AZƏRBAYCAN RESPUBLİKASI DAXİLİ İŞLƏR NAZİRLİYİ

POLİS AKADEMİYASI

″DİO-nun İNZİBATİ FƏALİYYƏTİ ″ KAFEDRASI

Akademiyanın kursantları üçün

″Müasir informasiya texnologiyaları″ fənni üzrə

M Ü H A Z İ R Ə

Mövzu № 7: "İnformasiya texnologiyalarının təhlükəsizliyi″

Vaxt - 4 saat

Mühazirə - 2 saat

Seminar– 2 saat

Bakı - 2019

AZƏRBAYCAN RESPUBLİKASI DAXİLİ İŞLƏR NAZİRLİYİ

POLİS AKADEMİYASI

"DİO-nun İNZİBATİ FƏALİYYƏTİ " KAFEDRASI

Akademiyanın kursantları üçün

"Müasir informasiya texnologiyaları" fənni üzrə

M Ü H A Z İ R Ə

Mövzu № 7: "İnformasiya texnologiyalarının təhlükəsizliyi"

Vaxt - 4 saat

Mühazirə - 2 saat

Seminar– 2 saat

Tərtib etdi:

Kafedranın baş müəllimi,

polis polkovnik-leytenantı **Heydərov H.M.**

Mühazirənin mətni kafedranın iclasında müzakirə olunmuş və təsdiq edilmişdir.

Protokol №*09* *" 30 "* *may* 2019-cu il.

Bakı - 2019

Mövzu № 7: "İnformasiya texnologiyalarının təhlükəsizliyi"

PLAN:

1. İnformasiya təhlükəsizliyinin əsas konseptual məsələləri
2. Kompüter sistemlərində və şəbəkələrində informasiya təhlükəsizliyi
3. Kompüter sistemlərində və şəbəkələrində informasiya təhlükəsizliyinin pozulmasi təhlükələri
4. İnformasiya təhlükəsizliyinin təmin edilməsi üsullari və vasitələri
5. İnformasiyanin qorunmasinin kriptoqrafik üsullari

Ə D Ə B İ Y Y A T :

1. "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının 03.04.1998-ci il tarixli Qanunu.
2. "Milli təhlükəsizlik haqqında" Azərbaycan Respublikasının 29.06.2004-cü il tarixli Qanunu.
3. "Biometrik informasiya haqqında" Azərbaycan Respublikasının 13.06.2008-ci il tarixli Qanunu.
4. Azərbaycan Respublikasının Cinayət Məcəlləsi. Bakı, 2010.
5. Əliquliyev R.M., Mahmudov R.Ş. "İnternetin tənzimlənməsi problemləri : ekspress-informasiya". Bakı, İnformasiya Texnologiyaları nəşriyyatı, 2010. 115 s.
6. Əliquliyev R.M., İmamverdiyev Y.N., Abdullayeva F.C. "Sosial şəbəkələr". Bakı, İnformasiya Texnologiyaları nəşriyyatı, 2010. 287 s.
7. Əliquliyev R.M., İmamverdiyev Y.N. "İnformasiya təhlükəsizliyi insidentləri". Bakı, İnformasiya Texnologiyaları nəşriyyatı, 2012. 219 s.
8. Əliquliyev R.M., İmamverdiyev Y.N. "Kriptoqrafiyanın əsasları". Bakı, İnformasiya Texnologiyaları nəşriyyatı, 2006. 688 s.
9. Kərimov S.Q., Həbibullayev S.B., İbrahimzadə T.İ. Dərslik. "İnformatika". Ali məktəblər üçün dərslik. Bakı, 2010. 434 s.
10. Kərimov S.Q. "İnformasiya sistemləri". Bakı : Elm, 2008. - 676 s.
11. İbrahimzadə T.İ, Sərdarov Y.B., İsmayılov M.A. "Kompüter sistemlərində mühafizənin təşkili". Ali məktəb tələbələri üçün dərs vəsaiti (I cild). Bakı, 2007.
12. Qasımov V.Ə. "İnformasiya təhlükəsizliyinin əsasları". Dərslik. Bakı, MTN Maddi Texniki Təminat Baş İdarəsinin Nəşriyyat- Poliqrafiya Mərkəzi, 2009.
13. Батурин Ю.М. Проблемы компьютерного права. Москва, 1991.
14. Люпунов Ю., Максимов В. Ответственность за компьютерные преступления. Законность, 1997.
15. İnformasiya təhlükəsizliyi sahəsində fəaliyyətin təkmilləşdirilməsi tədbirləri haqqında Azərbaycan Respublikası Prezidentinin Fərmanı// http://president.az/articles/6298
16. Milli informasiya təhlükəsizliyi üzrə mükəmməl strategiya // http://webcityhost.net/vergiler/upload/File/art-818.pdf
17. Azərbaycan Prezidenti informasiya təhlükəsizliyi sahəsində fəaliyyətin təkmilləşdirilməsi tədbirləri haqqında fərman imzalayıb //http://www.aztelekom.org/index.php?id=725

GİRİŞ

İnformasiya texnologiyaları sahəsində elmi-texniki tərəqqi nəticəsində milli dövlət sərhədləri informasiya resurslarının axını, telekommunikasiya sistemlərinin və qlobal kompüter şəbəkələrinin fəaliyyəti, transmilli biznes, maliyyə və bank hesablaşmaları üçün "şəffaf' olmuşdur. Belə ki, müasir dövrdə informasiya resursları, habelə maliyyə vəsaitləri yer kürəsini bir neçə saniyə ərzində dövr etmək imkanına malikdir.

Yeni informasiya texnologiyaları bu gün elə sürətlə inkişaf edir ki, onun doğuracağı bəzi fəsadlar ya əvvəlcədən təsəvvürə belə gəlmir, ya da cəmiyyət tərəfindən çox gec başa düşülür. Ümumiyyətlə, belə bir fikir mövcuddur ki, hər hansı kritik həddi aşdıqdan sonra elmi-texniki tərəqqi də bəşəriyyətin əleyhinə işləməyə başlayır. Bu fikrin sübutu kimi, müasir dağıdıcı silahları, nüvə texnologiyasını, sənayenin inkişafı nəticəsində yaranmış ciddi ekoloji problemləri və s. göstərmək olar.

Hazırda analoji situasiya informasiya texnologiyaları sahəsində də yaranmışdır. Belə ki, yeni informasiya texnologiyalarının inkişafı ayrı-ayrı şəxslərin, təşkilatların və bütövlükdə dövlətin informasiya resursları üçün təhlükələrin meydana gəlməsinə səbəb olmuşdur.

Başqa sözlə, fərdi kompüterlərin, coğrafi cəhətdən paylanmış kompüter sistemlərinin və şəbəkələrinin, ümumi istifadə üçün nəzərdə tutulmuş informasiya və şəbəkə resurslarının sürətli inkişafı və bütün fəaliyyət sahələrində geniş yayılması nəticəsində saxlanılan, emal olunan və ötürülən informasiyanın təhlükəsizliyinin təmin edilməsi çox ciddi məsələyə çevrilmişdir.

Dövlət və hökumət orqanlarında, özəl müəssisələrdə kompüter sistemlərinin və şəbəkələrinin, ələlxüsus fərdi kompüterlərin gündəlik xidməti fəaliyyəti və şəxsi məqsədlər üçün geniş istifadəsi cəmiyyətin müxtəlif təbəqələrində informasiya texnologiyalarına, o cümlədən informasiya resurslarına münasibətdə ciddi dəyişikliklər yaratmışdır. Nəticədə, şəxsi maraqların, niyyətlərin və tələbatların ödənilməsi məqsədilə informasiya sistemlərinin işinə icazəsiz qarışmaq, qəsdən və ya təsadüfən, qərəzli və ya qərəzsiz şəkildə bu sistemlərə daxil olmaq, onları sıradan çıxarmaq, informasiya resurslarında və sistem parametrlərində dəyişikliklər apar- maq, onları istifadə və məhv etmək kimi təhlükəli hallar günbəgün çoxalır. Çox təəssüf ki, bu cəhdlərin bir çoxu müvəffəqiyyətlə həyata keçirilir, informasiya sahiblərinə əhəmiyyətli maddi və mənəvi ziyanlar vurulur.

Xüsusi halda, bu problemlərə kompüterlərin, kompüter sistemlərinin və şəbəkələrinin işinə qeyri-qanuni müdaxilə, kompüter informasiyasının oğurlanması, mənimsənilməsi, zorla, şantaj yolu ilə alınması kimi təhlükəli yeni sosial təzahürləri aid etmək olar. Bu təhlükələri çox vaxt "kompüter cinayətkarlığı" və ya "kompüter terrorçuluğu" adlandırırlar.

Məlum olduğu kimi, bu gün bütün yer kürəsini hörümçək toru kimi örtən İnternet şəbəkəsi informasiya təhlükəsizliyi probleminin daha da kəskinləşməsinə təkan verən əsas amillərdən biridir. Belə ki, dünyanın istənilən nöqtəsindən İnternet şəbəkəsinə qoşulmaq, onun vasitəsilə müxtəlif növ məlumatları ötürmək və almaq mümkündür.

Paylanmış kompüter şəbəkələrindən ibarət olan İnternet şəbəkəsinin xidmətləri istifadəçilərə öz iş yerlərini və evlərini tərk etmədən dünyanın, praktiki olaraq, istənilən nöqtəsində olan müxtəlif informasiya sistemlərinə və ya məlumat bazalarına qoşulmaq, eləcə də onları maraqlandıran zəruri informasiya ilə taniş olmaq və məlumatları əldə etmək imkanları verir.

Statistika göstərir ki, İnternet istifadəçilərinin sayı astronomik sürətlə artır. Açıq informasiya mənbələrinin məlumatlarına görə, bu gün İnternet dünyanın bütün dövlətlərini əhatə etməklə, hər bir şəxsə, o cümlədən xakerə, cinayətkara və terrorçuya da öz cinayətkar niyyətlərini həyata keçirmək üçün tamamilə eyni imkanlar yaradır. Bu gün telekommunikasiya sistemləri və kompüter şəbəkələri, o cümlədən İnternet şəbəkəsi siyasətçilər, iş adamları, dini təşkilatlar, terrorçu qruplar, cinayətkar qruplaşmalar, habelə düşmən ölkələrin xüsusi xidmət orqanları tərəfindən informasiya mübarizəsi, qarşıdurması, hətta müharibəsi vasitəsi və aləti kimi istifadə olunur.

İnformasiya təhlükəsizliyi probleminə diqqətin artırılmasını tələb edən ən vacib amillərdən biri də kompüter viruslarıdır. Təbii viruslara analoji olaraq, müxtəlif xarakterli funksiyalara malik olan kompüter virusları proqramların tərkibinə, yaddaş qurğularına, fayllara gizlicə əlavə olunaraq (yazılaraq) yayılırlar. Sonradan öz-özünə digər proqramlara, fayllara və s. ötürülən kompüter virusları hər hansı bir məlumatın ekrana çıxarılmasından tutmuş, informasiya resurslarının pozulması, disk qurğularının sıradan çıxması və s. kimi ağır nəticələrə, digər çox ciddi problemlərin yaranmasına gətirib çıxara bilər.

Lakin bununla yanaşı, kompüter sistemləri üçün əsas təhlükəni ziyankar rolunu oynayan və informasiya texnologiyaları sahəsində peşəkar mütəxəssis olan şəxslər - hakerlər təşkil edirlər. Belə ki, onlar kompüter sistemlərinin və şəbəkələrinin, telekommunikasiya qurğularının və informasiya sistemlərinin, eləcə də təhlükəsizlik sistemlərinin incəliklərini, o cümlədən zəif yerlərini bilir, təhlükəsizliyin təmin edilməsi mexanizmlərini təhlil etmək, sındırmaq, ziyanverici proqramlar yaratmaq və yaymaq üçün bütün zəruri proqram texniki bazaya və imkanlara malik olurlar.

Dövlətin milli təhlükəsizliyinin vacib tərkib hissələrindən biri kimi informasiya təhlükəsizliyinin təmin edilməsi məsələsi transmilli (sərhədsiz) kompüter cinayətkarlığının və kiberterrorçuluğun meydana gəlməsi kontekstində xüsusilə kəskin şəkildə ortaya çıxır.

Mühazirədə informasiya təhlükəsizliyinin əsas konseptual məsələləri, müddəaları, və modeli, kompüter sistemlərində və şəbəkələrində informasiya təhlükəsizliyi məsələsi şərh olunmuş, informasiya təhlükəsizliyinin pozulması təhlükələri, onların qarşısının alınmasının üsulları və vasitələri təsvir edilmişdir. Eləcə də, informasiyanın qorunmasının kriptoqrafik üsulları barədə ətraflı məlumat verilmişdir.

Sual 1. İnformasiya təhlükəsizliyinin əsas konseptual məsələləri

Milli təhlükəsizlik və onun təmin edilməsində informasiya təhlükəsizliyinin rolu və yeri. Bu gün təhlükəsizliyin təmin edilməsi bütövlükdə bəşəriyyətin ən əsas və qlobal problemlərindən biridir. Adi həyatda təhlükəsizlik anlayışı özündə normal (təhlükəsiz) yaşayış, iş, məişət, istirahət şəraitinin təmin olunmasını ehtiva edir. Bütövlükdə isə *təhlükəsizlik* – havanın təmizliyi, ərzağın və suyun keyfiyyəti, mənzil şəraiti, kriminala və terrorçuluğa qarşı effektiv mübarizə, nəqliyyatda, küçədə və ictimai yerlərdə təhlükəsizlik, tibbi təminatın və sosial müdafiənin səviyyəsi, xidmət sahələrində mənəvi-etik mühitin yaradılması, əmək haqqının sərf edilən əməyə uyğunluğu və s. ilə xarakterizə olunur.

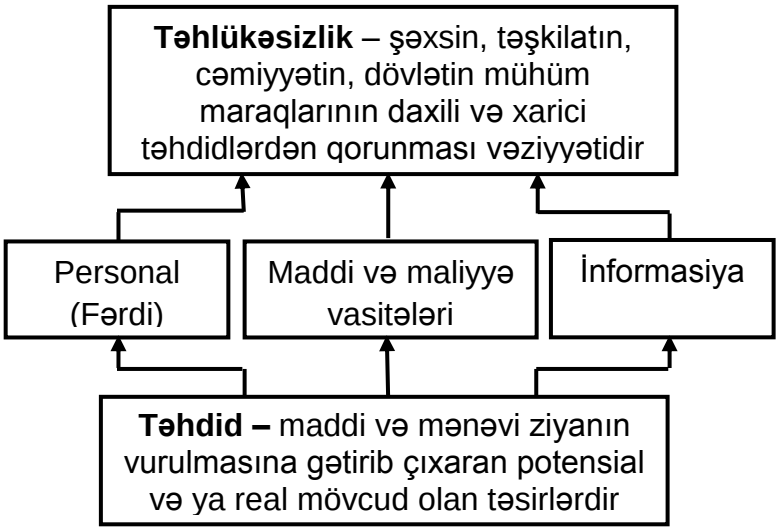
Milli təhlükəsizlik termini rəsmi olaraq ilk dəfə 1947-ci ildə ABŞ-da meydana gəlmişdir. Həmin dövrdə ABŞ-da prezidentin milli məsələlər üzrə xüsusi köməkçisi dövlət vəzifəsi təsis edilmiş və Milli Təhlükəsizlik Şurası yaradılmışdır.

Milli təhlükəsizlik – milli maraqların ona yönəlmiş təhdidlərdən qorunmasının təmin edilməsidir.

Özündə şəxsin, təşkilatın, cəmiyyətin və dövlətin mühüm (həyat əhəmiyyətli) maraqlarının daxili və xarici təhdidlərdən qorunması vəziyyətini ehtiva edən təhlükəsızlik aşağıdakı komponentlərlə xarakterizə olunur (şəkil.1 1)

- personal;
- maddi və maliyyə vəsaitləri;
- informasiya.

Yaranmış təhdidlər bu komponentlərdən birinə təsir etməklə digər komponentlər və bütövlükdə obyekt üçün təhlükə yaradır. İnformasiya təhdidləri isə obyektə və onun təhlükəsizliyinin digər komponentlərinə təsiri, bir qayda olaraq, onun informasiya mühitinə, o cümlədən informasiyasına və informasiya ehtiyatlarına təsir vasitəsilə həyata keçirir.



Şək.1.1. Təhlükəsizliyin komponentləri

Sovet İttifaqı dağıldıqdan sonra müstəqillik qazanmış Azərbaycan Respublikası sosializmdən yeni münasibət formasına keçid dövründə iqtisadi, siyasi-sosial və hərbi böhranlarla müşayiət olunan bir sıra problemlərlə üzləşdi. Bu problemlər respublikanın iqtisadiyyatının səviyyəsinin aşağı düşməsinə, əhalinin həyat səviyyəsinin pisləşməsinə, elm, təhsil və tibb sahəsində böhranlı vəziyyətin yaranmasına, Azərbaycanın sərhədlərinin pozulmasına və müharibənin baş verməsinə gətirib çıxardı.

Respublikanı belə böhranlı vəziyyətdən çıxarmaq məqsədilə ölkə rəhbərliyi tərəfindən daxili və xarici təhlükəsizliyin təmin olunması, regional və beynəlxalq təhlükəsizlik üzrə tədbirlərdə iştirak edilməsi, iqtisadiyyatın, sosial vəziyyətin, elmin, təhsilin, mədəniyyətin səviyyəsinin yüksəldilməsi istiqamətində atılan addımlar Azərbaycanın müstəqilliyinin və dövlətçiliyinin qorunması, milli təhlükəsizliyinin təmin edilməsinə yönəlmişdir.

Azərbaycan Respublikasının milli təhlükəsizliyi məsələləri və milli maraqlan Azərbaycan Respublikasının Konstitusiyası, Milli Təhlükəsizlik Konsepsiyası və "Milli təhlükəsizlik haqqında" Azərbaycan Respublikasının Qanunu ilə müəyyən olunmuşdur.

3 avqust 2004-cü ildə qəbul edilmiş "Milli təhlükəsizlik haqqında" Azərbaycan Respublikasının Qanununda qeyd olunur ki, *Azərbaycan Respublikasının milli təhlükəsizliyi* – dövlətin müstəqilliyinin, suverenliyinin, ərazi bütövlüyünün, konstitusiya quruluşunun, xalqın

və ölkənin milli maraqlarının, insanın, cəmiyyətin və dövlətin hüquq və mənafelərinin daxili və xarici təhdidlərdən qorunmasının təmin edilməsidir.

Azərbaycan Respublikasının milli maraqları dedikdə Azərbaycan xalqının fundamental dəyər və məqsədlərini, habelə insanın, cəmiyyətin və dövlətin inkişaf və tərəqqisini təmin edən siyasi, iqtisadi, sosial, hərbi, informasiya, ekoloji, elm, təhsil, mədəni və mənəvi tələbatları nəzərdə tutulur.

Göründüyü kimi, Qanunda milli təhlükəsizliyin obyektləri kimi insan, cəmiyyət və dövlət müəyyən edilmişdir.

İnsanın maraqları dedikdə onun hüquq və azadlıqlarının, təhlükəsizliyinin, fiziki, mənəvi, intellektual inkişafı üçün şəraitin təmin edilməsi, rifahının yüksəldilməsi nəzərdə tutulur.

Cəmiyyətin maraqları – onun demokratikləşməsini, hüquqi və dünyəvi dövlətin qurulması prosesinin davam etdirilməsini, ictimai sabitliyin, milli həmrəyliyin yaranmasını və qorunub saxlanmasını, mədəni, tarixi, milli, mənəvi dəyərlərin qorunmasını və inkişaf etdirilməsini özündə ehtiva edir.

Dövlətin maraqları – onun müstəqilliyinin, suverenliyinin, konstitusiya quruluşunun, ərazi bütövlüyünün qorunmasından, siyasi, iqtisadi və sosial stabilliyin, qanunların aliliyinin təmin edilməsindən, beynəlxalq əməkdaşlığın inkişaf etdirilməsindən ibarətdir.

Qanunun 6.6 bəndində informasiya sahəsində əsas milli maraqlar aşağıdakı kimi müəyyən edilmişdir.

"Azərbaycan Respublikasının informasiya sahəsində əsas milli maraqlan aşağıdakılardır:

- məlumatların qanuni yolla əldə edilməsi, ötürülməsi, hazırlanması və yayılması kimi vətəndaşların konstitusiya hüquqlarının təmin edilməsi;
- informasiya ehtiyatlarının qorunması və inkişaf etdirilməsi;
- informasiya məkanının formalaşdırılması və onun qorunmasının təmin edilməsi;
- dünya rabitə və informasiya sisteminə daxil olma".

Qanunun 7.9 bəndində informasiya sahəsində Azərbaycan Respublikasının milli təhlükəsizliyinə təhdidlər də müəyyən edilmişdir.

- "İnformasiya sahəsində əsas təhdidlər aşağıdakılardır:
- informasiya texnologiyaları sahəsində geriləmə və dünya informasiya məkanına daxil olmağa maneələrin mövcudluğu;
- informasiya azadlığı əleyhinə yönəlmiş qəsdlər;
- dövlət sirrinin aşkarlanmasına yönəlmiş qəsdlər;
- digər ölkələr tərəfindən informasiya təcavüzü, beynəlxalq aləmdə Azərbaycan həqiqətlərinin təhrif edilməsi;
- informasiya sisteminə və ehtiyatlarına qarşı qəsdlər".

Göründüyü kimi, Qanunda müəyyən edilmiş informasiya sahəsində Azərbaycan Respublikasının milli maraqları və milli təhlükəsizliyinə təhdidlər ümumi halda informasiya təhlükəsizliyinin baza prinsiplərini və onların pozulması formalarını özündə təzahür etdirir.

Qeyd olunanlara uyğun olaraq, Qanunun 20-ci maddəsində informasiya sahəsində milli təhlükəsizliyin təmin olunması məsələləri əksini tapmışdır:

"Azərbaycan Respublikasının informasiya sahəsində milli təhlükəsizliyinin təmin olunması dövlət, ictimai və fərdi informasiya ehtiyatlarının qorunması, habelə informasiya sahəsində milli maraqların müdafiəsinə yönəlmiş tədbirlər kompleksinin həyata keçirilməsidir.

Azərbaycan Respublikasının informasiya sahəsində milli təhlükəsizliyinin təmin olunması üçün görülən əsas tədbirlər aşağıdakılardır:

- Azərbaycan Respublikasında informasiyanın, həmçinin informasiya ehtiyatlarının müdafiəsi sahəsində milli sistemin yaradılması və möhkəmləndirilməsi;
- dövlət orqanları və vəzifəli şəxslər tərəfindən qərarların qəbul edilməsinin informasiya təminatının həyata keçirilməsi məqsədilə obyektiv və qabaqlayıcı məlumatların toplanması;

- informasiya infrastrukturunun inkişaf etdirilməsi;
- dövlət sirlərinin qorunmasının hüquqi mexanizmlərinin təkmilləşdirilməsi;
- kompüter informasiyası sahəsində cinayətkarlığa qarşı mübarizə;
- informasiya təhlükəsizliyinin və azadlığının təmin olunması".

Bu istiqamətdə növbəti rəsmi dövlət sənədi olan "Azərbaycan Respublikasının Milli Təhlükəsizlik Konsepsiyası" 23 may 2007-ci il tarixində təsdiq edilmişdir. Konsepsiyanın 4.3.11 saylı bəndində Azərbaycan Respublikasının milli təhlükəsizlik siyasətinin əsas istiqamətlərindən biri kimi informasiya təhlükəsizliyi siyasəti müəyyən edilmişdir.

"Azərbaycan Respublikasının informasiya təhlükəsizliyi siyasəti dövlət, ictimai və fərdi informasiya ehtiyatlarının qorunmasına, habelə informasiya sahəsində milli maraqların müdafiəsinə yönəlmiş tədbirlər kompleksinin həyata keçirilməsindən ibarətdir.

Azərbaycan Respublikasının informasiya sahəsində milli təhlükəsizliyinin təmin edilməsi üçün ölkədə informasiyanın, həmçinin dövlət informasiya ehtiyatlarının müdafiəsi sahəsində milli sistem və informasiya infrastrukturu inkişaf etdirilir və möhkəmləndirilir. Dövlət orqanları və vəzifəli şəxslər tərəfindən qərarların qəbul edilməsinin informasiya təminatının həyata keçirilməsi məqsədi ilə obyektiv və mühüm məlumatlar toplanılır.

Kəşfiyyat və əks-kəşfiyyat qabiliyyətinin uzlaşdırılması və səmərəliliyinin artırılması, habelə məxfi informasiyanın mühafizə olunmasının koordinasiyası milli təhlükəsizlik sektorunun bu sahəsində əsas məsələlərdəndir. Azərbaycan Respublikası öz kəşfiyyat və əks-kəşfiyyat qabiliyyətini artıracaq və dövlət sirrinə aid edilmiş məlumatların mühafizəsi ilə bağlı fəaliyyətin təkmilləşdirilməsini davam etdirəcəkdir.

İnformasiya təhlükəsizliyini tənzimləmək məqsədilə dövlət sirri təşkil edən məlumatların mühafizəsinin hüquqi mexanizmləri təkmilləşdirilir və informasiya azadlığı təmin olunur. Hüquqi və inzibati mexanizmlər vətəndaşların hüquqlarını və dövlət strukturlarının fəaliyyəti üzərində demokratik nəzarəti təmin edəcəkdir".

Qeyd olunduğu kimi, informasiya cəmiyyətinin formalaşması və inkişafı prosesində insan fəaliyyətinin bütün sahələrində müxtəlif informasiya-kommunikasiya texnologiyaları (İKT) işlənib hazırlanır və tətbiq edilir. İnformasiya və informasiya ehtiyatlan insanın, cəmiyyətin və dövlətin inkişafının həlledici amillərindən birinə çevrilmişdir. İKT-nin, o cümlədən kompüter texnikasının geniş imkanları dövlət, iqtisadiyyat, sosial, müdafiə və digər sahələrdə obyekt və sistemlərin monitorinqi və idarə olunması proseslərini avtomatlaşdırmağa, bu proseslər haqqında böyük həcmdə məlumatları yüksək sürətlə almağa, toplamağa, emal etməyə və ötürməyə imkan verir. Beləliklə, tam əminliklə demək olar ki, bu gün informasiyalaşdırma bəşəriyyətin inkişafında müsbət həlledici rol oynayır.

Qeyd etmək lazımdır ki, elmi nailiyyətlər, o cümlədən müasir informasiya texnologiyalarının imkanları heç də həmişə insanların, cəmiyyətin və dövlətin maraqları baxımından istifadə olunmur. Belə ki, ayrı-ayrı insanlar, təşkilatlar, dövlətlər və onların birlikləri tərəfindən öz maraqlarının ödənilməsi, eləcə də iqtisadi, kommersiya, hərbi qarşıdurmada ehtimal olunan rəqiblərinin maraqlarına əks-təsir (müqavimət) göstərmək məqsədilə informasiyanı, informasiya ehtiyatlarmı, vasitələrini və texnologiyalarını əldə etməyə can atması təbiidir.

Göründüyü kimi, informasiya, informasiya ehtiyatları və İKT rəqib tərəflərin maraqlarına müəyyən təhdidlər qismində çıxış edir. Qeyd olunan vəziyyət informasiya təhlükəsizliyi problemini doğurur. İnformasiya təhlükəsizliyinin konseptual və elmi metodiki əsasları son dövrlərdə işlənib hazırlanmağa başlanmışdır. Ona görə də, terminologiyanın dəqiqləşdirilməsi, informasiya təhlükəsizliyi probleminin elmi əsaslandırılması, bu sahədə həyati vacib maraqların və informasiya təhdidlərinin mənbələrinin təsnif edilməsi, informasiya təhlükəsizliyinin göstəriciləri, meyarları, normativləri, eləcə də digər xarakteristika və xassələri elmi-tədqiqat obyekti kimi gələcəkdə hələ çox tədqiqatların mövzusu olacaqdır.

Informasiya təhlükəsizliyi, informasiya təhlükəsi, informasiya təhdidləri, informasiyanın qorunması, informasiya maraqlan, informasiya mühiti və s. baza anlayışlarının da daxil

olduğu anlayışlar sisteminin yaradılması informasiya təhlükəsizliyi nəzəriyyəsinin yaradılmasının ilk məsələlərindən biridir.

Qeyd etmək lazımdır ki, təhlükəsizlik heç də həmişə qoruma nəticəsində təmin edilmir. Belə ki, təhlükəsizlik obyektlərin uyğun davranış və qarşılıqlı əlaqə qaydalarına riayət olunması, yüksək peşəkar personalın hazırlanması, texnikanın işinin sazlığının və informasiya təhlükəsizliyi obyektlərinin fəaliyyətinin etibarlılığının təmin edilməsi yolu ilə əldə oluna bilər.

Azərbaycan Respublikasının "Milli təhlükəsizlik haqqında" Qanunundan irəli gələrək aşağıda şəxsin, cəmiyyətin və dövlətin informasiya təhlükəsizliyi anlayışları verilir.

Şəxsin informasiya təhlükəsizliyi – insanı əhatə edən informasiya fəzasına təsir etmək yolu ilə onun şəxsiyyətinə əhəmiyyətli ziyanın vurulmasının mümkün olmadığı vəziyyətidir.

Cəmiyyətin informasiya təhlükəsizliyi – cəmiyyətin informasiya mühitinə təsir etmək yolu ilə ona əhəmiyyətli ziyanın vurulmasının mümkün olmadığı vəziyyətidir.

Dövlətin informasiya təhlükəsizliyi – dövlətin informasiya mühitinə təsir etmək yolu ilə ona əhəmiyyətli ziyanın vurulmasının mümkün olmadığı vəziyyətidir.

Sonda qeyd etmək lazımdır ki, milli təhlükəsizliyin təmin edilməsi üçün onun bütün istiqamətləri (iqtisadi, siyasi, sosial, hərbi, ekoloji, informasiya, elm, mədəniyyət və s.) üzrə təhlükəsizlik təmin edilməlidir. Aydındır ki, təhlükəsizlik bu istiqamətlər üzrə bir-birindən təcrid olunmuş şəkildə təmin edilə bilməz.

Bu baxımdan informasiya təhlükəsizliyi istiqaməti milli təhlükəsizliyin digər istiqamətləri ilə sıx bağlıdır və onların təmin edilməsinə bilavasitə təsir edir. Belə ki, qeyd olunduğu kimi, bütün fəaliyyət sahələrində idarəetmənin və qərar qəbuletmənin əsasmı informasiya təşkil edir. Ona görə də informasiyanın saxlanılması, emalı, ötürülməsi və istifadəsi zamanı onun təhlükəsizliyini təmin etmədən digər istiqamətlərdə milli təhlükəsizliyi təmin etmək mümkün deyil.

İnformasiya təhlükəsizliyi sahəsində əsas anlayışlar. İnformasiya təhlükəsizliyi probleminin daha ətraflı şərhinə keçməzdən əvvəl, informasiya cəmiyyətinin əsasmı təşkil edən informasiya anlayışı haqqında məlumatın verilməsi zəruridir. Belə ki, informasiya anlayışı olduqca geniş və müxtəlif anlamlarda işlədilir. Elə fəaliyyət sahəsi tapmaq mümkün deyil ki, orada informasiya anlayışı istifadə olunmasın. Burada informasiya anlayışı aşağıdakı kimi başa düşülür.

İnformasiya – təqdimat formasından asılı olmayaraq şəxslər, əşyalar, faktlar, hadisələr, təzahürlər, proseslər və anlayışlar haqqında məlumatlar və biliklərdir.

İnformasiya kompüterə daxil edilmiş verilənlər, proqram kodları, məktub, yaddaş qeydləri, işlər, düsturlar, sxemlər, çertyojlar, diaqramlar, məhsulun modelləri, prototiplər, dissertasiyalar, məhkəmə sənədləri və s. formalarda ola bilər.

Öz şəxsi maraqlarını, o cümlədən iqtisadi, kommersiya və s. məqsədlərini reallaşdırmaq üçün insanlarda informasiyaya tələbat (ehtiyac) yaranır, həmin insanları informasiyanın istehlakçısı adlandırırlar.

İnformasiya tələbatı – qeyri-maddi tələbatların bir növü olub özündə konkret məsələnin həlli və ya hər hansı məqsədin əldə olunması üçün zəruri olan informasiyaya tələbatı ehtiva edir.

İnformasiya təhlükəsizliyi sahəsində anlayışlara mövzu sahəsindən asılı olaraq bir neçə aspektdən yanaşılır və müxtəlif ədəbiyyatlarda informasiya təhlükəsizliyi sahəsində mövcud anlayışlara müxtəlif tərifiər verilir. Ona görə də burada bəzi anlayışların bir neçə tərifı verilmişdir. Kontekstdən asılı olaraq bu tərifiərdən biri istifadə olunur.

İnformasiya təhlükəsizliyi dedikdə, şəxslərin, təşkilatların və cəmiyyətin maraqlarına uyğun olaraq, informasiya mühitinin qorunmasının vəziyyəti, həmçinin informasiya təhlükəsizliyinin pozulması təhdidlərinin, bu təhdidlərin mənbələrinin, reallaşdırılması üsullarının və məqsədlərinin, təhlükəsizliyin pozulmasına gətirib çıxaran digər şərait və hərəkətlərin vaxtında aşkar edilməsi və qarşısının alınması vəziyyəti başa düşülür. Ədəbiyyatlarda informasiya təhlükəsizliyi anlayışının aşağıdakı tərifiərinə də rast gəlinir.

İnformasiya təhlükəsizliyi – informasiyanın emalı, saxlanılması və ötürülməsi zamanı məxfılik, tamlıq və əlyetərlilik kimi xassələrə qoyulan tələblərin təmin edilməsi qabiliyyəti ilə xarakterizə olunan vəziyyətdir.

İnformasiya təhlükəsizliyi informasiyanın və ya informasiyanı saxlayan infrastrukturun onun sahiblərinə və istifadəçilərinə ziyan vura biləcək süni və təbii xarakterli, təsadüfi və ya qəsdən törədilən təsirlərdən qorunması vəziyyətini özündə ehtiva edir.

İnformasiya təhlükəsizliyi – informasiya mühitində dövlətin, fiziki və hüquqi şəxslərin qorunmasının vəziyyətidir.

İnformasiya təhlükəsizliyi – vətəndaşların, təşkilatların və dövlətin maraqları çərçivəsində cəmiyyətin informasiyalaşdırılmasını təmin edən informasiya mühitinin qorunmasıdır.

İnformasiyanın qorunması – informasiyanın gizliliyinin, tamlığının və ona girişin (əlyetərliliyin) təmin edilməsinə yönəlmiş fəaliyyətdir.

İnformasiyanın qorunması – reallaşdırılması informasiyanın sahiblərinə və istifadəçilərinə ziyanın vurulması ilə nəticələnən təbii və süni xarakterli təhlükələrin təsir göstərdiyi şəraitlərdə informasiyanın gizliliyini, tamlığını və ona girişi (əlyetərliliyi) təmin edən müvafiq üsul və vasitələr kompleksi kimi dövlət, xidməti (kommersiya) və ya şəxsi sirlərin, eləcə də istənilən məzmunlu informasiya daşıyıcılarının qorunmasına yönəlmiş olur.

Informasiyanın qorunmasının məqsədləri aşağıdakılardan ibarətdir:

- dövlətin, ictimaiyyətin, vətəndaşların təhlükəsizliyinin təmin edilməsi;
- dövlət sirri təşkil edən və məxfı informasiyanın məxfıliyinin qorunması;
- informasiyanın məhvinin, itməsinin, təhrif edilməsinin, saxtalaşdırılmasının, surətinin çıxarılmasının, təcrid edilməsinin qarşısının alınması;
- informasiya proseslərində və informasiya sistemlərinin, texnologiyalarının və onların təminat vasitələrinin işlənməsi, istehsalı, tətbiqi zamanı fiziki və hüquqi şəxslərin hüquqlarının təmin olunması.

İnformasiya təhlükəsi anlayışına iki mənada – təhlükəni yaradan və təhlükəyə məruz qalan obyektlər baxımından tərif verilir.

İnformasiya təhlükəsi – informasiya mühitinə təsir etmək yolu ilə əhəmiyyətli zərər və ya ziyan vura biləcək imkanların mövcud olduğu obyektin və ya onun ətraf mühitinin vəziyyətidir.

İnformasiya təhlükəsi – obyektin hər hansı başqa obyektin informasiya mühitinə təsir etməklə ona əhəmiyyətli zərər və ya ziyan vura bilmək qabiliyyətini xarakterizə edən xassəsidir.

Praktikada informasiya təhlükəsi anlayışı ilə yanaşı informasiya təhdidi anlayışından da istifadə olunur. Bu anlayışlar bəzən səhvən eyniləşdirilir. Lakin qeyd olunmalıdır ki, bu anlayışlar tamamilə fərqli mahiyyətə malikdirlər və onları eyniləşdirmək olmaz.

İnformasiyanın təhlükəsizliyi dedikdə informasiya sistemində saxlanan və emal edilən informasiyanın mühafizəsi başa düşülür. İS-də informasiyanın mühafizəsi probleminə proqram və aparat vasitələrinin mühafizəsi problemi ilə birlikdə baxılması məqsədəuyğun hesab edilir, çünki İS-ın fəaliyyət mühitinin əsasını proqram və aparat vasitələri təşkil edirlər.

Informasiya təhdidi – obyektin hər hansı başqa obyektin informasiya mühitinə təsir etmək yolu ilə ona əhəmiyyətli zərər vurmaq niyyəti, yəni həmin obyektə qarşı yaratdığı təhlükədir. Başqa sözlə, informasiya təhdidi dedikdə obyekt üçün informasiya təhlükəsi yaradan amil və ya amillər toplusu başa düşülür.

Təhlükələrə misal olaraq əməkdaşların səhv, səhlənkar hərəkətlərini, davranışlarını, texniki nasazlıqları, təsadüfı prosesləri, təbiət hadisələrini və s. göstərmək olar. Təhdidlərə isə təhlükə yarada biləcək və qəsdən düşünülmüş hərəkətləri, davranışları və s. aid etmək olar.

Təsir üsullarına və vasitələrinə görə təhdidlərin aşağıdakı növlərini fərqləndirirlər:

- informasiya təhdidləri;
- proqram-riyazi təhdidlər;

- fiziki təhdidlər;
- təşkilati təhdidlər.

Informasiya təhdidləri informasiyanın hüquqazidd istifadəsi, neqativ manipulyasiya edilməsi (dezinformasiya, informasiyanın təhrif edilməsi, gizlədilməsi), informasiyanın emalı texnologiyasının korlanması və s. məqsədlər üçün informasiya ehtiyatlarına icazəsiz girişin həyata keçirilməsi və oğurlanması şəklində reallaşdırılır.

Proqram-riyazi təhdidlər sənədlərdə təsvir olunmayan və proqramların fəaliyyətinin, işlənib hazırlanmasının effektivliyini azaldan funksiyaları reallaşdıran komponentlərin aparat və proqram sistemlərinə yeridilməsi, sistemin, o cümlədən informasiyanın qorunması sisteminin normal fəaliyyətini pozan ziyanverici proqramların (kompüter viruslarının, "troya atlarının" və s.) yayılması yolu ilə reallaşdırılır.

Fiziki təhdidlər informasiya sistemlərinə və onların elementlərinə fiziki təsir edilməsi (məhv olunması, korlanması, oğurlanması), ötürmə kanallarında və ya otaqlarda informasiyanın siqnallar şəklində tutulması yolu ilə həyata keçirilir.

Təşkilati təhdidlər qanunvericilik bazasının zəif olması, normativ-hüquqi sənədlərin olmaması, iş rejiminin nizamlanmaması, qorunan informasiyanın, onun emal olunduğu və ya saxlandığı sistemin və kompüter texnikasının saxlandığı yerə girişin məhdudlaşdırılmaması, personalın peşəkarlığının aşağı olması, vəzifəsinə laqeyd və səhlənkar yanaşması, eləcə də texniki, istismar, təhlükəsizlik və digər qaydalara riayət olunmaması kimi səbəblərdən istifadə etməklə reallaşdırılır.

Ümumi halda, məqsəd və nəticələrinə görə təhdidləri üç yerə bölmək olar:

- qorunan informasiyanın əldə edilməsi və onunla tanış olma;
- şəxsi mənfəət məqsədilə informasiyanın dəyişdirilməsi (təhrif edilməsi);
- birbaşa maddi və mənəvi ziyan vurmaq məqsədilə informasiyanın məhv edilməsi.

İnformasiya təhlükəsizliyi ilə bağlı aşağıdakı anlayışların da verilməsi zəruridir.

İnformasiya mühiti – müəyyən şəkildə strukturlaşdırılmış informasiya ehtiyatlan toplusudur. İnformasiya mühiti dedikdə, həmçinin obyekt və ya subyektlərin informasiyanın yaradılması, əldə olunması, emalı, ötürülməsi və işlədilməsi ilə bağlı olan fəaliyyətlərin həyata keçirildiyi mühit başa düşülür. İnformasiya mühitinin təhlükə və ya təhdidlərə məruz qala biləcək əsas obyektləri – informasiya infrastrukturu, informasiya resursu, informasiya sistemi və digər sistemlərdir. İnformasiya mühitində qarşıdurmanın özəyini kompüter sistemləri və şəbəkələri təşkil edir.

İnformasiya müharibəsi – maddi, hərbi, siyasi və ya ideoloji sahələrdə müəyyən üstünlük əldə etmək məqsədilə sistemlərin bir-birinə açıq və gizli məqsədyönlü informasiya təsirləridir.

Başqa sözlə, informasiya müharibəsi – informasiya üstünlüyü əldə etmək məqsədilə özünəməxsus olan informasiya resurslarmı, informasiyaya əsaslanmış prosesləri və informasiya sistemlərini qorumaq, eləcə də rəqibin informasiya resurslarına, informasiyaya əsaslanmış proseslərinə və informasiya sistemlərinə ziyan vurmaq yolu ilə həyata keçirilən əməliyyatlardır.

Informasiya silahı – bütövlükdə informasiya infrastrukturunun və onun ayrı-ayrı elementlərinin funksiyalarının və ya xidmətlərinin müvəqqəti və ya tamamilə sıradan çıxarılması üçün tətbiq olunan xüsusi (fiziki, informasiya, proqram, radioelektron və s.) üsul və vasitələr toplusudur.

İnformasiya silahı, həmçinin informasiya müharibəsi zamanı düşmənə informasiya təsiri göstərməyə imkan verən üsul və vasitələr toplusu kimi başa düşülür, dövlətin və ya onun silahlı qüvvələrinin informasiya obyektlərini, eləcə də onların qorunması sistemlərini sarsıdan, dağıdan, məhv edən vasitə, qurğu və texnologiyaların tətbiqinə əsaslanan dağıdıcı təsirlərə malik xüsusi silahdır.

İnformasiya kriminalı – ayrı-ayrı şəxslərin və ya qrupların tamahkarlıq və ya xuliqanlıq məqsədilə informasiya mühitinə və ya onun istifadəsinə ziyan vurulmasına, o cümlədən

kompüter şəbəkələrində və informasiya sistemlərində informasiyanın oğurlanmasına və ya məhv edilməsinə yönəlmiş düşünülmüş cinayətkar əməllərdir.

İnformasiya terrorçuluğu – terrorçu təşkilat və ya ayrı-ayrı terrorçular tərəfindən siyasi, iqtisadi, dini və başqa maraqlarının reallaşdırılması məqsədilə dövlətin və ya beynəlxalq təşkilatın məcbur edilməsi üçün şüurlu və məqsədyönlü şəkildə informasiya təsirini və ya belə təsirin göstərilməsi təhdidini özündə ehtiva edən, qorxu, vahimə əhval-ruhiyyəsi, hakimiyyətə etibarın itirilməsi və siyasi qeyri-stabilliyin yaradılması üçün cəmiyyətə emosional təsirlə müşayiət olunan terrorçuluğun və zorakılığın xüsusi formasıdır.

İnformasiya təhlükəsizliyinin konseptual modeli. İnformasiya təhlükəsizliyi sahəsində vəziyyətin təhlili göstərir ki, informasiyanın qorunması üzrə artıq formalaşmış konsepsiya və yanaşma mövcuddur. Onun əsasmı aşağıdakılar təşkil edir:

- sənaye yolu ilə istehsal olunan informasiyanın qorunması vasitələrinin inkişaf etmiş arsenalının olması;
- informasiyanın qorunması məsələlərinin həlli ilə məşğul olan çoxlu sayda ixtisaslaşmış mütəxəssislərin və təşkilatların mövcudluğu;
- bu problemə kifayət qədər dəqiq müəyyənləşmiş baxışlar sisteminin formalaşması;
- əhəmiyyətli dərəcədə praktiki təcrübənin olması və s.

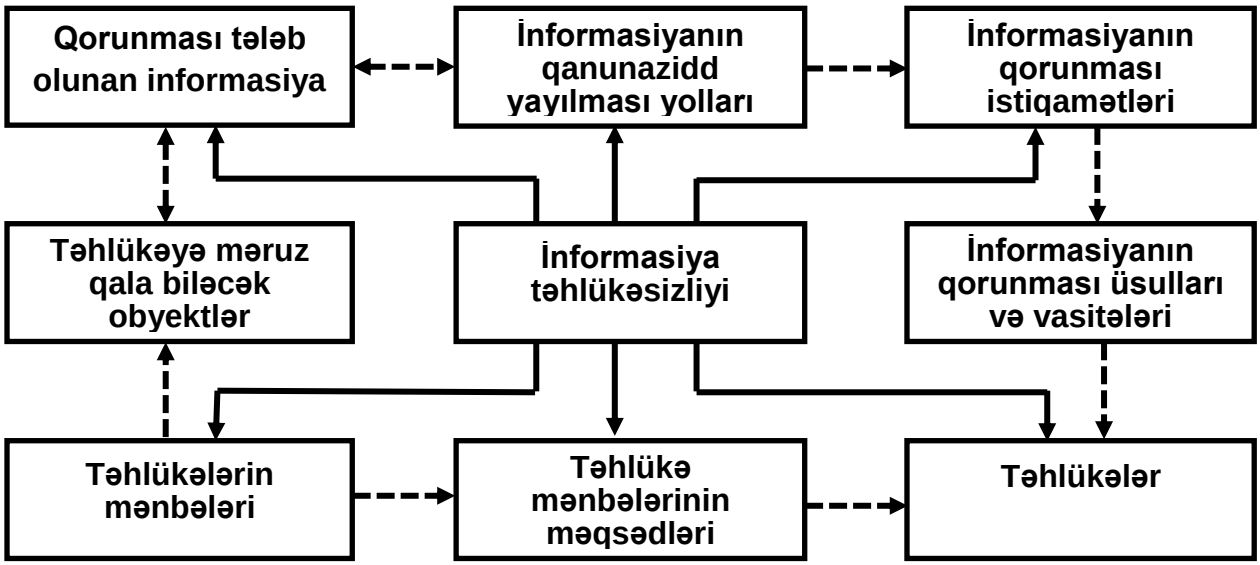
Amma buna baxmayaraq, informasiyaya, informasiya ehtiyatlarına və sistemlərinə qarşı bədniyyətli hərəkətlər azalmır, əksinə, bu sahədə kifayət qədər artım tendensiyası müşahidə olunur. İnformasiya təhlükəsizliyinin təmin edilməsində peşəkar mütəxəssislər, rəhbərlik, inzibatçılar, əməkdaşlar və istifadəçilər fəal surətdə birgə iştirak etməlidirlər.

İnformasiyanın qorunması prosesi kəsilməz, planlı, məqsədyönlü, konkret, fəal, etibarlı, universal, kompleks şəkildə həyata keçirilməlidir.

Qeyd olunanlar nəzərə alınmaqla informasiyanın qorunması xüsusi şəkildə təşkil olunmuş, özündə bütün zəruri üsullar, vasitələr və tədbirlər toplusunu birləşdirən informasiya təhlükəsizliyi (informasiyanın qorunması) sistemi (İTS) vasitəsilə həyata keçirilir.

İnformasiya təhlükəsizliyinin effektiv təmin edilməsi üçün qorunması tələb olunan informasiya resurslarının, onların qiymətlilik dərəcələrinin, eləcə də onlara qarşı yarana biləcək təhlükələrin, bu təhlükələrin mənbələrinin, məqsədlərinin, həyata keçirilməsi mexanizmlərinin müxtəlifliyini nəzərə alaraq, informasiya təhlükəsizliyinin real vəziyyətini, mühiti və mümkün hərəkətləri özündə ehtiva edən konseptual modeli qurmaq böyük əhəmiyyət kəsb edir.

İnformasiya təhlükəsizliyinin konseptual modelinə aşağıdakı əsas komponentlər daxil edilir (şəkil 1.2):



Şəkil 1.2 İnformasiya təhlükəsizliyinin konseptual modeli.

- təhlükəyə məruz qala biləcək obyektlər;
- qorunması tələb olunan informasiya;
- təhlükələr;
- təhlükələrin mənbələri;
- təhlükələrin mənbələrinin məqsədləri;
- qorunan informasiyanın qanunazidd şəkildə yayılması (sızması) yolları;
- informasiya təhlükəsizliyinin təmin edilməsinin istiqamətləri;
- informasiyanın qorunması üsulları və vasitələri.

Təhlükəyə məruz qala biləcək obyektlər dedikdə, informasiya daşıyıcıları (mənbələri), o cümlədən insanlar, sənədlər, nəşrlər, informasiya resursları, onların texniki daşıyıcıları, istehsal və əmək fəaliyyətinin təmin edilməsinin texniki vasitələri, istehsalat məhsulları və tullantılar və s. başa düşülür.

Qorunması tələb olunan informasiya – təhlükəyə məruz qala biləcək obyektlər və bu obyektlər haqqında (o cümlədən onların tərkibini, məzmununu, vəziyyətini və fəaliyyətini əks etdirən) məlumatlardır.

Təhlükələr – qorunan informasiyanın məxfiliyinin, tamlığının (bütövlüyünün) və əlyetərliliyinin (ona giriş imkanlarının) pozulması ilə nəticələnən hallarını özündə ehtiva edir.

Təhlükələrin mənbələri qismində rəqiblər, cinayətkarlar, inzibati idarəetmə və xüsusi xidmət orqanları, əməkdaşlar, həvəskar proqramçılar və s. çıxış edə bilərlər.

Təhlükələrin mənbələri qorunan məlumatlarla tanış olmaq, onları dəyişdirmək və ya məhv etmək, maddi ziyan vurmaq, qərarların qəbuluna və ya dəyişdirilməsinə təsir etmək, intiqam almaq, öz imkanlarmı, bacarığını nümayiş etdirmək kimi qərəzli və qərəzsiz məqsədlər güdə bilərlər.

- İnformasiya təhlükəsizliyinin konseptual modelində qorunan informasiyanın qanunazidd şəkildə aşağıdakı yollarla yayılmasının mümkünlüyü fərz edilir:
- qorunan məlumatların mənbələri (sahibləri və ya müəllifləri) tərəfindən qəsdən və ya təsadüfən açılması və ya sızdırılması;
- texniki vasitələrin köməyi ilə rəqib və ya kənar şəxslər tərəfindən məqsədyönlü şəkildə ələ keçirilməsi;
- qorunan informasiyaya icazəsiz giriş (daxilolma).

Modeldə, informasiya təhlükəsizliyinin təmin edilməsinin, əsasən, aşağıdakı istiqamətlərdə həyata keçirildiyi nəzərdə tutulur:

1. qanunvericilik;
2. təşkilati tədbirlər;
3. mühəndis-texniki vasitələr;
4. mənəvi-etik normalar.

İnformasiyanın qorunmasının əsas vasitələrinə fiziki qurğular, aparat vasitələri, proqram təminatları və kriptoqrafik üsullar aid edilir. Qeyd edilməlidir ki, kriptoqrafık üsullar həm proqram, həm texniki, həm də proqram-texniki vasitələr şəklində reallaşdırıla bilər.

Konseptual modelə daxil edilmiş komponentlər informasiya təhlükəsizliyinin təmin edilməsi, daxili və xarici təhlükələrdən qorunması üçün kompleks yanaşmanı reallaşdırmağa imkan verir, bütün mümkün tədbirləri, mexanizmləri və hərəkətləri özündə birləşdirir, qanunazidd əməllərin və icazəsiz girişin xəbərdar edilməsi, qarşısının alınması və baş vermiş təhlükələrin nəticələrinin aradan qaldırılması yollarını nəzərdə tutur.

İnformasiya təhlükəsizliyinin əsas istiqamətləri və baza prinsipləri. Yuxarıda qeyd olunduğu kimi, informasiya təhlükəsizliyinin pozulmasının bütün mümkün hallarını, əsasən, üç kateqoriyaya ayırmaq olar:

- informasiyanın məxfiliyinin pozulması;
- informasiyanın tamlığının pozulması;
- sistemin iş qabiliyyətinin pozulması (xidmətin göstərilməsindən imtina).

Məxfiliyin pozulması təhlükələri məxfi informasiyanın və ya sirlərin açılmasına yönəlmiş olur. Bu növ təhlükələr reallaşdıqda informasiya ona giriş hüququ olmayan şəxslərin əlinə keçə və ya onlara bəlli ola bilər. Kompüter sistemlərində və şəbəkələrində saxlanılan və ya ötürülən məxfi informasiyaya hər dəfə icazəsiz giriş əldə edildikdə və ya buna cəhd göstərildikdə, uyğun olaraq, onun gizliliyi pozulur və ya gizliliyinin pozulması təhlükəsi yaranır.

Saxlanılan və ya ötürülən informasiyanın tamlığının pozulması təhlükələri onun təhrif olunmasına, keyfiyyətinin pozulmasına və ya tam məhvinə gətirib çıxaran dəyişikliklərin edilməsi ilə xarakterizə olunur. İnformasiyanın tamlığı ziyankar (bədniyyətli) şəxslərin düşünülmüş fəaliyyəti, eləcə də ətraf mühitin obyektiv təsiri nəticəsində pozula bilər.

Sistemin iş qabiliyyətinin pozulması (xidmətin göstərilməsindən imtina edilməsi) təhlükəsi müəyyən düşünülmüş hərəkətləri, eləcə də təsadüfi hadisə və proseslər nəticəsində avtomatlaşdırılmış sistemlərin, o cümlədən kompüter sistemlərinin və şəbəkələrinin fəaliyyətinin pozulmasına, iş qabiliyyətinin zəifləməsinə, informasiya resurslarına icazəli və ya qanuni girişin məhdudlaşdırılmasına, tamamilə bağlanmasına gətirib çıxaran vəziyyətlərin reallaşdırılmasına yönəlmiş olur.

Göründüyü kimi, informasiya məxfilik, tamlıq və əldə olunması (ona girişin təmin edilməsi) baxımından qiymətli ola (əhəmiyyət kəsb edə) bilər. Başqa sözlə, informasiyanın məxfiliyi və ya tamlığı pozulduqda, ona icazəli giriş təmin edilmədikdə qiymətliliyinin itməsi təhlükəsi yaranır.

İnformasiya resurslarına qarşı yönəlmiş bu təhlükələrin təsnifatına uyğun olaraq onların qarşısının alınması və informasiya təhlükəsizliyinin təmin edilməsi məsələsinə də, əsasən, üç aspektdən baxılır. Bu istiqamətlər informasiya təhlükəsizliyinin üç əsas baza prinsipini müəyyən edir:

- informasiyanın gizliliyinin təmin edilməsi;
- informasiyanın tamlığının təmin edilməsi;
- informasiyaya icazəli girişin təmin edilməsi (informasiyanın təcrid edilməsinin qarşısının alınması və ya informasiyaya əlyetərliliyin təmin edilməsi).

İnformasiyanın gizliliyinin təmin edilməsi dedikdə, informasiyaya giriş hüququ olan istifadəçilər qrupunun müəyyənləşdirilməsi, informasiyaya, onun saxlandığı, emal olunduğu, ötürüldüyü sistem və şəbəkələrə kənardan, ələlxüsus icazəsiz müdaxilələrin və müdaxilə cəhdlərinin qarşısının alınması başa düşülür.

Informasiyanın gizliliyi – onun məzmununun icazəsi olmayan digər istifadəçilərdən və kənar şəxslərdən gizli saxlanılması xassəsidir. Bu, icazəsiz olaraq məxfi informasiyanın məzmununun açılması, proqramların, məlumat bazalarının, sistem cədvəllərinin və parametrlərinin istifadəsi və onlara müdaxilə təhlükələrinin qarşısının alınmasının təmin edilməsini nəzərdə tutur.

Aydındır ki, istifadəçilərin müəyyən informasiya resurslarına girişinə məhdudiyyətlərin qoyulması digər istifadəçilərin, o cümlədən informasiya resurslarına sahiblərinin qanuni hüquqlarını qorumaq zərurətindən meydana gəlir.

Əgər informasiya məxfilik (konfidensiallıq) baxımından qiymətlidirsə, onda icazəsi olmayan şəxslər tərəfindən onun məğzi açıldıqda o, qiymətini itirmiş olur. Belə informasiyanın məğzinin kənar şəxslərdən gizli saxlanması üçün müvafiq üsullar reallaşdırılır.

İnformasiyanın tamlığının təmin edilməsi – sistemdə saxlanılan, emal olunan və ötürülən informasiyanın təhrif olunmamış (yəni onun hər hansı qeyd olunmuş vəziyyətinə münasibətdə dəyişilməmiş) şəkildə mövcud olmasının və ünvana çatdırılmasının təmin

edilməsini özündə ehtiva edir. İnformasiyanın bu xassəsi onun icazəsiz olaraq qəsdən və ya təsadüfən dəyişdirilməsinə, korlanmasına, təcrid olunmasına və ya məhv edilməsinə, eləcə də informasiyanın itirilməsinə gətirib çıxaran proqram-texniki nasazlıqlar və sıradan çıxmalar kimi təhlükələrdən də qorunmasını tələb edir.

Bəzən istifadəçiləri informasiyanın həqiqiliyinin (doğruluğunun) təmin edilməsi daha çox maraqlandırır. Bu mənada informasiyanın həqiqiliyi xassəsi mövzu sahəsinin vəziyyətinin adekvat (dolğun və dəqiq) əks olunmasını və bilavasitə informasiyanın tamlığını, yəni mövzu sahəsinin təhrif olunmamış şəkildə təsvirini nəzərdə tutur. Lakin informasiya təhlükəsizliyi baxımından yalnız informasiyanın ilkin formasının tamlığının təmin edilməsi məsələsi maraq kəsb edir, mövzu sahəsinin əks olunmasının adekvatlığı isə informasiya təhlükəsizliyi problemlərindən kənara çıxır, ona görə də burada baxılmır.

Əgər informasiya tamlıq baxımından qiymətli hesab edilirsə, bu, o deməkdir ki, icazəsi olmayan şəxslər tərəfindən onun məzmununda dəyişikliklərin aparılmasına və ya məhv edilməsinə yol verilə bilməz. Əgər informasiya icazəsiz dəyişdirilərsə və ya məhv edilərsə, onda o, qiymətini itirmiş hesab olunur. Belə halların qarşısının alınması üçün informasiyanın tamlığının təmin olunması üsulları tətbiq edilir.

İnformasiyaya girişin təmin edilməsi – informasiyanın saxlanılması, emalı və ötürülməsi sistemlərinin (mühitinin, vəsaitlərinin və texnologiyalarının) etibarlılıq və sıradan çıxmalara davamlılıq xassələrinə qoyulan başlıca tələb olub, informasiya və sistem resurslarına icazəli girişə rədd cavablarının verilməsinin qarşısının alınması, istifadəçilərin onları maraqlandıran və giriş hüquqları olan bütün informasiya resurslarına maneəsiz və vaxtında girişinin təmin edilməsi, eləcə də istifadəçilərdən daxil olan bütün sorğuların müvafiq avtomatlaşdırılmış xidmətlər tərəfindən yerinə yetirilməsi qabiliyyətini xarakterizə edir.

İnformasiyaya girişin təmin edilməsi prinsipini onun sahibindən, qanuni icazəsi olan şəxslərdən təcrid edilməsinin qarşısının alınması və ya informasiyaya əlyetərliliyin təmin edilməsi kimi də başa düşmək olar.

Qanuni hüququ olan şəxslərin müraciəti zamanı onların lazımi informasiyaya vaxtında girişlə təmin edilməməsi səbəbindən informasiya öz qiymətliliyini (əhəmiyyətini) itirmiş olarsa, onda deyirlər ki, belə informasiyanın əldə edilməsi imkanlarının pozulması, yəni təcrid olunması təhlükəsi yaranmışdır. Bu təhlükənin aradan qaldırılması üçün bütün qanuni müraciətlər zamanı informasiyaya girişin təmin edilməsi məqsədilə sistemdə zəruri tədbirlər nəzərdə tutulur.

Ümumiyyətlə, nəzərə almaq lazımdır ki, informasiya təhlükəsizliyinin pozulması yalnız ayrı-ayrı kompüter sistemlərinin və şəbəkələrinin sıradan çıxmasından, ayrı-ayrı şəxslərə (o cümlədən istifadəçilərə) və ya təşkilatlara maddi və mənəvi ziyanın vurulmasından ibarət deyil.

Belə ki, elektron ödəmələrin, kağızsız sənəd dövriyyəsinin və digər texnologiyaların reallaşdırıldığı ayrı-ayrı kompüterlərdə və kompüter şəbəkələrində informasiya təhlükəsizliyinin pozulması, həmçinin şirkətlərin, bankların və digər böyük təşkilatların işinin dayanmasına, dövlət səviyyəsində ciddi problemlərin yaranmasına və əhəmiyyətli dərəcədə maddi itkilərə gətirib çıxara bilər.

Qeyd etmək lazımdır ki, ayrı-ayrı fəaliyyət sahələrində (bank və maliyyə qurumlarında, dövlət idarəetmə sistemlərində, müdafiə və xüsusi xidmət orqanlarında) həll edilən məsələlərin xarakterindən və vacibliyindən asılı olaraq, kompüter sistemlərində və şəbəkələrində informasiya təhlükəsizliyinin təmin edilməsi məqsədilə müxtəlif səviyyələrdə əlavə tədbirlərin görülməsi, onların fəaliyyətinin etibarlılığının yüksəldilməsi tələb olunur.

Məxfi xarakterli məlumatların saxlandığı, emal olunduğu və ötürüldüyü kompüter şəbəkələrinə və sistemlərinə malik olan hər bir təşkilatda (dövlət və hökumət

orqanlarında, özəl müəssisələrdə), bir qayda olaraq, informasiya təhlükəsizliyinə cavabdeh olan mütəxəssislər və ya struktur bölməsi fəaliyyət göstərir. Onlar bu təşkilatlarda saxlanılan və emal olunan informasiyanın tamlığını, məxfiliyini və əlyetərliliyini təmin etmək üçün vahid İTS-in işlənib hazırlanmasını və düzgün istismarını təşkil edirlər. İTS-in funksiyalarına, həmçinin, fiziki (texniki vəsaitlər, rabitə xətləri və uzaq məsafədə olan kompüterlər) və məntiqi (məlumat bazaları, tətbiqi proqramlar, əməliyyat sistemləri) baxımdan informasiyanın qorunması məsələləri də aiddir.

Sual 2. Kompüter sistemlərində və şəbəkələrində informasiya təhlükəsizliyi

İnformasiya təhlükəsizliyi baxımından kompüter sistemlərinin və şəbəkələrinin xüsusiyyətləri. Şirkətlər, nazirlik və komitələr səviyyəsində qurulan və bu təşkilatlar çərçivəsində informasiyanın emalı, saxlanılması və ötürülməsini həyata keçirən kompüter sistemlərində və şəbəkələrində (KSŞ) informasiyanın qorunması məsələsi bu gün çox aktualdır. Belə ki, dövlət və hökumət orqanlarında, eləcə də özəl şirkətlərdə yaradılmış kompüter şəbəkələrində informasiya emalı və saxlanması sistemlərində şəxsi, kommersiya və dövlət sirləri təşkil edən böyük həcmdə müxtəlif təyinatlı məlumatlar emal olunur, saxlanılır, rabitə kanalları vasitəsilə ötürülür.

İnformasiya təhlükəsizliyinin təmin edilməsi üçün sistemə və şəbəkəyə girişin idarə olunması, istifadəçilərin identifikasiyası, rabitə kanalları ilə ötürülən məlumatların məzmununun gizlədilməsi, məlumatların, istifadəçinin və şəbəkənin həqiqiliyinin müəyyən edilməsi, imzaların təsdiq olunması, eləcə də rabitə kanallarının, informasiya daşıyıcılarının, xidməti personalın və s. fiziki qorunması həlli tələb olunan məsələlərdir. Bu siyahını çox genişləndirmək olar, lakin qeyd olunanlar KSŞ-də informasiya təhlükəsizliyi probleminə kompleks yanaşmanın zəruriliyini kifayət qədər nümayiş etdirir.

Əvvəlki fəsildə qeyd olunduğu kimi, KSŞ-də informasiyanın təhlükəsizliyinin zəmanətli təmin edilməsi məqsədilə mümkün təhlükələrin qarşısının alınması üçün sistemdə bütün zəruri üsul və vasitələrin reallaşdırılması və vahid İTS-in yaradılması məsələlərinə kompleks şəkildə baxılmalıdır.

Məhz buna görə də KSŞ-nin xüsusiyyətlərinin araşdırılması və bu şəbəkələrdə yarana biləcək təhlükələrin təsnif edilməsi, hər bir mümkün təhlükəyə qarşı heç olmasa bir üsul və ya vasitənin reallaşdırılmasını təmin edən təhlükəsizlik sisteminin modelinin qurulması və ona verilən tələblərin müəyyən edilməsi zəruridir.

Aydındır ki, İTS-in konseptual və riyazi modellərinin qurulması, yaradılma prinsiplərinin elmi əsaslarla işlənməsi yolu ilə KSŞ-də İTS-in fəaliyyətinin effektivliyi təmin edilə və informasiyanın təhlükəsizliyinə zəmanət verilə bilər.

KSŞ qarşılıqlı əlaqəli kompüter şəbəkələrini, məlumatların emalı və ötürülməsi sistemlərini, telekommunikasiya qurğuları və avadanlıqları kompleksini özündə birləşdirən, qorunması tələb olunan şəbəkə – informasiya fəzasıdır. Onun tərkibinə bir çox funksional elementlər daxil olur. Bu funksional elementləri iki kateqoriyaya ayırmaq olar: əsas və əlavə funksional elementlər.

Əsas funksional elementlər aşağıdakılardan ibarətdir:

- işçi stansiyalar (istifadəçi kompüterləri) – istifadəçilərin (abonentlərin, operatorların) avtomatlaşdırılmış iş yerlərinin reallaşdırıldığı ayrı-ayrı kompüterlər və ya uzaq məsafədə yerləşən terminallardan ibarət olub, bir otaq və ya bina daxilində cəmləşə, eləcə də böyük ərazidə və ya bir-birindən uzaq məsafədə qeyri-məhdud şəkildə paylana bilər;
- funksional serverlər – KSŞ-də böyük həcmdə məlumatların toplanması, saxlanılması, emal edilməsi, istifadəçilərə müxtəlif xidmətlərin göstərilməsi funksiyalarını reallaşdıran, böyük yaddaşa və sürətə malik olan kompüterlərdir;

- telekommunikasiya qurğuları və rabitə vasitələri – KSŞ-də işçi stansiyalar, işçi stansiyalarla serverlər, şəbəkə seqmentləri arasında qarşılıqlı əlaqəni təmin edən komponentlər (şəbəkələrarası körpülər, şlüzlər, kommutatorlar, konsentratorlar, kommutasiya mərkəzləri və s.), eləcə də lokal, telefon (ayrılmış və ya kommutasiya edilən) və optik rabitə xətləri, radio və peyk kanallarını özündə ehtiva edir.
- qarşılıqlı əlaqə xidmətləri – şəbəkə, o cümlədən Internet, faks, telefon və digər xidmətlərini özündə ehtiva edir.

Əlavə funksional elementlərə aşağıdakı sistem və modulları aid etmək olar:

- şəbəkənin istismarı, diaqnostikası və nəzarəti sistemləri;
- şəbəkənin effektivliyinin idarə olunması sistemi;
- informasiya təhlükəsizliyinin təmin edilməsi sistemi.

KSŞ-də informasiya təhlükəsizliyinin təmin edilməsi dedikdə, icazəsiz olaraq onların fəaliyyət prosesinə müdaxilə, informasiya resurslarına giriş, onların oğurlanması, dəyişdirilməsi, məhv edilməsi, sistem komponentlərinin və informasiya daşıyıcılarının sıradan çıxarılması və ya məhv edilməsi hallarının qarşısının alınması, proqram-texniki təminatın, informasiya resurslarının, avadanlıqların, rabitə kanallarının və xidməti personalın kompleks qorunması və onların fəaliyyətinə nəzarət olunması məsələləri nəzərdə tutulur.

KSŞ-də informasiya təhlükəsizliyinin təmin edilməsi zamanı onun aşağıdakı əsas xüsusiyyətləri nəzərə alınmalıdır:

- informasiyanın saxlanılması, emalı və ötürülməsi üçün istifadə edilən üsulların, kompüter texnikasının, telekommunikasiya vasitələrinin və rabitə kanallarının, eləcə də proqram təminatının spektri genişdir;
- kompüter sistemlərinin və şəbəkələrinin komponentləri coğrafı baxımdan bir-birindən uzaq məsafədə yerləşir və onlar arasında intensiv informasiya mübadiləsi həyata keçirilir;
- müxtəlif subyektlərə aid olan müxtəlif təyinatlı məlumatlar vahid məlumat bazası çərçivəsində inteqrasiya olunur və əksinə, hər hansı subyektə lazım olan informasiya kompüter şəbəkəsinin uzaq məsafələrdə olan müxtəlif qovşaqlarında yerləşir;
- informasiya sahibləri fiziki qurğulardan, avadanlıqlardan və informasiyanın saxlanması yerlərindən təcrid edilmiş olur;
- informasiya resursları şəbəkənin qovşaqları üzrə paylanmış olur, onlar kollektiv şəkildə istifadə və emal edilir, bu resurslara eyni zamanda çoxlu sayda müraciətlər olunur;
- avtomatlaşdırılmış informasiya emalı prosesində çoxlu sayda istifadəçi və müxtəlif kateqoriyalı personal iştirak edir;
- informasiya emalı sistemlərində geniş istifadə edilən texniki vəsaitlərin əksəriyyətində aparat səviyyəsində xüsusi qoruma vasitələri reallaşdırılmır.

Qeyd olunanlara əsasən, demək olar ki, KSŞ-nin qurulması və istismarı zamanı istifadə olunan proqram təminatı və texniki vasitələr, o cümlədən kompüter texnikası, telekommunikasiya qurğuları, əməliyyat sistemləri, ofis və tətbiqi proqramlar, məlumat bazaları və digər informasiya resursları hücum obyekti ola və təhlükəyə məruz qala bilərlər.

Kompüter sistemlərində və şəbəkələrində informasiyanın qorunmasının xüsusiyyətləri. Kompüterlərin, KSŞ-nin geniş yayılması, güclü şəbəkə infrastrukturlarının yaranması, informasiya resurslarının kütləvi istifadəsi və proqramlaşdırma texnologiyasının təkmilləşməsi informasiya təhlükəsizliyinin təmin olunmasını daha böyük əmək tələb edən və baha başa gələn proseduraya çevirmişdir. Bu problemin daha da kəskinləşməsində nəhəng kompüter şəbəkəsi olan İnternetin də əhəmiyyətli rolu olmuşdur.

İnformasiyanın emalı texnologiyalarının təkmilləşməsi böyük həcmdə və müxtəlif növ məlumatları özündə saxlayan nəhəng məlumat bazalarının yaranmasına gətirib çıxarmışdır ki, bu da informasiya təhlükəsizliyinin təmin edilməsinə əlavə tələblər qoyur. Belə ki, müasir informasiya sistemləri uzaq məsafədə olan terminallardan çoxsaylı istifadəçilərin sistem və şəbəkə resurslarına eyni zamanda girişini təmin edir.

Bununla əlaqədar olaraq, informasiyanın rabitə kanalları ilə ötürülməsi zamanı informasiya sisteminin hər hansı istifadəçisinə (istifadəçilərinə) məxsus olan proqramların və məlumatların digər istifadəçilərin icazəsiz müdaxiləsindən qorunması problemi də böyük aktuallıq kəsb edir.

İnformasiyanın qorunması vasitələrinin işlənib hazırlanması təcrübəsinin təhlili göstərir ki, informasiya təhlükəsizliyi sahəsində meydana çıxan problemlər, adətən, çoxlu sayda informasiya sistemləri kütləvi şəkildə sıradan çıxdıqdan və ya xarab olduqdan sonra diqqəti cəlb etməyə başlayır.

Ona görə də böyük KSŞ-də informasiyanın təhlükəsizliyinin etibarlı təmin edilməsi üçün bu məsələyə sistemin layihələndirilməsi mərhələsində başlamaq lazımdır. Bu baxımdan əvvəlcədən müvafıq təhlil aparılmadan informasiyanın qorunması sistemlərini layihələndirmək, müvafıq proqram-texniki vasitələri almaq və quraşdırmaq məqsədəuyğun hesab olunmur.

İnformasiya təhlükəsizliyi baxımından mümkün risklərin təhlili bir çox amillərin (sistemin sıradan çıxması, işinin dayanması, kommersiya itkiləri nəticəsində dəyən ziyanlar, sistemin hazırlıq əmsalının aşağı düşməsi, ictimai münasibətlərin pozulması, hüquqi problemlərin yaranması və s.) obyektiv qiymətləndirilməsini, təhlükələrin növlərinin və səviyyələrinin müəyyənləşdirilməsini təmin etməlidir.

Son zamanlar çoxlu sayda dövlət və özəl təşkilatlar mühüm həyati vacib korporativ məlumatları böyük hesablama sistemlərindən açıq tipli kompüter şəbəkələrinə keçirmələri ilə əlaqədar olaraq, belə şəbəkələrdə İTS-in reallaşdırılmasına daha çox zərurət yaranmışdır. Belə sistemlərin istismarı prosesində informasiya təhlükəsizliyi baxımından yeni və daha ciddi problemlər meydana çıxır.

Ona görə də hazırda əksər təşkilatlar paylanmış məlumat bazalarının, biznes və kommersiya məlumatlarının idarə edilməsi üçün müştəri-server texnologiyasına əsaslanan, təhlükəsizlik tələblərinə bu və ya digər dərəcədə cavab verən əlavə proqram təminatlarını reallaşdırırlar. Belə sistemlərin KSŞ üzrə paylanma dərəcəsi artdıqca, məlumatlara icazəsiz giriş və onların təhrif olunması riski də artır.

Aydındır ki, fərdi kompüterlər (işçi stansiyalar) təhlükəyə məruz qala biləcək obyekt olmaqla yanaşı, həm də təhlükələrin yaranması vasitəsi, yəni aləti rolunu oynaya bilər.

Adətən, KSŞ-də informasiyanın əldə olunması və onların emalı sistemlərinin və vasitələrinin fəaliyyətinə icazəsiz müdaxilə edilməsi üçün bir çox imkanlar mövcud olur.

Başqa sözlə, kənardan daxilolmanı (müdaxiləni) və informasiya resurslarına icazəsiz girişi reallaşdırmağa imkan verən proqram və texniki boşluqların, spesifık kanalların və ya zəif yerlərin olması belə KSŞ üçün xarakterikdir.

Qeyd olunduğu kimi, statistik məlumatlara əsasən, dünyanın əksər ölkələrini əhatə edən İnternet şəbəkəsi yüz milyonlarla istifadəçiyə özünün xidmət və resurslarını təqdim edir. İnternet şəbəkəsində olan serverlərin sayı hazırda bir neçə milyonu ötüb keçmişdir. Artıq, demək olar ki, İnternetə bütün dövlət və hökumət orqanları, akademik və elmi-tədqiqat institutları, universitetlər, korporativ şəbəkələr, özəl və kommersiya təşkilatlan, ayrı-ayrı istifadəçilər və s. qoşulmuşdur.

Açıq şəbəkə olduğundan İnternetdə informasiya təhlükəsizliyi məsələsi korporativ və lokal şəbəkələrə nisbətən daha ciddi şəkildə durur və getdikcə daha kəskin xarakter alır.

Hazırda KSŞ-nin layihələndirilməsi zamanı əsas tələblərdən biri kimi informasiyanın qorunması vasitələrinin sistemin tərkibində reallaşdırılması qoyulur. İnformasiyanın

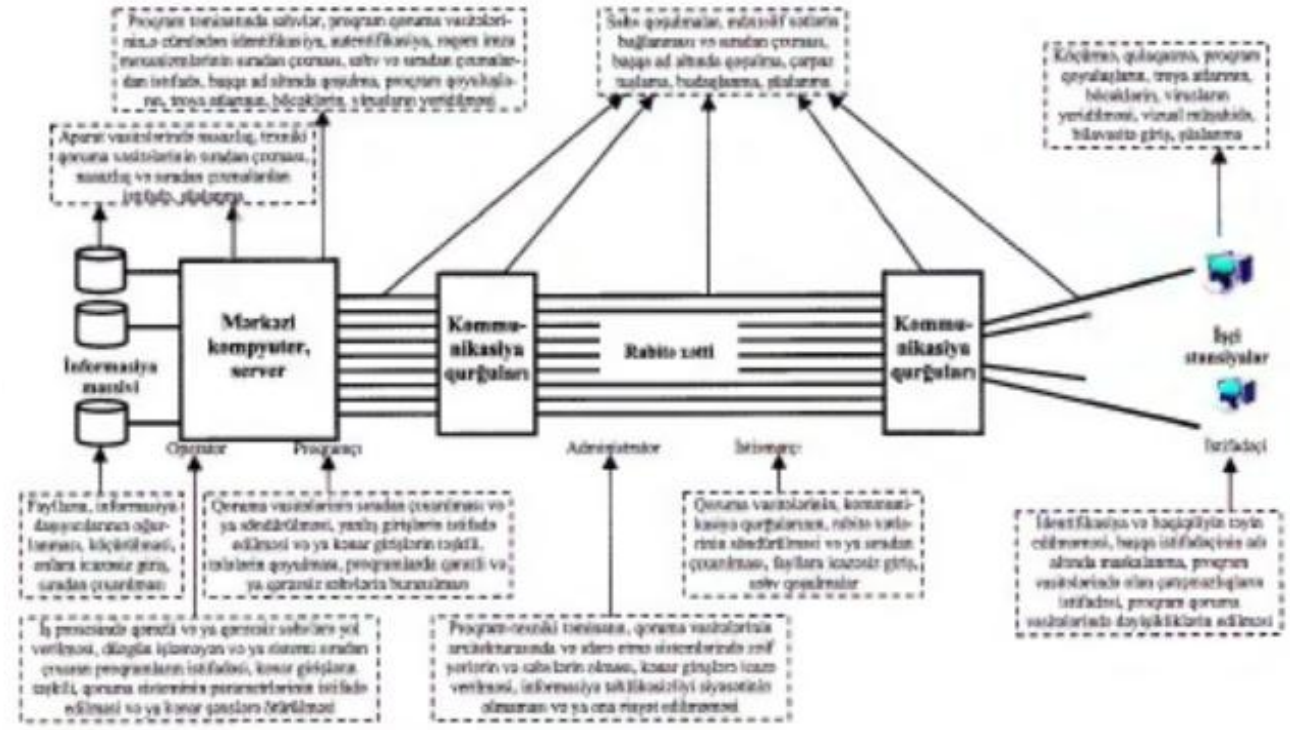
qorunması qapılara adi qıfılın qoyulmasından, qanun və əmrlərlə qadağa edilməsindən tutmuş, ən müasir proqram-texniki vəsaitlərin reallaşdırılmasına qədər müxtəlif növ qoruma vasitələrini əhatə edən bir kompleksin qurulmasını tələb edir.

Beləliklə, informasiya təhlükəsizliyi probleminin həlli daimi və kompleks xarakter daşımalı və böyük məsrəflərin tələb olunmasına baxmayaraq zəruri tədbirlərin həyata keçirilməsini nəzərdə tutmalıdır.

Təcrübə göstərir ki, kompüter şəbəkələrində informasiyanın icazəsiz ələ keçirilməsi təhlükəsinin ciddiliyi zaman keçdikcə və informasiya texnologiyaları inkişaf etdikcə azalmır, əksinə daha da kəskinləşir.

Belə ki, informasiya təhlükəsizliyi sahəsində səylərin daima artmasına baxmayaraq, kompüter texnikası, informasiya emalı vəsaitləri, proqram təminatı və ondan istifadə mexanizmləri inkişaf etdikcə kompüter sistemlərində informasiyanın ələ keçməsi imkanları daha da artır. Ümumiyyətlə, demək olar ki, kompüter şəbəkələrində informasiyanın qorunması probleminin aktuallığı daim yüksəlir.

Kompüter sistemlərində və şəbəkələrində zəif yerlər və informasiyanın sızması yolları. KSŞ-də iş prosesində informasiya təhlükəsizliyinin baza prinsiplərinin pozulmasına, yəni informasiyanın məxfiliyinin açılmasına, məhv edilməsinə, tamlığının itirilməsinə, təcrid olunmasına, sızmasına və s. səbəb ola biləcək çoxlu sayda müxtəlif xarakterli zəif yerlər olur (şək.2.1).



Şək.2.1. KSŞ-də informasiyanın sızması yolları

KSŞ-də informasiya təhlükəsizliyi baxımından *zəif yerlər* dedikdə, kompüter, şəbəkə və informasiya resurslarının, o cümlədən proqram texniki və informasiya təminatının, rabitə kanallarının təhlükəsizliyinin pozulmasının, sistemə, şəbəkə və informasiya resurslarına qanunsuz və icazəsiz daxil "olmaların mümkün olduğu və daha çox ehtimal edildiyi yerlər (qovşaqlar, komponentlər) başa düşülür.

Müxtəlif kompüterləri, **telekommunikasıya** qurğularını, rabitə kanallarını, informasıyanın saxlanması, emalı və ötürülməsi vasitələrini özündə birləşdirən kompüter şəbəkələrində təhlükəsizliyin pozulmasına daha asan və tez-tez məruz qala biləcək əsas funksional struktur komponentlərə serverlər, işçi stansiyalar, onların proqram təminatı, telekommunikasiya qurğuları, rabitə kanalları aid edilir.

İşçi stansiyalar kompüter şəbəkələrində informasiya sistemlərinə ən çox giriş imkanı verən komponentlər olduğuna görə icazəsiz əməliyyatların həyata keçməsinə daha çox məhz bu stansiyalardan cəhdlər edilir. Belə ki, informasiyanın emalı proqramların yüklənməsi, məlumatların daxil edilməsi və redaktəsi prosesləri işçi stansiyalarda həyata keçirilir, onların informasiya daşıyıcılarında (yaddaş qurğularında) bədniyyətli şəxsləri maraqlandıran vacib məlumatlar, eləcə də onların emalı proqramları yazılmış olur.

Müxtəlif funksiyaları yerinə yetirən, verilənlərə və digər sistem resurslarına girmək üçün müxtəlif səlahiyyətlərə malik olan istifadəçilər (operatorlar) kompüterlərdə (işçi stansiyalarda) işləyən zaman məhz bu növ məlumatlar monitora və ya çap qurğularına (printerlərə) çıxarılır.

Bu baxımdan belə kompüterlər kənar şəxslərin müdaxiləsindən (vizual, proqram-texniki və fiziki) etibarlı qorunmalı və müxtəlif səlahiyyətlərə malik olan qanuni istifadəçilər tərəfindən öz resurslarına girişlərə məhdudiyyətlərin qoyulması üçün müvafiq vasitələr reallaşdırılmalıdır.

Bundan əlavə, təhlükəsizliyin təmin edilməsi vasitələri kompüter sistemlərinin parametrlərinin və konfiqurasiyalarının təcrübəsiz (səhlənkar) istifadəçilər tərəfindən dəyişdirilməsinin və ya normal iş rejiminin sıradan çıxmasının qarşısını almalıdır.

Kompüter şəbəkələrinin bədniyyətli şəxslər üçün daha cəlbedici elementləri olan serverlər, mərkəzi kompüterlər, körpülər və digər kommunikasiya qurğuları xüsusilə ciddi qorunmalıdır. Belə ki, serverlərdə böyük həcmli məlumatlar toplanır, körpülər isə şəbəkənin müxtəlif seqmentlərində mübadilə protokollarının uzlaşdırılması zamanı məlumatların (açıq və ya şifrlənmiş təqdimat formasında) çevrilməsini həyata keçirir.

Serverlərin və kommunikasiya qurğularının təhlükəsizliyinin yüksəldilməsi üçün fiziki qoruma vasitələrinin və onların təcrid olunması üzrə təşkilati tədbirlərin tətbiqi zəruridir. Belə ki, bu üsullar xidməti personal arasından serverlərə və körpülərə bilavasitə girişi olan şəxslərin saymı minimuma endirməyə imkan verir. Başqa sözlə, təcrid olunmuş serverlərə, kommunikasiya qurğularına xidməti personalın təsadüfi təsirinin və ya bədniyyətli şəxslərin qabaqcadan düşünülmüş (qəsdən) müdaxiləsinin baş verməsi ehtimalı daha azdır.

Eyni zamanda serverlərə və kommunikasiya qurğularına uzaq məsafədən giriş yolu ilə 'kütləvi hücumların baş verə biləcəyini gözləmək olar. Burada bədniyyətli şəxslər hər şeydən əvvəl mübadilə protokollarında, informasiya və sistem resurslarına uzaqdan girişin məhdudlaşdırılması vasitələrində mümkün çatışmazlıqları istifadə etməklə serverlərin müxtəlif alt sistemlərinin və kommunikasiya qurğularının işinə təsir imkanlarını əldə etməyə çalışırlar. İTS-i adlayıb keçmək (sındırmaq) üçün bədniyyətli şəxslər standart üsullarla (komponentlərdə dəyişiklik edilməsi ilə) yanaşı xüsusi aparat vasitələrinin qoşulması (bir qayda olaraq, kanallar kənardan qoşulmalara qarşı zəif müdafiə edilmiş olurlar) və yüksək səviyyəli proqramların tətbiq edilməsi kimi müxtəlif üsul və vasitələrdən istifadə edə bilərlər.

Əlbəttə, yuxarıda qeyd olunan üsulların reallaşdırılması server və kommunikasiya qurğularına uzaq məsafədən icazəsiz giriş imkanları yaradan aparat və proqram qoşulmalarına cəhdlərin olmayacağını deməyə əsas vermir. Aparat və proqram qoşulmaları həm uzaq məsafədə olan stansiyalardan (virusların və ya digər vasitələrin köməyi ilə), həm də təmir, texniki xidmət, yeniləşdirmə, proqram təminatının yeni versiyalarının qurulması, avadanlıqların dəyişdirilməsi zamanı bilavasitə qurğulara və serverlərin proqram təminatına tətbiq oluna bilər.

Rabitə kanallarının və vasitələrinin qorunması, informasiya təhlükəsizliyinin təmin edilməsi üçün böyük əhəmiyyət kəsb edir. Rabitə xətləri, bir qayda olaraq, böyük məsafələrdən (adətən, nəzarət edilməyən və ya zəif nəzarət edilən ərazilərdə) keçdiyinə

görə, praktik olaraq, onlara qoşulmaq və ya məlumatların ötürülməsi prosesinə müdaxilə etmək imkanlarının mövcudluğu həmişə nəzərə alınmalıdır.

İnformasiyanın sızmasının və ona icazəsiz girişin əldə olunmasının əsas yollan aşağıdakılardır:

- şəbəkə avadanlıqlarına və rabitə xətlərinə qoşulma;
- elektromaqnit şüalanmalarının tutulması;
- uzaq və yaxın məsafədən şəkilçəkmə;
- qulaqasma qurğularının tətbiq edilməsi;
- informasiya daşıyıcılarının, çap olunmuş vərəqlərin və istehsal məsrəflərinin oğurlanması və məhv edilməsi;
- icazəsi olan (həqiqi) istifadəçilər sistemdə işləyən zaman onun "ilişməsindən" istifadə edərək bu istifadəçinin adı altında sistemə qoşulma;
- qeydiyyatdan keçmiş istifadəçilərin terminallarından icazəsiz istifadə edilməsi;
- parolların və girişi məhdudlaşdıran digər rekvizitlərin oğurlanması yolu ilə qeydiyyatdan keçmiş istifadəçilərin adı altında maskalanaraq sistemə daxilolma;
- istifadəçi səlahiyyətindən istifadə etməklə digər istifadəçilərin informasiya massivlərindən məlumatların oxunması;
- əməliyyat sisteminin və ya icazəsi olan istifadəçilərin sorğuları altında pərdələnmək yolu ilə sistemə daxilolma və məlumatların əldə edilməsi;
- icazəli sorğu yerinə yetirildikdən sonra yaddaş qurğusundan qalıq informasiyanın oxunması;
- informasiya daşıyıcılarında olan məlumatların köçürülməsi;
- proqram "tələləri"nin və qoyuluşların istifadə edilməsi;
- sistemə və ya proqramlara "troya atları"nın daxil edilməsi;
- kompüter viruslarına bilmədən yoluxma və ya qəsdən yoluxdurma;
- icazə verilən əməliyyatlar kombinasiyasını tətbiq etmək yolu ilə qorunan məlumatların ələ keçirilməsi;
- proqramlaşdırma dillərində, əməliyyat sistemlərində və şəbəkə proqram təminatında olan boşluqların və çatışmazlıqların istifadə olunması;
- tətbiqi proqram təminatının, informasiya resurslarının və məlumatların qəsdən korlanması, sistemin parametrlərinin dəyişdirilməsi;
- texniki qurğularda və şəbəkə analizatorlarında baş verən nasazlıqlardan və sıradan çıxmalardan istifadə olunması.

Kənar şəxslərin sistemə müdaxiləsinin, sistemə təsir edən və ya edə biləcək hadisələrin və informasiyanın sistemdən kənara sızmasının bütün mümkün hallarını ümumi halda iki yerə bölmək olar:

- birbaşa müdaxilə;
- dolayı yolla müdaxilə.

Birbaşa müdaxilə zamanı bədniyyətli şəxslər bilavasitə sistemin komponentlərinin yerləşdiyi yerə (binaya, otağa və s.) daxil olur. Birbaşa müdaxilə sistemin komponentlərində dəyişiklik etmədən və ya onları dəyişdirmək yolu ilə baş verə bilər.

Dolayı yolla müdaxilə zamanı isə informasiyanın əldə edilməsi və ya sıradan çıxarılması üçün sistemin komponentlərinin yerləşdiyi yerə (otağa və ya binaya) girmək tələb olunmur.

İnformasiyanın sızması yollarının təhlili göstərir ki, kompüter şəbəkələrində effektiv İTS işləyib hazırlamaq və reallaşdırmaq üçün informasiya təhlükəsizliyinə olan təhdidlər (təhlükəsizliyin pozulması təhlükələri) çoxluğu təsnif edilməli, hər bir təhlükənin qarşısının alınması üçün müvafiq üsul və vasitələr işlənib hazırlanmalıdır.

<u>İnformasiya təhlükəsizliyinin təmin edilməsinin əsas aspektləri.</u> İnformasiya təhlükəsizliyinin təmin edilməsi – informasiyanın gizliliyinin, tamlığımın və ona girişin (əlyetərliliyin) təmin edilməsinə yönəlmiş fəaliyyətdir.

İnformasiyanın emalı və ötürülməsi sistemlərində, o cümlədən KSŞ-də informasiyanın təhlükəsizliyinin təmin edilməsi – toplanan, saxlanılan, emal edilən və ötürülən informasiyanın icazəsiz (icazəsi olmayan şəxslər, eləcə də baş verən proseslər tərəfindən) istifadəsi, pozulması, korlanması, təhrif və təcrid edilməsi hallarının aradan qaldırılması üçün nəzərdə tutulmuş üsul, vasitə və qaydaların təşkilini və tətbiqini özündə ehtiva edir.

Başqa sözlə, informasiya təhlükəsizliyinin təmin edilməsi dedikdə, reallaşdırılması informasiyanın sahiblərinə və istifadəçilərinə ziyanın vurulması ilə nəticələnən təbii və süni xarakterli təhlükələrin təsir göstərdiyi şəraitlərdə informasiyanın gizliliyini, tamlığım və ona girişi (əlyetərliliyi) təmin edən müvafıq üsul və vasitələr kompleksi kimi dövlət, xidməti (kommersiya) və ya şəxsi sirlərin, eləcə də digər məxfı məzmunlu informasiya daşıyıcılarının qorunması başa düşülür.

KSŞ-də informasiya resurslarından icazəsiz istifadə təhlükəsinin qarşısını almaq üçün ilk reaksiya əlavə proqram vəsaitlərinin işlənib hazırlanması və kompüterlərin proqram təminatının (ilk öncə əməliyyat sistemlərinin) tərkibinə daxil edilməsi olmuşdur. Bu proqram vasitələri, kompüterlərə, əməliyyat sistemlərinə və kompüter şəbəkələrinə daxilolma, informasiyaya giriş və onların istifadəsi məsələlərinin nizamlanmasını, eləcə də kompüter sistemlərinin yaradılması və istismarı zamanı bir sıra tədbirlərin həyata keçirilməsini nəzərdə tutur.

Hazırda KSŞ-nin layihələndirilməsi zamanı əsas tələblərdən biri kimi informasiyanın qorunması vasitələrinin sistemin tərkibində reallaşdırılması qoyulur. Informasiyanın qorunması qapılara adi qıfılın qoyulmasından, qanun və əmrlərlə qadağa edilməsindən tutmuş, ən müasir proqram-texniki vəsaitlərin reallaşdırılmasına qədər müxtəlif növ qoruma vasitələrini əhatə edən bir kompleksin qurulmasını tələb edir.

Kompüter sistemlərində informasiya təhlükəsizliyinin bilavasitə təmin edilməsi məqsədilə digər üsullarla yanaşı şifrləmə üsul və vasitələrindən də istifadə olunur.

Şifrləmə vasitələri informasiyanın məğzinin gizlədilməsi, tamlığının təmin edilməsi, imzalanması, informasiyanın və onun sahibinin həqiqiliyinin təsdiq olunması və digər vacib məsələləri həll etməyə kömək edir.

KSŞ-də informasiya təhlükəsizliyinin təmin edilməsi aşağıdakı iki istiqamətdə həyata keçirilir:

- ayrı-ayrı kompüterlərin, kompüter sistemlərinin və serverlərin, eləcə də onlarda olan informasiyanın kənar şəxslərin, başqa kompüterlərin, kompüter sistemlərinin və şəbəkələrinin pis niyyətli müdaxiləsindən qorunması;
- rabitə kanalları vasitəsilə ötürmə zamanı informasiyanın qorunması.

İnformasiya təhlükəsizliyinin təmin edilməsi zamanı həll edilməsi vacib olan əsas məsələlər aşağıdakılardır:

- təşkilatın informasiya təhlükəsizliyi siyasətinin müəyyən edilməsi;
- informasiya təhlükəsizliyinin mümkün pozulması nəticəsində dəyə biləcək potensial ziyanın və maddi zərərin qiymətləndirilməsi;
- sistemin informasiya resurslarının təhlükəsizliyinə mümkün təhdidlərin tam siyahısının tərtib edilməsi və onların parametrlərinin müəyyənləşdirilməsi;
- kompüter şəbəkəsində informasiya təhlükəsizliyini müntəzəm olaraq təmin etməyə imkan verən vahid İTS-in işlənib hazırlanması və tədqiq edilməsi;
- informasiya təhlükəsizliyinin effektiv təmin edilməsi və effektiv İTS-in yaradılması üçün zəruri üsul və vasitələr kompleksinin işlənib hazırlanması və reallaşdırılması;

- İTS-in effektivliyinin təmin edilməsi və artırılması üçün zəruri olan şərtlər sisteminin formalaşdırılması;
- informasiya təhlükəsizliyi göstəricilərinin və xarakteristikalarının qiymətləndirilməsi, proqnozlaşdırılması və təkmilləşdirilməsi mexanizmlərinin işlənib hazırlanması.

KSŞ-də informasiya təhlükəsizliyinin təmin edilməsi məqsədilə reallaşdırılmış İTS-də əsasən aşağıdakı mexanizmlərdən istifadə olunur:
- əməliyyat sistemlərində reallaşdırılmış daxili təhlükəsizlik funksiyaları;
- kompüter şəbəkəsinə və sisteminə girişin məhdudlaşdırılması;
- sistemin və istifadəçinin (abonentin) həqiqiliyinin müəyyən edilməsi;
- informasiyanın tamlığının təmin edilməsi;
- informasiyanın və ya onun sahibinin şəxsiyyətinin təsdiq edilməsi;
- tətbiqi proqramların və informasiya resurslarının icazəsiz köçürülmədən və istifadədən qorunması;
- ayrı-ayrı fərdi kompüterlərin işinə nəzarət;
- informasiya təhlükəsizliyi protokollarının tətbiqi;
- kriptoqrafık şifrləmə üsullarının reallaşdırılması;
- rəqəm imza texnologiyasının reallaşdırılması;
- antivirus proqramlarının istifadə olunması;
- proqram-texniki qoyuluşların aşkarlanması və aradan qaldırılması mexanizmlərinin reallaşdırılması;
- fiziki qurğulara və rabitə xətlərinə nəzarət.

KSŞ üçün İTS-in, o cümlədən ayrı-ayrı qoruma üsul və vasitələrinin işlənib hazırlanması zamanı aşağıdakı məqamlar nəzərə alınmalıdır:
- KSŞ-də informasiya təhlükəsizliyinin təmin edilməsi – sistematik nəzarəti, sistemdə mümkün zəif yerlərin aşkar olunmasını, İTS-i təkmilləşdirmək və inkişaf etdirmək üçün ən rasional yolların tapılmasını, reallaşdırılmasını və s. özündə cəmləşdirən və ardıcıl həyata keçirilən kəsilməz prosesdir;
- KSŞ-də informasiya təhlükəsizliyi yalnız bütün mümkün qoruma üsul və vasitələrindən kompleks şəkildə istifadə etməklə təmin oluna bilər;
- heç bir İTS tam etibarlı hesab oluna bilməz, istənilən vaxt KSŞ-də informasiyaya giriş üçün zəif yeri axtarıb tapa biləcək bacarıqlı bədniyyətli şəxslər tapıla bilər;
- istifadəçilərin və xidməti personalın tələb olunan səviyyədə hazırlığım, eləcə də onlar tərəfindən təhlükəsizlik qaydalarına riayət olunmasını təmin etmədən heç bir İTS informasiya təhlükəsizliyinə tam təminat verə bilməz.

Ümumiyyətlə, informasiya təhlükəsizliyinin təmin edilməsi zamanı aşağıdakı prinsiplərə riayət edilməlidir:
- qanunilik;
- şəxsiyyətin, cəmiyyətin və dövlətin maraqlarına riayət olunması;
- bütün informasiya təhlükəsizliyi subyektlərinin fəaliyyətlərinin uzlaşdırılması;
- informasiya təhlükəsizliyinin təmin edilməsi üzrə tədbirlərin komplekslilіyi;
- informasiya mühitində hüquq pozuntularına görə informasiya təhlükəsizliyi subyektlərinin məsuliyyəti;
- beynəlxalq təhlükəsizlik sistemlərinə inteqrasiya;
- qorunan informasiyanın mühafizəsinin təşkili;
- informasiya mühitində hüquqazidd hərəkətlər (hərəkətsizlik) nəticəsində dəyə biləcək ziyanın ölçüsünün informasiya təhlükəsizliyinin təmin edilməsi üzrə tədbirlərə uyğunluğu.

Yuxanda deyilənləri nəzərə alaraq, belə nəticəyə gəlmək olar ki, KSŞ-də informasiya təhlükəsizliyi ayrı-ayrı üsul və vasitələri tətbiq etməklə deyil, öz funksiyalarını sistemin əsas komponentləri ilə qarşılıqlı əlaqədə yerinə yetirən proqram-texniki qoruma vasitələri kompleksini reallaşdırmaqla təmin edilə bilər.

İnformasiya təhlükəsizliyinin təmin edilməsi üçün həyata keçirilən tədbirlər sistemi. Ümumi halda, informasiyanın qorunmasının məqsədi informasiya resurslarına qarşı hüquqazidd hərəkətlərin, o cümlədən məxfi informasiyanın açılmasının, yayılmasının və sızmasının qabağının alınması, məxfi informasiya mənbələrinə icazəsiz girişə yol verilməməsi, məxfilik rejiminə riayət olunması, informasiyanın bütövlüyünün (tamlığının), dolğunluğunun, ona icazəli girişin, eləcə də müəlliflik hüququnun təmin edilməsindən ibarətdir.

Qeyd olunduğu kimi, informasiya təhlükəsizliyinin təmin edilməsi üçün konkret təşkilati, təşkilati-texniki, texniki hərəkət və tədbirlər planlaşdırılır və həyata keçirilir.

Qorunan obyektlərin əsas xarakteristikalarına və növlərinə görə qoruma mexanizmlərini aşağıdakı kimi təsnif etmək olar:

- **əhatə dairəsinə görə**
  - ərazinin qorunması;
  - binaların qorunması;
  - ayrı-ayrı otaqların qorunması;
  - avadanlıqların, texniki vəsaitlərin və sistemlərin konkret növünün qorunması;
  - ayrı-ayrı komponentlərin qorunması.
- **qoruma tədbirlərinin yönəldiyi obyektlərin növünə görə**
  - personalın qorunması;
  - maddi vəsaitlərin qorunması;
  - maliyyə vəsaitlərin qorunması;
  - informasiya ehtiyatlarının qorunması.
- **təhlükələrə qarşı mübarizə üsullarına görə**
  - təhlükələrin qarşısının alınması;
  - təhlükələrin aşkar edilməsi;
  - təhlükələrin müəyyən edilməsi;
  - təhlükələrin aradan qaldırılması;
  - təhlükələrin nəticələrinin aradan qaldırılması və vəziyyətin bərpa edilməsi.
- **istifadə olunan tədbirlərin növünə görə**
  - hüquqi tədbirlər;
  - təşkilati tədbirlər;
  - mühəndis-texniki tədbirlər.

KSŞ-də zəmanətli informasiya təhlükəsizliyi müfəssəl surətdə işlənib hazırlanan və planlı şəkildə həyata keçirilən tədbirlər sistemi vasitəsilə təmin oluna bilər. *Tədbirlər sistemi* təhlükələrə qarşı mübarizə üzrə hər bir mərhələdə bütün zəruri tədbirləri özündə birləşdirməlidir:

1. Təhlükələrin yaranması imkanlarının qarşısını almaq məqsədilə qabaqlayıcı tədbirlər. Mümkün təhlükələrin və hüquqazidd hərəkətlərin qabaqlanması müxtəlif üsul və tədbirlərin köməyi ilə həyata keçirilə bilər. Bura əməkdaşların informasiya təhlükəsizliyi probleminə məsuliyyətlə yanaşmasının təmin edilməsindən tutmuş, fiziki, aparat, proqram, kriptoqrafık və digər üsul və vasitələri özündə birləşdirən informasiya təhlükəsizliyi sisteminin yaradılmasınadək müxtəlif mexanizmlər aid edilir.

Bu məqsədlə təşkilatda təhlükəsizlik xidmətinin rolundan da istifadə oluna bilər. Belə ki, bu xidmətin əməkdaşları vəziyyətin qiymətləndirilməsi üçün öz informatorları vasitəsilə təşkilatda, rəqiblər və cinayətkarlar qruplar arasında təhlükəli hərəkətlərin mümkünlüyü öyrənilməli və zəruri tədbirlər görülməlidir. Bu zaman planlaşdırılan bütün hüquqazidd hərəkətlər, o cümlədən oğurluqlar, belə hərəkətlərə hazırlıq işləri və cinayətkar fəaliyyətin digər elementləri diqqətdən qaçırılmamalıdır.

Bu baxımdan təhlükəsizlik xidməti tərəfindən kriminal vəziyyətin, rəqiblərin və bədəməl şəxslərin fəaliyyətinin dərin təhlilinə əsaslanan informasiya-analitik fəaliyyəti böyük əhəmiyyətə malikdir.

2. Təhlükələrin baş verməsi imkanlarının aşkar edilməsi tədbirləri. Real və potensial təhlükələrin baş verməsi imkanlarının sistematik təhlil edilməsi, nəzarətdə saxlanması və onların qarşısının vaxtında alınması üçün aşkar etmə tədbirləri həyata keçirilir.

Burada əsas məqsəd kriminal strukturlar və ya rəqiblər tərəfindən cinayətkar hərəkətlərin mümkün planlaşdırılması və hazırlanması haqqında məlumatların əldə olunması, toplanması və analitik emalı tədbirlərinin keçirilməsindən ibarətdir. Bu zaman əməkdaşların öyrənilməsinə xüsusi fıkir verilməli, narazı və təcrübəsiz işçilər daim nəzarətdə saxlanmalıdır.

3. Təhdidlərin və cinayətkar əməllərin müəyyən edilməsi tədbirləri. Real ziyan vura biləcək prinsipial və konkret təhdidlərin (məsələn, oğurluq, dələduzluq, məxfi informasiyanın yayılması, informasiyaya icazəsiz giriş və s. halların aşkarlanması), eləcə də onların **mənbələrinin müəyyən edilməsi məqsədilə həyata keçirilən tədbirlərdir.**

4. Təhdidlərin və cinayətkar əməllərin lokallaşdırılması tədbirləri. Fəaliyyətdə olan təhdidlərin və cinayətkar əməllərin aradan qaldırılmasına yönəlmiş tədbirlərdir.

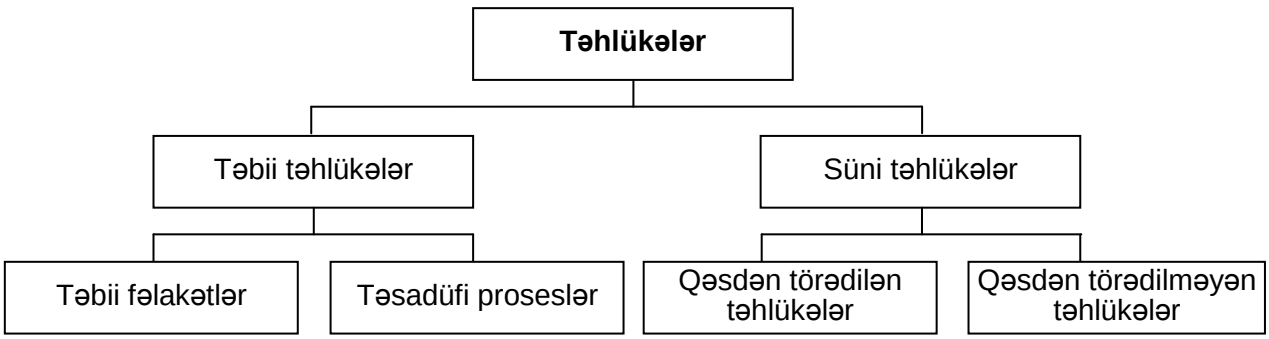
5. Təhdidlərin və ya konkret cinayətkar əməllərin ləğv edilməsi. Təhdidlərin və cinayətkar əməllərin nəticələrinin ləğv edilməsi, onlar baş verənə qədər mövcud olmuş vəziyyətin bərpa olunması məqsədilə həyata keçirilən tədbirlərdir.

Sual 3. Kompüter sistemlərində və şəbəkələrində informasiya təhlükəsizliyinin pozulmasi təhlükələri

Kompüter sistemlərində və şəbəkələrində informasiya resurslarına qarşı yönəlmiş təhlükələrin təsnifatı. Təhlükəsizliyin pozulması təhlükəsi (informasiya təhlükəsizliyinə təhdidlər) dedikdə ayrı-ayrı şəxslərin, təşkilatların, cəmiyyətin və ya dövlətin maraqlarına ziyan vurulmasına gətirib çıxaran, informasiyanın təsadüfən və ya düşünülmüş şəkildə (qəsdən) məhv edilməsi, icazəsiz açılması və dəyişdirilməsi təhlükəsini, eləcə də kompüterlərdə saxlanılan, emal olunan və şəbəkədə ötürülən, qorunması tələb olunan informasiyaya qeyri-qanuni və icazəsiz girişin əldə olunması imkanlarını yaradan mümkün potensial hadisələr, hərəkətlər və təsirlər başa düşülür.

KSŞ-də mümkün potensial təhlükələri əmələgəlmə təbiətinə görə iki kateqoriyaya ayırmaq olar (şək.3.1):

- təbii təhlükələr;
- süni təhlükələr.



Şəkil 3.1. İnformasiya təhlükəsizliyinə olan təhlükələrin növləri

Təbii təhlükələr – insanlardan asılı olmadan baş verən obyektiv fiziki proseslərin və ya təbiət hadisələrinin KSŞ-yə, eləcə də onların elementlərinə təsiri nəticəsində yaranan təhlükələrdir. Təbii təhlükələri təbii fəlakətlər və təsadüfi proseslər kimi iki qrupa bölmək olar.

Təbii fəlakətlərə yanğın, su basına, zəlzələ, şimşək, torpaq sürüşməsi və s. aid edilir. Bu təhlükələrin qarşısını almaq üçün kompüter sistemləri və şəbəkələri, eləcə də onların yerləşdiyi bina və ya otaqlar layihələndirilən zaman bəzi məqamlar nəzərə alınmalıdır.

Belə ki, yanğın, su basına, zəlzələ və digər təbii hadisələrin qarşısının alınması zamanı kompüter texnikasının, telekommunikasiya qurğularının və digər informasiya daşıyıcılarının, eləcə də onlarda saxlanılan və emal olunan məlumatların təhlükəsizliyinin təmin edilməsi üçün binaların tikintisi zamanı müvafıq tədbirlər görülməlidir. Məsələn, yanğından mühafizə sistemi qurularkən nəzərə alınmalıdır ki, yanğının söndürülməsi prosesində istifadə olunan su və digər vasitələr kompüter texnikasına, qurğu və avadanlıqlara ciddi xəsarət vura bilər.

Təsadüfi proseslər informasiya təhlükəsizliyinin pozulmasının daha tez-tez rast gəlinən formalarıdır. Bu növ təhlükələrə nümunə kimi gərginliyin gözlənilmədən (təsadüfən) qalxması və düşməsi, elektrik cərəyanının kəsilməsi, maqnit sahəsinin təsiri, birləşdirici kabellərin, qurğuların və soyutma sisteminin sıradan çıxması və s. kimi hadisələri göstərmək olar.

Elektrik nasazlıqları yarandıqda ağır nəticələrin qarşısını almaq üçün texniki vəsaitlər, qurğular və avadanlıqlar elektrik xəttinə sabitləşdirici qurğular (stabilizatorlar) və ya gərginlik fıltrləri, eləcə də fasiləsiz qidalanma mənbələri vasitəsilə qoşulur.

Eyni zamanda nəzərə alınmalıdır ki, avadanlıqlarda baş verən nasazlıqlar, kabellərin və kommunikasiya vasitələrinin sıradan çıxması ciddi informasiya itkisinə səbəb. ola, maqnit sahəsinin maqnit informasiya daşıyıcılarına təsiri nəticəsində bu qurğularda saxlanılan informasiya təhlükəyə məruz qala və korlana bilər.

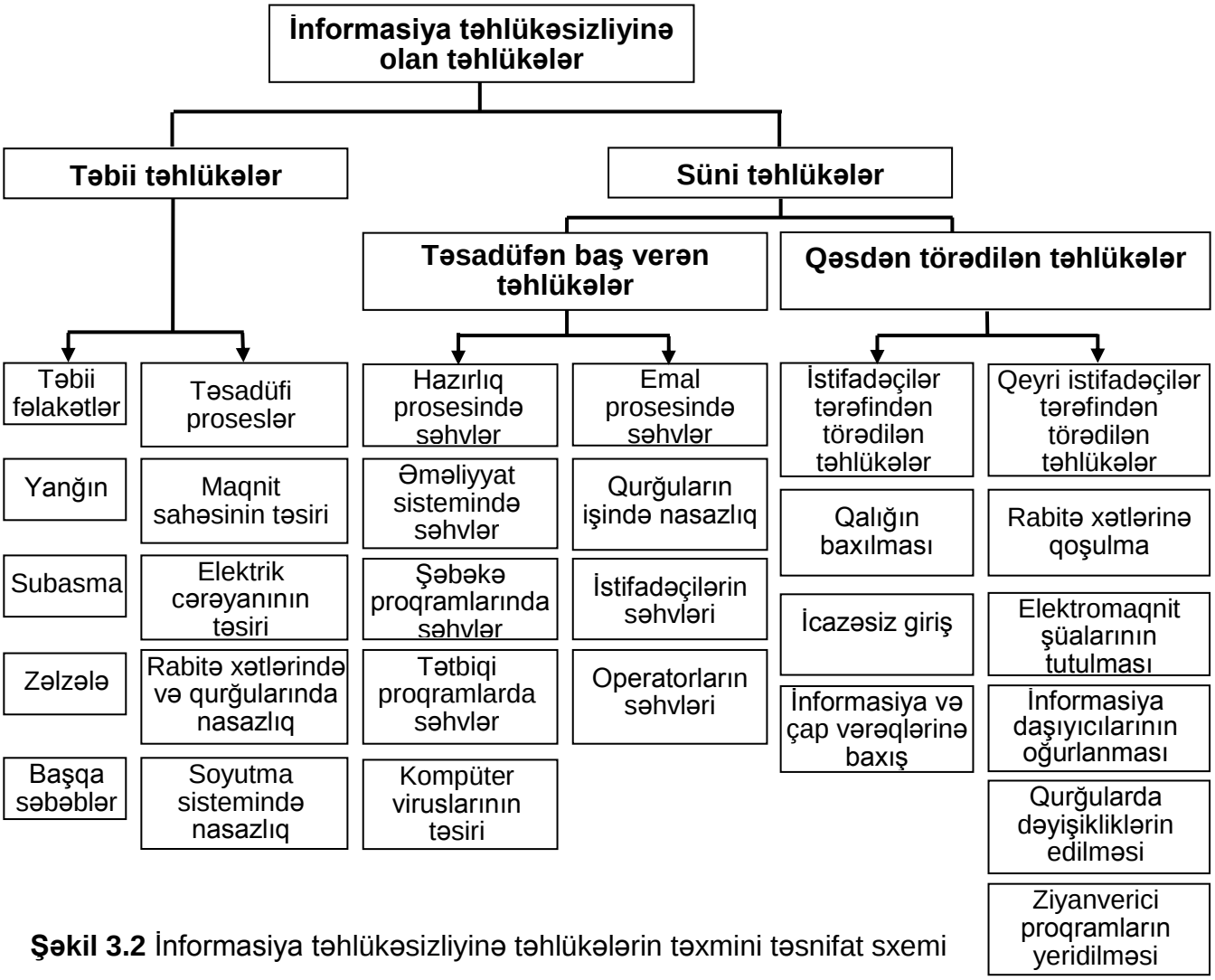
Soyutma sisteminin işinin dayanması avadanlıqların və kompüter texnikasının texniki işləmə şərtlərinin təmin edilməməsinə, bu isə öz növbəsində onların düzgün fəaliyyətinin pozulmasına gətirib çıxara bilər.

Süni təhlükələr – KSŞ-də insanların fəaliyyəti və təsiri nəticəsində meydana çıxan təhlükələrdir. Yaranma səbəblərini və hərəkətlərin əsaslarmı nəzərə alaraq, süni təhlükələri iki yerə ayırırlar (şək.3.2):

- qəsdən törədilməyən (qərəzsiz və ya təsadüfən baş verən) təhlükələr – KSŞ-nin, eləcə də onların elementlərinin layihələndirilməsi, proqram-texniki təminatın işlənib hazırlanması prosesində, işçi personalın fəaliyyətində və s. səhlənkarlıq, səriştəsizlik və təcrübəsizlik səbəbindən buraxılan səhvlər nəticəsində yaranır. Belə təhlükələr informasiyanın sahibinə ziyan vurmaq məqsədi daşımır;
- qəsdən törədilən (qərəzli) təhlükələr – insanların (ziyankarların) bədniyyətli (məkrli) fəaliyyəti nəticəsində yaranan təhlükələrdir.

<u>Təsadüfən baş verən təhlükələr və onların informasiya təhlükəsizliyinə təsiri.</u> KSŞ-də təsadüfən baş verən, yəni qəsdən törədilməyən təhlükələrə, əsasən, aşağıdakıları aid etmək olar:

- sistemin qismən və ya tam sıradan çıxmasına, aparat, proqram və informasiya resurslarının məhvinə (avadanlıqların korlanmasına, vacib məlumatlan özündə saxlayan faylların və proqramların, o cümlədən sistem fayllarının pozulmasına və təhrif edilməsinə və s.) gətirib çıxaran düşünülməmiş hərəkətlər;
- icazə olmadan avadanlıqların söndürülməsi və ya qurğu və proqramların iş rejimlərinin dəyişdirilməsi;
- informasiya daşıyıcılarının bilməyərəkdən xarab edilməsi;
- səriştəsiz istifadə səbəbindən sistemin iş qabiliyyətinin itməsinə (ilişməsinə) gətirib çıxaran texnoloji proqramların yüklənməsi və ya sistemdə bərpası mümkün olmayan dəyişikliklərin aparılması (informasiya daşıyıcılarının formatlaşdırılması və ya strukturunun dəyişdirilməsi, məlumatların və ya faylların pozulması və s.);



Şəkil 3.2 İnformasiya təhlükəsizliyinə təhlükələrin təxmini təsnifat sxemi

- sistem resurslarının izafi məsrəfinə (prosessorun yüklənməsinə, əməli yaddaşın və xarici informasiya daşıyıcılarmda olan yaddaşın tutulmasına) səbəb ola biləcək nəzərdə tutulmamış proqramların qeyri-leqal tətbiqi və icazəsiz istifadəsi;
- kompüter viruslarına yoluxma;
- məxfi məlumatın yayılmasına gətirib çıxaran və ya ümumi istifadəsinə imkan yaradan ehtiyatsız hərəkətlər;
- sistemin fəaliyyətinə və informasiyanın təhlükəsizliyinə təhdidlərin reallaşdırılmasına imkan verən arxitekturanın layihələndirilməsi, məlumatların emalı texnologiyalarının və tətbiqi proqramların işlənib hazırlanması;
- sistemdə işləyən zaman müəyyən edilmiş qaydalara və təşkilati məhdudiyyətlərə riayət olunmaması;
- mühafizə vasitələrindən yan keçməklə sistemə daxilolma (məsələn, disketlərdən digər əməliyyat sisteminin yüklənməsi yolu ilə sistemə daxilolma və s.);
- təhlükəsizlik vasitələrinin xidməti personal tərəfindən səriştəsiz istifadəsi, onların parametrlərinin dəyişdirilməsi və icazəsiz söndürülməsi;
- istifadəçinin (abonentin) və ya kompüterin ünvanının səhv göstərilməsi səbəbindən məlumatların başqa ünvana göndərilməsi;
- səhv məlumatların daxil edilməsi;
- bilməyərəkdən rabitə kanallarının sıradan çıxarılması və korlanması.

3.2 saylı şəkildən göründüyü kimi, qəsdən törədilməyən təhlükələr, əsasən, informasiyanın emalına hazırlıq və bilavasitə emal prosesində buraxılan səhvlər nəticəsində meydana çıxa bilər.

İnformasiya emalı sistemlərində emala hazırlıq prosesi dedikdə, əməliyyat sistemlərinin parametrlərinin seçilməsi və qoyulması, sistem və şəbəkə proqram-texniki vasitələrinin, tətbiqi və istifadəçi proqramlarının işlənib hazırlanması nəzərdə tutulur.

Məlum olduğu kimi, əməliyyat sistemlərində səhvlərin olması qaçılmazdır. Belə səhvlər, bir qayda olaraq, adi vəziyyətlərdə sistemin işinə təsir etmir, lakin onlar düzgün olmayan nəticələrin (çıxış verilənlərinin) alınmasına səbəb ola bilər.

Tətbiqi və istifadəçi proqramlarında olan səhvlər də ciddi nəticələrin yaranmasına səbəb olur. Çox istifadəçisi olan və çoxməsələli sistemlərdə aşkar olunmamış səhvləri özündə saxlayan istifadəçi proqramları düzgün işləyən digər proqramlar üçün təhlükə yarada bilər.

Belə ki, bu proqramlar müəyyən vəziyyətlərdə yaddaşın onlara məxsus olmayan hissələrindən informasiyanı oxuya və ya ora informasiya yaza bilər ki, bu da sistemin ilişməsinə, informasiyanın pozulmasına, zərurət olmadan dəyişməsinə və ya informasiya massivinin tamamilə məhvinə səbəb ola bilər.

Əməliyyat sistemlərində və istifadəçi proqramlarında olan səhvlər KSŞ-də məlumatlara icazəsiz giriş üçün imkanın yaranmasının ilk səbəblərindən biridir.

İnformasiyanın emalı prosesində avadanlıqların və qurğuların işində baş verən nasazlıqlar, istifadəçilərin və operatorların buraxdıqları səhvlər, kompüter viruslarını təsiri və s. informasiya təhlükəsizliyi üçün təhlükə yaradan ciddi amillərdir.

Belə səhvlər kompüterlərin, serverlərin, işçi stansiyaların və kommunikasiya qurğularının işində ayrı-ayrı elementlərin, sxemlərin və ya komponentlərin sıradan çıxması nəticəsində aşkar oluna bilər.

Kompüter virusları proqram təminatının, əməliyyat sistemlərinin və kompüter şəbəkələrinin işi, o cümlədən informasiya resursları üçün ciddi təhlükə yaradır. Onların təsirini qabaqcadan müəyyən etmək olmur. Belə ki, kompüter virusları bütün şəbəkəni iflic vəziyyətinə sala, sistemi, kompüterin yaddaşında olan proqramları və informasiya resurslarını məhv edə bilər.

Qəsdən törədilən təhlükələrin formaları. KSŞ-nin və onun komponentlərinin işinin pozulmasına, sıradan çıxmasına, sistemə və informasiyaya icazəsiz daxilolmaya, sistem və informasiya resurslarının əldə edilməsinə və ya qanuni istifadəçilərindən təcrid olunmasına və s. səbəb olan, düşünülmüş şəkildə həyata keçirilən təhlükələrə, əsasən, aşağıdakıları aid etmək olar:

- sistemin fiziki məhv edilməsi (partlatma, yandırma və s.), onun bütün və ya bəzi daha vacib komponentlərinin (qurğuların, vacib sistem məlumatlarının daşıyıcılarının, xidməti personala daxil olan şəxslərin və s.) sıradan çıxarılması;
- KSŞ-nin fəaliyyətini təmin edən alt sistemlərin (elektrik qidalanması, soyuducu, hava dəyişən qurğular, rabitə və s.) söndürülməsi və ya sıradan çıxarılması;
- sistemin fəaliyyətinin pozulmasına səbəb olan hərəkətlər (qurğuların və ya proqramların iş rejimlərinin dəyişdirilməsi, tətil, işçi personalın sabotajı, sistem qurğularının iş tezliklərinə uyğun güclü radiomaneələrin qoyulması və s.);
- sistemin işçi personalı arasına (o cümlədən təhlükəsizliyə məsul olan administratorlar qrupuna) agentlərin yeridilməsi;
- müəyyən səlahiyyətlərə malik olan personalın və ya istifadəçilərin cəlb edilməsi (maddi maraqlandırmaq, hədə-qorxu gəlmək və s. yolla);
- qulaq asına, uzaq məsafədən şəkil və video çəkmə qurğularının və s. tətbiqi;

- qurğulardan və rabitə xətlərindən kənar elektromaqnit, akustik və digər şüalanmaların tutulması, eləcə də informasiya emalında bilavasitə iştirak etməyən texniki vasitələrin (telefon və elektrik xətlərinin, qızdırıcı qurğuların və s.) istifadəsi;
- rabitə kanalları vasitəsilə ötürülən məlumatların tutulması və mübadilə protokollarının, əlaqəyə girmə və istifadəçilərin avtorizə edilməsi qaydalarının öyrənilməsi və gələcəkdə sistemə keçmək üçün istifadəsi;
- informasiya daşıyıcılarının (maqnit disklərinin və lentlərinin, CD disklərin, mikrosxemlərin, əməli yaddaşların və bütövlükdə kompüterin) və istehsal tullantılarının (çap vərəqlərinin, yazıların, istehsaldan çıxarılmış informasiya daşıyıcılarının və s.) oğurlanması;
- informasiya daşıyıcılarının məzmunlarının icazəsiz köçürülməsi;
- əməli yaddaşdan və xarici yaddaş qurğusundan qalıq informasiyanın oxunması;
- parolların və girişi məhdudlaşdıran digər rekvizitlərin qeyri-qanuni yolla (agentlərin köməyi ilə, istifadəçilərin səhlənkarlığından istifadə etməklə, seçmə üsulu ilə, sistemin interfeysini imitasiya etməklə və s.) ələ keçirilməsi və sonradan qeydiyyatdan keçmiş istifadəçinin adı altinda maskalanma;
- istifadəçilərin unikal fiziki xassələrə malik olan terminallarının (işçi stansiyanın şəbəkədə nömrəsinin, fiziki ünvanın, rabitə sistemində ünvanın, kodlaşdırma üçün aparat blokunun və s.) icazəsiz istifadəsi;
- çoxməsələli əməliyyat sistemlərinin və proqramlaşdırma dillərinin çatışmazlıqlarını istifadə etməklə asinxron rejimdə əməli yaddaşın əməliyyat sistemi (o cümlədən digər proqramlar) və ya digər istifadəçilər tərəfindən istifadə olunan hissələrindən informasiyanın oxunması;
- informasiyanın kriptoqrafık qorunması şifrlərinin açılması;
- xüsusi aparat vasitələrinin, proqram və aparat qoyuluşlarının, eləcə də virusların (o cümlədən "troya atlan"nın və "qurdlar"ın) tətbiqi, nəzərdə tutulmuş funksiyaların yerinə yetirilməsi üçün lazım olmayan, lakin mühafizə sistemini keçmək, qeydiyyata düşmək, vacib məlumatlan ötürmək və ya sistemin fəaliyyətinin pozmaq məqsədilə sistem resurslarına gizli və qeyri-qanuni daxilolma imkanlarını reallaşdıran proqramların istifadəsi;
- qanuni istifadəçinin adı altında yanlış məlumatların daxil edilməsi və ya ötürülən məlumatların dəyişdirilməsi üçün həmin istifadəçi sistemdə işləyən zaman yaranan fasilələrdən və sistemdə baş verən nasazlıqlardan istifadə etməklə "sətirlərarası" işləmək məqsədilə rabitə xətlərinə qeyri-qanuni qoşulma;
- dezinformasiya aparmaq və yanlış məlumatlan yaymaq məqsədilə qanuni istifadəçi sistemə daxil olduqdan sonra onun kompüterini şəbəkədən fiziki ayırmaq və sonradan onun adı altında audentifikasiya prosedurasını uğurla keçmək (adlamaq) yolu ilə bilavasitə bu istifadəçini əvəz etmək üçün rabitə xətlərinə qeyri-qanuni qoşulma.

İnformasiya təhlükəsizliyinə qarşı qəsdən törədilən təhlükələr, bir qayda olaraq, informasiya resurslarına, onların saxlandığı, emal olunduğu, ötürüldüyü sistemlərə icazəsiz girişin əldə olunmasına yönəlmiş olur.

Ümumi halda, bu təhlükələrin səbəbkarı olan və meydana gəlməsində iştirak edən şəxslərin statusuna görə onları iki qrupa bölmək olar:

- kompüter sistemlərinin və şəbəkələrinin, informasiya resurslarının, ayrı-ayrı kompüterlərin və digər avadanlıq və qurğuların qanuni istifadəçiləri tərəfindən törədilən təhlükələr;
- istifadəçi olmayan kənar şəxslər tərəfindən həyata keçirilən təhlükələr.
- İstifadəçilər tərəfindən törədilə biləcək təhlükələrin əsas aşağıdakı növlərini qeyd etmək olar:
- əməli yaddaşda olan qalıq informasiyanın baxılması və təhlili;

- sistemdə saxlanılan informasiyaya icazəsiz girişin əldə edilməsi və öz məqsədləri üçün ondan istifadə olunması;
- avtorizə edilmiş istifadəçinin adı altinda pərdələnmə;
- özgə faylların və məlumatların baxılması, təhlili və s.

İstifadəçi olmayan şəxslərin informasiya emalı və ötürülməsi sistemlərinə düşünülmüş nüfuz etməsi (daxilolması) cəhdləri ***passiv*** və ya ***aktiv*** ola bilər.

Passiv təhlükələr – sistemin istifadəçisi olmayan pozucu tərəfindən informasiya emalı və ötürülməsi prosesinə qarışmadan trafıkə passiv nəzarət edilməsindən ibarətdir. Belə ki, pozucu sistemin istənilən nöqtəsində rabitə xətlərindən elektromaqnit şüalanmaların tutulması və toplanması üçün bu xətlərə qoşulur və ya xüsusi texniki vasitələrdən istifadə edir və sistemin işinə heç bir təsir göstərmir.

Sistemə aktiv nüfuzetmə dedikdə informasiya emalı və ötürülməsi sistemlərində saxlanılan qorunan informasiyaya birbaşa giriş, onların baxılması, götürülməsi, dəyişdirilməsi və ya pozulması başa düşülür. Sistemə belə nüfuzetmə, əsasən, gizli, yəni informasiyanın qorunmasını təmin edən nəzarət proqramlarını adlamaq yolu ilə həyata keçirilir.

Bir qayda olaraq, belə hərəkətlər aşağıdakı kimi daxil olma proseduraları vasitəsilə reallaşdırılır:

- sistemə və ya onun hissəsinə daxil olmaq, maraq kəsb edən informasiyanı saxlayan fayllara müraciət etmək üçün əvvəlcədən məlum olan vasitələrdən istifadə edilməsi;
- ziyanverici proqramların, o cümlədən emal olunan və ötürülən informasiyam tutan, müəyyən fayla yazan və ya müəyyən ünvana göndərən proqram qoyuluşlarının ("troya atlan"nın, kompüter viruslarının və s.) sistemə yeridilməsi;
- həqiqi istifadəçinin parolunu və digər giriş rekvizitlərini ələ keçirdikdən sonra bu istifadəçinin adı altında maskalanma;
- xidməti mövqedən istifadə, yəni təşkilatın əməkdaşları tərəfından fayllarda olan informasiyanın plandan kənar baxılması və ya giriş hüquqlarının kənar şəxslərə verilməsi;
- sistemdə proqramçılar və xidməti personal tərəfından qoyulmuş və ya sistem yoxlamaları zamanı aşkar olunmuş giriş nöqtələrindən istifadə olunması;
- qanuni istifadəçi kompüteri (işçi stansiya) ilə mərkəzi kompüter arasındakı əlaqəni kəsmək yolu ilə sistemə daxilolmam təmin edən xüsusi terminalın rabitə xəttinə qoşulması, sonradan kəsilmiş əlaqənin səhv qoşulma kimi bərpası və ya qanuni istifadəçi kanalı məşğul edərək fəallıq göstərmədikdə kanaldan istifadə edilməsi;
- sistemdə işin başa çatması haqqında istifadəçinin siqnalının ləğv edilməsi və sonradan onun adı altında işin davam etdirilməsi.

Bundan əlavə, istifadəçi olmayan şəxslər tərəfindən informasiya daşıyıcılarının və təsvirlərinin oğurlanması, kompüter texnikasının parametrlərinin dəyişdirilməsi, avadanlığın sıradan çıxarılması və s. kimi təhlükələr törədilə bilər. Qeyd olunmalıdır ki, ziyankarlar öz məqsədinə çatmaq üçün yuxarıda sadalanan mexanizmlərdən birini deyil, eyni zamanda bir neçəsini reallaşdıra bilər.

Ziyanverici proqramlar. Xüsusi şəkildə proqramlara daxil edilən, kompüterin digər proqramlarına, habelə rabitə kanalları və ya informasiya daşıyıcıları vasitəsilə KSŞ-nin digər qovşaqlarına və kompüterlərinə yayılmaq qabiliyyətinə malik olan ziyanverici proqramlar son dövrlərdə informasiya təhlükəsizliyinə real təhlükə kimi meydana çıxmışdır. Kompüter şəbəkələrində bir kompüterə düşmüş ziyanverici proqramın qarşısı vaxtında alınmadıqda, o, nəzarətsiz olaraq həmin kompüterdən digərlərinə yayıla, böyük şəbəkələrdə isə bu problem "həqiqi epidemiya" xarakteri ala bilər.

Bu gün bir çox istifadəçilər bu və ya digər şəkildə kompüterə ziyan vuran bütün ziyanverici proqramları kompüter virusları adlandırırlar. Əslində bu belə deyil. Belə ki, elə

ziyanverici proqramlar var ki, müxtəlif virus texnologiyalarını istifadə etmələrinə baxmayaraq mahiyyət etibarı ilə onlar virus deyillər.

Son dövrlərin tendensiyası göstərir ki, hakerlər ziyanverici proqramların yaradılması və yayılmasından qeyri-leqal gəlir əldə etmək məqsədi güdürlər. Belə ki, əvvəllər ziyanverici proqramları zövq almaq, özünü nümayiş etdirmək və s. məqsədlərlə yazır və yayırdılarsa, hazırda bu iş bir gəlir mənbəyinə çevrilmişdir. Bu "biznes" aşağıdakı yollarla reallaşdırılır:

- bank hesablarına giriş əldə etmək üçün bank məlumatlarının oğurlanması;
- kredit kartlarının nömrələrinin oğurlanması;
- sonradan dayandırmaq üçün pul tələb etmək məqsədilə DDoS tipli paylanmış şəbəkə hücumlarının təşkili (kompüter reketi);
- spamların yayılması və kommersiya məqsədilə istifadə üçün troya proksi-serverləri şəbəkələrinin yaradılması;
- çoxməqsədli tətbiq üçün zombi-şəbəkələrin formalaşdırılması;
- arzu olunmayan reklamın göstərilməsi üçün sistemi köçürən və quraşdıran proqramların yaradılması;
- pullu telefon nömrələrinə istifadəçidən xəbərsiz zəng edən troya proqramlarının kompüterlərə tətbiqi.

Araşdırmalar göstərir ki, 2017-ci il ərzində troya proqramlarının sayı təxminən üç dəfə çoxalmış, antivirus proqramlarının həcmi də bir o qədər artmışdır. Ziyanverici proqramların yalnız 5%-i zövq almaq, 75%-i pul əldə etmək, qalan 20% isə digər məqsədlər üçün yaradılmışdır.

Ziyanverici proqramlara aşağıdakılar aid edilir:

- kompüter virusları;
- şəbəkə qurdlan;
- troya proqramları;
- spamlar;
- haker utilitləri.

Kompüter virusları. **Kompüter virusları** – kompüterdə çoxalmaq, həmçinin rabitə kanalları, kompüter şəbəkələri və informasiya daşıyıcıları (CD və maqnit disklər və s.) vasitəsilə digər kompüterlərə və şəbəkələrə yayılmaq (ötürülmək) qabiliyyətinə malik olan ziyanverici proqramlardır.

Kompüter virusları, bir qayda olaraq, ziyankar (məkrli niyyəti olan) proqramçılar tərəfindən hazırlanır və xüsusi şəkildə hər hansı proqramın tərkibinə yerləşdirilərək kompüterin yaddaşına daxil edilir. Belə proqramın yüklənməsi virusun işə düşməsinə səbəb olur. Bundan sonra, viruslar növündən asılı olaraq, kompüterin yaddaşına, yaddaşda olan informasiya resurslarına, yüklənmiş proqramlara və s. yayılır, müəyyən olunmuş vaxtda təyinatı üzrə xəbərdaredici və ziyan vurucu işləri yerinə yetirirlər.

Qeyd etmək lazımdır ki, əksər hallarda məhz serverlər kompüter viruslarının hədəfinə çevrilir. Bir qayda olaraq, kompüter şəbəkələri, o cümlədən İnternet virusların yayılması üçün potensial vasitə rolunu oynayır. Belə ki,

viruslar serverdə olan proqramları yoluxdura, şəbəkə vasitəsilə ona qoşulmuş kompüterlərə (işçi stansiyalara) yayıla və bütün şəbəkəyə ciddi ziyan vura bilər.

Bəzən kompüter virusu yarandığı ilk anda fəaliyyət göstərmir. Kompüterin yaddaşında və ya proqramlarda "yaşayan" belə viruslar yalnız müəyyən olunmuş vaxtlarda işə düşür. Viruslar emal olunan bütün informasiyalan izləyir və informasiya bir yerdən başqa yerə ötürüldükdə virus da onunla birlikdə yerini dəyişir.

Ümumiyyətlə, bioloji viruslar canlı orqanizmlərə yoluxduğu kimi, kompüter virusları da kompüterlərə və kompüter proqramlarına yoluxur və onları "xəstələndirir". Kompüterin

əməliyyat sistemi, tətbiqi proqramlar, drayverlər, əməli yaddaşlar və s. kompüter viruslarına yoluxa bilər.

Virusların yayılmasının ən asan yolu yoluxmuş faylların disketlər, CD disklər, kompüter şəbəkələri vasitəsilə köçürülməsidir. Belə ki, virusa yoluxmuş kompüterdə istifadə olunan disket və ya bu disketə yazılan yeni proqram həmin virusa yoluxa bilər. Başqa sözlə, virus daşıyıcısı olan disketin tamamilə "sağlam" kompüterdə istifadəsi və ya bu kompüterə viruslu proqramın yüklənməsi həmin kompüteri də yoluxdurur.

Kompüter virusları proqram təminatında və yaddaş qurğularında yerləşməsi, KSŞ-də yayılması, fəallaşması üsullarına və vurduğu ziyanın xarakterinə görə fərqlənirlər.

Kompüter virusları yazılmış informasiyanın və proqramların təhrif olunması, korlanması və ya məhv edilməsi, istifadəçilərin sorğularına sistemin reaksiya verməsi və proqramların yerinə yetirilməsi üçün tələb olunan vaxtın artması, kompüterin düzgün fəaliyyətinin pozulması, disk qurğularının sıradan çıxması və s. kimi ağır nəticələr verə bilər.

Viruslar bəzən xoşxassəli əlamətlərə də malik ola bilərlər. Məsələn, proqramların yerinə yetirilmə sürəti azala, ekranda simvollar və ya işıqsaçan nöqtələr əmələ gələ bilər.

Bəzi viruslara inkişaf edən əlamətlər xas olur. Başqa sözlə, "xəstəlik" getdikcə kəskinləşir. Məsələn, aydın olmayan səbəblərdən proqramların həcmi hər istifadə zamanı əhəmiyyətli dərəcədə artır və yaddaş qurğuları dolur. Nəticədə, bu, faylların silinməsinə və proqram təminatının məhvinə gətirib çıxara bilər.

İnformasiya təhlükəsizliyi baxımından kompüter viruslarının müsbət cəhətini də qeyd etmək lazımdır. Belə ki, proqram təminatlarında virusların mövcud ola bilməsi faktı proqram oğurluğunun qarşısının alınmasında yaxşı mühafizəçi rolunu oynayır.

Bəzən proqramı hazırlayanlar öz proqramlarını və disklərini hər hansı virusla qəsdən yoluxdururlar ki, icazəsiz şəkildə proqramı və ya diski köçürənlər kompüterlərində virusların yayılması problemi ilə qarşılaşsınlar.

Şəbəkə qurdları. Şəbəkə qurdlan kateqoriyasına ziyanvericilik fəaliyyətini həyata keçirmək məqsədilə öz sürətlərini aşağıdakı yollarla lokal və ya qlobal kompüter şəbəkələri vasitəsilə yayan ziyanverici proqramlar aid edilir:

- uzaq məsafədə olan kompüterlərə soxulmaq;
- öz surətini uzaq məsafədə olan kompüterlərdə işə salmaq;
- gələcəkdə şəbəkənin digər kompüterlərinə yayılmaq.

Şəbəkə qurdları disklərdə olan faylları dəyişdirmirlər, lakin kompüter şəbəkələrində yayılır, kompüterin əməliyyat sisteminə girir, digər kompüterlərin və ya istifadəçilərin ünvanlarmı tapır və müxtəlif yayma vasitələrindən istifadə etməklə özünün surətini həmin ünvanlara göndərir.

Özlərinin yayılması üçün şəbəkə qurdlan müxtəlif kompüter və mobil şəbəkələrdən istifadə edirlər. Belə şəbəkələrə misal olaraq aşağıdakıları göstərmək olar:

- İnternet, o cümlədən elektron poçtu;
- məlumatların ani (interaktiv) mübadiləsi sistemləri;
- faylların mübadiləsi şəbəkələri;
- İRC (İnternet Relay Chat) şəbəkələr;
- lokal şəbəkələr;
- mobil qurğular (telefonlar, cib kompüterləri və s.) arasında məlumatların mübadiləsi şəbəkələri.

Əksər məşhur şəbəkə qurdlan fayllar şəklində – elektron məktuba əlavə, Veb və ya FTP resurslarda, İCQ və İRC məlumatlarda yoluxmuş fayla istinadlar, P2P (Peer to Peer) mübadilə kataloqunda fayl şəklində yayılırlar. Bəzi şəbəkə qurdlan şəbəkə paketləri şəklində yayılaraq kompüterin yaddaşına daxil olur və öz kodunu aktivləşdirir. Belə şəbəkə qurdlarını "faylsız" və ya "paket" qurdlan adlandırırlar.

Şəbəkə qurdları istifadəçi tərəfindən hər hansı hərəkət edilmədən yoluxmuş maşınlara daxil olurlar. Onlar öz təbiətlərinə görə bioloji prototiplərinə çox yaxındırlar. Hələ ki, qabaqlayıcı tədbirlər, o cümlədən antivirus skanerləri və vaksinləri şəbəkə qurdları ilə mübarizədə çox qeyri-effektiv olaraq qalırlar. Onlar viruslardan fərqli olaraq, özlərinin yayılması üçün lokal və qlobal şəbəkələrin protokollarından və imkanlarından fəal surətdə istifadə edirlər, ona görə də onları şəbəkə qurdları adlandırırlar.

Uzaq məsafədə olan kompüterə daxil olmaq və öz surətini işə salmaq üçün şəbəkə qurdları müxtəlif üsullardan istifadə edirlər:

- sosial mühəndislik – social engineering (məsələn, qoşma faylı açmağa çağıran elektron məktubun mətni);
- şəbəkənin konfıqurasiyasında olan nöqsanlar (məsələn, tam giriş üçün açıq olan diskə köçürmə);
- əməliyyat sistemlərinin və əlavələrin təhlükəsizlik xidmətlərində səhvlər;
- xüsusi toplayıcı proqram – virus və ya qurd olmayan bu proqram özü kompüterə daxil olur, sonra isə şəbəkə qurdunu və ya virusu hissə-hissə şəbəkədən kompüterə köçürür. Qurd və ya virus kompüterə hissə-hissə köçürüldüyündən antivirus proqramları onu aşkar edə bilmir.

Bəzi şəbəkə qurdlan digər ziyanverici proqramların xassələrinə malik olurlar. Məsələn, bəzi şəbəkə qurdlan özündə troya funksiyalarını saxlayır və ya kompüter viruslarına analoji olaraq lokal diskdə yerinə yetirilən faylları yoluxdura bilirlər. Başqa sözlə, şəbəkə qurdlan troya proqramlarının və ya kompüter viruslarının xassələrinə malik olurlar.

Troya proqramları. Troya proqramları (troya atları) – yad kompüterlərə uzaq məsafədən girişi təqdim edən, həmin kompüterdə müxtəlif manipulyasiyalar etməyə, məxfi məlumatları (parolları, kredit kartların nömrələrini, İnternetə və kompüterə giriş adlarını və s.) ötürməyə imkan verən ziyanverici proqramlardır. Onlar kompüter virusları deyillər, hər hansı pozucu funksiyaya malik olmur və digər kompüterlərin idarə olunması və ya orada yerinə yetirilən proseslərin nəzarət edilməsi üçün nəzərdə tutulmuşdur.

Troya proqramları, adətən, başqa faylları yoluxdurmurlar, öz-özünə çoxalmırlar, amma məşhur (geniş yayılmış) proqramlarda maskalanaraq istifadəçini həmin proqramı öz kompüterinə köçürməyə və ziyanvericini kompüterdə quraşdıraraq işə salmağa təhrik edirlər.

Kompüterə düşdükdən sonra troya proqramları özünü şübhə doğurmayan (məsələn, winrun32dll.exe) adla sistem qovluqlarına köçürür. Bundan sonra əməliyyat sistemi yenidən yüklənəndə yerinə yetirilən proqramların qeydiyyatının aparıldığı reyestrə (HKEY_LOCAL_MACHINE\- SOFTW ARE\Microsoft\Windows\Current Version\Run), eləcə də Run, RunOnce, Runservices, RunservicesOnce adlı bölmələrə yazır.

Yerinə yetirdiyi ziyanverici hərəkətlərinə görə troya proqramlarını şərti olaraq aşağıdakı növlərə bölmək olar:

- uzaq məsafədən icazəsiz idarəetmə utilitləri – yoluxmuş kompüterin bədniyyətli şəxs tərəfindən uzaq məsafədən idarə edilməsinə imkan verir;
- DDoS (Distributed Denial of Service – "xidmət göstərməkdən imtina edilməsi") həyata keçirmək üçün utilitlər –yoluxmuş kompüterin informasiya sisteminin resurslarmı tükəndirir ki, bunun da nəticəsində sistem öz funksiyalarını yerinə yetirə bilmir və əlçatmaz olur;
- casus proqramları – istifadəçinin hərəkətlərini gizli olaraq müşahidə edir və bədniyyətli şəxsi maraqlandıran məlumatlan öz "jurnalına" yazır;
- reklam proqramları – daha tez-tez istifadə olunan proqramlara reklam və elan xarakterli məlumatlan yerləşdirməyə imkan verir;

- zəng etmə proqramları – modem və ya telefon xətlərinin köməyi ilə kommersiya əsaslı serverə zəng edərək istifadəçini xidmətlərin haqqını ödəməyə təhrik edir;
- spamların yayılması serveri – kənar şəxsin kompüterini spamların yayılması serverinə çevirməyə imkan verir;
- çoxkomponentli troya proqramları-yükləyicilər – digər ziyanverici proqramları və ya onların komponentlərini İnternetdən köçürür və sistemə yeridir.

Troya atlarının müasir dövrdə daha tez-tez istifadə olunan əsas aşağıdakı növlərini qeyd etmək olar: *Mail Senders, BackDoor, Log Writers* və ya *KeyLoger*.

Mail Senders – quraşdırıldığı kompüterdən məlumatları "sahibinə" göndərir. Bu tip troya atlarını digər kompüterlərə yeridən şəxslər onların köməyi ilə İnternetə, o cümlədən İCQ, elektron poçtu, Chat xidmətlərinə giriş parollarını əldə edə bilər. Bu zaman hətta kompüter sahibinin xəbəri olmur ki, kimsə onun poçtunu oxuyur, onun adından İnternetə qoşulur, İCQ identifikatorundan istifadə etməklə əlaqə siyahısında olan digər istifadəçilərə analoji troya atlanın yayır. Mail Senders sahibindən, yəni onu quraşdıran şəxsdən asılı olmadan fəaliyyət göstərir, ona bütün "tapşırıqlar" quraşdırılma zamanı verilir və o, bütün funksiyalarını plan üzrə həyata keçirir.

BackDoor – Mail Senders troya atlarının bütün imkanlarını yerinə yetirməklə yanaşı digər kompüterlərin uzaq məsafədən (məsələn İnternet vasitəsilə) idarə edilməsi üçün 10-a qədər əlavə funksiya təqdim edir. BackDoor sözünün hərfi tərcüməsi arxa qapı və ya gizli giriş mənasını verir. Belə troya atlan istənilən şəxsə yoluxmuş kompüterə tam giriş imkanı verir. O, müştərinin qoşulmasını gözləyir. Yoluxmuş kompüterdə müştəri İnternetə və ya lokal şəbəkəyə qoşulduqdan sonra troya atı topladığı məlumatlan öz sahibinə göndərir və bu kompüterə girişi açır. Belə ki, o, müəyyən sistemdə şəbəkə portlarmı açır və bu barədə öz sahibinə məlumat verir.

BackDoor proqramları iki növə bölünür:

Lokal BackDoor – müəyyən lokal imtiyazlar təqdim edir. Məsələn, kompüterdə qeydiyyatdan keçmiş bir neçə istifadəçi sistem administratorunun hüquqlarına malik olmurlar, lakin kompüterə yeridilmiş lokal BackDoor troya atı onun sahibi olan istifadəçiyə sistem administratorunun hüquqlarını təqdim edir.

Uzaqda olan BackDoor – uzaq məsafədən kompüterə shell təqdim edə bilər. Girişin təqdim edilməsi – shell proqramının iki növü mövcuddur: BindShell və Back Connect.

BindShell – daha geniş yayılmışdır, "müştəri-server" texnologiyasına əsasən işləyir, yəni sahibinin qoşulmasını gözləyir.

Back Connect – brandmauerləri adlamaq üçün tətbiq olunur. O, sahibinin kompüterinə qoşulmağa cəhd edir.

Log Writers və ya ***Key loggers*** – kompüterdə klaviaturadan daxil edilən bütün məlumatlan köçürür və fayla yazır. Bu fayl sonradan ya elektron poçtu vasitəsilə müəyyən ünvana göndərilir, ya da FTP vasitəsilə baxılır. Son vaxtlar bu proqramlar bir sıra əlavə funksiyalar da yerinə yetirirlər: proqramların pəncərələrindən informasiyanın tutulması; siçanın düyməsinin basılmasının tutulması; ekranın və aktiv pəncərələrin şəklinin çəkilməsi, göndərilən və alınan bütün məktubların qeydiyyatının aparılması; faylların istifadəsi fəallığının, sistem reyestrinin və printerə göndərilmiş tapşırıqlar növbəsinin monitorinqi, kompüterə qoşulmuş mikrofondan səsin və veb-kameradan videonun tutulması və s.

Key loggers proqramlarının beş növü məlumdur:

- hökumət təşkilatlarının himayəsi altında işlənib hazırlanan və tətbiq edilən (məsələn, ABŞ-da Magic Lantern proqramı, Cyber Knight layihəsi) casus proqramları;
- müxtəlif əməliyyat sistemlərinin istehsalçıları tərəfindən işlənib hazırlanan və əməliyyat sisteminin özəyinə daxil edilən casus proqramları;

- istifadəçinin kompüterindən mühüm informasiyanın oğurlanması ilə bağlı konkret məsələnin həlli üçün məhdud sayda (çox vaxt bir və ya bir neçə nüsxədə) yaradılan casus proqramları;
- kommersiya, xüsusən, korporativ proqramlar – çox nadir hallarda siqnatura bazasına daxil edilirlər (yalnız siyasi motivlərə görə);
- virus proqramlarının tərkibinə daxil olan keylogging modulundan ibarət olan casus proqramları. Siqnatura məlumatları virus bazalarına daxil edilənədək bu modullar naməlum qalırlar. Belə proqramlara nümunə kimi klaviaturada düymənin basılmasının tutulması və əldə olunmuş məlumatların İnternet vasitəsilə ötürülməsi modulunu özündə saxlayan məşhur virusları göstərmək olar.

Bundan əlavə, troya proqramlarının daha iki növü mövcuddur: ***Trojan-Dropper*** və ***Trojan-Downloader***. Hər iki proqram məqsədi kompüterə şəbəkə qurdu və ya troya atı kimi ziyanverici proqramların yüklənməsindən ibarətdir, yalnız onların fəaliyyət prinsipləri fərqlənir.

Trojan-Dropper özündə artıq məlum ziyanverici proqramları saxlaya və ya onların yeni versiyalarını yükləyə bilər. Onlar kompüterə bir deyil, eyni zamanda bir-birindən fərqlənən və ayrı-ayrı adamlar tərəfindən yazılmış bir neçə ziyanverici proqramı yükləyə bilər.

Trojan-Downloader proqramları virus yazanlar tərəfından fəal istifadə olunur. Bunun əsas səbəbləri məlum troya proqramlarının onun tərkibində gizlədilməsinin mümkünlüyü, onun ölçüsünün Trojan-Dropper proqramlarına nisbətən kiçik olması, eləcə də troya atlarının yeni versiyalarının işə salınmasının asanlığı ilə bağlıdır.

Hər iki növ ziyanverici proqramlar yalnız troya proqramlarının deyil, həmçinin müxtəlif virus, reklam (adware) və ya pornoqrafik (pornware) proqramların kompüterlərdə quraşdırılması üçün istifadə olunur.

Spamlar. Spam – xüsusi proqramlar vasitəsilə siyasi, kommersiya, reklam və digər növ məlumatların, bu məlumatlan almaq arzusunu bildirməyən insanlara kütləvi və anonim şəkildə göndərilməsidir.

Burada ***anonim yayma*** dedikdə, məlumatların gizli və ya saxta əks ünvanla avtomatik yayılması başa düşülür. Hazırda elə spam göndərən yoxdur ki, o öz ünvanını və göndərmə yerini gizlətməsin. ***Kütləvi yayma*** hər hansı spam göndərən tərəfından müəyyən məlumatın eyni zamanda yüzlərlə, minlərlə, hətta milyonlarla ünvana göndərilməsini nəzərdə tutur. Qeyd etmək lazımdır ki, məktubun səhvən başqa ünvana göndərilməsi spam deyil, arzuolunmaz poçt kimi qəbul edilir. ***Alınması arzu olunmayan göndəriş*** alan şəxsin arzusunun, hətta iradəsinin əksinə olaraq hər hansı məlumatın onun ünvanına göndərilməsini ehtiva edir. Lakin konfranslar və planlaşdırılan digər tədbirlər barədə məlumatlandırıcı poçt göndərişləri spamlara aid edilməməlidir.

Spamların daha geniş yayılmış növlərinə aşağıdakıları aid etmək olar:

- **Reklam.** Leqal bizneslə məşğul olan bəzi şirkətlər öz məhsullarmı və xidmətlərini daha ucuz və rahat yolla spamların köməyi ilə yayırlar. Onlar öz reklamlarının yayılmasını müstəqil şəkildə özləri həyat keçirə və ya bu sahədə ixtisaslaşan təşkilatlara (şəxslərə) sifariş edə bilərlər.
- **Qeyri-qanuni məhsulun reklamı.** Spamlar vasitəsilə çox vaxt başqalarına məlumat vermək, yaymaq mümkün olmayan məhsulları (pornoqrafıyam, saxta malları, dövriyyəsi məhdudlaşdınlmış dərman məhsullarını, qeyri-qanuni yolla alınmış gizli məlumatlan, verilənlər bazasını və s.) reklam edirlər.
- **Əks-reklam.** Spam, həmçinin reklam haqqında qanunla qadağan edilmiş informasiyanın (məsələn, rəqibləri və onları pisləyən, ləkələyən) yayılması üçün istifadə olunur.

- **Nigeriya məktubu.** Spam məktub göndərilən adamdan pul qoparmaq üçün istifadə olunur. Belə məktublar daha çox Nigeriyadan göndərildiyinə görə onları daha çox "Nigeriya məktubları" adlandırırlar. Belə məktublarda məlumat verilir ki, məktubu alan şəxs hər hansı yolla böyük məbləğdə pul əldə edə bilər və məktub göndərən bu işdə ona kömək edə bilər. Maraq göstərildiyi halda, məktub göndərən müxtəlif bəhanələrlə (bankda hesab açmaq, sənədləri rəsmiləşdirmək və s.) bir az pul köçürülməsini xahiş edir. Fırıldaqçıların məqsədi məhz bundan ibarətdir. Belə fırıldaqçılığın nisbətən az yayılmış adı skam və ya skam419 (Nigeriya CM-də maddənin nömrəsinə uyğun olaraq) adlanır.
- **Fişinq.** İngilis dilində olan phishing və ya fishing (balıq tutmaq) sözündəndir. Məktub göndərən alan şəxsdən kredit kartının nömrəsini və ya elektron (online) ödəmə sisteminə giriş parolunu öyrənmək üçün Fişinqdən istifadə edir. Belə məktublar, adətən, bankın administratoru tərəfindən yazılmış məktub kimi göndərilir. Məsələn, məktubda göstərilir ki, müştəri özü haqqında məlumatları təsdiq etməlidir, əks halda onun hesabı bağlanacaqdır. Sonda ona doldurmaq üçün müvafiq formanın yerləşdiyi saytın ünvanı təklif olunur. Bu formada digər məlumatlarla yanaşı lazım olan rekvizitlərin də doldurulması tələb olunur.

Praktikada spamların aşağıdakı növlərindən də istifadə olunur:

- Xoşməramlı məktublar.
- Siyasi təbliğatın yayılması.
- Poçt sisteminin sıradan çıxarılması üçün kütləvi göndərişlər təşkil etmək.
- Hər hansı şəxsə qarşı mənfı münasibət yaratmaq məqsədilə onun adından kütləvi göndərişlər təşkil etmək.
- Kompüter viruslarını saxlayan məktubların kütləvi göndərilməsini təşkil etmək.

Qeyd etmək lazımdır ki, müəyyən növ məlumatların kütləvi yayılması üçün alanların razılığının tələb olunmaması azadlığı (qanuniliyi) hər bir ölkənin qanunvericiliyində təsbit oluna bilər. Məsələn, yaxınlaşan təbii fəlakət, vətəndaşların kütləvi səfərbərliyi, seçkilər və s. barədə məlumatlar üçün yayılma azadlığı təmin edilə bilər. Lakin insanların almaq istəmədiyi məlumatların onların iradəsinin əleyhinə göndərilməsi arzuolunmaz haldır. Bu, insanların vaxtının və maddi imkanlarının lazımsız sərfinə, mənəvi və fiziki yüklənməsinə səbəb olur. Belə məlumatlar son dövrlərdə elektron informasiya vasitələri (İnternet, mobil telefonlar, televiziya və radio və s.) ilə daha çox yayılmağa başlanmışdır.

Spamlar yayılması aşağıdakı yollarla həyata keçirilə bilər:

- **Elektron poçtu.** Spamların yayılması üçün müəyyən zəif yerləri olan və ya imkanlar yaradan serverlərdən, vebmail serverlərindən, kompüter-zombilərdən və s. istifadə olunur.
- **Usenet**. Hazırda istifadəçilər əksər, ələlxüsus nizamlanmayan Usenet xəbərlər qruplarını tərk edir və nizamlanan konfranslardan istifadə edirlər, çünki ənənəvi Usenet qrupları, demək olar ki, yalnız reklamları özündə saxlayır.
- **Məlumatların ani göndərilməsi,** yəni interaktiv məlumat mübadiləsi sistemləri (ICQ və s.) də spamların göndərilməsi üçün fəal istifadə olunur. Belə spamları SPİM (SPam + Instant Messenger) adlandırırlar.
- **SPIT** (Spam over IT) – IP-telefon vasitəsilə yayılan spam.
- **Bloqlar, vikilər, forumlar və elan lövhələri.** Son dövrlərdə istifadəçilərə öz qeydlərini yazmaq, məlumatlar daxil etmək, dəyişikliklər aparmaq və s. imkanları verən veb-saytlar geniş yayılmışdır. Məhz bu imkanlardan spamların göndərilməsi və yayılması üçün istifadə edirlər.
- **Şəbəkə məlumatları,** o cümlədən şəbəkə ilə reklam məlumatlarının göndərilməsi.
- **SMS-məlumatlar.** Mobil telefonlara spam xarakterli SMS-mesajların göndərilməsi üçün geniş istifadə olunur.

Digər ziyanverici proqramlar. Qeyd etmək lazımdır ki, ziyanverici proqramların kifayət qədər müxtəlif növləri mövcuddur. Yuxarıda sadalanan növlərlə yanaşı aşağıdakı ziyanverici proqramların – haker utilitlərinin adlarını da qeyd etmək olar: Root-Kit, snifferlər, Exploit, HackTool, Nuker, Flooder, Constructor, Bad-Joke, Hoax, FileCryptor, PolyCryptor, PolyEngine, VirTool, Riskware, Adware (Advware, Spyware, Browser Hijackers), Pornware (Porn-Dialer, Porn-Downloader, Porn-Tool).

Təhlükələr və onların informasiya təhlükəsizliyinin baza prinsiplərinə təsiri. Aydındır ki, informasiyanın təhlükəsizliyini poza biləcək təhlükələrin təbiətini qabaqcadan dəqiq müəyyən etmək mümkün olmur. Lakin təhlükələri kompüter sistemlərinə və şəbəkələrinə, onların informasiya resurslarına göstərdiyi təsirə, eləcə də informasiya təhlükəsizliyinin baza prinsiplərinin pozulması xarakterinə görə fərqləndirirlər.

Yuxarıda qeyd olunduğu kimi, informasiya təhlükəsizliyinin baza prinsipləri dedikdə informasiyanın məxfiliyinin və tamlığının, eləcə də onlara icazəli girişin təmin edilməsi başa düşülür. 3.1 saylı cədvəldə KSŞ-də rast gəlinən əsas təhlükələrin siyahısı verilmiş və hər bir konkret təhlükə meydana çıxdıqda informasiya təhlükəsizliyinin hansı baza prinsipinin pozulmasının mümkünlüyü göstərilmişdir.

Praktiki olaraq, hər bir təhlükənin baş verməsi nəticəsində informasiya təhlükəsizliyinin baza prinsiplərindən biri, ikisi və ya üçü pozula bilər, lakin bunu həmişə qabaqcadan müəyyən etmək mümkün olmur.

İnformasiyanın təhlükələrdən qorunması üçün onların fəaliyyəti və təsirləri xüsusi diqqətlə təhlil edilməlidir. Çoxlu sayda təhlükələrin yaranması ehtimalını azaltmaq məqsədilə onların qarşısının alınması üçün konkret tədbirlərin görülməsi, başqa sözlə, qabaqlanması olduqca vacibdir. Lakin elə təhlükələr ola bilər ki, onları qabaqcadan aşkar etmək və qarşısını almaq çox çətin olur, bəzən isə heç mümkün olmur.

İnformasiya təhlükəsizliyinin pozulması baxımından kompüter sisteminin təsirə məruz qala biləcək obyektləri və bu təsir nəticəsində baş verə biləcək pozuntu halları barədə məlumat 3.2 saylı cədvəldə verilmişdir.

Cədvəl 3.1. Təhlükələr və informasiya təhlükəsizliyinin baza prinsipləri

№	Baza prinsipləri / Təhlükələr	Məxfiliyin pozulması	Tamlığın pozulması	Təcridetmə
1.	Təbii fəlakətlər (yanğın, su basına, zəlzələ və s.)	X	X	X
2.	Aparaturanın sıradan çıxması	X	X	X
3.	Elektromaqnit şüalanmaların toplanması	X		
4.	Müxtəlif siqnalların tutulması	X		
5.	İnformasiya daşıyıcılarının fiziki və məntiqi korlanması		X	X
6.	Məlumatların və proqramların qəsdən korlanması		X	X
7.	İnformasiya daşıyıcılarının oğurlanması	X	X	X
8.	Giriş hüquqlarının başqa şəxslərə verilməsi	X	X	
9.	Avtorizə edilmiş istifadəçinin adı altında maskalanma	X	X	X
10.	Ehtiyatsız davranma, səhlənkarlıq	X	X	X
11.	Məlumatların və sənədlərin dəyişdirilməsi	X	X	X
12.	Sistem utilitlərinin istifadəsi	X	X	X
13.	Qanuni istifadəçilərin hüquqlarından istifadə edilməsi	X	X	X
14.	Təhrifetmə, aldatma	X	X	
15.	Sistemin həddən artıq yüklənməsi və ilişməsi		X	X
16.	Proqramlaşdırmada səhvlər	X	X	X
17.	Əməliyyat sistemlərinin və proqramların versiyalarının müxtəlifliyi		X	X
18.	Qeyri-dəqiq və ya köhnəlmiş informasiya		X	

19.	Istifadəyə maneçilik yaratma			X
20.	Qalıq informasiyanın toplanması	X		
21.	Məntiqi bombalar	X	X	X
22.	Gizli gedişlərin edilməsi və «deşiklər»in istifadəsi	X	X	X
23.	Kompüter virusları	X	X	X
24.	Troya atları	X	X	X
25.	Səhv marşrutlaşdırma	X	X	X
26.	Şəbəkə analizatorları	X	X	

Cədvəl 3.2. Təhlükəsizliyin pozulması üsulları

Təhlükəsizliyin pozulması üsulları	**Təsir obyektləri**			
	Avadanlıq	**Proqramlar**	**Məlumatlar**	**Personal**
İnformasiyanın məxfiliyinin açılması (sızması)	İnformasiya daşıyıcılarının oğurlanması, rabitə xətlərinə qoşulma, resursların icazəsiz istifadəsi	İcazəsiz köçürmə, tutma, ələ keçirmə	Oğurlama, köçürmə, tutma	Qoruma haqqında məlumatların başqa şəxslərə ötürülməsi, yayılması, səhlənkarlıq
İnformasiyanın tamlığının pozulması	Qoşulma, dəyişiklik etmə, xüsusi qoyuluş, iş rejimlərinin dəyişdirilməsi, resursların icazəsiz istifadəsi	"Troya atları"nın və "qurdlar"ın yeridilməsi	Təhrifetmə, dəyişdirmə	Personalın cəlb edilməsi
Avtomatlaşdırılmış sistemlərin iş qabiliyyətinin pozulması	Sistemin iş rejiminin dəyişdirilməsi, sıradan çıxarılması, oğurladılması, məhv edilməsi	Təhrifetmə, pozma, başqası ilə dəyişdirmə	Təhrifetmə, pozma, yanlış məlumatların istifadəsinə vadar etmə	Xidmət göstərilməsi, fiziki ayrılma
İnformasiyanın surətinin qanunsuz çoxaldılması	Lisenziya olmadan analoqların hazırlanması	Qeyri-qanuni surətlərin istifadəsi	Müəlliflərin razılığı olmadan nəşretmə	Giriş hüquqlarının kənar şəxslərə verilməsi
İnformasiyanın təcrid edilməsi (icazəli girişin rədd edilməsi)	Sıradan çıxarılması	İş rejiminin dəyişdirilməsi, sıradan çıxarılması	Pozulması, məhv edilməsi	İş prosesində səhv etmə, iş rejimini pozma

Sual 4. İnformasiya təhlükəsizliyinin təmin edilməsi üsulları və vasitələri

<u>İnformasiya təhlükəsizliyinin təmin edilməsi üsul və vasitələrinin təsnifatı.</u> Növündən və xarakterindən asılı olmadan baş verə biləcək istənilən təhlükələrin qarşısının alınması, başqa sözlə sistemdə toplanan, saxlanan və emal olunan, eləcə də şəbəkə vasitəsilə ötürülən informasiyanın təhlükəsizliyinin təmin olunması məqsədilə indiyədək çoxlu sayda müxtəlif üsullar, vasitələr və tədbirlər sistemi işlənib hazırlanmışdır.

İnformasiya təhlükəsizliyi problemi meydana çıxdığı ilk dövrlərdə informasiyanın qorunması üçün, əsasən, təşkilati və fiziki tədbirlər həyata keçirilirdi. Lakin informasiya texnologiyalarının, o cümlədən kompüter texnikasının və kommunikasiya avadanlıqlarının inkişafı informasiyanın qorunması məsələsinə daha ciddi və kompleks yanaşma zərurətini yaratdı.

İlk dövrlərdə elə fikir formalaşmışdır ki, informasiyanın emalı və ötürülməsi sistemlərində təhlükəsizlik proqram vasitələrinin köməyi ilə daha asan təmin edilə bilər. Ona görə də həmin dövrlərdə informasiyanın qorunması üçün məhz proqram vasitələri

daha çox inkişaf edirdi. Bu vasitələrin etibarlığını artırmaq məqsədilə onlar, əlavə olaraq, zəruri təşkilati tədbirlərin və fiziki qoruma mexanizmlərinin köməyi ilə möhkəmləndirilirdi.

Lakin təcrübə göstərdi ki, informasiyanın etibarlı qorunması üçün yalnız proqram vasitələrinin reallaşdırılması, hətta əlavə təşkilati tədbirlərin tətbiq edilməsi kifayət etmir.

Real həyatda praktiki baxımdan informasiya təhlükəsizliyinə qarşı elə təhlükələr yaranır ki, onların qarşısını almaq üçün bu vasitələrin tətbiqi mümkün olmur, bəzən isə bu mexanizmlər arzu olunan nəticəni vermir. Məhz bu səbəb informasiyanın qorunması üçün texniki qurğuların və sistemlərin, o cümlədən aparat vasitələrinin intensiv inkişafına təkan verdi.

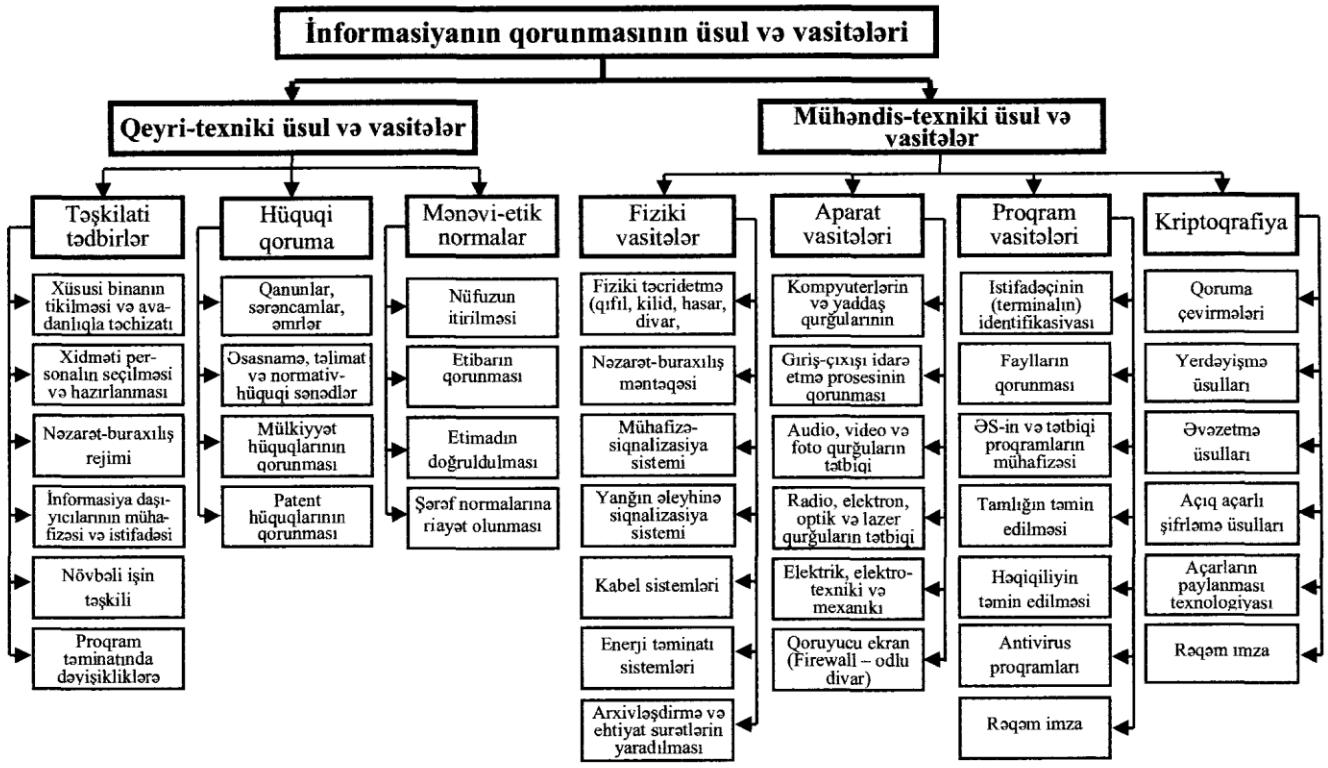
İnformasiya təhlükəsizliyi konsepsiyasının formalaşması prosesində tədricən aydın oldu ki, qoruma vasitələrinin kompleks şəkildə (proqram, texniki, təşkilati və s.) işlənib hazırlanması və tətbiqi daha da səmərəli olur, yalnız bu yolla arzu olunan nəticə əldə edilə bilər.

İnformasiya təhlükəsizliyinin təmin edilməsi üçün reallaşdırılan üsullar, vasitələr və tədbirlər, bir qayda olaraq, iki istiqamətdə inkişaf edir:

- qeyri-texniki qoruma vasitələri;
- mühəndis-texniki qoruma vasitələri.

İnformasiya təhlükəsizliyinin təmin edilməsi üsul və vasitələrinin təsnifatı sxematik olaraq 4.1 saylı şəkildə verilmişdir.

Qeyd etmək lazımdır ki, informasiyanın qorunması məsələsinə kompleks yanaşma texniki və qeyri-texniki vasitələrin birgə tətbiqini tələb edir. Məsələn, məlumatlara, proqramlara, sistemə və şəbəkəyə girişin nəzarət olunmasının yüksək səviyyədə işlənib hazırlanmış proqram vasitələri informasiya təhlükəsizliyinin etibarlığına zəmanət vermir. Belə ki, xidməti personalın səhlənkarlığı və ya təşkilatın əməkdaşlarının səriştəsizliyi nəticəsində parolların yayılmasına (onlar qəsdən yayıla bilər), beləliklə də məxfiliyin itməsinə gətirib çıxaran səhvlər yarana bilər.



Şək.4.1. İnformasiyanın qorunmasının üsulları, vasitələri və tədbirləri

İnformasiyanın qorunmasının qeyri-texniki vasitələri. Qeyri-texniki qoruma vasitələrini üç əsas hissəyə bölürlər:

- təşkilati qoruma tədbirləri;
- hüquqi qoruma tədbirləri;
- mənəvi-etik normalar.

Təşkilati qoruma tədbirləri. **Təşkilati tədbirlər** dedikdə məxfi informasiyanın hüquqazidd əldə olunmasını, daxili və xarici təhdidlərin meydana gəlməsini istisna etmək və ya əhəmiyyətli dərəcədə çətinləşdirmək məqsədilə təşkilatın və onun əməkdaşlarının fəaliyyətinin, eləcə də icraçıların qarşılıqlı münasibətlərinin normativ-hüquqi əsaslarla nizamlanması nəzərdə tutulur.

Təşkilati tədbirlər bütün struktur elementlərin mövcud olduğu və fəaliyyət göstərdiyi hər bir mərhələni (binanın tikintisi, sistemin layihələndirilməsi, struktur elementlərinin və avadanlıqlarının alınması, quraşdırılması, sazlanması, sınaqdan keçirilməsi və istismarı zamanı) əhatə edir.

Təşkilati tədbirlər sistemi, həmçinin istifadəçilərin və texniki personalın işinə nəzarət olunmasını, qorunan sistem və informasiya resursları ilə onların iş vaxtının məhdudlaşdırılmasını, proqram-texniki vasitələrdən istifadə reqlamentlərinin, eləcə də istifadəçilərin qorunan sistemə, sistemin yerləşdiyi binaya və ya otağa giriş hüquqlarının və sistemdə onlara verilən səlahiyyətlərin təyin edilməsini, nəzarət-buraxılış rejiminin həyata keçirilməsini, növbələrin planlaşdırılmasını və s. özündə ehtiva edir.

Təşkilati tədbirlərə, əsasən, aşağıdakıları aid etmək olar:

- *rejimin və mühafizənin təşkili – əraziyə, binaya və ya otağa kənar şəxslərin gizli daxil olması imkanlarını istisna edən, əməkdaşların və qonaqların daxil olmasının və hərəkətinin rahat nəzarətinin təmin edilməsi, müstəqil giriş sistemi olan ayrıca məxfi iş yerlərinin yaradılması, iş vaxtı və ərazidə olma rejiminə riayət edilməsinin nəzarətdə saxlanması, əməkdaşların və qonaqların etibarlı buraxılış rejiminin və nəzarətinin təşkili və saxlanılması və digər tədbirlərdən ibarətdir.*
- *xidməti personalla işin təşkili – personalın seçilməsi və yerləşdirilməsi, əməkdaşlarla tanış olma, onların öyrənilməsi, məxfi informasiya ilə iş qaydalarının öyrənilməsi, informasiya təhlükəsizliyi qaydalarının pozulmasına görə məsuliyyət tədbirləri ilə tanış olma və s. tədbirləri nəzərdə tutur.*
- *sənədlərlə və sənədləşdirilmiş informasiya ilə işin təşkili – məxfi informasiya olan sənədlərin və daşıyıcıların işlənib hazırlanması və istifadəsi, uçotu, icrası, qaytarılması, saxlanılması və məhv edilməsi işlərinin təşkili tədbirlərini əhatə edir.*
- məxfi informasiyanın yığılması, emalı, toplanması və saxlanmasında *texniki vasitələrdən istifadənin təşkili.*
- məxfi informasiyaya qarşı yönəlmiş mümkün *daxili və xarici təhdidlərin təhlili,* informasiyanın təhlükəsizliyinin təmin edilməsi üçün tədbirlərin işlənməsi üzrə işin təşkili;
- personalın məxfi informasiya ilə işinə, sənədlərin və informasiya daşıyıcılarının qeydiyyatı, saxlanılması və məhv edilməsi qaydalarına riayət olunmasına *sistemli nəzarətin aparılması üzrə işin təşkili.*
- Qeyd edilməlidir ki, informasiya təhlükəsizliyinin təmin edilməsində təşkilati tədbirlər əhəmiyyətli rol oynayır. Belə ki, məxfi informasiyaya icazəsiz giriş hallan çox vaxt texniki amillərlə deyil, istifadəçilərin və təhlükəsizlik personalının səhlənkarlığı, diqqətsizliyi və laqeydliyi ilə bağlı olur.

Bu baxımdan, təşkilati tədbirlər kompleksi KSŞ-nin yaradılması, onun proqram-texniki komponentlərinin, rabitə və telekommunikasiya avadanlıqlarının quraşdırılması və istismarı prosesində informasiyanın qorunması üçün həyata keçirilən təşkilati-texniki və təşkilati-hüquqi tədbirləri özündə birləşdirməlidir.

Hüquqi qoruma vasitələri. Daha ciddi rejimli təşkilatlarda zərurət yarandıqda qorunan informasiyanın saxlanılması, emalı və ötürülməsi üzrə müəyyən edilmiş qaydalara istifadəçilər və xidməti personal tərəfindən riayət olunmasını təmin etmək məqsədilə məcburi tədbirlər sistemi (bu, informasiya təhlükəsizliyi siyasətinin tərkibinə də daxil edilə bilər) işlənib hazırlanır və tətbiq edilir. Burada istifadəçilərin və xidməti personalın icazəsiz və qeyri-qanuni hərəkətlərinə görə maddi, inzibati və cinayət məsuliyyətinə cəlb olunması nəzərdə tutula bilər.

Qanunvericilik tədbirləri məhdud girişli informasiyanın istifadəsi, emalı, saxlanması və ötürülməsi qaydaların nizamlayan, eləcə də bu qaydalar pozulduqda məsuliyyət tədbirlərini nəzərdə tutan hüquqi aktlarla müəyyən edilir.

Qanunvericilik tədbirləri özündə dövlət orqanlarının, təşkilatların, əhalinin (ayrı-ayrı şəxslərin) həyat və fəaliyyətinin ayrı-ayrı sahələrinə münasibətdə dövlət tərəfindən müəyyən olunmuş və təsdiq edilmiş ümumi məcburi davranış qaydaları və normaları toplusunu, eləcə də bu normaların pozulduğu təqdirdə həyata keçirilən tədbirlər sistemini ehtiva edir.

İnformasiyanın qorunmasının hüquqi forması dedikdə, dövlətin konstitusiyasının və qanunlarının maddələrinin, mülki və cinayət məcəllələrinin müddəalarının, habelə informatika, informasiya münasibətləri və informasiyanın qorunması sahəsində digər normativ-hüquqi sənədlərə əsaslanan qoruma mexanizmlərinin tətbiqi başa düşülür.

İnformasiyanın qorunmasının hüquqi forması informasiya münasibətləri subyektlərinin hüquq və vəzifələrini, orqanların, texniki qurğuların və informasiyanın qorunması vasitələrinin hüquqi statusunu nizamlayır və informasiyanın qorunması sahəsində mənəvi-etik normaların yaradılması üçün baza təşkil edir.

Bir resurs kimi informasiyanın hüquqi qorunması beynəlxalq və dövlət səviyyəsində tanınan normativ-hüquqi sənədlərlə, dövlətlərarası müqavilələr, sazişlər, konvensiyalar, bəyannamələr ilə müəyyən olunur, patentlər, müəlliflik hüququ şəhadətnamələri və lisenziyalar şəklində reallaşdırılır.

Qeyd etmək lazımdır ki, Azərbaycan Respublikasında informasiyanın qorunması sahəsində bir çox qanunvericilik aktları qəbul edilmişdir. Belə ki, "Milli təhlükəsizlik haqqında", "İnformasiya, informasiyalaşdırma və informasiyanın qorunması haqqında", "Rəqəm imza və elektron sənəd haqqında", "Dövlət sirri haqqında" Azərbaycan Respublikasının Qanunlarında, eləcə də Azərbaycan Respublikasının Cinayət-Prosessual Məcəlləsində elektron sənəd dövriyyəsi zamanı informasiya təhlükəsizliyinin təmin edilməsi, şəxslərin və təşkilatların müəlliflik hüquqlarının qorunması, elektron informasiyanın imzalanması, informasiya resurslarının oğurlanmasına, məhv edilməsinə və açılmasına görə cəzasızlıq probleminin həlli və digər məsələlər nəzərdə tutulur.

Hüquqi nizamlama informasiya resurslarına qarşı hüquqazidd hərəkətlərin qarşısının alınması mexanizminin təkmilləşdirilməsi, bu sahədə ayrı-ayrı subyektlərin vəzifə, hüquq və səlahiyyətlərinin dəqiqləşdirilməsi və möhkəmləndirilməsi, vətəndaşların və təşkilatların hüquqlarının və qanuni maraqlarının qorunması üçün zəruridir.

Mənəvi-etik tədbirlər. *Mənəvi-etik tədbirlər* şəbəkə və informasiya texnologiyalarının yayılması və istifadəsi dövründə ənənəvi olaraq yaranmış və ya yaranmaqda olan davranış normalarından ibarətdir.

Mənəvi-etik təsirlər vasitəsilə təhlükəsizliyin təmin edilməsi istifadəçilər və xidməti personal, eləcə də ziyankarlar və bədniyyətli şəxslər tərəfindən ölkədə və cəmiyyətdə illərlə formalaşmış mənəvi-etik normalara riayət olunmasının təmin edilməsini nəzərdə tutur.

Bu normaların yerinə yetirilməsi qanunvericilik tədbirlərindən fərqli olaraq məcburi deyildir, lakin bu normaların pozulması nüfuzun, hörmətin, etibarın və s. itirilməsinə gətirib çıxarır.

İnformasiyanın qorunmasının mühəndis-texniki üsulları və vasitələri. Mühəndis-texniki qoruma vasitələri dedikdə, məxfi informasiyanın qorunması üçün istifadə olunan xüsusi orqanlar, texniki vasitələr və tədbirlər toplusu başa düşülür. Qorumanın məqsəd, vəzifə və obyektlərinin, eləcə də həyata keçirilən tədbirlərin müxtəlifliyi nəzərə alınaraq, onların müəyyən xarakteristikalara görə təsnif edilməsi məqsədəuyğun hesab olunur.

Funksional təyinatına görə mühəndis-texniki vasitələr aşağıdakı qruplara bölünür:

- fiziki vasitələr;
- aparat vasitələri;
- proqram vasitələri;
- kriptoqrafik vasitələr;
- steqanoqrafık vasitələr.

Fiziki qoruma vasitələri. Fiziki qoruma vasitələri informasiyanın, KSŞ-nin qorunmasının ilk sərhədini təşkil edir. Ona görə də belə sistemlərin, eləcə də onlara daxil olan qurğuların və texniki vasitələrin fıziki qorunması, mühafızəsi informasiya təhlükəsizliyinin təmin edilməsinin zəruri şərtlərindən biridir.

Hələ informasiyanın qorunması problemlərinin meydana gəlməsindən xeyli əvvəl fiziki qoruma vasitələrindən istifadə olunurdu. Belə ki, bu üsullar prinsip etibarı ilə bankların, muzeylərin, mağazaların, evlərin, həyətyanı sahələrin və s. qorunması üçün istifadə olunan köhnə ənənəvi vasitələrdən fərqlənmirlər. Lakin qeyd olunmalıdır ki, müasir dövrdə informasiyanın, eləcə də onun saxlandığı, dövr etdiyi, emal və istifadə olunduğu yerin (otaq və ya binanın) qorunması üçün daha mürəkkəb və mükəmməl vasitələrdən istifadə olunur.

Fiziki vasitələr qorunan informasiyanın saxlandığı yerə daxilolmanın məhdudlaşdırılması, qarşısının alınması, ona aparan yolda fiziki və psixoloji maneənin yaradılması üçün nəzərdə tutulur, müstəqil reallaşdırılır və ya digər informasiya qoruma vasitələri ilə birlikdə kompleks şəklində tətbiq olunurlar.

İnformasiyanın fiziki qorunmasını təmin etmək üçün hasarlar, divarlar, barmaqlıqlar, barılar, tikanlı məftillər çəkilir, ekranlar, seyflər və şkaflar quraşdırılır, kodlar, mexaniki, elektron və radio ilə idarə olunan kilidlərdən istifadə olunur, yanğına, oda və tüstüyə qarşı ötürücülər və s. tətbiq edilir.

Fiziki qoruma vasitələri, həmçinin akustik, fiksəedici, tele-video və fotoçəkmə, optik, lazer, mexaniki, elektron, elektron-mexaniki, elektrik qurğularından, yüksəktezlikli, radio və radiolokasiya texnologiyalarından istifadə etməklə reallaşdırılır. Onlar ayrı-ayrı qurğuların, avtomatlaşdırılmış sistemlərin texniki vasitələrinin və qurğular kompleksinin tərkibində, eləcə də müstəqil şəkildə ayrı-ayrı konstruksiyalar, qurğular və hissələr kimi reallaşdırıla və fəaliyyət göstərə bilərlər.

Ümumiyyətlə, informasiyanın fiziki qorunması vasitələri, əsasən, aşağıdakı məsələlərin həlli üçün tətbiq olunur:

- ərazinin mühafızəsi;
- daxili binaların və otaqların (kompüter və ya hesablama zallarının, serverlərin və digər kommunikasiya qurğularının yerləşdiyi otaqların, operatorların, proqramçıların, administratorların iş yerlərinin və s.) mühafizəsi, onların müşahidə olunması;
- avadanlıqların və daşınan informasiya daşıyıcılarının (maqnit və lazer disklərinin, disketlərin, fləş yaddaş qurğularının, çap vərəqlərinin və s.) mühafızəsi;
- qorunan zonalara girişin nəzarət edilməsi;
- kompüter sistemlərinin və şəbəkələrinin avadanlıq və qurğularından, eləcə də rabitə xətlərindən şüalanmaların və çarpaz kəsişmələrin neytrallaşdırılması;
- iş yerlərinin, monitorların, çap materiallarının və s. vizual müşahidəsinin qarşısının alınması;

- yanğından mühafızənin təşkili;
- bədəməl şəxslərin, o cümlədən oğruların, hakerlərin, kompüter cinayətkarlarının hüquqazidd və icazəsiz əməllərinin qarşısının alınması.

Funksional təyinatına görə fiziki qoruma vasitələrini üç kateqoriyaya ayırmaq olar:

- *hasarlama və fiziki təcridetmə sistemləri – obyektin, o cümlədən onun ərazisinin, bina və otaqlarının, ayrı-ayrı element və konstruksiyalarının qorunmasını təmin edir;*
- *kilidləmə qurğuları və saxlanclar – qorunan informasiyanın, eləcə də onun emal edildiyi sistemin yerləşdiyi yerin (otağın və ya binanın) mexaniki, elektromexaniki, elektron və s. qurğularla kilidlənməsini, müxtəlif şkafların, seyflərin və saxlancların istifadəsini nəzərdə tutur;*
- girişə nəzarət sistemləri – qorunan obyektlərə, o cümlədən sənədlərə, fayllara, informasiyaya, onların saxlanıldığı, emal edildiyi və ötürüldüyü sistemlərə və *şəbəkələrə girişə nəzarəti təmin edir.*

<u>İnformasiyanın qorunmasının aparat vasitələri.</u> Qorumanın aparat vasitələrinin məqsədi fəaliyyət sahəsində istifadə olunan texniki vasitələrlə məxfi informasiyanın yayılması və sızması, eləcə də ona icazəsiz girişin əldə olunması təhlükələrindən qorunmasıdır.

İnformasiyanın qorunmasının aparat vasitələri informasiya təhlükəsizliyinin təmin edilməsi vasitələri kimi KSŞ-də tətbiq olunan müasir kompüter texnikasının, texniki qurğuların və kommunikasiya vasitələrinin tərkibinə daxil edilir.

KSŞ-nin, o cümlədən təhlükəsizlik sisteminin komponentlərinə, eləcə də onların saxlandığı yerə kənar şəxslərin bilavasitə girişi və müdaxiləsi hallarının qarşısını almaq üçün tətbiq edilən müxtəlif təyinatlı mexaniki, elektrik, elektromexaniki, elektron, elektron-optiki, radio və radiolokasiya texnologiyalarına əsaslanan qurğular, sistemlər və avadanlıqlar və s. informasiyanın qorunmasının aparat vasitələrinə aid edilir.

Aparat vasitələri, bir qayda olaraq, aşağıdakı məsələlərin həll edilməsi üçün tətbiq olunur:

- informasiyanın sızmasının mümkün kanallarının aşkar edilməsi məqsədilə texniki vasitələrin xüsusi yoxlanmasının həyata keçirilməsi;
- müxtəlif obyektlərdə, otaqlarda və binalarda informasiyanın sızması kanallarının aşkarlanması;
- informasiyanın sızması kanallarının yerinin lokallaşdırılması;
- sənaye casusluğu vasitələrinin axtarılması və tapılması;
- məxfı informasiya mənbələrinə icazəsiz girişin və digər hüquqazidd və ziyankar hərəkətlərin qarşısının alınması.

Göstərilən məsələlərin tələb olunan səviyyədə həll edilməsi üçün audio, video müşahidələr və şəkilçəkmə, optik, lazer, yüksəktezlikli və radiolokasiya sistemlərinin, akustik və təsbitedici qurğular, identifikasiya kartları, fiziki əlamətlərə görə identifikasiya edən, ekranlaşdıran və səs-küy yaradan qurğular və digər texnik vəsaitlər tətbiq olunur.

Qeyd olunduğu kimi, onlar ayrı-ayrı qurğuların, avtomatlaşdırılmış sistemlərin texniki vasitələrinin, texniki qurğular kompleksinin tərkibi hissəsi kimi və ya təhlükəsizliyin təmin edilməsi funksiyalarını yerinə yetirmək imkanlarına malik olan müstəqil qurğular şəklində reallaşdırıla bilər.

Hazırda informasiya təhlükəsizliyinin təmin edilməsi məqsədilə praktikada çoxlu sayda aparat vasitələrindən istifadə olunur. Onlar, əsasən, aşağıdakı texnoloji elementlər şəklində reallaşdırılırlar:

- qorunma rekvizitlərinin (parolların, identifikasiya kodlarının, qriflərin və məxfilik dərəcəsinin və s.) saxlanılması üçün xüsusi registrlər;

- qurğuların qoşulması, informasiya resurslarına, sistemə və s. müraciət zamanı onların identifikasiya kodlarının avtomatik generasiyası üçün nəzərdə tutulmuş kod generatorları;
- sistemin texniki vasitələrinin işə salınması üçün kilidlərin istifadəsini təmin edən maqnit kartlarının oxunması üçün qurğular;
- insanların identifikasiyası və ya tanınması məqsədilə onların fərdi xüsusiyyətlərinin (səsinin, barmaq izlərinin, üz quruluşunun və s.) ölçülməsi qurğuları;
- informasiya daşıyıcılarının hissələrinə müraciətlərin qanuniliyinin müəyyən edilməsi məqsədilə onun ünvanlarının sərhədlərinə nəzarət edilməsi sxemi;
- informasiya daşıyıcılarının hissələrində saxlanılan informasiyanın məxfilik dərəcəsini müəyyən edən və bu hissələrə aid olan xüsusi məxfilik bitləri;
- məlumatların verilməsi ünvanlarının dövri yoxlanması məqsədilə rabitə xətti ilə informasiyanın ötürülməsi prosesinin kəsilməsi sxemi;
- cütlük xassəsinə görə informasiyanın yoxlanması sxemi;
- informasiyanın şifrlənməsi qurğuları;
- xüsusi kodlu "səs-küy" yaratma alqoritmlərini reallaşdıran qurğular.

Funksional təyinatına görə aparat vasitələrini aşağıdakı kimi təsnif etmək olar:
- aşkarlama və müəyyən etmə vasitələri;
- axtarış və dəqiq ölçmə vasitələri;
- fəal və passiv müqavimət vasitələri.

Texniki imkanlarına görə isə informasiyanın qorunmasının aparat vasitələrini iki qrupa bölmək olar:
- *ümumi təyinatlı vasitələr – ilkin qiymətləndirmə məqsədilə qeyri-peşəkarlar tərəfindən istifadə üçün nəzərdə tutulmuş vasitələrdir. Bu növ vasitələrə tətbiq siqnallarının geniş spektrinə və kifayət qədər kiçik həssaslığa malik olan elektromaqnit şüalanma indikatorlarını misal göstərmək olar.*
- *peşəkar komplekslər – sənaye casusluğu vasitələrinin mükəmməl axtarışmı, aşkarlanmasını və onların bütün xarakteristikalarının çox dəqiq ölçülməsini həyata keçirməyə imkan verən aparat vasitələridir. Radioötürücülərin, radiomikrofonların, telefon qoyuluşların və şəbəkə radioötürücülərinin avtomatik aşkarlanması və yerinin müəyyən edilməsi üçün nəzərdə tutulan aşkar etmə və pelenqləmə kompleksləri (məsələn, "Delta" kompleksi) belə vasitələrə nümunə ola bilər.*

İnformasiyanın sızması kanallarının axtarılması vasitələrini də iki yerə bölmək olar:
- informasiyanın çıxarılması (götürülməsi) vasitələrinin axtarılması avadanlıqları – bədəməllər tərəfindən artıq yeridilmiş icazəsiz giriş vasitələrinin axtarılması və lokallaşdırılmasını yerinə yetirir;
- informasiyanın sızması kanallarının tədqiq edilməsi avadanlıqları.

Qeyd olunduğu kimi, fiziki təbiətinə görə informasiyanın sızmasının çox müxtəlif kanalları, eləcə də əsasında informasiyaya icazəsiz giriş sistemləri reallaşdırılan fiziki qurğular mövcuddur. Ona görə də onların axtarılması və aşkarlanması məqsədilə çox müxtəlif və həddən artıq baha olan aparat vasitələrindən və avadanlıqlardan istifadə edilməsi tələb olunur. Adətən, belə avadanlıqlara bu sahədə ixtisaslaşan və daim müvafiq araşdırmalar aparan təşkilatlar (xüsusi dövlət qurumları, böyük təhlükəsizlik xidmətləri, ixtisaslaşmış firmalar və s.) malik olurlar.

İnformasiyanın qorunmasının aparat vasitələri KSŞ-nin, eləcə də telekommunikasiya sistemlərinin təhlükəsizliyinin təmin edilməsi üçün də geniş istifadə olunur. Belə vasitələr, əsasən, serverlərin, işçi stansiyaların, yaddaş qurğularının və informasiya daşıyıcılarının, terminalların, giriş-çıxış qurğularının, o cümlədən kompüterlərə və sistemə, onların saxlandığı yerə girişin təhlükəsizliyinin təmin edilməsi üçün istifadə olunur.

Aparat vasitələrinin serverlərdə və işçi stansiyalarda tətbiqi informasiya resurslarına istifadəçilərin girişinə nəzarət edilməsinə, kənar şəxslərin girişinin qarşısının alınmasına, kompüter texnikasının və digər qurğuların işində proqram-texniki səhvlərin aşkarlanmasına və qarşısının vaxtında alınmasına imkan verir.

Bundan əlavə, informasiya resurslarının, o cümlədən yaddaş qurğularının və informasiya daşıyıcılarının xarici və daxili təhlükələrdən qorunmasını təmin etmək məqsədilə də aparat vasitələrindən istifadə olunur.

Xarici təhlükəsizliyin təmin edilməsi məqsədilə aparat vasitələri ərazinin, binanın, otağın qorunması, istifadəçilərin müşahidəsinin və tanınmasının təşkili və s. üçün texniki imkanları özündə reallaşdırır. Bu vasitələr bəzən fiziki qoruma vasitələri kimi qəbul edilir. Burada daxili təhlükəsizlik dedikdə sistemin və şəbəkənin proqram-texniki kompleksi çərçivəsində informasiya təhlükəsizliyinin təmin edilməsi başa düşülür.

Aparat vasitələrinin inkişafına aşağıdakı amillər bilavasitə təsir edir:

- aparat vasitələrinin proqram vasitələrinə nisbətən sürətlə işləməsi;
- aparat vasitələrinin element bazasının intensiv və sürətlə inkişafı;
- aparat vasitələrinin və element bazasının qiymətinin (maya dəyərinin) ciddi aşağı düşməsi və s.

Aparat vasitələrinin qiymətinin digər təhlükəsizlik vasitələrinə nisbətən yüksək olması səbəbindən informasiya resurslarının təhlükəsizliyinin təmin edilməsi üçün yalnız bu növ vasitələrin tətbiqi məqsədəuyğun hesab olunmur.

Aparat vasitələrinin proqram vasitələri, fiziki mexanizmlər və təşkilati tədbirlərlə birgə tətbiqi avadanlıqların, texniki vasitələrin, informasiya resurslarının fiziki məhv olmadan, sıradan çıxmalardan, eləcə də icazəsiz və qeyri-qanuni girişlərdən və istifadədən daha etibarlı qorunmasını təmin etməyə imkan verir.

İnformasiyanın qorunmasının proqram vasitələri. İnformasiyanın qorunmasının *proqram vasitələri* informasiyanın emalı və ötürülməsi proqramlarının, şəbəkə əməliyyat sistemlərinin və şəbəkənin idarə olunması proqram təminatının tərkibində, eləcə də ayrı-ayrı proqramlar şəklində reallaşdırılır.

İnformasiyanın qorunmasının proqram vasitələri, həmçinin istifadəçilər tərəfindən müstəqil şəkildə özlərinin şəxsi informasiya resurslarının təhlükəsizliyinin təmin olunması üçün istifadə edilə bilər.

İnformasiyanın qorunması üçün istifadə edilən mexanizmlər arasında proqram vasitələri əhəmiyyətli yer tutur və qoruma üsullarının daha geniş yayılmış növü hesab olunur. Buna proqram vasitələrinin reallaşdırılmasının universallığı, sadəliyi, fiziki platformaya daha asan uzlaşması, dəyişikliklərin aparılması və inkişaf etdirilməsi üçün böyük imkanların olması, nisbətən ucuz qiymətə başa gəlməsi və s. kimi amillər müsbət təsir göstərir.

Ümumi halda, informasiyanın qorunmasının proqram vasitələrini aşağıdakı qruplara bölmək olar:

- ümumi proqram təminatlarında nəzərdə tutulan özünüqoruma vasitələri – proqram təminatlarının özlərinə məxsus olan, istehsalçılar tərəfindən işlənib hazırlanan, onun satışını müşayiət edən və qeyri-qanuni hərəkətlərin qarşısını alan qoruma mexanizmləridir.
- hesablama sistemlərinin tərkibində reallaşdırılan qoruma vasitələri – avadanlıqların, yaddaş qurğularının, şəbəkə və telekommunikasiya vasitələrinin, mülki qurğuların qorunması vasitələridir.
- informasiya sorğusu ilə qoruma vasitələri – informasiyanın qorunmasını həyata keçirmək üçün istifadəçilərin səlahiyyətlərinin identifikasiyası məqsədilə əlavə informasiyanın daxil edilməsini tələb edən qoruma vasitələridir.

- fəal qoruma vasitələri – müstəqil proqram şəklində reallaşdırılan və xüsusi vəziyyətlər yarandıqda işə düşən qoruma vasitələridir. Burada xüsusi vəziyyət dedikdə parolun düzgün daxil edilməməsi, proqram yüklənən zaman tarixin və vaxtın səhv göstərilməsi, icazə olmadan informasiyaya girişin əldə edilməsinə cəhd göstərilməsi və s. nəzərdə tutulur.
- passiv qoruma vasitələri – cinayətlərin açılmasına yardım etmək (onların açılmasının qaçılmazlığını göstərmək) məqsədilə ehtiyat və nəzarət tədbirlərinin görülməsinə, sübut və dəlil axtarışına yönələn qoruma mexanizmləridir.

İnformasiyanın qorunmasının proqram vasitələrinə antivirus proqramlarını, kriptoqrafik şifrləmə vasitələrini, girişin məhdudlaşdırılması sistemlərini, şəbəkələrarası ekranları, icazəsiz (qeyri-qanuni) daxilolmanın aşkarlanması sistemini və s. nümunə göstərmək olar.

Proqram vasitələri məxfi informasiyanın və proqram təminatının, əsasən, aşağıdakı təhlükələrdən qorunması üçün tətbiq edilir:

- informasiyanın, proqramın və sistemin icazəsiz girişdən qorunması;
- informasiyanın və proqramın köçürülmədən qorunması;
- informasiyanın, proqramın, sistemin və şəbəkənin viruslardan qorunması;
- rabitə kanallarının qorunması.

Praktikada informasiyanın bu və ya digər növ təhlükələrdən qorunması üçün müxtəlif növ proqram sistemləri reallaşdırılır və istifadə olunur. Bu sistemlər, bir qayda olaraq, aşağıdakı funksiyaları yerinə yetirirlər:

- texniki vasitələrin (terminalların, giriş-çıxışın idarə edilməsi qurğularının, kompüterlərin, informasiya daşıyıcılarının və s.), proqramların, proseslərin, istifadəçilərin, informasiya massivlərinin identifikasiyası;
- qorunan informasiya resurslarının emal olunduğu sistemlərdə və şəbəkələrdə texniki vasitələrin və istifadəçilərin işinin qeydiyyatının aparılması və onlara nəzarət edilməsi;
- istifadəçilərin, sistemlərin və şəbəkənin həqiqiliyinin təyin edilməsi, yəni audentifıkasiyası;
- rəqəm imza, yəni informasiyanın və onun müəllifının həqiqiliyinin təsdiq edilməsi;
- açarların paylanması və mübadiləsi;
- texniki vasitələrə qoyulan məhdudiyyətlərin (məsələlərin və informasiya resurslarının istifadəsinə icazə verilən iş günlərinin, vaxtlarının və s.) və istifadəçilərin hüquqlarının (hüquq və səlahiyyətlərinin) müəyyən edilməsi;
- əməliyyat sistemlərinin və istifadəçi proqramlarının qorunması;
- saxlanılan, emal olunan və ötürülən məlumatların qorunması;
- informasiyanın istifadəsi və emalı prosesi başa çatdıqdan sonra yaddaş qurğularından qalıqların təmizlənməsi və ya məhv edilməsi;
- icazəsiz əməliyyatlar aşkar olunduqda həyəcan siqnalının işə düşməsi, məsul operatorun və şəbəkə inzibatçısının xəbərdar edilməsi;
- qorunan məlumatlara bütün müraciətlərin, xüsusən də onlara icazəsiz giriş cəhdlərinin qeydiyyatının aparılması;
- informasiyanın kriptoqrafik şifrlənməsi və deşifrlənməsi, informasiyanın mənasının gizlədilməsi üçün kriptoqrafik alqoritmlərin tətbiqi;
- qoruma mexanizmlərinin işinə nəzarət edilməsi;

Qeyd olunduğu kimi, aparat və proqram vasitələrinin birgə reallaşdırılması daha səmərəli olur. Belə ki, aparat qoruma sistemlərinin əksəriyyəti, adətən, müvafıq proqram vasitələrinin reallaşdırılmasını və istifadəsini tələb edirlər. Ona görə də qoruma vasitələrinin inkişafında güclü qoruma imkanlarına malik proqram-aparat sistemlərinin kompleks inkişafı əsas yer tutur.

Kabel sistemlərinin qorunması. Kabel sistemi lokal kompüter şəbəkələri üçün informasiya təhlükəsizliyi baxımından əsas elementlərdən biridir. Belə ki, kompüter şəbəkələrində sıradan çıxma hallarının yarıdan çoxunun səbəbi kabel sistemləri ilə bağlı olur. Bununla əlaqədar olaraq, şəbəkələrin layihələndirilməsi mərhələsindən başlayaraq kabel sistemləri və onların qorunması mexanizmləri xüsusi ilə diqqətdə saxlanılmalıdır.

Kabel sisteminin düzgün quraşdırılmaması səbəbindən yaranan problemlərin aradan qaldırılmasının ən yaxşı yolu son vaxtlarda daha geniş yayılmağa başlayan strukturlaşdırılmış kabel sistemlərinin istifadə olunmasıdır. Strukturlaşdırılmış kabel sistemləri lokal kompüter şəbəkələrində, lokal telefon şəbəkələrində məlumatların ötürülməsi, habelə yanğın təhlükəsizliyi və mühafizə sistemlərində video məlumatların və ya digər siqnalların verilməsi üçün tətbiq edilir. Belə kabel sistemlərinə AT&T şirkətinin SYSTI-MAX SCS, Digital şirkətinin OPEN DEC connect, IBM şirkətinin kabel sistemini aid etmək olar.

Strukturlaşdırılmış kabel sistemlərinə əsasən binada qurulan kabel sistemlərinin onun komponentlərinin təyinatından və yerləşdiyi yerdən asılı olaraq, onların bir neçə səviyyəyə bölünməsi nəzərdə tutulur.

AT&T şirkəti kabel sisteminin aşağıdakı altsistemlər (səviyyələr) şəklində reallaşdırılmasını təklif edir:

- xarici kabelləşdirmə altsistemi (campus subsystem);
- aparat altsistemi (equipment room);
- idarəetmə altsistemi (administrative subsystem);
- magistral kabelləşdirmə altsistemi (backbone cabling);
- üfüqi kabelləşdirmə altsistemi (horizontal subsystem);
- iş yerlərinin kabelləşdirilməsi altsistemi (work location subsystem).

Xarici kabelləşdirmə altsistemi mis və ya optik kabeldən, elektrik qoruma və torpaqlama (torpağa birləşdirmə) qurğularından ibarət olub, binada (və ya bir neçə binada kompleks şəklində) olan kommunikasiya və emaletmə avadanlıqlarını birləşdirir. Bundan əlavə, bu altsistemə xarici kabel xətərinin daxili kabel xətləri ilə uzlaşmasını həyata keçirən qurğular daxil olur.

Aparat altsistemləri idarəetmə altsisteminin işini təmin etmək üçün nəzərdə tutulmuş müxtəlif kommunikasiya avadanlıqlarının yerləşdirilməsinə xidmət edir.

İdarəetmə altsistemi xidməti personalın və ya şöbələrin yerləşdirilməsi planında dəyişikliklər aparılan zaman kabel sisteminin tez və asan idarə olunması üçün nəzərdə tutulmuşdur. Onun tərkibinə daxili kabel altsistemi (ekranlaşdırılmamış burulmuş naqillər cütü və ya optik kabel), magistralın üfüqi altsistemlə kommutasiyası və uzlaşdırılması qurğuları, birləşdirici naqillər, təsbitedici vasitələr və s. daxil olur.

Magistral kabelləşdirmə altsistemi mis kabeldən və ya mis və optik kabellərin kombinasiyasından, eləcə də yardımçı avadanlıqlardan ibarət olur. O, binanın mərtəbələrinin və ya eyni mərtəbənin böyük sahələrini öz aralarında birləşdirir.

Üfüqi kabelləşdirmə altsistemi burulmuş mis məftil vasitəsilə əsas magistralın mərtəbənin administrasiya sisteminin giriş nöqtəsindən iş yerlərinə qədər çatdırılmasına xidmət edir.

Nəhayət, iş yerlərinin kabelləşdirilməsi altsistemi özündə birləşdirici naqilləri, adapterləri, uzlaşdırma qurğularmı birləşdirir. Bu altsistem iş yerlərində olan avadanlıqlarla üfüqi kabelləşdirmə altsistemi arasında mexaniki və elektrik birləşmələrini təmin edir.

Kabellərin fiziki (bəzən temperatur və ya kimyəvi təsirlərdən) qorunmasının ən yaxşı üsulu müxtəlif qoruma dərəcələrinə malik olan novlardan (qutulardan) istifadə olunmasıdır.

Elektromaqnit şüalanmaları olan mənbələrin yanından kompüter şəbəkəsi kabeli çəkilən zaman aşağıdakı tələblərin yerinə yetirilməsi nəzərə alınmalıdır:

- ekranlaşdırılmamış burulmuş naqillər cütü elektrik xəttindən, rozetkalardan, transformatorlardan və s. azı 15-30 sm. aralı olmalıdır;
- koaksil kabellər elektrik xətlərindən və cihazlarından azı 10-15 sm. aralı keçməlidir.

Bundan əlavə, kabel sisteminin düzgün quraşdırılması və kəsilməz fəaliyyət göstərməsini təmin etmək üçün onun bütün komponentlərinin qəbul olunmuş beynəlxalq standartların tələblərinə uyğun qurulması (quraşdırılması) və istismar edilməsi ən vacib məsələlərdən biridir.

Ehtiyat enerji təminatı (elektrik qidalanma) sistemləri. Elektrik enerjisinin qısamüddətli söndürülməsi zamanı informasiya itkisinin qarşısını almaq üçün daha etibarlı vasitə fasiləsiz qida mənbəyinin istifadəsidir. Özünün texniki və istehlakçı parametrlərinə görə müxtəlif olan müvafıq qurğular gərginliyin bərpa edilməsi və informasiyanın yaddaş qurğularında saxlanması üçün tələb olunan vaxt intervalında lokal şəbəkənin, ayrı-ayrı kompüterlərin və ya digər avadanlıqların qidalanmasını təmin edə bilər.

Fasiləsiz qidalanma mənbələrinin əksəriyyəti, həmçinin gərginliyin sabidəşdirilməsi funksiyasını da yerinə yetirir. Bu isə informasiyanın emalı, saxlanılması, ötürülməsi sistemlərinə daxil olan texniki vasitələrin, üsulların, o cümlədən qurğu və avadanlıqların, əlavə olaraq, elektrik şəbəkəsində gərginliyin sıçrayışlarından qorunmanı təmin edir. Bir çox mühüm şəbəkə qurğuları (serverlər, konsentratorlar, körpülər və s.) məxsusi olaraq təkrarlanan elektrik qidalanması sistemləri ilə təchiz olunurlar.

Adətən, böyük şirkətlər qəza hallan üçün nəzərdə tutulmuş xüsusi elektrik generatorları və ya ehtiyat elektrik xətti quraşdırırlar. Əsas və ehtiyat xətlər müxtəlif elektrik altstansiyalarına qoşulurlar və onlardan biri (əsas) sıradan çıxdıqda elektrik təminatı digər altstansiyanın (ehtiyat) xəttindən həyata keçirilir.

İnformasiyanın arxivləşdirilməsi və ehtiyat surətlərinin yaradılması sistemləri. Etibarlı və səmərəli arxivləşdirilmə sisteminin təşkili kompüter sistemlərində və şəbəkələrində informasiyanın qorunması, tamlığının, ona icazəli girişin təmin edilməsi və onun təcrid olunmasının qarşısının alınması üzrə ən vacib məsələlərdən biridir. Bir və ya iki server quraşdırılmış şəbəkələrdə arxivləşdirilmə sistemləri çox vaxt bilavasitə serverlərdə olan sərbəst slotlara quraşdırılır. Daha böyük korporativ şəbəkələrdə ayrıca xüsusiləşdirilmiş arxivləşdirmə serverinin təşkil olunması daha məqsədəuyğun hesab olunur.

Əlahiddə qiymətə malik olan arxiv informasiyasının saxlanması xüsusi qorunan otaqda təşkil olunmalıdır. Mütəxəssislər yanğın və ya digər təbii fəlakətlərin baş verməsinin mümkünlüyünü nəzərə alaraq, daha qiymətli məlumatların arxivlərinin ikinci surətinin başqa binada saxlanmasını tövsiyə edirlər.

İnformasiyanın kompüter viruslarından qorunması. Kompüter viruslarının sistemə və ya şəbəkəyə daxil olması və yayılması, eləcə də onun sahiblərinə maddi və mənəvi ziyan vura bilməsi təhlükələrinin ciddiliyini nəzərə alaraq, KSŞ-nin, eləcə də onlarda olan informasiya resurslarının kompüter viruslarının hücumundan qorunması üçün daim zəruri tədbirlərin görülməsi, xüsusi proqram təminatlarının (antivirusların) işlənib hazırlanması, tətbiq olunması və nəzarətdə saxlanması zəruridir. Bu problem istifadəçilər və şəbəkə inzibatçıları tərəfindən daim diqqət mərkəzində saxlanmalıdır.

Kompüter viruslarının aşkarlanmasının yeganə vasitəsi sistemin fəaliyyətini dayandırmadan fasiləsiz şəkildə antivirus profılaktikasının həyata keçirilməsindən və onların qarşısının alınması üçün antivirus proqramların istifadəsindən ibarətdir.

Antivirus proqramları iş prosesində kompüterin yaddaşını, sistemdə olan proqramları, istifadə olunan faylları, emal edilən informasiya resurslarmı və s. yoxlayır və

nəzarətdə saxlayır. Daim yeni-yeni kompüter viruslarının yaranması, onların təbiətinin əvvəlcədən məlum olmaması səbəbindən universal qabaqlayıcı antivirus proqramlarının yaradılmasının qeyri-mümkünlüyü, sistemin viruslardan qoruma səviyyəsinin qiymətləndirilməsi metodikasının olmaması və s. amillər kompüter virusları probleminin aktuallığının yüksək olduğunu göstərir.

Kompüter viruslarına qarşı mübarizə aparmaq və onlardan qorunmaq üçün istifadə olunan antivirus proqramlarını funksional təyinatına görə üç kateqoriyaya ayırmaq olar:

- *filtrləyici antivirus proqramları – kompüterdə yerinə yetirilən bütün proqramları "süzgəcdən" keçirir, virusların sistemə keçməsinə mane olur;*
- *yoluxmaya qarşı antivirus proqramları – sistemin fəaliyyətini daim nəzarətdə saxlayır, kompüterin və proqramların virusa yoluxmasının qarşısını alır;*
- *virusları müalicə edən antivirus proqramları – sistemə və proqramlara yoluxmuş ayrı-ayrı virusları aşkarlayır və "müalicə" edir.*

Qeyd olunmalıdır ki, antivirus proqramlarının inkişafı, adətən, virus proqramlarının yaranması və yayılması sürətindən geri qalır. Belə ki, mövcud antivirus proqramları məlum olan virusların sistemdə yayılmasının qarşısını ala, onları məhv edə və proqramları bu viruslardan təmizləyə bilir. Lakin tamamilə yeni yaranmış virusu tanımaq və onun qarşısını almaq üçün yeni antivirus proqramının yaradılması və ya mövcud antivirus proqramında yeni virus haqqında məlumatın nəzərə alınması tələb olunur.

Müasir antivirus proqramlarının funksiyalarına aşağıdakılar aid edilir:

- *müəyyən edilmiş vaxtlarda yaddaşın və disklərin məzmununun yoxlanması;*
- *rezident modulların köməyi ilə real vaxt rejimində kompüterin əməli yaddaşının, eləcə də yazılan və oxunan faylların yoxlanılması;*
- *atributları (ölçüsü, dəyişdirilmə tarixi, nəzarət cəmi və s.) dəyişmiş olan fayların seçim yolu ilə yoxlanılması;*
- *arxiv faylların yoxlanılması;*
- *kompüter virusları üçün xarakterik olan davramşların tanınması (müəyyən edilməsi);*
- *sistem inzibatçısının kompüterindən uzaq məsafədən antivirus proqramlarının quraşdırılması, sazlanması və idarə edilməsi;*
- *virus hücumları ilə bağlı hadisələr haqqında elektron poçtu, peycer və digər yollarla şəbəkə inzibatçısına xəbər verilməsi;*
- *korporativ şəbəkəyə qoşulan kompüterlərin məcburi yoxlanması;*
- *antivirus proqram təminatının və viruslar haqqında məlumat bazasının uzaq məsafədən yeniləşdirilməsi, eləcə də viruslar üzrə məlumat bazalarının İnternet vasitəsilə təzələnməsi;*
- *SMTP, FTP, HTTP və s. protokollar vasitəsilə ötürülən və ya alınan fayllarda, o cümlədən proqramlarda, sənədlərdə və s. mümkün virusların aşkarlanması məqsədilə İnternet trafikin süzgəcdən keçirilməsi;*
- *potensial təhlükəli Java-apletlərin və ActiveX modulların aşkarlanması;*
- *müxtəlif server və müştəri platformalarında, eləcə də korporativ şəbəkələrdə fəaliyyət göstərilməsi;*
- *antivirus qorunması üzrə hadisələr barədə məlumatları özündə saxlayan protokolların (jurnalların) aparılması.*

Qeyd etmək lazımdır ki, kompüter viruslarının hücumlarından qorunmaq üçün ən yaxşı vasitə ona yoluxmanın qarşısının alınmasıdır. Viruslara yoluxmanın qarşısının alınması üçün aşağıdakı tövsiyələri diqqət mərkəzində saxlamaq lazımdır:

- *antivirus proqram təminatmı istehsalçılar tərəfindən müəyyən edilmiş şəkildə quraşdırmalı;*
- *yalnız lisenziyalaşdırılmış proqram təminatından istifadə etməli;*

- *istifadəçinin sistemdə quraşdıra biləcəyi proqramların (IRC, ICQ, Chat və s.) sayını minimuma endirməli;*
- *istifadə olunan proqram təminatında məlum zəif yerləri aradan qaldırmalı;*
- *disketlərin, CD, DVD və digər informasiya daşıyıcılarının istifadəsinə nəzarət etməli, kənardan bu daşıyıcılar vasitəsilə hər hansı informasiya gətirildikdə istifadə etməzdən qabaq antivirus proqramları vasitəsilə onları yoxlamalı;*
- *elektron poçtu vasitəsilə daxil olmuş müəllifi bəlli olmayan, eləcə də müəllifi tanış olan əlavə sənəd, fayl və ya proqram qoşulmuş məktubları antivirus proqramı ilə yoxlamadan açmamalı;*
- *sənədlərin emalım həyata keçirən proqram əlavələrinin təhlükəsizliyi siyasətini işləyib hazırlamalı.*

Hazırda bir çox məşhur antivirus proqramları geniş yayılmışdır və kompüter istifadəçiləri tərəfindən müvəffəqiyyətlə istifadə olunur. Bunlara Symantec AntiVirus, Norton AntiVirus, DrWeb, Kasperski AVP, ADinf, Aids-test və s. nümunə göstərmək olar.

Bütün antiviruslar mövcud viruslar haqqında məlumatları özündə saxlayan bazaya malik olurlar. Viruslar peyda olduqca, onlar haqqında məlumatlar da həmin bazalara daxil edilir. Bu baxımdan hər bir antivirus proqramını kompüterdə və ya kompüter şəbəkəsində quraşdırarkən mövcud viruslar haqqında onun ən son bazasını əldə etmək lazımdır. Belə ki, yeni viruslar barədə məlumat bazada olmasa, onda antivirus proqramları həmin virusları zərərsizləşdirə bilməz. Əksər antivirus proqramları öz bazalarını İnternet vasitəsilə avtomatik olaraq yeniləşdirirlər.

Sual 5. İnformasiyanin qorunmasinin kriptoqrafik üsullari

Kriptologiya, kriptoqrafiya, kriptoanaliz. Yuxarıda qeyd olunduğu kimi, informasiya təhlükəsizliyinin əsas istiqamətləri olan informasiyanın gizliliyinin, tamlığının təmin olunması və xidmət göstərməkdən imtina edilməsi hallarının qarşısının alınması üçün müxtəlif üsul və vasitələrdən istifadə olunur və zəruri tədbirlər görülür. Lakin bütün bunlara baxmayaraq, sistemdə mümkün boşluqlardan, buraxılan səhvlərdən istifadə edən hakerlər, rəqiblər, bədniyyətli şəxslər bəzən informasiyaya giriş əldə edə bilirlər.

Bu halda məxfi informasiyanın məzmununun kənar şəxslər tərəfindən oxunmasının qarşısını almaq üçün atılan ciddi addımlardan biri də informasiyanın mənasının və məzmunun gizlədilməsi, yəni şifrlənməsi üsullarının tətbiqindən ibarətdir. İnformasiyanın şifrlənməsi rəqib (bədniyyətli şəxs) qarşısında daha ciddi bir maneənin (səddin) yaradılmasını təmin edir.

İnformasiyanı şifrləmək və icazəsi olmayan şəxslər tərəfindən onun istifadəsinin qarşısını almaq yolu ilə informasiyanın gizliliyinin təmin edilməsi məsələləri ilə kriptologiya elmi məşğul olur.

Kriptologiya – informasiyanın çevrilməsi və başqa şəklə salınması (şifrlənməsi) yolu ilə informasiyanın qorunması, eləcə də onların açılması üsullarını öyrənən elmdir. Kriptologiya bir elm kimi iki istiqamətə bölünür: kriptoqrafiya və kriptoanaliz.

Kriptoqrafiya – məlumatların məzmununu gizlətmək, icazəsiz istifadəsinin və ya gizli dəyişdirilməsinin qarşısını almaq məqsədilə onların çevrilməsi prinsiplərini, üsul və vasitələrini öyrənən elm sahəsidir. Kriptoqrafiya dedikdə istənilən formada olan, o cümlədən disk qurğularında saxlanılan və ya kompüterdə emal olunan, eləcə də rabitə kanalları vasitəsilə ötürülən informasiyanın məzmununun gizlədilməsi üsulları məcmusu başa düşülür.

Kriptoanaliz şifrləmə açarını bilmədən informasiyanın məxfiliyinin açılması və audentikliyinin (əsli ilə eyniliyinin) pozulması üçün reallaşdırılan riyazi üsulları özündə ehtiva edir. Kriptoanaliz məxfi xarakterli informasiyanın əldə olunması (çıxarılması) məqsədilə şifrlənmiş mətnin açılması üçün kriptoqrafık sistemin, şifrləmə alqoritminin, onun açarının və s. təhlilinə əsaslanan, kriptoqrafiyaya qarşı yönələn elm sahəsidir.

Kriptoanalizdə əsas pozucu şəxs rolunu kriptoanalitik oynayır. *Kriptoanalitik (pozucu)* dedikdə, kriptoqrafik üsulların köməyi ilə qorunan məlumatların açılması, oxunması və ya saxtalaşdırılması məqsədi güdən şəxs və ya şəxslər qrupu başa düşülür.

Kriptoanalizdə fəaliyyətin həyata keçirilməsi baxımından pozucuya münasibətdə bir sıra fərziyyələr qəbul edilir:

- pozucu şifrləmə alqoritmini və onun reallaşdırılması xüsusiyyətlərini bilir, lakin gizli açarı bilmir.
- pozucunun bütün şifrlənmiş mətnlərə girişi vardır və o, şifr mətnləri bəlli olan bəzi ilkin mətnləri əldə etmək imkanına malikdir.
- pozucu özünü kriptoanaliz nəticəsində əldə olunacaq informasiyanın potensial qiymətliliyi ilə doğruldan hesablama, kadr, zaman və digər resurslara malikdir.

Bu fərziyyələr, bir qayda olaraq, riyazi və digər modellərin əsasını təşkil edir.

Kriptoanalitik üsullarının köməyi ilə şifrlənmiş mətnin açılması və ya saxtalaşdırılması və açarın hesablanması cəhdləri *kriptoqrafik hücum* və ya *şifrə hücum* adlanır. Əgər kriptoqrafık hücum uğurla başa çatarsa, onda ona *sındırma (şifrin sındırılması)* deyilir.

Şifrin naməlum açara görə açılmaya davamlılığım müəyyən edən xarakteristikasını *kriptoqrafik davamlılıq* adlandırırlar. *Kriptoqrafik davamlılıq* – istənilən kriptoqrafik sistemin başlıca parametridir.

Kriptoqrafik davamlılığın əsas göstəriciləri kimi aşağıdakıları göstərmək olar:

- bütün mümkün açarların sayı və ya verilmiş müddət ərzində verilmiş resurslarla açarın seçilməsi ehtimalı;
- verilmiş ehtimalla verilmiş resurslarla şifrin sındırılması üçün zəruri olan əməliyyatların sayı və vaxt;
- açarın və ya ilkin mətnin hesablanmasının qiyməti.

Bütün bu göstəricilər mümkün kriptoqrafik hücumun səviyyəsini nəzərə almalıdır. Lakin qeyd olunmalıdır ki, informasiyanın kriptoqrafık üsulların köməyi ilə qorunmasının effektivliyi yalnız şifrin kriptoqrafik davamlılığından asılı olmur. O, həmçinin, bir çox digər amillərdən, məsələn, kriptoqrafik sistemin qurğu və ya proqram şəklində reallaşdırılmasından asılıdır.

Kriptoqrafık sistemin davamlılığı təhlil olunarkən eyni zamanda insan amili də nəzərə alınmalıdır. Belə ki, zəruri informasiyaya girişi olan əməkdaşı ələ almaq şifrin sındırılması üçün superkompüterin yaradılmasından dəfələrlə ucuz başa gələ bilər.

Müasir kriptoanaliz ehtimallar nəzəriyyəsi, riyazi statistika, cəbr, ədədlər nəzəriyyəsi, alqoritmlər nəzəriyyəsi və digər riyazi elmlərə əsaslanır. Bundan irəli gələrək kriptoanalizin bütün üsullarını dörd əsas istiqamətə bölmək olar:

- statistik kriptoanaliz – ilkin və şifrlənmiş məlumatların statistik qanunauyğunluqlarının öyrənilməsi əsasında kriptoqrafik sistemlərin sındırılması imkanlarını tədqiq edir;
- cəbri kriptoanaliz – riyazi baxımdan kriptoqrafik alqoritmlərin zəif halqalarının axtarışı ilə məşğul olur;
- diferensial (fərqi) kriptoanaliz – şifrlənmiş mətnin dəyişməsinin ilkin mətnin dəyişməsindən asılılığının təhlilinə əsaslanan üsullardır;
- xətti kriptoanaliz – ilkin və şifrlənmiş mətnlər arasında xətti aproksimasiyanın tədqiqinə əsaslanan üsullardır.

Kriptoqrafik sistemlərin sındırılması təcrübəsinin tədqiqi göstərir ki, açarların seçilməsi (yoxlanması) bu istiqamətdə başlıca üsul olaraq qalır. Eyni zamanda, qeyd olunmalıdır ki, kriptoqrafik sistemlərin reallaşdırılması zamanı yol verilən diqqətsizlik (laqeydlik) amili onların sındırılmasında böyük rol oynayır.

Kriptoanalitikin əlində olan informasiyanın həcmindən və növündən asılı olaraq, kriptoqrafik hücumların üç səviyyəsini qeyd etmək olar:

- səviyyə KA1: şifrlənmiş mətnə görə hücum – kriptoanalitikə bütün və ya bəzi şifrlənmiş mətnlər məlumdur;
- səviyyə KA2: "ilkin mətn – şifrlənmiş mətn" cütlüyünə görə hücum – kriptoanalitikə bütün və ya bəzi şifrlənmiş mətnlə və onlara uyğun ilkin mətnlər məlumdur;
- səviyyə KA3: seçilmiş "ilkin mətn – şifrlənmiş mətn" cütlüyünə görə hücum – kriptoanalitikə ilkin mətni seçmək, ona uyğun şifrlənmiş mətni əldə etmək və onlar arasındakı asılılığın təhlili əsasında açarı hesablamaq imkanına malikdir.

Qeyd olunmalıdır ki, bütün müasir kriptoqrafık sistemlər kifayət qədər, hətta KA3 səviyyəli hücumlara (pozucu şifrləyici qurğunu əldə edərsə) qarşı davamlılığa malikdirlər.

İnformasiyanın məzmununu çevirməklə kənar şəxslərdən qorunmasını təmin edən kriptologiya elmi ilə yanaşı, informasiyanın varlığı, saxlanılması, emal olunması və ötürülməsi faktının gizlədilməsi yolu ilə qorunması məsələləri ilə steqanoqrafiya elmi məşğul olur. Steqanoqrafiya tarixən daha qədim dövrlərdən mövcud olmuşdur və bu gün də inkişaf etməkdədir.

Steqanoqrafiyanın məqsədi məlumatı olmayan şəxslərdən informasiyanın mövcudluğu faktının özünün gizlədilməsindən ibarətdir. Məsələn, hər hansı məxfı informasiya şəkil, audio və ya video fayllara daxil edilərək onların tərkibində, eləcə də disklərin adi qurğular tərəfindən istifadə olunmayan sektorlarında gizlədilə bilər. Belə məlumatlar faylların adını, parolu və ya diskdə yazıldığı yeri bilməyən istənilən şəxs üçün görünməz olur.

Kriptoqrafik sistemlərin yaradılması və tətbiqinin zəruriliyi informasiyanın saxlanılması və mübadiləsinin həyata keçirildiyi şəraitdən irəli gəlir. Belə ki, müasir informasiya sistemlərindən istifadə edən kollektivlərdə çox vaxt informasiya mübadiləsinin həyata keçirilməsi zərurəti yaranır. Bir qayda olaraq, müəyyən obyektiv və ya subyektiv səbəblərdən belə kollektivlərin üzvləri bir-birlərinə etibar etmir və ya ehtiyatlanırlar. Məsələn, müqavilələrin və ya digər sənədlərin imzalanması, maliyyə əməliyyatlarının aparılması, qərarların birgə qəbul edilməsi və s. hallarda mübadilə və ya saxlanılma prosesində informasiyanın təhrif edilməyəcəyinə və tamamilə dəyişdirilməyəcəyinə zəmanət verən vasitələr tələb olunur. Məhz belə məqamlarda kriptoqrafik sistemlərin tətbiqi etibarlı zəmanət rolunu oynaya bilər.

Kritoqrafik sistemlərin inkişaf tarixi. Cəmiyyətdə yazının meydana gəlməsi və yayılması yazılı məlumatların və məktubların mübadiləsinə tələbat yaratdı ki, bu da onların məzmununun kənar şəxslərdən gizlədilməsi zərurətini doğurdu. Məhz bu səbəbdən kriptoqrafiyanın tarixi insanların yazı tarixi ilə yaşıd hesab olunur.

Kriptoqrafiyanın inkişaf tarixini dörd əsas mərhələyə bölmək olar:

- sadə kriptoqrafiya;
- formal kriptoqrafiya;
- elmi kriptoqrafiya;
- kompüter kriptoqrafiyası.

Sadə kriptoqrafiya XIV əsrə qədərki dövrü əhatə edir və gizlədilən mətnlərin məzmununun rəqibin başa düşməməsi üçün istənilən sadə, primitiv üsul və vasitələrin istifadəsini nəzərdə tutur. Bu mərhələdə informasiyanın qorunması üçün kodlaşdırma və steqanoqrafik üsullarından istifadə olunurdu.

Həmin dövrün əksər şifrləmə üsulları yerdəyişmə və ya əvəzetmə prinsiplərinə əsaslanırdı. İlk belə şifrlərdən biri Sezar şifridir. Bu şifrdə ilkin mətnin hər bir hərfi əlifbada sıraca ondan müəyyən olunmuş sayda sonrakı mövqedə duran hərflə əvəz olunurdu.

Qədim dövrə aid şifrləmə üsullarından biri də yunan yazıçısı Polibiyə məxsusdur. Onun şifr çox əlifbalı əvəzetmə prinsipinə əsaslanır. Belə ki, yunan əlifbası əvvəlcədə 5x5 ölçülü kvadrat cədvələ yazılır, soma isə ilkin mətnin hər bir hərfı bu kvadratda tapılır və ondan aşağıdakı sətirdə (eyni sütunda) yerləşən hərflə əvəz olunur.

15-ci əsrin sonundan 20-ci əsrin əvvəlinə qədərki dövrü əhatə edən *formal kriptoqrafiya* formallaşdırılmış və nisbətən davamlı şifrləmə üsullarının yaranması ilə xarakterizə olunur. Bu dövrdə yaranan şifrlərə Vijiner, Trisemus, Pleyfer və s. üsullar göstərmək olar.

Bununla yanaşı, həmin dövrdə şifrləmənin avtomatlaşdırılması (mexaniki vasitələrin köməyi ilə) istiqamətində müəyyən addımlar atılmışdır. Belə ki, əsasını rotor sistemləri təşkil edən mexaniki maşınlar, o cümlədən T.Cefersonun maşını (ABŞ), E.Xebernin Enigma maşını (Almaniya), Sigaba (ABŞ), Typex (Böyük Britaniya), Red Orange və Purple (Yaponiya) işlənib hazırlanmış və istifadə olunmuşdur.

Formal kriptoqrafiyanın ən yüksək nailiyyəti olan rotor sistemləri çox davamlı şifrləri reallaşdırmağa imkan vermişdi. Bu şifrlərə hücumlar, onların sındırılması yalnız elektron hesablama maşınları meydana gəldikdən soma ötən əsrin 40-cı illərində mümkün olmuşdur.

Elmi kriptoqrafiya kriptodavamlılıq baxımında ciddi riyazi təminata malik kriptoqrafik sistemlərin yaranması ilə bağlıdır. O, təxminən 20-ci əsrin 30-60-cı illərini əhatə edir. Belə ki, 30-cu illərin əvvəllərinə riyaziyyatın kriptoqrafiyanın elmi əsaslarını təşkil edən bölmələri formalaşmışdır. Bura, riyazi statistikam, ümumi cəbri, ehtimallar və ədədlər nəzəriyyələrini və s. aid etmək olar. Bununla yanaşı, həmin dövrdə alqoritmlər nəzəriyyəsi, informasiya nəzəriyyəsi, kibernetika elmi inkişaf etməyə başlamışdı.

Ötən əsrin 40-cı illərində K.Şennon "Məxfı sistemlərdə rabitə nəzəriyyəsi" əsərində informasiyanın kriptoqrafik qorunmasının nəzəri əsaslarını formalaşdırdı, "səpələnmə" və "qarışdırma" anlayışlarını daxil edərək istənilən qədər davamlı kriptoqrafik sistemlərin yaradılmasının mümkünlüyünü əsaslandırdı.

60-cı illərdə rotorla şifrləməyə nisbətən daha davamlı blokla şifrləmə üsullarının yaradılmasının əsası qoyuldu. Lakin bu üsulların yalnız rəqəmli elektron qurğular şəklində reallaşdırılması mümkün idi.

Kompüter kriptoqafiyası ötən əsrin 70-ci illərindən sonrakı dövrü əhatə edir və hesablama sistemlərinin, o cümlədən kompüter texnikasının yaranması ilə formalaşmışdır. Kompüter kriptoqrafiyası "əllə" və ya mexaniki şifrləmə üsullarına nisbətən dəfələrlə yüksək kriptoqrafik davamlılığı və sürəti təmin edir.

O dövrdə DES – Amerika şifrləmə standartı (1978-ci il), SSRİ-nin dövlət şifrləmə standarti ГОСТ 28147-89 (hazırda Rusiya Federasiyasında standart kimi istifadə edilir) işlənib hazırlanmışdır. 70-ci illərin ortalarında ənənəvi kriptoqrafik şifrləmə üsullarında köklü surətdə fərqlənən yeni istiqamətin – asimmetrik kriptoqrafik sistemlərin yaranması bu sahədə çox böyük imkanlar yaratdı. Ənənəvi (simmetrik – bir açarlı) üsullardan istifadə zamanı şifr mətnlə yanaşı şifrləmə açarının ötürülməsi lazım gəlirdisə, asimmetrik (iki açarlı) şifrləmə üsulları isə şifrləmə açarının ötürülməsini tələb etmirdi.

Asimmetrik kriptosistemlərin elmi əsası ilk olaraq U.Diffı və M.Helman tərəfından 1976-cı ildə çap olunan "Müasir kriptoqrafıyanın yeni istiqamətləri" əsərində verilmişdi. Bundan bir qədər sonra R.Rivest, A.Şamir və L.Adleman praktikada ilk asimmetrik kritoqrafik sistemi – böyük sadə ədədlərin hasilinə əsaslanan RSA sistemini işləyib hazırlamışlar.

Asimmetrik kriptoqrafiya bu gün böyük əhəmiyyət kəsb edən elektron rəqəm imza texnologiyasının əsasını təşkil edir.

Kriptoqrafik sistemlər və onlara qoyulan tələblər. Qeyd olunduğu kimi, kriptoqrafık üsullar informasiyanın şifrlənməsi alqoritmlərinin köməyi ilə informasiyanın gizliliyini təmin etməyə, məzmununu kənar şəxslərdən gizlətməyə, göndərilən informasiyanı elektron imza vasitəsilə imzalamağa, onun həqiqiliyini təsdiq etməyə, istifadəçinin və serverin həqiqiliyini müəyyənləşdirməyə və digər audentifikasiya

proseduralarını yerinə yetirməyə, eləcə də açarların paylanması protokollarını reallaşdırmağa imkan verir.

Kriptoqrafik sistem – şifrləmə və ya şifrin açılması üsullarını reallaşdıran və birgə tətbiq edilən sənədlər, qurğular, avadanlıqlar və müvafiq üsullar kompleksidir. Başqa sözlə, kriptoqrafik sistemlər informasiyanın kriptoqrafik çevrilməsini və açarların paylanması prosesinin idarə olunmasını təmin edən proqram-texniki üsullar, vasitələr və təşkilati tədbirlər kompleksinin reallaşdırılmasını nəzərdə tutur.

Kriptoqrafik şifrləmə üsulları, bir qayda olaraq, informasiyanın saxlanılması, emalı və ötürülməsi zamanı onun təhlükəsizliyinin təmin edilməsi üçün tətbiq olunur. Rabitə kanalları ilə ötürmə zamanı informasiyanın qorunması üçün kriptoqrafık şifrləmə üsulları yeganə etibarlı vasitə hesab olunur. Kriptoqrafiya, həmçinin, proqram təminatının qorunması üçün də tətbiq oluna bilər.

Burada *gizlilik (məxfilik)* dedikdə əlavə məlumat (açar) olmadan informasiyanın dəyişdirilmiş (çevrilmiş) massivdən (şifr mətndən) alınmasının qeyri-mümkünlüyü xassəsi başa düşülür.

İnformasiyanın autentikliyi dedikdə onun həqiqiliyi və tamlığı, eləcə də müəllifinin həqiqiliyi başa düşülür.

Qeyd olunmalıdır ki, son zamanlar kriptoqrafık qorunma üsulları və vasitələri digər qoruma mexanizmlərinə nisbətən daha sürətlə inkişaf edir və geniş tətbiq olunur. Bunu aşağıdakı səbəblərlə izah etmək olar:

- qorunan informasiyanın kriptoqrafik şifrlənməsi daha universal vasitədir;
- informasiyanın kriptoqrafik şifrlənməsi üsullarının və alqoritmlərinin reallaşdırılması vasitələrinin işlənib hazırlanması sahəsində son dövrlərdə sürətli inkişaf baş vermiş və böyük nailiyyətlər əldə olunmuşdur;
- müasir avtomatlaşdırılmış informasiya sistemlərində kriptoqrafik şifrləmə üsullarının praktiki reallaşdırılması əhəmiyyətli çətinlikləri dəf etməyə imkan verir.

Kütləvi istifadə üçün nəzərdə tutulmuş kriptoqrafik sistemlərə, o cümlədən şifrləmə alqoritmlərinə bir sıra tələblər qoyulur:

- şifr mətn yalnız şifrləmə açarı olduqda oxuna bilər;
- şifr mətnin fraqmentinə və ona uyğun açıq mətnə görə istifadə olunmuş şifrləmə açarının müəyyən edilməsi üçün zəruri olan əməliyyatların sayı mümkün açarların ümumi sayından kiçik olmamalıdır;
- şifrləmiş açarının cüzi dəyişdirilməsi şifr mətnin şəklinin əhəmiyyətli dəyişməsinə gətirib çıxarmalıdır;
- açıq mətnin cüzi dəyişməsi hətta eyni bir açar istifadə olunduqda belə şifr mətnin şəklinin əhəmiyyətli dəyişməsinə gətirib çıxarmalıdır;
- şifrlənmə alqoritminin məlum olması qorunmanın etibarlığına mənfi təsir etməməlidir;
- şifrlənmə alqoritminin struktur elementləri dəyişilməz qalmalıdır;
- şifrləmə prosesində istifadə olunmuş məlumatlar və şifrləmə açarı daim nəzarətdə saxlanmalıdır;
- şifrləmə prosesində mətnə daxil edilən əlavə bitlər şifr mətndə tam və etibarlı şəkildə gizlənməlidir;
- şifrlənmiş mətnin uzunluğu açıq mətnin uzunluğundan böyük olmamalıdır;
- şifrləmə prosesində ardıcıl istifadə olunan açarlar arasında sadə və asan müəyyən edilən əlaqələr olmamalıdır;
- mümkün açarlar çoxluğundan götürülmüş istənilən açar şifrlənmiş informasiyanın qorunmasını etibarlı təmin etməlidir;

- kriptoqrafik alqoritmin proqram və ya aparat təminatı şəklində reallaşdırılması mümkün olmalıdır, bu zaman açarın uzunluğunun dəyişdirilməsi alqoritmin xarakteristikalarının pisləşməsinə gətirib çıxarmalıdır.

Kriptoqrafık sistemlərin davamlılığı üç aspektdən qiymətləndirilir.

- nəzəri davamlılıq;
- praktiki davamlılıq;
- mükəmməl davamlılıq.

Kriptoanalitik ələ keçirilmiş kriptoqramın təhlili üçün kifayət qədər vaxta və bütün zəruri vasitələrə malik olduqda kriptoqrafık sistemin etibarlılıq dərəcəsini göstərən davamlılıq qabiliyyəti *nəzəri davamlılıq* adlanır. Nəzəri davamlılıq məsələsinə baxış kriptoqrafik qoruma dərəcəsinə aydınlıq gətirir, lakin pessimist nəticəni nümayiş etdirir. Belə ki, nəzəri cəhətdən davamlı şifrin qurulması üçün tələb olunan açarın ölçüsü əksər sahələrdə tətbiqi çox mürəkkəb olan, hətta mümkün olmayacaq dərəcədə böyükdür.

Kriptoanalitik ələ keçirilmiş kriptoqramın təhlili üçün məhdud vaxta və hesablama imkanlarına malik olduqda kriptoqrafik sistemin etibarlılıq dərəcəsi *praktiki davamlılıq* adlanır.

Mükəmməl davamlılıq dedikdə bütün mümkün açıq mətnlər və kriptoqramlar üçün onlar arasında statistik asılılığın olmaması başa düşülür. Başqa sözlə, mükəmməl davamlılıq təmin edildikdə, kriptoanalitik zaman və hesablama imkanlarından asılı olmayaraq, naməlum kriptoqrama görə açıq mətnin hesablanması göstəriciləri ilə müqayisədə məlum kriptoqrama görə açıq mətnin hesablanması göstəricilərini yaxşılaşdırmaq mümkün olmur.

NƏTİCƏ

Kütləvi kompüterləşmə, ən yeni informasiya texnologiyalarının tətbiqi və inkişafı təhsil, biznes, sənaye istehsalı və elmi tədqiqatlar sahəsində irəliyə doğru hiss olunan sıçrayışa gətirib çıxarmışdır. Elmi-texniki inqilab informasiya cəmiyyətinin yaranmasına səbəb olmuşdur. Bu cəmiyyətdə informasiya ən mühüm resurs və başlıca amil olmuşdur. Müasir cəmiyyət tədricən öz informasiya infrastrukturunun vəziyyətindən müəyyən asılılıq qazanır. XXI əsrdə vətəndaşların, cəmiyyətin və dövlətin həyatında informasiyanın, informasiya resurslarının və texnologiyalarının rolunun artması milli təhlükəsizliyin təmin olunması sistemində informasiya təhlükəsizliyi məsələlərini ön plana çıxarır.

Elmi texniki tərəqqinin inkişafı artdıqca şəxsiyyətin, cəmiyyətin, dövlətin informasiya təhlükəsizliyi artmaqdadır və onun təhlükəsizliyi dövlət siyasətində müvafiq yeri tutmalıdır. İnformasiya irimiqyaslı qəzalara, hərbi konfliktlərə, dövlət idarəçiliyi, maliyyə sistemi və elmi mərkəzlərin fəaliyyətinin pozulmasına səbəb ola bilən faktora çevrilmişdir. Cəmiyyətin informasiyalaşdırılması və intellektuallaşdırılması səviyyəsinin artması onun informasiya təhlükəsizliyini daha etibarlı edir.

Müasir dövrdə bəşəriyyət, kütləvi şəkildə informasiya-kommunikasiya texnologiyalarının (İKT) istifadəsinə əsaslanan informasiya cəmiyyətinə keçid dövrünü yaşamaqdadır. İnformasiya texnologiyaları cəmiyyətin inkişafına təsir göstərən əsas amillərdən birinə çevrilmişdir. Onlar dövlət strukturlarını və vətəndaş cəmiyyəti institutlarını, iqtisadi və sosial sahələri, elm və təhsili, mədəniyyəti və bütövlükdə insanların həyat tərzini əhatə etməklə cəmiyyətin informasiyalaşdırmasına, ölkənin inkişafına, demokratik cəmiyyət quruculuğuna, beynəlxalq aləmə inteqrasiya olunmasına xidmət edir.

Cəmiyyət tədricən öz informasiya infrastrukturunun vəziyyətindən müəyyən asılılıq vəziyyətinə düşür. Hazırda informasiya milli strateji resurs olub, dövlətin ən əsas sərvətlərindən biri hesab edilir. İnformasiyalaşdırmanın təsiri altında cəmiyyətin bütün sahələri çeviklik və dinamiklik kimi yeni keyfiyyətlər almaqdadır. Müasir dövrdə dövlətin milli təhlükəsizliyi informasiya təhlükəsizliyinin təmin edilməsindən əhəmiyyətli dərəcədə asılıdır.

İnformasiya münasibətlərində olan subyektlərin, o cümlədən informasiya sahibləri və onun istifadəçilərinin səlahiyyətində olan informasiyanın və onun infrastrukturunun təbii və süni xarakterli, təsadüfi və ya qəsdli təsirlərdən mühafizəsi məqsədilə həyata keçirilən informasiya təhlükəsizliyi informasiya mühitində şəxsiyyətin, cəmiyyətin və dövlətin balanslaşdırılmış maraqları ilə təyin edilən milli maraqların mühafizəsini, informasiya sistemində saxlanan və emal edilən informasiyanın toxunulmazlığını təmin edir.

Bu gün təhlükəsizliyin təmin edilməsi bütövlükdə bəşəriyyətin ən əsas və qlobal problemlərindən biridir. Adi həyatda təhlükəsizlik anlayışı özündə normal (təhlükəsiz) yaşayış, iş, məişət, istirahət şəraitinin təmin olunmasını ehtiva edir. Bütövlükdə isə təhlükəsizlik - havanın təmizliyi, ərzağın və suyun keyfiyyəti, mənzil şəraiti, kriminala və terrorçuluğa qarşı effektiv mübarizə, nəqliyyatda, küçədə və ictimai yerlərdə təhlükəsizlik, tibbi təminatın və sosial müdafiənin səviyyəsi, xidmət sahələrində mənəvi-etik mühitin yaradılması, əmək haqqının sərf edilən əməyə uyğunluğu və s. ilə xarakterizə olunur.