilə ötürülür.
- Xüsusi kameralarməişət əşyası şəklində (siqaret qutusu, çanta, kitab, qol saatı) ola bilər.

Gizli foto və video çəkiliş üçün nəzərdə tutulan avadanlıqlar bir qayda olaraq xüsusi obyektivlər və ucluqlarla təchiz olunur.

Müşahidə - vizual yolla və ya optik vasitələrin tətbiqi ilə obyekt haqqında informasiya əldə etmək məqsədi ilə aparılan kəşfiyyat üsuludur.

İnsanlar, onların piyada və nəqliyyat vasitələri ilə hərəkəti, görüşləri, digər fəaliyyətləri, evləri müşahidə oluna bilər. Gündüz vaxtı müşahidə gecə vaxtı müşahidəyə nisbətdə daha asandır.

Müşahidə növünə, müddətinə, intensivliyinə və məqsədinə görə fərqlənir. Müşahidə görmə məsafəsində və uzaq məsafədən xüsusi optik sistemlər və televiziya sistemləri vasitəsilə həyata keçirilə bilər.

Müşahidə olunan faktların sənədləşdirilməsi (rəsmiləşdirilməsi) və təhlil edilməsi məqsədi ilə onların fotoşəkli və video görüntüsü çəkilir. Fotoşəklin çəkilməsinin öz şərtlərinin olduğu da məlumdur.

Müşahidədən və fotoşəklin çəkilməsindən mühafizə olunmaq üçün:

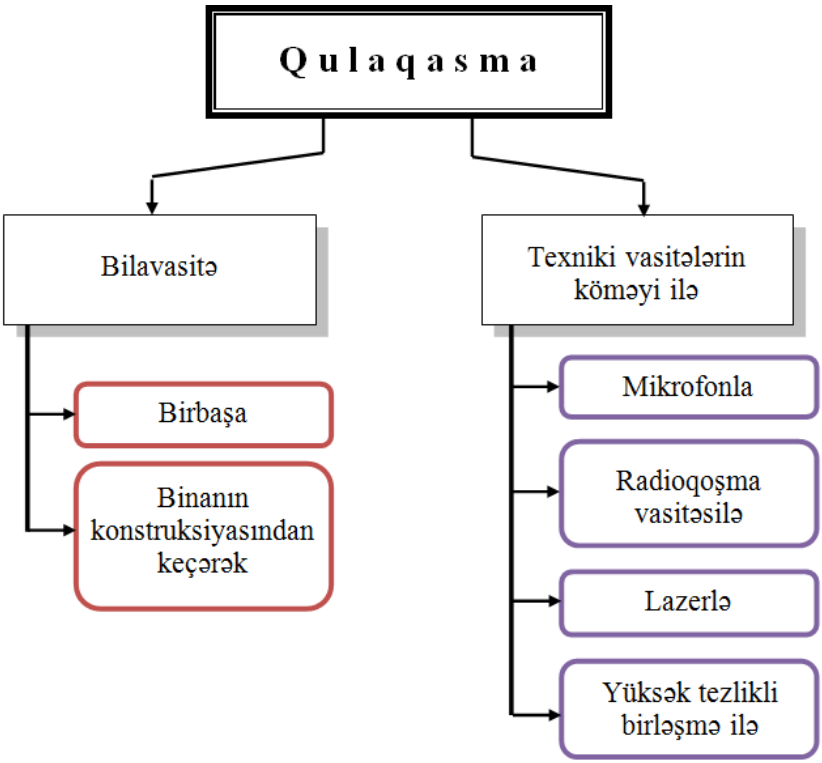
- Birbaşa və ya distansion müşahidəyə mane olmaq üçün informasiya əks olunan obyektin (kompüter, sənəd) optimal yerini seçmək;
- İşıq keçirməyən şüşələrin, pərdələrin, tüllərin və digər mühafizə vasitələrinin (qəfəslərin, pəncərə qapılarının) istifadə olunması;
- Pəncərələri təhlükəsiz yerə açılan otaqların seçilməsi;
- Müəyyən vaxtdan sonra kompüterlərin ekranının sönməsi proqramından istifadə edilməsi.

Qulaq asmadan mühafizə.

Qulaqasma – agentlər, müşahidəçilər, xüsusi dinləmə postları vasitəsilə tətbiq olunan sənaye casusluğu və kəşfiyyat

üsuludur. Texniki rabitə vasitələri ilə ötürülən danışıqların və mesajların da dinlənilməsi həyata keçirilir.

Məlumdur ki, danışanın akustik dalğaları birbaşa və ya binanın konstruksiyalarından keçərək dinləyiciyə çatarsa, bu zaman dinlənilmə bilavasitə hesab olunur. Lakin müxtəlif texniki vasitələrdən (mikrofonlar, radioqoşma, lazerlər, yüksək tezlikli rəqslər) istifadə etməklə danışıqlara qulaq asma geniş yayılmışdır (şəkil 6.32).



Şəkil 6.32. Qulaq asma növləri

Mikrofon sistemləri ilə dinlənilmənin qarşısının alınması.

Mikrofon texniki vasitələrin köməyi ilə dinlənilmə sisteminin birinci halqasını təşkil edir.

Məlumdur ki, insan tərəfindən qəbul edilməyə görə səs diapazonu aşağıdakı kimi təsnif olunur:

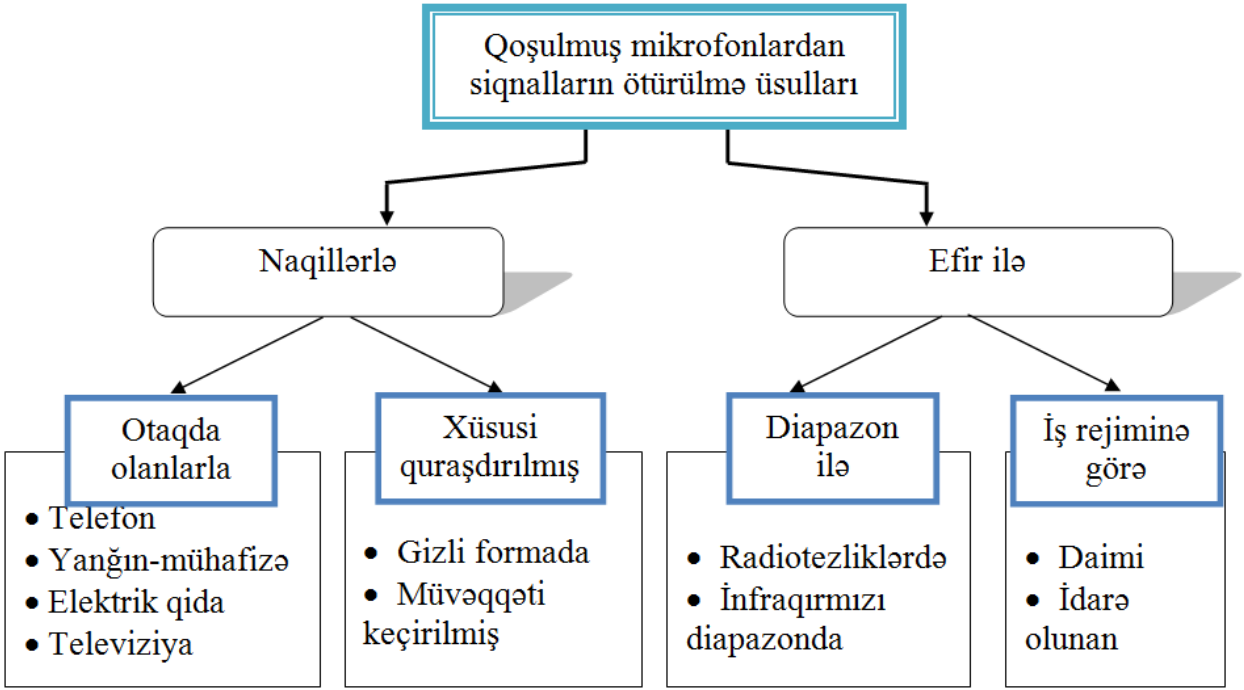
- Eşidilməyə görə (16-20000 Hs);
- İnfrasəs (16 Hs-dən aşağı);
- Ultrasəs (20 000 Hs-dən yuxarı).

Mübarizə tədbiri kimi mikrofona ultrasəs tezlikli akustik təsirlər tətbiq olunur. Belə təsir danışıqların aparılmasına mane olmur, lakin digər siqnallara böyük təsir göstərir.

Mikrofon tərəfindən qəbul olunan səs elektrik rəqslərinə çevrilir və bunlar qəbul edilərək emal olunan qurğulara göndərilir.

Məsafədən idarə olunan mikrofonların bir nümunəsi də "telefon qulaq" qurğusunu hesab etmək olar. Bu qurğuda mikrofon və mikrofonun idarə olunma sxemi telefon qovşağına quraşdırılır. Belə qurğu vasitəsilə ofislərdə, evdə və digər müəssisələrdə danışıqların dinlənilməsini şəhərin istənilən telefonundan, hətta digər şəhərdən və ölkədən həyata keçirmək mümkündür. Dinləyici aparatın işə salınması üçün qurğu quraşdırılan telefon aparatına zəng vurmaq lazımdır.

- İlk zəngdən sonra aktiv rejimə keçir,
- 10-15 saniyədən sonra ikinci zəngdə 40 saniyə müddətində məşğul olmasına dair yalan siqnallar verir, bundan sonra həmin siqnallar dayanır və mikrofon işə düşür, dinlənilmə başlanır. Əgər abonent kiməsə zəng etmək üçün telefonun dəstəyini qaldırarsa, dinlənilmə dayanır, adi zəng zamanı da aşkarlanmır.



Şəkil 6.33. Qoşulmuş mikrofonlardan siqnalların ötürülmə üsulları

Strateji təyinatlı obyektlərdə müşavirələrin, danışıqların və konfidensial, məxfi söhbətlərin aparılması, cinayətkarın qarşısının alınması üçün xüsusi, dinlənilmədən mühafizə olunmuş otaqlar yaradılır. Belə otaqlara xüsusi status verilir, onlar aşağıdakı tələblər nəzərə alınmaqla təchiz olunur:

- Belə otaqlar yerləşdirilən binalar 24 saatmühafizə olunmalı və siqnalizasiya sisteminə malik olmalıdır;
- Otaq mümkün qədər binanın ortasında, rəhbərliyin otağı ilə yanaşı yerləşməlidir;
- Əgər otaqda pəncərənin olmasına ehtiyac varsa, onlar eyvansız olmalı, digər qonşu bina tərəfə çıxmamalı, daxili həyətə istiqamətlənməli və ya dəmir qəfəslə bağlanmalıdır;
- Otaq daxilində minimum sayda mebel olmalıdır; mebellərin konstruksiyası dinləmə texnikasının aşkarlanması üzrə mütəxəssisə mane olmamalıdır;
- Otaqda mümkün qədər radioelektron qurğular, kompüterlər, televizorlar, maqnitofonlar olmamalıdır;

Bundan əlavə, şəffaf, üzvü şüşədən və plastikdən hazırlanmış kabinədə danışıqların keçirilməsi üsulu da məlumdur. Bu, onun üçün edilmişdir ki, istənilən kənar (şəffaf olmayan) predmeti, həmçinin kimsə tərəfindən qoyulmuş qulaqasma aparatını dərhal seçmək mümkün olsun. Belə kabinədə bütün predmetlər, həmçinin mebel də şəffaf plastikdən hazırlanır.

Mühafizə üsulunu seçərkən yadda saxlamaq lazımdır ki, obyektdaxili rejimin qorunması ilə yüksək effektə nail olmaq mümkündür.

Telefon danışıqlarının təhlükəsizliyinin təmin olunması.

Cəmiyyətin kommunikasiya texnologiyaları dövründə telefon danışıqlarının tam mühafizəsi problemi aktual məsələyə çevrilir, belə ki, cinayətkarlar xidməti və şəxsi telefonlara

qulaq asmaqla məşğul olurlar. Belə hallarda telefon xətlərinə qoşulma, yüksək tezlikli qoşulmalar və digər dinləmə üsullarından tez-tez istifadə edilir. Ən çox telefon radioqoşmalarından istifadə olunur.

Telefon radioqoşması binada telefon danışıqları nəzarət olunmalı yerlərə quraşdırılır. Bunun üçün telefon radioqoşması bilavasitə telefon aparatına, telefon rozetkasına, və otağın istənilən yerində telefon naqilinə, otaqdan kənarda isə binanın bölüşdürücü qutusuna qoşula bilər. Bundan əlavə, telefon qovşağı (Telefon stansiyası) da zəif nöqtə hesab oluna bilər, belə ki, radioqoşmaları birbaşa telefon qovşağında da quraşdırmaq mümkündür.

Baş verə biləcək halların çox olması telefon danışıqlarının mühafizəsinin mümkün tədbirlərini və üsullarını müəyyən edir. Aydındır ki, telefon rabitə kanalının təhlükəsizliyini təmin etmək çətin və bahadır. Telefon kanalları ilə ötürülən mesajları bağlayan qurğulardan istifadə etmək, ya danışıqların konfidensiallığını və ya məxfiliyini təmin edən təşkilati tədbirlər görmək iqtisadi baxımdan daha əlverişlidir.

Telefon danışıqlarının dinlənilməsi ilə mübarizə üsullarından sadəsi, həmçinin də mühüm olanı telefon danışıqlarının həyata keçirilməsi zamanı ciddi intizamın təmin edilməsi tədbiridir. Xarici telefon əlaqəsi ilə müəyyən qrup insan məşğul olmalıdır. Danışıqlar zamanı təşkilatların, müəssisələrin, vəzifəli şəxslərin adları və digər vacib məlumatlar hallanmamalıdır. Telefonla tapşırıqların, göstərişlərin, müəssisənin və təşkilatın vəziyyəti haqqında məlumatların verilməsi qadağan olunmalıdır.

Bundan əlavə, təşkilati tədbirlərin də görülməsi vacibdir. Məsələn, binaların və otaqların telefon xətlərinin çəkilməsi zamanı planlaşdırmaq lazımdır ki, onlara nəzarət etmək rahat, dinləmə imkanından istifadə etmək çətin olsun. Telefon xətləri keçirilərkən onların paralel çəkilməsi və bir-biri ilə kəsişməsini minimal həddə çatdırmaq lazımdır.

Kənar qoşulmaları vaxtında müəyyən etmək üçün rabitəyə cavabdeh əməkdaşlar telefon xətlərinin vəziyyətinə daim nəzarət etməlidirlər. Danışıqların eşidilməsinin dəyişməsi və küylərin, xışıltıların, tıqqıltıların olması dərhal nəzərə alınmalıdır. Belə olan halda telefon aparatı xətdən tamam ayrılmalıdır ki, bütün dinlənilmə ehtimalları sıfra endirilsin.

Danışıqların dinlənilməsi ilə mübarizədə daha bir effektli tədbir məxfi danışıqların aparılması üçün skrembler və nitqin maskiratorudur. Skrembler – naqillə və radioəlaqə ilə dinlənilə bilən məlumatların gizlədilməsi üçün avtonom və ya qoşulmuş qurğudur.

Fəsil üzrə yoxlama sualları

Qeyd olunan fikrin səhv və ya düz olduğunu müəyyənləşdirin

	Düz	Səhv
1. Vizual-optik kanalla da informasiyanın sızması həyata keçə bilər	☐	☐
2. İnsan nitqinin tezliyi 20 – 20000 Hs aralılığındadır.	☐	☐
3. Divarların və tavanların üzlənməsi üçün xüsusi hermetik akustik panellərdən istifadə etməklə elektromaqnit kanallarla sızmadan mühafizə olunmaq olar.	☐	☐

Test suallarını cavablandırın:

1. Elektromaqnit sızma kanalları necə təsnif olunur?

a) Yaranmasına görə
b) Şüalanma diapazonuna görə
c) Yayılma mühitinə görə
d) Tezliyinə görə

2. İnformasiyanın sızma kanallarının yaranma səbəbləri hansılardır

a) Ehtiyatsız davranma
b) Tətbiq olunan sxemlərin mükəmməl olmaması
c) Elementlərin istismar baxımından köhnəlməsi
d) İnformasiyanın kənar şəxslərin əlinə keçməsi

3. Danışıqlara qulaq asma əsasən hansı yollarla həyata keçirilə bilər?

a) Bilavasitə
b) Vizual
c) Maddi-materialın köməyi ilə
d) Texniki vasitələrin köməyi ilə

Açıq sualların cavablarını əhatəli qeyd edin:

1.Lifli optik xətlərdə və rabitə sistemlərində sızmadan mühafizə necə həyata keçirilir?

_____
_____
_____
_____
_____

2. Əməkdaşlığa məcbur etmə necə həyata keçirilir?_____
_____
_____
_____
_____
_____

TERMİNLƏR

Açıq informasiya– əldə olunması, işlənməsi, verilməsi və ya istifadəsi Azərbaycan Respublikasının qanunvericiliyi ilə məhdudlaşdırılmayan və ümumi istifadə üçün təyin olunmuş sənədləşdirilmiş informasiya;

Biometrik identifikasiya – biometrik informasiya ehtiyatında verilmiş biometrik məlumatın mənsub olduğu şəxsin müəyyənləşdirilməsi üçün aparılan sorğu–axtarış işləri üzrə tədbirlər;

Biometrik informasiya – identifikasiya və verifikasiya məqsədi ilə informasiya sistemlərində toplanılan, saxlanılan, işlənilən və ötürülən biometrik məlumatlar;

Biometrik informasiya ehtiyatı – fərdi məlumatların informasiya ehtiyatlarının tərkibində biometrik məlumatlar olan resurslar;

Biometrik informasiya xidmətləri – biometrik informasiya ehtiyatlarının müəyyən olunmuş istiqamətlərdə toplanılması, işlənilməsi və mübadiləsi üzrə fəaliyyət.

Biometrik məlumatlar – identifikasiya edilmiş və ya identifikasiya olunan fiziki şəxsin fizioloji xüsusiyyətlərini xarakterizə edən, onu birmənalı və ya digər məlumatlarla uzlaşdıraraq identifikasiya etməyə imkan verən (əl–barmaq və ovuc izləri, üz təsviri, gözün qüzehli və tor qişası, səs fraqmenti və onun akustik parametrləri, dezoksiribonuklein turşusu (DNT) analizinin nəticələri, bədən ölçüləri, bədənin xüsusi əlamətlərinin və qüsurlarının təsviri, yazı xətti və imzası və s.), müvafiq standartlar tətbiq olunan və maddi daşıyıcıda əks etdirilən fərdi məlumatlar;

Biometrik məlumatların subyekti – barəsində biometrik məlumatların toplanılması, işlənilməsi və mühafizəsi həyata keçirilən identifikasiya edilmiş və ya identifikasiya olunan fiziki şəxs;

Biometrik texnologiyalar – informasiya prosesləri zamanı istifadə edilən biometrik məlumatlarla əlaqədar olan informasiya texnologiyaları;

Biometrik verifikasiya – verilmiş biometrik məlumatla biometrik informasiya ehtiyatında olan biometrik məlumatın müqayisəsi üzrə tədbirlər;

Cinayətkar (pis niyyətli şəxs) – İnformasiya prosesinin normal fəaliyyətini pozmaq məqsədi ilə ona təsir göstərən subyekt;

Dövlət sirri – dövlətin hərbi, xarici–siyasi, iqtisadi, kəşfiyyat, əks–kəşfiyyat və əməliyyat–axtarış fəaliyyəti ilə bağlı olub, dövlət tərəfindən mühafizə edilən və yayılması Azərbaycan Respublikasının təhlükəsizliyinə ziyan vura bilən məlumatlardır;

Dövlət sirri ilə işləməyə buraxılma – vətəndaşların dövlət sirri təşkil edən məlumatlarla tanış olmağa, müəssisə, idarə və təşkilatların isə belə məlumatlardan istifadə etməklə işlərin icrasına buraxılması hüququnun rəsmiləşdirilməsi qaydasıdır;

Dövlət sirri təşkil edən məlumatların daşıyıcıları – dövlət sirri təşkil edən məlumatların rəmzlər, obrazlar, siqnallar, texniki qərarlar və proseslər şəklində əks olunduğu maddi obyektlər, o cümlədən fiziki sahələrdir;

Dövlət sirri təşkil edən məlumatların siyahısı – müvafiqliyinə görə məlumatların qanunvericiliklə müəyyən olunmuş əsaslarla və qaydada dövlət sirrinə aid edildiyi və məxfiləşdirildiyi məlumat qruplarının məcmusudur.

Dövlət sirri təşkil edən məlumatlarla tanış olmağa buraxılma – səlahiyyətli vəzifəli şəxsin icazəsi ilə konkret şəxsin dövlət sirri təşkil edən məlumatlarla tanış olması qaydasıdır;

Dövlət sirrinin mühafizəsi sistemi – dövlət sirrini mühafizə orqanlarının, dövlət sirri təşkil edən məlumatların və həmin məlumatların daşıyıcılarının mühafizəsi üçün bu

orqanların istifadə etdikləri vasitə və metodların, habelə bu məqsədlə həyata keçirilən tədbirlərin məcmusudur;

Feldyeger rabitəsi xidməti – xüsusi kuryerlərin köməyi ilə əhəmiyyətli və gizli sənədlərin göndərilməsi ilə məşğul olan xüsusi xidmət;

Fərdi məlumat (şəxsi və ailə həyatına dair məlumat) – şəxsiyyəti birbaşa və ya dolayısı ilə identikləşdirməyə imkan verən hadisələr, fəaliyyətlər, vəziyyətlər barədə faktlar, rəylər, bilgilər;

İctimai informasiya – qanunlarla və ya digər normativ hüquqi aktlarla müəyyənləşdirilən ictimai vəzifələrin yerinə yetirilməsi prosesində yaradılan və ya əldə edilən faktlar, rəylər, bilgilər;

İctimai maraq – cəmiyyətin sabitliyi, əmin–amanlığı, təhlükəsizliyi və dayanıqlı inkişafı, dövlətin idarə olunmasında aşkarlığın təmin olunması ilə bağlı ayrı–ayrılıqda hər kəsin, bütövlükdə hamının bilgiləndirilməsini zəruri edən meyar.

İnformasiya – yaranma tarixindən, təqdimat formasından və təsnifatından asılı olmayaraq istənilən fəaliyyət nəticəsində yaradılan, yaxud əldə olunan faktlar, rəylər, xəbərlər və ya digər xarakterli məlumatlar;

İnformasiya ehtiyatları – informasiya sistemlərində (kitabxanalarda, arxivlərdə, fondlarda, məlumat banklarında və s.), habelə ayrıca mövcud olan sənədlər və sənəd toplusu;

İnformasiya xidmətləri – sorğu ilə müraciət edən hər kəsi informasiya ilə təmin etmək üçün göstərilən fəaliyyət;

İnformasiya istifadəçisi – informasiya əldə etmək, yaxud informasiya ilə işləməyə buraxılmaq üçün səlahiyyətli orqanlara yazılı sorğu verən fiziki və ya hüquqi şəxs;

İnformasiya məhsulları – istifadəçilərin tələblərinə əsasən yaradılmış və onların tələbatlarının ödənilməsi üçün təyin olunmuş və ya tətbiq edilən sənədləşdirilmiş informasiya, informasiya sistemləri, texnologiyaları və onların təminat vasitələri;

İnformasiya prosesləri– informasiyanın yaradılması, yığılması, işlənməsi, saxlanması, axtarışı, yayılması;

İnformasiya sahəsi (mühiti) – İnformasiyanın yaradılması, çevrilməsi və istifadəsi ilə bağlı subyektlərin fəaliyyət sahəsi;

İnformasiya sahibi – informasiya əldə etmək hüququnu təmin etmək üçün dövlət orqanları, bələdiyyələr, mülkiyyət növündən asılı olmayaraq yaradılmış hüquqi şəxslər və fiziki şəxslər;

İnformasiya sistemi – informasiya texnologiyaları və sənədlərinin təşkilati və texniki qaydada, o cümlədən hesablama texnikasından istifadə edilməklənizamlanmış məcmusu;

İnformasiya sistemləri texnologiyaları, ehtiyatları və onların təminat vasitələrinin sahibi – göstərilən obyektlər üzərində qanunla müəyyən olunmuş qaydada sahiblik və istifadə hüququnu həyata keçirən subyekt;

İnformasiya sistemləri və texnologiyalarının təminat vasitələri – informasiya sistemlərinin və texnologiyalarının yaradılması zamanı hazırlanan və onların istismarını təmin edən proqram, texniki, linqvistik, hüquqi, təşkilati vasitələr;

İnformasiya sistemləri, texnologiyaları, ehtiyatları və onların təminat vasitələrinin mülkiyyətçisi – göstərilən obyektlər üzərində tam sahiblik, istifadə, sərəncam vermə hüququnu həyata keçirən subyekt;

İnformasiya sorğusu – informasiya əldə etmək üçün yazılı və ya şifahi müraciət;

İnformasiya sorğusu verən (bundan sonra – sorğucu) informasiya əldə etmək üçün yazılı və ya şifahi şəkildə müraciət edən hüquqi və ya fiziki şəxs;

İnformasiya texnologiyaları – informasiya prosesləri zamanı, o cümlədən hesablama və rabitə texnikasının tətbiqi ilə istifadə edilən üsul və vasitələr sistemi;

İnformasiya təhlükəsizliyi – Daxili və xarici təhlükələrdən insanların, cəmiyyətin və dövlətin strateji maraqları mühafizə səviyyəsi;

İnformasiyalaşdırma – informasiya ehtiyatlarının formalaşdırılması, təqdim edilməsi, istifadə olunması əsasında dövlət hakimiyyəti və yerli özünüidarə orqanlarının, təşkilati–hüquqi və mülkiyyət formasından asılı olmayaraq bütün müəssisə, idarə və təşkilatların, vətəndaşların informasiya tələbatlarının və bu sahədəki hüquqlarının təmin edilməsinin optimal şəraitinin yaradılması üçün təşkilati, sosial–iqtisadi və elmi–texniki proses.

İnformasiyanın istifadəçisi – özü üçün zəruri informasiyanın alınması məqsədi ilə bilavasitə informasiya sisteminə və ya vasitəçiyə müraciət edən və ondan yalnız yararlanmaq hüququna malik olan subyekt;

İnformasiyanın kütləyə açıqlanması – informasiyanın sorğu verilmədən kütləvi informasiya vasitələrində, rəsmi nəşrlərdə, sorğu və ya məlumat kitabçalarında yayılması, İnternet informasiya ehtiyatlarında yerləşdirilməsi, brifinqlərdə, mətbuat relizlərində və ya konfranslarında elan edilməsi, rəsmi və ya kütləvi tədbirlərdə bildirilməsi.

İnformasiyanın mühafizə vasitələri – gizli məlumatların mühafizəsi üçün nəzərdə tutulan texniki, kriptoqrafik, proqramlı və başqa vasitələr, onların əks olunduğu vasitələr, habelə məlumatın mühafizəsinin səmərəliliyinə nəzarət vasitələridir;

İnternet informasiya ehtiyatı – internet şəbəkəsində yaradılan, informasiyanın yayılması üçün istifadə olunan, müraciət edilməsi üçün domen adına və sahibi tərəfindən müəyyənləşdirilmiş digər işarələnməyə malik olan informasiya ehtiyatı;

İnternet informasiya ehtiyatının sahibi – internet informasiya ehtiyatından istifadə edilməsi, o cümlədən burada informasiya yerləşdirilməsi qaydalarını sərbəst olaraq müəyyən

edən, internet informasiya ehtiyatına sahiblik və istifadə hüquqlarına malik olan şəxs;

Kommersiya sirri – hüquqi və fiziki şəxslərin istehsal, texnoloji, idarəetmə, maliyyə və başqa fəaliyyəti ilə bağlı, sahibinin razılığı olmadan açıqlanması, onların qanuni maraqlarına ziyan vura bilən məlumatlar;

Kommersiya sirrini yaymaq – müvafiq qanunvericiliyin, yaxud müqavilə şərtlərinin pozulması yolu ilə kommersiya sirrinin başqa şəxslərə açıqlanması;

Kommersiya sirrinin daşıyıcıları – kommersiya sirrinin işarələr, təsvirlər, düsturlar, texnoloji proseslər, siqnallar və başqa formada ifadə edildiyi maddi və qeyri–maddi obyektlər;

Kommersiya sirrinin əldə olunmasının qeyri–qanuni üsulları – kommersiya sirrinin sənədləri oğurlamaq, fotoşəklini çəkmək, surətini çıxarmaq, zor tətbiq etmək və ya hədələmək, rüşvət vermək, kommersiya sirrinin rejiminə riayət olunması öhdəliklərini pozmaq və ya pozmağa təhrik (vadar) etmək, məlumatların ötürülmə kanallarına qoşulmaq, danışıqlara qulaq asmaq və müşahidə aparmaq kimi qeyri–qanuni üsullarla əldə edilməsi.

Kommersiya sirrinin konfidenti – kommersiya sirrini qanuni əsaslarla kommersiya sirrinin sahibindən əldə edən hüquqi və ya fiziki şəxs;

Kommersiya sirrinin rejimi – kommersiya sirrinin əldə edilməsinin məhdudlaşdırılması üzrə kommersiya sirrinin sahibi və ya konfident tərəfindən müəyyən olunmuş hüquqi, təşkilati, texniki və digər tədbirlər sistemi;

Kommersiya sirrinin sahibi – kommersiya sirrinə qanuni əsaslarla malik olan hüquqi və ya fiziki şəxs;

Konfidensial informasiya– vətəndaşların, mülkiyyət növündən asılı olmayaraq yaradılmış idarə, müəssisə və təşkilatların, digər hüquqi şəxslərin qanuni maraqlarının qorunması məqsədi ilə əldə olunmasına məhdudiyyət qoyulan

məlumatlar, habelə peşə (həkim, vəkil, notariat), kommersiya, istintaq və məhkəmə sirləri;

Məxfilik qrifi – məlumat daşıyıcısının özündə və ya ona qoşulan sənədlərdə qoyulan, daşıyıcısı olduğu məlumatın məxfilik dərəcəsini göstərən rekvizitlərdir;

Məlumat – təbiətdə və cəmiyyətdə baş verən hadisələr, proseslər, təzahürlər, fəaliyyətlər və əşyalar barədə faktlar, rəylər, bilgilər;

Məlumat toplularının hüquqi qorunması – məlumat toplularının quruluşunun müəlliflik hüququ və məzmununun xüsusi qorunma hüququ ilə bir–birindən asılı olmayan ikili qorunma forması;

Məlumat toplusunun dərc edilməsi – məlumat toplusunun kompüterin yaddaşına yazılması və çap mətninin buraxılması da daxil olmaqla nüsxələrin sayının zəruri ehtiyacları ödəməsi şərti ilə əhalinin qeyri–müəyyən dairəsinə təqdim edilməsi;

Məlumat toplusunun istifadəsi – məlumat toplusunun surətçıxarılması, dərc edilməsi, kütləvi nümayişi, ifası və bildirişi, yayılması, o cümlədən onun yenidən işlənməsi (modifikasiyası) və mülki dövriyyəyə buraxılması üzrə digər hərəkətlər. Dərc edilmiş məlumat toplusu barədə kütləvi informasiya vasitələrində məlumat verilməsi onun istifadəsi sayılmır;

Məlumat toplusunun kütləvi nümayişi və ifası – məlumat toplusunun əhalinin qeyri–müəyyən dairəsinin qavramasını mümkün edən istənilən nümayiş və ifa formasında təqdim edilməsi;

Məlumat toplusunun surətçıxarılması – məlumat toplusunun bir və ya daha çox nüsxədə hər hansı maddi daşıyıcıya köçürülməsi, o cümlədən kompüterin yaddaşına yazılması;

Məlumat toplusunun yenidən işlənməsi (modifikasiyası) – məlumat toplusunun uyğunlaşdırılmasına aid olmayan digər dəyişikliklərin aparılması;

Məlumat toplusunun yayılması – məlumat toplusunun orijinalının və nüsxələrinin satış və ya mülkiyyət hüququnun başqa yolla verilməsi ilə kütləyə çatdırılması;

Məlumat toplusu – sistemli və ya metodik qaydada tərtib edilmiş və elektron, yaxud digər vasitələrlə əldə oluna bilən əsərlərin, verilənlərin və digər materialların təqdiminin obyektiv forması;

Məlumat toplusununkütləvi bildirişi (kütləyə çatdırmaq məqsədilə bildirişi) – məlumat toplusunun naqil və ya naqilsiz rabitə vasitələri ilə hər hansı üsulla kütləvi bildirişi, o cümlədən elə tərzdə kütləyə çatdırılması ki, hər kəs öz seçiminə uyğun olaraq istənilən yerdə və istənilən vaxtda bu toplunu əldə edə bilsin;

Məlumat toplusununuyğunlaşdırılması (adaptasiyası) – istifadəçinin konkret texniki avadanlığında və ya istifadə etdiyi proqrama uyğun işləməsini təmin etmək məqsədilə məlumat toplusunda dəyişikliklərin aparılması;

"Nou–hau" – əqli fəaliyyətin nəticəsi kimi kommersiya sirrinə aid edilən, qanunvericiliyə, yaxud sahibinin mülahizələrinə əsasən patentlə mühafizə olunmayan məlumatlar;

Səlahiyyətli orqan – informasiya ehtiyatlarına sahiblik, istifadə və sərəncam vermək hüququ olan dövlət orqanları, bələdiyyələr, dövlət büdcəsindən tam və ya qismən maliyyələşən hüquqi şəxslər;

Sənədləşdirilmiş informasiya (sənəd) – maddi daşıyıcıda mətn, səs və ya təsvir formasında qeydə alınan və identikləşdirməyə imkan verən istənilən rekvizitli informasiya mənbəyindən, saxlanma yerindən, rəsmi statusundan, mülkiyyət növündən, mənsub olduğu təşkilat tərəfindən

yaradılıb-yaradılmamasından asılı olmayaraq sənədləşdirilmiş informasiya;

Texniki mühafizə vasitələri – məlumat toplusuna daxilolmanı nəzarətdə saxlayan, hüquq sahibinin və ya istehsalçının icazə vermədiyi hərəkətlərin qarşısını alan, yaxud məhdudlaşdıran istənilən texniki qurğular və ya onların hissələri.

ƏLAVƏLƏR

İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında

Azərbaycan Respublikasının Qanunu

I fəsil

ÜMUMI MÜDDƏALAR

Maddə 1. **Qanunun təsir dairəsi**

Bu Qanun informasiyanın yığılması, işlənməsi, saxlanması, axtarışı, yayılması əsasında informasiya ehtiyatlarının formalaşdırılması, informasiya sistemləri, texnologiyaları, onların təminat vasitələrinin yaradılması və onlardan istifadə olunması, informasiyanın mühafizəsi ilə əlaqədar olaraq yaranan münasibətləri tənzimləyir və informasiya proseslərində iştirak edən subyektlərin hüquqlarını müəyyən edir.

Bu Qanun "Kütləvi informasiya vasitələri haqqında" və "Müəlliflik hüququ və əlaqəli hüquqlar haqqında" Azərbaycan Respublikasının qanunları ilə tənzimlənən münasibətlərə şamil edilmir.

Maddə 2. **Əsas anlayışlar**

Qanunda aşağıdakı anlayışlar işlədilmişdir:

informasiya – yaranma tarixindən, təqdimat formasından və təsnifatından asılı olmayaraq istənilən fəaliyyət nəticəsində yaradılan, yaxud əldə olunan faktlar, rəylər, bilgilər, xəbərlər və ya digər xarakterli məlumatlar;

sənədləşdirilmiş informasiya (sənəd) – maddi daşıyıcıda mətn, səs və ya təsvir formasında qeydə alınan və identikləşdirməyə imkan verən istənilən rekvizitli informasiya

mənbəyindən, saxlanma yerindən, rəsmi statusundan, mülkiyyət növündən, mənsub olduğu təşkilat tərəfindən yaradılıb-yaradılmadığından asılı olmayaraq sənədləşdirilmiş informasiya;

açıq informasiya – əldə olunması, işlənməsi, verilməsi və ya istifadəsi Azərbaycan Respublikasının qanunvericiliyi ilə məhdudlaşdırılmayan və ümumi istifadə üçün təyin olunmuş sənədləşdirilmiş informasiya;

konfidensial informasiya – vətəndaşların, mülkiyyət növündən asılı olmayaraq yaradılmış idarə, müəssisə və təşkilatların, digər hüquqi şəxslərin qanuni maraqlarının qorunması məqsədilə əldə olunmasına məhdudiyyət qoyulan məlumatlar, habelə peşə (həkim, vəkil, notariat), kommersiya, istintaq və məhkəmə sirləri;

informasiya prosesləri – informasiyanın yaradılması, yığılması, işlənməsi, saxlanması, axtarışı, yayılması;

informasiya texnologiyaları – informasiya prosesləri zamanı, o cümlədən hesablama və rabitə texnikasının tətbiqi ilə istifadə edilən üsul və vasitələr sistemi;

informasiya sistemi – informasiya texnologiyaları və sənədlərinin təşkilati və texniki qaydada, o cümlədən hesablama texnikasından istifadə edilməklə, nizamlanmış məcmusu;

informasiya ehtiyatları – informasiya sistemlərində (kitabxanalarda, arxivlərdə, fondlarda, məlumat banklarında və s.) olan sənədlər və sənəd massivləri, habelə ayrıca mövcud olan sənədlər və onların massivləri;

internet informasiya ehtiyatı– internet şəbəkəsində yaradılan, informasiyanın yayılması üçün istifadə olunan, müraciət edilməsi üçün domen adına və sahibi tərəfindən müəyyənləşdirilmiş digər işarələnməyə malik olan informasiya ehtiyatı;

internet informasiya ehtiyatının sahibi– internet informasiya ehtiyatından istifadə edilməsi, o cümlədən burada

informasiya yerləşdirilməsi qaydalarını sərbəst olaraq müəyyən edən, internet informasiya ehtiyatına sahiblik və istifadə hüquqlarına malik olan şəxs;

domen adı– internet şəbəkəsində yerləşdirilən informasiya ehtiyatına müraciətin təmin olunması üçün verilən unikal simvol düzülüşü;

domen adının sahibi– müqaviləyə əsasən domen adına müddətli sahiblik edən şəxs;

internet provayder– internet şəbəkəsinə telekommunikasiya vasitələri ilə qoşulmaq üçün texniki imkanı təmin edən təchizatçı;

host provayder– internet informasiya ehtiyatının istifadəsinin təmin edilməsi üçün öz informasiya sistemlərində yerləşdirilməsi xidmətini göstərən təchizatçı;

domen adlarının milli inzibatçısı– "az" ölkə kodlu yüksək səviyyəli domen zonasında domen adlarının inzibatçılığını həyata keçirən səlahiyyətli şəxs;

domen adlarının qeydiyyatçısı– domen adların milli inzibatçısı ilə bağlanılmış müqaviləyə əsasən "az" ölkə kodlu yüksək səviyyəli domen zonasında domenlərin qeydiyyatı üzrə xidmət göstərən şəxs;

informasiya sistemləri və texnologiyalarının təminat vasitələri – informasiya sistemlərinin və texnologiyalarının yaradılması zamanı hazırlanan və onların istismarını təmin edən proqram, texniki, linqvistik, hüquqi, təşkilati vasitələr;

informasiya sistemləri, texnologiyaları, ehtiyatları və onların təminat vasitələrinin mülkiyyətçisi – göstərilən obyektlər üzərində tam sahiblik, istifadə, sərəncamvermə hüququnu həyata keçirən subyekt;

informasiya sistemləri texnologiyaları, ehtiyatları və onların təminat vasitələrinin sahibi – göstərilən obyektlər üzərində qanunla müəyyən olunmuş qaydada sahiblik və istifadə hüququnu həyata keçirən subyekt;

informasiyanın istifadəçisi – özü üçün zəruri informasiyanın alınması məqsədilə bilavasitə informasiya sisteminə və ya vasitəçiyə müraciət edən və ondan ancaq istifadə hüququna malik subyekt;

informasiya məhsulları – istifadəçilərin tələblərinə əsasən yaradılmış və onların tələbatlarının ödənilməsi üçün təyin olunmuş və ya tətbiq edilən sənədləşdirilmiş informasiya, informasiya sistemləri, texnologiyaları və onların təminat vasitələri;

informasiya xidmətləri – istifadəçilərin informasiya məhsulları ilə təmin edilməsi üzrə subyektlərin (mülkiyyətçilər, sahiblər və ya vasitəçilərin) fəaliyyəti;

informasiyalaşdırma – informasiya ehtiyatlarının formalaşdırılması, təqdim edilməsi, istifadə olunması əsasında dövlət hakimiyyəti və yerli özünüidarə orqanlarının, təşkilati-hüquqi və mülkiyyət formasından asılı olmayaraq bütün müəssisə, idarə və təşkilatların, vətəndaşların informasiya tələbatlarının və bu sahədəki hüquqlarının təmin edilməsinin optimal şəraitinin yaradılması üçün təşkilati, sosial-iqtisadi və elmi-texniki proses.

Maddə 3. **İnformasiyalaşdırma sahəsində dövlət siyasəti**

İnformasiyalaşdırma sahəsində dövlət siyasətinin əsas istiqamətləri aşağıdakılardan ibarətdir:

- milli informasiya fəzasının formalaşdırılması;
- informasiyalaşdırma üzrə fəaliyyətin başlıca istiqamətlərinin təyini və meydana çıxan münasibətlərin tənzimlənməsi;
- informasiya ehtiyatları, sistemləri, texnologiyaları və onların təminat vasitələri üzərində mülkiyyətin bütün formalarının inkişafına, informasiya məhsulları və xidmətləri bazarının formalaşmasına yardım edilməsi;

- dövlət informasiya ehtiyatlarının formalaşdırılması və mühafizəsi üçün zəruri olan şəraitin yaradılması;
- ərazi informasiya şəbəkələrinin yaradılması, onların beynəlxalq informasiya şəbəkələri ilə uzlaşması, qarşılıqlı əlaqəsinin təmin edilməsi üçün lazımi təşkilati, hüquqi, texniki siyasətin təyin edilməsi;
- dövlət informasiya ehtiyatları əsasında dövlət hakimiyyəti və yerli özünüidarə orqanları, təşkilati-hüquqi və mülkiyyət formasından asılı olmayaraq bütün müəssisə, idarə və təşkilatların, vətəndaşların müvafiq informasiya ilə təmin olunması üçün şərait yaradılması;
- informasiya fəzasında milli təhlükəsizliyin təmin edilməsi;
- informasiya məhsulları və xidmətləri bazarında informasiya münasibətlərinin subyektləri, o cümlədən xarici subyektlər tərəfindən inhisar fəaliyyəti və haqsız rəqabətin qarşısının alınması və yol verilməməsi;
- informasiyalaşdırma mühitində dövlət hakimiyyəti və yerli özünüidarə orqanlarının, təşkilati-hüquqi və mülkiyyət formasından asılı olmayaraq bütün müəssisə, idarə və təşkilatların, vətəndaşların hüquqlarının təmin olunması;
- informasiyalaşdırma mühitində elmi-texniki və istehsal siyasətinin formalaşdırılması və həyata keçirilməsi;
- informasiyalaşdırma layihələri və proqramlarının dəstəklənməsi, onların işlənməsi və həyata keçirilməsi üçün investisiyaların cəlb olunması sisteminin və stimullaşdırma mexanizminin yaradılması;
- informasiya prosesləri, informasiyalaşdırma və informasiyanın mühafizəsi sahəsində hüquqi bazanın inkişaf etdirilməsi.

II fəsil

İNFORMASİYA EHTİYATLARI

Maddə 4. **İnformasiya ehtiyatlarının hüquqi rejimi**

İnformasiya ehtiyatları fiziki, hüquqi şəxslərin və dövlətin münasibət obyektləridir. Onlar Azərbaycan Respublikasının informasiya ehtiyatları hesab olunur və digər ehtiyatlar kimi qanunla qorunur.

İnformasiya ehtiyatlarının hüquqi rejimi aşağıdakı normalarla müəyyən edilir:

- informasiyanın sənədləşdirilməsi qaydaları;
- sənəd və sənəd massivləri üzərində mülkiyyət hüququ;
- işləməyə buraxılmaq növünə görə informasiyanın kateqoriyaları;
- informasiyanın mühafizə olunmasının hüquqi qaydaları.

Maddə 5. **İnformasiyanın sənədləşdirilməsi**

İnformasiyanın sənədləşdirilməsi onun informasiya ehtiyatlarına daxil edilməsinin mütləq şərtidir. İnformasiyanın sənədləşdirilməsi Azərbaycan Respublikasının təhlükəsizliyi, kargüzarlıq, sənəd və sənəd massivlərinin standartlaşdırılması məsələlərinin təşkilinə cavabdeh olan müvafiq icra hakimiyyəti orqanlarının müəyyən etdiyi qaydalar əsasında həyata keçirilir.

Azərbaycan Respublikası qanunvericiliyinə müvafiq surətdə informasiya sistemlərindən, o cümlədən avtomatlaşdırılmış sistemlərdən alınmış sənəd vəzifəli şəxs tərəfindən imzalandıqdan sonra hüquqi qüvvəyə malik olur.

İnformasiya və telekommunikasiya sistemlərində dövr edən sənəd elektron imzası vasitəsilə də təsdiq edilə bilər.

Maddə 6. **İnformasiya ehtiyatları, sistemləri, texnologiyaları və onların təminat vasitələri üzərində mülkiyyət hüququ**

İnformasiya ehtiyatları, sistemləri, texnologiyaları və onların təminat vasitələri üzərində mülkiyyətin Azərbaycan Respublikası qanunvericiliyində nəzərdə tutulmuş bütün formalarına yol verilir.

Fiziki və hüquqi şəxslər onların vəsaitləri hesabına yaradılmış, qanuni yolla əldə edilmiş, yaxud bağışlama, vərəsəlik qaydasında toplanmış informasiya ehtiyatlarının, informasiya sistemlərinin, texnologiyalarının və onların təminat vasitələrinin mülkiyyətçisidirlər.

Azərbaycan Respublikasının büdcə vəsaitləri və dövlət idarə, müəssisə və təşkilatlarının vəsaitləri hesabına yaradılan, əldə edilən, toplanan informasiya ehtiyatları, sistemləri, texnologiyaları və onların təminat vasitələri dövlət mülkiyyətidir.

İnformasiya ehtiyatları, sistemləri, texnologiyaları və onların təminat vasitələri üzərində mülkiyyət hüququnun həyata keçirilməsi qaydası Azərbaycan Respublikasının qanunvericiliyi ilə müəyyən edilir.

Sənədləşdirilmiş informasiyanı Azərbaycan Respublikasının qanunvericiliyi ilə müəyyən edilmiş qaydada icra hakimiyyəti orqanlarına müvafiq təşkilatlara təqdim edən subyektlər bu sənədlərə mülkiyyət və onlardakı informasiyadan istifadə etmək hüquqlarını itirmirlər. Bu sənədlərədövlət və onları təqdim etmiş subyektlər birgə sahiblik hüququna malikdirlər.

İnformasiya məhsulu və xidmətinin qiymətləri Azərbaycan Respublikasının qanunvericiliyinə müvafiq olaraq icra hakimiyyəti orqanları tərəfindən və ya bağlanmış müqavilələrlə müəyyən edilir.

İnformasiya proseslərində iştirak edən, informasiya məhsulu və xidmətlərini azad realizə edən bütün fiziki və

hüquqi şəxslər ümumi informasiya bazarının iştirakçıları sayılırlar.

İnformasiya istifadəçiləri, informasiya məhsul və xidmətlərinin mülkiyyətçiləri, sahibləri vasitəçilərini, informasiya növünü və işlənmə üsulunu, informasiya məhsulları və xidmətlərinin nomenklaturasını, Azərbaycan Respublikası qanunvericiliyində nəzərdə tutulmuş hallar istisna olmaqla, azad seçmək hüququna malikdirlər.

İnformasiyanın işlənmə vasitələri üzərində mülkiyyət hüququ informasiya ehtiyatları üzərində mülkiyyət hüququ yaratmır.

İşlənmə vasitələrinin birgə istifadə olunması halında ilkin sənədlər sahibə məxsus olur, törəmə məhsulun məxsusluğu isə müqavilə ilə müəyyən olunur. İnformasiya ehtiyatlarının mülkiyyətçisi onun yaratdığı informasiyanın keyfiyyətinə görə məsuliyyət daşıyır.

Dövlət sirri təşkil edən informasiya ehtiyatları ilə işləmə qaydaları və mülkiyyət münasibətləri "Dövlət sirri haqqında" Azərbaycan Respublikasının Qanununa və digər qanunvericilik aktlarına əsasən tənzimlənir.

Maddə 7. **Dövlət informasiya ehtiyatları**

Dövlət informasiya ehtiyatlarının formalaşdırılmasında dövlət hakimiyyəti və yerli özünüidarə orqanları, təşkilati-hüquqi və mülkiyyət formasından asılı olmayaraq bütün müəssisə, idarə və təşkilatlar, vətəndaşlar iştirak edə bilərlər.

Dövlət hakimiyyəti orqanları onların sərəncamında dövlət informasiya ehiyatlarını formalaşdırır və səlahiyyətləri daxilində onlardan istifadəni təmin edirlər.

Dövlət hakimiyyət orqanları və təşkilatlarının dövlət informasiya ehtiyatlarının formalaşdırılması sahəsindəki fəaliyyəti dövlət büdcəsindən, xüsusi vəsaitlərdən və digər fondlardan maliyyələşdirilir.

Maddə 8. **Dövlət informasiya ehtiyatlarının formalaşdırılması üçün sənədləşdirilmiş informasiyanın təqdim olunması**

İnformasiya ehtiyatlarının formalaşdırılması və işlənməsinə cavabdeh olan orqan və təşkilatların siyahısı, eləcə də dövlət hakimiyyəti və yerli özünüidarə orqanları, təşkilati-hüquqi və mülkiyyət formasından asılı olmayaraq bütün müəssisə, idarə və təşkilatlar, vətəndaşlar tərəfindən sənədləşdirilmiş informasiyanın təqdim olunma qaydasını müvafiq icra hakimiyyəti orqanı müəyyən edir.

Dövlət sirri təşkil edən konfidensial informasiyanın formalaşdırılma və işlənmə qaydaları Azərbaycan Respublikasının qanunvericiliyi ilə müəyyən edilir.

Maddə 9. **Milli informasiya ehtiyatları**

Dövlət hakimiyyəti və yerli özünüidarə orqanları, təşkilati-hüquqi və mülkiyyət formasından asılı olmayaraq bütün müəssisə, idarə və təşkilatlar vətəndaşların informasiya ehtiyatları və ya onların müəyyən hissələri Azərbaycan Respublikasının qanunvericiliyinə əsasən milli informasiya ehtiyatları elan edilə bilər və milli sərvət kimi mühafizə edilməlidir.

Maddə 10. **İnformasiyanın təsnifatı**

Əldə olunma növünə görə informasiya ümumi istifadə üçün açıq və alınması məhdudlaşdırılan informasiyalara bölünür. Azərbaycan Respublikasının qanunu ilə əldə olunması məhdudlaşdırılmayan informasiyalar açıq informasiyalar sayılır.

Əldə edilməsi qanunla məhdudlaşdırılan informasiyalar hüquqi rejiminə görə məxfi və gizli (konfidensial) olur. Dövlət sirri məxfi, vətəndaşların, mülkiyyət növündən asılı olmayaraq yaradılmış idarə, müəssisə və təşkilatların, digər hüquqi şəxslərin qanuni maraqlarının qorunması məqsədilə əldə

olunmasına məhdudiyyət qoyulan peşə (həkim, vəkil, notariat), kommersiya, istintaq və məhkəmə sirləri, konfidensial xarakter daşıyır. Fərdi məlumatlar daxilolma (əldə olunma) növünə görə konfidensial və açıq kateqoriyalara bölünür.

Məlumatların dövlət sirrinə aid edilməsi, istifadəsi qaydaları və mühafizəsi "Dövlət sirri haqqında" Azərbaycan Respublikasının Qanunu ilə müəyyən edilir. Konfidensial informasiyanın toplanmasına, işlənməsinə, istifadəsinə və yayılmasına yalnız Azərbaycan Respublikasının qanunvericiliyində müəyyən edilmiş hallarda yol verilə bilər.

III fəsil

İNFORMASİYA EHTİYATLARININ İSTİFADƏ OLUNMASI

Maddə 11. **İnformasiya ehtiyatları ilə işləməyə buraxılma hüququ**

Alınması məhdudlaşdırılmış sənədləşdirilmiş informasiya istisna olmaqla informasiya ehtiyatları ilə işləməyə buraxılmaqda istifadəçilər bərabər hüquqlara malikdirlər və məlumatlardan istifadə edilməsinin zəruriliyini informasiya ehtiyatlarının mülkiyyətçisi və ya sahibi qarşısında əsaslandırmağa məcbur deyillər.

İstifadəçilər tərəfindən qanuni əsaslarla informasiya ehtiyatlarından əldə olunmuş informasiyadan kommersiya məqsədləri üçün törəmə informasiya məhsulunun yaradılmasına yalnız alınma mənbəyinə istinad edilməklə istifadə olunmasına icazə verilir. Bu halda istifadəçiyə məxsus olan mənfəət dövlət informasiya ehtiyatlarından alınmış informasiyadan deyil, törəmə informasiya məhsulunun yaradılması nəticəsində olur.

İstifadəçilərə informasiya ilə işləməyə buraxılmanın qaydası, bu Qanunun tələblərinə əməl edilməklə müvafiq icra hakimiyyəti orqanı və ya mülkiyyətçi tərəfindən müəyyən edilir. Bu qaydalar və göstərilən xidmətlər haqqında məlumatların verilməsi üçün haqq alınmır.

İnformasiya ehtiyatlarından istifadə edənlərə haqqı ödənilmədən və ya xidmətlərə çəkilən xərcləri qismən ödəməklə təqdim olunan informasiya xidmətlərinin siyahısı müvafiq icra hakimiyyəti orqanı tərəfindən müəyyən olunur. Göstərilmiş xidmətlərə çəkilmiş xərclərdəki fərqin kompensasiyası dövlət büdcəsindən, xüsusi vəsaitlərdən və digər mənbələrdən ödənilir.

Maddə 12. **Fiziki və hüquqi şəxslərin özləri barəsində informasiyaya buraxılmaq hüququ**

Fiziki və hüquqi şəxslər barəsində sənədləşdirilmiş informasiyanın siyahısı və onların informasiya sistemlərində istifadə edilməsi qaydası Azərbaycan Respublikasının qanunvericiliyi ilə müəyyən edilir.

Fiziki və hüquqi şəxslər özləri barəsindəki sənədləşdirilmiş informasiyaya, Azərbaycan Respublikasının qanunvericiliyi ilə müəyyən edilmiş hallar istina edilməklə, maneəsiz olaraq buraxılmaq, bu informasiyada dəqiqləşdirmələr aparılmasını tələb etmək, informasiyadan kimlərin vəhansı məqsədilə istifadə etdiyini bilmək hüququ vardır.

Maddə 13. **İnformasiya ehtiyatları mülkiyyətçisi və ya sahibinin məsuliyyəti**

İnformasiya ehtiyatlarından istifadə qaydalarının pozulmasına, istifadəçilərin hüquqlarının əsassız olaraq məhdudlaşdırılmasına görə mülkiyyətçi və ya sahib, habelə vəzifəli şəxslər Azərbaycan Respublikasının qanunvericiliyi ilə müəyyənləşdirilmiş qaydada məsuliyyət daşıyırlar.

III-I fəsil

İNTERNET İNFORMASİYA EHTİYATLARI

Maddə 13-1. **İnternet informasiya ehtiyatının yaradılması və uçotu**

13-1.1. İnternet informasiya ehtiyatı üçün domen adı "az" ölkə kodlu yüksək səviyyəli domen zonasında və ya digər domen adları zonalarında seçilə bilər.

13-1.2. "az" ölkə kodlu yüksək səviyyəli domen adlarının qeydiyyatı domen adlarının milli inzibatçısı və qeydiyyatçıları tərəfindən həyata keçirilir. Domen adlarının milli inzibatçısı qeydiyyatdan keçmiş domen adlarının reyestrini aparır və reyestr məlumatlarından sorğu əsasında istifadəni təmin edir.

13-1.3. "az" ölkə kodlu yüksək səviyyəli domen adlarının qeydiyyatı və istifadəsi qaydaları, habelə domen adlarının reyestrinə daxil edilən məlumatlar müvafiq icra hakimiyyəti orqanı tərəfindən müəyyən edilir.

Maddə 13-2. **İnternet informasiya ehtiyatında informasiyanın yayılması**

13-2.1. İnternet informasiya ehtiyatının sahibi həmin informasiya ehtiyatında yerləşdirilən informasiyanın tərkibi və onun yerləşdirilməsi qaydasının müəyyən edilməsində müstəqildir. İnternet informasiya ehtiyatının və onun domen adının sahibi həmin informasiya ehtiyatının qanunauyğun fəaliyyətini təmin etməlidir və buna görə şəxsən məsuliyyət daşıyır.

13-2.2. İnternet informasiya ehtiyatının və onun domen adının sahibi hüquqi şəxsdirsə adı, təşkilati-hüquqi forması, elektron poçt ünvanı, fiziki şəxsdirsə adı, soyadı və atasının adı və elektron poçt ünvanı həmin saytda aydın oxuna bilən yerdə və formada yerləşdirməlidir.

13-2.3. İnternet informasiya ehtiyatının və onun domen adının sahibi həmin informasiya ehtiyatında aşağıdakı yayılması qadağan edilən informasiyanın yerləşdirilməsinə yol verməməlidir:

13-2.3.1. terrorçuluğun təbliği və maliyyələşdirilməsi, terrorçuluğun həyata keçirilməsinin üsul və vasitələri, terrorçuluq məqsədi ilə təlim təşkil etmə və ya keçirmə barədə məlumatlar, habelə terrorçuluğa açıq çağırışlar;

13-2.3.2. zorakılığın və dini ekstremizmin təbliğinə dair məlumatlar, milli, irqi və ya dini nifrət və düşmənçiliyin salınmasına, dövlətin konstitusiya quruluşunun zorla dəyişdirilməsinə, ərazi bütövlüyünün parçalanmasına, hakimiyyətin zorla ələ keçirilməsinə və ya saxlanmasına, kütləvi iğtişaşların təşkil edilməsinə yönələn açıq çağırışlar;

13-2.3.3. dövlət sirri təşkil edən məlumatlar;

13-2.3.4. odlu silahın, onun komplekt hissələrinin, döyüş sursatının, partlayıcı maddələrin və qurğuların hazırlanma qaydası və ya üsulları barədə məlumatlar;

13-2.3.5. narkotik vasitələrin, psixotrop maddələrin və onların prekursorlarının hazırlanma və ya istifadə üsulları və qaydası, onların qanunsuz əldə edilməsi yerləri, habelə tərkibində narkotik maddələr olan bitkilərin kultivasiya yerləri və ya üsulları barədə məlumatlar;

13-2.3.6. pornoqrafiyaya, o cümlədən uşaq pornoqrafiyasına aid məlumatlar;

13-2.3.7. qumar və digər qanunsuz mərc oyunlarının təşkilinə və həmin oyunlarda iştiraka təhrik edən məlumatlar;

13-2.3.8. intiharı problemlərin həlli üsulu qismində təbliğ edən, intihara bəraət qazandıran, onu əsaslandıran və ya törədilməsinə təhrik edən, intiharın törədilməsi üsullarını izah edən və ya qrup şəklində bir neçə şəxsin intihar etməsini təşkil etmək məqsədi ilə yayılan məlumatlar;

13-2.3.9. təhqir və ya böhtan xarakteri daşıyan, habelə şəxsi həyatın toxunulmazlığını pozan məlumatlar;

13-2.3.10. əqli mülkiyyət hüquqlarını pozan məlumatlar;

13-2.3.11. Azərbaycan Respublikasının qanunları ilə yayılması qadağan edilən digər informasiya.

13-2.4. İnternet informasiya ehtiyatının və onun domen adının sahibi həmin informasiya ehtiyatında yayılması qadağan edilən informasiyanın olduğunu aşkar etdikdə və ya bu barədə ona müraciət daxil olduqda, belə informasiyanın informasiya ehtiyatından götürülməsini təmin edir.

13-2.5. Host provayder öz informasiya sistemlərində yerləşdirilmiş internet informasiya ehtiyatlarında yayılması qadağan edilən informasiya aşkar etdikdə və ya ona bu barədə məlumat daxil olduqda, dərhal onun informasiya ehtiyatının sahibi tərəfindən götürülməsi üçün tədbirlər görür.

Maddə 13-3. **İnternet informasiya ehtiyatlarında yayılması qadağan edilən informasiyanın yerləşdirilməsinin qarşısının alınması**

13-3.1. Müvafiq icra hakimiyyəti orqanı yayılması qadağan edilən informasiyanın internet informasiya ehtiyatında yerləşdirilməsi hallarını bilavasitə aşkar etdikdə və ya fiziki, hüquqi şəxslərdən, yaxud dövlət qurumlarından daxil olmuş əsaslandırılmış məlumatlar əsasında müəyyən etdikdə, bu barədə internet informasiya ehtiyatının və onun domen adının sahibinə və host provayderə yazılı xəbərdarlıq edir.

13-3.2. Xəbərdarlıq edildiyi vaxtdan 8 saat ərzində yayılması qadağan edilən informasiya internet informasiya ehtiyatından götürülmədikdə müvafiq icra hakimiyyəti orqanı həmin orqanın yerləşdiyi yer üzrə rayon (şəhər) məhkəməsinə internet informasiya ehtiyatına müraciətin məhdudlaşdırılması barədə müraciət edir.

13-3.3. Dövlətin və cəmiyyətin qanunla qorunan maraqlarına təhdid yarandığı və ya insanların həyat və sağlamlığı üçün real təhlükə olduğu təxirəsalınmaz hallarda internet informasiya ehtiyatına müraciət müvafiq icra

hakimiyyəti orqanının qərarı əsasında müvəqqəti olaraq məhdudlaşdırılır.

13-3.4. Müvafiq icra hakimiyyəti orqanı bu Qanunun 13-3.3-cü maddəsində nəzərdə tutulmuş qərarı qəbul etdikdə, eyni zamanda, internet informasiya ehtiyatına müraciətin məhdudlaşdırılması barədə məhkəməyə müraciət edir. İnformasiya ehtiyatına müraciətin müvəqqəti məhdudlaşdırılması barədə qərar məhkəmə tərəfindən internet informasiya ehtiyatına müraciətin məhdudlaşdırılması barədə müraciətə baxılanadək və ya həmin qərar ləğv edilənədək qüvvədə qalır.

13-3.5. Məhkəmə internet informasiya ehtiyatına müraciətin məhdudlaşdırılması barədə müraciətə 5 günədək müddətdə baxır və qərar qəbul edir. Qərar qəbul edildikdən dərhal sonra qüvvəyə minir və qərardan şikayətin verilməsi onun icrasını dayandırmır.

13-3.6. Məhkəmə internet informasiya ehtiyatına müraciətin məhdudlaşdırılması haqqında, müvafiq icra hakimiyyəti orqanı isə internet informasiya ehtiyatına müraciətin müvəqqəti məhdudlaşdırılması barədə qərar qəbul etdikdə, müvafiq icra hakimiyyəti orqanı həmin informasiya ehtiyatını "Yayılması qadağan edilən informasiyanın yerləşdirildiyi informasiya ehtiyatlarının Siyahısı"na daxil edir. Siyahıdakı məlumatların tərkibi, siyahının tərtibi, tətbiqinə nəzarət edilməsi və host və internet provayderlərlə qarşılıqlı əlaqənin təşkil edilməsi qaydaları müvafiq icra hakimiyyəti orqanı tərəfindən müəyyən edilir.

13-3.7. İnternet informasiya ehtiyatı "Yayılması qadağan edilən informasiyanın yerləşdirildiyi informasiya ehtiyatlarının Siyahısı"na daxil edildikdən dərhal sonra host provayder və internet provayderlər internet informasiya ehtiyatına müraciəti məhdudlaşdırmalı və bu barədə internet informasiya ehtiyatının sahibinə məlumat verməlidirlər.

13-3.8. İnternet informasiya ehtiyatının sahibi məlumatın götürülməsini bu Qanunun 13-2.4-cü maddəsində nəzərdə tutulmuş qaydada təmin etmədikdə və informasiyanın internet informasiya ehtiyatında yayılmasının qadağan edilməsi ilə əlaqədar qüvvəyə minmiş məhkəmə qərarı mövcud olduqda, müvafiq icra hakimiyyəti orqanı həmin informasiya ehtiyatını şəxsin müraciəti əsasında "Yayılması qadağan edilən informasiyanın yerləşdirildiyi informasiya ehtiyatlarının Siyahısı"na daxil edir. Həmin internet informasiya ehtiyatına müraciətin məhdudlaşdırılması üçün bu Qanunun 13-3.7-ci maddəsində nəzərdə tutulmuş tədbirlər həyata keçirilir.

Maddə 13-4. **İnternet informasiya ehtiyatında yayılması qadağan edilən informasiyanın yerləşdirilməsi ilə əlaqədar məsuliyyət**

Bu fəslin müddəalarının pozulmasına görə internet informasiya ehtiyatının sahibi, domen adının sahibi, host və internet provayderlər qanunla müəyyən edilmiş qaydada məsuliyyət daşıyırlar.

IV fəsil

İNFORMASİYALAŞDIRMA, İNFORMASİYA SİSTEMLƏRİ, TEXNOLOGİYALARI VƏ ONLARIN TƏMİNAT VASİTƏLƏRİ

Maddə 14. **İnformasiya sistemləri, texnologiyaları və onların təminat vasitələrinin yaradılması və istehsalı**

Dövlət hakimiyyəti və yerli özünüidarə orqanları, təşkilati-hüquqi və mülkiyyət formasından asılı olmayaraq bütün müəssisə, idarə və təşkilatlar, vətəndaşların informasiya sistemləri, texnologiyaları və onların təminat vasitələrinin yaradılması və istehsalında bərabər hüquqları vardır.

Dövlət informasiya sistemlərinin, texnologiyalarının və onların təminat vasitələrinin yaradılması və istehsalı sahəsində elmi və təcrübi-layihə işlərinin aparılmasına şərait yaradır.

İnformasiyalaşdırmanın aparıcı istiqamətlərinin müəyyən edilməsi, onun inkişafı üçün müvafiq tədbirlərin görülməsi, dövlət informasiya sistemlərinin yaradılması müvafiq icra hakimiyyəti orqanları tərəfindən müəyyən edilir və görülən işlər dövlət büdcəsi, xüsusi vəsaitlər və digər mənbələrdən maliyyələşdirilir.

Maddə 15. **İnformasiya sistemləri, texnologiyaları və onları təminat vasitələrinə müəlliflik hüququ**

İnformasiya sistemləri, texnologiyaları və onların təminat vasitələrinə müəlliflik hüququ və onun müdafiəsi Azərbaycan Respublikasının müvafiq qanunvericiliyi ilə tənzimlənir.

Maddə 16. **İnformasiya sistemləri, texnologiyaları və onların təminat vasitələrinin sertifikasiyası, yaradılması və istifadəsi sahəsində xüsusi qaydalar**

Vətəndaşların və təşkilatların informasiya təminatı üçün nəzərdə tutulan informasiya sistemləri, verilənlər bazası və verilənlər bankı, konfidensial informasiyanın işlənməsini həyata keçirən dövlət orqanları, idarə, müəssisə və təşkilatların informasiya sistemləri, habelə bu sistemlərin mühafizə vasitələri müəyyənləşdirilmiş qaydada sertifikasiyalaşdırılmalıdır.

İnformasiya mühafizə vasitələrinin layihələşdirilməsi və istehsalı sahəsində fəaliyyət xüsusi razılıq əsasında həyata keçirilir.

V fəsil

İNFORMASİYANIN MÜHAFİZƏSİ

Maddə 17. **İnformasiya ehtiyatları və prosesləri sahəsində mühafizənin məqsədləri**

İnformasiyanın mühafizəsinin məqsədləri aşağıdakılardan ibarətdir:

- informasiyanın məhvinin, itməsinin, saxtalaşdırılmasının qarşısının alınması;
- dövlətin, ictimaiyyətin, vətəndaşların təhlükəsizliyinin təmin edilməsi;
- informasiyanın məhvi, modifikasiyası, surətinin çıxarılması, təcrid edilməsi ilə bağlı sanksiyalaşdırılmamış hərəkətlərin qarşısının alınması;
- dövlət sirri təşkil edən və konfidensial informasiyanın qorunması;
- informasiya proseslərində və informasiya sistemlərinin, texnologiyalarının və onların təminat vasitələrinin işlənməsi, istehsalı, tətbiqi zamanı fiziki və hüquqi şəxslərin hüquqlarının təmin olunması.

Maddə 18. **İnformasiyanın mühafizəsinin təşkili**

Barəsində qanunsuz əməliyyatlar və davranış nəticəsində mülkiyyətçiyə, sahibə, istifadəçiyə və ya başqa şəxslərə ziyan vurula bilən hər hansı sənədləşdirilmiş informasiya mühafizə olunmalıdır.

İnformasiyanın mühafizə rejimi onun hüquqi rejimindən asılı olaraq "Dövlət sirri haqqında" Azərbaycan Respublikasının Qanunu ilə, bu Qanunla, "İnformasiya əldə etmək haqqında" Azərbaycan Respublikasının Qanunu ilə, digər normativ hüquqi aktlarla, habelə mülkiyyətçi tərəfindən müəyyən edilir.

İnformasiya ehtiyatlarının mülkiyyətçisi və ya Azərbaycan Respublikasının qanunvericiliyinə müvafiq olaraq informasiya mühafizəsi üçün məsul struktur bölmələr informasiya mühafizəsi tələblərinə əməl edilməsinə nəzarət etmək, bu tələblər pozulduqda isə informasiya ilə işləməyi qadağan etmək və ya dayandırmaq hüququna malikdirlər.

Sənədləşdirilmiş informasiyanın mülkiyyətçisi və ya sahibi informasiya sistemlərindəki ona məxsus informasiyanın mühafizəsinin norma və tələblərinə riayət olunmasını müəyyənləşdirmək üçün müvafiq orqanlara müraciət edə bilərlər. Bu orqanlar informasiyanın özünün vəyoxlamanın nəticələrinin məxfiliyi şərtlərinə əməl etməlidirlər.

Maddə 19. **İnformasiyanın mühafizəsi sahəsində subyektlərin hüquq və vəzifələri**

Sənədlərin, sənəd massivlərinin, informasiya sistemlərinin mülkiyyətçisi və ya müvafiq icra hakimiyyəti orqanları informasiyanın istifadəçiyə təqdim edilməsinin qaydalarını bu Qanuna və "İnformasiya əldə etmək haqqında" Azərbaycan Respublikasının Qanuna uyğun olaraq müəyyən edir və istifadəçilərin sənədlərlə işləməyə buraxılmasını təmin edirlər.

Sertifikatlaşdırılmamış informasiya sistem və vasitələrdən istifadə olunması və xidmətlərin göstərilməsi ilə bağlı məsuliyyəti bu sistem və vasitələrin mülkiyyətçisi və ya sahibi, belə sistemlərdən əldə olunan informasiyadan istifadə üçün isə məsuliyyəti istifadəçi daşıyır.

Maddə 20. **İnformasiyalaşdırma mühitində subyektlərin hüquqlarının müdafiəsi**

İnformasiyanın istifadəçisi informasiya mülkiyyətçisi və ya sahibinin hüquqlarına riayət edilməməsinə görə məsuliyyət daşıyır.

İnformasiya məhsulları və xidmətlərinin mülkiyyətçiləri ilə istifadəçilər arasında münasibətlər Azərbaycan Respublikasının qanunvericiliyində nəzərdə tutulmuş qaydalarla, müqavilələrlə rəsmiləşdirilir. Onlar arasında yaranan mübahisələr Azərbaycan Respublikasının qanunvericiliyində müəyyən olunmuş qaydada məhkəmə vasitəsilə həll edilir.

İnformasiyanı korlamaqla və ya dəyişdirməklə onun sahibinə ziyan vuran fiziki və hüquqi şəxslər hərəkətlərinə görə Azərbaycan Respublikasının qanunvericiliyinə uyğun olaraq məsuliyyət daşıyırlar.

İnformasiya ehtiyatlarının formalaşdırılması, istifadə olunması, işlənməsi, informasiya sistemləri, texnologiyaları və onların təminat vasitələrinin istehsalı və tətbiqi sahəsində fiziki və hüquqi şəxslərin hüquqlarının müdafiəsi qanun pozuntularının qarşısının alınması, pozulmuşhüquqların bərpa edilməsi, dəymiş ziyanın ödənilməsi məqsədini daşıyır. Bu hüquqların müdafiəsi Azərbaycan Respublikasının qanunvericiliyi ilə müəyyən edilmiş qaydada müvafiq orqanlar tərəfindən həyata keçirilir.

İstifadəçinin açıq informasiya ilə işləməsinə məhdudiyyətlər qoyulması və ya buraxılmaması, bilərəkdən yanlış informasiya verilməsi və Azərbaycan Respublikasının qanunvericiliyi və ya bağlanmış müqavilələrin şərtləri yerinə yetirilmədiyi hallarda istifadəçi məlumat sahibinin yuxarı orqanına və Azərbaycan Respublikasının İnsan hüquqları üzrə müvəkkilinə (ombudsmana) şikayət etmək, habelə məhkəməyə şikayət vermək, o cümlədən bu hərəkətlər nəticəsində dəymiş ziyanın ödənilməsini tələb etmək hüququna malikdir.

Vətəndaşların informasiya ilə işləmək hüququnun əsassız olaraq məhdudlaşdırılmasında təqsirli olan vəzifəli şəxslər Azərbaycan Respublikasının qanunvericiliyinə uyğun olaraq məsuliyyət daşıyırlar.

VI fəsil

İNFORMASİYA SAHƏSİNDƏ BEYNƏLXALQ MÜNASİBƏTLƏR

Maddə 21. **İnformasiya sahəsində beynəlxalq fəaliyyət**

İnformasiya sahəsində dövlətlərarası əməkdaşlıq Azərbaycan Respublikasının imzaladığı müqavilələrə uyğun olaraq həyata keçirilir.

Azərbaycan Respublikasının beynəlxalq müqavilələrində bu Qanunda nəzərə alınmış qaydalardan fərqlər müəyyən olunduqda beynəlxalq müqavilələrin müddəaları tətbiq olunur.

Azərbaycan Respublikasının Prezidenti
HEYDƏR ƏLİYEV

Bakı şəhəri, 3 aprel 1998-ci il
№ 460-IQ

ƏDƏBİYYAT SİYAHISI

Azərbaycan dilində olan ədəbiyyatlar:

1. Azərbaycan Respublikasının Konstitusiyası. Bakı, 2009.
2. Biometrik informasiyahaqqında Azərbaycan Respublikasının Qanunu, Bakı, 2008.
3. Dövlət sirrinə aid edilən məlumatların Siyahısının təsdiq edilməsi haqqında Azərbaycan Respublikası Prezidentinin Fərmanı. Bakı, 2005.
4. Dövlət hakimiyyəti orqanlarında, idarə, təşkilat və müəssisələrində məxfi sənədlərlə iş üzrə kargüzarlığın aparılması Qaydasının təsdiq edilməsi haqqında Azərbaycan Respublikasi Prezidentinin Fərmanı. Bakı, 2005.
5. Mülki aviasiya hava gəmilərinin uçuşlarının təhlükəsizliyinə dair məlumatların toplanması və işlənməsi sistemlərində informasiyanın qorunması Qaydalarının təsdiq edilməsi barədə Azərbaycan Respublikasının Nazirlər Kabinetinin Qərarı. Bakı, 2011.
6. Dövlət sirri haqqında Azərbaycan Respublikasının Qanunu, Bakı, 2004.
7. İnformasiya əldə etmək haqqında Azərbaycan Respublikasının Qanunu, Bakı, 2005.
8. Fərdi məlumatlar haqqında Azərbaycan Respublikasının Qanunu, Bakı, 2010.
9. İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında Azərbaycan Respublikasının Qanunu, Bakı, 1999.
10. Kommersiya sirri haqqında Azərbaycan Respublikasının Qanunu, Bakı, 2001.
11. Məlumat azadlığı haqqında Azərbaycan Respublikasının Qanunu, Bakı, 1998.
12. Məlumat toplularının hüquqi qorunması haqqında Azərbaycan Respublikasının Qanunu, Bakı, 1998.
13. Qasımov V.Ə. İnformasiya təhlükəsizliyinin əsasları. Dərslik, Bakı: MTN Maddi-texniki Təminat Baş İdarəsinin NPM. 2009.
14. Qasımov V.Ə. İnformasiya təhlükəsizliyi: Kompüter cinayətkarlığı və kiberterrorçuluq. Bakı: Elm, 2007.

15. Milli təhlükəsizlik haqqında Azərbaycan Respublikasının Qanunu. Bakı, 2004.
16. Musayev H.M. Beynəlxalq terrorçuluğa qarşı mübarizədə xüsusi xidmət orqanlarının fəaliyyətinin prinsip və xüsusiyyətləri. Bakı, Çaşıoğlu, 2009.
17. R.Əliquliyev, Y.İmamverdiyev, V.Musayev. Biometrik texnologiyalar. Bakı: "İnformasiya texnologiyaları" nəşriyyatı, 2009.
18. www.cert.az/ziyankar.html
19. www.dtx.gov.az/haqqimizda1.php
20. www.dtx.gov.az/tarix3.php
21. www.ict.az;

Rus dilində olan ədəbiyyatlar:

22. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. - М.: Академический Проект; Гаудеамус, 2-е изд.- 2004.
23. Сидорин Ю.С. Технические средства защиты информации: Учеб. пособие. Издательство Политехнического университета, Санкт-Петербург, 2005.
24. Корнюшин П.Н., Костерин С.С. Информационная безопасность, Владивосток, 2003.
25. Волковский Н.Л. История информационных войн. В 2 ч. Ч. 1. - СПб.: ООО «Издательство Полигон», 2003. -512 с.
26. Волковский Н.Л. История информационных войн. История информационных войн. В 2 ч. Ч. 2. - СПб.: ООО «Издательство Полигон». - 2003. - 736 с.
27. Петров С.В., Петров В.П. Информационная безопасность человека и общества: учебное пособие, 2007.
28. Соловьев А.А., Метелев С.Е., Зырянова С.А. Защита информации и информационная безопасность: Учебник. Омск: Изд-во Омского института (филиала) РГТЭУ, 2011. - 426 с.
29. Разин Е.А. История военного искусства. СПб.: Полигон, 1999. - 562 с.
30. Конрад Н.И. Сунь-цзы: Трактат о военном искусстве. М., 1950. - 480 с.

31. Манфред А.З. Наполеон Бонапарт. Изд. 4-ое. М.: Изд-во Мысль, 1987. - 776 с.
32. Апполонский С.М. Справочник по расчету электромагнитных экранов. - Л.: Энергоатомиздат, 1988.
33. Коровин В.В. История отечественных органов безопасности. - М.: 1998.
34. Рыбников, В.В., Алексушин, Г. В. История право-охранительных органов Отечества: учебн. пособ. для вузов. - М.: Щит-М, 2007.
35. Максимов А. Главная тайна ГРУ. - М.: Яуза: Эксмо, 2010. - 416 с.
36. Doc 9944. Рекомендации в отношении записей регистрации пассажиров (PNR). ISBN 978-92-9231-691-4, ИКАО, 2010.
37. Ржавский К.В. Информационная безопасность: практическая зашита информационных технологий и телекоммуникационных систем: Учебное пособие. - Волгоград: Изд-во ВолГУ, 2002. - 122 с.
38. Мартынов, А. И. Методы и задачи криптографической защиты информации: учебное пособие для студентов специальности «Вычислительные машины, комплексы, системы и сети». - Ульяновск: УлГТУ, 2007. - 92 с.

İngilis dilində olan ədəbiyyatlar:

39. Doc 8973.Aviation Security Manual. ICAO, 2014.
40. Nina Agrawal. There's more than the CIA and FBI: The 17 agencies that make up the U.S. intelligence community // Los Angeles times, 2017. http://www.latimes.com/nation/la-na-17-intelligence-agencies-20170112-story.html.
41. Graves, Melissa. "FBI Historiography: From Leader to Organisation" in Christopher R. Moran, Christopher J. Murphy, eds. Intelligence Studies in Britain and the US: Historiography since 1945 (Edinburgh UP, 2013) pp. 129-145.
42. McCoy, Alfred W. A Question of Torture: CIA Interrogation, from the Cold War to the War on Terror. New York: Owl Books (Henry Holt & Co.). 2006, 304 pg.
43. www.structure.mil.ru/structure/ministry_of_defence/detailshtm?id=9711@egOrganization.

44. James Bamford. Body of Secrets: Anatomy of the Ultra-Secret National Security Agency. - Anchor, 2009. - 784 p.
45. Elias, Bartholomew. Airport and aviation security: U.S. policy and strategy in the age of global terrorism. Taylor & Francis Group. ISBN 978-1-4200-7029-3411, 2010.
46. Bernard Lim. Aviation Security. Emerging Threats from Cyber Security in Aviation - Challenges and Mitigations / Journal of Aviation Management, 2014, pp. 81-91.

X.İ.Abdullayev, N.T.Nağıyev, R.M.Muxtarov

MÜƏSSİSƏNİN İNFORMASİYA TƏHLÜKƏSİZLİYİ

Dərslik

Dərslik «Mülki Aviasiya»
redaksiya heyəti tərəfindən baxılmış
və çapına icazə verilmişdir.

Çapa hazırlanmışdır 08.02.2019.

Texniki redaktor: Ramazanzadə A.M.
Korrektor: ƏliyevaO.V.

Dərslik«Azərbaycan Hava Yolları»
Qapalı Səhmdar Cəmiyyəti
Milli Aviasiya Akademiyasının
Poliqrafiya Mərkəzində çap olunmuşdur.

Format – 60x84 $^{1}/_{8}$
Tirajı 20 nüsxə.