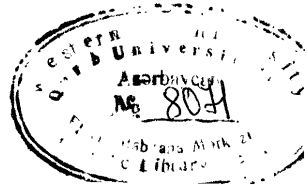
VAQİF QASIMOV

İnformasiya təhlükəsizliyinin əsasları

Dərslik

Azərbaycan Respublikası Milli Təhlükəsizlik Nazirliyinin Heydər Əliyev adına Akademiyasının Elmi Şurasının 29 aprel 2009-cu il tarixli iclasının qərarı ilə (protokol №15) nəşrə tövsiyə edilmişdir.

BAKI-2009



Elmi redaktor: **AMEA-nın həqiqi üzvü, t.e.d., prof. Ə.M.Abbasov**

Rəy verənlər: **AMEA-nın müxbir üzvü, t.e.d., prof. S.Q.Kərimov**

t.e.d., prof. Ə.Ə.Əliyev

Qasımov V.Ə. İnformasiya təhlükəsizliyinin əsasları. Dərslik. Bakı: MTN Maddi-texniki Təminat Baş İdarəsinin Nəşriyyat-Poliqrafiya Mərkəzi. 2009, 340 s.

Texnika elmləri doktoru Vaqif Qasımovun «İnformasiya təhlükəsizliyinin əsasları» kitabında informasiya təhlükəsizliyinin konseptual və formal modelləri, baza prinsipləri və əsas müddəaları, kompyuter sistemlərində və şəbəkələrində mümkün təhlükələr, onların qarşısının alınması üsulları və vasitələri, o cümlədən kriptoqrafik və steqanoqrafik üsullar, elektron imza texnologiyası, eləcə də informasiya təhlükəsizliyinin təmin edilməsinə kompleks yanaşma və informasiya təhlükəsizliyi sistemlərinin yaradılması prinsipləri ətraflı şərh olunmuşdur.

Dərslik Milli Təhlükəsizlik Nazirliyinin Heydər Əliyev adına Akademiyasının kursant və dinləyiciləri, habelə nazirliyin əməkdaşları üçün nəzərdə tutulmuşdur. Dərslikdən respublikanın digər ali təhsil müəssisələrinin tələbələri və müəllimləri, eləcə də bu sahədə çalışan elmi işçilər və mütəxəssislər də istifadə edə bilərlər.

ISBN 978-9952-443-50-9

MÜNDƏRİCAT

Müəllifdən

İlk öncə, elmə və təhsilə göstərdikləri xüsusi qayğıya, yaratdıqları gözəl və münbit şəraitə, eləcə də müasir informasiya-kommunikasiya texnologiyalarının öyrənilməsi və gündəlik praktiki fəaliyyətdə tətbiqinə verdikləri böyük diqqətə görə Azərbaycan Respublikasının milli təhlükəsizlik naziri general-leytenant cənab Eldar Mahmudova və MTN-in Heydər Əliyev adına Akademiyasının rəisi general-leytenant Ziya Yusifzadəyə öz dərin minnətdarlığımı bildirirəm.

Həmçinin verdikləri faydalı məsləhət və tövsiyələrə, sərf etdikləri vaxta və əməyə görə kitabın elmi redaktoru Azərbaycan Respublikasının rabitə və informasiya texnologiyaları naziri, akademik, texnika elmləri doktoru, professor Əli Abbasova, kitabın rəyçiləri Azərbaycan Dövlət Neft Akademiyasının «Kompyuter texnologiyaları və proqramlaşdırma» kafedrasının müdiri, AMEA-nın müxbir üzvü, texnika elmləri doktoru, professor Sabit Kərimova və Bakı Dövlət Universitetinin «İnformasiya texnologiyaları və proqramlaşdırma» kafedrasının müdiri, texnika elmləri doktoru, professor Ələkbər Əliyevə, eləcə də kitabın ərsəyə gəlməsində rolu olmuş bütün şəxslərə dərin təşəkkürümü bildirirəm.

Müasir dövrdə informasiya-kommunikasiya texnologiyalarının sürətli inkişafı və müxtəlif fəaliyyət sahələrində geniş tətbiqi nəzərə alınaraq, Milli Təhlükəsizlik Nazirliyinin Heydər Əliyev adına Akademiyasında informasiya təhlükəsizliyi problemlərinin öyrənilməsinə və tədrisinə böyük yer ayrılır. İnformasiya təhlükəsizliyi

sahəsində kadr hazırlığını təmin etmək məqsədilə Akademiyada "İnformasiya təhlükəsizliyi" fakültəsinin yaradılması və 2009-2010-cu tədris ilində fəaliyyətə başlaması özündə bu problemə verilən xüsusi diqqəti təcəssüm etdirir.

Təqdim olunan "İnformasiya təhlükəsizliyinin əsasları" dərsliyi nazirliyin və Akademiyanın rəhbərliyi tərəfindən qarşımızda qoyulmuş vəzifələrin icrası istiqamətində atılan növbəti addımdır. Düşünürəm ki, dərslik Akademiyanın kursant və dinləyiciləri, bu sahədə calışan elmi işçilər və mütəxəssislər, eləcə də informasiya təhlükəsizliyi problemi ilə maraqlanan hər bir şəxs üçün faydalı olacaqdır.

GİRİŞ

İnformasiya texnologiyaları sahəsində elmi-texniki tərəqqi nəticəsində milli dövlət sərhədləri informasiya resurslarının axını, telekommunikasiya sistemlərinin və qlobal kompyuter 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 kompyuterlərin, coğrafi cəhətdən paylanmış kompyuter 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 kompyuter sistemlərinin və şəbəkələrinin, ələlxüsus fərdi kompyuterlərin 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 aparmaq, 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 kompyuterlərin, kompyuter sistemlərinin və şəbəkələrinin işinə qeyri-qanuni müdaxilə, kompyuter informasiyasının oğurlanması, mənimsənilməsi, zorla, şantaj yolu ilə alınması kimi təhlükəli yeni sosial təzahürləri aid etmək olar. Bu təhlükələri çox vaxt "kompyuter cinayətkarlığı" və ya "kompyuter 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 kompyuter 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 tanış 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 160-dan artıq ölkəsini əhatə edir. 1998-ci ildə İnternet şəbəkəsinə, təxminən, 143 milyon istifadəçi qoşulmuşdusa, 2002-ci ildə onların sayı 700 milyonu ötüb keçmişdir. Hazırda İnternet istifadəçilərinin sayı ABŞ-da 158, Avropada – 95, Asiyada – 90, Latın Amerikasında – 14, Afrikada – 3, Rusiyada – 8, Ukraynada isə 1 milyondan çoxdur. Azərbaycanda İnternet şəbəkəsinin xidmətlərindən istifadə edənlərin sayı yüz minlərlə ölçülür.

Aydındır ki, İnternet şəbəkəsi istifadəçi qismində onun xidmətlərindən istifadə edə biləcək hər bir şəxsə, o cümlədən hakerə, cinayətkara və terrorçuya da öz cinayətkar niyyətlərini həyata keçirmək üçün tamamilə eyni imkanlar yaradır. Bu gün telekommunikasiya sistemləri və kompyuter şəbəkələri, o cümlədən İnternet şəbəkəsi siyasətçilər, iş adamları, dini təşkilatlar, terrorçu qruplar, cinayətkar qruplaşmalar, habelə rəqib (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 kompyuter viruslarıdır. Təbii viruslara analoji olaraq, müxtəlif xarakterli funksiyalara malik olan kompyuter virusları proqramların tərkibinə, yaddaş qurğularına, fayllara gizlicə əlavə olunaraq (yazılaraq) yayılırlar. Sonradan öz-özünə digər proqramlara, fayllara və s. ötürülən kompyuter 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, kompyuter sistemləri üçün əsas təhlükəni ziyankar (bədəməl) rolunu oynayan və informasiya texnologiyaları sahəsində peşəkar mütəxəssis olan şəxslər – hakerlər təşkil edirlər. Belə ki, onlar kompyuter 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) kompyuter cinayətkarlığının və kiberterrorçuluğun meydana gəlməsi kontekstində xüsusilə kəskin şəkildə ortaya çıxır.

Qeyd olunanlar nəzərə alınaraq, dərslik informasiya təhlükəsizliyi problemlərinə həsr olunmuşdur. Dərslikdə informasiya təhlükəsizliyinin əsas konseptual məsələləri, müddəaları, baza prinsipləri və modeli, kompyuter sistemlərində və şəbəkələrində informasiya təhlükəsizliyi məsələsi şərh olunmuş, informasiya təhlükəsizliyinin pozulması təhlükələri, onların qarşısının alınmasının üsulları və vasitələri təsvir və təsnif edilmişdir.

Dərslikdə, həmçinin informasiyanın qorunmasının kriptoqrafik üsulları, elektron imza texnologiyası və steqanoqrafiya barədə ətraflı məlumat verilmişdir. İnformasiya təhlükəsizliyinin təmin edilməsinə kompleks yanaşma, informasiya təhlükəsizliyi konsepsiyası, strategiyası və siyasətinin qurulması məsələlərinə baxılmış, təklif olunan informasiya təhlükəsizliyi sisteminin təxmini strukturu təsvir edilmişdir.

I FƏSİL

İNFORMASİYA TƏHLÜKƏSİZLİYİNİN ƏSAS KONSEPTUAL MƏSƏLƏLƏRİ

Milli təhlükəsizlik və onun təmin edilməsində informasiya təhlükəsizliyinin rolu və yeri

İnformasiya təhlükəsizliyi sahəsində əsas anlayışlar

İnformasiya təhlükəsizliyinin konseptual modeli

İnformasiya təhlükəsizliyinin əsas istiqamətləri və baza prinsipləri

1.1. Milli təhlükəsizlik və onun təmin edilməsində informasiya təhlükəsizliyinin rolu və yeri

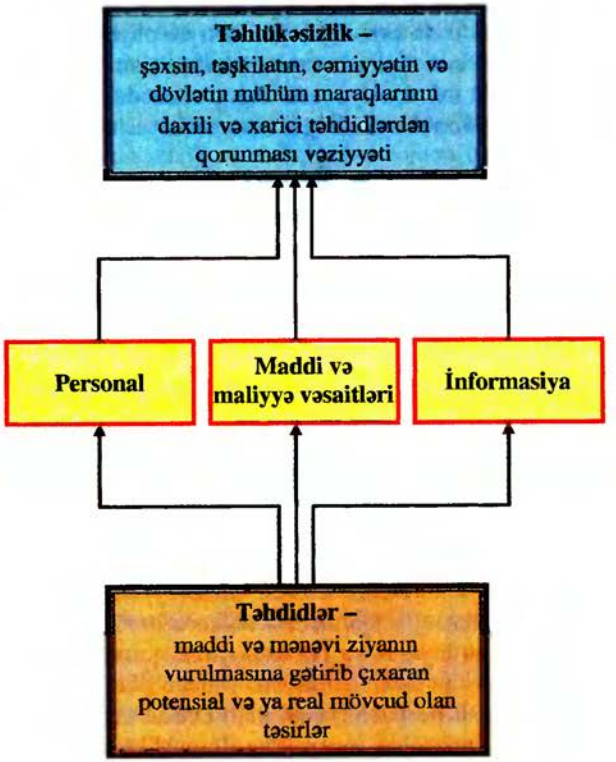
Bu gün təhlükəsizliyin təmin edilməsi bütövlükdə bəşəriyyətin ən əsas və qlobal problemlərindən biridir. Adi həyatda təhlükəsizlik anlayışı özündə normal (təhlükəsiz) yaşayış, iş, məişət, istirahət şəraitinin təmin olunmasını ehtiva edir. Bütövlükdə isə *təhlükəsizlik* – havanın təmizliyi, ərzağın və 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, əməkhaqqının 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 təhlükəsizlik aşağıdakı komponentlərlə xarakterizə olunur (şək.1.1):

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



Şək.1.1. Təhlükəsizliyin komponentləri

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.

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 maraqları 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 maraqları 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 informa-

siya 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;
- kompyuter 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. Konsepsi-

yanın 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 ehtiyatları insanın, cəmiyyətin və dövlətin inkişafının həlledici amillərindən birinə çevrilmişdir. İKT-nin, o cümlədən kompyuter 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 ehtiyatlarını, 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.

İnformasiya təhlükəsizliyi, informasiya təhlükəsi, informasiya təhdidləri, informasiyanın qorunması, informasiya maraqları, 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 əsasını 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.

1.2. İnformasiya təhlükəsizliyi sahəsində əsas anlayışlar

İnformasiya təhlükəsizliyi probleminin daha ətraflı şərhinə keçməzdən əvvəl, informasiya cəmiyyətinin əsasını 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 kompyuterə 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 təriflər verilir. Ona görə də burada bəzi anlayışların bir neçə tərifi verilmişdir. Konteksdən asılı olaraq bu təriflərdən 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 tərifinə də rast gəlinir.

İnformasiya təhlükəsizliyi – informasiyanın emalı, saxlanılması və ötürülməsi zamanı məxfilik, 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.

İnformasiyanın qorunmasının məqsədləri aşağıdakılardan ibarətdir:

- dövlətin, ictimaiyyətin, vətəndaşların təhlükəsizliyinin təmin edilməsi;
- dövlət sirri təşkil edən və məxfi informasiyanın məxfiliyinin 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.

İnformasiya 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, təsadüfi 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.

İnformasiya 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 (kompyuter

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 kompyuter 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 tanışolma;
- 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 ehtiyatları 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 kompyuter 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 resurslarını, 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.

İnformasiya 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 kompyuter 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.

1.3. İnformasiya təhlükəsizliyinin konseptual modeli

İnformasiya təhlükəsizliyi sahəsində vəziyyətin təhlili göstərir ki, informasiyanın qorunması üzrə artıq formalaşmış konsepsiya və yanaşma mövcuddur. Onun əsasını 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 (şək.1.2):

- təhlükəyə məruz qala biləcək obyektlər;

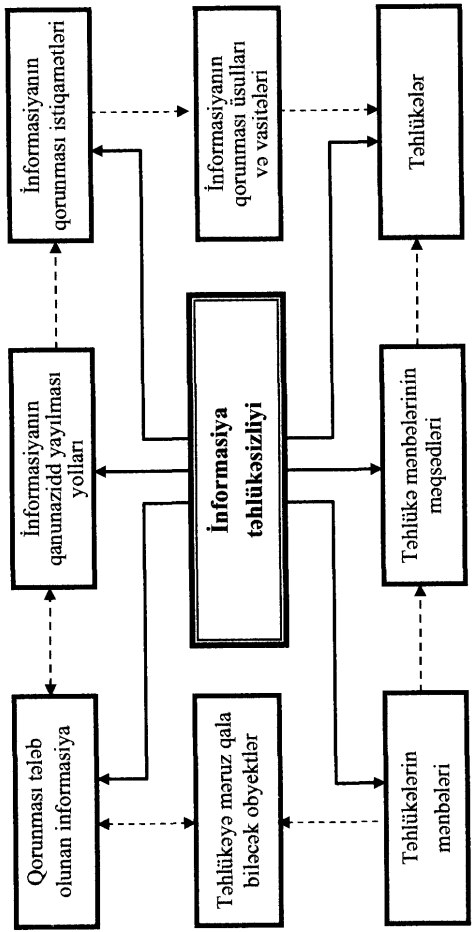
- qorunması tələb olunan informasiya;
- təhlükələr;
- təhlükələrin mənbələri;
- təhlükələrin mənbələrinin məqsədləri;
- qorunan informasiyanın qanunazidd şəkildə yayılması (sızması) yolları;
- informasiya təhlükəsizliyinin təmin edilməsinin istiqamətləri;
- informasiyanın qorunması üsulları və vasitələri.

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.



Şək.1.2. İnformasiya təhlükəsizliyinin konseptual modeli

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 imkanlarını, 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:

- qanunvericilik;
- təşkilati tədbirlər;
- mühəndis-texniki vasitələr;
- mənəvi-etik normalar.

İnformasiyanın qorunmasının əsas vasitələrinə fiziki qurğular, aparat vasitələri, proqram təminatları və kriptoqrafik üsullar aid edilir. Qeyd edilməlidir ki, kriptoqrafik 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.

1.4. 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. Kompyuter 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 kompyuter 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.

İnformasiyanın 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 resurslarının 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 kompyuter 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 kompyuterlərdə və kompyuter 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, kompyuter 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 kompyuter 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 kompyuterlər) və məntiqi (məlumat bazaları, tətbiqi proqramlar, əməliyyat sistemləri) baxımdan informasiyanın qorunması məsələləri də aiddir.

II FƏSİL

KOMPYUTER SİSTEMLƏRİNDƏ VƏ ŞƏBƏKƏLƏRİNDƏ İNFORMASİYA TƏHLÜKƏSİZLİYİ

İnformasiya təhlükəsizliyi baxımından kompyuter sistemlərinin və şəbəkələrinin xüsusiyyətləri

Kompyuter sistemlərində və şəbəkələrində informasiyanın qorunmasının xüsusiyyətləri

Kompyuter sistemlərində və şəbəkələrində zəif yerlər və informasiyanın sızması yolları

İnformasiya təhlükəsizliyinin təmin edilməsinin əsas aspektləri

İnformasiya təhlükəsizliyinin təmin edilməsi üçün həyata keçirilən tədbirlər sistemi

2.1. İnformasiya təhlükəsizliyi baxımından kompyuter sistemlərinin və şəbəkələrinin xüsusiyyətləri

Şirkətlər, nazirlik və komitələr səviyyəsində qurulan və bu təşkilatlar çərçivəsində informasiyanın emalı, saxlanılması və ötürülməsini həyata keçirən kompyuter sistemlərində və şəbəkələrində (KSŞ) informasiyanın qorunması məsələsi bu gün çox aktualdır. Belə ki, dövlət və hökumət orqanlarında, eləcə də özəl şirkətlərdə yaradılmış kompyuter 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 kompyuter 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 kompyuterləri) – istifadəçilərin (abonentlərin, operatorların) avtomatlaşdırılmış iş yerlərinin reallaşdırıldığı ayrı-ayrı kompyuterlər və ya uzaq məsafədə yerləşən terminallardan ibarət olub, bir otaq və ya bina daxilində cəmləşə, eləcə də böyük ərazidə və ya birbirindən uzaq məsafədə qeyri-məhdud şəkildə paylana bilər;
- *funksional serverlər* – KSŞ-də böyük həcmdə məlumatların toplanması, saxlanılması, emal edilməsi, isti-

fadəçilərə müxtəlif xidmətlərin göstərilməsi funksiyalarını reallaşdıran, böyük yaddaşa və sürətə malik olan kompyuterlərdir;

- *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 İnternet, 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, kompyuter texnikasının, telekommunikasiya vasitələrinin və rabitə kanallarının, eləcə də proqram təminatının spektri genişdir;
- kompyuter sistemlərinin və şəbəkələrinin komponentləri coğrafi 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 kompyuter 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 kompyuter texnikası, telekommunikasiya qurğuları, əməliyyat sistemləri, ofis və tətbiqi proqramlar, məlumat bazaları və digər informasiya resursları hücum obyekti ola və təhlükəyə məruz qala bilərlər.

2.2. Kompyuter sistemlərində və şəbəkələrində informasiyanın qorunmasının xüsusiyyətləri

Kompyuterlərin, 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 kompyuter 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 müvafiq təhlil aparılmadan informasiyanın qorunması sistemlərini layihələndirmək, müvafiq 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 kompyuter 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 kompyuterlər (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, spesifik 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 təşkilatları, 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, kompyuter 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, kompyuter texnikası, informasiya emalı vəsaitləri, proqram təminatı və ondan istifadə mexanizmləri inkişaf etdikcə kompyuter sistemlərində informasiyanın ələ keçməsi imkanları daha da artır. Ümumiyyətlə, demək olar ki, kompyuter şəbəkələrində informasiyanın qorunması probleminin aktuallığı daim yüksəlir.

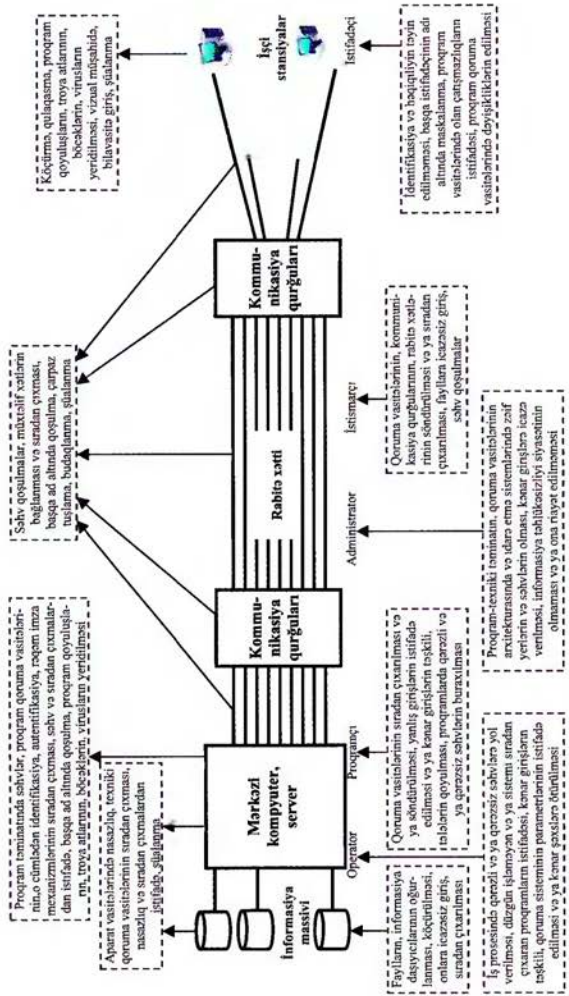
2.3. Kompyuter sistemlərində və şəbəkələrində zəif yerlər və informasiyanın sızması yolları

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

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

Əvvəlki fəsillərdə qeyd olunduğu kimi, müxtəlif kompyuterləri, telekommunikasiya qurğularını, rabitə kanallarını, informasiyanın saxlanması, emalı və ötürülməsi vasitələrini özündə birləşdirən kompyuter 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 kompyuter 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, məlumat-



Şək.2.1. KSŞ-də informasiyanın sızması yolları

ların 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) kompyuterlərdə (işçi stansiyalarda) işləyən zaman məhz bu növ məlumatlar monitora və ya çap qurğularına (printerlərə) çıxarılır.

Bu baxımdan belə kompyuterlər 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 kompyuter sistemlərinin parametrlərinin və konfiqurasiyalarının təcrübəsiz (səhlənkar) istifadəçilər tərəfindən dəyişdirilməsinin və ya normal iş rejiminin sıradan çıxmasının qarşısını almalıdır.

Kompyuter şəbəkələrinin bədniyyətli şəxslər üçün daha cəlbedici elementləri olan serverlər, mərkəzi kompyuterlər, 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 sayını 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 yolları 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;
- kompyuter 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, kompyuter 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.

2.4. İnformasiya təhlükəsizliyinin təmin edilməsinin əsas aspektləri

İnformasiya təhlükəsizliyinin təmin edilməsi – informasiyanın gizliliyinin, tamlığının 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, tamlığını və ona girişi (əlyetərliliyi) təmin edən müvafiq üsul və vasitələr kompleksi kimi dövlət, xidməti (kommersiya) və ya şəxsi sirlərin, eləcə də digər məxfi məzmunlu informasiya daşıyıcılarının qorunması başa düşülür.

KSŞ-də informasiya resurslarından icazəsiz istifadə təhlükəsinin qarşısını almaq üçün ilk reaksiya əlavə proqram vəsaitlərinin işlənib hazırlanması və kompyuterlərin proqram təminatının (ilk öncə əməliyyat sistemlərinin) tərkibinə daxil edilməsi olmuşdur. Bu proqram vasitələri, kompyuterlərə, əməliyyat sistemlərinə və kompyuter şəbəkələrinə daxilolma, informasiyaya giriş və onların istifadəsi məsələlərinin nizamlanmasını, eləcə də kompyuter 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. 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.

Kompyuter 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 kompyuterlərin, kompyuter sistemlərinin və serverlərin, eləcə də onlarda olan informasiyanın kənar şəxslərin, başqa kompyuterlərin, kompyuter 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;
- kompyuter 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;
- kompyuter 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 kompyuterlərin işinə nəzarət;
- informasiya təhlükəsizliyi protokollarının tətbiqi;
- kriptoqrafik 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 hazırlığını, 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.

Yuxarıda 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.

2.5. 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, kriptoqrafik 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 aşkaretmə 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 fikir 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.

III FƏSİL

KOMPYUTER SİSTEMLƏRİNDƏ VƏ ŞƏBƏKƏLƏRİNDƏ İNFORMASİYA TƏHLÜKƏSİZLİYİNİN POZULMASI TƏHLÜKƏLƏRİ

Kompyuter sistemlərində və şəbəkələrində informasiya resurslarına qarşı yönəlmiş təhlükələrin təsnifatı

Təsadüfən baş verən təhlükələr və onların informasiya təhlükəsizliyinə təsiri

Qəsdən törədilən təhlükələrin formaları

Ziyanverici proqramlar. Kompyuter virusları. Şəbəkə qurdları. Troya proqramları. Spamlar

Təhdidlər və onların informasiya təhlükəsizliyinin baza prinsiplərinə təsiri

3.1. Kompyuter sistemlərində və şəbəkələrində informasiya resurslarına qarşı yönəlmiş təhlükələrin təsnifatı

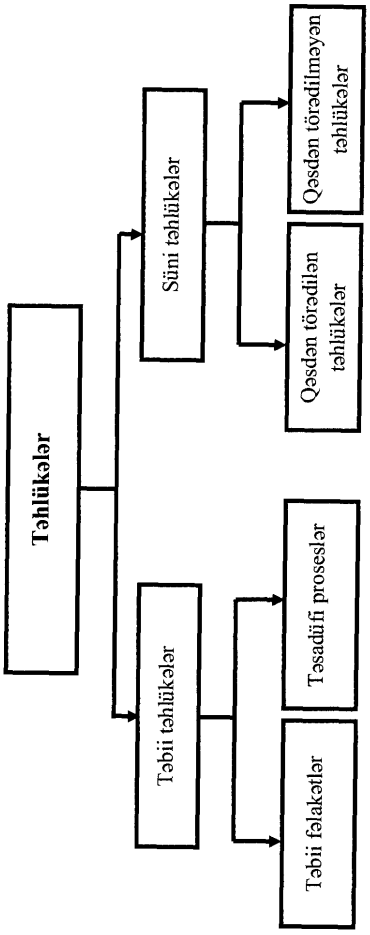
Təhlükəsizliyin pozulması təhlükəsi (informasiya təhlükəsizliyinə təhdidlər) dedikdə ayrı-ayrı şəxslərin, təşkilatların, cəmiyyətin və ya dövlətin maraqlarına ziyan vurulmasına gətirib çıxaran, informasiyanın təsadüfən və ya düşünülmüş şəkildə (qəsdən) məhv edilməsi, icazəsiz açılması və dəyişdirilməsi təhlükəsini, eləcə də kompyuterlərdə 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.

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, subasma, zəlzələ, şimşək, torpaq sürüşməsi və s. aid edilir. Bu təhlükələrin qarşısını almaq üçün kompyuter sistemləri və şəbəkələri, eləcə də onların yerləşdiyi bina və ya otaqlar layihələndirilən zaman bəzi məqamlar nəzərə alınmalıdır.



Şək.3.1. İnformasiya təhlükəsizliyinə olan təhlükələrin növləri

Belə ki, yanğın, subasma, zəlzələ və digər təbii hadisələrin qarşısının alınması zamanı kompyuter texnikasının, telekommunikasiya qurğularının və digər informasiya daşıyıcılarının, eləcə də onlarda saxlanılan və emal olunan məlumatların təhlükəsizliyinin təmin edilməsi üçün binaların tikintisi zamanı müvafiq tədbirlər görülməlidir. Məsələn, yanğından mühafizə sistemi qurularkən nəzərə alınmalıdır ki, yanğının söndürülməsi prosesində istifadə olunan su və digər vasitələr kompyuter 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 filtrləri, 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 kompyuter 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 əsaslarını 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.

3.2. Təsadüfən baş verən təhlükələr və onların informasiya təhlükəsizliyinə təsiri

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 məlumatları özündə saxlayan faylların və proqramların, o cümlədən sistem fayllarının pozulmasına və təhrif edilməsinə və s.) gətirib çıxaran düşünülməmiş hərəkətlər;

Şək.3.2. İnformasiya təhlükəsizliyinə təhlükələrin təxmini təsnifat sxemi

- 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.);
- sistem resurslarının izafi məsrəfinə (prosessorun yüklənməsinə, əməli yaddaşın və xarici informasiya daşıyıcılarında olan yaddaşın tutulmasına) səbəb ola biləcək nəzərdə tutulmamış proqramların qeyri-leqal tətbiqi və icazəsiz istifadəsi;
- kompyuter 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 kompyuterin 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, kompyuter viruslarının təsiri və s. informasiya təhlükəsizliyi üçün təhlükə yaradan ciddi amillərdir.

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

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

3.3. 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, sərinləşdirici, 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 inzibatçılar qrupuna) agentlərin yeridilməsi;
- müəyyən səlahiyyətlərə malik olan personalın və ya istifadəçilərin cəlb edilməsi (maddi maraqlandırmaq, hədə-qorxu gəlmək və s. yolla);
- qulaqasma, uzaq məsafədən şəkil və videoçəkmə 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, əlaqəyəgirmə 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 kompyuterin) 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 altında 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 kriptoqrafik qorunması şifrlərinin açılması;
- xüsusi aparat vasitələrinin, proqram və aparat qoyuluşlarının, eləcə də virusların (o cümlədən "troya atları"nın və "qurdlar"ın) tətbiqi, nəzərdə tutulmuş funksiyaların yerinə yetirilməsi üçün lazım olmayan, lakin mühafizə sistemini keçmək, qeydiyyata düşmək, vacib məlumatları 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 məlumatları yaymaq məqsədilə qanuni istifadəçi sistemə daxil olduqdan sonra onun kompyuterini şəbəkədən fiziki ayırmaq və sonradan onun adı altında autentifikasiya 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:
- kompyuter sistemlərinin və şəbəkələrinin, informasiya resurslarının, ayrı-ayrı kompyuterlərin 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 altında 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 ötrülməsi prosesinə qarışmadan trafikə 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 daxilolma 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 informasiyanı tutan, müəyyən fayla yazan və ya müəyyən ünvana göndərən proqram qoyuluşlarının ("troya atları"nın, kompyuter 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 tərəfindən fayllarda olan informasiyanın plandan kənar baxılması və ya giriş hüquqlarının kənar şəxslərə verilməsi;
- sistemdə proqramçılar və xidməti personal tərəfindən qoyulmuş və ya sistem yoxlamaları zamanı aşkar olunmuş giriş nöqtələrindən istifadə olunması;
- qanuni istifadəçi kompyuteri (işçi stansiya) ilə mərkəzi kompyuter arasındakı əlaqəni kəsmək yolu ilə sistemə daxilolmanı 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, kompyuter 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.

3.4. Ziyanverici proqramlar

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

Bu gün bir çox istifadəçilər bu və ya digər şəkildə kompyuterə ziyan vuran bütün ziyanverici proqramları kompyuter 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 (kompyuter 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 kompyuterlərə tətbiqi.

Araşdırmalar göstərir ki, 2005-ci il ərzində troya proqramlarının sayı təxminən iki 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:

- kompyuter virusları;
- şəbəkə qurdları;
- troya proqramları;
- spamlar;
- haker utilitləri.

3.4.1. Kompyuter virusları

Kompyuter virusları – kompyuterdə çoxalmaq, həmçinin rabitə kanalları, kompyuter şəbəkələri və informasiya daşıyıcıları (CD və maqnit disklər və s.) vasitəsilə digər kompyuterlərə və şəbəkələrə yayılmaq (ötürülmək) qabiliyyətinə malik olan ziyanverici proqramlardır.

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

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

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

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

Ümumiyyətlə, bioloji viruslar canlı orqanizmlərə yoluxduğu kimi, kompyuter virusları da kompyuterlərə və kompyuter proqramlarına yoluxur və onları "xəstələndirir". Kompyuterin əməliyyat sistemi, tətbiqi proqramlar, drayverlər, əməli yaddaşlar və s. kompyuter viruslarına yoluxa bilər.

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

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

Kompyuter 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, kompyuterin 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 kompyuter 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 kompyuterlərində virusların yayılması problemi ilə qarşılaşsınlar.

3.4.2. Şəbəkə qurdları

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

- uzaq məsafədə olan kompyuterlərə soxulmaq;
- öz surətini uzaq məsafədə olan kompyuterlərdə işə salmaq;
- gələcəkdə şəbəkənin digər kompyuterlərinə yayılmaq.

Şəbəkə qurdları disklərdə olan faylları dəyişdirmirlər, lakin kompyuter şəbəkələrində yayılır, kompyuterin əməliyyat sisteminə girir, digər kompyuterlərin və ya istifadəçilərin ünvanlarını tapır və müxtəlif yayma vasitələrindən istifadə etməklə özünün surətlərini həmin ünvanlara göndərir.

Özlərinin yayılması üçün şəbəkə qurdları 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 kompyuterləri və s.) arasında məlumatların mübadiləsi şəbəkələri.

Əksər məşhur şəbəkə qurdları 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 qurdları şəbəkə paketləri şəklində yayılaraq kompyuterin yaddaşına daxil olur və öz kodunu aktivləşdirir. Belə şəbəkə qurdlarını "faylsız" və ya "paket" qurdları 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 kompyuterə daxilolmaq 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 konfiqurasiyasında 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 kompyuterə daxil olur, sonra isə şəbəkə qurdunu və ya virusu hissə-hissə şəbəkədən kompyuterə köçürür. Qurd və ya virus kompyuterə hissə-hissə köçürüldüyündən antivirus proqramları onu aşkar edə bilmir.

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

3.4.3. Troya proqramları

Troya proqramları (troya atları) – yad kompyuterlərə uzaq məsafədən girişi təqdim edən, həmin kompyuterdə müxtəlif manipulyasiyalar etməyə, məxfi məlumatları (parolları, kredit kartların nömrələrini, İnternetə və kompyuterə giriş adlarını və s.) ötürməyə imkan verən ziyanverici proqramlardır. Onlar kompyuter virusları deyillər, hər hansı pozucu funksiyaya malik olmur və digər kompyuterlərin 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 kompyuterinə köçürməyə və ziyanvericini kompyuterdə quraşdıraraq işə salmağa təhrik edirlər.

Kompyuterə 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\-SOFTWARE\Microsoft\Windows\CurrentVersion\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 kompyuterin bədniyyətli şəxs tərəfindən uzaq məsafədən idarə edilməsinə imkan verir;

- DDoS (Distributed Denial of Service – "xidmət göstərməkdən imtina edilməsi") həyata keçirmək üçün utilitlər – yoluxmuş kompyuterin informasiya sisteminin resurslarını 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 məlumatları öz "jurnalına" yazır;
- reklam proqramları – daha tez-tez istifadə olunan proqramlara reklam və elan xarakterli məlumatları yerləşdirməyə imkan verir;
- zəngetmə proqramları – modem və ya telefon xətlərinin köməyi ilə kommersiya əsaslı serverə zəng edərək istifadəçini xidmətlərin haqqını ödəməyə təhrik edir;
- spamların yayılması serveri – kənar şəxsin kompyuterini 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 kompyuterdən məlumatları "sahibinə" göndərir. Bu tip troya atlarını digər kompyuterlərə yeridən şəxslər onların köməyi ilə İnternetə, o cümlədən İCQ, elektron poçtu, Chat xidmətlərinə giriş parollarını əldə edə bilər. Bu zaman hətta kompyuter sahibinin xəbəri olmur ki, kimsə onun poçtunu oxuyur,

onun adından İnternetə qoşulur, İCQ identifikatorundan istifadə etməklə əlaqə siyahısında olan digər istifadəçilərə analoji troya atlarını 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 kompyuterlərin 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 atları istənilən şəxsə yoluxmuş kompyuterə tam giriş imkanı verir. O, müştərinin qoşulmasını gözləyir. Yoluxmuş kompyuterdə müştəri İnternetə və ya lokal şəbəkəyə qoşulduqdan sonra troya atı topladığı məlumatları öz sahibinə göndərir və bu kompyuterə girişi açır. Belə ki, o, müəyyən sistemdə şəbəkə portlarını açır və bu barədə öz sahibinə məlumat verir.

BackDoor proqramları iki növə bölünür:

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

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

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

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

Log Writers və ya *Key loggers* – kompyuterdə klaviaturadan daxil edilən bütün məlumatları 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, kompyuterə qoşulmuş mikrofondan səsin və vebkameradan 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 kompyuterindən 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 proqramın məqsədi kompyuterə 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 kompyuterə bir deyil, eyni zamanda bir-birindən fərqlənən və ayrı-ayrı adamlar tərəfindən yazılmış bir neçə ziyanverici proqramı yükləyə bilər.

Trojan-Downloader proqramları virus yazanlar tərəfindən 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 kompyuterlərdə quraşdırılması üçün istifadə olunur.

3.4.4. Spamlar

Spam – xüsusi proqramlar vasitəsilə siyasi, kommersiya, reklam və digər növ məlumatların, bu məlumatları 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 tərəfindən 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 məhsullarını və xidmətlərini daha ücüz 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 (pornoqrafiyanı, saxta malları, dövriyyəsi məhdudlaşdırılmış dərman məhsullarını, qeyri-qanuni yolla alınmış gizli məlumatları, 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 inzibatçıları 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 mənfi münasibət yaratmaq məqsədilə onun adından kütləvi göndərişlər təşkil etmək.
- Kompyuter viruslarını saxlayan məktubların kütləvi göndərilməsini təşkil etmək.

Qeyd etmək lazımdır ki, müəyyən növ məlumatların kütləvi yayılması üçün alanların razılığının tələb olunması 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, kompyuter-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.

3.4.5. 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).

3.5. Təhlükələr və onların informasiya təhlükəsizliyinin baza prinsiplərinə təsiri

Aydındır ki, informasiyanın təhlükəsizliyini poza biləcək təhlükələrin təbiətini qabaqcadan dəqiq müəyyən etmək mümkün olmur. Lakin təhlükələri kompyuter 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 təhlükəsiz-

liyinin 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 kompyuter 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	Maxfiliyin pozulması	Tamlığın pozulması	Təcrid-edilmə
1.	Təbii fəlakətlər (yanğın, subasma, 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.	İstifadəyə 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.	Kompyuter 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 daşıyıcıların oğurlanması, rabitə xətlərinə qoşulma, resursların icazəsiz istifadəsi	İcazəsiz köçürmə, tutma, əlaqeçirmə	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, oğurlanması, 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 səhvetmə, iş rejimini pozma

IV FƏSİL

İNFORMASİYA TƏHLÜKƏSİZLİYİNİN TƏMİN EDİLMƏSİ ÜSULLARI VƏ VASİTƏLƏRİ

İnformasiya təhlükəsizliyinin təmin edilməsi üsul və vasitələrinin təsnifatı

İnformasiyanın qorunmasının qeyri-texniki vasitələri. Təşkilati qoruma tədbirləri. Hüquqi qoruma vasitələri. Mənəvi-etik tədbirlər

İnformasiyanın qorunmasının mühəndis-texniki üsulları və vasitələri. Fiziki qoruma vasitələri. Aparat vasitələri. Proqram vasitələri

İnformasiyanın kompyuter viruslarından qorunması

4.1. İnformasiya təhlükəsizliyinin təmin edilməsi üsul və vasitələrinin təsnifatı

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 kompyuter texnikasının və kommunikasiya avadanlıqlarının inkişafı informasiyanın qorunması məsələsinə daha ciddi və kompleks yanaşma zərurətini yaratdı.

İlk dövrlərdə elə fikir formalaşmışdı 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 etibarlılığını 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.

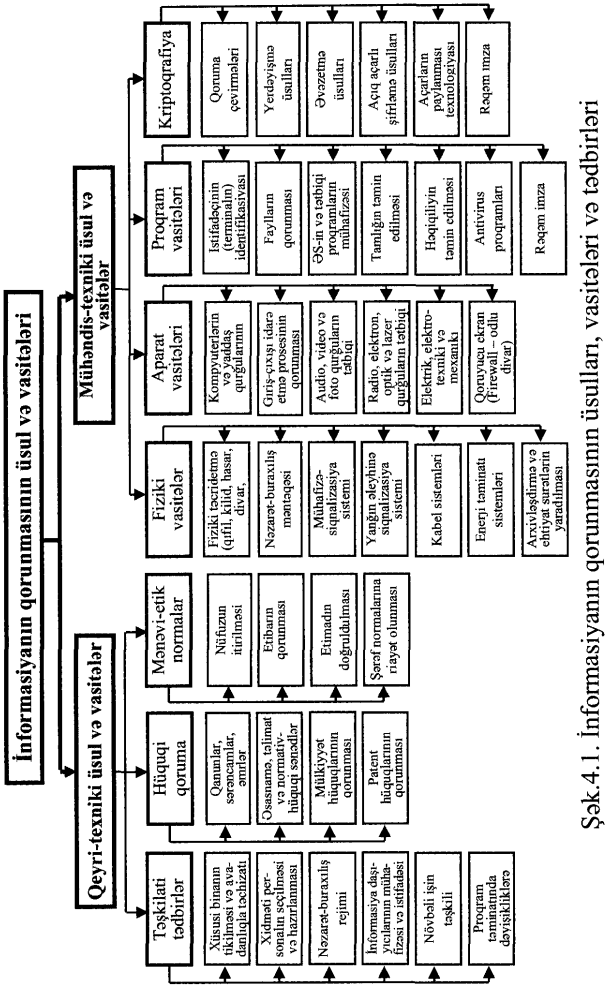
İnformasiya təhlükəsizliyi konsepsiyasının formalaşması prosesində tədricən aydın oldu ki, qoruma vasitələrinin kompleks şəkildə (proqram, texniki, təşkilati və s.) işlənib hazırlanması və tətbiqi daha da səmərəli olur, yalnız bu yolla arzu olunan nəticə əldə edilə bilər.

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 etibarlılığına 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

4.2. İnformasiyanın qorunmasının qeyri-texniki vasitələri

Qeyri-texniki qoruma vasitələrini üç əsas hissəyə bölürlər:

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

4.2.1. 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 ərazidəolma 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 halları 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.

4.2.2. 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 qaydalarını

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.

4.2.3. 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.

4.3. 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;
- steqanoqrafik vasitələr.

4.3.1. 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 fiziki qorunması, mühafizəsi 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 mühafizəsi;
- daxili binaların və otaqların (kompyuter 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, flash yaddaş qurğularının, çap vərəqlərinin və s.) mühafizəsi;
- qorunan zonalara girişin nəzarət edilməsi;
- kompyuter 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 mühafizənin təşkili;
- bədəməl şəxslərin, o cümlədən oğruların, hakerlərin, kompyuter 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.

4.3.2. İnformasiyanın qorunmasının aparat vasitələri

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 kompyuter 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;
- məxfi 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 müəyyənetmə vasitələri;
- axtarış və dəqiqölçmə 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 axtarışını, 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 aşkaretmə 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 kompyuterlərə 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, kompyuter 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.

4.3.3. 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, kompyuterlərin, 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 autentifikasiyası;
- rəqəm imza, yəni informasiyanın və onun müəllifinin 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, müvafiq 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.

4.3.4. Kabel sistemlərinin qorunması

Kabel sistemi lokal kompyuter şəbəkələri üçün informasiya təhlükəsizliyi baxımından əsas elementlərdən biridir. Belə ki, kompyuter şəbəkələrində sıradançıxma 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 kompyuter 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 xətlərinin 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 qurğularını 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 kompyuter 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.

4.3.5. 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 müvafiq qurğular gərginliyin bərpa edilməsi və informasiyanın yaddaş qurğularında saxlanması üçün tələb olunan vaxt intervalında lokal şəbəkənin, ayrı-ayrı kompyuterlərin və ya digər avadanlıqların qidalanmasını təmin edə bilər.

Fasiləsiz qidalanma mənbələrinin əksəriyyəti, həmçinin gərginliyin sabitləşdirilməsi 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 halları 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.

4.3.6. İnformasiyanın arxivləşdirilməsi və ehtiyat surətlərinin yaradılması sistemləri

Etibarlı və səmərəli arxivləşdirilmə sisteminin təşkili kompyuter 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.

4.4. İnformasiyanın kompyuter viruslarından qorunması

Kompyuter 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 kompyuter 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.

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

Antivirus proqramları iş prosesində kompyuterin yaddaşını, sistemdə olan proqramları, istifadə olunan faylları, emal edilən informasiya resurslarını və s. yoxlayır və nəzarətdə saxlayır. Daim yeni-yeni kompyuter 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 kompyuter virusları probleminin aktuallığının yüksək olduğunu göstərir.

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

- *filtrləyici antivirus proqramları* – kompyuterdə yerinə yetirilən bütün proqramları "süzgəcdən" keçirir, virusların sistemə keçməsinə mane olur;

- *yoluxmaya qarşı antivirus proqramları* – sistemin fəaliyyətini daim nəzarətdə saxlayır, kompyuterin 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 kompyuterin 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;
- kompyuter virusları üçün xarakterik olan davranışların tanınması (müəyyən edilməsi);
- sistem inzibatçısının kompyuterindən 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 kompyuterlərin 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, kompyuter viruslarının hücumlarından qorunmaq üçün ən yaxşı vasitə ona yoluxmanın qarşısının alınmasıdır. Viruslara yoluxmanın qarşısının alınması üçün aşağıdakı tövsiyələri diqqət mərkəzində saxlamaq lazımdır:

- antivirus proqram təminatını 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 emalını həyata keçirən proqram əlavələrinin təhlükəsizliyi siyasətini işləyib hazırlamalı.

Hazırda bir çox məşhur antivirus proqramları geniş yayılmışdır və kompyuter istifadəçiləri tərəfindən müvəffəqiyyətlə istifadə olunur. Bunlara Symantec AntiVirus, Norton AntiVirus, DrWeb, Kasperski AVP, ADinf, Aidstest 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 kompyuterdə və ya kompyuter 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.

V FƏSİL

İNFORMASİYANIN QORUNMASININ KRİPTOQRAFİK ÜSULLARI

Kriptologiya, kriptoqrafiya, kriptoanaliz

Kritoqrafik sistemlərin inkişaf tarixi

Kriptoqrafik sistemlər və onlara qoyulan tələblər

Kriptoqrafik sistemin modeli

Kriptoqrafik sistemlərin təsnifatı. Simmetrik (biraçarlı) şifrləmə üsulları. Asimmetrik (ikiaçarlı) şifrləmə üsulları. Əvəzetmə üsulları. Qammalaşdırma üsulları. Yerdəyişmə üsulları. Axmla şifrləmə üsulları. Bloklarla şifrləmə üsulları

Sadə şifrləmə üsullarının nümunələri

Biraçarlı kriptoqrafik şifrləmə sistemləri. DES standartı. AES standartı. Rusiya şifrləmə standartı - ГОСТ 28147–89

İkiaçarlı kriptoqrafik sistemlər. RSA kriptoqrafik sistemi. Əl-Qamal şifrləmə alqoritmi

5.1. 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 kompyuterdə emal olunan, eləcə də rabitə kanalları vasitəsilə ötürülən informasiyanın məzmununun gizlədilməsi üsulları məcmusu başa düşülür.

Kriptoanaliz şifrləmə açarını bilmədən informasiyanın məxfiliyinin açılması və autentikliyinin (əsli ilə eyniliyinin) pozulması üçün reallaşdırılan riyazi üsulları özündə ehtiva edir. Kriptoanaliz məxfi xarakterli informasiyanın əldə olunması (çıxarılması) məqsədilə şifrlənmiş mətnin açılması üçün kriptoqrafik 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, şifrmətnləri 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 kriptoqrafik hücum uğurla başa çatarsa, onda ona *sındırma* (*şifrin sındırılması*) deyilir.

Şifrin naməlum açara görə açılmaya davamlılığını 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 kriptoqrafik 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.

Kriptoqrafik sistemin davamlılığı təhlil olunarkən eyni zamanda insan amili də nəzərə alınmalıdır. Belə ki, zəruri informasiyaya girişi olan əməkdaşı ələ almaq şifrin sındırılması üçün superkompyuterin 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 kriptoqrafik 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 məxfi 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.

5.2. 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;
- kompyuter 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 şifri çox əlifbalı əvəzetmə prinsipinə əsaslanır. Belə ki, yunan əlifbası əvvəlcədə 5x5 ölçülü kvadrat cədvələ yazılır, sonra isə ilkin mətnin hər bir hərfi 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 sonra 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 formalaşmışdı. Bura, riyazi statistikanı, 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 "Məxfi 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.

Kompyuter kriptoqafiyası ötən əsrin 70-ci illərindən sonrakı dövrü əhatə edir və hesablama sistemlərinin, o cümlədən kompyuter texnikasının yaranması ilə formalaşmışdır. Kompyuter 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 standartı 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 – biraçarlı) üsullardan istifadə zamanı şifr

mətnlə yanaşı şifrləmə açarının ötürülməsi lazım gəlirdisə, asimmetrik (ikiaçarlı) şifrləmə üsulları isə şifrləmə açarının ötürülməsini tələb etmirdi.

Asimmetrik kriptosistemlərin elmi əsası ilk olaraq U.Diffi və M.Helman tərəfindən 1976-cı ildə çap olunan "Müasir kriptoqrafiyanın 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 hazırlamışdılar.

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

5.3. Kriptoqrafik sistemlər və onlara qoyulan tələblər

Qeyd olunduğu kimi, kriptoqrafik 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 autentifikasiya 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 kriptoqrafik 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 (şifrmətndən) alınmasının qeyri-mümkünlüyü xassəsi başa düşülür.

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

Qeyd olunmalıdır ki, son zamanlar kriptoqrafik 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:

- şifrmətn yalnız şifrləmə açarı olduqda oxuna bilər;
- şifrmətnin 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 şifrmətnin şəklinin əhəmiyyətli dəyişməsinə gətirib çıxarmalıdır;
- açıq mətnin cüzi dəyişməsi hətta eyni bir açar istifadə olunduqda belə şifrmətnin şəklinin əhəmiyyətli dəyişməsinə gətirib çıxarmalıdır;
- şifrlənmə alqoritminin məlum olması qorunmanın etibarlılığına 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 şifrmətndə 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.

Kriptoqrafik sistemlərin davamlılığı üç aspektdən qiymətləndirilir:

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

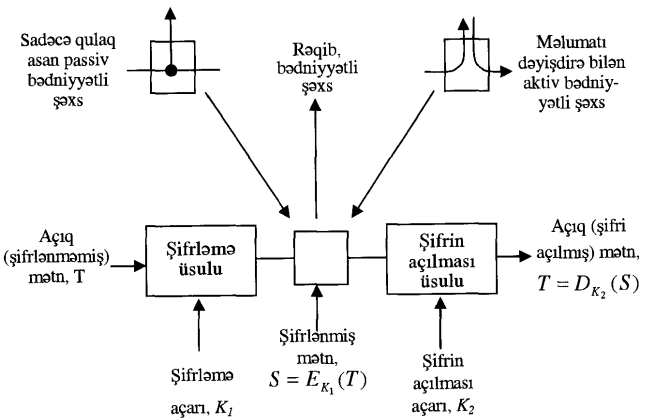
Kriptoanalitik ələ keçirilmiş kriptoqramın təhlili üçün kifayət qədər vaxta və bütün zəruri vasitələrə malik olduqda kriptoqrafik sistemin etibarlılıq dərəcəsini göstərən davamlılıq qabiliyyəti *nəzəri davamlılıq* adlanır. Nəzəri davamlılıq məsələsinə baxış kriptoqrafik qoruma dərəcəsinə aydınlıq gətirir, 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.

5.4. Kriptoqafik sistemin modeli

Kriptoqrafik sistemin modeli özündə abonentlərin rabitə xətti vasitəsilə məlumat mübadiləsi aparması, ötürülən və ya alınan məlumatların rəqib tərəfindən tutulması mümkün olan informasiya sistemini ehtiva edir. Modelə iki və ya daha çox abonent (qanuni istifadəçilər), abonentlər arasında məlumat mübadiləsinin aparılması üçün rabitə kanalı və ya kanalları, habelə ötürülən məlumata müdaxilə etmək istəyən rəqib (qeyri-qanuni istifadəçi) daxildir (şək.5.1).



Şək.5.1. Kriptoqrafik sistemin modeli

Qeyd olunmalıdır ki, rəqib həm daxili, həm də xarici ola bilər. *Daxili rəqib* dedikdə sistemin abonenti, *xarici rəqib* dedikdə isə sistemin abonenti olmayan xarıcı istifadəçilər nəzərdə tutulur. İkinci halda, sistemə qoşularaq icazəsi (hüququ) olmayan məlumatlara (məsələn, digər abonentlərin göndərdikləri məxfi məlumatlara) giriş əldə etməyə cəhd edən xarici istifadəçi *qeyri-qanuni istifadəçi* adlanır.

Eyni zamanda, rəqib, məlumatları müxtəlif məqsədlər üçün (tutulan məlumatın açıqlanması, öz məqsədləri üçün istifadə edilməsi, başqa şəxsə ötürülməsi, dəyişdirilməsi, imitasiyası və s. məqsədilə) tuta bilər. Təhdidlər kateqoriyasına aid edilən belə fəaliyyətin qarşısının alınması üçün müxtəlif kriptoqrafik üsullar tətbiq olunur.

Nəzərə almaq lazımdır ki, kriptoqrafik sistemlərin təsvir olunan modeli məlumat mübadiləsindən fərqli təhlükələrin qarşısının alınması üçün də istifadə oluna bilər. Məsələn, kompyuterdə saxlanılan məlumatların qorunması zamanı hesab etmək olar ki, modeldə göstərilən hər iki abonent məlumatların saxlandığı kompyuterdə müxtəlif vaxtlarda işləyən istifadəçilərdir, rabitə kanalı isə məlumatların saxlanıldığı kompyuterin yaddaş (məsələn, bərk disk) qurğusudur.

Beləliklə, ümumi halda modeldə fərz edilir ki, rəqib məlumatların ötürülməsi kanalına girişə malikdir. Ona görə də məlumatı ötürən abonent məxfi xarakterli ilkin informasiyanı (açıq mətni) əvvəlcə gizli mətnə (şifrmətnə, şifrlənmiş mətnə, kriptoqrama) çevirməlidir. Açıq mətnin şifrmətnə çevrilməsi *şifrləmə* adlanır. Şifrmətni alan abonent onu əks çevirmə yolu ilə açır və ilkin mətni bərpa edir.

İnformasiyanın şifrlənməsi və şifrin açılması üçün məxfi məlumat olan *açardan* istifadə olunur. Şifrləmə və şifrin açılması üçün istifadə olunan açarlar bəzi kriptoqrafik sistemlərdə eyni, digərlərində isə fərqli olur. Açarlar yalnız onun məxsus olduğu abonentlərə məlum olur, rəqib isə açarı bilmir. Buna baxmayaraq rəqib şifri açmağa cəhd edə, uyğun açar seçə və ya şifri hər hansı başqa üsulun köməyi ilə aça bilər.

Şifrin formal modelini aşağıdakı kimi müəyyən etmək olar. Tutaq ki, T, S və K – uyğun olaraq, mümkün açıq mətnlərin, şifrmətnlərin və açarların sonlu çoxluğudur. Adətən, bu çoxluqların hər biri hər hansı əlifbada müəyyən edilmiş sözlər çoxluğunu təşkil edir. Burada qeyd olunmalıdır ki, açıq mətnlərin, şifrmətnlərin və açarların əlifbaları müxtəlif ola bilər. Müasir kriptoqrafik sistemlərin əksəriyyəti üçün açıq mətnlər, şifrmətnlər və açarlar $\{0,1\}$ əlifbasında formalaşdırılmış sözlərdən, yəni sıfır və birlər ardıcıllığından ibarət olur.

Bu modelə əsasən şifrləmə prosedurasını hər hansı açardan asılı olaraq açıq mətnlər çoxluğunu şifrmətnlər çoxluğuna inikas etdirən aşağıdakı funksiya kimi vermək olar:

$$E_k : T \to S, k \in K .$$

Analoji olaraq, şifrin açılması prosedurasını k açarından asılı olaraq şifrmətnlər çoxluğunu açıq mətnlər çoxluğuna inikas etdirən funksiya kimi vermək olar:

$$D_k : S \to T, k \in K .$$

Şifrmətni alan tərəf həmişə onun əsasında ilkin mətni bərpa etmək imkanına malik olması üçün istənilən $k \in K$

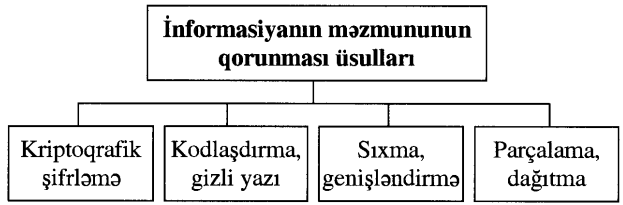
açarına görə E_k və D_k funksiyaları aşağıdakı şərtləri ödəməlidir:

$$D_k : E_k = I ,$$

Burada I – T çoxluğunun öz-özünə eyniliklə inikasıdır.

5.5. Kriptoqrafik üsulların təsnifatı

İnformasiyanın məzmununun gizlədilməsi (çevrilməsi) üsul və alqoritmlərini bir neçə kateqoriyaya ayırmaq olar: kriptoqrafik şifrləmə, kodlaşdırma və ya gizli yazı, sıxma, parçalama, dağıtma və s. (şək.5.2).



Şək.5.2. İnformasiyanın məzmununun gizlədilməsi üsulları

Kodlaşdırma və ya gizli yazı. Məlumatı göndərən və alan tərəflər onun üzərində yalnız onlara məlum olan çevirmələri (şifrləmə əməliyyatlarını) aparırlar. Şifrləmə alqoritmi kənar şəxslərə məlum olmur. Bir çox mütəxəssislər gizli yazını kriptoqrafiya hesab etmirlər.

Kodlaşdırma dedikdə açıq mətnin elementlərinin (hərflərinin, sözlərinin, cümlələrinin və s.) müəyyən kodlarla əvəz olunması başa düşülür. Kodlaşdırmanın iki əsas növündən istifadə olunur: simvol kodlaşdırması və məna kodlaşdırması.

Simvol kodlaşdırması zamanı ilkin mətnin əlifbasının hər bir hərfi bu və ya digər əlifbanın digər hərfi ilə əvəz olunur. Simvol kodlaşdırmasına nümunə olaraq, Morze əlifbasını, şifrləmənin əvəzetmə və yerdəyişmə üsullarını göstərmək olar.

Məna kodlaşdırması zamanı ilkin əlifbada yalnız ayrı-ayrı simvollar (hərflər) deyil, daha tez-tez istifadə olunan sözlər, ifadələr və hətta cümlələr başqaları ilə dəyişdirilir.

Sıxma. Kompyuterdə böyük informasiya massivlərinin saxlanması üçün müxtəlif sıxma üsullarından istifadə olunur. İnformasiyanın sıxılmasını da kodlaşdırma kimi qəbul etmək olar. Belə ki, sıxma üsulları məlumatda təkrarlanan simvolları və simvol sətirlərini elə çevirir ki, o, yaddaşda az yer tutsun. Sıxma üsullarını iki sinfə bölürlər: statistik və dinamik (adaptiv) sıxma üsulları.

Statistik sıxma üsulları mətndə simvolların rast gəlinmə tezlikləri cüzi dəyişdikdə daha effektiv olur. *Adaptiv sıxma üsulları* isə simvolların rast gəlinmə tezliklərinin qeyri-müntəzəmliyini izləyir və onların rast gəlinməsi ehtimallarının dəyişməsini yadda saxlayır. Adaptiv sıxma üsulları kodlaşdırma prosesində açıq mətndə baş verən dəyişikliyə dinamik reaksiya verir.

Parçalama və dağıtma. Bu növ üsulların köməyi ilə bir faylın məzmunu elə şəkildə bloklara bölünür və ayrı-ayrı fayllara dağıdılır ki, bu fayllar ayrı-ayrılıqda heç bir

informasiya daşımasın və onların yenidən bir vahid fayla toplanması asanlıqla həyata keçirmək mümkün olsun.

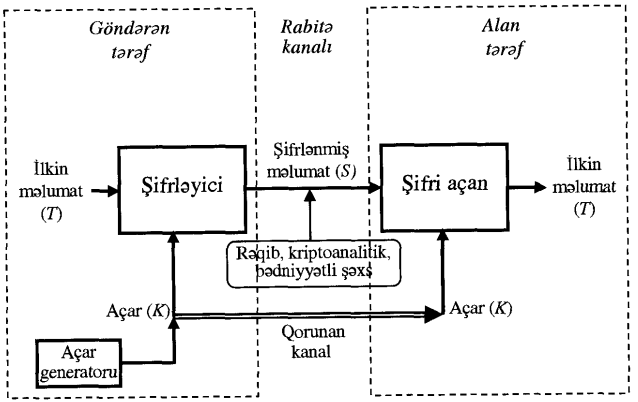
Kriptoqrafik şifrləmə. Qeyd olunduğu kimi, şifrləmə üsulları dedikdə istənilən formada olan, o cümlədən disk qurğularında saxlanılan və ya kompyuterdə emal olunan, eləcə də rabitə kanalları vasitəsilə ötürülən informasiyanın məzmununun gizlədilməsi üsulları (alqoritmləri) başa düşülür. Burada fərz edilir ki, şifrləmə alqoritmi hamıya məlumdur. Lakin şifrin açılmasını yalnız göndərən və alan tərəflərə məlum olan açar vasitəsilə həyata keçirmək mümkündür.

Kriptoqrafik şifrləmə üsullarını (alqoritmlərini) aşağıdakı əlamətlərə görə təsnif etmək olar:

- *istifadə olunan açarların növünə görə*: simmetrik şifrləmə üsulları və asimmetrik şifrləmə üsulları.
- *şifrləmə alqoritminə görə*: əvəzetmə üsulları, qammalaşdırma üsulları, yerdəyişmə üsulları, kombinasiya (kompozisiya) edilmiş üsullar.
- *şifrləmə ardıcıllığına görə*: bloklarla şifrləmə və axınla şifrləmə.

5.6. Simmetrik (biraçarlı) şifrləmə üsulları

Gizli açarlı kriptoqrafik şifrləmə sistemlərinin ən vacib elementi gizli açarın ötürülməsi üçün "ciddi qorunan kanal"ın olmasıdır (şək.5.3). Şəkildən göründüyü kimi, gizli açarlı kriptoqrafik sistemə əsasən, məlumatı göndərən şəxs gizli şifrləmə açarını və alqoritmini istifadə etməklə açıq məlumatı şifrləyir və göndərilməsi nəzərdə tutulan şəxsə ötürür.



Şək.5.3. Simmetrik kriptoqrafik sistemlərin ümumi sxemi

Məlumatları göndərən və alan tərəflərin hər ikisinin eyni bir açardan istifadə etməsi faktını vurğulamaq üçün, adətən, gizli açarlı şifrləmə üsullarını *biraçarlı* və ya *simmetrik şifrləmə sistemləri* adlandırırlar.

Şifrləmə açarı, bir qayda olaraq, açar generatoru tərəfindən yaradılır, rəqibin (kriptoanalitikin və ya bədniyyətli şəxsin) əlinə keçməsindən ciddi qorunur, qabaqcadan ciddi qorunan kanal vasitəsilə nəzərdə tutulan şəxsə çatdırılır. Alan tərəf həmin açarı tətbiq etməklə ona çatan şifrmətni açır. Burada şifrləmə açarı (K) – hər hansı sonlu əlifbanın simvollarından ibarət olan ardıcıllıqdır. Belə əlifba qismində çox vaxt ikilik əlifbadan $\{0,1\}$ istifadə olunur.

Təklif olunan modelə əsasən məlumatı göndərən tərəf açıq mətni $T=\{t_1, t_2, ..., t_n\}$ yaradır və şifrləyici vasitəsilə

onu şifrləyir. Yuxarıda qeyd olunduğu kimi, şifrləmə prosedurasını

$$S = E_K(T)$$

çevirmə funksiyası vasitəsilə ifadə etmək olar. Aydındır ki, kriptoqrafik şifrləmə funksiyası K açarını istifadə etməklə T açıq mətninə tətbiq edilir.

Sxemdən göründüyü kimi, alan tərəfdə olan şifri açan alqoritm əks çevirməni yerinə yetirməyə qadirdir. Lakin qeyd olunduğu kimi, bunun üçün həmin K gizli açarı tələb olunur. Bu açara malik olan alan tərəf

$$T = D_K(S)$$

funksiyasının köməyi ilə şifrmətni açır və ilkin mətni əldə edir.

Burada ehtimal olunur ki, rəqibə (kriptoanalitikə və ya bədniyyətli şəxsə) ilkin mətn və açardan başqa şifrləmə prosesinin bütün digər detalları bəlli olur. Başqa sözlə, kriptoanalitik rabitə kanalı vasitəsilə ötürülən şifrmətni ələ keçirsə də şifrləmə açarını bilmədiyi üçün onu açа bilmir.

Şifrləmə zamanı açıq mətn üzərində yerinə yetirilən çevirmələrin növündən asılı olaraq, simmetrik şifrləmə sistemləri əvəzetmə, yerdəyişmə və kombinasiyalı şifrləmə üsulları əsasında reallaşdırılır. Bu şifrləmə üsullarına növbəti paraqraflarda baxılacaqdır.

Simmetrik şifrləmə üsullarının əsas çatışmazlığı ondan ibarətdir ki, gizli açar həm göndərənə, həm də alana məlum olmalıdır. Bu, o deməkdir ki, simmetrik kriptoqrafik sistemdən istifadəyə başlamazdan əvvəl hər iki (göndərən və alan) tərəf gizli açarı mütləq bilməlidir. Bu baxımdan burada, əlavə olaraq, açarın gizli (ciddi qorunan) kanalla

digər tərəfə göndərilməsi problemi yaranır. Açarın ötürülməsi elə həyata keçirilməlidir ki, potensial rəqib (bədniyyətli şəxs) onu əldə edə (tuta) bilməsin.

Digər çatışmazlıq kimi, alan tərəf əlində olan şifrlənmiş və açıq mətnlərə görə bu məlumatı hər hansı konkret şəxsdən (göndərəndən) aldığını sübut edə bilməməsini, eləcə də hər hansı məlumatı və onun şifrmətnini generasiya edərək başqasından aldığını iddia etmək imkanının mümkünlüyünü göstərmək olar. Belə ki, o, əlində olan məxfi açarla digər tərəfdən asılı olmadan analoji məlumatı generasiya edə, şifrləyə və şifri açа bilər.

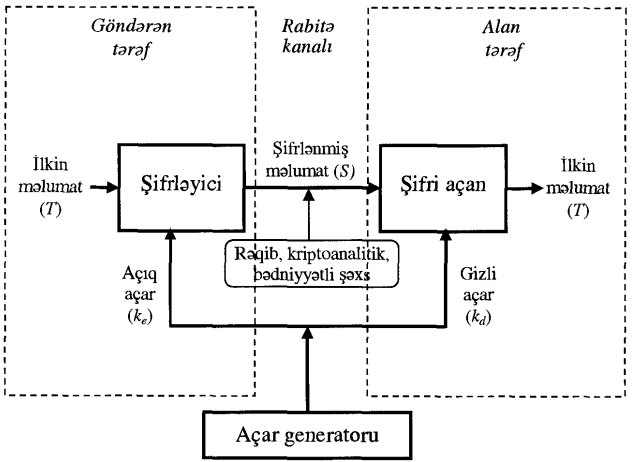
5.7. Asimmetrik (ikiaçarlı) şifrləmə üsulları

Qeyd olunduğu kimi, simmetrik şifrləmə sistemlərinin praktiki istifadəsi zamanı meydana çıxan əsas problemlərdən biri gizli saxlanılan (ciddi qorunan) şifrləmə açarının paylanması və saxlanılmasıdır. Əgər sistemdə n sayda abonent varsa, onda onlar arasında məxfi informasiya mübadiləsini təmin etmək məqsədi ilə sistemin istifadəçilərinin hər bir cütü üçün bir gizli acar mövcud olmalıdır.

Beləliklə, hər bir istifadəçi digər istifadəçilərlə informasiya mübadiləsi aparmaq üçün n-1 sayda məxfi açara malik olmalı, onları saxlamalı və kənar şəxslərdən qorumalıdır. Ümumiyyətlə, sistemdə $n*(n-1)/2$ sayda məxfi açarın generasiya edilməsi, sahibinə çatdırılması və qorunması tələb olunur.

Bu problemin aradan qaldırılması üçün açıq açarlı kriptoqrafik sistemlər təklif olunmuşdur. Bu sistemlərdə məlumatların mübadiləsi üçün iki açardan istifadə olunur.

Başqa sözlə, açıq açarlı şifrləmə sistemləri şifrləmə və şifrin açılması üçün iki müxtəlif açardan istifadə edir. Belə sistemlər üçün k açarı (k_e, k_d) cütlüyü şəklində təqdim olunur (şək.5.4). Burada k_e – şifrləmə üçün istifadə olunan açar, k_d isə şifrin açılması üçün istifadə edilir. Açarlardan biri *gizli* saxlanılır, digəri isə *açıq* olur, yəni ümumi istifadə üçün nəzərdə tutulur.



Şək.5.4. Asimmetrik kriptoqrafik sistemlərin ümumi sxemi

İki açarın istifadə olunması səbəbindən bu sistemləri *ikiaçarlı*, şifrləmə və şifrin açılması üçün istifadə olunan açarların müxtəlif olması səbəbindən isə onları *asimmetrik* kriptoqrafik sistemlər adlandırırlar. Bütün asimmetrik krip-

toqrafik sistemlərin əsasını sekretli biristiqamətli funksiyalar təşkil edir.

Əgər aşağıdakı iki şərt yerinə yetirilərsə, onda $F:X\rightarrow Y$ funksiyasına *biristiqamətli funksiya* deyilir:

- istənilən $x\in X$ üçün $F(x)$ funksiyasının qiymətini hesablayan effektiv alqoritm mövcuddur;
- $F(x)$ funksiyasının tərsini (inversiyasını) tapmağa, yəni $F(x)$ funksiyasının qiymətinə görə x dəyişəninin qiymətini müəyyən etməyə imkan verən effektiv alqoritm mövcud deyil.

Burada *effektiv alqoritm* dedikdə nəticənin alınması üçün tələb olunan addımların sayı sonsuz olmayan alqoritm başa düşülür.

Daha tez-tez istifadə olunan biristiqamətli funksiyalara nümunə qismində iki sadə ədədin hasili, diskret loqarifmləmə, "çantanın yığılması", mürəkkəb ədədlərin qüvvətə yüksəldilməsi və s. məsələləri göstərmək olar.

Təbii ki, istənilən biristiqamətli funksiya şifrləmə alqoritmi üçün istifadə oluna bilməz. Belə ki, əgər T açıq mətni $S=F(T)$ biristiqamətli funksiyasının köməyi ilə şifrlənərsə, onda S şifrmətninə görə ilkin T mətnini heç kəs, hətta informasiyanı qanuni alan şəxs belə bərpa edə bilməz.

Biristiqamətli funksiya o vaxt kriptoqrafiyada istifadə oluna bilər ki, onun əsasında aparılan şifrləmə çevirmələrinin əksinin alınması məsələsi gizli açarı bilən şəxs tərəfindən münasib müddət ərzində həll edilə bilsin, yəni $S=F_k(T)$ funksiyasına görə $T=F_k^{-1}(S)$ qiymətlərini hesablamaq mümkün olsun. Məhz belə funksiyalara *gizli yollu (sekretli) biristiqamətli funksiyalar* deyilir.

Aşağıdakı şərtləri ödəyən, $k\in K$ parametrindən asılı olan $F_k:X\rightarrow Y$ funksiyasına *sekretli biristiqamətli funksiya* deyilir:

- istənilən $k\in K$ parametrinə görə istənilən $x\in X$ üçün $F_k(x)$ funksiyasının qiymətini hesablayan effektiv alqoritm mövcuddur;
- k parametri naməlum olduqda $F(x)$ funksiyasının tərsini (inversiyasını), yəni $F(x)$ funksiyasının qiymətinə görə x dəyişəninin qiymətini hesablamağa imkan verən effektiv alqoritm mövcud deyil;
- k parametri məlum olduqda $F_k(x)$ funksiyasının tərsini (inversiyasını) hesablayan effektiv alqoritm mövcuddur.

Qeyd etmək lazımdır ki, biristiqamətli funksiyaların, o cümlədən sekretli biristiqamətli funksiyaların mövcudluğu hələ isbat edilməmişdir. Əgər verilən funksiyaların tərsinin (inversiyasının) tapılması hesablama baxımından həqiqətən çətin məsələ olarsa, onda belə funksiyalar biristiqamətli funksiya kimi qəbul oluna bilər.

Aşağıda ümumi şəkildə sekretli biristiqamətli funksiyaların şifrləmə üçün istifadə edilməsi prinsiplərinə baxılır. Kriptosistemin hər bir abonenti k sekretli E_k biristiqamətli funksiyasını seçir. Bu funksiyalar ümumi məlumat kitabçasına daxil edilir. Lakin hər bir abonent özünəməxsus olan k – sekretinin qiymətini gizli saxlayır.

Tutaq ki, A abonenti B abonentinə T məlumatını göndərmək istəyir. Bunun üçün A abonenti əvvəlcə məlumat kitabçasından B abonentinin E_k funksiyasını götürür və onun köməyi ilə T məlumatını şifrləyir, yəni aşağıdakı çevirməni həyata keçirir:

$$S=E_k(T).$$

Sonra S şifrmətnini B abonentinə göndərir. Şifrmətni alan B abonenti k sekretinin köməyi ilə E_k funksiyasını inversiya edir və T ilkin məlumatını hesablayır.

$$T=D_k(S).$$

k sekreti yalnız B abonentinə məlum olduğu üçün S şifrmətnini ondan başqa heç kəs açа bilməz.

Qeyd olunmalıdır ki, effektivliyə və davamlılığa görə asimmetrik şifrləmə üsullarına nisbətən simmetrik şifrləmə üsulları üstünlüyə malikdir. Belə ki, eyni uzunluqlu açara görə simmetrik şifrləmə üsulları asimmetrik şifrləmə üsulları ilə müqayisədə daha sürətlə işləyir və məxfiliyi daha yüksək təmin edir. Ona görə də praktikada asimmetrik şifrləmə üsulları müstəqil deyil, simmetrik şifrləmə üsulları ilə kompleksdə istifadə olunur.

Belə kompleks istifadəyə nümunə kimi aşağıdakı yanaşmanı göstərmək olar. Tutaq ki, Z_1 – simmetrik şifrləmə alqoritmi, Z_2 isə asimmetrik şifrləmə alqoritmidir. Onda məlumatların şifrlənməsini aşağıdakı kimi həyata keçirmək mümkündür.

- Z_1 alqoritmi üçün təsadüfi k_1 açarı generasiya edilir;
- k_1 açarının köməyi ilə məlumatlar şifrlənir: $S'=Z_1(T,k_1)$;
- k_1 açarı Z_2 alqoritmi vasitəsilə göndərənin k_e açıq açarını istifadə etməklə şifrlənir: $S''=Z_2(k_1,k_e)$;
- göndərilən şifrmətn $S=(S',S'')$ cütlüyündən ibarət olur.

Burada k_e açarı məlumat göndərilən tərəfin açıq açarıdır. Alınmış $S=(S',S'')$ şifrlənmiş məlumatın açılması

üçün alan tərəf S'' şifrmətninə görə k_1 açarını bərpa edir, onun köməyi ilə S' şifrmətnini açır və ilkin mətni bərpa edir. k_1 açarının uzunluğu məlumatın uzunluğuna nisbətən çox kiçik olduğuna görə bu cür şifrləmə sxeminin sürəti əhəmiyyətli dərəcədə yüksək olur.

5.8. Əvəzetmə üsulları

Əvəzetmə üsulları özündə açıq mətnin fraqmentlərinin (ayrı-ayrı simvollarının və ya bloklarının) şifrmətndə başqa simvollarla və bloklarla əvəz edilməsinə əsaslanır.

Ən sadə əvəzetmə üsulu *birəlifbalı əvəzetmə üsuludur*. Bu üsulu çox vaxt *sadə əvəzetmə* adlandırırlar. Bu üsulda şifrləmə açarı açıq mətnin T əlifbasının şifrmətnin S əlifbasına qarşılıqlı birqiymətli F inikasından ibarətdir.

$$F:T\to S.$$

Tutaq ki, qeyd olunmuş S və T əlifbalarında simvolların nömrələr aşağıdakı kimi təsbit olunmuşdur:

$$T=\{t_1,t_2,...,t_n\} \text{ və } S=\{s_1,s_2,...,s_n\}.$$

Onda F inikası faktiki olaraq $n=|T|=|S|$ ölçülü π yerdəyişməsi ilə verilir. π yerdəyişməsi şifrləmə zamanı açıq mətnin s_i simvolunu şifrmətnin $y_{\pi(i)}$ simvolu ilə əvəz edir. Bu əvəzetmə ya cədvəllə, ya da hər hansı düsturun köməyi ilə verilə bilər. İkinci halda $\pi(i)$ parametrinin qiyməti i-dən asılı olan riyazi ifadə şəklində təqdim olunur.

Əvəzetmə üsullarına bariz nümunə kimi Sezar şifrini göstərmək olar. Bu şifrə əsasən açıq mətnin hər bir hərfi əlifbada ondan bir neçə (məsələn, 3) mövqe sonra dayanan hərflə dəyişdirilir. Bu zaman əlifba dairəvi yazılmış hesab olunur, yəni mətndə əlifbanın sonuncu hərfləri rast gəlindikdə dairəvi prinsiplə əlifbanın əvvəlində olan hərflərlə əvəz olunur. Məsələn, Sezar şifrinə əsasən (sürüşmə – 3) "kriptoqrafiya" sözü "mtqşvrotçhqbç" şifrinə çevrilir.

Ümumi halda Sezar şifrini düstur şəklində də vermək olar. Bunun üçün əlifbanın hərfləri ardıcıl nömrələnir. Məsələn, Azərbaycan əlifbası üçün: a=0, b=1, c=2, ..., z=31. Onda Sezar əvəzetməsini aşağıdakı kimi yazmaq olar:

$$s_i = (t_i + k) \bmod 32,$$

burada t_i – ilkin mətnin simvolunun nömrəsi, s_i şifrmətnin müvafiq simvolunun nömrəsi, k – əlifbada sürüşməni (neçə mövqe sonrakı hərfin götürüləcəyini) göstərən sabit, "mod 32" isə 32-yə (32 – Azərbaycan əlifbasında olan simvolların sayıdır) bölmədə qalığın hesablanması əməliyyatıdır. Burada şifrin açarı k ədədidir.

Yuxarıdakı nümunədə "t" hərfini şifrləmək üçün onun nömrəsinin (t_i=16) üzərinə sürüşməni (k=3) əlavə edərək şifrmətndəki hərfin nömrəsini alırıq:

$s_i=(t_i+3) \bmod 32=(16+3) \bmod 32 =19 \bmod 32=19.$

19 nömrəsi isə əlifbada "v" hərfini göstərir, yəni "t" hərfi "v" hərfi ilə əvəz olunur.

"y" hərfi üçün:

$s_i=(t_i+3) \bmod 32=(30+3) \bmod 32 =33 \bmod 32 =1.$

1 nömrəsi isə əlifbada "b" hərfini göstərir, yəni "y" hərfi "b" hərfi ilə əvəz olunur.

Bu üsulun daha genişlənmiş variantı affin şifrləridir. Affin şifrinə görə N simvoldan ibarət $A=\{a_1,a_2,...,a_N\}$ əlifbası üçün ilkin mətnin hər bir a_i simvolu elə a_j simvolu ilə əvəz olunur ki, $j=(l\cdot i+k) \bmod N$ olsun, burada k – sürüşmə, l isə ixtiyari sabitdir.

Davamlılığı zəif olduğundan sadə əvəzetmə şifrləri hazırda istifadə olunmur. Belə şifrlərin sındırılması ayrı-ayrı simvolların və onların kombinasiyalarının rast gəlinmə tezliklərinin statistik təhlilinə əsaslanır. Belə ki, istənilən dildə müxtəlif hərflərin, onların iki, üç və ya daha çox sayda kombinasiyalarının mətndə təkrarlanmaları xarakterik xüsusiyyətlərə malikdir. Ona görə də aydındır ki, sadə əvəzetmə şifrləməsi zamanı şifrmətndə şifrlənmiş simvolların təkrarlanması açıq mətndə olan təkrarlanmalar ilə üst-üstə düşür. Bu isə şifri çox asanlıqla açmağa imkan verir.

Əvəzetmə şifrlərinin davamlılığını yüksəltmək məqsədilə çoxəlifbalı əvəzetmə üsulundan istifadə olunur. Çoxəlifbalı əvəzetmə prosedurasında əvəzetmələr (əlifbalar) çoxluğu və bu çoxluqların tətbiq olunması ardıcıllığını müəyyən edən paylama funksiyası istifadə olunur. Belə ki, hər hansı simvolun şifrlənməsi zamanı o, şifrləmə açarı və paylama funksiyasının qiyməti ilə müəyyən edilən əlifbadan simvol ilə əvəz edilir.

Çoxəlifbalı əvəzetmə üsulunun xüsusi halı kimi Vijiner şifrini göstərmək olar. Bu üsulda şifrləmə açarı m ədəddən ibarət çoxluq seçilir: $k=(k_1, k_2,..., k_m)$. $T=(t_1, t_2,..., t_n)$ açıq mətninin $S=(s_1, s_2,..., s_n)$ şifrmətninə çevrilməsi üçün ümumiləşdirilmiş Sezar şifrindən istifadə olunur:

$$s_i=(t_i+k_i) \bmod N.$$

Burada N – əlifbanın simvollarının sayıdır. Açarın bütün m simvolu istifadə olunub qurtardıqdan sonra $(m+1)$-ci simvol qismində dairəvi prinsip üzrə açarın birinci simvolu (k_1) götürülür. Faktiki olaraq, açar qismində ilkin açarın simvollarının dövri təkrarlanması şəklində formalaşan sonsuz $k_1, k_2,\ldots, k_m, k_1, k_2,\ldots, k_m,\ldots$ ardıcıllığı istifadə olunur. Belə ardıcıllığı *qamma ardıcıllıq* adlandırırlar. Qamma ardıcıllığın formalaşdırılması (qammalaşdırma) üsullarına növbəti paraqrafda baxılacaqdır.

Çoxəlifbalı əvəzetmə şifrini də sındırmaq kifayət qədər asan olsa da sadə əvəzetmə şifrinə nisbətən bir qədər çətindir.

5.9. Qammalaşdırma üsulları

Qammalaşdırma – ilkin mətnin simvollarının müəyyən qaydada formalaşdırılmış psevdotəsadüfi simvollar ardıcıllığı ilə əlifbanın gücünə (simvollarının sayına) bərabər modulla toplanması yolu ilə çevrilməsini özündə ehtiva edir.

Qammalaşdırma üsulunu, formal olaraq, çoxəlifbalı əvəzetmə üsulları sinfinə aid etmək olar. Lakin reallaşdırılmasının və formal təsvir olunmasının asanlığı baxımından qammalaşdırma üsulu geniş istifadə olunur və ona görə də onları ayrı sinfə ayırırlar.

Qammalaşdırma üsulunun mahiyyəti aşağıdakından ibarətdir. Məxfi k açarının köməyi ilə $g_1, g_2,\ldots, g_i,\ldots$ simvollar ardıcıllığı generasiya olunur. Bu ardıcıllıq qamma adlanır. Şifrləmə zamanı qamma $T=(t_1, t_2,\ldots, t_n)$ açıq mətni ilə üst-üstə qoyulur. Şifrmətnin simvolları açıq mətnin və qammanın uyğun simvolları üzərində aparılmış tərsi olan əməliyyatın köməyi ilə alınır:

$$s_i=t_i \cdot g_i,\ i=1,2,\ldots$$

Tərsi olan əməliyyat qismində əlifbanın gücünə (hərflərinin sayına – N) bərabər modulla toplama

$$s_i=(t_i+k_i) \bmod N$$

və ya açıq mətnin simvollarının ikilik kod şəklində təqdim olunması zamanı 2 moduluna görə mərtəbələrlə toplama (bitlərlə XOR)

$$s_i=t_i \oplus g_i$$

əməliyyatlarından istifadə oluna bilər.

Qammalaşdırmaya əsaslanmış şifrləmə sistemlərinin davamlılığı qammanın xarakteristikalarından – onun uzunluğundan və qammanın simvollarının rast gəlinməsi ehtimallarının paylanmasının müntəzəmliyindən asılıdır.

Bərabər ehtimallı təsadüfi sonsuz qamma ilə qammalaşdırma üsulu daha davamlı hesab olunur. Bu üsullar zəruri olan aşağıdakı üç şərti ödəməlidirlər:

- qammanın bütün simvolları tam təsadüfidir və qammada bərabər ehtimalla rast gəlinirlər;
- qammanın uzunluğu açıq mətnin uzunluğuna bərabərdir və ya ondan uzundur:
- hər bir açar (qamma) yalnız bir mətnin şifrlənməsi üçün istifadə olunur və sonra məhv edilir.

Belə şifr prinsip etibarı ilə sındırıla bilməz, yəni mütləq davamlı olur. Lakin mütləq davamlı şifrlərin tətbiqi çox da

rahat olmadığından praktikada, demək olar ki, istifadə olunmurlar. Adətən, qamma ya təsbit edilmiş uzunluqlu açar ardıcıllığının dövri təkrarlanması yolu ilə alınır, ya da hər hansı qayda ilə (məsələn, psevdotəsadüfi ədədlərin generatorunun köməyi ilə) generasiya olunur. Belə generatorlar, adətən, bir neçə məxfi açar parametrlərini istifadə edən rekurrent riyazi düsturlara əsaslanırlar. Psevdotəsadüfi ədədlərin sadə generatoruna nümunə kimi aşağıdakı rekurrent düsturu göstərmək olar:

$$g_i=(a\cdot g_{i-1}+b) \bmod n,$$

burada g_i – psevdotəsadüfi ədədlər ardıcıllığının i-ci üzvü, a, b, n və g_0 – açar parametrləridir. Bu ardıcıllıq 0-dan m-1-ədək ədədləri əhatə edir. Əgər g_i və g_j elementləri üst-üstə düşərsə, onda növbəti elementlər də üst-üstə düşərlər, yəni $g_{i+1}= g_{j+1}$, $g_{i+2}= g_{j+2}$ və s. Ona görə də $\{g_i\}$ ardıcıllığı dövri ardıcıllıqdır və onun dövri m-dən böyük olmur.

Yuxarıda qeyd olunan düstura görə generasiya olunmuş psevdotəsadüfi ədədlər ardıcıllığının dövrünün maksimal (m-ə bərabər) olması üçün bu düsturun parametrləri aşağıdakı şərtləri ödəməlidir:

- b və m – qarşılıqlı sadə ədədləridir;
- a-1 ədədi m ədədinin istənilən sadə böləninə bölünür;
- əgər m ədədi 4-ə bölünəndirsə, onda a-1 ədədi də 4-ə bölünəndir.

5.10. Yerdəyişmə üsulları

Yerdəyişmə üsulları şifrləmə zamanı müəyyən olunmuş qaydada açıq mətnin simvollarının yerini dəyişir. Bu, o

deməkdir ki, şifrləmə açarının uzunluğu şifrlənən (ilkin) mətnin uzunluğuna bərabər olmalıdır. Məxfi açardan yerdəyişmə üsullarında istifadə üçün əlverişli olan şifrləmə açarını almaq üçün bir sıra üsullar mövcuddur. Belə üsullardan birinin köməyi ilə marşrut yerdəyişməsi adlanan şifrləmə üsulu formalaşdırılır. Bu üsul vasitəsilə şifrmətni almaq üçün açıq mətni hər hansı həndəsi fiqura (məsələn, düzbucaqlıya) müəyyən trayektoriya ilə yazır, sonra isə onu başqa trayektoriya ilə köçürürlər.

Üsulu əyani nümayiş etdirmək üçün aşağıdakı nümunəyə baxaq. Tutaq ki, "kriptoqrafik şifrləmə üsulları" mətnini şifrləmək lazımdır. Onda probelləri nəzərə almadan bu mətni 4x7 ölçülü düzbucaqlı cədvələ sətirlərlə soldan sağa doğru yazaq.

k	r	i	p	t	o	q
r	a	f	i	k	ş	i
f	r	l	ə	m	ə	ü
s	u	l	l	a	r	ı

Şifrmətni almaq üçün bu cədvəldən hərfləri sütunlarla yuxarıdan aşağı hərəkət etməklə yazmaq lazımdır. Onda aşağıdakı mətn alınar: "krfsraruifllpiəltkmaoşərqiüı".

Davamlığının zəif olması baxımından yerdəyişmə şifrləri müasir şifrləmə sistemlərində yalnız digər şifrləmə üsulları ilə kombinasiyada istifadə olunurlar.

Kombinasiya edilmiş şifrləmə üsulları dedikdə özündə bir çox müxtəlif növ şifrləmə proseduralarının ardıcıl tətbiqini ehtiva edən kompleks üsullar başa düşülür.

5.11. Axınla şifrləmə üsulları

Əgər şifrləmə zamanı ilkin mətnin simvolları hər hansı müəyyən alqoritmə uyğun olaraq şifrmətnin müvafiq simvollarına ardıcıl şəkildə çevrilirsə, onda belə sistem axınla şifrləmə sistemi adlanır. Belə alqoritmi ümumi şəkildə aşağıdakı kimi vermək olar:

$$t_i = E_k(s_i).$$

Axınla şifrləmə üsulları qammalaşdırmanın bir növüdür və açıq mətni bit-bit şifrmətnə çevirir. Belə ki, şifrmətnin alınması üçün ilkin mətnin (p_1, p_2,..., p_i,...) bitləri ardıcıllığı (k_1, k_2,..., k_i,...) açar ardıcıllığı bitləri ilə 2 moduluna görə toplanır.

Burada (k_1, k_2,..., k_i,...) açar ardıcıllığı açar ardıcıllığının generatoru tərəfindən generasiya olunur. Alan tərəfdə şifrmətnin ilkin mətnə çevrilməsi üçün o, identik açar ardıcıllığı ilə toplanır.

Axınla şifrləmə alqoritmlərində şifrləmə vahidi bir bitdir. Şifrləmənin nəticəsi əvvəl şifrlənmiş axından asılı olmur. Axınla şifrləmə alqoritmləri axınların ötürülməsi sistemlərində, yəni informasiyanın ötürülməsinin ixtiyari vaxtda başlaması və sona çatması, eləcə də təsadüfən qırılması mümkün olan sistemlərdə tətbiq olunur.

Sistemin davamlılığı açar ardıcıllığının daxili strukturundan tam asılıdır. Əgər generator kiçik dövrə malik ardıcıllıq verirsə, onda davamlılıq yüksək olmur. Əksinə, generator sonsuz ardıcıllıq verirsə, onda ideal davamlılığa malik bir dəfə istifadə olunan bloknot alınar.

Axınla şifrləmənin real davamlılığı çoxəlifbalı əvəzetmə şifrinin davamlılığı ilə bir dəfə istifadə olunan bloknotun davamlılığı arasında dəyişir.

5.12. Bloklarla şifrləmə üsulları

Bloklarla şifrləmə zamanı ilkin mətn bloklara (uzunluğu təsbit olunmuş hissələrə) bölünür, şifrləmə alqoritmi blokları ardıcıl şəkildə, bloklara daxil olan simvolların hamısını isə eyni zamanda şifrləyir. Belə ki, bloklarla şifrləmə üsulları ilkin mətnin bloklarının tərsi olmayan çevrilmələri ailəsini təşkil edir. Bloklarla şifrləmə üsulu, faktiki olaraq, blokun əlifbası çərçivəsində əvəzetmə üsulundan ibarətdir. Bu çevirmə bloklarla şifrləmə rejimindən asılı olaraq birəlifbalı və ya çoxəlifbalı ola bilər.

Bloklarla şifrləmə sistemlərində şifrləmə vahidi bir neçə baytdan (4-dən 32-yə qədər) ibarət olur. Blokun şifrlənməsinin nəticəsi həmin blokun bütün ilkin baytlarından asılı olur.

Bloklarla şifrləmə üsullarının əvəzetmə üsullarının xüsusi halı olmasına baxmayaraq, aşağıdakı səbəblərdən onlarına ayrıca baxılır. Əvvəla, informasiyanın ötürülməsi sistemlərində istifadə olunan simmetrik şifrlərin əksəriyyəti bloklarla şifrləmə üsullarıdır. İkincisi, adi əvəzetmə üsullarından fərqli olaraq, bloklarla şifrləmə üsullarını alqoritmik şəkildə təsvir etmək çox rahatdır.

Bloklarla şifrləmə üsullarına qoyulan əsas tələbləri aşağıdakı kimi formalaşdırmaq olar:

- bloklar kataloqunun tərtib edilməsi və saxlanılmasını çətinləşdirmək məqsədilə onların uzunluğunun kifayət qədər böyük (64 və ya ondan böyük) olması;
- kənar şəxslər tərəfindən açarların seçilməsi imkanlarını aradan qaldırmaq məqsədilə açarlar fəzasının kifayət qədər böyük olması;
- ilkin və şifrlənmiş mətnlərin uyğunluğuna əsasən ilkin mətnin və ya açarın müəyyən edilməsinin analitik və ya statistik üsullarının reallaşdırılmasının mümkün qədər qarşısının alınması üçün ilkin və şifrlənmiş mətnlər arasında əlaqələrin mürəkkəb olması.

Bloklarla şifrləmə üsullarının ciddi çatışmazlıqlarından biri ondan ibarətdir ki, açıq mətnin bir-birinin eyni olan blokları şifrmətndə də bir-birinin eyni olan bloklara çevrilir. Aydındır ki, bu amil bloklarla şifrləmə üsulunun davamlılığını aşağı salır. Belə ki, əgər rəqibin əlinə uyğun şifrmətnlə birlikdə ilkin mətnin nümunəsi düşərsə, onda o, analoji blokları olan şifrmətnləri asanlıqla hissə-hissə açа bilər.

Belə çatışmazlığın aradan qaldırılması üçün blokların qarışdırılması rejimindən istifadə olunur. Bu rejimdə növbəti blokun şifrlənməsi zamanı açıq mətnin əvvəlki blokları da istifadə olunur. Məsələn, açıq mətnin cari bloku şifrmətnin əvvəlki bloku ilə iki moduluna görə bitlərlə toplanır və sonra nəticəyə şifrləmə alqoritmi tətbiq edilir. Burada ilkin blok qismində ya yalnız sıfırlardan ibarət blok, ya da təsadüfi seçilən blok istifadə olunur. İkinci halda təsadüfi blok şifrmətnə əlavə edilir.

Belə proseduraların tətbiqi şifrmətnin bütün növbəti bloklarının açıq mətnin əvvəlki bloklarından asılılığını təmin edir. Ona görə də açıq mətnin hər hansı blokunun

dəyişdirilməsi şifrmətnin yalnız uyğun blokunun deyil, onun bütün sonrakı bloklarının dəyişməsinə gətirib çıxarır.

İxtiyari uzunluqlu ilkin mətnlərin şifrlənməsi üçün bloklarla şifrləmə üsulları bir sıra rejimlərdə istifadə oluna bilər. Kriptoqrafik şifrləmə sistemlərində bloklarla şifrləmə üsullarının tətbiqi üçün aşağıda qeyd olunan dörd rejim daha tez-tez rast gəlinir:

Elektron kodlaşdırma kitabı (ECB – Electronic Code Book). Bu rejimdə ilkin mətnin hər bir bloku digər bloklardan asılı olmadan bloklarla şifrləmə üsulu vasitəsilə şifrlənir. Onun davamlılığı şifrləmənin davamlılığına bərabərdir. Lakin bu zaman ilkin mətnin quruluşu gizlədilmir. İlkin mətnin eyni məzmunlu bloklarının şifrlənməsi nəticəsində şifrmətndə də eyni bloklar yaranır. Blokların pozulması, təkrarlanması və ya yerlərinin dəyişdirilməsi yolu ilə ilkin mətnlə manipulyasiya etmək mümkündür. Burada şifrləmənin sürəti bloklarla şifrləmənin sürətinə bərabərdir.

Şifrlənmiş mətnin bloklarının qarışdırılması (CBC – Cipher Block Chaining) *rejimi*. Bu rejimdə ilkin mətnin hər bir bloku şifrlənmiş mətnin əvvəlki bloku ilə 2 moduluna görə mərtəbələr üzrə toplanır, sonra isə şifrlənir. Şifrləmə prosesinin başlanması üçün açıq şəkildə rabitə kanalına ötürülən başlanğıc vektordan istifadə olunur.

CBC rejiminin davamlılığı onun əsasını təşkil edən bloklarla şifrləmə üsulunun davamlılığına bərabərdir. Bundan əlavə, açıq mətnin növbəti bloku ilə şifrlənmiş mətnin əvvəlki blokunun toplanması hesabına açıq mətnin strukturu gizlədilir. Açıq mətnlə birbaşa manipulyasiya mümkün olmadığından CBC rejimində şifrləmənin da-

vamlılığı bir qədər yüksəlir. CBC rejimində şifrləmənin sürəti isə bloklarla şifrləmə üsulunun sürətinə bərabərdir.

Praktikada CBC rejiminin modifikasiyaları mövcuddur.

- *Şifrlənmiş mətnin bloklarının paylanma ilə qarışdırılması* (PCBC – Propagating Cipher Block Chaining) *rejimi* – CBC rejimindən fərqli olaraq, bu rejimdə ilkin mətnin cari bloku şifrlənən zaman o, şifrlənmiş mətnin əvvəlki bloku ilə yanaşı ilkin mətnin əvvəlki bloku ilə də toplanır.
- *Şifrlənmiş mətnin bloklarının nəzarət cəmi ilə qarışdırılması* (CBCC – Cipher Block Chaining with Cheksum) *rejimi* – cari blok şifrlənən zaman ona ilkin mətnin bütün əvvəlki blokları 2 moduluna görə mərtəbələrlə əlavə edilir. Bu, ötürülən mətnin tamlığını çox da böyük olmayan əlavə məsrəflər hesabına nəzarətdə saxlamağa imkan verir.

Şifrlənmiş mətnə görə əks əlaqənin tətbiqi (CFB – Cipher Feedback) *rejimi*. Bu rejimdə şifrlənmə üçün şifrmətnin əvvəlki bloku təkrarən şifrlənir, alınmış nəticə ilkin mətnin cari bloku ilə 2 moduluna görə toplanır, sonra isə şifrlənir. Şifrləmə prosesinin başlanması üçün başlanğıc vektordan istifadə olunur.

CBF rejiminin davamlılığı onun əsasını təşkil edən bloklarla şifrləmə üsulunun davamlılığına bərabərdir. Açıq mətnin növbəti blokunun şifrlənmiş mətnin əvvəlki bloku ilə 2 moduluna görə mərtəbələrlə toplanması hesabına açıq mətnin strukturu gizlədilir. Şifrlənmiş mətndən ilk və sonuncu blokların silinməsi yolu ilə açıq mətnlə manipulyasiya mümkün olmur. CBC rejimində şifrləmənin davamlılığı bir qədər yüksəlir. CBC rejimində şifrləmənin sürəti isə bloklarla şifrləmə üsulunun sürətinə bərabərdir.

Əgər şifrlənmiş mətnin iki bloku eynidirsə, onda CBF rejimində növbəti addımda onların şifrlənməsinin nəticəsi də eyni olacaqdır ki, bu da ilkin mətn haqqında əlavə məlumatın sızmasına gətirib çıxara bilər. Bu rejimdə də şifrləmənin sürəti isə bloklarla şifrləmə üsulunun sürətinə bərabər olur. CBF rejimində şifrin açılması zamanı rast gəlinən hər hansı səhv bit növbəti blokların şifrlərinin səhv açılmasına gətirib çıxarır.

Çıxışa görə əks əlaqə (OFB – Output Feedback) *rejimi*. Bu rejim CBF rejimi ilə eynilik təşkil edir, lakin burada ilkin mətnin şifrlənən bloku ilə 2 moduluna görə toplanan kəmiyyət ilkin və şifrlənmiş mətnlərdən asılı olmadan generasiya olunur. Bu rejimdə də şifrləmə prosesinin başlanması üçün başlanğıc vektor istifadə olunur. CBF rejimi ilə müqayisədə OFB rejimi aşağıdakı üstünlüyə malikdir: ötürmə prosesində bitlər səviyyəsində meydana çıxan istənilən səhv növbəti blokların şifrinin açılmasına təsir etmir. Lakin şifrlənmiş mətinin dəyişdirilməsi yolu ilə ilkin mətn üzərində sadə manipulyasiya aparmaq mümkündür. Praktikada bu rejimin çıxışa görə xətti funksiya ilə əks əlaqə modifikasiyası mövcuddur.

Bloklarla şifrləmə üsulları hazırda praktikada daha geniş yayılmış üsullardır. Onlara nümunə kimi aşağıdakıları göstərmək olar:

- *məlumatların kriptoqrafik şifrlənməsinin Amerika standartı – DES* (Data Encryption Standard). 1978-ci ildə qəbul edilmişdir. Bu şifr aparat və proqram vasitələri şəklində effektiv reallaşdırıla bilər. Bu zaman saniyədə bir neçə meqabayta qədər şifrləmə sürətini əldə etmək mümkündür.

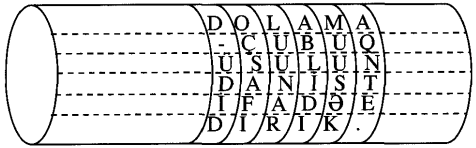
- *məlumatların kriptoqrafik şifrlənməsinin yeni Amerika standartı – AES* (Advanced Encryption Standard). 2000-ci ildə qəbul edilmiş və onun əsası kimi Rijndeal alqoritmi seçilmişdir. Bu şifr aparat və proqram vasitələri şəklində effektiv reallaşdırıla bilər. Bu zaman saniyədə bir neçə meqabayta qədər şifrləmə sürətini əldə etmək mümkündür.
- *RC6 alqoritmi.* RSA Data Security, İnc. şirkəti tərəfindən AES standartı üçün alqoritm qismində təklif olunmuş və seçimlərdə ikinci turu keçmişdir.
- *ГОСТ 28147–89 Rusiya şifrləmə standartı.* Rusiya Federasiyasında informasiya emalı sistemlərində məlumatların şifrlənməsi üçün qəbul edilmiş vahid standartdır. O, bütün dövlət və hökumət orqanları, bank sistemləri və dövlətin informasiya təhlükəsizliyinin təmin edilməsi üzrə fəaliyyətlə məşğul olan bütün təşkilatlar üçün məcburi, digər təşkilatlar və fərdi şəxslər üçün tövsiyəvi xarakter daşıyır. Aparat və proqram vasitələri şəklində reallaşdırılmaq üçün nəzərdə tutulmuşdur, qorunan informasiyanın məxfilik dərəcəsinə məhdudiyyətlər qoymur və kriptoqrafik tələbləri ödəyir.

5.13. Sadə şifrləmə üsullarının nümunələri

5.13.1. *Dolama-çubuq.* Eramızdan əvvəl V-IV əsrlərdə Spartada və Yunanıstanda bizə məlum olan ilk kriptoloji qurğudan – verilmiş (məxfi) diametrli dolama-çubuqdan istifadə edirdilər. Şifrləmə üçün əvvəlcə uzun nazik papirus zolağını həmin çubuğun üzərinə ara qoymadan dolayır, sonra şifrlənən mətni çubuq boyu papirusun üzərinə yazırdılar. Bundan sonra çubuqdan açılan papirus üzərində şifrlənmiş yazı alınır. Dolama-çubuq üsulu yerdəyişmə şifrləmə üsullarına aiddir.

Şifrin açarı: çubuğun diametri.

Məsələn, dolama-çubuq üzərinə dolanmış lentin 6 zolağında 6 sətirdə "DOLAMA-ÇUBUQ ÜSULUNDAN İS-TİFADƏ EDİRİK" mətnini aşağıdakı kimi yazmaq olar (şək.5.5).



Şək.5.5. Dolama-çubuğun təxmini görünüşü

Papirus zolağı açıldıqdan sonra lentin üzərində

"D-ÜDİDOÇSAFİLUUNARABLİDİMUUSƏKAQNTE."

şifrmətni alınar.

Burada lent üzərində kəsilməz yazı (arası kəsilən yazı çubuğun diametrinin tapılmasını, yəni şifrin açılmasını asanlaşdırır) almaq üçün yazı çubuğun bütün çevrəsi boyu lent üzərinə yazılmalıdır. Sətirlərin və sətirlərdə simvolların sayı elə seçilməlidir ki, yazı çubuğun çevrəsi boyu bərabər paylanmış olsun.

Tutaq ki, N hərfdən ibarət yazı çubuğun çevrəsi boyu K sətirdə yazılır. Onda hər sətirdə olan simvolların sayı

M=INT(N/K)+1 olar. Əgər sonuncu sətirdə boş yerlər qalarsa, onda həmin yerlər ixtiyari hərflərlə doldurulur.

5.13.2. *Qoşa disk.* Eramızdan əvvəl IV əsrdə romalılar şifrləməni sadələşdirmək üçün eyni oxa malik iki diskdən istifadə edirdilər. Disklərin üzərinə əlifbanın hərflərini təsadüfi, lakin bir-birindən fərqli ardıcıllıqla yazırdılar. Mətni şifrləmək üçün onun hər bir hərfini bir diskin üzərində taparaq digər diskdə həmin hərfin qarşısında duran hərflə əvəz edirdilər. Göründüyü kimi, bu şifr əvəzetmə üsulları sinfinə aiddir.

Şifrin açarı: əvvəlcədən hazırlanmış disklər.

5.13.3. *Bibliya kodu.* Bəzi mütəxəssislərin fikirlərinə görə bibliyanın tərkibində açıq mətnin içərisində gizli məlumatlar verilmişdir. Gizli məlumatın ümumi mətnin tərkibində verilməsi üçün hərflərin yazıda ekvidistant ardıcıllığı prinsipindən istifadə olunmuşdur.

Ekvidistant ardıcıllıq dedikdə mətndə hər hansı hərfdən başlayaraq müəyyən addımlarla (məsələn, beş hərfdən bir) hərflər götürülməklə məlumatların yazılması başa düşülür. Məsələn, bu bəndin ilk üç sətrində "Bəzi" sözünün birinci hərfindən başlayaraq hər 13-cü hərfi (probellər və durğu işarələri nəzərə alınmaqla) götürdükdə "Bilik milli..." məlumatı alınar.

Şifrin açarı: gizli məlumatın başlanğıcının açıq mətndə mövqeyi və hərflərarası addım.

5.13.4. *Polibiy kvadratı.* Eramızdan əvvəl ikinci əsrdə yunan yazıcısı və tarixçisi Polibiy 5x5 ölçülü kvadrat şifrləmə cədvəli icad etmişdi. Bu cədvəl ixtiyari əlifba ilə

(məsələn, yunan əlifbasının 24 hərfi və bir boş yer; iki "i" və "j" hərflərini bir xanada yazmaq şərti ilə latın əlifbasının 26 hərfi) doldurulur.

Mətnin şifrlənməsi üçün onun hər bir hərfi kvadrat cədvəldə tapılır və bu hərfin əvəzinə cədvəldə ondan aşağıdakı sətirdə eyni sütunda yerləşən hərf yazılır. Hərf sonuncu sətirdə yerləşərsə, onun əvəzinə həmin sütunda birinci sətirdə yerləşən hərf götürülür. Şifrləmə üsulu əvəzetmə sinfinə aiddir.

Şifrin açarı: kvadratın ölçüsü və əlifba.

Məsələn, latın əlifbası üçün

A	B	C	D	E
F	G	H	I,J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

kvadratını götürsək, "KRİPTOQRAFİYA" sözünün şifrkodu "PWOUTVWFODF" olar.

5.13.5. *Nömrələnmiş kvadrat.* Yunanlar və romalılar gizli əlaqə üçün əlifbanın hərfləri ilə ardıcıl doldurulmuş və nömrələnmiş Polibiy kvadratından istifadə edirdilər. Belə ki, əlifbanın hərfləri ilə doldurulmuş Polibiy kvadratının sətirləri və sütunları 1-dən 5-dək nömrələnir.

Mətnin şifrlənməsi üçün onun hərfləri kvadratda tapılır və hərfin əvəzinə onun yerləşdiyi sətrin və sütunun nömrələri cütü yazılır. Bu üsul əvəzetmə şifrləri sinfinə aiddir.

Şifrin açarı: sütunları və sətirləri nömrələnmiş kvadrat.

Məsələn, latın əlifbası üçün düzəldilmiş

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

kvadrata əsasən "KRİPTOQRAFİYA" sözünün şifrkodu "25 42 24 35 44 34 41 42 11 21 24 54 11" olar.

5.13.6. *"Atbaş" şifrləməsi.* Hələ qədim dövrlərdə yəhudilər dini mətnlərini sadə əvəzetmə yolu ilə şifrləyirdilər. Belə ki, əlifbanın birinci hərfinin əvəzinə sonuncu hərfini, ikinci hərfinin əvəzinə sonuncudan əvvəlki hərfi və s. yazırdılar. Belə şifri "atbaş" adlandırırdılar.

Əvəzetmə sinfinə aid edilən şifrin açarı: əlifba və onun hərfləri ardıcıllığı.

İeremiya peyğəmbər kitabında yazır: "... ÇAR CECCAXA ONLARDAN SONRA İÇƏCƏK". Lakin tarixdə belə çar və ya çarlıq ümumiyyətlə heç vaxt mövcud olmamışdır. Qeyd olunan əvəzetmə üsulu ilə şifrlənmiş "CECCAXA" kodunun açılması nəticəsində "VAVİLON" alınmışdır.

5.13.7. *Sezar şifri.* Bizim eranın I əsrində Yuli Sezar senata göndərdiyi məktubları hərfləri əlifbada 3 mövqe sürüşdürmə yolu ilə şifrləyirdi. Belə ki, bu zaman mətnin hər bir hərfi əlifbada ondan sonra üçüncü mövqedə duran hərflə əvəz olunurdu. Əgər hərf əlifbanın sonunda yerləşirdisə və ondan sonra üç hərf yox idisə, onda dairəvi prinsiplə əlifbanın əvvəlinə keçir və sıranın növbəti hərfləri

kimi oradakı hərflərdən istifadə olunurdu. Aydındır ki, şifr əvəzetmə üsulları sinfinə daxildir.

Şifrin açarı: əlifba və sürüşmə.

Məsələn, latın əlifbası üçün Sezar "VENI VEDI VICI" (Gəldim, gördüm, qalib gəldim) ifadəsini əlifbada 3 hərf sağa sürüşdürməklə "YHQL YHGL YLFL" kimi şifrləmişdi.

Beləliklə, Sezarın sadə əvəzetmə cədvəlini aşağıdakı kimi təsvir etmək olar:

İlkin mətnin hərfləri

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Şifrmətnin hərfləri

Eramızın I əsrində imperator Avqust şifrləmə üçün mətnin hərflərini əlifbada növbəti hərflə əvəz edirdi:

İlkin mətnin hərfləri

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A

Şifrmətnin hərfləri

5.13.8. *Sütunların (sətirlərin) transpozisiyası.* Məlumatın şifrlənməsi üçün hərflərinin yerdəyişməsi üçün sadə *MxN* ölçülü şifrləmə cədvəlindən istifadə edilir. Burada *M* – cədvəlin sətirlərinin sayı, *N* isə sütunlarının sayıdır. Şifrləmə üçün məlumat cədvəlin içərisinə sətirlərlə (və ya sütunlarla) yazılır və sütunlarla (və ya sətirlərlə) oxuyurlar. Beləliklə, ilkin məlumatın hərfləri yerlərini dəyişmiş olur.

Şifrləmənin açarı: cədvəlin ölçüsü.

Məsələn, "MƏLUMATIN SADƏ ŞİFRLƏNMƏSİ" cümləsini 4x6 ölçülü cədvəl vasitəsilə aşağıdakı kimi şifrləmək olar. Məlumat cədvələ sətirlərlə yazılır:

M	Ə	L	U	M	A
T	I	N	S	A	D
Ə	Ş	İ	F	R	L
Ə	N	M	Ə	S	İ

Belə cədvəldə yazılmış məlumatı sütunlarla oxuduqda

"MTƏƏƏIŞNLNİMUSFƏMARSADLİ"

şifri alınar.

5.13.9. *Marşrut transpozisiyası.* Bu üsul əvvəlki bənddə baxılan üsulun modifikasiyasıdır. Belə ki, məlumat cədvələ spiral üzrə yazılır və spiralın istiqamətindən asılı olaraq sətir və ya sütunlar üzrə oxunur.

Şifrin açarı: cədvəlin ölçüsü və spiralın istiqaməti.

Məsələn, əvvəlki nümunədə olan mətnə bu üsul tətbiq edildikdə

M	Ə	L	U	M	A
F	R	L	Ə	N	T
İ	İ	S	Ə	M	I
Ş	Ə	D	A	S	N

"MFİŞƏRİƏLLSDUƏƏAMNMSATIN"

şifri alınar.

5.13.10. *Açara görə sətirlərin (və ya sütunların) yerdəyişməsi.* Şifrləmə üçün *MxN* ölçülü cədvəl və *M* və ya *N* simvollu açar söz tələb olunur. Belə ki, əvvəlcə məlumat cədvələ yazılır. Cədvəlin üstündən (və ya qarşısından) *M* (və ya *N*) hərfli açar söz yazılır. Açar sözün hərfləri əlifbada rast gəlinmə ardıcıllığına uyğun olaraq nömrələnir. Əgər açar sözdə hər hansı hərf birdən artıq sayda olarsa, onda onlar sözdə rast gəlinmə ardıcıllığına görə nömrələnir. Bundan sonra açar sözün hərfləri onların nömrələrinə görə düzülür və uyğun sütunların (sətirlərin) yerləri də müvafiq qaydada dəyişdirilir. Bu zaman məlumat cədvələ sətirlər və ya sütunlar üzrə doldurula bilər.

Şifrləmənin açarı: cədvəlin ölçüsü və açar söz.

Məsələn, 8-ci nümunədəki cədvəl və mətni, eləcə də "QARTAL" açar sözünü götürək. Qeyd olunmalıdır ki, açar sözlərin hərflərinin sayı (*N*=6) cədvəlin sütunlarının sayına bərabər olduğuna görə şifrləmə zamanı cədvəlin sütunlarının yerdəyişməsindən istifadə olunacaq.

Birinci addımda məlumat sütunlarla cədvələ doldurulur, açar söz cədvəlin yuxarısında yazılır və onun hərfləri nömrələnir:

Açar söz	Q	A	R	T	A	L
Hərflərin nömrəsi	3	1	5	6	2	4
Şifrlənən məlumat	M	M	N	Ə	R	M
	Ə	A	S	Ş	L	Ə
	L	T	A	İ	Ə	S
	U	I	D	F	M	İ

İkinci addımda açar sözün hərflərinin nömrələrinə uyğun olaraq cədvəlin sütunlarının yerləri dəyişdirilir:

Açar söz	A	A	Q	L	R	T
Hərflərin nömrəsi	1	2	3	4	5	6
Şifrlənən məlumat	M	R	M	M	N	Ə
	A	L	Ə	Ə	S	Ş
	T	Ə	L	S	A	İ
	I	M	U	İ	D	F

Üçüncü addımda dəyişdirilmiş cədvəldən sətirlər üzrə hərflər köçürülür və şifr mətn alınır:

"MRMMNƏALƏƏSŞTƏLSAİIMUİDF".

Eyni məlumatın şifrlənməsini sətirlərin yerdəyişməsinə görə də yerinə yetirmək olar. Tutaq ki, "ŞİFR" açar sözdür. Birinci addımda

Açar söz	Hərflərin nömrələri	Şifrlənən məlumat					
Ş	4	M	Ə	L	U	M	A
İ	2	T	I	N	S	A	D
F	1	Ə	Ş	İ	F	R	L
R	3	Ə	N	M	Ə	S	İ

cədvəli tərtib olunur. İkinci addımda cədvəl

Açar söz	Hərflərin nömrələri	Şifrlənən məlumat					
F	1	Ə	Ş	İ	F	R	L
İ	2	T	I	N	S	A	D
R	3	Ə	N	M	Ə	S	İ
Ş	4	M	Ə	L	U	M	A

şəklini alır. Üçüncü adımda cədvəldən hərflər sütunlar üzrə oxunduqda aşağıdakı şifr alınar:

"ƏTƏMŞINƏİNMLFSƏURASMLDİA".

5.13.11. *Sətir və sütunların ikiqat yerdəyişməsi.* Burada məlumat cədvələ doldurulduqdan sonra əvvəlki nümunədə göstərilən hər iki (sətrə və sütuna görə) yerdəyişmə ardıcıl

tətbiq olunur. Sətrə və sütuna görə yerdəyişmənin ardıcıllığının fərqi yoxdur.

Şifrləmənin açarı: cədvəlin ölçüsü və iki ədəd açar söz.

Məsələn, əvvəlki nümunədəki məlumatı, açar sözləri götürək. Məlumatı sütunlar üzrə yazaraq həmin ölçüdə cədvələ aşağıdakı kimi tərtib edək:

		Q	A	R	T	A	L
		3	1	5	6	2	4
Ş	4	M	M	N	Ə	R	M
İ	2	Ə	A	S	Ş	L	Ə
F	1	L	T	A	İ	Ə	S
R	3	U	I	D	F	M	İ

Birinci mərhələdə birinci acar sözə görə sütunların yerdəyişməsi aparılır:

		A	A	Q	L	R	T
		1	2	3	4	5	6
Ş	4	M	R	M	M	N	Ə
İ	2	A	L	Ə	Ə	S	Ş
F	1	T	Ə	L	S	A	İ
R	3	I	M	U	İ	D	F

İkinci mərhələdə ikinci açar sözə görə sətirlərin yerdəyişməsi həyata keçirilir:

		A	A	Q	L	R	T
		1	2	3	4	5	6
F	1	T	Ə	L	S	A	İ
İ	2	A	L	Ə	Ə	S	Ş
R	3	I	M	U	İ	D	F
Ş	4	M	R	M	M	N	Ə

Üçüncü mərhələdə cədvəldən hərflər sətirlər üzrə oxunur və aşağıdakı şifrmətn alınır:

"TƏLSAİALƏƏSŞIMUİDFMRMMNƏ".

5.13.12. *Sehrli kvadrat.* Sehrli kvadrat dedikdə xanalarında 1-dən 9-a, 16-ya, 25-ə və s. qədər ədədlər yazılmış elə 3, 4, 5 və s. ölçülü kvadrat cədvəllər nəzərdə tutulur ki, həmin kvadratın sətir, sütun və diaqonalları üzrə xanalarda yazılmış ədədlərin cəmi bərabər olsun.

Məsələn, 5x5 ölçülü cədvəldə 1-dən 25-ə qədər olan ədədləri aşağıdakı kimi yazmaq olar:

11	24	7	20	3
4	12	25	8	16
17	5	13	21	9
10	18	1	14	22
23	6	19	2	15

Bu cədvəldə bütün sətirlər, sütunlar və diaqonallar üzrə ədədlərin cəmi 65-ə bərabərdir.

Şifrləmə üçün ilkin mətndə olan hərflər sıra nömrəsinə uyğun olaraq, kvadratdakı ədədlərin yanında yazılır, sonra isə kvadratın sətirləri və ya sütunları üzrə oxunur.

Şifrləmə açarı: sehrli kvadratın ölçüsü və ədədlərin düzülüşü.

Məsələn, "ÜSUL SEHRLİ KVADRAT ŞİFRİDİR" mətninin sehrli kvadrat şifrinin köməyi ilə şifrlənməsinə baxaq. Əvvəlcə mətnin hərfləri nömrələnir:

Ü	S	U	L	S	E	H	R	L	İ	K	V	A
1	2	3	4	5	6	7	8	9	10	11	12	13

D	R	A	T	Ş	İ	F	R	İ	D	İ	R
14	15	16	17	18	19	20	21	22	23	24	25

Mətnin hərfləri 5x5 ölçülü sehrli kvadrata yazılır:

11 K	24 İ	7 H	20 F	3 U
4 L	12 V	25 R	8 R	16 A
17 T	5 S	13 A	21 R	9 L
10 İ	18 Ş	1 Ü	14 D	22 İ
23 D	6 E	19 İ	2 S	15 R

Sonda sehrli kvadratın xanalarında olan hərflər sütunlar üzrə köçürülür və

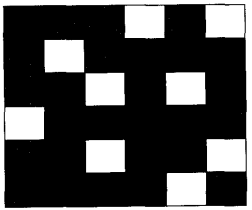
"KLTİDİVSŞEHRAÜİFRRDSUALİR"

şifri alınır.

5.13.13. *Kardanonun sehrli kvadratı.* Kardano kvadratı – sətir və sütunlarının sayı cüt olan kvadrat cədvəldir. Onun xanalarının dörddəbiri (25%) elə şəkildə kəsilib çıxarılır ki, belə kvadratı dörd dəfə 90° fırlatmaqla ilkin kvadratın bütün xanalarını örtmək mümkün olsun. Xanaları kəsilmiş kvadrat *trafaret* və ya *qəfəs* adlanır. Şifrləmə üçün trafaret kvadratın üzərinə qoyulur və mətnin hərfləri sətirlər üzrə kəsik xanalara yazılır, sonra trafaret 90° fırladılır və növbəti hərflər kəsik xanalara yazılır. Bu proses kvadratın bütün xanaları dolanadək davam etdirilir.

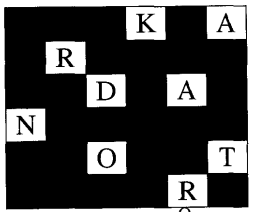
Şifrin açarı: kvadratın ölçüsü və trafaret.

Tutaq ki, "KARDANO TRAFARET VASİTƏSİLƏ ŞİFRLƏYİRDİ" mətni verilmişdir. Aşağıdakı şəkildə trafaret götürək.

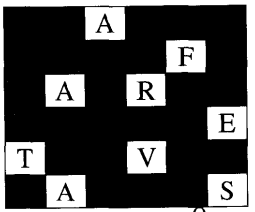


Kardano trafareti

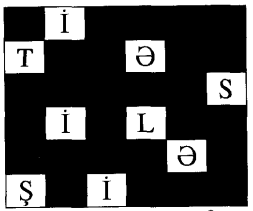
Bu trafaretin kəsilmiş xanalarında sətirlər üzrə yazıb 90^{o} fırlatmaqla dörd mərhələdə ilkin kvadrat doldurulur.



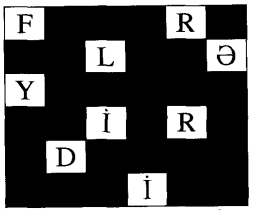
I mərhələ (0^{o})



II mərhələ (90^{o})



III mərhələ (180^{o})



IV mərhələ (270^{o})

Nəticədə kvadrat aşağıdakı şəkildə doldurulmuş olur:

F	İ	A	K	R	A
T	R	L	Ə	F	Ə
Y	A	D	R	A	S
N	İ	İ	L	R	E
T	D	O	V	Ə	T
Ş	A	İ	İ	R	S

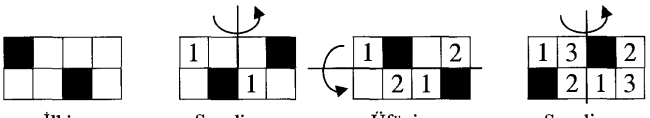
və hərflər kvadratdan sətirlərlə oxunmaqla

"FİAKRATRLƏFƏYADRASNİİLRETDOVƏTŞAİİRS"

şifrmətni alınar.

Bu üsulda 90^{o} fırlatma əvəzinə üfüqi və şaquli oxlara görə 180^{o} çevirmədən istifadə oluna bilər.

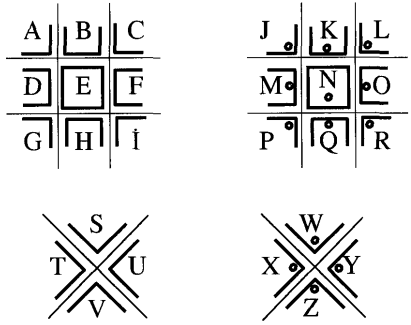
Bu üsulda, həmçinin, kvadrat əvəzinə düzbucaqlı cədvəldən istifadə etmək olar, lakin bu zaman yalnız 180^{o} çevirmələr tətbiq edilə bilər. Məsələn, əvvəlcə şaquli oxa görə çevirmə, sonra üfüqi oxa görə çevirmə, yenidən şaquli oxa görə çevirmə. Əyani nümayiş etdirmək üçün 2x4 ölçülü düzbucaqlı cədvəlin çevrilməsinə baxaq.



İlkin vəziyyət | Şaquli oxa görə 180^{o} | Üfüqi oxa görə 180^{o} | Şaquli oxa görə 180^{o}

5.13.14. *Pigpen şifri.* Bu şifrə əsasən ilkin məlumatın hərfləri simvollarla əvəz olunur. Belə ki, əlifbanın hərfləri əvvəlcədən xüsusi formalı cədvəllərin (şəbəkənin) xanalarına yazılır və onların tutduğu mövqeyə uyğun olaraq şəbəkənin hissəsi ilə işarə olunur.

Tutaq ki, əlifbanın (ingilis əlifbasının) hərfləri aşağıdakı şəkildə şəbəkələrə yerləşdirilmişdir.



Beləliklə, şifrin açarı aşağıdakı kimi olar:

A	B	C	...	M	N	...	X	Y	Z
⌟	⌴	⌞	...	⌝	◘	...	⟩	⟨	^

5.13.15. *Sadə əvəzetmə şifri.* Orta əsrlərdə tacirlər tərəfindən gəlib çatma tarixini, vaxtını, malların qiymətini şifrləyərək ötürmək üçün istifadə olunurdu. Tacirlər açar sözü əvvəlcədən razılaşdıraraq, onun hərflərini sıra ilə rəqəmlərlə nömrələyirdilər. Burada açar sözün hərflərinin sayı rəqəmlərin sayına uyğun olmalıdır. Şifrləmə üçün məlumatda olan tarix, qiymət və s. rəqəmlər açar sözün müvafiq hərfi ilə əvəz olunurdu.

Şifrin açarı: açar söz.

Məsələn, aşağıdakı açar söz verilmişdir:

Açar söz	–	A	Z	Ə	R	B	A	Y	C	A	N
İlkin mətnin rəqəmləri	–	0	1	2	3	4	5	6	7	8	9

Onda "QİYMƏT 148650 MANATDIR" mətni "QİYMƏT ZBAYAA MANATDIR" şifrmətni şəklinə çevrilmiş olar.

5.13.16. *Qronefeld şifri.* Mürəkkəb çoxəlifbalı şifr olan bu üsul Sezar şifrinin modifikasiyasıdır və şifrləmə üçün ədədi açardan istifadə edir. Belə ki, açarın rəqəmləri şifrləmə zamanı ilkin mətnin hərflərinin əlifbada sürüşməsini müəyyən edir.

Şifrin açarı: ədədi açar.

Tutaq ki, "MÜRƏKKƏB ÇOXƏLİFBALI ŞİFR" mətni və "71935" açarı verilmişdir. Açarın rəqəmləri ardıcıl olaraq ilkin mətnin hərflərinin altına yazılır:

M	Ü	R	Ə	K	K	Ə	B		Ç	O	X	Ə	L	İ	F	B	A	L	I		Ş	İ	F	R
7	1	9	3	5	7	1	9		3	5	7	1	9	3	5	7	1	9	3		5	7	1	9

Şifrləmə zamanı "M" hərfi əlifbada ondan 7 mövqe, "Ü" hərfi – 1 mövqe, "R" hərfi – 9 mövqe sonrakı hərflə və s. əvəz olunur. Beləliklə, qeyd olunan mətnin şifri aşağıdakı kimi olar:

"ŞVAĞOPFH ƏŞMFTQIGBTK YOGA".

5.13.17. *Vijiner cədvəli.* XVI əsrdə yaşamış kriptoqrafik sistemlərin təkmilləşdirilməsi ilə məşğul olan diplomat Vijinerin adı ilə bağlıdır. O, şifrləmə üçün açar sözdən və əlifbanın hərflərinin sayına (*N*) bərbər ölçüdə xüsusi şəkildə yaradılmış kvadrat cədvəldən istifadə olunur. Cədvəlin sətir və sütunları əlifbanın hərfləri ilə nömrələnir və aşağıdakı kimi doldurulur:

- I sətir: əlifbanın *N* hərfi əvvəldən axıradək xanalara yazılır;

- II sətir: ilk N-1 xanaya əlifbanın ikinci hərfdən başlayaraq sonadək bütün hərfləri, N-ci xanaya isə əlifbanın birinci hərfi yazılır;

...

- N-ci sətir: birinci xanaya əlifbanın N-ci hərfi və ikinci xanadan başlayaraq əlifbanın ilk N-1 hərfi yazılır.

Şifrləmə zamanı ilkin mətn bir sətirdə, onun hərflərinin altından isə açar sözün hərfləri yazılır. Əgər açar sözün uzunluğu ilkin mətnin uzunluğundan qısa olarsa, onda açar söz təkrarlanır. İlkin mətnin hərfi ona uyğun sütunla açar sözün onun altında olan hərfinə uyğun sətrin kəsişməsində duran hərflə əvəz olunur.

Şifrin açarı: əlifba və açar söz.

Azərbaycan əlifbası üçün Vijiner cədvəli aşağıdakı şəkildə olar:

	A	B	C	D	E	...	V	Y	Z	Əlifbanın hərfləri
A	A	B	C	Ç	D	...	V	Y	Z	-sürüşməsiz
B	Z	A	B	C	Ç	...	Ü	V	Y	-1 hərf sürüşmə ilə
C	Y	Z	A	B	C	...	U	Ü	V	-2 hərf sürüşmə ilə
D	V	Y	Z	A	B	...	T	U	Ü	-3 hərf sürüşmə ilə
E	Ü	V	Y	Z	A	...	Ş	T	U	
...	...	...	...	...	...	...	...	...	...	
V	Ç	D	E	Ə	F	...	A	B	C	
Y	C	Ç	D	E	Ə	...	Z	A	B	
Z	B	C	Ç	D	E	...	Y	Z	A	

Məsələn, "ƏLİFBA" açar sözünə görə "KRİPTOQRAFİK ŞİFRLƏMƏ" mətnini aşağıdakı kimi şifrləmək olar:

K R İ P T O Q R A F İ K Ş İ F R L Ə M Ə - İlkin mətn
Ə L İ F B A Ə L İ F B A Ə L İ F B A Ə L - Açar söz
Ö G T V U O P G İ J J K Z Y O Y M Ə S R - Şifrmətn

5.13.18. *Trisemus cədvəli.* Almaniyalı abbat Trisemus 1508-ci ildə gizli yazı haqqında ilk kitabı ("Poliqrafiya) çap etdirmiş və bu əsərində bir sıra şifrləmə üsulları barədə məlumat vermişdir. Trisemus öz əsərində şifrləmə üçün Polibiy üsulunun xüsusi şəkildə tərtib olunmuş cədvələ tətbiqini təklif etmişdir. Belə ki, cədvələ sətir üzrə əvvəlcə açar söz, sonra isə əlifbanın açar sözündə olmayan hərfləri ardıcıl şəkildə yazılır. Burada nəzərə alınmalıdır ki, açar sözündə əlifbanı eyni hərfi yalnız bir dəfə istifadə oluna bilər. Verilmiş ilkin mətn Polibiy üsulu vasitəsilə bu cədvəldən istifadə etməklə şifrlənir.

Şifrin açarı: açar söz və əlifba.

Məsələn, Azərbaycan əlifbası üçün "ABORİGEN" açar sözünə görə aşağıdakı cədvəli tərtib etmək olar:

A	B	O	R	İ	G	E	N
C	Ç	D	Ə	F	Ğ	H	X
I	J	K	Q	L	M	Ö	P
S	Ş	T	U	Ü	V	Y	Z

Onda "SABAH GƏLİRƏM" mətni bu cədvələ əsasən Polibiy üsulu vasitəsilə aşağıdakı kimi şifrlənər:

"ACÇCÖ ĞQÜFƏQV".

5.13.19. *Trisemus şifri.* Sezar şifrinin təkmilləşdirilmiş variantı olub çoxəlifbalı açarlı şifrdir. Əlifbanın bütün hərfləri 0-dan N-1-dək nömrələnir. Burada N - əlifbanın hərflərinin sayıdır. İlkin mətn bir sətirdə, açar sözün hərfləri mətnin hərfləri altında yazılır. Əgər açar sözün uzunluğu mətnin uzunluğundan kiçik olarsa, onda açar söz təkrarlanır. Şifrləmə üçün ilkin mətnin və açar sözün uyğun hərflərinin nömrələri toplanır. Alınan ədədlər

şifrmətnin hərflərinin nömrəsi kimi qəbul edilir və əlifbadan müvafiq hərf götürülür. Əgər toplama nəticəsində alınan ədəd *N*-dən böyük və ya bərabər olarsa, onda həmin ədəddən *N* çıxılır və alınan nəticə müvafiq hərfin nömrəsi kimi qəbul edilir.

Şifrin açarı: açar söz və əlifba.

Azərbaycan əlifbasının hərfləri və onların nömrələri cədvəldə göstərilmişdir:

A	B	C	Ç	D	E	Ə	F	G	Ğ	H	X	I	İ	J	K
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Q	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Bu üsulun köməyi ilə "HAKER" açar sözünü istifadə etməklə "OBYEKT YERİNDƏDİR" mətni aşağıdakı kimi şifrlənər:

İlkin mətnin hərfləri	O	B	Y	E	K	T	Y	E	R	İ	N	D	Ə	D	İ	R
İlkin mətnin hərflərinin nömrəsi	20	1	30	5	15	26	30	5	23	13	19	4	6	4	13	23
Açar sözün hərfləri	H	A	K	E	R	H	A	K	E	R	H	A	K	E	R	H
Açar sözün hərflərinin nömrəsi	10	0	15	5	23	10	0	15	5	23	10	0	15	5	23	10
Şifrmətnin hərflərinin nömrəsi	30	1	13	10	6	4	30	20	28	4	29	4	21	9	4	1
Şifrmətnin hərfləri	Y	B	İ	H	Ə	D	Y	O	Ü	D	V	D	Ö	Ğ	D	B

Beləliklə, "YBİHƏD YOÜDVDÖĞDB" şifrmətni alınar.

5.13.20. *Kitab üzrə şifrləmə.* Burada şirləmə üçün əvvəlki bənddə göstərilən şifrləmə sistemindən istifadə olunur. Lakin bu zaman açar qismində tərəflərin (göndərən və alan) hər ikisində olan hər hansı kitabın mətnindən fraqment istifadə olunur. Bu fraqmentin uzunluğu şifrlənən məlumatın uzunluğuna bərabər götürülür.

Qeyd olunmalıdır ki, göndərilən şifrlənmiş məlumatın əvvəlinə şifrləmə açarının kitabın hansı hissəsindən götürüldüyünü göstərən bir cüt ədəd əlavə edilir. Birinci ədəd kitabın səhifəsinin, ikinci ədəd isə həmin səhifədə sətrin nömrəsini göstərir.

Şifrin açarı: kitab, onun səhifəsini və səhifədəki sətri göstərən iki ədəd.

Bu üsulun xüsusi halı kimi, "şeirə görə" şifrləmə üsulu mövcuddur. Şifrləməni həyata keçirmək məqsədilə əvvəlcədən əlifbanın bütün hərfləri rast gəlinən uzun şeir götürülür (əzbərlərnir). Məlumatın şifrlənməsi zamanı onun hər bir hərfi iki ədədlə əvəz olunur. Bu ədədlərin birincisi həmin hərfin rast gəlindiyi sətri, ikincisi isə sətirdəki sırasını göstərir.

5.13.21. *Playfair biqram şifri.* İlkin məlumatın hərflərini iki-iki şifrləyən üsulları *biqram şifrlər* adlandırırlar. Playfair biqramı I Dünya müharibəsi zamanı Böyük Britaniyada istifadə olunmuşdur. Playfair əvvəlcə ilkin məlumatın hər birində iki hərf olmaqla bloklara (biqramlara) bölünməsini, sonra isə aşağıdakı qaydada şifrlənməsini təklif edir. Bu zaman əvəzetmə üçün hər hansı cədvəldən (məsələn, Trisemus cədvəlindən) istifadə oluna bilər.

Bu məqsədlə tərəflər əvvəlcədən cədvəlin ölçüsü və açar sözü müəyyənləşdirirlər. Tutaq ki, 18 bənddə veril-

miş Trisemus cədvəli istifadə olunur (cədvəlin ölçüsü – 4x8, açar söz isə "ABORİGEN"):

A	B	O	R	İ	G	E	N
C	Ç	D	Ə	F	Ğ	H	X
I	J	K	Q	L	M	Ö	P
S	Ş	T	U	Ü	V	Y	Z

Playfair şifrləməsi özündə bir sıra əvəzetmə qaydalarını özündə ehtiva edir.

Əgər açıq mətnin biqramının hərfləri cədvəldə eyni sütunda yerləşirlərsə, onda bu hərflər, uyğun olaraq, həmin sütunda onlardan aşağıdakı sətirdə yerləşən hərflə əvəz olunur. Əgər biqramın hərfi sonuncu sətirdə olarsa, onda onun əvəzinə həmin sütunda birinci sətirdə olan hərf götürülür. Məsələn, "RQ" biqramı "ƏU","BŞ" biqramı isə "ÇB" kimi şifrlənmiş olar.

Əgər açıq mətnin biqramının hərfləri cədvəlin eyni sətrində yerləşirlərsə, onda bu hərflər, uyğun olaraq, həmin sətirdə onlardan sağdakı sütunda yerləşən hərflə əvəz olunur. Burada da dairəvi prinsip tətbiq olunur. Belə ki, sonuncu sütunda yerləşən hərfin əvəzinə həmin sətirdə birinci sütunda yerləşən hərf götürülür. Məsələn, "ÇH" biqramı "DX","ON" biqramı isə "RA" şəklində şifrlənər.

Əgər açıq mətnin biqramının hərfləri cədvəlin müxtəlif sətir və sütunlarında yerləşirlərsə, onda şifrləmə aşağıdakı qaydada həyata keçirilir. Biqramın birinci hərfi onun yerləşdiyi sətirlə ikinci hərfinin yerləşdiyi sütunun kəsişməsində duran hərflə, biqramın ikinci hərfi isə onun yerləşdiyi sətirlə birinci hərfinin yerləşdiyi sütunun kəsişməsində duran hərflə əvəz olunur. Məsələn, "AQ" biqramı "RI" şifrini,"ET" biqramı isə "OY" şifrini verir.

Qeyd etmək lazımdır ki, ilkin mətnin biqramlarında hərflər müxtəlif olmalıdır. Əgər biqram iki eyni hərfdən ibarət olarsa, onda onların arasına, eləcə də sonuncu biqramda bir hərf qalarsa, onda onun sonuna bir hərf (məsələn, "x") əlavə edilir.

Şifrin açarı: cədvəlin ölçüsü və açar söz.

19-cu bənddə baxılan "OBYEKT YERİNDƏDİR" məlumatını Playfair sistemi vasitəsilə aşağıdakı kimi şifrləmək olar:

OB	YE	KT	YE	Rİ	ND	ƏD	İR
EO	EH	TO	EH	İG	OX	FƏ	Gİ

Beləliklə, şifr "EOEHTOEHİGOXFƏGİ" olar.

5.13.22. *İkiqat biqram cədvəli.* 1854-cü ildə Ç.Uinston tərəfindən təklif olunmuşdur. Bu üsul əvvəlki bənddəki üsula oxşarlıq təşkil edir. Lakin burada bir cədvəl əvəzinə əlifbanın hərfləri ilə təsadüfi qaydada doldurulmuş iki cədvəldən istifadə olunur. Şifrləmə üçün ilkin biqramın hərflərinin biri birinci cədvəldən, digəri isə ikinci cədvəldən götürülür. Onların əsasında da elə düzbucaqlı qurulur ki, biqramın hərfləri onun diaqonalboyu qarşılıqlı təpələrində yerləşmiş olsun. Bu düzbucaqlının digər iki təpəsində yerləşən hərflər şifrlənmiş biqramı əmələ gətirir.

Əgər biqramın hər iki hərfi eyni sətirdə yerləşərsə, onda şifrmətnin biqramı aşağıdakı kimi tapılır. Şifrmətnin biqramının birinci hərfi ikinci cədvəlin həmin sətrindən götürülür. Sütun nömrəsi isə ilkin biqramın birinci hərfinin birinci cədvəldə yerləşdiyi sütunun nömrəsi qəbul edilir. Şifrmətnin biqramının ikinci hərfi isə birinci cədvəlin həmin sətrindən götürülür. Sütun nömrəsi ilkin

biqramın ikinci hərfinin ikinci cədvəldə yerləşdiyi sütunun nömrəsi ilə müəyyən edilir.

Şifrin açarı: əlifbanın hərfləri ilə təsadüfi qaydada doldurulmuş iki cədvəl.

Tutaq ki, 8x4 ölçüdə iki cədvəl verilmişdir və onlar Azərbaycan əlifbasının hərfləri ilə təsadüfi qaydada doldurulmuşdur.

Ğ	S	D	J
Q	A	P	G
I	T	O	C
Y	E	L	Ü
N	Z	B	R
Ş	İ	V	X
Ç	U	K	Ə
F	Ö	H	M

Ə	M	Ç	H
B	Ö	S	İ
K	X	U	N
R	J	Y	E
P	Ğ	F	Q
U	C	I	T
D	O	Ş	G
L	Z	A	V

Nümunə qismində 19-cu bənddəki misala baxaq. "OB-YEKT YERİNDƏDİR" məlumatının şifrlənməsi üçün onu biqramlara bölür və şifrləyirlər. Qeyd olunan qaydalara uyğun olaraq, "OB" biqramı "KP", "YE" biqramı "RÜ" və s. şifrlənmiş biqrama çevrilir. Beləliklə verilmiş məlumat aşağıdakı kimi şifrlənmiş olar:

OB	YE	KT	YE	Rİ	ND	ƏD	İR
KP	RÜ	GV	RÜ	QG	PÇ	GÇ	UE

Nəticədə

"KPRÜGVRÜOGPÇGÇUE"

şifrmətni alınar.

5.13.23. *ADFGVX şifri.* Bu şifrdə həm əvəzetmə, həm də yerdəyişmədən istifadə olunur. Əvvəlcə 6x6 ölçülü (ingilis əlifbası üçün) kvadrat cədvəl götürülür. Cədvəlin sətir və sütunları A, D, F, G, V, X hərfləri ilə nömrələnir. Sonra əlifbanın hərfləri və rəqəmlər ixtiyari qaydada cədvələ doldurulur.

	A	**D**	**F**	**G**	**V**	**X**
A	4	İ	Z	8	F	2
D	M	A	H	O	S	K
F	X	1	Q	0	U	6
G	9	P	T	Y	D	B
V	E	V	5	G	W	L
X	7	N	J	R	C	3

Birinci mərhələdə şifrləmə zamanı ilkin məlumatın hərfləri yerləşdikləri sətir və sütunun nömrələrinin birləşməsindən əmələ gələn hərflər cütü ilə əvəz edilir. Məsələn "T" hərfinin yerinə "GF" hərfləri, "8" rəqəminin yerinə isə "AG" hərfləri yazılır.

İkinci mərhələdə şifrləmə biraçarlı yerdəyişmə cədvəli ilə davam etdirilir. Belə ki, verilmiş açar sözə və ölçüyə görə cədvəl qurulur. Birinci mərhələnin sonunda alınmış şifrmətn sütunlar və ya sətirlər üzrə cədvələ doldurulur və cədvəlin sütunlarının üstündən və ya sətirlərinin qarşısında açar söz yazılır.

Sonra açar sözün hərfləri əlifbadakı ardıcıllığa uyğun olaraq düzülür və uyğun sətirlərin yerləri də müvafiq qaydada dəyişdirilir. Belə yerdəyişmədən sonra sonda cədvəldəki hərflər sətirlər və ya sütunlar üzrə köçürülür, alınan ardıcıllıq yekun şifrmətn olur.

Şifrin açarı: doldurulmuş ADFGVS cədvəli, açar söz və yerdəyişmə cədvəlinin ölçüsü.

Tutaq ki, "METHOD ADFGVX" mətni və "KADR" açarı verilmişdir. Onda birinci mərhələdə yuxarıda tərtib edilmiş cədvələ uyğun olaraq, bu mətn aşağıdakı kimi şifrlənmiş olar:

M	E	T	H	O	D	A	D	F	G	V	X
DA	VA	GF	DF	DG	GV	DD	GV	AV	VG	VD	FA

İkinci mərhələdə sütunları açar sözün hərfləri işarələnmiş 4x6 ölçülü cədvələ alınmış şifrmətn sətirlərlə doldurulur:

K	D	G	D	D	A	V
A	A	F	G	D	V	D
D	V	D	G	G	V	F
R	A	F	V	V	G	A

Sonra açar sözün hərflərinin əlifbadakı mövqelərinə görə cədvəlin sətirlərinin yerləri dəyişdirilir:

A	A	F	G	D	V	D
D	V	D	G	G	V	F
K	D	G	D	D	A	V
R	A	F	V	V	G	A

Sonuncu cədvəldən hərflər sətirlərlə köçürülür və

"AFGDVDVDGGVFDGDDAVAFVVGA"

şifrmətni alınır.

5.13.24. *"Cəfəngiyat" şifri.* Bu şifr yalnız samitlərin sadə əvəz edilməsindən ibarət olan bu şifr Rusiyada istifadə olunurdu. Şifrləmə zamanı saitlər dəyişməz qalır. Məsələn, samitlərin əvəz olunması üçün aşağıdakı ardıcıllıq götürülə bilər:

B	C	Ç	D	F	G	Ğ	H	X	J	K	Q
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
L	M	N	P	R	S	Ş	T	V	Y	Z	.

Şifrin açarı: samitlərin əvəz edilməsi ardıcıllığı.

Bu cədvələ əsasən "SABAH UÇACAĞIQ" mətni "GALAT UNAMAŞI." şifrmətninə çevrilər.

5.13.25. *Qoşa şifr.* Əvəzetmə cədvəlini düzəltmək üçün burada 16 hərfdən az olmayaraq (əlifbanın hərflərinin yarısından az olmayaraq) uzunluğa malik açar ifadə götürülür. Bu ifadə bir sətirdə yazılır, onun hərflərinin altından əlifbanın bu ifadədə olmayan hərfləri ardıcıl şəkildə yazılır. Məsələn, "SABAHKI REYS GÖZLƏNİLİR"

S	A	B	A	H	K	I	R	E	Y	S	G	Ö	Z	L	Ə	N	İ	L	İ	R
1	2	3		4	5	6	7	8	9		10	11	12	13	14	15	16			
C	Ç	D		F	Ğ	X	J	Q	M		O	P	Ş	T	U	Ü	V			

Beləliklə, aşağıdakı əvəzetmə cədvəli alınır:

A	B	C	Ç	D	E	Ə	F	G	Ğ	H	X	I	İ	J	K
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
Ç	D	S	A	B	Q	U	H	O	K	F	I	X	V	R	Ğ

Q	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
E	T	Y	Ü	G	P	Ö	J	C	Z	L	Ə	N	İ	M	Ş

Şifrin açarı: açar ifadə.

Belə qurulmuş şifrləmə cədvəlinə əsasən "UÇUŞ TƏXİRƏ SALINDI" məlumatı "ƏAƏZ LUIVJU CÇTXÖBX" kimi şifrlənər.

5.13.26. *Ceffersonun şifrləmə təkərləri.* Bu şifr Tomas Cefferson (sonradan ABŞ-ın üçüncü prezidenti olmuşdur) tərəfindən 1790-cı ildə ixtira edilmişdir. Şifrləmə disklərinin iş prinsipi uzun açara görə məlumatın çoxəlifbalı əvəz edilməsi üsuluna əsaslanır. Açarın uzunluğunun dövrü şifrləmə təkərlərinin dövrlərinin ən kiçik ortaq böləni ilə müəyyən olunur. Məsələn, dövrləri 13, 15, 17 və 19 olan 4 disk üçün böyük dövrə (13x15x17x19=62985) malik açar alınır. Belə açarla şifrlənmiş məlumatın açılması olduqca çətin idi.

Şifrin açarı: əvvəlcədən hazırlanmış disklər.

5.13.27. *Bazeri silindri.* Sadə cihaz olan bu silindr Etyen Bazeri tərəfindən 1891-ci ildə təklif olunmuşdur. O, çevrələri boyunca əlifbanın hərfləri təsadüfi qaydada yazılmış 20 diskdən ibarət idi. Şifrləmədən əvvəl disklər açarla müəyyən olunan qaydada ümumi oxa keçirilir. Disklər üzərindəki hərflərin köməyi ilə mətnin ilk 20 hərfi bir sıraya yığılır, sonra onlar birlikdə fırladılır və digər sırada duran hərflər ardıcıllığı şifrlənmiş mətn qismində götürülür. Bu proses məlumatın mətni tam şifrlənib qurtaranadək davam etdirilir.

Şifrin açarı: 20 diskdən ibarət silindr.

5.13.28. *Enigma.* Müasir kriptoqrafik maşınların sələfi sayılan ilk rotor maşını Edvard Xabern tərəfindən 1917-ci ildə ixtira edilmişdir. Sonradan Enigma (ingiliscədən tərcüməsi "tapmaca" deməkdir) adlandırılan bu maşınların ilk sənaye nümunəsini Siemens şirkəti hazırlamış, müstəqil sənaye variantı isə alman mühəndisi Artur Kirx tərəfindən yaradılmışdır. Qurğunun ilk variantı bir ox ətrafında fırlanan 4 diskdən ibarət idi. Disklərin hər iki tərəfində çevrəsi üzrə əlifbanın hərflərinin sayına uyğun olaraq 25 elektrik kontaktı qoyulurdu.

Disk barabanlarının hər iki üzündə olan kontaktlar 25 naqil vasitəsilə təsadüfi qaydada cüt-cüt birləşdirilirdi. Bu birləşmələr əlifbanın simvollarının əvəz olunmasını təmin edirdi. Disklər üst-üstə qoyulurdu. Bir-birinə toxunan kontaktlar elektrik impulslarının bütün disklər paketi boyunca, sağ barabanın sağ tərəfindən (şifrləmə düyməsindən) sol barabanın sol tərəfinə (şifrləmə lampalarına) keçməsini təmin edirdi. Bu şəkildə qurulmuş qurğu sadə əvəzetmə şifrinin milyondan yuxarı variantını təmin edir.

Şifrləməyə başlamazdan əvvəl barabanlar elə fırladılır ki, bir sırada verilmiş açar söz (kod) alınsın, eləcə də düymə basıldıqda və növbəti simvol kodlaşdırıldıqda sağ baraban bir addım fırlanmış olsun, bu baraban bir dövr etdikdən sonra isə növbəti baraban bir addım fırlansın. Beləliklə, açar məlumatın mətnindən xeyli uzun olur.

Məsələn, tutaq ki, birinci sağ barabanın bir üzündə L hərfinə uyğun kontakt o biri üzündə olan B hərfinə uyğun kontakta qoşulmuşdur. Əgər baraban bir addım fırlanarsa, onda bu naqil L hərfindən sonrakı M hərfi B hərfindən sonrakı C hərfi ilə əvəz edilməsinə uyğun olur.

Barabanın kontaktları bir-birinə toxunduqlarına görə ilkin mətnin hərfinə uyğun düymənin basılmasından yaranan elektrik impulsu barabanların sonunda çıxışa çatanadək dörd dəyişməyə (hər barabanda bir dəyişmə) məruz

qalır. Şifrin açılmasını çətinləşdirmək məqsədilə mütəmadi olaraq barabanların yerlərini dəyişir və ya başqası ilə əvəz edirdilər.

Bu maşının növbəti təkmilləşdirilmiş variantında barabanlar xaotik hərəkət edirdilər, disklərin sayı əvvəl 5-ə, sonra isə 6-ya qədər artırılmışdır. Belə maşını adi portfelə yerləşdirmək olardı. Onun iş prinsipi çox sadə idi və adi rabitəçilər tərəfindən asanlıqla mənimsənilirdi.

5.14. Biraçarlı kriptoqrafik sistemlər

5.14.1. DES standartı

Məlumatların kriptoqrafik gizlədilməsi üzrə 1978-ci ildə Amerika standartı kimi qəbul edilmiş DES (*Data Encryption Standard*) şifr blokla şifrləmə ailəsinə daxildir. DES alqoritminin saniyədə bir neçə meqabayt şifrləmə sürətini təmin edən həm aparat, həm də proqram təminatı şəklində reallaşdırılması mümkündür.

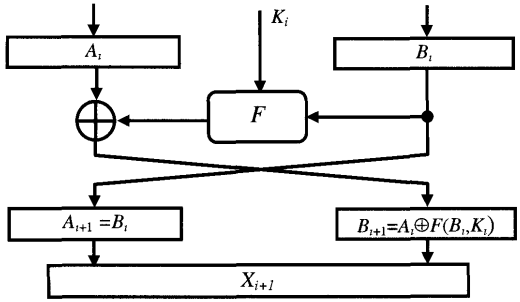
DES şifrinin əsasında Feystel şəbəkəsi durur. Feystel şəbəkəsinin əsasını isə ixtiyari funksiyanın (adətən, F-funksiya adlanır) bloklar çoxluğunda yerdəyişmə çevrilməsi üsulu təşkil edir. F-funksiya mətnin blokları üzərində həyata keçirilən inikas etmə iterasiyalarından ibarətdir.

Əgər X – şifrlənən mətn, $X_i = \{A_i, B_i\}$ isə onun bloku olarsa, onda Feystel şəbəkəsinin bir iterasiyasını və onun sonunda alınan nəticəni aşağıdakı kimi ifadə etmək olar (şək.5.6):

$$X_{i+1} = B_i \| (A_i \oplus F(B_i, k_i)).$$

Burada k_i – şifrləmə açarı, $\|$ – konkatenasiya əməliyyatı, $\oplus$ – 2 moduluna görə bit-bit toplama (VƏ YA) əməliyyatıdır.

DES alqoritmi ilə şifrləmənin həyata keçirilməsi üçün dörd işçi rejimdən istifadə olunur: elektron kodlaşdırma kitabı – ECB (Electronic Code Book), şifr bloklarının qarışdırılması – CBC (Cipher Block Chaining), şifrlənmiş mətnə görə əks əlaqə – CFB (Cipher Feedback) və çıxışa görə əks əlaqə – OFB (Output Feedback).



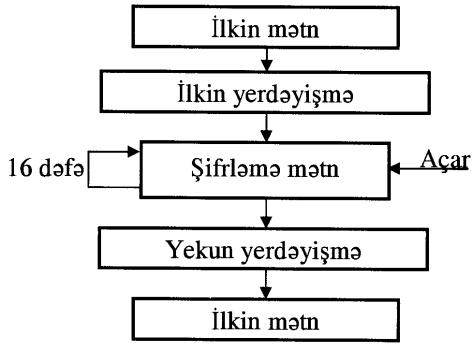
Şək.5.6. Feystel şəbəkəsinin iterasiyasının strukturu

DES alqoritmi şifrləmə zamanı çoxsaylı əvəzetmə və yerdəyişmə əməliyyatları kombinasiyasından istifadə edir. DES 64 bit uzunluğa malik bloklarla işləyir və onların 16 qat yerdəyişməsinə əsaslanır.

Şifrləmə üçün 56 bit (8 ədəd yeddi bitlik ASCII simvol) uzunluğa malik açardan istifadə olunur. Əslində açarın uzunluğu 64 bit olur, lakin onların 56-sı əhəmiyyətə malikdir, qalan 8-i isə yoxlama-nəzarət məqsədilə istifadə

olunur. Başqa sözlə, parolun uzunluğu 8 simvoldan artıq ola bilməz. Əgər parolda yalnız hərf və rəqəmlərdən istifadə olunarsa, onda parol variantlarının sayı maksimal mümkün saydan (2^{56}) əhəmiyyətli dərəcədə kiçik olar.

DES alqoritmində şifrləmə prosesinin ümumiləşdirilmiş sxemi 5.7 saylı şəkildə göstərilmişdir.



Şək.5.7. DES alqoritmində şifrləmə prosesinin ümumiləsdirilmiş sxemi

Qeyd etmək lazımdır ki, DES alqoritmi vasitəsilə şifrləmək üçün çoxlu sayda cədvəllərdən istifadə olunur. Açarın seçilməsi vasitəsilə şifrin açılması prosesini maksimal dərəcədə çətinləşdirmək məqsədilə müəlliflər tərəfindən diqqətlə tərtib olunmuş bu cədvəllər standart cədvəllər kimi qəbul edilməli və DES alqoritminin reallaşdırılması zamanı dəyişdirilmədən istifadə olunmalıdır.

Tutaq ki, T – ilkin mətnin 64 bit (8 bayt) uzunluğunda bloku, L (left) – T blokunun sol 32 bitlərinin ardıcıllığı, R (right) – T blokunun sağ 32 bitlərinin bitlər ardıcıllığıdır.

5.1. saylı cədvəldə göstərilən IP matrisinə uyğun olaraq, T blokunun bitlərinin yerləri dəyişdirilir:

$$T_0=\mathrm{IP}(T).$$

Yerdəyişmə nəticəsində T blokunun 58-ci, 50-ci, 42-ci və s. bitləri T_0 blokunun, uyğun olaraq, 1-ci, 2-ci, 3-cü və s. bitləri olur.

Cədvəl 5.1. IP ilkin yerdəyişmə matrisi

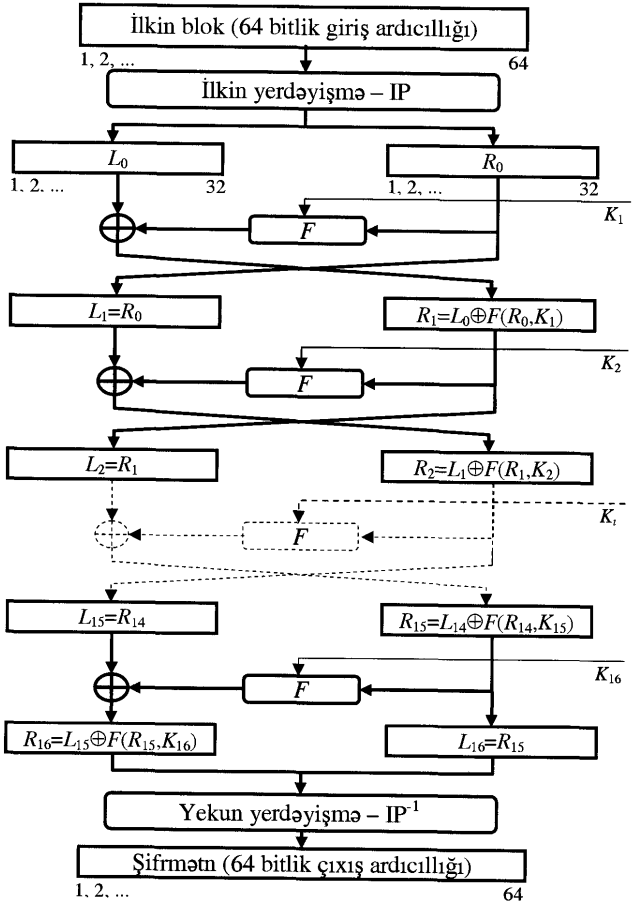
58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

Bundan sonra 16 addımdan ibarət olan aşağıdakı şifrləmə prosesi iterativ şəkildə yerinə yetirilir (şək.5.8). Tutaq ki,

$$T_i = L_i \| R_i$$

i-ci iterasiya nəticəsində alınmış 64 bitdən ibarət blok, $L_i = t_1 t_2 t_3 ... t_{32}$ – T_i blokunun ilk 32 bitindən ibarət sol alt bloku, $R_i = t_{33} t_{34} t_{35} ... t_{64}$ isə axırıncı 32 bitdən ibarət sağ alt blokudur. Onda 16 addımdan ibarət olan hər bir i iterasiyasının nəticəsini aşağıdakı düsturla təsvir etmək olar:

$$L_i = R_{i-1},\ i = \overline{1,16},$$



Şək.5.8. DES alqoritminin strukturu

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i),\ i = \overline{1,16}.$$

Qeyd etmək lazımdır ki, sonuncu iterasiyada alınan R_{16} və L_{16} ardıcıllıqların yerləri dəyişdirilmədən birləşdirilir və bir 64 bitlik ardıcıllıq alınır. Şifrləmə prosesinin sonunda alınan bu ardıcıllıqdan IP^{-1} yekun yerdəyişməsi matrisinin köməyi ilə bitlərin mövqeləri bərpa olunur (cədvəl 5.2).

Burada F – şifrləmə (Feystel) funksiyasıdır. Onun arqumentləri əvvəlki iterasiyada alınmış 32 bitlik R_{i-1} ardıcıllığı və 64 bitlik açarın çevrilməsi nəticəsində alınan 48 bitlik K_i açarıdır.

Cədvəl 5.2. IP^{-1} əks (yekun) yerdəyişmə matrisi

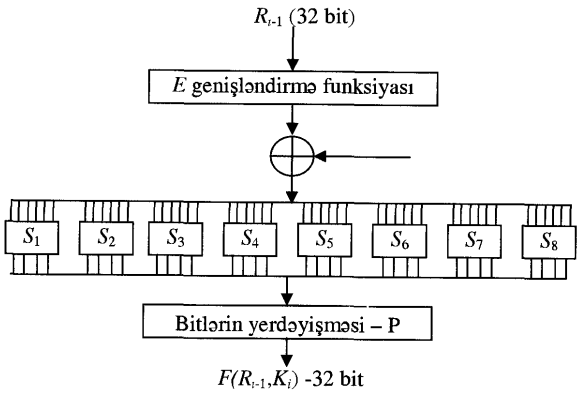
40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

$F(R_{i-1}, K_i)$ şifrləmə funksiyasının qiymətinin hesablanması sxemi 5.9 saylı şəkildə göstərilmişdir. Şəkildən göründüyü kimi, F funksiyasının qiymətinin hesablanması üçün aşağıdakı funksiyalardan istifadə olunur:

- 32 bitlik R_{i-1} ardıcıllığının 48 bitə qədər genişləndirilməsini yerinə yetirən E funksiyası;
- 6 bitlik ədədin 4 bitə çevrilməsi üçün səkkiz ədəd S_1, S_2, ... S_8 funksiyaları;
- 32 bitlik ardıcıllıqda bitlərin yerlərinin dəyişdirilməsini təmin edən P funksiyası.

32 bitlik R_{i-1} ardıcıllığının E funksiyası vasitəsilə 48 bitə qədər genişləndirməsi 5.3. saylı cədvələ əsasən həyata

keçirilir. Burada $E(R_{i-1})$ funksiyası nəticəsində alınan ardıcıllığın ilk üç biti ilkin ardıcıllığın 32, 1, 2-ci bitləri, sonuncu bitləri isə ilkin ardıcıllığın 31, 32, 1-ci bitləridir.



Şək.5.9. F şifrləmə funksiyasının qiymətinin hesablanması sxemi

Cədvəl 5.3. E genişləndirmə funksiyası

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Genişləndirmə nəticəsində alınmış 48 bit açarın 48 bitlik cari qiyməti ilə 2 moduluna görə toplanır və alınan ardıcıllıq səkkiz ədəd 6 bitlik bloklara bölünür:

$$E(R_{i-1})\oplus K_i=B_1B_2...B_8.$$

S_i funksiyaları B_i bloklarında olan 6 biti 4 bitə çevirmək üçün 5.4 saylı cədvəldən istifadə edir. Bu, aşağıdakı alqoritm vasitəsilə həyata keçirilir. Tutaq ki, $B_j=b_1b_2b_3b_4b_5b_6$ – 6 bitlik blokdur. Onda S_i funksiyası b_1b_6 iki bitlik ədədinə görə cədvəlin sətrin nömrəsini, $b_2b_3b_4b_5$ dörd bitlik ədədinə görə isə sütunun nömrəsini müəyyən edir. Həmin sətirlə sütunun kəsişməsində duran ədəd götürülür və ikilik sistemə çevrilərək müvafiq dörd bit kimi qəbul edilir.

Tutaq ki, S_1 funksiyasının girişinə altı bitlik $B_1=b_1b_2b_3b_4b_5b_6=111001_{(2)}$ verilmişdir, onda iki bitlik $b_1b_6=11_{(2)}=3_{(10)}$ ədədi 5.4 saylı cədvəlin S_1-ə uyğun matrisinin 3-cü sətrini, dörd bitlik $b_2b_3b_4b_5=1100_{(2)}=12_{(10)}$ ədədi isə həmin matrisin 12-ci sütununu göstərir. Bu, o deməkdir ki, $B_1=111001_{(2)}$ bloku S_1 cədvəlindən 3-cü sətirlə 12-ci sütunun kəsişməsində duran elementlə, yəni dörd bitlik $10_{(10)}=1010_{(2)}$ ardıcıllığı ilə əvəz olunur.

Belə çevirmə nəticəsində 8 ədəd 6 bitlik blok, yəni 48 bitlik $B_1B_2...B_8$ ardıcıllığı əvəzinə 8 ədəd 4 bitlik blok, yəni 32 bitlik $S_1(B_1)$, $S_2(B_2)$, ... $S_8(B_8)$ ardıcıllığı alınır. Bu ardıcıllıq da öz növbəsində 5.5 cədvəlinə uyğun olaraq çevrilir və şifrləmə funksiyasının

$$F(R_{i-1},K_i)=P(S_1(B_1),S_2(B_2),...,S_8(B_8))$$

qiyməti hesablanmış olur.

Cədvəl 5.4. S_1, S_2, ... S_8 çevirmə funksiyaları matrisi

Sətrin nömrəsi	Sütunun nömrəsi																
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	S_1
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	
2	4	1	4	8	13	6	2	11	15	12	9	7	3	10	5	0	
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	S_2
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	S_3
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	S_4
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4	
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	S_5
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	
0	0	12	1	10	15	9	2	6	8	0	133	4	14	7	5	11	S_6
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	1	6	
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	S_7
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	S_8
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

Cədvəl 5.5. *P* bitlərin yerdəyişməsi funksiyası

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

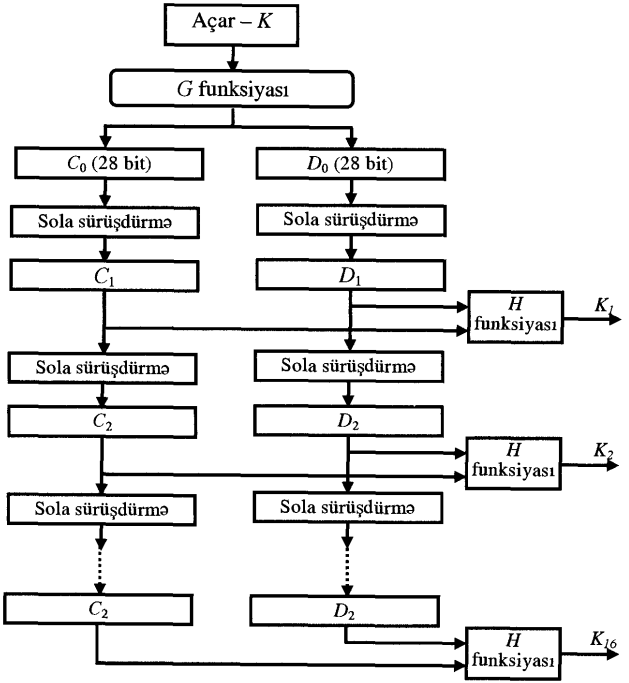
Qeyd olunduğu kimi, şifrləmənin hər addımında K şifrləmə açarının 48 bitlik yeni K_i qiyməti istifadə olunur. K_i qiymətləri K ilkin açarının qiymətindən 5.10 şəklində göstərilən alqoritmə uyğun olaraq hesablanır. 64 bit uzunluğa malik ilkin açarın 8 biti, yəni 8, 16, 24, 32, 40, 48, 56, 64 saylı bitləri cütlüyün yoxlanması üçün istifadə olunur. Yeni qiymətin hesablanması üçün əvvəlcə G funksiyanın köməyi ilə açarın 5.6 cədvəlinə əsasən yoxlama bitləri silinir və istifadəyə hazırlanır.

Nəticədə alınan 56 bitdən ibarət $G(K)$ ardıcıllığı hər biri 28 bitdən ibarət iki C_0 və D_0 bloklarına bölünür. Belə ki, C_0 bloku $G(K)$ ardıcıllığının ilk 28 bitini, D_0 bloku isə son 28 bitini təşkil edir.

Cədvəl 5.6. Açarın ilkin hazırlanması funksiyası – G

57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36
63	55	47	39	31	23	15	7	63	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

C_0 və D_0 blokları müəyyən edildikdən sonra, 3.4 saylı şəkildə göstərildiyi kimi, rekursiv qaydada C_i və D_i, i=1,2,...,16 blokları hesablanır. Hesablama zamanı hər iterasiyada alınan ardıcıllıqlar iterasiya nömrəsindən asılı olaraq, dövri şəkildə 1 və ya 2 bit sola sürüşdürülür (cədvəl 5.7).



Şək.5.10. K_i açarının hesablanması alqoritminin sxemi

Cədvəl 5.7. Açarın hesablanması üçün sürüşdürmə cədvəli

İterasiyanın №-si	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Sola sürüş-mələrin sayı	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Hər iterasiyanın sonunda alınan K_i açarı 56 bitlik $C_i \| D_i$ ardıcıllığından H funksiyasının (cədvəl 5.8) köməyi ilə seçilmiş və yerləri dəyişdirilmiş 48 bitlik ardıcıllıqdan ibarətdir:

$$K_i = H(C_i D_i)$$

Cədvəl 5.8. Açarın emalını yekunlaşdıran H funksiyası

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

5.14.2. AES standartı

AES (Advanced Encryption Standard) 2000-ci ildə DES standartının əvəzinə ümummilli standart kimi istifadə üçün qəbul edilmişdir. Onun əsasını blok şifri olan Rijndael alqoritmi təşkil edir. Alqoritmin təsviri zamanı Feystel şəbəkəsindən deyil, $GF(2^8)$ Qalua meydanından istifadə olunur. $GF(2^8)$ meydanı

$$m(x) = x^8 + x^4 + x^3 + x + 1$$

çoxhədlisinin kökləri üzrə $GF(2)$ meydanının genişlənməsi şəklində qurulur.

Qeyd olunmalıdır ki, verilənlərin bitləri 0-dan başlayaraq, böyükdən kiçiyə doğru nömrələnir. Alqoritmdə əsas məsələ kodların polinom çoxhədli şəklində təsvir edilməsindən ibarətdir. Belə ki, "10110101" şəklində bayt "$x^7+x^5+x^4+x^2+1$" çoxhədlisi kimi təqdim olunur. Burada yuxarıda göstərilən $m(x)$ çoxhədlisi meydanın element-

lərinin təqdim olunmasının effektivliyi səbəbindən seçilmişdir.

Rijndael alqoritmində blok və açar dəyişən uzunluğa malikdir, onların uzunluqları bir-birindən asılı olmadan 128, 192 və ya 256 bitə bərabər seçilə bilər.

Şifrləmə prosesi State (vəziyyət) adlanan hər hansı aralıq struktur (blok) üzərində yerinə yetirilən iterasiyalar ardıcıllığından ibarətdir. State və açar baytları matrislər şəklində təsvir olunurlar. Bu matrislərin sətirlərinin sayı – 4, sütunlarının sayı isə, uyğun olaraq, $N^b/32$ və $N^k/32$ olur. Burada N^b – blokun, N^k isə açarın uzunluğudur.

Alqoritmin giriş və çıxış qiymətləri baytların müvafiq uzunluqda birölçülü massivi şəklində təqdim olunur. State və açar massivləri giriş massivlərindən əvvəlcə sütunlarla, sonra isə sətirlərlə doldurulur.

Şifrləmə prosesi iterasiyalı şəkildə dörd müxtəlif çevirməni yerinə yetirən proseduralardan ibarətdir.

- SubByte - baytların əvəz edilməsi prosedurası;
- ShiftRows – sətirlərin sürüşdürülməsi prosedurası;
- MixColumn – sütunların qarışdırılması prosedurası;
- AddRoundKey – dövr (raund) açarının əlavə edilməsi (toplanması) prosedurası.

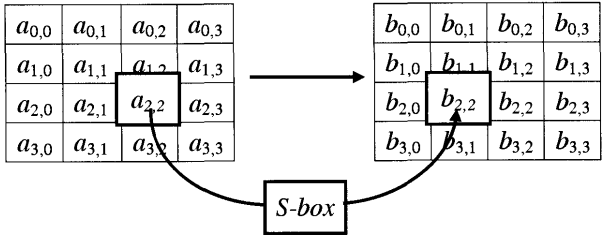
Alqoritmin iterasiyalarının sayı (N^r) blokun və açarın uzunluqlarından (N^b və N^k) asılı olaraq aşağıdakı cədvələ uyğun müəyyən edilir:

	N^b=4 (128b)	N^b=6 (192b)	N^b=8 (256b)
N^k=4 (128b)	10	12	14
N^k=6 (192b)	12	12	14
N^k=8 (256b)	14	14	14

SubByte prosedurası

SubByte (Byte Substitution) prosedurasında baytların əvəz edilməsi S-blok və ya S-box adlanan əvəzetmə cədvəli vasitəsilə həyata keçirilir. Bu cədvəl bir-birindən asılı olmadan State blokunun hər bir baytına tətbiq olunur, onların qeyri-xətti çevirməsini təmin edir (şək.5.11):

$$b_{ij} = S(a_{ij}), i, j = 1,2,3.$$



Şək.5.11. SubByte prosedurası

Əvəzetmə prosedurası iki əməliyyatı özündə birləşdirir:

1. Hər bir bayt GF(2^8) meydanında multiplikativ vurmaya nəzərən tərsi ilə əvəz edilir:

$$b_i^{-1} = b_i \bmod m(x).$$

Bu zaman "00" baytı öz-özünə çevrilir.

2. Hər bir bayt üçün GF(2) meydanında aşağıdakı düsturla müəyyən edilən affin çevirməsi həyata keçirilir:

$$b_i = b_i \oplus b_{(i+4) \bmod 8} \oplus b_{(i+5) \bmod 8} \oplus b_{(i+6) \bmod 8} \oplus b_{(i+7) \bmod 8} \oplus c_i,$$

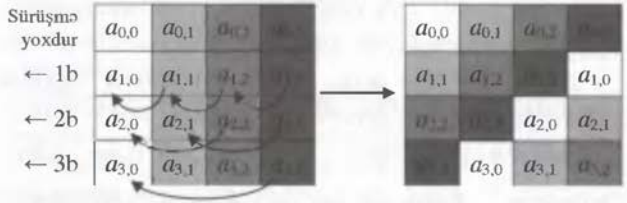
burada b_i – b-nin i-ci biti, c_i isə c={63}={01100011} baytının i-ci bitidir, $i = \overline{1,8}$.

Bu çevirməni matrislərin köməyi ilə aşağıdakı kimi yazmaq olar:

$$\begin{Vmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{Vmatrix} = \begin{Vmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{Vmatrix} * \begin{Vmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{Vmatrix} + \begin{Vmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{Vmatrix}$$

ShiftRows prosedurası

Bu çevirmə zamanı State cədvəlinin sətirləri dövri olaraq sola doğru r_i bayt sürüşdürülür. 0-cı sətir sürüşdürülmür, yəni r_i=0, 1-ci sətir 1b sürüşdürülür, yəni r=1b və s. Beləliklə, ShiftRows prosedurasından sonra alınan çıxış State cədvəlinin sütunları başlanğıc (giriş) State cədvəlinin hər sütunundan bir baytı özündə birləşdirir (şək.5.12).



Şək.5.12. ShiftRows prosedurası

N^b qiymətindən asılı olaraq, r_i kəmiyyətinin qiymətləri aşağıdakı cədvəldə göstərilmişdir:

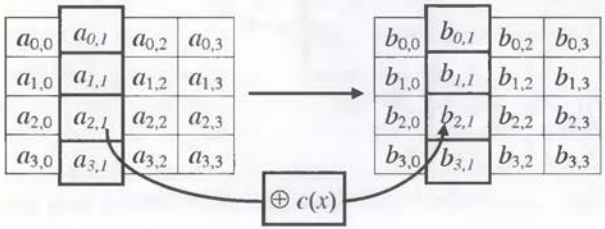
N^b	r_1	r_2	r_3
4	1	2	3
6	1	2	3
8	1	3	4

Cədvəldən göründüyü kimi, burada 128 və 192 bitlik sətirlər üçün sürüşmənin qiyməti eyni, 256 bitlik sətirlər üçün isə fərqlidir.

MixColumns prosedurası

Bu prosedura zamanı tərsi olan xətti çevirmə vasitəsilə State cədvəlinin sütunlarının baytları qarışdırılır (şək.5.13). Bunun üçün cədvəlin hər bir sütunu ayrı-ayrılıqda emal olunur. Sütunlardan dörd dərəcəli polinom düzəldilir və bu polinom GF(2^8) meydanında x^4+1 moduluna görə təsbit edilmiş $c(x)=3x^3+x^2+x+2$ çoxhədlisinə vurulur:

$$b(x) = c(x) \cdot a(x) \bmod (x^4 + 1).$$



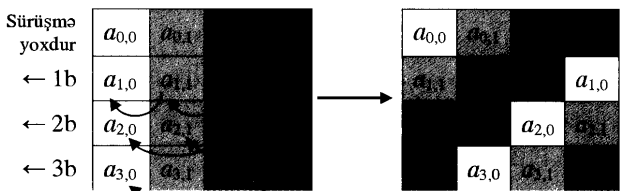
Şək.5.13. MixColumns prosedurası

Bu çevirməni matrislərin köməyi ilə aşağıdakı kimi yazmaq olar:

$$\begin{Vmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{Vmatrix} = \begin{Vmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{Vmatrix} * \begin{Vmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{Vmatrix} + \begin{Vmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{Vmatrix}$$

ShiftRows prosedurası

Bu çevirmə zamanı State cədvəlinin sətirləri dövri olaraq sola doğru r_i bayt sürüşdürülür. 0-cı sətir sürüşdürülmür, yəni r_i=0, 1-ci sətir 1b sürüşdürülür, yəni r=1b və s. Beləliklə, ShiftRows prosedurasından sonra alınan çıxış State cədvəlinin sütunları başlanğıc (giriş) State cədvəlinin hər sütunundan bir baytı özündə birləşdirir (şək.5.12).



Şək.5.12. ShiftRows prosedurası

N^b qiymətindən asılı olaraq, r_i kəmiyyətinin qiymətləri aşağıdakı cədvəldə göstərilmişdir:

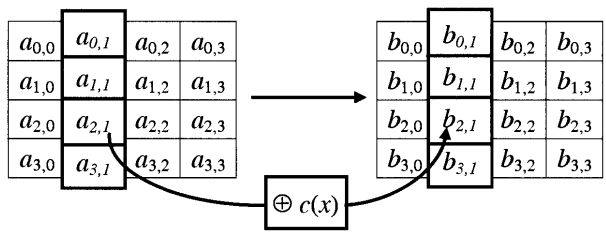
N^b	r_1	r_2	r_3
4	1	2	3
6	1	2	3
8	1	3	4

Cədvəldən göründüyü kimi, burada 128 və 192 bitlik sətirlər üçün sürüşmənin qiyməti eyni, 256 bitlik sətirlər üçün isə fərqlidir.

MixColumns prosedurası

Bu prosedura zamanı tərsi olan xətti çevirmə vasitəsilə State cədvəlinin sütunlarının baytları qarışdırılır (şək.5.13). Bunun üçün cədvəlin hər bir sütunu ayrı-ayrılıqda emal olunur. Sütunlardan dörd dərəcəli polinom düzəldilir və bu polinom GF(2^8) meydanında x^4+1 moduluna görə təsbit edilmiş $c(x)=3x^3+x^2+x+2$ çoxhədlisinə vurulur:

$$b(x) = c(x) \cdot a(x) \bmod (x^4 + 1).$$



Şək.5.13. MixColumns prosedurası

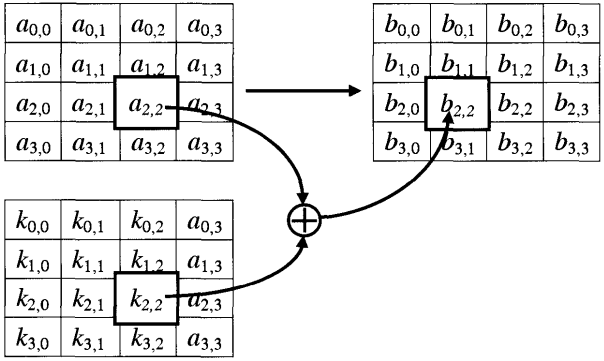
Bu ifadəni matris şəklində aşağıdakı kimi təsvir etmək olar:

$$\begin{Vmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{Vmatrix} = \begin{Vmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 01 \end{Vmatrix} \cdot \begin{Vmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{Vmatrix}$$

x^4+1 və $c(x)$ çoxhədliləri qarşılıqlı sadə olduğuna görə vurma əməliyyatının tərsi vardır.

AddRoundKey prosedurası

Bu prosedurada hər itersiyada State blokuna itersiya açarı (RoundKey) əlavə edilir (şək.5.14).



Şək.5.14. AddRoundKey prosedurası

RoundKey açarı KeyExpansion prosedurası vasitəsilə alınır. Onun uzunluğu State blokunun uzunluğuna bərabərdir. AddRoundKey prosedurası State blokunun hər bir

baytı ilə açarın uyğun baytını 2 moduluna görə bit-bit toplayır. Bu çevirmənin tərsi elə həmin çevirmənin özüdür.

KeyExpansion prosedurası

Bu prosedura iki alt proseduradan ibarətdir. Birinci alt prosedura kriptoqrafik şifrləmə açarının K genişlənməsinə xidmət edir. Bütövlükdə alqoritm üçün $N^b*(N^r+1)$ sözdən (sözün uzunluğu 4 baytdır) ibarət genişlənmiş açar (N^b sözdən ibarət 1 başlanğıc açar alqoritmin girişi üçün və N^b sözdən ibarət N^r ədəd iterasiya açarı itersiyalar üçün) tələb olunur. Məsələn, 256 bit uzunluqlu blok və 14 itersiya üçün genişlənmiş açarın uzunluğu 128*(14+1)=1920 bit olar.

KeyExpansion prosedurasının girişinə ilkin məxfi şifrləmə açarı K (CipherKey) verilir və nəticədə $N^b*(N^r+1)$ sayda sözdən ibarət xətti massiv alınır. Bu massivi $\{w_i\}, i=\overline{0, N^b\cdot(N^r+1)}$ kimi işarə olunur.

Genişlənmiş açar aşağıdakı kimi formalaşdırılır. Onun ilk N^k sözü ilkin şifrləmə açarını (CipherKey) özündə saxlayır. Onun hər bir növbəti w_i sözü w_{i-1} (1 mövqe əvvəlki) və w_{i-N^k} (N^k mövqe əvvəlki) sözlərinin 2 moduluna görə toplanması nəticəsində alınır. N^k ədədinə bölünən mövqedə olan sözlər aşağıdakı qaydada müəyyən edilir: əvvəlcə w_{i-1} sözü 1b sola doğru dövri sürüşdürülür və bu iterasiya üçün qəbul edilmiş $Rcon_i$ sabiti ilə 2 moduluna görə toplanır, bundan sonra alınan nəticə w_{i-N^k} sözü ilə 2 moduluna görə toplanır.

İkinci alt prosedura iterasiya açarının seçilməsini təmin edir. Belə ki, i saylı iterasiyanın açarını almaq üçün

genişlənmiş açar massivindən $w\lfloor N^b \cdot i \rfloor$-dən $w\lfloor N^b \cdot (i+1) \rfloor$ -yə qədər olan sözlər götürülür.

5.14.3. Rusiya şifrləmə standartı - ГОСТ 28147–89

ГОСТ 28147-89 – 1990-cı ildə qəbul edilmiş Rusiya (Sovet) simmetrik şifrləmə standartıdır. O, dövlət orqanları, təşkilatları, bank və fəaliyyəti dövlətin informasiya təhlükəsizliyinin təmin edilməsi ilə bağlı olan müəssisələr üçün məcburi, digər təşkilatlar üçün isə tövsiyə xarakteri daşıyır.

Alqoritm aparat və proqram reallaşdırılması üçün nəzərdə tutulmuşdur və qorunan informasiyanın məxfilik dərəcəsinə heç bir məhdudiyyət qoyulmur. Onun işlənib hazırlanması zamanı mövcud dünya təcrübəsi, o cümlədən DES alqoritminin çatışmazlıqları və reallaşdırılmamış imkanları nəzərə alınmışdır.

ГОСТ 28147-89 standartı bloklarla şifrləmə alqoritmidir. Alqoritmdə emal edilən şifrlənən blokun uzunluğu 64 bit, şifrləmə açarının uzunluğu 256 bit, şifrləmə çevirmələrinin sayı isə 32 dövrdür. Alqoritm Feystel şəbəkəsinə əsaslanmışdır.

Bloklarla şifrləmə rejimində şifrləmə üçün əvvəlcə ilkin mətn iki yerə bölünür: A – kiçik bitlər və B – böyük bitlər. Dövrün i-ci itersiyasında K_i alt açarından istifadə etməklə aşağıdakı hesablamalar yerinə yetirilir:

$$A_{i+1} = B_i \oplus F(A_i, K_i),$$
$$B_{i+1} = A_i.$$

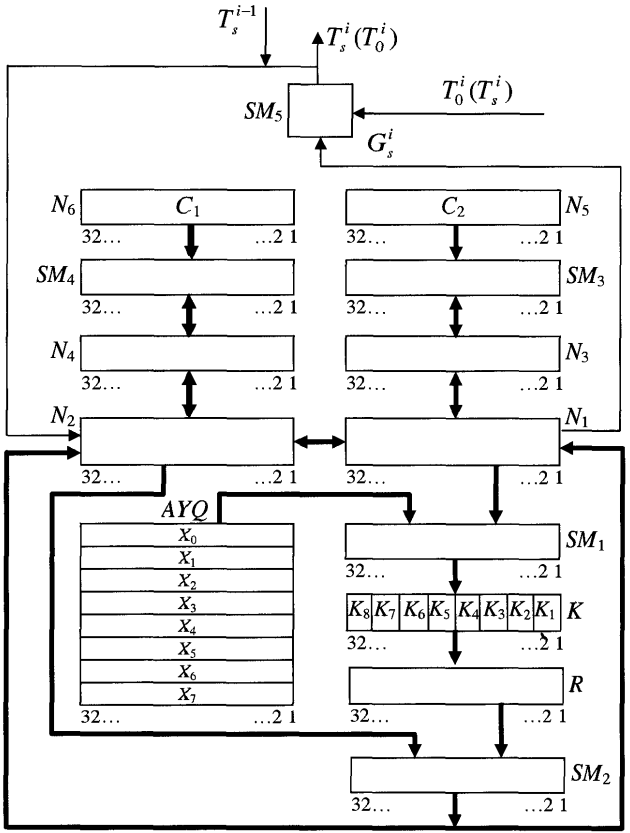
Şifrləmə alqoritminin 32 dövrünün sonunda alınan A_{33} və B_{33} blokları birləşdirilir və alınan ardıcıllıq

şifrləmənin nəticəsi olur. Bu zaman nəzərə alınmalıdır ki, A_{33} – yekun ardıcıllığının böyük bitlərini, B_{33} isə kiçik bitlərini təşkil edir.

ГОСТ 28147-89 kriptoqrafik şifrləmə alqoritminin ümumi struktur sxemi 5.15 saylı şəkildə verilmişdir. Şəkildən göründüyü kimi, kriptosxem aşağıdakıları özündə birləşdirir:

- AYQ – uzunluğu 256 bit olan açar yaddaş qurğusu, AYQ səkkiz ədəd 32 bitlik yığıcı X_0, X_1, X_2, X_3, X_4, X_5, X_6, X_7 registrlərindən ibarətdir;
- N_1, N_2, N_3, N_4, N_5, N_6 – 32 bitlik yığıcı registrlər, N_5 və N_6 registrlərinə əvvəlcədən C_2 və C_1 sabitləri yazılır;
- SM_1, SM_2, SM_3, SM_4, SM_5 –32 bitlik cəmləyicilər, SM_1 və SM_3 – 2^{32} moduluna, SM_2 – 2 moduluna, SM_3 – (2^{32}-1) moduluna, SM_5 – bitlərin sayına məhdudiyyət qoyulmadan 2 moduluna görə toplamanı yerinə yetirir;
- K – əvəzetmə bloku;
- R – böyük dərəcəyə doğru 11 addım dövri sürüşmə registri.

K əvəzetmə bloku hər biri 64 bitlik yaddaşa malik olan səkkiz ədəd K_1, K_2, K_3, K_4, K_5, K_6, K_7 və K_8 əvəzetmə qovşağından ibarətdir. Əvəzetmə blokuna daxil olan 32 bitlik vektor ardıcıl gələn səkkiz ədəd 4 bitlik alt vektorlara bölünür. Bu alt vektorlar da öz növbəsində əvəzetmə cədvəlinin 16 ədədi özündə saxlayan və S-blok adlanan qovşaqlarının girişinə verilir. K_1 – birinci S-blokun, K_2 – ikinci S-blokun girişinə və s. düşür. Alt vektorun qiyməti S-blokda ədədin mövqeyini müəyyən edir. Sayı alt vektorların sayına, yəni səkkizə bərabər olan S-bloklar daxil olan alt vektorun 0-la 15 arasında müəyyən ədədə çevrilməsini təmin edir.



Şək.5.15. ГОСТ 28147-89 alqoritminin struktur sxemi

S-blok {7, 3, 11, 1, 9, 14, 6, 0, 5, 12, 2, 15, 4, 8, 10, 13} şəklində olarsa, onda onun girişinə 1 verildikdə çıxışda 7, 4 verildikdə 1, 9 verildikdə 5 və s. alınar.

Sonda, alınmış bütün səkkiz ədəd 4 bitlik çıxış alt vektorlar ardıcıl olaraq birləşdirilir və 32 bitlik yekun vektoru alınır. Bu vektor isə 11 addım böyük dərəcəli bitə doğru dövri olaraq sürüşdürülür.

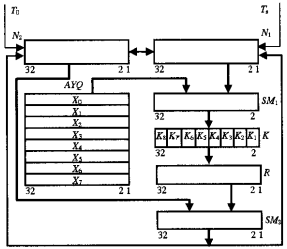
Qeyd etmək lazımdır ki, AYQ və K açarının, eləcə də S-bloklarının əvəz edilməsi cədvəlinin doldurulmasını təmin edən açarlar məxfi hesab olunurlar və müəyyən olunmuş qaydada verilirlər.

Göründüyü kimi, alqoritmin reallaşdırılması zamanı S-bloklar müxtəlif ola bilər, yəni əvəzetmə cədvəli fərqli seçilə bilər. ГОСТ P34.11-94 standartında yoxlama məqsədilə aşağıdakı S-bloklar təklif olunur:

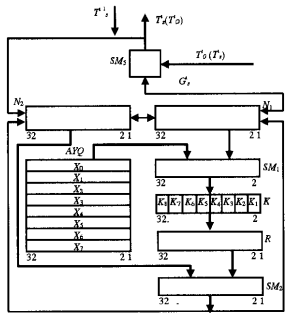
S_1	4	10	9	2	13	8	0	14	6	11	1	12	7	15	5	3
S_2	14	11	4	12	6	13	15	10	2	3	8	1	0	7	5	9
S_3	5	8	1	13	10	3	4	2	14	15	12	7	6	0	9	11
S_4	7	13	10	1	0	8	9	15	14	4	6	12	11	2	5	3
S_5	6	12	7	1	5	15	13	8	4	10	9	14	0	3	11	2
S_6	4	11	10	0	7	2	1	13	3	6	8	5	9	12	15	14
S_7	13	11	4	1	3	15	5	9	0	10	14	7	6	8	2	12
S_8	1	15	13	0	5	7	10	4	9	2	3	14	6	11	8	12

ГОСТ 28147-89 standartında kriptoqrafik şifrləmə sisteminin dörd iş rejimi nəzərdə tutulmuşdur:

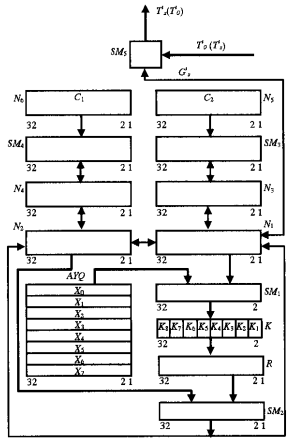
- sadə əvəzetmə rejimi (şək.5.16);
- qammalaşdırma rejimi (şək.5.17);
- əks əlaqə ilə qammalaşdırma rejimi (şək.5.18);
- imitasiya əlavə etməsi rejimi.



Şək.5.16. Sadə əvəzetmə rejimi



Şək.5.18. Əks əlaqə ilə qammalaşdırma rejimi



Şək.5.17. Qammalaşdırma rejimi

ГОСТ 28147-89 standartının müsbət cəhətlərinə reallaşdırmanın effektivliyi, yüksək sürəti, yalan verilənlərin yeridilməsindən qorunanın olması, bütün dörd rejimdə dövrlərin eyni olması və s. amilləri aid etmək olar.

5.15. İkiaçarlı kriptoqrafik sistemlər

5.15.1. RSA kriptoqrafik sistemi

RSA alqoritmi Massaçuset Texnoloji İnstitutunun üç alimi – R.Rayvest (Rivest), A.Şamir (Shamir) və A.Adleman (Adleman) tərəfindən 1978-ci ildə işlənib təklif olunmuşdur. Alqoritm adını məhz həmin alimlərin soyadlarının birinci hərflərinin birləşməsindən almışdır. RSA həm şifrləmə, həm də elektron imza üçün tətbiq olunan ilk mükəmməl açıq açarlı kriptoqrafik alqoritmdir. Onun elektron imza texnologiyasında reallaşdırılmasına növbəti fəsildə baxılacaqdır. Burada yalnız məlumatın şifrlənməsi alqoritminə baxılır.

RSA alqoritmi hesablama baxımından biristiqamətli funksiya olan böyük sadə ədədlərin çoxhədlilərə ayrılması və hasili məsələsinə əsaslanmışdır. Beləliklə, RSA alqoritmini etibarlılığı böyük ədədlərin çoxhədlilərə ayrılması və diskret loqarifmin hesablanmasının mürəkkəbliyi ilə müəyyən edilir.

Qeyd edildiyi kimi, açıq açarlı kriptoqrafik sistemlərdə hər bir iştirakçı iki açara – açıq açara (public key) və gizli açara (secret key) malik olur. RSA kriptoqrafik sistemində hər bir iştirakçı özünün hər biri iki ədəddən ibarət olan açıq və məxfi açarlarını müstəqil şəkildə yaradır. Hər bir iştirakçının açıq və gizli açarları qarşılıqlı uzlaşdırılmış olur, belə ki, onlar bir-birlərinin qarşılıqlı əksini təşkil edir. Onlar məxfi açarlarını gizli saxlayır, açıq açarlarını isə sərbəst şəkildə hamıya verir və yayırlar.

RSA kriptoqrafik sistemində T açıq mətni, S şifrmətni, K_e açıq açarı və K_d gizli açarı

$$Z_n=\{0,1,2,...,N-1\}$$

tam ədədlər çoxluğuna daxildir. Burada $N=P*Q$ – modul, P və Q – təsadüfi böyük sadə ədədlərdir. Maksimal təhlükəsizliyi təmin etmək üçün bu ədədləri eyni uzunluqda seçirlər və gizli saxlayırlar.

Tutaq ki, iki istifadəçi – göndərən tərəf (birinci istifadəçi) və alan tərəf (ikinci istifadəçi) RSA kriptoqrafik sistemi vasitəsilə məlumat mübadiləsi aparmaq istəyirlər. Məlumatın şifrlənməsi və şifrin açılması proseduraları alan tərəfin açıq və gizli açarlarına əsasən həyata keçirilir.

I. *Alan tərəfin (ikinci istifadəçinin) açarlarının generasiyası.* İkinci istifadəçi:

1. Təsadüfi böyük sadə P və Q ədədlərini seçir.
2. N modulunun qiymətini hesablayır: $N=P*Q$.
3. Eyler funksiyasının qiymətinin hesablayır:
$$\varphi(N)=(P-1)(Q-1).$$
$\varphi(N)$ – 0-dan N-ə qədər intervalda olan N ilə qarşılıqlı sadə müsbət ədədlərin sayını göstərir.
4. K_e açıq açarının aşağıdakı şərtləri ödəyən qiymətini seçir:
$$1<K_e\le\varphi(N),\ \text{ƏBOB}(K_e,\varphi(N))=1.$$
İkinci şərt K_e və $\varphi(N)$ ədədlərinin qarşılıqlı sadə olduğunu göstərir.
5. Genişlənmiş Evklid alqoritmindən istifadə etməklə $K_d * K_e \equiv 1(\text{mod}\,\varphi(N))$ ifadəsinə əsasən K_d məxfi açarını hesablayır:
$$K_d = K_e^{-1}(\text{mod}\,\varphi(N)).$$
6. (K_e,N) ədədləri cütünü açıq (qorunmayan) kanalla birinci istifadəçiyə göndərir.

II. *Göndərən şəxs tərəfindən məlumatın şifrlənməsi.* Birinci istifadəçi:

7. T ilkin mətnini 0,1,2,...,N-1 intervalında olan tam ədədlər ardıcıllığı şəklində təqdim edilən T_i bloklarına bölür.
8. Ədədlər ardıcıllığı şəklində təqdim olunmuş T_i mətn bloklarını ikinci istifadəçinin K_e açıq açarını istifadə etməklə
$$S_i = T_i^{K_e}(\text{mod}\,N)$$
düsturuna əsasən şifrləyir.
9. Şifrləmə nəticəsində alınmış S_1, S_2, S_3,..., S_i,... şifrmətnlərini ikinci istifadəçiyə göndərir.

III. *Alan şəxs tərəfindən şifrin açılması.* İkinci istifadəçi:

10. Özünün (K_d,N) gizli açarını istifadə etməklə birinci istifadəçidən aldığı S_1, S_2, S_3,..., S_i,... şifrmətnlərini
$$T_i = S_i^{K_d}(\text{mod}\,N)$$
düsturuna əsasən açır.
11. Alınmış T_1, T_2, T_3,..., T_i,... ədədlər ardıcıllıqlarından ibarət blokları ardıcıl birləşdirir və ilkin T mətnini alır.

RSA alqoritminin iş prinsipini əyani nümayiş etdirmək üçün aşağıdakı nümunəyə baxaq.

İkinci istifadəçi:

1. P=3557 və Q=2579 ədədlərini seçir.
2. $N=P*Q$=3557*2579=9173503 qiymətini hesablayır.
3. N=9173503 üçün Eyler funksiyasının qiymətini hesablayır:
φ(9173503)=3556*2578=9167368.
4. K_e açıq açarının
$1<K_e\le 9167368$, ƏBOB(K_e,9167368)=1
şərtləri ödəyən qiymətini seçir. Məsələn, K_e=3.

5. Genişlənmiş Evklid alqoritmindən istifadə etməklə K_d məxfi açarını hesablayır:

$$K_d=6111579.$$

6. $(K_e,N)=(3,9173503)$ ədədləri cütünü açıq (qorunmayan) kanalla birinci istifadəçiyə göndərir.
7. $(K_d,N)=(6111579,9173503)$ ədədlərini gizli açar kimi məxfi saxlayır.

Birinci istifadəçi:

8. T ilkin mətnini 0,1,2,...,31 intervalında olan tam ədədlər ardıcıllığı şəklində təqdim edir. Tutaq ki, ilkin mətn T="111111".
9. İkinci istifadəçinin $(K_e,N)=(3,9173503)$ açıq açarını istifadə etməklə T mətnini şifrləyir:

$$S = T^{K_e} (\mathrm{mod}\, N) = 111111^3 \bmod 9173503 = 4051753.$$

10. S=4051753 ədədlər ardıcıllığını şifrmətn kimi ikinci istifadəçiyə göndərir.

İkinci istifadəçi:

11. Özünün $(K_d,N)=(6111579,9173503)$ gizli açarını istifadə etməklə birinci istifadəçidən aldığı S=4051753 şifrmətnini açır:

$$T = S^{K_d} (\mathrm{mod}\, N) = 4051753^{6111579} \bmod 9173503 = 111111.$$

5.15.2. Əl-Qamal şifrləmə alqoritmi

Əl-Qamal şifrləmə alqoritmi 1985-ci ildə işlənib hazırlanmış və təklif olunmuşdur. Bu alqoritm məlumatın şifrlənməsi ilə yanaşı elektron imzanın reallaşdırılması üçün istifadə oluna bilər. Onun davamlılığı sonlu meydanda diskret loqarifmin hesablanmasının mürəkkəbliyinə əsaslanmışdır.

Alqoritmin iş prinsipi aşağıdakından ibarətdir:

I. *Şifrləmə açarlarının (açıq və gizli açarların) generasiyası.*

1. Uzunluğu n olan böyük sadə P ədədi generasiya olunur.
2. İxtiyari $G<P$ şərtini ödəyən böyük tam ədəd götürülür.
3. Aşağıdakı şərtləri ödəyən təsadüfi böyük tam X ədədi götürülür.
   - $X<P$;
   - X və $(P-1)$ ədədləri qarşılıqlı sadə ədədlərdir.
4. $Y = G^X \bmod P$ qiyməti hesablanır.

   Alınan (P,G,Y) ədədləri açıq açar hesab olunur və digər istifadəçilər arasında paylana bilər, X ədədi isə məxfi açardır və gizli saxlanılır.

II. *Məlumatın şifrlənməsi.*

5. Aşağıdakı şərtlərə cavab verən təsadüfi tam K ədədi seçilir:
   - $1<K<P-1$;
   - *K və $(P-1)$ ədədləri qarşılıqlı sadə ədədlərdir.*
6. T ilkin mətninə görə A və B ədədləri hesablanır:

$$A=G^K \bmod P,$$
$$B=Y^K \cdot T \bmod P.$$

7. $S=(A,B)$ ədədləri cütü şifrmətn olur. Göründüyü kimi, şifrmətnin uzunluğu ilkin T mətnin uzunluğundan iki dəfə böyük olur.

III. *Şifrin açılması.*

8. Alınmış $S=(A,B)$ şifrmətninə əsasən

$$T=B/A^X \bmod P$$

hesablanır. Aydındır ki, $A^X=G^{KX} \bmod P$ olduğuna görə

$$B/A^X = Y^K \cdot T/A^X = G^{KX} \cdot T/G^{KX} = T,$$

olar, yəni $T = B/A^X \bmod P$ doğrudur.

Alqoritmin iş prinsipini əyani nümayiş etdirmək üçün aşağıdakı nümunəyə baxaq.

Açarların generasiyası.

1. $P=13$, $G=3$ ədədlərini və $X=7$ məxfi açarını seçək.
2. Açıq açarı hesablayaq: $Y=G^X \bmod P=3^7 \bmod 13=2187 \bmod 13=3$.
   Beləliklə, açıq açar $Y=3$ olar.

Şifrləmə.

3. $T=8$ götürək.
4. Hər hansı təsadüfi $K=5$ ədədini seçək. ƏBOB$(K,P-1)$=ƏBOB$(5,12)=1$, yəni onlar qarşılıqlı sadə ədəddirlər.
5. A və B ədədlərini hesablayaq:
   $A=G^K \bmod P=3^5 \bmod 13=243 \bmod 13=9$,
   $B=Y^K \cdot T \bmod P=3^5 \cdot 8 \bmod 13=1944 \bmod 13=7$.
   Beləliklə, şifrmətn $S=(A,B)=(9,7)$ olar.

Şifrin açılması.

Verilmiş düstura əsasən T mətnini hesablayaq:

$$T=B/A^X \bmod P=7/9^7 \bmod 13=7/4782969 \bmod 13,$$
$$4782969 \cdot T=7 \bmod 13,$$

Bu bərabərlikdə T elə qiymət alır ki, onu 4782969 ədədinə hasilinin 13-ə bölünməsi nəticəsində qalıqda 7 qalsın:

$$T=8.$$

Qeyd etmək lazımdır ki, real şifrləmə sistemlərdə P ədədinin modulu qismində ikilik sistemdə 512-1024 bit uzunluqda ikilik ardıcıllıq şəklində təqdim oluna biləcək böyük tam ədəd götürülür.

VI FƏSİL

ELEKTRON İMZA

Elektron sənəd dövriyyəsi və autentifikasiya problemi

Elektron imza texnologiyası

Biristiqamətli heş funksiyalar və onların qurulması prinsipləri

Elektron imza alqoritmləri

Açarların idarə olunması və açıq açar infrastrukturu

Effektiv açıq açar infrastrukturunun yaradılması metodikası

6.1. Elektron sənəd dövriyyəsi və autentifikasiya problemi

Müasir dövrdə dövlət və hökumət strukturlarında, özəl və kommersiya təşkilatlarında, yerli özünüidarəetmə orqanlarında informasiya mübadiləsi məqsədilə kompyuter şəbəkələri, o cümlədən korporativ kompyuter şəbəkələri qurulur və İnternetə qoşularaq istifadə olunur. Bu istiqamətdə respublikada həyata keçirilən işlər günbəgün intensivləşir, kompyuter şəbəkələrinin əhatə dairəsi getdikcə daha da genişlənir.

Məlumdur ki, korporativ kompyuter şəbəkələri elektron (kağızsız) sənəd dövriyyəsinin həyata keçirilməsi üçün baza rolunu oynayır. Belə ki, korporativ kompyuter şəbəkələrində şəxsi, kommersiya və dövlət sirləri təşkil edən böyük həcmdə müxtəlif kateqoriyalı məlumatlar emal olunur, saxlanılır və şəbəkə (o cümlədən rabitə kanalları) vasitəsi ilə ötürülür.

Bu gün dövlət və özəl qurumlarda, kommersiya təşkilatlarında və biznes strukturlarında elektron sənəd dövriyyəsi artıq gündəlik fəaliyyətin real, ayrılmaz hissəsinə çevrilmişdir.

Elektron sənəd dövriyyəsi – informasiya sistemində elektron sənədin nizamlanmış hərəkəti (dövriyyəsi, mübadiləsi) ilə bağlı informasiya prosesləridir.

Elektron sənəd dövriyyəsinə keçid idarəetmənin və icraya nəzarətin effektivliyinin yüksəldilməsinə, sənədlərin qeydiyyatı jurnallarının ləğvinə, onların təkrar qeydiyyatının qarşısının alınmasına, bir sənədlə çoxlu sayda istifadəçinin eyni zamanda işləməsi üçün şəraitin yaradılmasına, mühüm sənədlərin itkisinin qarşısının alınmasına,

effektiv axtarış sisteminin yaradılmasına, kağız sənədlərin surətlərinin çoxaldılması zərurətinin aradan qalxmasına, işçi personalın informasiya texnologiyalarından istifadəsinin genişləndirilməsinə gətirib çıxarır.

Kağızsız sənəd dövriyyəsi texnologiyasının tətbiqi və genişlənməsi bir çox müsbət cəhətləri ilə yanaşı gündəlik fəaliyyətdə bəzi əlavə məsələlərin həllini tələb edir. Bu məsələlər, əsasən, məlumatların autentifikasiyası problemi ilə bağlı olur. Autentifikasiya məsələsi aşağıdakı ziyankar əməllərin qarşısının alınmasını özündə ehtiva edir:

- imtina – bir abonent digər abonentə məlumat göndərməsinə baxmayaraq, bu faktdan imtina edir və məlumatı göndərmədiyini bildirir;
- saxtalaşdırma (dəyişmə) – bir abonent digər abonentdən aldığı sənədi dəyişdirir və ya yeni sənəd yaradır və onun başqa abonent tərəfindən bu şəkildə göndərildiyini iddia edir;
- fəal əlaqəçirmə – pozucu şəbəkəyə qoşularaq bir istifadəçinin digər istifadəçiyə göndərdiyi məlumatı ələ keçirir və dəyişdirir;
- maskalanma – bir abonent ikinci abonentə tamamilə başqa (üçüncü) abonentin adından sənəd göndərir, yəni pozucu başqa şəxsin adı altında maskalanır;
- təkraretmə – abonent əvvəllər hər hansı başqa (ikinci) abonent tərəfindən digər (üçüncü) abonentə göndərilmiş sənədi təkrar olaraq həmin (üçüncü) abonentə göndərir.

Bu kimi hərəkətlər öz fəaliyyətində kompyuter texnologiyalarını tətbiq edən dövlət müəssisələrinə və təşkilatlarına, bank və kommersiya strukturlarına, fərdi şəxslərə ciddi ziyan vura bilər.

Bu baxımdan elektron sənəd dövriyyəsi zamanı kağız üzərində qoyulmuş yazılı imzaya və möhürün şəklinə görə sənədin həqiqiliyinin təyin edilməsi üçün istifadə olunan ənənəvi üsullar tamamilə yararsızdır. Qeyd olunan problemin əlverişli və yeni həlli elektron imza texnologiyasının tətbiqindən ibarətdir.

Dövlət və hökumət orqanlarında elektron sənəd dövriyyəsinin təşkili və bu zaman elektron imzanın tətbiqi mexanizmləri "Elektron imza və elektron sənəd haqqında" Azərbaycan Respublikasının Qanunu ilə nizamlanır. Bu qanuna uyğun olaraq elektron imza və elektron sənəd, qanunvericilikdə nəzərdə tutulmuş hallar istisna olmaqla, müvafiq vasitələr tətbiq olunan bütün fəaliyyət sahələrində istifadə oluna bilər.

Elektron sənəd vasitəsilə rəsmi və qeyri-rəsmi yazışmalar, hüquqi məsuliyyət və öhdəliklər doğuran sənəd və informasiya mübadiləsi həyata keçirilir. Burada *elektron sənəd* dedikdə informasiya sistemlərində istifadə üçün elektron formada təqdim edən və elektron imza ilə təsdiq olunan sənədlər nəzərdə tutulur.

Belə ki, elektron imza adi imzaya analoji olaraq, hüquqi statusa malik olub aşağıdakıları təmin edir:

- Sənədi göndərən mənbəni, yəni sənədin həqiqətən onu imzalayan şəxs tərəfindən göndərildiyini təsdiq edir. Sənədin təyinatından asılı olaraq, "müəllif", "edilmiş dəyişikliklər", "tarix" və digər atributlar imzalana bilər.
- Sənədi imzalayan və alan şəxslərin bu sənədlə bağlı hər hansı məsuliyyətdən (müəlliflikdən, sənədi alması və ya göndərməsi faktından və s.) imtina etməsinə imkan vermir.

- Göndərilən sənədin tamlığının, yəni onun təhrif olunmadan ünvana çatdırılmasının təmin edilməsinə zəmanət verir. Sənəddə (imzada) təsadüfən və ya qəsdən edilmiş istənilən (hətta kiçik) dəyişiklik heş funksiyanın qiymətinin dəyişməsinə gətirib çıxarır ki, bunun da nəticəsində elektron imza etibarsız olur və ya qüvvəsini itirir.
- Hüquqi statusa malik elektron sənəd dövriyyəsini təşkil etməyə imkan yaradır.

6.2. Elektron imza texnologiyası

Elektron imza texnologiyası korporativ kompyuter şəbəkələrində elektron sənəd dövriyyəsini, elektron sənədin və informasiya mübadiləsi aparan tərəflərin hüquqlarının qorunmasını təmin etməyə imkan verir.

Elektron imza – elektron sənədin ümumi hissəsini təşkil edən informasiyanın, eləcə də elektron sənədin və onun müəllifinin həqiqiliyinin təsdiq edilməsi üçün nəzərdə tutulan, elektron imza vasitələri tərəfindən yaradılan və elektron sənədin ayrılmaz hissəsi olan informasiya bloku, yəni simvollar ardıcıllığıdır.

Burada, *elektron imza vasitələri* dedikdə elektron imzanın yaradılması və yoxlanılmasını təmin edən, imza yaratma və imza yoxlama məlumatlarının yaradılması üçün istifadə edilən, uyğunluq sertifikatına malik olan proqram və texniki vasitələr başa düşülür.

Başqa sözlə, elektron imza vasitələri aşağıdakı funksiyalardan birinin reallaşdırılmasını həyata keçirən aparat və proqram vasitələridir:

- elektron imza üçün gizli və açıq açarların yaradılması;
- gizli açarı istifadə etməklə elektron sənəddə elektron imzanın yaradılması;
- açıq açardan istifadə etməklə elektron sənəddə olan elektron imzanın həqiqiliyinin təsdiq edilməsi.

Beləliklə, elektron imza imzalanan informasiya ilə birlikdə göndərilən kiçik ölçülü əlavə şifrlənmiş rəqəm informasiyadır. Başqa sözlə, elektron imza – elektron sənədin saxtalaşdırılmasının qarşısını almaq üçün nəzərdə tutulan, gizli açardan istifadə etməklə kriptoqrafik çevrilmə nəticəsində yaradılan və imzalama açarı sertifikatının sahibini tanımağa (identikləşdirməyə), eləcə də elektron sənəddə informasiyanın təhrif olunub-olunmadığını müəyyən etməyə imkan verən və elektron sənədin tərkib hissəsi olan rekvizitidir.

Burada *elektron imzanın açıq açarı* dedikdə elektron imzanın gizli açarına uyğun olan, informasiya sisteminin istənilən istifadəçisi tərəfindən əldə oluna və istifadə edilə bilən, elektron sənəddə elektron imzanın həqiqiliyinin təsdiq olunması üçün nəzərdə tutulan unikal simvollar ardıcıllığı nəzərdə tutulur. Elektron imzanın açıq açarı maraqlı şəxslərin hamısı tərəfindən əldə oluna bilən və elektron imzanın yoxlanması zamanı istifadə edilən simvollar yığımıdır. O, elektron imza vasitələrini tətbiq etməklə şəxsi imzalama açarının əsasında yaradılır.

Elektron imzanın gizli açarı – yalnız imzalama açarı sertifikatının sahibinə məlum olan və elektron imza vasitələrinin köməyi ilə elektron sənədlərdə elektron imzaların yaradılması üçün nəzərdə tutulan unikal simvollar ardıcıllığıdır.

Elektron imza aşağıdakı məlumatları özündə saxlayır:

- imzalama tarixi;
- imzalama açarının qüvvədə olmasının son müddəti;
- sənədi imzalayan şəxs haqqında məlumatlar (adı, soyadı, atasının adı, iş yerinin qısa adı, vəzifəsi və s.);
- imzalayan şəxsin identifikatoru (açıq açarı);
- bilavasitə elektron imza.

Ümumiyyətlə, elektron imza texnologiyası informasiyanı göndərənin identifikasiyası ilə yanaşı elektron sənədin (məlumatın) həqiqiliyini yoxlamağa imkan verir, yəni autentifikasiyanı da təmin edir. Bir qayda olaraq, elektron imzanın qoyulması (müəlliflikdən imtinanın qeyri-mümkünlüyü) və məlumatın autentikliyinin yoxlanması (sənədin həqiqiliyinin, yəni tamlığının təmin edilməsi) məsələlərini fərqləndirirlər. Elektron imza alqoritmləri asimmetrik şifrləmə üsulları, autentikliyin yoxlanması alqoritmləri isə simmetrik şifrləmə üsulları vasitəsilə reallaşdırılır.

Elektron imza sistemi elektron imza vasitələrinin köməyi ilə aşağıdakı iki proseduranı özündə birləşdirir:

- elektron imzanın yaradılması;
- elektron imzanın yoxlanılması.

Elektron imzanın yaradılması funksiyası sənədə və istifadəçinin gizli açarına əsasən məhz imzanın hesablanmasını, yəni onun yaradılmasını həyata keçirir. Alqoritmdən asılı olaraq, imzanın yaradılması funksiyası deterministik və ya ehtimallı funksiyalar ola bilər.

Deterministik funksiyalar həmişə eyni giriş məlumatlarına əsasən eyni imzanı hesablayır. Ehtimallı funksiyalar isə imzaya təsadüfilik xüsusiyyəti daxil edir ki, bu da elektron imza alqoritminin kriptoqrafik davamlılığını gücləndirir. Lakin ehtimallı funksiyalar üçün etibarlı təsadüfilik mənbəyinin (aparat səs-küy generatoru və ya psevdo-

təsadüfi bitlərin etibarlı kriptoqrafik generatoru) olması zəruridir. Bu isə reallaşdırmanı xeyli çətinləşdirir.

Hazırda deterministik funksiyalar, praktiki olaraq, istifadə olunmur. Hətta əvvəllər deterministik olan alqoritmlər müəyyən dəyişikliklər edilməklə ehtimallı funksiyalara çevrilmişlər. Məsələn, deterministik alqoritmi reallaşdıran PKCS#1 standartının ikinci versiyası özündə məlumatların qabaqcadan çevrilməsini, o cümlədən səs-küy yaratmanı nəzərdə tutan RSA alqoritmi ehtimallı xarakter daşıyır.

İmzanın yoxlanması funksiyası alınmış elektron imzanın alınmış imzalanmış sənədə və istifadəçinin açıq açarına uyğunluğunu yoxlayır. Aydındır ki, istifadəçinin açıq açarı hamıya məlumdur və istənilən şəxs verilmiş sənədə əlavə edilmiş elektron imzanı yoxlaya bilər.

İmzalanan sənədlər dəyişkən və ya kifayət qədər böyük uzunluğa malik olduğuna görə elektron imza sistemlərində imza sənədin özünə deyil, onun "heş" qiymətinə qoyulur. "Heş" qiymətin hesablanması üçün kriptoqrafik heş funksiyalardan istifadə olunur ki, bu da sənəddə baş vermiş dəyişikliklərin imzanın yoxlanması zamanı aşkar edilməsinə zəmanət verir.

Qeyd olunmalıdır ki, heş funksiya elektron imza alqoritminə daxil deyil, ona görə də bu məqsədlə istənilən etibarlı heş funksiyadan istifadə oluna bilər.

Elektron imzanın formalaşdırılması üçün göndərən tərəf ilk olaraq imzalanan informasiyanın heş funksiyasını hesablayır. Heş funksiyanın qiyməti imzalanan informasiyanın məzmununu tam xarakterizə edən kiçik ölçülü informasiya blokudur. O, məlumatı göndərənin məxfi açarı ilə şifrlənir. Alınmış informasiya elektron imza qismində imzalanan informasiya ilə birlikdə ünvana göndərilir.

Alan tərəf imzanın yoxlanılması üçün kanal vasitəsilə aldığı imzalanmış informasiyanın heş funksiyasını hesablayır. Sonra göndərənin açıq açarı vasitəsilə heş funksiyanın yeni hesablanmış qiyməti ilə göndərəndən alınmış qiyməti müqayisə edir. Əgər bu qiymətlər eyni olarsa, onda imza təsdiq olunur. Əks halda hesab edilir ki, ya kanal vasitəsilə alınmış informasiya təhrif olunmuşdur, ya da imza doğru deyildir.

6.3. Biristiqamətli heş funksiyalar və onların qurulması prinsipləri

Heş funksiya – tərsini almaq çox çətin olan informasiya çevrilməsi, yəni tərsi olmayan biristiqamətli funksiyadır. Heş funksiya (ingilis dilində "hash" – xırdalamaq və qarışdırmaq mənasını verir) imzalanan sənədi bir neçə on və ya yüz bitə qədər sıxmaq üçün nəzərdə tutulmuşdur.

Heş funksiya $h(\cdot)$ kimi işarə olunur. O, arqument qismində ixtiyari uzunluqda olan T məlumatını (sənədini) qəbul edir və hesablamanın nəticəsi kimi təsbit edilmiş uzunluqlu heş qiyməti $H=h(T)$ verir.

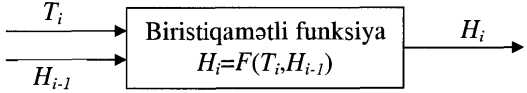
Qeyd olunmalıdır ki, heş funksiyanın qiyməti $h(T)$ çox mürəkkəb şəkildə T sənədindən asılı olur və onu bərpa etməyə imkan vermir. Adətən, heş qiymət ixtiyari uzunluqlu ilkin məlumatın sıxılmış ikilik təqdimatından ibarət olur.

Heş funksiya aşağıdakı tələblərə cavab verməlidir:

- heş funksiya ilkin mətndə bütün mümkün dəyişikliklərə (əlavəetmə, kəsib çıxarma, yerdəyişmə, əvəzetmə və s.) həssas olmalıdır;

- heş funksiya tərsinin alınmasının qeyri-mümkünlüyü xassəsinə malik olmalıdır, başqa sözlə, heş funksiyanın tələb olunan qiymətini verən T′ sənədinin seçilməsi məsələsi hesablama baxımından həll edilən olmamalıdır;
- uzunluqlarından asılı olmadan iki müxtəlif sənədin heş funksiyalarının qiymətlərinin üst-üstə düşməsi ehtimalı çox kiçik olmalıdır.

Qeyd olunduğu kimi, heş funksiyaların əksəriyyəti biristiqamətli $F(\cdot)$ funksiyası əsasında blokların qarışdırılması ilə simmetrik şifrləmə üsulları vasitəsilə qurulur. Bu funksiya girişdə n uzunluqlu iki qiymət (ilkin sənədin T_i bloku və əvvəlki blokunun H_{i-1} heş qiyməti) verildikdə çıxışda n uzunluqlu qiyməti verir (şək.6.1).



Şək.6.1. Biristiqamətli heş funksiyanın modeli

Şəkildən göründüyü kimi, hər blokun heş funksiyası hesablanarkən əvvəlki blokun heş funksiyasının qiyməti istifadə olunur. Sonuncu blokun şifrlənməsinin nəticəsi əvvəlki bütün bloklardan asılı olur və bütöv informasiyanın heş funksiyasının qiyməti kimi qəbul edilir.

Heş funksiyaların qurulması üçün ümumi qəbul edilmiş prinsip kimi ardıcıl iterativ sxemdən istifadə olunur. Bu alqoritmin əsasını k sayda bitlər ardıcıllığını n sayda bitlər ardıcıllığına çevirməkdən ibarətdir. n – kəmiyyəti heş

funksiyanın nəticəsinin mərtəbəliliyini, k – isə n-dən böyük ixtiyari ədəddir.

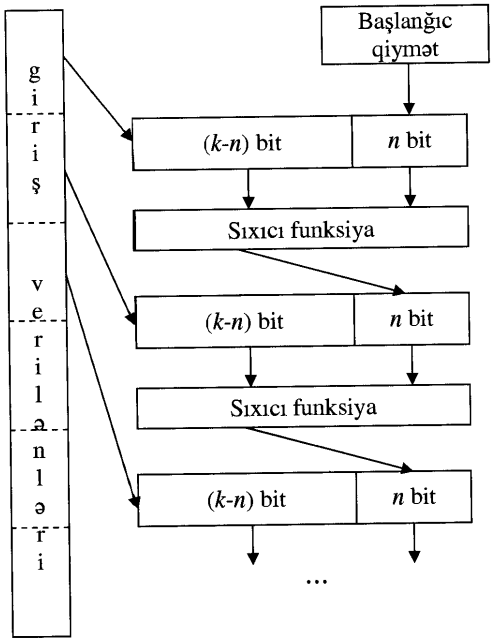
Baza çevirməsi heş funksiyanın bütün xassələrinə (tərsinin olmaması, giriş verilənlərinin invariant dəyişdirilməsinin qeyri-mümkünlüyü) malik olmalıdır. Heş qiymətin hesablanması n bitdən ibarət dəyişən mərtəbəli aralıq köməkçi dəyişənin köməyi ilə həyata keçirilir. Başlanğıc qiymət qismində hər iki tərəfə məlum olan ixtiyari qiymət (məsələn, 0) götürülür.

Məlumatın heş qiymətinin hesablanması prosesində giriş verilənləri (k-n) sayda bitdən ibarət bloklara bölünür. Hər iterasiyada giriş verilənlərinin (k-n) sayda bitdən ibarət bloku əvvəlki iterasiyada alınmış aralıq kəmiyyətin qiyməti ilə birləşdirilir və alınmış k sayda bitdən ibarət blok üzərində baza çevirməsi həyata keçirilir. Nəticədə bütün giriş məlumatı köməkçi kəmiyyətin başlanğıc qiyməti ilə qarışdırılmış olur.

Çevirmə xarakterinə görə baza funksiyasını çox vaxt sıxıcı funksiya adlandırırlar. Sonuncu itersiyadan sonra köməkçi kəmiyyətin qiyməti heş funksiyanın çıxışına verilir (şək.6.2).

Bəzən alınan qiymət üzərində əlavə çevirmələr həyata keçirirlər. Lakin sıxıcı funksiya kifayət qədər davamlılıq dərəcəsinə malik olarsa, onda belə çevirmələrə ehtiyac qalmır.

Heş funksiyanın iterativ sxemə görə layihələndirilməsi zamanı meydana biri ilə qarşılıqlı əlaqəli iki məsələ çıxır:
- (k-n) ədədinə bölünməyən verilənlərlə nə etməli?
- əgər tələb olunarsa, sənədin uzunluğunu yekun heş qiymətə necə əlavə etməli?



Şək.6.2. İterativ heş funksiya

Bu məsələlərin həllinin iki variantı mövcuddur. Birinci variantda heş qiymətin hesablanması prosesinə başlamazdan qabaq sənədin əvvəlinə təsbit edilmiş uzunluqda (məsələn, 32 bit) sahə əlavə edilir və ora sənədin ilkin uzunluğu ikilik formada yazılır. Sonra birləşdirilmiş

verilənlər blokunun bitlərinin sayı (k-n) ədədinə bölünən ən yaxın ədədə qədər tamamlanır.

İkinci variantda sənəd sağdan əvvəlcə bir ədəd "1" biti, sonra isə (k-n) ədədinə bölünən ən yaxın ədədə qədər tamamlamaq üçün tələb olunan sayda "0" bitləri əlavə edilir.

Bu halda sənədin uzunluğu sahəsinə ehtiyac qalmır, belə ki, hər hansı iki müxtəlif sənəd fraqmentləri sərhədlərinə görə belə hamarlandıqdan sonra heç vaxt eyni ola bilməz.

Heş qiymətin hesablanmasının daha populyar birkeçidli alqoritmləri ilə yanaşı çoxkeçidli alqoritmləri də mövcuddur. Bu halda giriş məlumat bloku genişlənmə mərhələsində dəfələrlə təkrarlanır, sonra isə yaxın sərhədə qədər tamamlanır.

6.4. Elektron imza alqoritmləri

Elektron imza alqoritmləri iki böyük sinfə bölünürlər:
- adi elektron imzalar;
- sənədin bərpasını təmin edən elektron imzalar.

Adi elektron imzaların imzalanan sənədə bağlanması zəruridir. Adi elektron imza alqoritmləri elliptik əyrilərə əsaslanan funksiyalar üzərində qurulur. Bu sinfə aid olan aşağıdakı daha məşhur alqoritmləri qeyd etmək olar:
- Amerika elektron imza standartı – DSA, ECDSA;
- Rusiya elektron imza standartı – ГОСТ Р 34.10-94 (hazırda qüvvədə deyil), ГОСТ Р 34.10-2001;
- Ukrayna elektron imza standartı – ДСТУ 4145-2002 və s.

Sənədin bərpasını təmin edən rəqəm imza özündə imzalanan sənədi saxlayır. Ona görə də imzanın yoxlanması prosesində sənədin özü də hesablanır. Bu növ alqoritmlərə aşağıdakı alqoritmlər aid edilir:

- PKCS#1 standartı, elektron imzanı RSA alqoritmi əsasında təsvir edir;
- Şnorr alqoritmi;
- Əl-Qamal (EGSA) alqoritmi;
- ehtimallı Rabin imzası alqoritmi və s.

Ümumiyyətlə, elektron imza sisteminin tətbiqi texnologiyası bir-birinə elektron sənədlər göndərən abonentlər şəbəkəsinin mövcud olduğunu nəzərdə tutur. Hər bir abonent üçün iki açar generasiya olunur:

- gizli açar;
- açıq açar.

Gizli açar abonent tərəfindən gizli saxlanılır və onun tərəfindən elektron imzanın formalaşdırılması (yaradılması) üçün istifadə olunur. Açıq açar isə bütün digər istifadəçilərə məlum olur və alınan imzalanmış sənədin elektron imzasının yoxlanması məqsədini daşıyır.

Başqa sözlə, açıq açar alınmış elektron sənədin və imza sahibinin həqiqiliyini yoxlamağa imkan verən zəruri alətdir. Açıq açar vasitəsilə gizli açarı hesablamaq (tapmaq) mümkün deyildir.

Asimmetrik şifrləmə sistemlərində olduğu kimi, elektron imza alqoritmlərində də gizli və açıq açarlar cütünün generasiyası üçün biristiqamətli funksiyaların tətbiqinə əsaslanan müxtəlif riyazi sxemlərdən istifadə olunur. Bu sxemlər iki əsas qrupa bölünürlər, onların əsasında məşhur mürəkkəb hesablama məsələləri durur:

- böyük tam ədədlərin vuruqlara ayrılması məsələsi;

- diskret loqarifmləmə alqoritmləri.

Elektron imza alqoritmini daha əyani şərh etmək üçün dünyada məşhur olan ilk elektron imza sistemlərindən birinə – RSA alqoritminə baxaq.

Sənədi göndərən, yəni onun müəllifi gizli və açıq açarlar cütünü hesablamaq üçün iki böyük P və Q sadə ədədlərini götürür, onların hasilini tapır

$$N=P*Q$$

və aşağıdakı funksiyanın qiymətini hesablayır:

$$\varphi(N)=(P-1)(Q-1).$$

Sonra aşağıdakı şərtlərə cavab verən E və D ədədlərini hesablayır:

$$E\le\varphi(N),\ \text{ƏBOB}(E,\ \varphi(N))=1,$$
$$D<N,\ E*D\equiv 1 \bmod \varphi(N).$$

Beləliklə, (E,N) ədədlər cütü məlumat göndərənin (imza sahibinin) açıq açarı olur. O, bu açarları özünün elektron imzasını yoxlamaq üçün tərəfdaşlarına göndərir. D ədədi isə gizli açar kimi müəllif tərəfindən məxfi saxlanılır və elektron imzanın yaradılması zamanı istifadə olunur.

Elektron imzanın yaradılması və yoxlanması üçün RSA alqoritminin ümumi sxemi 6.3 saylı şəkildə verilmişdir.

Qeyd olunduğu kimi, elektron imza prosesi iki hissədən ibarətdir. Birinci hissə elektron imzanın yaradılması prosedurasından ibarət olub göndərən şəxs tərəfindən icra olunur. Elektron imzanın yaradılması prosedurasının mahiyyəti aşağıdakı kimidir. Əvvəlcə, imzalanan T məlumatı heş funksiyanın köməyi ilə sıxılır, yəni onu xarakterizə edən heş qiyməti hesablanır: $t=h(T)$.

Sonra heş qiymət imza funksiyası vasitəsilə məxfi açardan (D,N) istifadə edilməklə şifrlənir:

$$S=t^D \bmod N.$$

Nəticədə, alınmış informasiya elektron imza qismində göndərilən məlumata əlavə edilərək (T,S) cütlüyü S elektron imzası ilə imzalanmış T sənədi qismində alan tərəfə göndərilir. Beləliklə, məlumat imzalanmış olur.

Elektron imza prosesinin ikinci hissəsində elektron imzanın yoxlanılması həyata keçirilir. Belə ki, alan tərəf rabitə kanalı vasitəsilə aldığı (T,S) cütlüyünə əsasən elektron imzanın həqiqiliyini yoxlayır.

Bunun üçün, o, əvvəlcə, T məlumatını sıxır, yəni göndərənin heş funksiyasına analoji olaraq, $t=h(T)$ heş qiymətini hesablayır. Sonra göndərənin açıq açarının (E,N) köməyi ilə S elektron imzasından heş funksiyanın qiymətini bərpa edir:

$$t'=S^E \bmod N.$$

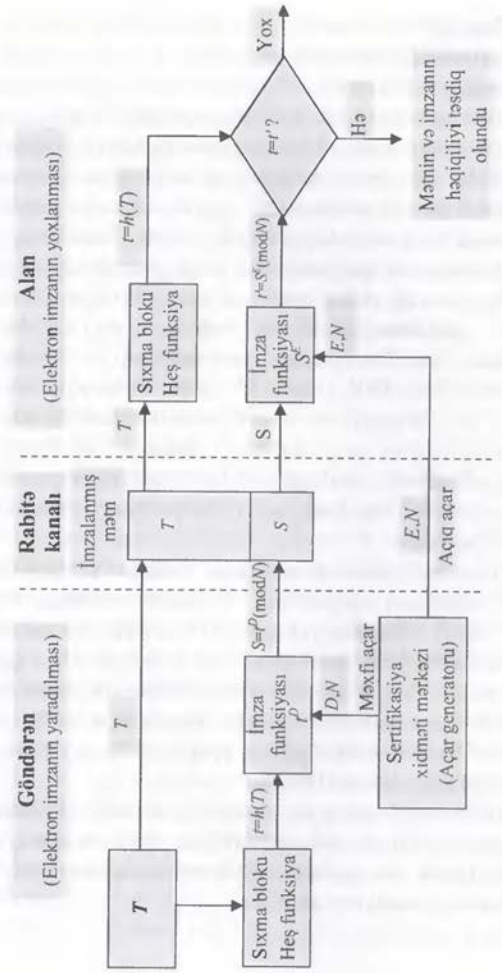
Nəhayət, alınmış t və t' qiymətləri müqayisə olunur.

Əgər bu qiymətlər bərabər olarsa, onda məlumatın və imzanın həqiqiliyi təsdiq edilir, əks halda isə imza və ya məlumat təhrif edilmiş hesab olunur.

6.5. Açarların idarə olunması və açıq açar infrastrukturu

Elektron imza texnologiyasının reallaşdırılması üçün həlli zəruri olan əsas məsələlərdən biri də açarların idarə olunmasıdır.

Açarların idarə olunması – aşağıdakı funksiyaları həyata keçirən informasiya prosesidir:



Şək.6.3. RSA elektron imza alqoritminin ümumiləşdirilmiş sxemi

Sonra heş qiymət imza funksiyası vasitəsilə məxfi açardan (D,N) istifadə edilməklə şifrlənir:

$$S=t^D \bmod N.$$

Nəticədə, alınmış informasiya elektron imza qismində göndərilən məlumata əlavə edilərək (T,S) cütlüyü S elektron imzası ilə imzalanmış T sənədi qismində alan tərəfə göndərilir. Beləliklə, məlumat imzalanmış olur.

Elektron imza prosesinin ikinci hissəsində elektron imzanın yoxlanılması həyata keçirilir. Belə ki, alan tərəf rabitə kanalı vasitəsilə aldığı (T,S) cütlüyünə əsasən elektron imzanın həqiqiliyini yoxlayır.

Bunun üçün, o, əvvəlcə, T məlumatını sıxır, yəni göndərənin heş funksiyasına analoji olaraq, $t=h(T)$ heş qiymətini hesablayır. Sonra göndərənin açıq açarının (E,N) köməyi ilə S elektron imzasından heş funksiyanın qiymətini bərpa edir:

$$t'=S^E \bmod N.$$

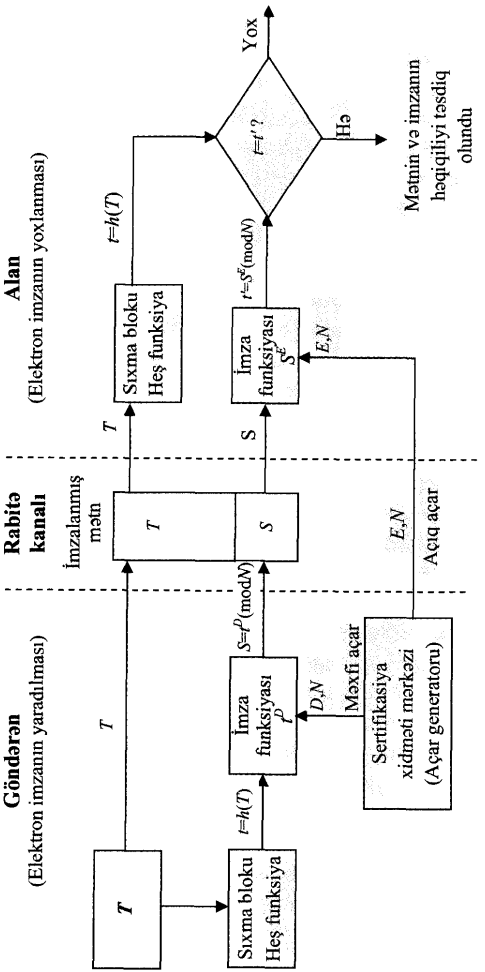
Nəhayət, alınmış t və t' qiymətləri müqayisə olunur.

Əgər bu qiymətlər bərabər olarsa, onda məlumatın və imzanın həqiqiliyi təsdiq edilir, əks halda isə imza və ya məlumat təhrif edilmiş hesab olunur.

6.5. Açarların idarə olunması və açıq açar infrastrukturu

Elektron imza texnologiyasının reallaşdırılması üçün həlli zəruri olan əsas məsələlərdən biri də açarların idarə olunmasıdır.

Açarların idarə olunması – aşağıdakı funksiyaları həyata keçirən informasiya prosesidir:



Şək.6.3. RSA elektron imza alqoritminin ümumiləşdirilmiş sxemi

- açarların generasiyası;
- açarların saxlanılması;
- açarların paylanması.

Açarların generasiyası dedikdə açarların yaradılması prosedurası və vasitələri başa düşülür. Ciddi informasiya sistemlərində açarların generasiyası üçün xüsusi aparat və proqram vasitələrindən (bir qayda olaraq, psevdotəsadüfi ədəd vericilərindən) istifadə olunur. Təbii təsadüfi proseslərə əsaslanan qurğular daha ideal generatorlar hesab edilir. Məsələn, ağ radio səs-küyü əsasında açar generasiya edən qurğuların ciddi nümunələri artıq praktikada mövcuddur. Belə ki, Pentium prosessorlarının özəyində təsadüfi ədədlərin fiziki vericiləri quraşdırılmışdır. Standart riyazi üsullar vasitəsilə hesablanan transsendent ədədlərin (məsələn, π və ya e ədədləri) onluq işarələri təsadüfi riyazi obyekt kimi qəbul edilə bilər. Praktikada psevdotəsadüfi ədədlərin hesablanması üçün proqram generatorları da reallaşdırılır.

Açarların saxlanılması dedikdə onların saxlanması, mühafizə olunması, qeydiyyatı və məhv edilməsi başa düşülür. Məxfi informasiyaya girişi açan ilk əsas obyekt kimi açar bədniyyətli şəxsi daha çox cəlb edir. Ona görə də oxunması və köçürülməsinin mümkünlüyü baxımından gizli açarlar, o cümlədən istifadə olunan açarlar barədə məlumatlar yaddaş qurğularında açıq şəkildə deyil, daim şifrlənmiş şəkildə saxlanılmalıdır.

Açar informasiyasının şifrlənməsi üçün istifadə olunan açarlar *master açarlar* adlanır. İstifadəçilərə master açarlarını hər hansı bir maddi daşıyıcıda saxlamamaları və əzbər bilmələri tövsiyə olunur.

Kifayət qədər mürəkkəb informasiya sistemlərində bir istifadəçi böyük həcmdə açar informasiyası ilə işləyə bilər. Bəzən, hətta açar informasiyası üzrə kiçik məlumat bazasının yaradılması zərurəti yaranır. Belə bazalar istifadə olunan açarların alınması, saxlanması, mühafizəsi, qeydiyyatı və silinməsi məsələlərinə cavabdeh olur.

Açar informasiyasının (həm adi açarların, həm də master açarların) dövri olaraq dəyişdirilməsi informasiya təhlükəsizliyi baxımından ən vacib şərtlərdən biridir. Daha məsuliyyətli informasiya sistemlərində açarların yeniləşdirilməsinin hər gün həyata keçirilməsi zəruridir.

Açarların paylanması – açarların idarə olunmasında ən vacib prosesdir. Ona iki tələb qoyulur:
- paylanmanın operativliyi və dəqiqliyi;
- paylanan açarların gizliliyi.

Simmetrik (biraçarlı) şifrləmə sistemlərində təhlükəsiz informasiya mübadiləsi aparmaq istəyən iki istifadəçi əvvəlcə təhlükəsiz ümumi açar təyin etməlidirlər. Bunun mümkün yollarından biri üçüncü tərəfin (məsələn, kuryerin) istifadə olunmasıdır. Praktikada təhlükəsizlik baxımından bu açarlar vaxtaşırı dəyişdirildiyi üçün kuryerin və ya digər müvafiq vasitənin istifadəsini baha başa gələn və qeyri-effektiv edir.

Ümumi açarların alınmasının alternativ yolu açarların paylanması mərkəzlərinin reallaşdırılmasıdır. Onun köməyi ilə hər bir istifadəçi cütləri ümumi açardan istifadə etməklə bir-biri ilə təhlükəsiz qarşılıqlı əlaqə qura bilərlər.

Açarların idarə olunması fəaliyyəti "Elektron imza və elektron sənəd haqqında" Azərbaycan Respublikasının Qanunu ilə nizamlanan açarların paylanma mərkəzi, yəni *sertifikasiya xidməti mərkəzi* tərəfindən həyata keçirilir.

Elektron imza infrastrukturunun qurulmasında sertifikasiya xidməti mərkəzlərinin yaradılması çox böyük əhəmiyyət kəsb edir. Bu mərkəzlər, açıq və məxfi açarların generasiyası ilə yanaşı, məxfi açarların sahiblərinə çatdırılmasını və saxlanılmasını, açıq açarların yayılmasını və yoxlanılmasını, elektron sertifikatların yaradılmasını və mərkəzləşdirilmiş qaydada idarə olunmasını, sertifikat sahiblərinin identikləşdirilməsini (tanınmasını) və digər funksiyaları yerinə yetirir. Sertifikat xidməti mərkəzi tərəfindən imzalanmış açıq açar "açıq açar sertifikatı" adlanır.

Belə mərkəzə müraciət edən istifadəçi bu və ya digər istifadəçinin sertifikatını, yəni açıq açarını ala, eləcə də bu və ya digər açıq açarın qüvvədə olub-olmamasını yoxlaya bilər. Bu baxımdan, istənilən istifadəçinin həqiqi açıq açarına bütün digər istifadəçilərin girişinin, bu açarların bədniyyətli şəxslər tərəfindən dəyişdirilməsindən qorunmasının, eləcə də etibardan düşmüş açarların geri çağırılmasının təmin edilməsi zəruridir.

Açarların dəyişdirilmədən qorunması məsələsi sertifikatlar vasitəsi ilə həll edilir. *Sertifikat* – sahibi haqqında ona daxil edilmiş məlumatları və onun açıq açarını hər hansı etibarlı şəxsin imzası ilə təsdiq etməyə imkan verir. Mərkəzləşdirilmiş sertifikat sistemlərində (məsələn, PKI) etibarlı təşkilatlar tərəfindən himayə edilən sertifikasiya mərkəzləri istifadə olunur. Paylanmış sertifikat sistemlərində (məsələn, PGP) tanışların və etibarlı şəxslərin sertifikatlarını çarpaz imzalamaq yolu ilə hər bir istifadəçi tərəfindən etibarlılıq şəbəkəsi yaradılır.

Qeyd olunduğu kimi, açıq açar infrastrukturu informasiya təhlükəsizliyi sisteminin aşağıdakı əsas məsələlərinin həllini təmin edir:

- informasiyanın saxlanılması və açıq rabitə kanalı vasitəsilə ötürülməsi zamanı şifrləmə alqoritmləri vasitəsilə ilə onun məxfiliyinin təmin edilməsi;
- informasiyanın saxlanılması və açıq rabitə kanalı vasitəsilə ötürülməsi zamanı elektron imza texnologiyasının köməyi ilə onun tamlığının təmin edilməsi;
- istifadəçilərin, həmçinin, onların müraciət etdikləri resursların autentifikasiyasının təmin edilməsi;
- informasiyaya müraciət edərkən istifadəçilər tərəfindən yerinə yetirilmiş hərəkətlərdən imtina olunmasının qeyri-mümkünlüyünün təmin edilməsi.

Açarların paylanması mərkəzi ilə istifadəçi arasında məlumat mübadiləsinin təşkili üçün qeydiyyat zamanı həmin istifadəçiyə xüsusi açar verilir. Hər bir istifadəçiyə ayrı-ayrı açarlar verildiyindən onlardan hər hansının ələ keçməsi o qədər də ciddi fəsadlar törətmir. Belə sxemdə zəif yer ondan ibarətdir ki, bədniyyətli şəxs bütün açarların toplandığı açarların idarə olunması mərkəzinə daxil ola, nəticədə isə bütün sistem təhlükə qarşısında qala bilər.

6.6. Effektiv açıq açar infrastrukturunun yaradılması metodikası

Açıq açar infrastrukturunun yaradılmasının kifayət qədər çətin və uzunmüddətli iş olduğunu nəzərə alaraq, açıq açar infrastrukturunun effektiv tətbiqi, eləcə də səhvlərin yaranması ehtimalının azaldılması məqsədilə Baltimore Technologies şirkəti tərəfindən KeySteps adlanan xüsusi metodika işlənib hazırlanmışdır.

Metodika yeddi mərhələdən ibarətdir:

Mərhələ 1. Sistemə qoyulan tələblərin təhlili. Açıq açar infrastrukturunun fəaliyyətinə qoyulan əsas tələblər, sistemin resurslarının informasiya təhlükəsizliyinin zəruri səviyyəsi, eləcə də normativ-hüquqi məhdudiyyətlər müəyyən edilir.

Mərhələ 2. Arxitekturanın müəyyən edilməsi. Açıq açar infrastrukturunun əsas arxitektura məsələləri, onun reallaşdırılması üsulları, proqram-texniki vasitələr, qarşılıqlı fəaliyyət rejimləri və digər sistem parametrləri müəyyən edilir.

Mərhələ 3. Proseduraların müəyyən edilməsi. Açıq açar infrastrukturunun komponentlərinin fəaliyyət rejimləri müəyyən edilir, effektivliyin təmin edilməsi üçün zəruri olan idarəetmə qaydaları (siyasəti) formalaşdırılır.

Mərhələ 4. Təhlükəsizlik sisteminin xülasəsi. Təklif olunan açıq açar infrastrukturunun müstəqil ekspert xülasəsi həyata keçirilir, eləcə də mümkün risklərin təhlili aparılır və onların minimuma endirilməsi tədbirləri işlənib hazırlanır.

Mərhələ 5. İnteqrasiya. Açıq açar infrastrukturunun eskiz modeli yaradılır, informasiya sisteminə inteqrasiyası həyata keçirilir, istifadəçilər və xidmət personalı öyrədilir, onun təcrübi istismarına başlanması planı formalaşdırılır.

Mərhələ 6. Quraşdırma və fəaliyyətə başlama. Açıq açar infrastrukturunun quraşdırılması, iş qabiliyyətinin yoxlanması, qəbul sınaqları həyata keçirilir.

Mərhələ 7. İstismar. Təcrübi istismarın nəticələrinə əsasən açıq açar infrastrukturu üzərində izlər sona çatdırılır, gələcək xidmət və inkişaf proseduraları planlaşdırılır.

Metodikanın istifadəsi açıq açar infrastrukturunun yaradılması və tətbiqi üçün tələb olunan xərcləri və müddəti azaltmağa imkan verir. Onun mərhələlərinin ardıcıl yerinə yetirilməsi açıq açar infrastrukturunun müvafiq tələblər səviyyəsində müvəffəqiyyətlə qurulmasına və tətbiqinə zəmanət verir.

VII FƏSİL

STEQANOQRAFİYA

Steqanoqrafiya və onun istiqamətləri

Klassik steqanoqrafiya və onun inkişaf tarixi

Praktikada daha çox istifadə olunan klassik steqanoqrafik üsullar

Kompyuter steqanoqrafiyası və onun əsas prinsipləri

Kompyuter steqanoqrafiyasının məşhur üsulları və proqramları

Rəqəmli steqanoqrafiya

7.1. Steqanoqrafiya və onun istiqamətləri

Qeyd olunduğu kimi, steqanoqrafiya elmi də informasiya təhlükəsizliyinin təmin edilməsi problemi ilə məşğul olur. Steqanoqrafiyanın vəzifəsi informasiyanın varlığını, saxlanılması, emal olunması və ötürülməsi faktını gizlətməkdən ibarətdir. Başqa sözlə, steqanoqrafik üsulların əsas məqsədi qorunan (o cümlədən məxfi) məlumatın varlığının rəqibdən gizli saxlanmasıdır.

Steqanoqrafiya kriptoqrafiyaya nisbətən daha qədim tarixə malikdir və daha erkən dövrlərdən istifadə edilməyə başlamışdır. "Steqanoqrafiya" sözünün yunan dilindən tərcüməsi "məxfi yazı" (steganos – sirr, məxfi görülən iş, graphy – yazı) mənasını verir.

Məlum olduğu kimi, əksər ölkələrdə kriptoqrafik üsul və vasitələrin reallaşdırılmasına, istifadəsinə və tətbiqinə qanunvericiliklə müəyyən ciddi məhdudiyyətlər, qadağalar qoyulur. Adətən, istifadə olunan şifrləmə sistemlərinin açarlarının dövlətə verilib-verilməməsi, aparat və ya proqram vasitələri şəklində reallaşdırılmasından asılı olmayaraq kriptoqrafik sistemlərin məcburi qeydiyyatı və lisenziyalaşdırılması kimi tələb qoyulur.

Kriptoqrafiyadan fərqli olaraq, müasir dövrdə steqanoqrafiyanın istifadəsinə belə məhdudiyyətlər, qadağalar qoyulmur və praktikada informasiyanın gizlədilməsi üçün effektiv vasitə kimi istifadə olunmaqda davam edir.

Qeyd edilməlidir ki, steqanoqrafiya kriptoqrafiyanı əvəz etmir, onu tamamlayır və məxfi informasiyanın bədniyyətli

şəxslərdən daha ciddi qorunmasını təmin edir. Belə ki, məlumatın steqanoqrafik üsullar vasitəsilə gizlədilməsi onun ötürülməsi faktının aşkarlanması ehtimalını əhəmiyyətli dərəcədə kiçildir. Əgər bu zaman məlumat həm də şifrlənərsə, onda o, əlavə olaraq daha bir qoruma səviyyəsi ilə təmin edilmiş olar.

Aydındır ki, hər hansı məlumatın varlığını daha böyük həcmli informasiya massivində gizlətmək (iynəni samanda gizlətmək kimi) daha asandır. Müasir dövrdə steqanoqrafiya əsasən məxfi məlumatın tamamilə başqa məzmunlu daha böyük həcmli informasiyanın içində gizlədilməsi (əridilməsi) prinsipinə əsaslanır.

Xüsusilə vurğulanmalıdır ki, steqanoqrafiya sadəcə məxfi məlumatın ötürülməsi zamanı deyil, məxfi məlumatın məxfi ötürülməsi zamanı daha faydalı olur. Əlbəttə, belə gizli məlumat mübadiləsi bir sıra çatışmazlıqlarla müşayiət olunur.

Əvvəla, istifadə olunan steqanoqrafik üsulun davamlılığını qiymətləndirmək və əsaslandırmaq olduqca çətindir. Belə ki, əgər məxfi məlumatın açıq məlumatlar massivinə qarışdırılması üsulu bədniyyətli şəxsə məlum olarsa, onda davamlılıq haqqında fikir söyləmək çox çətindir.

İkincisi, steqanoqrafik üsulların istifadəsi zamanı məxfi məlumatların qarışdırıldığı saxlanılan və ötürülən ümumi məlumatların həcmi çox zaman xeyli böyüyür. Bu da məlumatların emalı sistemlərinin məhsuldarlığına ciddi, mənfi təsir göstərir.

Ümumiyyətlə, steqanoqrafik üsullar müasir dövrdə əsasən aşağıda qeyd olunan məsələlərin həlli üçün istifadə edilir:

- məxfi informasiyanın icazəsiz girişdən qorunması;
- şəbəkə resurslarının monitorinqi və idarə olunması sistemlərini adlamaq (dəf etmək);
- informasiyanın və onu emal edən proqram təminatının kamuflyaj edilməsi (gizlədilməsi);
- müəyyən növ intellektual mülkiyyət üzərində müəlliflik hüququnun qorunması.

Aparılmış tədqiqatlar göstərir ki, steqanoqrafiyanı üç əsas kateqoriyaya ayırmaq olar:

- klassik steqanoqrafiya;
- kompyuter steqanoqrafiyası;
- rəqəmli steqanoqrafiya.

7.2. Klassik steqanoqrafiya və onun inkişaf tarixi

Tarixi mənbələrdə steqanoqrafiya haqqında rast gəlinən ilk məlumat Heradota məxsusdur. O, e.ə.477-ci ildə öz əsərində iki steqanoqrafik məktubun göndərilməsi faktını təsvir etmişdir.

Birinci fakt İran hökmdarı Daranın fərmanı ilə Suzda saxlanılan qəddar tiran Qisti ilə bağlıdır. O, Miletdə yaşayan bir qohumu ilə əlaqə saxlamaq istəyir. Məktubunun kənar əllərə düşməsinin qarşısını almaq üçün Qisti bir qulun saçını daz qırxdıraraq onun başının dərisinə məxfi məktubu döydürmüş (tatuirovka etdirmiş), saçın uzanmasını gözləmiş və yalnız bundan sonra qulu bir bəhanə

ilə Miletə göndərmişdir. Orada qulun saçını yenidən daz qırxaraq məktubu oxumuşlar.

İkinci halda, mumlanmış taxta parçasının üzərindən əvvəlcə mumu qazıyıb təmizləmiş və bilavasitə taxtanın üzərinə məxfi məktubu cızmış, sonra yenidən taxtanın üzərinə mum çəkmiş və mumun üzərinə iti çubuqla açıq məktubun mətnini yazmışlar. Belə şəkildə hazırlanmış göndəriş ünvana çatdırılmışdır. Ünvanda mumu təmizləməklə məxfi məktubu oxumuşlar.

Çində məxfi məktubları ipək parçanın zolaqlarına yazırmışlar. Məlumatı gizlətmək üçün ipək parça zolaqlarını kürələr şəklində yumurlayaraq üstünü mum ilə örtürmüşlər. Məlumatı aparan kuryer belə hazırlanmış kürələri udaraq ünvana çatdırarmış.

Qədim Romada məxfi məlumatı digər yazılar üzərində sətirlər arasında meyvə şirəsi, süd, sidik və s. vasitəsilə yazırdılar. Bu üsuldan yaxın tarixdə də istifadə olunmuşdur. Belə ki, Rusiyada 20-ci əsrin əvvəlində inqilabçılar, o cümlədən V.İ.Lenin də öz əsərlərini yazmaq üçün süddən istifadə etmişdir.

Steqanoqrafiya orta əsrlərdə də daim istifadə olunmuş və inkişaf etmişdir. XV əsrdə kriptoqrafiya və steqanoqrafiya ilə məşğul olan rahib Triteius (1462-1516-cı illərdə yaşamışdır) 1499-cu ildə yazdığı "Steganographia" əsərində məlumatların gizli ötürülməsi üçün çoxlu sayda üsulları təsvir etmişdir.

Fransanın Bordo şəhərində üsyan etmiş kəndlilər tərəfindən həbs edilmiş rahib Berto da öz həyatını xilas etmək

üçün gizli yazıdan istifadə etmişdir. Belə ki, üsyançılar rahib Bertoya tanışı keşiş Bleyə məktub yazmağa icazə verirlər. Məktubda gizli yazı yazan Berto məktubun sonunda "Sizə məlhəm göndərirəm, onunla gözünüzü silin və Siz yaxşı görəcəksiniz" cümləsini qeyd edir. Bununla o, gizli yazının necə oxunmasını da tanışı keşiş Bleyə çatdırır. Beləliklə, gizli məktubun oxunması nəticəsində Berto ölümdən xilas edilir.

Steqanoqrafik üsullardan XVIII əsrdə vətəndaş müharibəsi zamanı amerikalılar da fəal istifadə etmişlər. Belə ki, 1799-cu ildə şimallıların iki agenti (Semuel Vudxull və Robert Tounsend) xüsusi mürəkkəbdən istifadə etməklə Corc Vaşinqtona məlumatlar ötürürdülər.

XX əsrin əvvəllərində və ortalarında baş vermiş birinci və ikinci dünya müharibələri steqanoqrafiyanın inkişafına əhəmiyyətli təkan verdi. Bu sahədə almanlar daha ciddi nailiyyətlər əldə etmişdilər. Belə ki, onlar müharibə dövründə mikrofotoqrafiya texnologiyasından geniş istifadə etmişlər.

Mikrofotoqrafiya standart çap vərəqlərinin, sxemlərin və çertyojların adi mətbəə nöqtəsi ölçüsündə mikro şəklinin çəkilməsinə imkan verirdi. Belə bir və ya bir neçə nöqtə adi məktublara yapışdırılır və ötürülürdü. Adi nöqtələr ölçüsündə olan belə mikro şəkilləri tapmaq və aşkar etmək olduqca çətin idi. Bu texnologiya çox böyük həcmli informasiyanı, o cümlədən sxemləri və çertyojları ötürməyə imkan verirdi.

7.3. Praktikada daha çox istifadə olunan klassik steqanoqrafik üsullar

Praktikada müxtəlif növ steqanoqrafik üsullardan istifadə olunmuşdur və bəziləri indiyədək istifadə olunmaqda davam edir. Tətbiq olunan mexanizm və vasitələrə görə steqanoqrafik üsulları iki kateqoriyaya bölmək olar:

- ənənəvi (qeyri-texniki) üsullar
- xüsusi texniki vasitələr istifadə edilməklə reallaşdırılan steqanoqrafik üsullar.

Ənənəvi (qeyri-texniki) üsullar dedikdə xüsusi texniki vasitələr istifadə olunmadan, gizli yazılar, şərti ifadələr, kodlaşdırma və s. yollarla həyata keçirilən üsullar başa düşülür. Qeyri-texniki üsullara nümunə kimi aşağıdakıları göstərmək olar:

- *Açıq mətnin konkret hərflərinə görə məlumatın ötürülməsi.* Məlumat açıq məktubun mətnində istifadə olunan sözlərinin (cümlələrinin, abzaslarının və s.) birinci və ya başqa sırada duran hərfinə görə yazılır və oxunur.
- *"İkibaşlı" yazının və kodlaşdırılmış (şərti) sözlərin və ya ifadələrin istifadəsi.* Açıq məlumatın mətni müəyyən şəkildə yozulur, ona ayrı məna verilir və ya əvvəlcədən şərtiləşdirilmiş ifadələr vasitəsilə kodlaşdırılır.
- *"Ave Mariya" şifri.* Məlumatın kodlaşdırılması üçün ilkin mətnin hər bir sözünün və ya söz birləşməsinin əvəzinə açıq dini mövzuda bir neçə söz qoyulur. Beləliklə, ötürülən məlumat tamamilə dini məzmunlu məxsusi yazı xarakteri alır.

- *Ümumi məlumatların istifadəsi.* Qarşı tərəfə zəruri informasiyanın çatdırılması üçün hər hansı əşya, fakt, hadisə (məsələn, malların siyahısı, topdansatış qiymətləri, televiziya verilişlərinin proqramı və s.) barəsində məlumat müəyyən olunmuş qaydada (ardıcıllıqda) xəbər verilir.
- *Hərflərin qeyd olunması.* Məlumat yazılması üçün hər hansı kitabın və ya qəzetin konkret yerində (səhifəsində) hərflər iti əşya (iynə və ya sancaq) batırmaqla qeyd olunur. Sözlərin sonu hərflər arasında deşik açmaqla (iynə və ya sancaq vasitəsilə) müəyyən edilir.
- *Trafaretə görə yazma.* Açıq məktubun yazılacağı təmiz vərəqin üzərinə qabaqcadan hazırlanmış "pəncərələri" (müəyyən olunmuş yerlərdə kəsilmiş xanaları) olan trafaret qoyulur. Ötürülən məlumat trafaretin pəncərələri vasitəsilə kağız üzərinə qeyd edilir və trafaret götürülür. Sonra kağız üzərinə səpələnmiş hərflərin arasına diqqətlə həmin hərflər istifadə olunmaqla açıq mətn yazılır.
- *Krossvordda yazma.* Məlumat məqsədli doldurulmuş krossvordun sütunlarında (və ya sətirlərində) yazılır, sətirlər (və ya sütunlar) isə ixtiyari qaydada doldurulur. Bu zaman məlumat birbaşa yazıla və ya əlavə olaraq kodlaşdırıla bilər.
- *"Korlanmış" makina yazısının istifadəsi.* Məlumatın yazılması üçün korlanmış makinada çap olunan yazıya oxşar kodlaşdırmadan istifadə edilir. Belə ki, yazıda bəzi hərflər korlanmış (xarab olmuş) makinadakı kimi sətrin yuxarısına və ya aşağısına düşür. Bu zaman bu

hərflərin ardıcıllığı və sayı, eləcə də onların rast gəlinmə tezliyi nəzərə alınır. Burada Morze əlifbası vasitəsilə kodlaşdırma mümkündür.
- *Not yazılarından istifadə.* Məlumatın kodlaşdırılması üçün not dəftərində notların əl ilə yazılmasından istifadə olunur. Bu zaman notlar müəyyən qiymətə (koda) malik olur. Belə not dəftərində Morze və ya digər əlifba vasitəsilə kodlaşdırmadan istifadə oluna bilər.
- *Kardioqramın və ya qrafikin istifadəsi.* Məlumatın kodlaşdırılması üçün kardioqramdan və ya hər hansı mexaniki prosesin qrafikindən istifadə olunur. Burada da Morze əlifbası və ya digər kodlaşdırma reallaşdırıla bilər. Məsələn, Morze əlifbası üçün qrafikin (kardioqramın) ən yuxarı piklərdən nöqtəni, ən aşağı piklərdən tireni, dişlər arasındakı xətlərdən hərflərarası məsafəni, xətlərin qırılmasından sözlərin sonunu və s. göstərmək üçün istifadə etmək mümkündür.
- *Kart və ya kağız dəstinin yan tərəfində yazma.* Məlumat müəyyən qaydada düzülmüş oyun kartı və ya kağız dəstinin (paçkasının) yan tərəflərində yazılır. Oyun kartı və ya kağız dəsti qarışdırılır və ünvana göndərilir. Orada həmin dəst müəyyən olunmuş qaydada düzülür və yazı oxunur.
- *Etiketə yazma.* Məlumat flakonun, bankanın, butulkanın və s. etiketlərinin arxasına yazılır və sonradan yapışdırılır.
- *Poçt markasının arxasına yazma.* Məlumat markanın arxasına yazılır və məktubun üzərinə yapışdırılır.

Həmçinin məlumat məktub üzərində marka üçün nəzərdə tutulmuş yerdə yazıla və sonra üstündən marka yapışdırıla bilər.

- *Kibrit qutusunun içəri tərəfinə yazma.* Əvvəlcə kibrit qutusu sökülür, onun içəri səthinə yazı yazılır və sonra qutu yenidən yapışdırılır.
- *Bişmiş yumurtanın içinə yazma.* Bunun üçün zəy, mürəkkəb və sirkə qarışığı götürülür. Lazım olan məlumatı bu qarışıqla yumurtanın qabığı üzərinə yazırlar. Qabığın səthindən yazının izini silmək üçün yumurtanı bir müddət tünd duzlu suda və ya sirkədə saxlayırlar. Bundan sonra yumurtanı bərk bişirirlər. Bu zaman bütün yazı yumurtanın qabığının altında zülalın üzərinə həkk olunur. Alan tərəf yumurtanın qabığını soymaqla yazını oxuyur.
- *Düyünlər vasitəsilə yazma.* Burada əlifbanın hərfləri barmağın çevrəsinin uzunluğu ilə və ya santimetrlərlə kodlaşdırılır. Məsələn, A – 1 sm. və ya 1 barmaq çevrəsi, B – 2 sm. və ya 2 barmaq çevrəsi və s.). Məlumatı ötürmək üçün hər hansı ipin üzərində bu ölçülərə uyğun olaraq düyünlər vurulur. İpi barmağa dolamaq və ya santimetrlərlə ölçmək yolu ilə yazını oxuyurlar.

Texniki vasitələrdən istifadə etməklə reallaşdırılan üsullara aşağıdakı nümunələri göstərmək olar:

- *Rəngsiz mürəkkəbin istifadəsi.* Məlumat rəngsiz xüsusi mürəkkəbdən istifadə etməklə adi məktubun sətirləri arasına yazılır. Belə yazı müəyyən fiziki və ya kimyəvi təsirlər nəticəsində görünür.

- *Xüsusi işıq effektləri altında görünən yazılar.* Məlumat xüsusi maddələrdən istifadə etməklə xüsusi kağız üzərinə gözə görünməz şəkildə yazılır. Belə yazı yalnız ultrabənövşəyi əksetmə, polyarlaşmış işıq və ya lüminessensiya zamanı görünür.
- *İşıq şüaları.* Məxfi məlumatın ötürülməsi üçün əlaqə daşıyıcılarının kəskin istiqamətlənmiş şüaları istifadə olunur.
- *İşıq fotonlarının kvant kanalı.* Məxfi məlumatın, o cümlədən məxfi açarın ötürülməsi üçün işıq fotonlarının kvant kanalı istifadə olunur.
- *Mikro fotoçəkiliş.* Məxfi məlumatın ötürülməsi üçün səhifələrin həddən artıq miniatür şəklinin çəkilməsi, yəni mikronöqtə texnologiyasından istifadə olunur. Adi mətbəə nöqtəsi böyüklükdə belə bir mikronöqtəyə bir standart çap vərəqini yerləşdirmək mümkündür.
- *Mikromətn texnologiyası.* Məxfi məlumat mikroçiplərin istehsalı texnologiyasından istifadə etməklə mikromətn şəklində yazılır və elektron mikroskop vasitəsilə oxunur.
- *Disklərə xüsusi şəkildə yazma.* Disklərin DOS əməliyyat sistemlərindən fərqli yolla formatlaşdırılır və informasiya belə sektorlarda gizlədilir. İnformasiyanın saxlanması üçün, həmçinin, DOS əməliyyat sistemi tərəfindən istifadə olunmayan, lakin başqa yollarla oxuna bilən cığırlardan istifadə oluna bilər. İnformasiya və ya viruslar xüsusi şəkildə ikilik kodlar

səviyyəsində korlanmış bloklara və ya dayanıqsız bitlərə yazılaraq gizlədilir.

- *Maskalanma.* Məxfi informasiyanın bitləri səs-küy, əngəl, maneə, səhv (təhrif olunmuş) bitlər adı altında maskalanır. Bu yanaşma kommersiya rabitə kanallarında, elektron rəqəmli fotolarda, video kadrlarda, səs (nitq) yazısında və s. reallaşdırıla bilər.

7.4. Kompyuter steqanoqrafiyası və onun əsas prinsipləri

Kompyuter texnologiyaları steqanoqrafiyanın inkişafına və təkmilləşməsinə yeni təkan verdi və informasiya təhlükəsizliyi sahəsində yeni bir istiqamətin – kompyuter steqanoqrafiyasının yaranmasına səbəb oldu.

Qlobal kompyuter şəbəkələrinin günbəgün inkişaf etməsi və daha geniş istifadə olunması ilə əlaqədar olaraq, steqanoqrafiya daha böyük əhəmiyyət kəsb etməyə başlayır. Kompyuter steqanoqrafiyasının inkişaf tendensiyasının təhlili göstərir ki, kompyuter steqanoqrafiyası üsulları artan tendensiya ilə inkişaf edir və yaxın illərdə bu üsulların inkişafına maraq getdikcə daha çox artacaqdır.

Eyni zamanda ümumi təyinatlı İnternet şəbəkəsinin hərtərəfli inkişafı və geniş yayılması, İnternet vasitəsilə informasiya mübadiləsi zamanı tələb olunan müəlliflik hüququnun qorunması, şəxsi sirrsaxlama hüququnun qorunması, elektron ticarətin təşkili, elektron bank əməliyyatlarının həyata keçirilməsi, hakerlərin, terrorçuların

fəaliyyətinin qarşısının alınması və s. kimi axıra qədər həll edilməmiş məsələlər informasiyanın qorunmasının yeni üsul və vasitələrinin reallaşdırılmasını zəruri edir. Digər tərəfdən, informasiya texnologiyalarının sürətli inkişafı təklif olunan yeni üsulları reallaşdırmağa imkan verir.

Əlbəttə, informasiyanın qorunması sahəsində reallaşdırılan kriptoqrafik üsullar müəyyən məsələləri həll etməyə imkan verir. Lakin qeyd olunmalıdır ki, ziyanverici proqramlar (kompyuter virusları, troya atları, məntiqi bombalar və s.), reklam, replika, spam xarakterli proqramlar və s. kimi informasiya silahlarının dağıdıcı təsirləri ilə bağlı məsələlər hələ də həll olunmamış qalır.

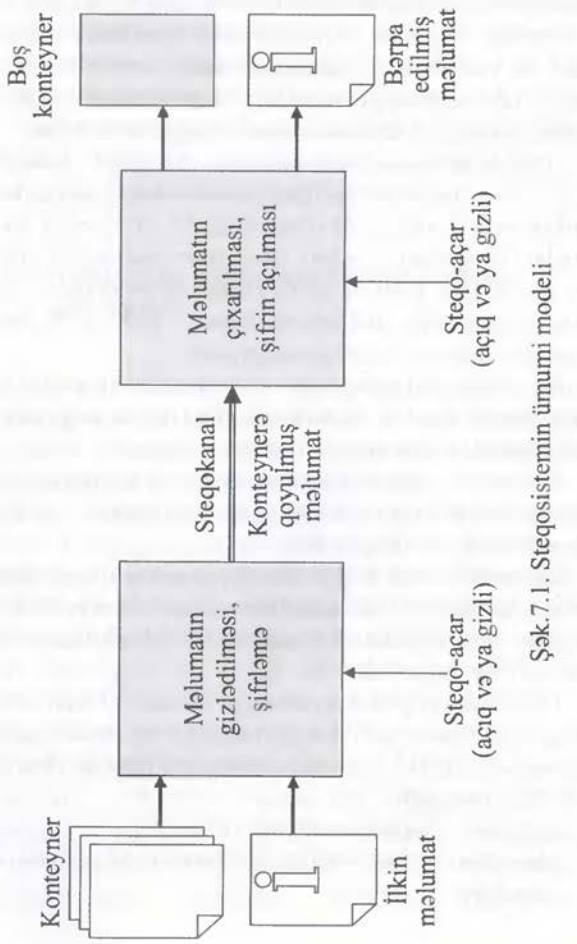
Bu baxımdan kompyuter steqanoqrafiyası üsullarının kriptoqrafik üsulları ilə birləşdirilməsi və ya birgə tətbiqi ciddi nəticələr əldə etməyə imkan verə bilər.

Kompyuter steqanoqrafiyası – klassik steqanoqrafiyanın kompyuter texnologiyaları əsasında inkişafı nəticəsində yaranmış yeni istiqamətidir.

Kriptosistemlərə analoji olaraq, steqanoqrafiyada steqosistem terminindən istifadə olunur. *Steqosistem* – informasiyanın gizli ötürülməsi kanalının formalaşdırılması üsul və vasitələri toplusudur.

Ümumiləşdirilmiş steqosistemin modeli 7.1 saylı şəkildə göstərilmişdir. Şəkildən göründüyü kimi, müasir steqosistemlərdə (yəni kompyuter steqanoqrafiyasında) əsas iki növ fayl mövcuddur:

- *məlumat* – gizlədilməsi tələb olunan fayl;
- *konteyner* – məlumatın gizlədilməsi üçün istifadə olunan fayl.



Şək.7.1. Steqosistemin ümumi modeli

Qeyd etmək lazımdır ki, konteynerlərin iki növünü fərqləndirirlər. *Orijinal* və ya "*boş*" konteyner – tərkibində gizli informasiya olmayan konteynerdir. *Yekun* və ya "*doldurulmuş*" konteyner – tərkibində gizli informasiya yerləşdirilmiş konteynerdir.

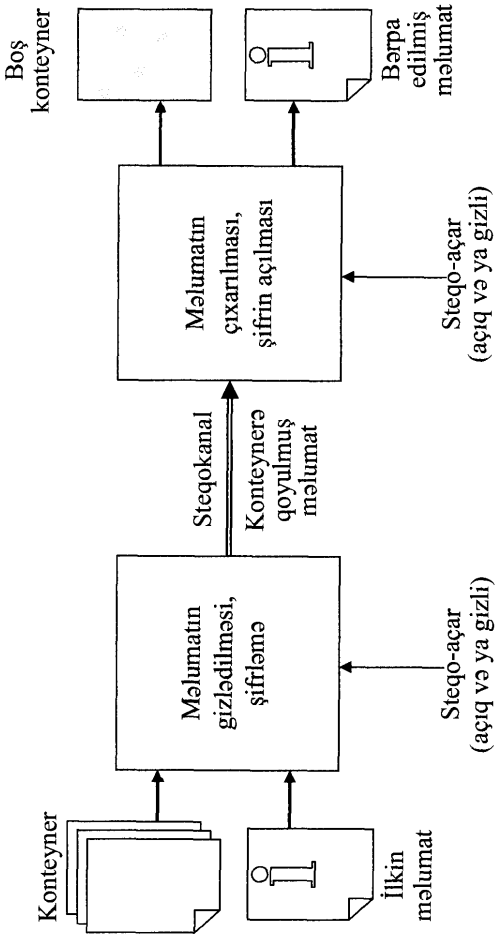
Steqanoqrafik açar dedikdə məlumatın konteynerə daxil edilməsi qaydalarını müəyyən edən məxfi element başa düşülür.

Steqanoqrafik üsulların kompyuterdə reallaşdırılması zamanı əsas müəyyənedici amil məlumatların kodlaşdırılması üsulunun seçilməsindən ibarətdir. Həmçinin, qeyd olunmalıdır ki, qlobal kompyuter şəbəkələrinin və multimedia vasitələrinin müasir tərəqqisi telekommunikasiya kanalları vasitəsilə ötürülən məlumatların təhlükəsizliyinin təmin edilməsi üçün nəzərdə tutulmuş yeni üsulların işlənib hazırlanmasına gətirib çıxarmışdır.

Bu üsullar, analoq tipli audio və video siqnalların rəqəmli formata çevrilməsi zamanı qurğularda yol verilən qeyri-dəqiqliklər, eləcə də siqnallarda izafiliyin mövcud olması məlumatların kompyuter fayllarında gizlədilməsinə imkan verir.

Kompyuter steqanoqrafiyası iki əsas prinsipin üzərində qurulur:

- mütləq dəqiqlik tələb edən digər növ məlumatlardan fərqli olaraq, öz funksionallığını itirmədən rəqəmli şəkil və ya səs fayllarının müəyyən dərəcədə dəyişdirilməsi mümkündür;
- insanın hissiyyat üzvləri şəkilin rəngində və ya səsin keyfiyyətində edilən cüzi dəyişikliyi fərqləndirmək qabiliyyətinə malik deyildir.



Şək.7.1. Steqosistemin ümumi modeli

Qeyd etmək lazımdır ki, konteynerlərin iki növünü fərqləndirirlər. *Orijinal* və ya "*boş*" konteyner – tərkibində gizli informasiya olmayan konteynerdir. *Yekun* və ya "*doldurulmuş*" konteyner – tərkibində gizli informasiya yerləşdirilmiş konteynerdir.

Steqanoqrafik açar dedikdə məlumatın konteynerə daxil edilməsi qaydalarını müəyyən edən məxfi element başa düşülür.

Steqanoqrafik üsulların kompyuterdə reallaşdırılması zamanı əsas müəyyənedici amil məlumatların kodlaşdırılması üsulunun seçilməsindən ibarətdir. Həmçinin, qeyd olunmalıdır ki, qlobal kompyuter şəbəkələrinin və multimedia vasitələrinin müasir tərəqqisi telekommunikasiya kanalları vasitəsilə ötürülən məlumatların təhlükəsizliyinin təmin edilməsi üçün nəzərdə tutulmuş yeni üsulların işlənib hazırlanmasına gətirib çıxarmışdır.

Bu üsullar, analoq tipli audio və video siqnalların rəqəmli formata çevrilməsi zamanı qurğularda yol verilən qeyri-dəqiqliklər, eləcə də siqnallarda izafiliyin mövcud olması məlumatların kompyuter fayllarında gizlədilməsinə imkan verir.

Kompyuter steqanoqrafiyası iki əsas prinsipin üzərində qurulur:

- mütləq dəqiqlik tələb edən digər növ məlumatlardan fərqli olaraq, öz funksionallığını itirmədən rəqəmli şəkil və ya səs fayllarının müəyyən dərəcədə dəyişdirilməsi mümkündür;
- insanın hissiyyat üzvləri şəkilin rəngində və ya səsin keyfiyyətində edilən cüzi dəyişikliyi fərqləndirmək qabiliyyətinə malik deyildir.

Müasir kompyuter steqanoqrafiyasının əsas müddəaları aşağıdakılardır:

- informasiyanın gizlədilməsi üsulları onun autentikliyini (həqiqiliyini) və tamlığını təmin etməlidir;
- fərz edilir ki, rəqibə (bədniyyətli şəxsə) bütün mümkün steqanoqrafik üsullar tam məlumdur;
- üsulların təhlükəsizliyi açıq şəkildə ötürülən fayla məxfi məlumat daxil edilən zaman onun əsas xassələrinin, eləcə də rəqibə (bədniyyətli şəxsə) qeyri-məlum olan hər hansı informasiyanın, yəni açarın steqanoqrafik çevirmələr vasitəsilə qorunmasına əsaslanır;
- hətta gizli məlumatın gizlədilməsi faktı hər hansı yolla rəqibə (bədniyyətli şəxsə) məlum olsa belə, məxfi məlumatın özünün çıxardılması (əldə olunması) mürəkkəb hesablama məsələsindən ibarət olmalıdır.

7.5. Kompyuter steqanoqrafiyasının geniş istifadə edilən üsulları və proqramları

Müasir dövrdə kompyuter steqanoqrafiyası üsulları iki əsas istiqamət üzrə inkişaf edir.

I. *Kompyuterlərdə istifadə olunan formatların xüsusi xassələrinin istifadəsinə əsaslanan üsullar:*

1.1. Kompyuter verilənlərinin formatlarının genişləndirilməsi üçün ehtiyat saxlanılan sahələrin istifadəsi üsulları. Nəzərə almaq lazımdır ki, genişləndirmə üçün nəzərdə tutulmuş sahələr əksər multimedia formatlarında vardır. Bu sahələr sıfır informasiya ilə doldurulur və adi proqramlar tərəfindən istifadə olunmurlar.

Üstünlükləri: istifadə üçün sadədirlər.

Çatışmazlıqları: gizlilik səviyyəsi aşağıdır və ötürülən informasiyanın həcmi məhduddur.

1.2. Mətn faylların xüsusi formatlaşdırılması üsulları. Bu üsullar da öz növbəsində bir neçə yerə bölünür.

1.2.1. Sözlərin, cümlələrin, abzasların yerlərinin dəyişdirilməsi üsulları. Bu üsullar sətirlərin yerlərinin və cümlələrdə sözlərin düzülüşünün müəyyən olunmuş qaydada dəyişdirilməsinə əsaslanır.

1.2.2. Hərflərin müəyyən mövqelərinin seçilməsi üsulu (sıfır şifr). Bu üsullar cümlələrdə, sətirlərdə və ya sözlərdə müəyyən mövqedə duran (məsələn, birinci) hərfləri istifadə etməklə məlumatın yazılmasına əsaslanır. Bu üsulların xüsusi halı kimi akrostix üsulunu (sətirlərin baş hərfləri məlumatı əmələ gətirir) göstərmək olar.

1.2.3. Formatların ekranda əks olunmayan sahələrinin xüsusi xassələrinin istifadə olunması üsulları. Bu üsullar haşiyə, sitat və istinadların qoyulması üçün gizli (görünməyən) xüsusi sahələrin istifadə olunması (məsələn, qara fonda qara rəngdə yazının mətnə daxil edilməsi) prinsiplərini özündə ehtiva edir.

Üstünlükləri: istifadə üçün sadədirlər və sərbəst (pulsuz) yayılan reallaşdırılmış proqram təminatı mövcuddur.

Çatışmazlıqları: gizlilik səviyyəsi zəif, məhsuldarlıq aşağı və ötürülən informasiyanın həcmi məhduddur.

1.3. Disk, disket, flash və digər yaddaş qurğularının istifadə olunmayan yerlərində məlumatların gizlədilməsi

üsulları. Gizlədilən informasiya yaddaş qurğularının adi vəziyyətlərdə standart proqramlar tərəfindən istifadə olunmayan yerlərinə (məsələn, sıfırıncı cığıra, "korlanmış" sektorlara və s.) yazılır.

Üstünlükləri: istifadə üçün sadədirlər və sərbəst (pulsuz) yayılan reallaşdırılmış proqram təminatı mövcuddur.

Çatışmazlıqları: gizlilik səviyyəsi zəif, məhsuldarlıq aşağı və ötürülən informasiyanın həcmi məhduddur.

1.4. İmitasiyaedici funksiyaların (mimic-function) istifadə edilməsi üsulları. Bu üsul mətnlərin generasiyası prinsipinə əsaslanmışdır və özündə akrostix üsulunun ümumiləşdirilməsini ehtiva edir. Gizli məlumat üçün başa düşülən ayrıca mətn generasiya olunur və məlumat onun içində gizlədilir.

Üstünlükləri: istifadə üçün sadədirlər və sərbəst (pulsuz) yayılan reallaşdırılmış proqram təminatı mövcuddur.

Çatışmazlıqları: nəticədə alınan mətn şəbəkənin monitorinqi sistemləri üçün şübhəli olmur.

1.5. Faylı identifikasiya edən başlığın pozulması üsulları. Gizlədilən fayl şifrlənir, alınan nəticə faylından onu identifikasiya edən başlıq pozulur və yalnız şifrlənmiş məlumat saxlanılır. Alan tərəf belə faylın xassələrini bilir və həmin pozulmuş başlığa malik olur.

Üstünlükləri: reallaşdırma sadədir və PGP şifrləmə alqoritmi vasitəsilə bu üsulu reallaşdırmağa imkan verən çoxlu sayda proqram vasitələri (məsələn, White Noise Storm, S-Tools) mövcuddur.

Çatışmazlıqları: məlumatın gizlədilməsi problemi qismən həll edilir və faylın pozulan hissəsinin əvvəlcədən digər tərəfə göndərilməsi zərurəti yaranır.

II. *Rəqəmli fotoşəkildə, rəqəmli səsdə və rəqəmli videoda izafiliyin istifadə edilməsinə əsaslanan üsulları.* Adətən, rəqəmli obyektlərdə istifadə olunan baytların kiçik bitləri (sağdan birinci bitlər) çox az faydalı informasiya daşıyırlar. Onların əlavə informasiya ilə doldurulması, praktiki olaraq, həmin rəqəmli obyektlərin qəbul edilməsinin keyfiyyətinə təsir etmir ki, bu da məxfi informasiyanın gizlədilməsinə imkan verir.

Üstünlükləri: böyük həcmdə informasiyanı gizli göndərməyə imkan verir, müəlliflik hüququnun, əmtəə nişanının, qeydiyyat nömrələrinin və s. gizli təsvir edilməsi mümkündür.

Çatışmazlıqları: əlavə informasiyanın daxil edilməsi hesabına rəqəmli axınların statistik xarakteristikaları təhrif olunur, etibardan sala biləcək əlamətlərin azaldılması üçün statistik xarakteristikaların korreksiyası tələb olunur, alan tərəfə informasiyanın bir hissəsinin əvvəlcədən göndərilməsi zəruridir.

Aşağıda nümunə kimi bəzi məşhur steqanoqrafik proqramlar haqqında qısa məlumat verilir.

- Steganos for Win95 – Windows əməliyyat sistemi mühitində faylların şifrlənməsi və VOC, WAV, ASCII, HTML tipli faylların içində gizlədilməsi üçün güclü imkanlara malik proqram təminatıdır. İstifadəni sadələş-

dirmək üçün proqram master-proqram şəklində reallaşdırılmışdır.

- Contraband – Windows əməliyyat sistemi mühitində istənilən faylı 24 bitli BMP formatlı qrafik fayllarda gizlətməyə imkan verən proqram təminatıdır.

- Jsteg – DOS əməliyyat sistemi mühitində məşhur JPG formatlı qrafik faylda informasiyanın gizlədilməsi üçün nəzərdə tutulmuş proqramdır;

- FFEncode – mətn fayllarında məlumatları gizlətməyə imkan verən DOS proqramıdır. Proqram müvafiq parametrlərlə əmrlər sətrindən yerinə yetirilir.

- StegoDos – şəkli seçməyə, onun tərkibində məlumatı gizlətməyə və onu başqa qrafik formatda saxlamağa imkan verən DOS mühiti üçün nəzərdə tutulmuş proqram paketidir.

- Wnstorm – DOS mühitində məlumatı şifrləməyə və PSX formatlı qrafik faylın içərisində gizlətməyə imkan verən proqram paketidir.

- Hide4PGP v1.1 – OS/2 əməliyyat sistemi mühitində informasiyanı BMP, WAV və VOC formatlı fayllarda gizlətməyə imkan verən proqramdır. İnformasiyanın gizlədilməsi üçün istənilən sayda ən kiçik bitlər istifadə oluna bilər.

- Texto – məlumatı ingilis mətninə çevirən steqanoqrafik proqramdır. Konteyner olan mətn faylı çevirmədən sonra hər hansı mənaya malik olmur, lakin sadə yoxlamanı keçmək üçün normal mətnə kifayət qədər yaxın olur.

- Wnstorm – Macintosh kompyuterləri üçün nəzərdə tutulmuş DOS versiyasına analoji proqramdır.

- Stego – xarici görünüşünü və ölçüsünü dəyişmədən PICT formatlı qrafik faylda məlumatların gizlədilməsinə imkan verən proqramdır.

- Paranoid – məlumatları İDEA və DES alqoritmləri ilə şifrləməyə və sonra alınmış faylı səs formatlı faylın içərisində gizlətməyə imkan verən proqramdır.

7.6. Rəqəmli steqanoqrafiya

Rəqəmli steqanoqrafiya – klassik steqanoqrafiyanın rəqəmli obyektlərin müəyyən (cüzi) təhrif olunması hesabına onlarda məxfi informasiyanın gizlədilməsi və ya yeridilməsi prinsiplərinə əsaslanan yeni istiqamətidir. Lakin bir qayda olaraq, qeyd olunan rəqəmli obyektlər multimedia (şəkil, video, audio, 3D-obyektlərin teksturası və s.) obyektləri olduğundan və edilən təhriflərin insanın hissiyyat orqanlarının orta statistik həddini aşmadığından bu obyektlərin gözə çarpan dəyişikliyinə gətirib çıxarmır.

Bundan əlavə, əvvəldən analoq formatında olan rəqəmli obyektlərdə həmişə kvantlama səs-küyü olur. Belə obyektlərin əks etdirilməsi (göstərilməsi, səsləndirilməsi) zamanı əlavə analoq tipli səs-küy və avadanlıqda qeyri-xətti təhriflər əmələ gəlir ki, bu da gizlədilən informasiyanın nəzərə çarpmaması üçün böyük imkanlar yaradır.

Rəqəmli steqanoqrafiyanın tətbiq sahələrindən biri də müasir dövrdə daha çox tələb olunan yeni istiqamətin – müəlliflik hüququnun qorunması sistemlərinin əsasını təşkil edən rəqəmli su nişanlarının (watermarking) rəqəmli

obyektlərə qoyulması texnologiyasının istifadəsi ilə bağlıdır. Bu istiqamətdə reallaşdırılan üsullar konteynerə müxtəlif çevrilmələrə (hücumlara) davamlı gizli nişanların (markerlərin) daxil edilməsinə əsaslanır.

Kövrək və yarım kövrək rəqəmli su nişanları analoq elektron imzası qismində ötürülən imza haqqında məlumatların qorunmasını, eləcə də konteynerin (məlumatların ötürülməsi kanalının) tamlığının pozulması cəhdlərinin qarşısının alınmasını təmin etmək üçün istifadə olunur.

Məsələn, Adobe Photoshop redaktoruna əlavə işlənib hazırlanmış Digimark proqram bloku bu redaktor vasitəsilə hazırlanan təsvirin özünə müəllif haqqında məlumatı daxil etməyə imkan verir. Təəssüf ki, belə nişan dayanıqlı deyil. Belə ki, Fabien Petitkolas adlı alim tərəfindən işlənib hazırlanmış Stirmark proqramı belə sistemlərə müvəffəqiyyətlə hücum edir və steqoqoyuluşu sındırır.

Ümumiyyətlə, gizli informasiyanın rəqəmli obyektlərə salınması alqoritmlərini bir neçə altqrupa bölmək olar:

- *rəqəmli siqnallarla işləyən üsullar* (məsələn, LSB üsulu);
- *gizli informasiyanın "lehimlənməsi"* – gizlədilən şəkil (səs, təsvir, mətn) orijinal şəklin (səsin, təsvirin, mətnin) üzərinə qoyulur (məsələn, rəqəmli su nişanlarının qoyulması);
- *faylların formatlarının xüsusiyyətlərinin istifadəsi* – bu zaman gizlədilən informasiya metaverilənlərə və ya faylın digər müxtəlif istifadə olunmayan ehtiyat sahələrinə yazılır.

İnformasiyanın rəqəmli obyektlərə daxil edilməsi üsullarına görə steqanoqrafik alqoritmləri bir neçə yerə ayırmaq olar:

- *xətti (additiv) alqoritmlər* – gizlədilən informasiyanın rəqəmli obyektə yeridilməsi ilkin təsvirin xətti modifikasiya etməklə, çıxarılması isə korrelyasiya üsullarının köməyi ilə həyata keçirilir. Bu zaman, adətən, rəqəmli su nişanları konteynerdə olan təsvirə ya əlavə olunur (toplanır), ya da onun içərisində "əridilir";
- *qeyri-xətti alqoritmlər* – gizlədilən informasiyanın rəqəmli obyektə yeridilməsi üçün skalyar və vektor kvantlamasından istifadə olunur.
- *fraktal kodlaşdırma* – informasiyanın rəqəmli obyektin daxilində gizlədilməsi üçün təsvirlərin fraktal kodlaşdırılması üsulları vasitəsilə həyata keçirilir.

Rəqəmli steqanoqrafik üsullara nümunə kimi LSB və Exo üsullarını göstərmək olar.

LSB (Least Significant Bit – qiyməti olan ən kiçik bit) üsulu – konteynerdə (şəkil, səs və ya videoyazı) daha az əhəmiyyətə malik olan ən kiçik mövqeli (sağdan birinci) bitlərin gizlədilən məlumatın bitləri ilə əvəz edilməsi prinsipi əsasında qurulmuşdur. Bu zaman boş və doldurulmuş konteynerlər arasındakı fərq insanın qavrama orqanları tərəfindən hiss ediləcək dərəcəsini aşmamalıdır.

LSB üsulu bütün növ hücumlara qarşı dayanıqlı deyil və yalnız məlumatların ötürülməsi kanalında səs-küy olmadıqda istifadə oluna bilər.

Exo üsulları rəqəmli audiosteqanoqrafiyada tətbiq edilir. Exo üsulları gizlədilən məlumatın bitləri ardıcıllığını kodlaşdırmaq üçün exo siqnallar arasındakı qeyri-bərabər aralardan (fasilələrdən) istifadə olunur. Bir sıra məhdudiyyətlər çərçivəsində insanların qəbul etməsi üçün hiss edilməzlik (nəzərə çarpmazlıq) şərtinə riayət olunmasını təmin etmək mümkündür. Bu üsullar zaman hücumlarına qarşı dayanıqlı olmasa da, amplitud və tezlik hücumlarına dayanıqlıdır.

VIII FƏSİL

İNFORMASİYA TƏHLÜKƏSİZLİYİ PROBLEMİNİN SİSTEMLİ HƏLLİ

İnformasiya təhlükəsizliyinin təmin edilməsinə kompleks yanaşma

İnformasiya təhlükəsizliyi konsepsiyası

İnformasiya təhlükəsizliyi strategiyası

İnformasiya təhlükəsizliyi siyasəti

Məhdudlaşdırma siyasəti (DP)

Çoxsəviyyəli siyasət (MLS)

Tamlığın qorunması üçün Biba təhlükəsizlik siyasəti

8.1. İnformasiya təhlükəsizliyinin təmin edilməsinə kompleks yanaşma

Məlum olduğu kimi, informasiya təhlükəsizliyinin təmin edilməsi üçün həyata keçirilən tədbirlər informasiya texnologiyalarının, o cümlədən avtomatlaşdırılmış informasiya sistemlərinin inkişaf səviyyəsindən daim geri qalır.

Adətən, informasiyanın qorunması vasitələrini istehsal edən şəxslər və ya təşkilatlar tərəfindən işlənib hazıranmış hər bir üsul və vasitə informasiya təhlükəsizliyinin ayrı-ayrı konkret məsələlərinin həlli üçün nəzərdə tutulur. Hazırda informasiya təhlükəsizliyi üzrə bütün məsələlərin həllini təmin edən vahid təhlükəsiz (qorunan) sistemlər nəzəriyyəsi mövcud deyil.

Müasir dövrdə kompyuter sistemlərinin və şəbəkələrinin reallaşdırıldığı təşkilatlarda informasiya təhlükəsizliyi probleminə müxtəlif baxışlar mövcuddur. Bu baxışlardan irəli gələrək informasiya təhlükəsizliyi probleminin həll edilməsi səviyyəsinə görə təşkilatları dörd kateqoriyaya ayırmaq olar.

Birinci kateqoriyaya (səviyyə 0) aid edilən təşkilatlarda informasiya təhlükəsizliyi məsələsinə xüsusi diqqət verilmir və heç kəs bu məsələ ilə ciddi məşğul olmur. Belə təşkilatlarda informasiya təhlükəsizliyi yalnız əməliyyat sistemlərinin, verilənlər bazalarının idarə olunması sistemlərinin və əlavə proqramların daxili imkanları hesabına həyata keçirilir.

İkinci kateqoriya (səviyyə 1) təşkilatlarda informasiya təhlükəsizliyinə texniki problem kimi baxılır və informasiya təhlükəsizliyinin təmin edilməsi sisteminin yaradılması üçün vahid proqram, eləcə də konsepsiya, strategiya və ya siyasət mövcud olmur. Bu halda əvvəlki səviyyədə baxıan vasitələrdən əlavə ehtiyat surətin saxlanması vasitələri, antivirus proqramları, şəbəkələrarası ekran, qorunan virtual xüsusi şəbəkələrin (VPN) təşkili mexanizmləri reallaşdırılır.

Üçüncü kateqoriyaya (səviyyə 2) daxil olan təşkilatlarda informasiya təhlükəsizliyi məsələsinə təşkilati və texniki tədbirlər kompleksi kimi baxılır, problemin vacibliyi başa düşülür və informasiya təhlükəsizliyinin təmin edilməsi sisteminin inkişafı üzrə proqram mövcud olur.

Burada birinci səviyyədəki vasitələrlə yanaşı güclü autentifikasiya, poçt məlumatlarının və Web kontentin təhlili, təhlükəsizliyin pozulmasının aşkar edilməsi, qorunma səviyyəsinin və vasitələrinin təhlili mexanizmləri, açıq açar infrastrukturu, təşkilati tədbirlər (giriş-çıxışa nəzarət, risklərin təhlili, informasiya təhlükəsizliyi siyasəti, əsasnamələr, proseduralar, reqlamentlər və s.) sistemi reallaşdırılmış olur.

Üçüncü kateqoriyadan fərqli olaraq, *dördüncü kateqoiya* (səviyyə 3) təşkilatlarda korporativ informasiya təhlükəsizliyi mədəniyyəti formalaşır, informasiya təhlükəsizliyinin idarə edilməsi sistemi reallaşdırılır, təhlükəsizlik məsələləri üzrə xüsusi struktur bölməsi və təhlükəsizliyin pozulması hallarına reaksiya qrupu fəaliyyət göstərir.

Göründüyü kimi, ilk iki kateqoriyaya aid olan təşkilatlarda (0 və 1 səviyyəli) informasiya təhlükəsizliyi məsələləri ilə fraqmentar şəkildə (qismən) məşğul olurlar.

Fraqmentar yanaşma müəyyən edilmiş şəraitlərdə konkret təhlükələrin (məsələn, girişin idarə olunması və ya informasiyanın şifrlənməsi üçün ayrı-ayrı vəsaitlər, antivirus proqramları və s.) qarşısını almaq üçün konkret vasitələrin reallaşdırılmasını nəzərdə tutur.

İnformasiya təhlükəsizliyi məsələsinə ciddi yanaşma isə yalnız üçüncü və dördüncü kateqoriya (səviyyə 2 və 3) təşkilatlarda həyata keçirilir. Belə yanaşma *kompleks yanaşma* adlanır. Korporativ şəbəkələrdə təhlükəsiz (qorunan mühitdə) informasiya emalını məhz kompleks yanaşmanın köməyi ilə təmin etmək mümkündür.

Bu yanaşma informasiya təhlükəsizliyi məsələlərinin vahid proqram çərçivəsində həllini, şəbəkədə meydana çıxa biləcək təhlükələrin qarşısının alınması üçün nəzərdə tutulmuş müxtəlif üsul və vasitələrin kompleks tətbiqini özündə ehtiva edir. Bu kompleksə informasiya təhlükəsizliyinin təmin edilməsi üçün hüquqi, mənəvi-etik və təşkilati-inzibati tədbirlər, proqram və texniki vasitələr daxil olur.

Qeyd olunanları nəzərə alaraq, informasiya resurslarının, kompyuter sistemlərinin və şəbəkələrinin təhlükəsizliyinin zəmanətli təmin edilməsi, o cümlədən kompyuter cinayətkarlığı və kiberterrorçuluq hadisələrinin vaxtında aşkar edilməsi, qabaqlanması, qarşısının alınması və zərərsizləşdirilməsi məqsədilə hər hansı təhlükəsizlik üsul, vasitə və sistemləri reallaşdırılmazdan əvvəl dövlətlər və təşkilatlar, habelə ayrı-ayrı şəxslər səviyyəsində böyük tədbirlər kompleksinin işlənib hazırlanması və həyata keçirilməsi tələb olunur.

Bu tədbirlər kompleksi üç tərkib hissədən ibarətdir:

- informasiya təhlükəsizliyi konsepsiyası;
- informasiya təhlükəsizliyi strategiyası;
- informasiya təhlükəsizliyi siyasəti.

8.2. İnformasiya təhlükəsizliyi konsepsiyası

İnformasiya təhlükəsizliyi konsepsiyası – müasir texnologiyalar və tendensiyalar nəzərə alınmaqla informasiya təhlükəsizliyi probleminə və onun həll edilməsi yollarına rəsmi qəbul edilmiş baxışlar sistemidir.

Konsepsiyada milli və korporativ maraqlar, informasiya təhlükəsizliyinin təmin edilməsi üsulları və saxlanması prinsipləri müəyyən edilir, eləcə də onların reallaşdırılması məsələləri formalaşdırılır. İnformasiya təhlükəsizliyi konsepsiyanın işlənib hazırlanması, adətən, bir neçə ardıcıl mərhələdə həyata keçirilir.

Birinci mərhələdə, qorunması tələb olunan qiymətli informasiya resursları, o cümlədən istehsal prosesləri, proqramlar, məlumatlar massivi, fayllar və s. təsnif edilir, bu resursların əhəmiyyətlilik dərəcələri müəyyən olunur, yəni qoruma vasitələrinin tətbiqinin tələb olunması səviyyəsinə uyğun olaraq qruplara bölünür.

İkinci mərhələdə, qorunan informasiya resurslarına münasibətdə baş verə biləcək potensial cinayətkar hərəkətlər araşdırılır və təsnif edilir. İqtisadi casusluq, terrorçuluq, sabotaj, oğurluq və s. kimi daha geniş yayılmış real təhlükələrin səviyyəsi müəyyən edilir, qorunan əsas informasiya resurslarına qarşı daha çox ehtimal olunan ziyankar hərəkətlər (o cümlədən cinayətkar əməllər) təhlil olunur.

Üçüncü mərhələdə, informasiya təhlükəsizliyinin təmin edilməsi üzrə mövcud vəziyyət, təşkilat daxili səciyyəvi şərait, istehsal prosesləri, eləcə də informasiya resurslarının qorunması üçün tətbiq oluna biləcək üsul və vasitələr araşdırılır.

Ümumiyyətlə, informasiya təhlükəsizliyi konsepsiyası qarşıya qoyulmuş vəzifələrdən asılı olaraq müəyyən olunmuş risk və minimal itkilər çərçivəsində maksimal təhlükəsizliyi təmin edə biləcək zəruri təşkilati, proqramtexniki, hüquqi və digər tədbirləri özündə birləşdirən kompleks yanaşmanı əks etdirməlidir.

İnformasiya təhlükəsizliyinin təmin edilməsi üzrə tədbirlər kompleksinin ikinci hissəsini təqdim olunan konsepsiya əsasında işlənib hazırlanmış informasiya təhlükəsizliyi strategiyası təşkil edir.

8.3. İnformasiya təhlükəsizliyi strategiyası

İnformasiya təhlükəsizliyi strategiyası – informasiya təhlükəsizliyi sahəsində fəaliyyətin təşkilinin ümumi istiqamətlərini müəyyən edir. İnformasiya təhlükəsizliyi strategiyası müvafiq sahədə obyektiv tələbatlar, strategiyanın həyata keçirilməsinin potensial mümkün şərtləri və təşkilinin mümkünlüyü nəzərə alınmaqla işlənib hazırlanır.

İnformasiyanın qorunması şəraitlərinin müxtəlifliyi nəzərə alınaraq, strateji məsələlərin həllinə yönəlmiş zəruri qoruma səviyyələrini təmin etməyə imkan verən bir neçə təhlükəsizlik strategiyası işlənib hazırlana bilər. Sonradan

konkret şəraitə uyğun olaraq müvafiq strategiya seçilir və reallaşdırılır.

Baxılan amillərin qiymətlərinin uzlaşdırılmasının ən real variantlarına uyğun olaraq, əsas üç qoruma strategiyası müəyyən edilir:

- *Müdafiə strategiyası* – artıq məlum olan təhdidlərdən avtonom şəkildə, informasiya sisteminə əhəmiyyətli təsir göstərmədən qorunma. Burada qorunmanın təmin edilən səviyyəsi yalnız məlum təhdidlərə münasibətdə kifayət qədər yüksək ola bilər.

  Müdafiə strategiyasının reallaşdırılması üçün məlum təhdidlərin neytrallaşdırılması üçün üsul və vasitələrin mövcud olması kifayətdir və əhəmiyyətli resurslar tələb olunmur. Qorunan informasiyanın məxfilik dərəcəsi yüksək olmadıqda və qorunmanın pozulacağı təqdirdə kiçik itkilər gözlənildikdə müdafiə strategiyasının tətbiqi tövsiyə olunur.
- *Hücum strategiyası* – bütün mümkün potensial təhdidlərdən qorunma. Onun həyata keçirilməsi zamanı təhlükəsizlik tələblərinin diktə etdiyi şərtlər informasiya sisteminin arxitekturasında və topologiyasında nəzərə alınmalıdır. O, yalnız təhdidlərin təbiəti və onların meydana çıxması haqqında mövcud təsəvvürlər hüdudunda qorumanın çox yüksək səviyyəsini təmin edə bilər.

  Hücum strategiyasının reallaşdırılması üçün aşağıdakıların olması zəruridir:
  - informasiyaya mümkün potensial təhdidlərin tam siyahısı və xarakteristikaları;

- qorumanın gücləndirilmiş üsul və vasitələri arsenalı barədə məlumat;
- informasiya sisteminin arxitekturasına və informasiya emalı texnologiyasına təsir etmək imkanları.

Hücum strategiyasının reallaşdırılması üçün zəruri olan resursların həcmi qorumaya verilən tələblərin yüksəlməsinə uyğun olaraq çox böyük sürətlə artır. Qorunan informasiya kifayət qədər yüksək məxfilik dərəcəsinə malik olduqda və qorumanın pozulacağı təqdirdə əhəmiyyətli itkilər gözlənildikdə bu strategiyanın tətbiqi tövsiyə olunur.

- *Qabaqlayıcı strategiya* – informasiyaya təhdidlərin meydana gəlməsi üçün şəraitin mövcud olmadığı informasiya mühitinin yaradılması. Qorunmanın təmin edilən səviyyəsi yalnız məlum təhdidlərə münasibətdə zəmanətli şəkildə çox yüksək ola bilər.

Qabaqlayıcı strategiyanın reallaşdırılması üçün zəruri şərt qorunan informasiya texnologiyasının mövcud olmasıdır. Bu zaman böyük kapital məsrəfləri, eləcə də unifikasiya olunmuş informasiya texnologiyaları olduqda hər konkret hal üçün, əlavə olaraq, kiçik resurslar tələb olunur.

Göründüyü kimi, informasiya təhlükəsizliyi strategiyası informasiyanın etibarlı qorunması sisteminin qurulmasının məqsədini, meyarlarını, prinsiplərini və proseduralarını özündə əks etdirir.

Etibarlı qorunmaya zəmanət vermək üçün strategiyada informasiya resurslarının qorunma dərəcəsi, təhlükələr və onların daxil ola biləcəyi zəif yerlər, brandmauerlərin və proxy serverlərin tətbiqolunma yerləri və s. əks olunmaqla

yanaşı, onların tətbiqi üsulları və proseduraları da dəqiq müəyyən edilir. Yalnız bundan sonra informasiya təhlükəsizliyinin təmin edilməsi üçün əsas tədbirlərdən biri olan informasiya təhlükəsizliyi siyasəti formalaşdırılır.

8.4. İnformasiya təhlükəsizliyi siyasəti

İnformasiya təhlükəsizliyi siyasəti – informasiya resurslarının təhlükəsiz idarə olunması (emalı, saxlanması, ötürülməsi), qorunması və paylanması məsələlərini nizamlayan normalar, qaydalar, praktiki üsullar və tədbirlər toplusunu əks etdirən sənəddir.

İnformasiya təhlükəsizliyi siyasəti informasiya resurslarının hansı təhlükələrdən, necə və hansı səviyyədə qorunmasını, bu resurslardan istifadə etmək hüququ olan istifadəçilər dairəsini, onların hüquq və səlahiyyətlərinin hüdudlarını, resurslara icazəli və icazəsiz giriş hüquqlarını və mexanizmlərini müəyyən edir.

İnformasiya təhlükəsizliyi siyasətinin yüksək səviyyəsi informasiyanın qorunmasının müxtəlif mümkün yolları arasından daha optimal variantın seçilməsi yolu ilə əldə oluna bilər. Bu siyasət qiymətli informasiya resurslarının qorunması üçün təklif olunan alternativ variantlar arasından bu resursların sahibləri tərəfindən daha münasib olanının seçilməsinə imkan verməlidir.

Aydındır ki, bu kompromisin nəticəsi olan təhlükəsizlik siyasəti qorunan informasiya ilə qarşılıqlı əlaqədə olan bütün tərəfləri eyni dərəcədə təmin edə bilməz. Lakin eyni zamanda siyasətin seçilməsi problemin həllinin yekun

qərarı olub qiymətli informasiya ilə davranış zamanı nəyin yaxşı və nəyin pis olduğunu müəyyən edir. Belə qərar, yəni təhlükəsizlik siyasəti qəbul edildikdən sonra onun əsasında qoruma mühiti və mexanizmləri, yəni təhlükəsizlik siyasətinin tələblərinin yerinə yetirilməsinin təmin edilməsi sistemi qurulur.

Təhlükəsizlik siyasətində girişə nəzarət, identifikasiya, autentifikasiya, uçot, qeydiyyat, nəzarət jurnalının aparılması, etibarlılıq, diqqətlilik və s. məqamlar mütləq öz əksini tapmalıdır.

Təhlükəsizlik siyasətində icazəsi olmayan şəxslərin, o cümlədən istifadəçilərin informasiya resurslarına (həmçinin, bu resursların saxlandığı yerə) girişinin qadağan edilməsi, istifadəçilərin statusunun, hüquq və səlahiyyətlərinin yoxlanması üçün parol və ya digər mexanizmlərin istifadəsi, şəbəkəyə daxil olan istifadəçinin şəbəkədə bütün hərəkətlərinin, sistemdə baş verən təhlükəsizliyin pozulması hallarının və yerlərinin, eləcə də sistemə icazəsiz giriş cəhdlərinin qeydiyyatının aparılması, qəsdən törədilməyən təsadüfi pozuntulardan qorunmanın təmin edilməsi, habelə belə pozuntuların qabaqlanması, sistem və informasiya resurslarının bir qovşaqda konsentrasiyasının (mərkəzləşməsinin) və ya bir istifadəçinin əlində toplanmasının qarşısının alınması, telekommunikasiya vasitələrinin və rabitə xətlərinin etibarlı qorunması və s. kimi tədbirlər öz əksini tapmalıdır.

İnformasiya təhlükəsizliyi siyasəti işlənib hazırlanarkən qorunması tələb olunan informasiya resursları, onların təyinatı və funksiyaları müəyyən edilir, potensial rəqibin bu resurslara maraq dərəcəsi, təhlükələrin və hücumların baş

verməsi ehtimalları, həyata keçirilməsi yolları və vasitələri, eləcə də onların vura biləcəyi ziyan qiymətləndirilir.

Bununla yanaşı, sistemdə və qoruma mexanizmlərində mümkün zəif yerlər, təhlükəsizliyin pozulması nəticəsində meydana çıxa biləcək problemlər, habelə təhlükəsizlik sisteminin reallaşdırılması üçün mövcud məhdudiyyətlər (maliyyə çatışmazlığı və s.) diqqətlə araşdırılmalı və təhlil olunmalıdır.

İnformasiyanın qorunması sahəsində dövlət siyasəti aşağıdakı əsas istiqamətləri özündə birləşdirir:

- informasiyanın qorunması sahəsində fəaliyyətin dövlət səviyyəsində idarə edilməsi mexanizmlərinin yaradılması;
- informasiyanın qorunması sahəsində qanunvericiliyin inkişaf etdirilməsi;
- dövlət və milli informasiya resurslarının qorunması;
- informasiyanın qorunması üzrə müasir texnologiya və xidmətlər bazarının inkişafı üçün şəraitin yaradılması;
- dövlətin və cəmiyyətin fəaliyyəti üçün daha mühüm avtomatlaşdırılmış informasiya sistemlərinin (dövlət hakimiyyət və idarəetmə orqanlarının, milli bank və ödəmə sistemlərinin, milli infrastrukturun strateji obyektlərinin, kritik texnoloji proseslərinin və digər kritik obyektlərinin idarə edilməsi sistemləri) qorunmasının təşkili;
- informasiyanın qorunması üzrə proqramların və layihələrin reallaşdırılması və dəstəklənməsi.

Qeyd olunanlar nəzərə alınaraq, informasiya təhlükəsizliyi siyasəti aşağıdakı əsas vəzifələrin yerinə yetirilməsinə yönəlmiş olur:

- maraqların qorunması üzrə planların və digər tədbirlərin işlənib hazırlanması və həyata keçirilməsi;
- informasiya təhlükəsizliyi orqanlarının, qüvvə və vasitələrinin formalaşdırılması, təmin edilməsi və inkişaf etdirilməsi;
- hüquqazidd hərəkətlər nəticəsində zərər çəkmiş qoruma obyektlərinin bərpa edilməsi.

Bu vəzifələrdən irəli gələrək reallaşdırılan İTS aşağıdakı məqsədlərin əldə olunmasını təmin edir:
- mümkün potensial təhdidlərin aşkarlanması;
- baş verə biləcək təhdidlərin vaxtında qarşısının alınması;
- baş vermiş təhdidlərin neytrallaşdırılması;
- baş vermiş təhdidlərin aradan qaldırılması;
- təhdidlərin nəticələrinin lokallaşdırılması;
- təhdidlərin dəf edilməsi;
- təhdidlərin məhv edilməsi.

İnformasiya təhlükəsizliyi sistemlərinin yaradılması zamanı bir neçə növ təhlükəsizlik siyasətlərindən istifadə olunur. Daha geniş istifadə olunan aşağıda göstərilən siyasətlərə növbəti paraqraflarda baxılır:
- məhdudlaşdırma siyasəti (Discretionary Polisy – DP);
- çoxsəviyyəli siyasət (Multilevel Security – MLS);
- tamlığın təmin olunması siyasəti (Biba Polisy).

Qeyd etmək lazımdır ki, sistemdə qəbul olunmuş informasiya təhlükəsizliyi siyasətinə riayət edilməsinə nəzarət məsələsi də ciddi problem olaraq qalır. Təhlükəsizlik siyasətinə riayət olunmasının təhlili üçün də bir sıra riyazi üsullar – modellər mövcuddur. Bu məqsədlə daha çox istifadə olunan modellərə nümunə kimi "Take-Grant",

"Bell-Lapadula", "Low-Water-Mark", "G-M" (J.Goguen, J.Meseguer) və s. modellərini göstərmək olar.

8.5. Məhdudlaşdırma siyasəti (DP)

Tutaq ki, $O=\{o_1,o_2,...,o_n\}$ – qorunan obyektlər çoxluğu, $S=\{s_1,s_2,...,s_m\}$ – kompyuter sisteminin və şəbəkəsinin aktiv elementləri olan subyektlər çoxluğu, $U=\{u_1,u_2,...,u_l\}$ – kompyuter sisteminin istifadəçiləri çoxluğudur.

Aydındır ki, *obyektlər* KSŞ-nin passiv elementləridir. Onlar informasiyanın saxlanması, emalı və ötürülməsi üçün istifadə olunur. Belə elementlərə yazıları, blokları, seqmentləri, faylları, qovluqları, bitləri, baytları, sözləri, eləcə də şəbəkənin terminallarını və qovşaqlarını aid etmək olar.

Subyektlər resursların əldə olunması üçün sorğu göndərə və onları hər hansı məqsədlərinin yerinə yetirilməsi üçün istifadə edə bilər.

Praktikada çox vaxt subyekt eyni zamanda obyekt rolunda da çıxış edə bilər. Məsələn, əməliyyat sistemi həm subyekt, həm də obyekt kimi təsnif olunur. Belə ki, əməliyyat sistemində yerinə yetirilən proseslər subyektlər, bu sistem mühitində yaradılan və istifadə olunan fayllar, qovluqlar və s. isə obyektlər kimi qəbul olunur. Ona görə də $S \subseteq O$ qəbul olunur.

İş prosesində subyektlər müxtəlif əməliyyatlar yerinə yetirirlər, başqa sözlə, subyektlərlə obyektlər arasında qarşılıqlı əlaqə baş verir. Belə qarşılıqlı əlaqə subyektlərin obyektlərə daxil olması adlanır. Daxil olma nəticəsində

informasiyanın subyektlər və obyektlər arasında daşınması (hərəkəti) baş verir.

Sistemdə olan obyektlərin hər birinin subyektlərin mülkiyyəti olmasını (başqa sözlə, subyektlərin müvafiq obyektlərin sahibi olması) faktı aşağıdakı inikas şəklində göstərilir:

$$own: O \rightarrow U .$$

Bu, eyni zamanda onu göstərir ki, subyektlər öz mülkiyyətində olan obyektlərlə bağlı bütün hüquqlara malikdirlər və bəzən onların bir hissəsini və ya hamısını başqa subyektlərə verə bilərlər.

Bundan əlavə, obyektin sahibi olan subyekt digər subyektlərin bu obyektə daxilolma hüquqlarını, yəni bu obyektə münasibətdə təhlükəsizlik siyasətini müəyyən edir. Subyektlərin obyektlərə qeyd olunan daxilolma hüquqları $m \times n$ öslçülü R matrisi şəklində müəyyən edilir. Onun r_{ij} elementi s_i subyektinin o_j obyektinə, eləcə də digər subyektlərə giriş hüquqlarını müəyyən edir.

$R=$

	o_1	O_2	...	o_n	s_1	...	s_m
s_1		own rw_{12}					
s_2	own r_{21}		...			...	
...	...	...	...	...	...	...	...
s_m				own w_{mn}			

Subyektlərin obyektlərə giriş hüquqlarını müəyyən edən matrisin verilməsi üçün aşağıdakı yanaşmalar mövcuddur:

- subyektlərin hüquqlarının siyahısı – hər bir s_i subyekti üçün onun giriş hüququ olan obyektlərin siyahısı (fayl) yaradılır;
- obyektlərə giriş hüquqlarının nəzarəti siyahısı – hər bir o_j obyekti üçün ona giriş hüququ olan bütün subyektlərin siyahısı (fayl) yaradılır.

Birinci halda hər bir siyahı matrisin sətrinə, ikinci halda isə sütununa uyğun gəlir.

Aparılmış tədqiqatlar göstərir ki, məhdudlaşdırma siyasəti informasiya təhlükəsizliyinin bir çox problemlərini həll etmək iqtidarında deyil. Xüsusilə, bu siyasətin daha əhəmiyyətli çatışmazlığı kompyuter virusları, "troya atları" və digər bu kimi təhlükələrin qarşısının alınmasının qeyri-mümkün olmasıdır. Bu, o deməkdir ki, məhdudlaşdırma siyasətini reallaşdıran təhlükəsizlik sistemi gizli şəkildə dağıdıcı və pozucu təsir göstərən vasitələrin qarşısını pis alır. Bunu troya atlarının nümunəsi üzərində nümayiş etdirmək olar.

Tutaq ki, U_1 – istifadəçi, U_2 – bədniyyətli (pozucu) şəxs olan istifadəçi, O_1 – qiymətli informasiyanı özündə saxlayan obyekt, O_2 – ziyanverici proqramlara, o cümlədən troya atlarına (T) "yoluxmuş" proqram, R – giriş hüquqlarını müəyyən edən matrisidir.

$R:$

	O_1	O_2
U_1	own r,w	own w
U_2		own r,w

Bədniyyətli U_2 istifadəçisi ziyanverici proqrama yoluxmuş hər hansı O_2 proqramını yaradır və xüsusi şəkildə maraqlandırmaqla (məsələn, O_2 proqramı çox maraqlı kompyuter oyunu ola bilər) çalışır ki, U_1 istifadəçisi bu proqramı öz kompyuterinə yükləsin. Nəticədə U_1 istifadəçisi O_2 proqramını öz kompyuterinə yükləyir və həmin proqramın daxilində gizlədilmiş T proqramını işə salmış olur.

T proqramı U_1 istifadəçisi tərəfindən yüklәndiyindən onun hüquqlarına malik olur və beləliklə də, O_1 obyektində olan informasiyanı köçürmək hüququnu əldə edir. T proqramı (yəni O_2 proqramı) bu hüquqdan istifadə edərək O_1 obyektində olan informasiyanı özünə köçürür. Bundan sonra, O_2 proqramının sahibi olan bədniyyətli U_2 istifadəçisi O_1 obyektinə məxsus olan informasiyanı məhdudiyyət olmadan oxuyur.

Məhdudlaşdırma siyasətinin növbəti problemi hüquq və səlahiyyətlərin müəyyən edilməsi ilə bağlıdır. Belə ki, subyekt və obyektlərin sayı çox olduğuna görə hər bir subyektin hər bir obyektə giriş hüquqlarının əvvəlcədən əllə daxil edilməsi mümkün deyil. Ona görə də giriş hüquqları matrisi müxtəlif üsullarla doldurulur.

Matrisin elementlərinə xüsusi şəkildə formalaşdırılmış funksiyanın qiymətlərinin hesablanması yolu ilə qiymətlər mənimsədilə bilər. Bu funksiyaların qiyməti vaxta görə və ya digər parametrlərdən asılı olaraq dəyişə bilər. Məhdudlaşdırma siyasətinin digər çətinliyi giriş hüquqlarının paylanmasına nəzarət problemidir.

Çox vaxt obyektin sahibi onda olan informasiyanın məzmununu başqasına verir. Bu halda informasiya alan

subyekt informasiyaya sahiblik hüququnu əldə etmiş olur. Beləliklə, sahiblik hüququnun verilməməsinə baxmayaraq, bu hüquq onun sahibinin iradəsindən asılı olmadan yayıla bilər.

8.6. Çoxsəviyyəli siyasət (MLS)

Sistemin s vəziyyətində α əmrinin yerinə yetirilməsi nəticəsində baş verən informasiya yerdəyişməsi X obyektindən Y obyektinə *informasiya axını* adlanır və

$$X \underset{\alpha}{\rightarrow} Y$$

kimi işarə olunur.

Əgər

$$I(X,Y)>0$$

olarsa, onda α əmri sistemi s vəziyyətindən s' vəziyyətinə gətirər. Burada $I(X,Y)$ kəmiyyəti X obyektindən Y obyektinə informasiya axınının qiyməti (bit ilə ölçülür) adlanır. Əgər α əmrləri ardıcıllığı mövcud s və s' vəziyyətləri üçün $s \underset{\alpha}{\rightarrow} s'$ və $X \underset{\alpha}{\rightarrow} Y$ təmin edərsə, onda X və Y obyektləri üçün J qiymətinə malik informasiya axını mövcud olar.

Tutaq ki, S_J – sonlu nizamlanmış çoxluq, $\leq$ – binar münasibətdir, eləcə də S_J çoxluğunun A, B və C elementləri üçün aşağıdakı şərtlər ödənilir:

- reflektivlik: $A \leq A$;
- tranzitivlik: $A \leq B, B \leq C \Rightarrow A \leq C$;
- antisimmetriklik: $A \leq B, B \leq A \Rightarrow A = B$.

Əgər aşağıdakı şərtlər ödənilərsə, onda $A, B \in SC$ üçün $C = A \oplus B \in SC$ elementi ən kiçik yuxarı sərhəd adlanır:

- $A \leq C$ və $B \leq C$;
- bütün $D \in SC$ üçün $A \leq D, B \leq D \Rightarrow C \leq D$.

Əgər aşağıdakı şərtlər ödənilərsə, onda $A, B \in SC$ üçün $E = A \otimes B \in SC$ elementi ən böyük aşağı sərhəd adlanır:

- $E \leq A$ və $E \leq B$;
- bütün $D \in SC$ üçün $D \leq A, D \leq B \Rightarrow D \leq E$.

$C = A \oplus B$ və $E = A \otimes B$ elementləri mövcud olmaya da bilər. Əgər ən kiçik yuxarı və ən böyük aşağı sərhəd mövcuddursa, onda antisimmetriklik xassəsindən onun yeganəliyi çıxır.

MLS siyasəti yalnız SC qəfəsində $c(X) \leq C(Y)$ şərti ödənildikdə $X \xrightarrow[\alpha]{} Y$ informasiya axınını icazə verilmiş hesab edir. MLS siyasəti sistemdə informasiya axınları çoxluğu ilə işləyir, onları çox sadə şərtlə icazə verilmiş və ya icazə verilməmiş kateqoriyalarına bölür. Lakin bu sadəlik sistemdə çox böyük sayda olan informasiya axınlarına aid edilir. Ona görə də yuxarıda verilmiş tərif qeyri-konstruktivdir. Konstruktiv tərifi girişlər dilinin köməyi ilə aşağıdakı kimi vermək olar.

Tutaq ki, iki giriş növü ("r" – oxuma, "w" – yazma) müəyyən edilmiş sistemlər sinfi baxılır və sistemdə S prosesi öz vəzifələrinin icrası gedişində ardıcıl olaraq O_1, O_2,..., O_n obyektlərinə müraciət edir.

$$S \xrightarrow{r} O_{i_1}, S \xrightarrow{r} O_{i_2}, ..., S \xrightarrow{r} O_{i_k}, S \xrightarrow{w} O_{i_1}, ..., S \xrightarrow{w} O_{i_{n-k}} \quad (8.1)$$

Yuxarıda verilmiş tərifl ərdən çıxır ki,

$$c(O_{i_t}) \leq C(S), t = \overline{1,k}$$

şərti ödənildikdə uyğun informasiya axınları MLS siyasəti tərəfindən icazə verilmiş istiqamətdə gedəcək,

$$c(O_{i_t}) \leq C(S), t = \overline{1,n-k}$$

olduqda isə "w" girişi ilə müəyyən edilmiş informasiya axınları da icazə verilmiş istiqamətdə hərəkət edəcəkdir.

Beləliklə, S prosesi tərəfindən məsələlərin yerinə yetirilməsi nəticəsində onunla bağlı olan informasiya axınları MLS siyasətinin tələblərinə cavab verir. Belə keyfiyyətli təhlil bütün proseslərin təhlili, eləcə də MLS siyasətinə riayət olunub-olunmaması barədə qərarın qəbul edilməsi üçün kifayət edir.

Əgər haradasa MLS siyasəti pozulursa, onda uyğun girişə icazə verilmir. (8.1) zəncirinə icazənin verilməməsi hələ o demək deyil ki, S subyekti $c(O) < C(S)$ şərtini ödəyən O obyektini yarada bilməz. Lakin o, oraya informasiya yazmaq hüququ vermir.

İdarəetmə ötürülən zaman S prosesindən O obyektinə gedən informasiya axını kəsilir. Bu zaman, əgər "r" və "w" üçün informasiya axını qaydaları yerinə yetirilirsə, onda MLS siyasətinə riayət olunur, əks halda müvafiq prosesə giriş verilmir.

Beləliklə, girişlərin nəzarət olunması vasitəsilə informasiya axınlarının idarə olunmasına gəlmiş oluruq. Nəticədə,

sistemlər sinfini müəyyən etmək üçün MLS siyasətinin konstruktiv təsvirini aşağıdakı kimi vermək olar.

İki "r" və "w" girişli sistemdə MLS siyasəti aşağıdakı qaydalarla müəyyən edilir:

$$X \xrightarrow{r} Y \Leftrightarrow c(Y) \le c(X),$$

$$X \xrightarrow{w} Y \Leftrightarrow c(X) \le c(Y).$$

Qəfəsin strukturu MLS siyasətinin saxlanılmasının təşkilinə çox kömək edir. Əslində informasiya axınlarının zəncirləri ardıcıllığı mövcuddur:

$$O_1 \underset{\alpha}{\rightarrow} O_2 \underset{\beta}{\rightarrow} O_3 \underset{\gamma}{\rightarrow} \ldots \underset{\delta}{\rightarrow} O_k .$$

Əgər bütün axınlara icazə verilmişdirsə, onda qəfəsin xassəsi birbaşa $O_1 \underset{\alpha}{\rightarrow} \ldots \underset{\delta}{\rightarrow} O_k$ axınına icazə verildiyini təsdiq etməyə imkan verir.

Həqiqətən də, əgər hər addımda informasiya axınına icazə verilmişdirsə, onda $c(O_i) \le C(O_{i+1})$ olar. Qəfəsin tranzitivlik xassəsinə görə $c(O_1) \le C(O_k)$ şərti də ödənilər ki, bu da birbaşa axına icazə verildiyini göstərir.

8.7. Tamlığın qorunması üçün Biba təhlükəsizlik siyasəti

MLS siyasəti, əsasən, informasiyanın gizliliyini təmin etmək üçün reallaşdırılır, lakin bu siyasətin köməyi ilə

informasiyanın tamlığı məsələsi həll edilmir və ya MLS siyasətində informasiyanın tamlığı məsələsinə ikinci dərəcəli məsələ kimi baxılır. İnformasiyanın tamlığının qorunması üçün Biba ayrıca təhlükəsizlik siyasəti təklif etmişdir.

Tutaq ki, informasiyanın gizliliyi təhlükəsi mövcud deyil və təhlükəsizlik siyasətinin yeganə məqsədi *SC* qiymətlər qəfəsinə daxil edilmiş informasiyanın tamlığının qorunmasından ibarətdir. Bununla əlaqədar olaraq, istənilən $X \underset{\alpha}{\rightarrow} Y$ informasiya axını *Y* obyektinin tamlığına təsir edə, *X* obyektinin tamlığına isə tamamilə təsir göstərməyə bilər.

Əgər *Y* obyektində *X* obyektinə nisbətən daha qiymətli informasiya varsa, onda az qiymətli obyektdən (*X*) daha qiymətli obyektə (*Y*) yönələn axın zamanı *Y*-də informasiyanın tamlığının pozulması nəticəsində dəyən ziyan əks istiqamətdə, yəni daha qiymətli obyektdən (*Y*) nisbətən az qiymətli obyektə (*X*) gedən axın zamanı *X*-də tamlığın pozulması nəticəsində dəyən ziyana nisbətən daha əhəmiyyətli olacaqdır.

Tamlığının qorunması üçün Biba təhlükəsizlik siyasətində yalnız və yalnız

$$c(Y) \le c(X)$$

olduqda $X \underset{\alpha}{\rightarrow} Y$ informasiya axınına icazə verilir.

Buna analoji olaraq göstərmək olar ki, bu siyasət daha geniş sistemlərdə aşağıdakı siyasətə ekvivalentdir.

"r" və "w" girişli sistemləri üçün

$$S \xrightarrow{r} O \Leftrightarrow c(O) \le c(S),$$

$$S \xrightarrow{w} O \Leftrightarrow c(S) \le c(O).$$

olarsa, onda Biba təhlükəsizlik siyasəti girişə icazə verir. Aydındır ki, bu siyasətin reallaşdırılması üçün də mandat nəzarəti daha münasibdir.

IX FƏSİL

KOMPYUTER SİSTEMLƏRİ VƏ ŞƏBƏKƏLƏRİ ÜÇÜN İNFORMASİYA TƏHLÜKƏSİZLİYİ SİSTEMİNİN REALLAŞDIRILMASI

İnformasiya təhlükəsizliyi sisteminin formal modeli

İnformasiya təhlükəsizliyi sisteminin yaradılması prinsipləri və ona qoyulan tələblər

İnformasiya təhlükəsizliyi sisteminin funksional strukturu, əsas modulları və proseduraları

Girişin idarə olunması modulu

İnformasiya emalının idarə olunması modulu

Məlumatların bilavasitə mühafizəsi modulu

Təhlükələrə nəzarət, vəziyyətin təhlili və qərarların qəbul edilməsi modulu

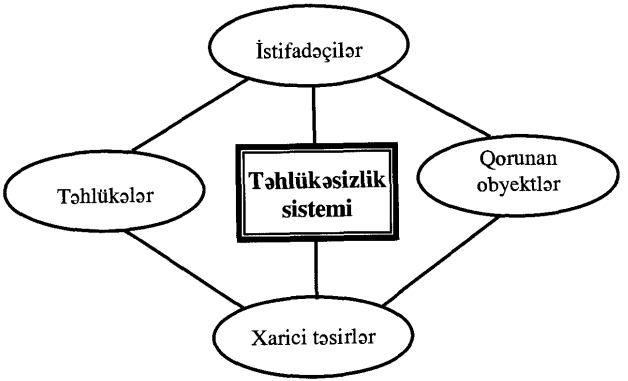
9.1. İnformasiya təhlükəsizliyi sisteminin formal modeli

KSŞ-yə və onun obyektlərinə hər bir mümkün daxil-olma (giriş) yolunda təhlükəsizliyin təmin olunması üçün İTS-də heç olmazsa bir vasitə reallaşdırılmalıdır. İTS-in konseptual modelində kompyuter sistemlərinin qorunması tələb olunan hər bir resursu (komponenti, obyekti) müəyyən edilir, şəbəkənin təhlükəsizliyində rolu və səmərəliyi baxımından informasiya təhlükəsizliyinin təmin edilməsinin bütün vasitələri qiymətləndirilir.

Təhlükəsizlik sistemini xarakterizə edən mühitin ümumi modeli 9.1 saylı şəkildə göstərilmişdir. Modeldə daha az əhəmiyyət kəsb edən "istifadəçi sahəsi" və "xarici təsirlər" təhlükələrin yaradılması vasitəsi və amili olduqları üçün bu komponentlər təhlükələr kateqoriyasına daxil edilir və nəticədə təhlükəsizlik mühiti daha sadə şəkil alır (şək.9.2).

Bu modelə uyğun olaraq, qorunması tələb olunan hər bir obyektə ziyankarın (bədəməl şəxsin) yerinə yetirə biləcəyi müəyyən hərəkətlər çoxluğu (təhlükə) istiqamətlənə bilər.

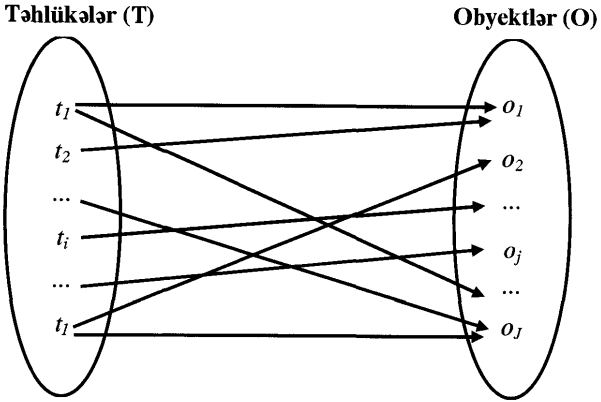
Tutaq ki, $T = \{t_i\}, i = \overline{1,I}$ – mümkün təhlükələr çoxluğu, $O = \{o_j\}, j = \overline{1,J}$ – təhlükələrin və ya ziyankar hərəkətlərin yönəldiyi obyektlər (informasiya resursları) çoxluğudur. Təhlükələr çoxluğuna daxil olan ziyankar əməllərin sistemdə mövcud obyektlərə qarşı baş verməsi ehtimalı bu çoxluğun əsas xarakteristikasını müəyyən edir.



Şək.9.1. Təhlükəsizliyin təmin olunması mühitinin ümumu görünüşü

Şək.9.2. Təhlükəsizliyin təmin olunmasının baza sistemi

Təhlükəsizlik sisteminin modelinin əsasını təşkil edən "obyekt-təhlükə" münasibətlərini ikihissəli qraf şəklində vermək olar (şək.9.3). Qrafın bir hissəsini sistemdə mövcud olan qorunan obyektlər, ikinci hissəsini isə bu obyektlərə yönələ biləcək təhlükələr çoxluğu təşkil edir.



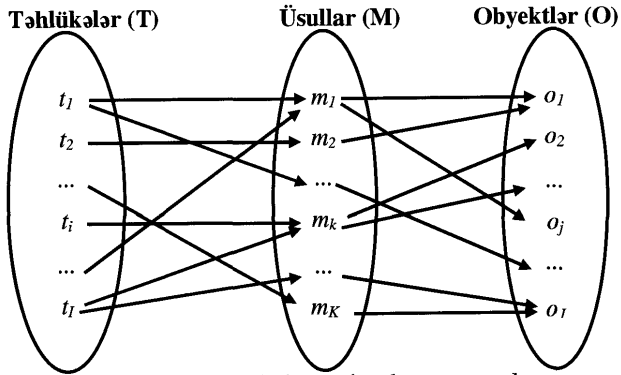
Şək.9.3. Təhlükəsizlik sistemi modelində "obyekt-təhlükə" münasibətləri

Əgər t_i təhlükəsi o_j obyektinə yönəlmişdirsə və tətbiq oluna bilərsə, onda bu qrafda (t_i,o_j) tili mövcud olur. Şəkildən göründüyü kimi, təhlükələrlə obyektlər arasında əlaqə "birin birə" şəklində deyil. Belə ki, hər bir təhlükə istənilən sayda obyektə yönələ və ya hər bir obyekt bir neçə təhlükənin təsirinə məruz qala bilər.

İnformasiya təhlükəsizliyinin təmin edilməsinin məqsədi ondan ibarətdir ki, bu qrafda hər hansı təhlükənin

obyektlərə daxil olması və təsir etməsi yollarını göstərən bütün mümkün tillər aradan qaldırılmış olsun.

Bu məqsədlə modelə təhlükəsizliyin təmin edilməsi vasitələri çoxluğu $M=\{m_k\}, k=\overline{1,K}$ daxil edilir. Nəticədə hər bir (t_i,o_c) tili (t_i,m_k) və (m_k,o_j) kimi iki tilə ayrılır və, beləliklə, ikihissəli qraf üçhissəli qrafa çevrilmiş olur (şək.9.4).



Şək.9.4. Təhlükəsizliyin təmin olunmasının baza sisteminin qraflarla təsviri

Aydındır ki, istənilən (t_i,o_j) tilinin olması qorunmayan o_j obyektini, yəni o_j obyektinin t_i təhlükəsinə məruz qala biləcəyini göstərir. Qrafa daxil edilən m_k qovşağı (qoruma vasitəsi) t_i təhlükəsinin o_j obyektinə birbaşa yönəldiyini göstərən hər hansı (t_i,o_j) tilini aradan götürür.

Həqiqətdə hər bir qoruma vasitəsi informasiya təhlükəsizliyinin təmin olunmasının müəyyən bir funksiyasını yerinə yetirir və təhlükənin daxil olmasına müəyyən dərəcədə müqavimət göstərilməsini təmin edir. Məhz təhlükələrə qarşı bu müqavimət $M=\{m_k\}, k=\overline{1,K}$ çoxluğunun hər bir elementinə xas olan xassədir.

Qeyd olunmalıdır ki, modelə görə, təhlükəsizliyin təmin edilməsinin eyni bir qoruma vasitəsi birdən çox təhlükənin qarşısını ala və ya birdən çox obyekti qoruya bilər. Eyni zamanda (t_i,o_j) tilinin olmaması o_j obyektinin təhlükəsizliyinin tam təmin olunduğuna zəmanət verə bilməz.

Qeyd olunanları nəzərə alaraq, İTS-i aşağıdakı beşlik şəklində təqdim etmək olar:

$$S=\{O,T,M,V,B\}$$

Burada O – qorunan obyektlər (informasiya resursları) çoxluğu, T – sistemdə gözlənilən təhlükələr çoxluğu, M – təhlükəsizliyin təmin edilməsi üsulları çoxluğu, V – sistemə və informasiya resurslarına icazəsiz girişin mümkün olduğu zəif yerlər çoxluğu $v_l=(t_i,o_j)$, B – müdafiə sədləri çoxluğu, yəni qorunmanın həyata keçirilməsinin tələb olunduğu nöqtələr çoxluğudur. Bu çoxluğun elementləri $b_m=(t_i,m_k,o_j)$ şəklində müəyyən edilir.

Əgər sistemdə hər bir mümkün təhlükənin qarşısını almaq üçün üsul və ya vasitə mövcuddursa, onda sistemin təhlükəsizliyi mütləq təmin edilmiş hesab edilir. Belə sistemdə (t_i,o_j) şəklində birbaşa daxilolma yolu olmur, obyektə yol yalnız (t_i,m_k,o_j) şəklində olur və bu yolun üzərində b_m müdafiə səddini təmin edir.

9.2. İnformasiya təhlükəsizliyi sisteminin yaradılması prinsipləri və ona qoyulan tələblər

KSŞ-nin strukturuna analoji olaraq, adətən, onlar üçün reallaşdırılan İTS, eləcə də informasiyanın qorunması prosesi çox səviyyəli struktura malik olur. Bir qayda olaraq, KSŞ-də informasiyanın qorunması üç səviyyədə həyata keçirilir

I səviyyə: ayrı-ayrı kompyuterlərin, işçi stansiyaların və terminalların təhlükəsizliyinin təmin edilməsi;

II səviyyə: lokal kompyuter şəbəkələrinin və funksional serverlərin təhlükəsizliyinin təmin edilməsi;

III səviyyə: korporativ kompyuter şəbəkəsinin ümumi təhlükəsizliyinin təmin edilməsi.

Birinci səviyyədə əməliyyat sisteminin istifadəçilərinin identifikasiyası və autentifikasiyası, malik olduqları hüquq və səlahiyyətlər çərçivəsində subyektlərin obyektlərə girişinə icazə verilməsi, bütün daxilolmaların və daxilolma cəhdlərinin qeydiyyatı və uçotunun aparılması, eləcə də proqram və informasiya təminatının tamlığının təmin edilməsi və qoruma vasitələrinin müntəzəm olaraq nəzarətdə saxlanması funksiyaları reallaşdırılır.

İkinci səviyyədə istifadəçilərin identifikasiyası, sistemə və onun komponentlərinə girişin həqiqiliyinin təyin edilməsi, autentifikasiya məlumatlarının qorunması və serverlərə qoşulma zamanı həqiqiliyin təyin edilməsi məsələlərinin həlli nəzərdə tutulur.

Üçüncü səviyyədə rabitə xətti ilə ötürmə zamanı mənbədən ünvana qədər olan məsafədə informasiyanın tamlığı, autentifikasiya, kommunikasiya xətlərinin həqiq-

iliyi, məlumatların ötürülməsi və qəbul edilməsi faktlarından tərəflərin imtina etməsinin qarşısının alınması, təqdim olunan xidmətlərin sıradançıxmaya davamlılığı, sistemin fasiləsiz fəaliyyəti, informasiyanın gizliliyi təmin edilir, eləcə də ötürmənin təhlükəsizliyi protokolu reallaşdırılır.

KSŞ-də effektiv İTS-in yaradılmasının əsas prinsipləri aşağıdakılardan ibarətdir:

- təhlükəsizliyin təmin edilməsinə sistemli yanaşma olmalıdır;
- tətbiq edilən üsul və vasitələr, görülən tədbirlər, qəbul edilən qərarlar kompleks təşkil etməlidir;
- qoruma vasitələri tələb olunan dərəcədə olmalıdır;
- qoruma vasitələrinin izafiliyi müəyyən həddi aşmamalıdır;
- qoruma vasitələrinin idarə edilməsi və tətbiqi çevik olmalıdır;
- qoruma mexanizmləri və alqoritmləri aşkar olmalıdır;
- qoruma üsullarının, vasitələrinin və tədbirlərinin tətbiqi sadə olmalıdır;
- qoruma vasitələri unifikasiya edilməlidir.

Ümumi halda, İTS aşağıdakı şərtlərə cavab verməlidir:

- informasiya fəaliyyətinin bütün texnoloji kompleksini əhatə etməlidir;
- istifadə olunan vasitələrə görə müxtəlif, iyerarxik, daxilolma ardıcıl və çoxsəviyyəli olmalıdır;
- informasiya təhlükəsizliyinin təmin edilməsi sistemi üsul, vasitə və tədbirlərinin dəyişdirilməsi və əlavə edilməsi üçün açıq olmalıdır;
- reallaşdırdığı imkanlar baxımından qeyri-standart olmalıdır;

- texniki xidmət üçün sadə və istifadəçilər tərəfindən istismar üçün rahat olmalıdır;
- etibarlı olmalı, texniki vəsaitlərin istənilən sıradan çıxması informasiyanın sızması üçün nəzarət olunmayan kanallar yaratmamalıdır;
- informasiya təhlükəsizliyi sistemi vahid proqram-texniki kompleks şəklində reallaşdırılmalıdır;
- informasiya resurslarına giriş üçün istifadəçilərin hüquq və səlahiyyətləri dəqiq müəyyən edilməlidir;
- istifadəçilərə tapşırılmış işin yerinə yetirilməsi üçün onlara zəruri olan minimal səlahiyyətlər verilməlidir;
- bir neçə istifadəçi üçün ümumi olan qoruma vasitələrinin sayı minimuma endirilməlidir;
- konfidensial informasiyaya icazəsiz giriş hallarının və buna cəhdlərin uçotu aparılmalıdır;
- informasiyanın konfidensiallıq dərəcəsinin qiymətləndirilməsi təmin edilməlidir;
- qoruma vasitələrinin bütövlüyünə nəzarət təmin edilməli və onlar sıradan çıxdıqda dərhal reaksiya verilməlidir.

Əvvəlki fəsillərdə qeyd olunduğu kimi, İTS-in qarşısında qoyulan vəzifələrin və funksiyaların yerinə yetirilməsi, eləcə də informasiya təhlükəsizliyinin zəruri səviyyəsinin təmin edilməsi üçün istifadə olunan üsul və vasitələri əsas beş kateqoriyaya ayırırlar: qanunvericilik tədbirləri, mənəvi-etik normalar, təşkilati tədbirlər, texniki vasitələr və proqram vasitələri.

Təhlükəsizliyin təmin edilməsinin qanunvericilik (hüquqi) tədbirləri Azərbaycan Respublikasında müvafiq qanunvericilik aktları ilə müəyyən olunur. Adətən, bu

normativ-hüquqi sənədlər məhdud girişli informasiyanın istifadəsi, emalı və ötürülməsi qaydalarını nizamlayır və bu qaydaların pozulmasına görə məsuliyyət tədbirlərini müəyyən edir.

Təhlükəsizliyin pozulmasının qarşısının alınmasına yönəlmiş mənəvi-etik tədbirlərə davranış normalarını aid edirlər. Bu normalar şəbəkə və informasiya texnologiyalarının inkişafı prosesində yaranaraq formalaşmışdır. Mənəvi-etik normalar, əsasən, məcburi xarakter daşımır, lakin onlara riayət olunmaması nüfuzun, etibarın və hörmətin itməsinə gətirib çıxarır.

Təşkilati (inzibati) tədbirlər özündə təşkilati-texniki və təşkilati-hüquqi tədbirləri ehtiva edir və telekommunikasiya avadanlıqlarının yaradılması və istismarı prosesində həyata keçirilir.

Təşkilati tədbirlər texniki vəsaitlərin həyat dövrünün bütün mərhələlərində (binanın tikintisi, sistemin layihələndirilməsi, avadanlığın quraşdırılması, sazlanması, sınaqdan keçirilməsi və istismarı) onların bütün struktur elementlərini əhatə edir.

9.3. İnformasiya təhlükəsizliyi sisteminin funksional strukturu, əsas modulları və proseduraları

Sistem iyerarxiyasının ən yuxarı səviyyəsində reallaşdırılan İTS, əsasən, aşağıdakı funksiyaların yerinə yetirilməsini təmin edir:

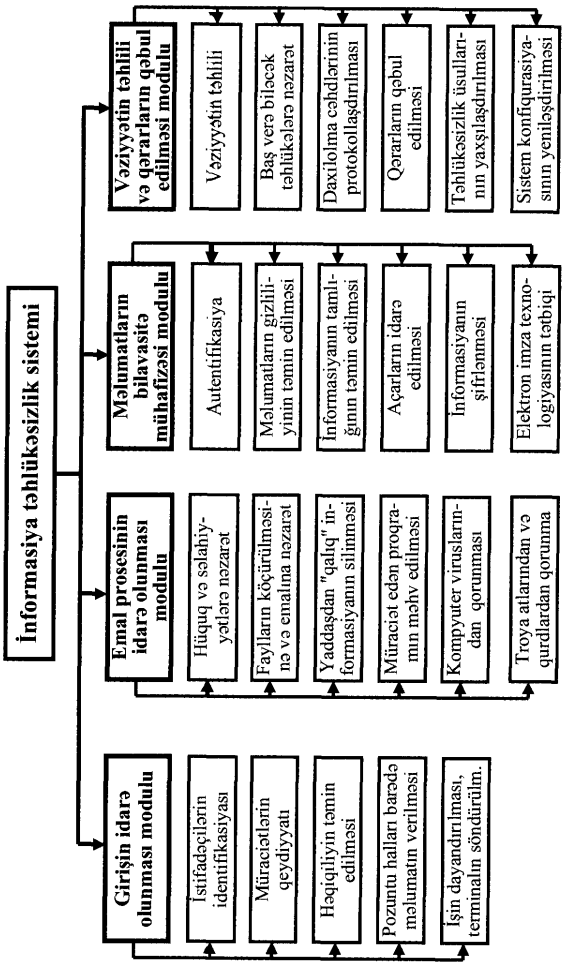
- istifadəçilərin sistemə girişlərinin idarə edilməsi;
- sistemə və onun resurslarına girişə nəzarət edilməsi;

- sistemə girişlərin və müraciətlərin qeydiyyatının aparılması;
- istifadəçinin, sistemin və şəbəkənin həqiqiliyinin müəyyən edilməsi;
- istifadəçilərin hüquq və səlahiyyətlərinin nəzarətdə saxlanması;
- informasiyanın kriptoqrafik şifrlənməsi və bilavasitə müdaxilədən qorunması xidməti;
- elektron imza texnologiyasının tətbiqi və istifadəçi açarlarının idarə edilməsi;
- informasiyanın tamlığının təmin olunması və həqiqiliyinin təsdiq edilməsi;
- sistemin obyektlərinin vəziyyətinin təhlili və təhlükələrə nəzarət edilməsi;
- sistemdə baş verən pozuntuların qarşısının alınması;
- təhlükəsizlik sisteminin struktur parametrlərinin yeniləşdirilməsi.

Yuxarıda sadalanan funksiyalar reallaşdırılması və birbiri ilə qarşılıqlı əlaqəsinin qurulması baxımından müxtəlif mürəkkəblik dərəcələrinə malik olurlar. Aşağıda onların yerinə yetirilməsi proseduralarına baxılır.

Qeyd olunduğu kimi, bu funksiyaların yerinə yetirilməsi, başqa sözlə, KSŞ-nin komponentlərinin, o cümlədən informasiya resurslarının qorunması üçün vahid İTS-in, yəni təhlükəsizliyi təmin edən bütün zəruri üsul və vasitələri, modul və proseduraları özündə birləşdirən kompleksin yaradılması zəruridir.

Belə təhlükəsizlik sisteminə daxil olan əsas modul və proseduralar 9.5 saylı şəkildə göstərilmişdir. Şəkildən göründüyü kimi, İTS-in təklif olunan strukturuna tələb edilən



Şək.9.5. İnformasiya təhlükəsizlik sisteminin əsas modul və proseduraları

funksiyaların yerinə yetirilməsi üçün zəruri olan bütün qoruma üsul və vasitələrini özündə birləşdirən dörd əsas modul daxil edilmişdir.

9.4. Girişin idarə olunması modulu

Girişin idarə olunması modulu sistemə giriş zamanı istifadəçilərin identifikasiyası, sistemə və onun resurslarına bütün müraciətlərin qeydiyyatı, sistemdə baş verən nasazlıqlar, sıradan çıxmalar və pozuntular barədə məsul operatora, şəbəkə inzibatçısına və ya "etibarlı monitor"a təcili məlumatın verilməsi, sistemə və onun resurslarına girişlərə məhdudiyyətin qoyulması, istifadəçinin, sistemin və şəbəkənin həqiqiliyinin müəyyən edilməsi funksiyalarını yerinə yetirir.

Bu modul informasiya resurslarının, proqram təminatının icazəsiz istifadəsinin qarşısını almaq yolu ilə onların təhlükəsizliyini, habelə digər istifadəçilərin hüquq və səlahiyyətlərini təmin edir. Ona daxil olan proseduralar aşağıdakı şəkildə qarşılıqlı fəaliyyət göstərirlər.

Sistemdə işləmək üçün hər bir istifadəçi əvvəlcə girişin idarə edilməsi modulu vasitəsilə sistemə daxil olmalıdır. Bu modul sistem haqqında ümumi məlumatı istifadəçiyə təqdim edir, ona özünün adını (identifikatorunu) və parolunu daxil etməyə imkan verir.

İstifadəçi adını və parolunu daxil etdikdən sonra sistemə və onun resurslarına girişə nəzarət edilməsi prosedurası işə başlayır. Bu modul tərəfindən istifadəçinin adı və parolu qəbul edilir, sistemə və tələb olunan resurslara

giriş hüququnun icazəli olub olmaması yoxlanılır. Əgər giriş icazəsiz olarsa, onda istifadəçiyə rədd cavabı verilir.

Girişin icazəli və ya icazəsiz olmasından asılı olmayaraq, girişlərin və müraciətlərin qeydiyyatı modulu tərəfindən sistemə edilən bütün müraciətlərin və girişin qeydiyyatı aparılır. Giriş icazəli olduqda girişlərin qeydiyyatı jurnalında, əks halda girişə icazəsiz cəhd faktı pozuntular jurnalında qeydiyyata alınır. Hər iki halda istifadəçinin daxil etdiyi ad və parol, eləcə də müraciətin tarixi, vaxtı və tələb olunan resursun adı qeydiyyat jurnalına yazılır və saxlanılır.

İstifadəçinin, sistemin və şəbəkənin həqiqiliyinin müəyyən edilməsi prosedurası müvafiq proqramların köməyi ilə istifadəçi sistemdə qeydiyyatdan keçdiyi zaman onun daxil etdiyi adın və parolun həqiqətən ona məxsus olmasını müəyyən edir. Burada ziyankarın və ya hakerin hər hansı həqiqi istifadəçinin adından və parolundan istifadə etməklə onun adı altında sistemə girməsi təhlükəsinin qarşısı alınır.

Bundan əlavə, həqiqi istifadəçi öz adı və parolu ilə sistemə və ya şəbəkəyə girən zaman ziyankar və ya haker xəttə və ya şəbəkəyə qoşula, özünü server kimi qələmə verə və istifadəçidən ad və parolu soruşa bilər. Bu halda əlaqəni serverlə həqiqi əlaqə kimi qəbul edən istifadəçi ad və parolunu daxil etdikdə, ziyankar onları qəbul edir və sistemin işini saxlayır (guya sistemdə ilişmə baş verdi və s.). Bundan sonra, o, bu ad və paroldan istifadə etməklə asanlıqla sistemə daxil ola bilir. Belə təhlükənin qarşısını almaq üçün modul istifadəçiyə qoşulduğu sistemin və ya

şəbəkənin həqiqi olub olmamasını müəyyən etməyə imkan verən prosedurları təqdim edir.

İdentifikasiya prosedurasının köməyi ilə hər bir istifadəçiyə, terminala, informasiya resurslarına, proqramlara və digər obyektlərə unikal identifikator mənimsədilir. Səhv identifikasiya hallarının qarşısını almaq məqsədilə bu identifikatorlara yoxlama ədədləri, parollar və ya digər nəzarət vasitələri uyğun qoyulur. Qeyd olunmalıdır ki, identifikatorun və parolun istifadəsi yalnız onun tanınması üçün deyil, həm də müraciətlərin qeydiyyata alınması üçün zəruridir.

Sistemə və onun resurslarına müraciətlərin qeydiyyatı informasiyanın sızmasının səbəbini və ya yerini müəyyənləşdirməyə kömək edə bilər. Əgər sistemdə müəyyən təhlükəsizlik səviyyəsi tələb olunarsa, onda istifadəçinin və sistemin həqiqiliyinin müəyyən edilməsi məqsədilə identifikasiya prosedurundan əlavə digər proseduralar da istifadə edilir.

İdentifikasiya sistemi həqiqiliyin müəyyən edilməsi prosedurası üçün baza rolunu oynayır. Həqiqiliyin müəyyən edilməsi prosedurası müraciət edən şəxsin həqiqətən də daxil edilmiş identifikatorun sahibi olmasını müəyyən etməlidir. Həqiqiliyin müəyyən edilməsi üçün sistem tərəfindən müraciət edən şəxsdən müxtəlif xarakterli suallara cavab verməsini tələb edə bilər. Bunun üçün çoxsəviyyəli parol sistemi və ya dialoq mexanizmləri tətbiq olunur. Yüksək səviyyəli təhlükəsizliyin təmin edilməsi üçün müəyyən şərtlər daxilində dövri olaraq təkrar yoxlamalar həyata keçirilir.

İstifadəçi tərəfindən sistem və ya şəbəkə ilə qarşılıqlı əlaqə yaratdıqda hər iki tərəfin həqiqiliyinin müəyyən olunması üçün də parol və ya dialoq mexanizmlərindən istifadə olunur.

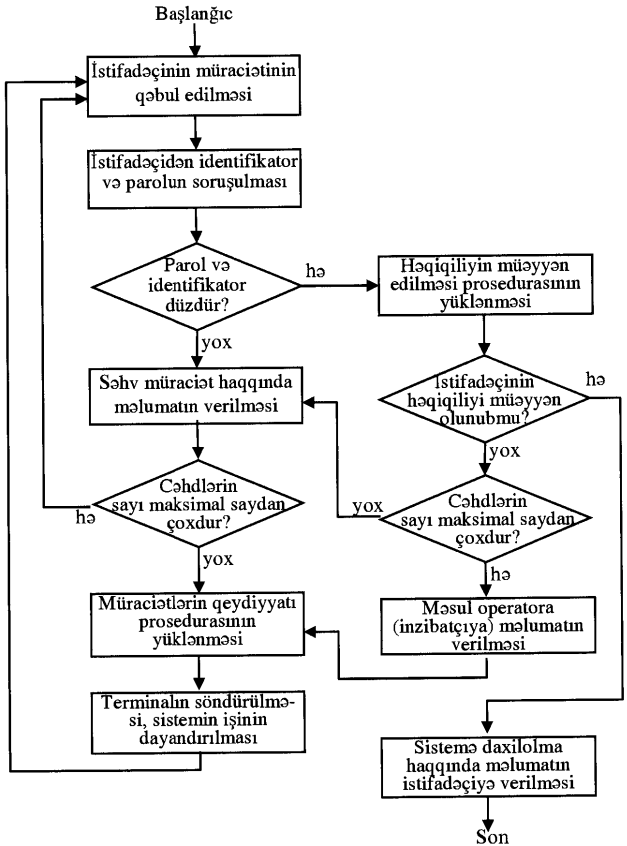
Sistemə və ya onun hər hansı resursuna icazəsiz daxil-olma və ya istifadəçilərin hüquqlarının pozulması zamanı bu barədə sistem tərəfindən operatorun və şəbəkə inzibatçısının terminalına, "etibarlı terminal"a, eləcə də resursun sahibinə və hüququ pozulan istifadəçiyə müvafiq məlumat verilir.

Sistemə və ya resurslara daxilolma prosedurasının funksional sxemi 9.6 saylı şəkildə göstərilmişdir.

9.5. İnformasiya emalının idarə olunması modulu

Əgər girişin məhdudlaşdırılması üsulları qaydaları pozan şəxslərin qarşısını saxlaya bilmirsə, onda onlar sistemə daxil olaraq yaddaş qurğularında saxlanılan informasiyanı ələ keçirə, dəyişdirə və ya məhv edə bilər. Emal prosesinə nəzarət proseduru mühüm məlumatları özündə saxlayan informasiya resurslarının, o cümlədən faylların emalına məhdudiyyətlər qoymağa imkan verir.

Məlum olduğu kimi, ümumiyyətlə, sistemə daxil olan istifadəçi yaddaş qurğusunda olan faylların oxunması, yüklənməsi və ya onlarda dəyişikliklərin aparılması və digər əməliyyatları yerinə yetirə bilər. Bir çox hallarda müəyyən istifadəçilər həmin fayllara baxmaq hüququna malik olur, lakin ona bu fayllarda dəyişikliklər etməyə icazə verilmir. Eyni zamanda, digər istifadəçilər bu fayllara baxa və onlarda dəyişikliklər apara bilər.



Şək.9.6. Girişin idarə olunması modulunun funksional sxemi

Analoji şəkildə istənilən informasiya resursunun (faylların, qovluqların, disklərin, disk qurğularının, proqramların, məlumat bazalarının və s.) istifadəsinə məhdudiyyətlər qoyula bilər.

Qeyd olunduğu kimi, istifadəçinin və ya şəbəkənin həqiqiliyi təsdiq olunduqdan sonra idarəetmə informasiyanın emalı prosesinin idarə olunması moduluna, o cümlədən bu modula daxil olan istifadəçilərin hüquq və səlahiyyətlərinin nəzarətdə saxlanması prosedurasına, əks halda isə sistemə girişlərin və müraciətlərin qeydiyyatının aparılması prosedurasına ötürülür. İstifadəçilərin hüquq və səlahiyyət-lərinin nəzarətdə saxlanması prosedurası seans müddətində istifadəçilərin işini nəzarətdə saxlayır.

İstifadəçilərin hüquq və səlahiyyətlərinin müəyyən edilməsi üçün ikiölçülü matrisdən istifadə olunur: $A = \{a_{ij}\}$, $i = \overline{1,N}, j = \overline{1,M}$, burada n – istifadəçilərin, m isə şəbəkə resurslarının sayıdır.

Matrisin sətirləri – abonentləri (istifadəçiləri), sütunları isə resursları göstərir. i sətri ilə j sütununun kəsişməsində yerləşən a_{ij} elementi i abonentinin j resursuna giriş kateqoriyasını (hüquq və səlahiyyətlərini) müəyyən edir. Bu matrisdə göstərilən hüquq və səlahiyyətlər şəbəkənin inzibatçısı və ya resursun sahibi tərəfindən müəyyən edilir və yalnız onların icazəsi ilə dəyişdirilə bilər.

Yüksək səviyyəli məxfiliyə malik olan məlumatları özündə saxlayan resurslara icazəsiz müraciət zamanı bu müraciəti həyata keçirən proqramın işinin dayandırılması, əlaqənin kəsilməsi, "ilişmə" vəziyyətinə keçilməsi və s. üçün tədbirlər görülür.

Məlum olduğu kimi, qanuni (avtorizə edilmiş) istifadəçi tərəfindən işə salınan və məxfi informasiyanı emal edən proqram işini başa çatdırdıqdan sonra bu informasiyanın qalıqları əməli yaddaşda və digər yaddaş qurğularında qalır. Bu qalıqlar digər istifadəçilər və ziyankarlar tərəfindən istifadə oluna bilər. Ona görə də təhlükəsizlik sistemində yaddaş qurğularından qalıq məlumatların silinməsi prosedurası da nəzərdə tutulur.

9.6. Məlumatların bilavasitə mühafizəsi modulu

İnformasiyanın bilavasitə müdaxilədən qorunması modulu təhlükəsizlik sistemində informasiya daşıyıcılarında saxlanılan, emal olunan və şəbəkə vasitəsilə ötürülən məlumatların icazəsiz istifadədən qorunmasını təmin edir.

Sistemə və resurslara giriş və onların emalı qaydalarını pozan şəxs müvafiq məhdudiyyətləri qeyri-qanuni yollarla adlayıb keçdikdən sonra bilavasitə məlumatlara və informasiya resurslarına icazəsiz giriş əldə etmiş olur. Bu halda kriptoqrafik sistemlərin və təhlükəsizlik protokollarının tətbiq edilməsi məlumatlara və informasiya resurslarına icazəsiz girişin qarşısının alınması üçün etibarlı vasitədir.

İTS tərkibinə daxil olan məlumatların kriptoqrafik qorunması modulu autentifikasiya, məlumatların tamlığının yoxlanması, məlumatların məxfiliyinin təmin edilməsi üçün kriptoqrafik şifrləmə, elektron imza və açarların idarə olunması proseduralarını özündə birləşdirir.

Autentifikasiya prosedurası məlumatların, istifadəçilərin və sistemin həqiqiliyinin müəyyən edilməsi funksiyala-

rını yerinə yetirir. Kommersiya və məxfi rabitə sistemləri, eləcə də məxfi məlumatlarla işləyən digər sistemlərin abonentləri üçün autentifikasiyanın həyata keçirilməsi olduqca vacibdir.

İstifadəçinin həqiqiliyinin təyin olunması prosedurası aşağıdakı məsələlərin həllini nəzərdə tutur:

- göndərən istifadəçi tərəfindən informasiyanın imzalanması;
- informasiyanın həqiqətən identifikasiya olunan istifadəçi tərəfindən göndərildiyinin təsdiq edilməsi;
- informasiyanın göndərilən ünvanda həqiqətən nəzərdə tutulan istifadəçi tərəfindən alınması və s.

Şəbəkənin həqiqiliyinin müəyyən edilməsi prosedurası istifadəçinin həqiqiliyinin təyin olunması prosedurasının əksinə olaraq, istifadəçiyə onun işlədiyi mühitin həqiqiliyini, yəni qoşulduğu şəbəkənin və ya sistemin həqiqətən onun qoşulma istəyi şəbəkə və ya sistem olduğunu təsdiq etməyə imkan verir.

Belə ki, ziyankar tərəf özünü qanuni istifadəçi kimi təqdim edə və həmin istifadəçinin adı altında onun ələ keçirilmiş rekvizitlərini istifadə etməklə sistemə daxil ola, məlumatlar hazırlaya, ala, ötürə, habelə öz məqsədləri üçün istifadə edə bilər.

Şəbəkədə informasiyanı alan və ya ötürən tərəflər (bəzən hər iki tərəf) onun həqiqiliyinin, yəni rabitə xətti vasitəsilə ötürülən zaman onun məzmununun təhrif olunmamasının təsdiqini tələb edə bilər.

Burada informasiyanın həqiqətən göndərilən şəkildə (təhrif olunmadan) ünvana çatması böyük əhəmiyyət kəsb edir. Bu məqsədlə məlumatların tamlığının təmin edilməsi

prosedurasından istifadə edilir. Bu prosedura informasiyanın saxlanması, emalı və ötürülməsi zamanı onun tamlığının təmin edilməsi vasitələrini özündə birləşdirir, alınan informasiyanın ilkin formaya və şəklə malik olmasını müəyyən edir.

Nəticə müsbət olduqda informasiyanın bilavasitə müdaxilədən qorunması və istifadəçilərin açarlarının idarə edilməsi modullarına bu barədə təsdiqedici məlumat qaytarır və onlar fəaliyyətini davam etdirirlər. Əks halda, bu xassələrin pozulması haqqında məlumat həmin modullara verilir və müvafiq tədbirlərin görülməsi barədə qərar isə onlar tərəfindən qəbul edilir.

Məlumatın məğzinin gizlədilməsi və icazəsiz müdaxilədən etibarlı qorunması üçün kriptoqrafik şifrləmə üsullarından istifadə edilir. Bu üsulların işlənib hazırlanması zamanı aşağıdakı amil nəzərə alınmalıdır: sistemə (o cümlədən sistemdə olan məlumatlara) giriş əldə etmiş ziyankar məlumatın şifrini açmaq, yəni məğzini (ilkin formasını) əldə etmək üçün olduqca böyük güc və vaxt sərf etməlidir və ya şifrin açılması real vaxt kəsiyində mümkün olmamalıdır.

Əvvəlki fəsillərdə qeyd edildiyi kimi, kriptoqrafik şifrləmə (o cümlədən asimmetrik şifrləmə) üsullarının və elektron imza texnologiyasının reallaşdırılması üçün açarlar tələb olunur. Bu baxımdan açarların generasiyası və ötürülməsi (onların sahiblərinə çatdırılması) İTS-in əsas problemlərindən biridir. Belə ki, gizli açarların tərəflərə etibarlı çatdırılması, asanlıqla yozulmayan (açılmayan) açarların generasiyası informasiya təhlükəsizliyinin təmin edilməsinin əsas şərtlərindən biridir.

Açarların generasiyası və paylanması mərkəzinin işi açarların idarə edilməsi prosedurası tərəfindən təşkil edilir, açarların ünvana çatdırılması üçün müvafiq təhlükəsiz mübadilə protokolları reallaşdırılır.

Bu modul açarların generasiyası, paylanması və saxlanması ilə yanaşı, köhnəlmiş açarların dəyişdirilməsi, istifadəçilər arasında açıq açarların mübadiləsi və digər funksiyaları yerinə yetirir.

9.7. Təhlükələrə nəzarət, vəziyyətin təhlili və qərarların qəbul edilməsi modulu

Vəziyyətin təhlili və təhlükələrə nəzarət modulu digər modullara nisbətən daha geniş funksiyalara malik olur. Bu funksiyalar bir neçə hissəyə bölünür:

- diaqnostika;
- sistemin fəaliyyətinin etibarlılığının təmin edilməsi;
- təhlükələrin və pozuntuların aşkar olunması.

Sistemə və onun resurslarına istənilən icazəsiz giriş və ya digər pozuntular barəsində məlumat daxil olduqda birinci növ funksiyalar işə düşür. Onlar istifadəçilərin sistemə girişlərinə, hüquq və səlahiyyətlərinə nəzarətin diaqnostikasını həyata keçirirlər.

Sistemin fəaliyyətinin etibarlılığının təmin edilməsi funksiyaları təhlükəsizlik sisteminin bütün modul və proseduralarının işini tənzimləyir və nəzarətdə saxlayır. Əgər sistemin hər hansı elementi sıradan çıxarsa, onda bu barədə şəbəkə inzibatçısına məlumat verilir və zərurət yarandıqda idarəetmə təhlükəsizlik sisteminin struktur parametrlərinin yeniləşdirilməsi moduluna verilir.

Üçüncü hissə funksiyalar təhlükələrin və pozuntuların aşkar olunması üzrə tədbirləri həyata keçirir. Bu funksiyalar dövri olaraq yerinə yetirilir, təhlükəsizlik sisteminin bütün qovşaqlarını, açarların mübadiləsi protokolunu və paylanması mərkəzinin işini yoxlayan test proseduralarını həyata keçirir.

Sistemin resurslarına icazəsiz giriş təhlükəsi, istifadəçilərin hüquq və səlahiyyətlərinin pozulması halları aşkar olunduqda sistemin inzibatçısına xəbərdarlıq edilir və idarəetmə baş verən pozuntuların qarşısının alınması moduluna verilir.

Sistemdə istənilən icazəsiz giriş və ya pozuntu halları olduqda baş verən pozuntuların qarşısının alınması modulu işə düşür. Bu modul sistemin işinin dayandırılması, pozuntu nəticəsində ziyan vurulduqda sistemin bərpası, ziyanın aradan qaldırılması, yaddaş qurğularından "qalıq"-ların silinməsi və s. funksiyalarını yerinə yetirir.

Sistemdə təhlükəsizlik baxımından zəif yerlər aşkar olunduqda idarəetmə sistemin struktur parametrlərinin yeniləşdirilməsi moduluna verilir.

Təhlükəsizlik sisteminin struktur parametrlərinin yeniləşdirilməsi modulu idarəetməni qəbul etdikdən sonra sistemin inzibatçısının rəhbərliyi altmda sistemin konfiqurasiyasında dəyişikliklərin aparılmasına başlayır. Bu modul sıradan çıxmış istənilən modulu təhlükəsizlik sistemində ayıra, başqası ilə əvəzləyə və ya yeni modulu əlavə edə bilər və s.

Aydındır ki, KSŞ-də və ya informasiya emalı sistemlərində həyata keçirilən istənilən, o cümlədən icazəsiz və qeyri-qanuni əməllər (hərəkətlər) onun vəziyyətini dəyişir. Ona görə də şəbəkənin və sistemin vəziyyəti daima nəzarətdə saxlanılır, onun konfiqurasiyasının zəif tərəfləri aşkar olunur, qoruma vasitələrində ən zəif yerlər müəyyən edilir və aradan qaldırılır.

Vəziyyətin təhlili üçün təhlükəsizliyin pozulmasına yönəlmiş bütün cəhdlər müntəzəm olaraq protokollaşdırılır və ekspert təhlili aparılır. Zəruri hallarda, gələcəkdə yerinə yetirilməsi tələb olunan tədbirlər barədə müvafiq qərarlar qəbul edilir. Məsələn:

- İTS-ə daxil olan qoruma üsullarının dəyişdirilməsi və ya təkmilləşdirilməsi;
- İTS-ə yeni qoruma üsul və vasitələrinin daxil edilməsi;
- KSŞ-nin və ya informasiya sisteminin, eləcə də İTS-in konfiqurasiyasının dəyişdirilməsi.

İTS paylanmış mürəkkəb kompleks olduğundan onun idarə edilməsi prosesinin səmərəliyini təmin etmək üçün süni intellektual üsul və vasitələrindən istifadə olunması daha effektiv nəticəni təmin edir. İTS-də məlumatların qorunması proseslərini üç kateqoriyaya ayırmaq olar:

- sürətlə baş verən proseslər – sistem resurslarına giriş hüquqlarının yoxlanması zamanı xidməti məlumat bazalarında növbələrin əmələ gəlməsi və çəkilməsi;
- asta baş verən proseslər – qoruma funksiyalarının reallaşdırılması barədə sorğuların intensivliyinin dəyişməsi;

- çox asta baş verən proseslər – açarların və parolların köhnəlməsi.

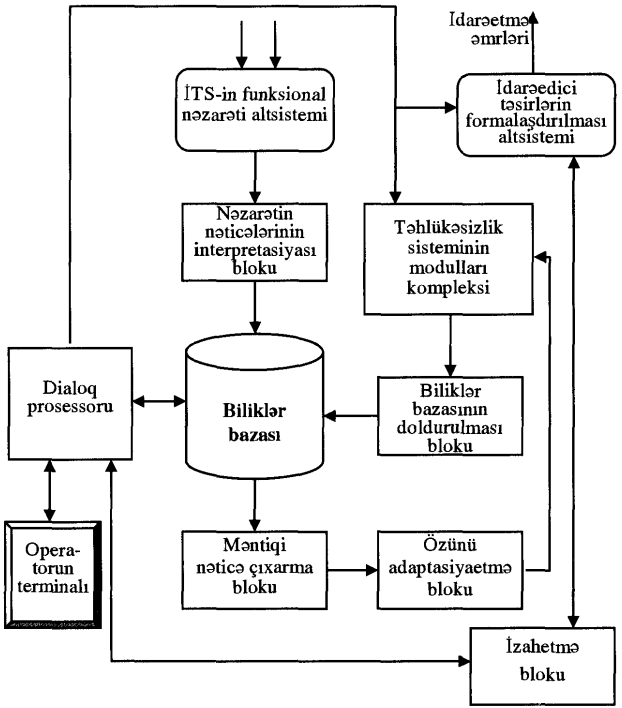
Bu proseslərin izlənməsi və baş verməsinin təhlili üçün müvafiq ekspert sisteminin yaradılması tövsiyə olunur. Şəbəkədə və ya sistemdə baş verən pozuntu və ya sıradan çıxma halları aşkar olunduqda reaksiyanın verilməsini avtomatlaşdırmaq və sürətləndirmək məqsədilə informasiya təhlükəsizliyinin təmin edilməsi vasitələrinin idarə olunması üzrə qərarların qəbul edilməsi proseduraları zəruri funksional komponentləri özündə birləşdirir (şək.9.7).

Təhlükəsizlik sisteminin funksional nəzarəti altsistemi qoruma vasitələrinin normal işləməsini yoxlamaq üçün test əmrlərini formalaşdırır və şəbəkəyə göndərir. Yoxlamaların nəticələri real vaxt masştabında bu altsistem tərəfindən toplanılır. Bu, baş verən pozuntulara operativ reaksiyanın verilməsi imkanlarını təmin edir.

Yoxlamanın nəticəsi haqqında sistemdən daxil olan məlumatlar onun cari vəziyyəti haqqında bilikləri yeniləşdirmək üçün istifadə olunur və əvvəlki biliklərlə birlikdə zəruri idarəedici tədbirlərin (təsirlərin) həyata keçirilməsi üçün əsas rolunu oynayır.

Daxil olan informasiyanın biliklər bazasının daxili formatına çevrilməsi və təhlükəsizlik sisteminin işinin modelləşdirilməsi üçün ilkin məlumatların formalaşdırılması nəticələrin interpretasiyası altsistemi tərəfindən yerinə yetirilir.

Məntiqi nəticə çıxarma bloku sistemdə və şəbəkədə baş verən pozuntu hallarının qarşısının alınması və ya kompensasiyası məqsədilə yerinə yetirilən idarəedici təsirlərin,



Şək.9.7. Qərar qəbuletmə proseduraşının funksional strukturu

sistemin və ya şəbəkənin elementlərinin və qoruma vasitələrinin növlərini müəyyən etmək üçün nəzərdə tutulmuşdur.

Şəbəkədə informasiyanın sızmasına, itməsinə və ya dəyişdirilməsinə gətirib çıxara biləcək pozuntu halları aşkar olunan zaman icazəsiz daxilolma yerinin dəqiqləşdirilməsi və lokallaşdırılması, eləcə də informasiyanın sızması kanalının müəyyənləşdirilməsi üçün süni intellekt aparatının elementlərindən istifadə etmək olar.

Qərarların qəbul edilməsi proseduraşının funksiyalarının yerinə yetirilməsi, eləcə də ekspert sisteminin reallaşdırılması üçün süni intellekt və qeyri-səlis çoxluqlar nəzəriyyələrinin imkanlarından istifadə edilir.

Ekspert sistemi təhlükəsizlik sisteminin vəziyyətini daim nəzarətdə saxlayır, biliklər bazasını real vaxt intervalında aparılmış yoxlamalar nəticəsində alınan məlumatlarla doldurur və məntiqi nəticə çıxarır.

Giriş hüquqlarının və səlahiyyətlərin pozulması halları, sistemdə zəif yerlər və informasiyanın sızması kanalları, şifrləmə üsullarında və informasiya mübadiləsi protokollarında boşluqlar aşkar edildikdə, eləcə də digər müvafiq hallarda məsul operatora idarəedici əmrlər və məlumatlar verilir. Bu əmrlərə nümunə kimi aşağıdakıları göstərmək olar:

- seansı təcili dayandırmaq;
- sıradan çıxmış qovşağı sistemdən və ya şəbəkədən ayırmaq;
- qoruma vasitəsini və mübadilə protokolunu yenisi ilə əvəz etmək;

- mütəmadi olaraq abonentlərin (istifadəçilərin) açarlarını dəyişdirmək və s.

Belə qurulmuş ekspert sistemi iş prosesində İTS-in fəaliyyətinin səmərəliyini və etibarlılığını təmin edir. Mövcud özünü adaptasiyaetmə bloku məntiqi nəticə çıxarma prinsipinə əsaslanaraq, sistemin etibarlığını və modulluluğunu yüksəltmək məqsədilə onun parametrlərini dəyişdirir.

Burada modulluluq dedikdə sistemin elementlərinin müstəqil və bir-birindən asılı olmadan reallaşdırılması və fəaliyyət göstərə bilməsi qabiliyyəti başa düşülür. Belə ki, hər hansı element sıradan çıxdıqda belə sistemdə informasiya sızmasına və onun işinin dayanmasına gətirib çıxarmamalıdır.

İnformasiya təhlükəsizliyinin təmin edilməsinin idarə olunması prosesində izahetmə blokunun və dialoq prosessorunun köməyi ilə məsul operatora və ya şəbəkə inzibatçısına məlumat göndərilir. Məsul operator və ya şəbəkə inzibatçısı istənilən mərhələdə idarəetmə prosesinə qarışmaq və idarəedici əmrlər vermək hüququna malikdir. Onun bütün hərəkətləri (əmrləri və idarəedici təsirləri) biliklər bazasında qeydiyyata alınmalı və ekspert sistemi tərəfindən real vaxtda təhlil olunmalıdır.

TÖVSİYƏ OLUNAN ƏDƏBİYYAT

Normativ-hüquqi aktlar

1. "İnformasiya, informasiyalaşdırma və informasiyanın qorunması haqqında" Azərbaycan Respublikasının Qanunu. Bakı. 3 aprel 1998-ci il.
2. "Elektron imza və elektron sənəd haqqında" Azərbaycan Respublikasının Qanunu. Bakı. 9 mart 2004-cü il.
3. "Milli təhlükəsizlik haqqında" Azərbaycan Respublikasının Qanunu. 3 avqust 2004-cü il.
4. "Dövlət sirri haqqında" AR. Qanunu. Bakı, 7 sentyabr 2004-cü il.
5. "Məlumat toplularının hüquqi qorunması haqqında" Azərbaycan Respublikasının Qanunu. 14 sentyabr 2004-cü il.
6. "Elektron ticarət haqqında" Azərbaycan Respublikasının Qanunu. 10 may 2005-ci il.
7. "İnformasiya əldə etmək haqqında" Azərbaycan Respublikasının Qanunu. 30 sentyabr 2005-ci il.
8. "Azərbaycan Respublikasının milli təhlükəsizlik konsepsiyası". 23 may 2007-ci il.

Azərbaycan dilində

9. "İnformasiya təhlükəsizliyi". İnformasiya bülleteni. Azərbaycan Respublikasının Prezidenti yanında Dövlət Sirrinin Mühafizəsi üzrə İdarələrarası Komissiya. 2008. № 1.

10. "İnformasiya təhlükəsizliyi". İnformasiya bülleteni. Azərbaycan Respublikasının Prezidenti yanında Dövlət Sirrinin Mühafizəsi üzrə İdarələrarası Komissiya. 2008. № 2.
11. Abbasov Ə.M., Əliyev F.Ə., Əliyev Ə.Ə., Əhmədov F.B. İnformatika, telekommunikasiya və radioelektronika üzrə ingiliscə-rusca-azərbaycanca lüğət. – Bakı. Elm, 2004. -296 s.
12. Əliquliyev R.M., İmamverdiyev Y.N. Rəqəm imza texnologiyası. Bakı. Elm, 2003. – 132 s.
13. Əliquliyev R.M., İmamverdiyev Y.N. Kriptoqrafiyanın əsasları. Bakı, "İnformasiya texnologiyaları". 2006. – 688 s.
14. Əliquliyev R.M., İmamverdiyev Y.N. Kriptoqrafiya tarixi. Bakı, "İnformasiya texnologiyaları". 2006. – 192 s.
15. Qasımov V.Ə. İnformasiya təhlükəsizliyi: kompyuter cinayətkarlığı və kiberterrorçuluq. Bakı. Elm, 2007. - 192 s.

Rus dilində

16. Аббасов А.М., Алгулиев Р.М., Касумов В.А. Проблемы информационной безопасности в компьютерных сетях. Баку: Элм, 1998. – 235 с.
17. Адигеев М.Г. Введение в криптографию. – Ростов-на-Дону: Изд-во Ростовского ГУ, 2002. -36 с.
18. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии.–М.: Гелиос АРВ, 2001.– 480 с.

19. Андрианов В.И., Бородин В.А., Соколов А.В. «Шпионские штучки» и устройства для защиты объектов и информации. Санкт-Петербург, Лань, 1996. 272 с.
20. Берент С., Пэйн С. Криптография. Официальное руководство RSA Security. –М.: ООО «Бином-Пресс», 2007. -384 с.
21. Биячуев Т.А. Безопасность корпоративных сетей. Учебное пособие.// Санкт-Петербург. СПб ГУ ИТМО, 2004. -161 с.
22. Болотов А.А. и др. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. –М.: КомКнига, 2006. 328 с.
23. Варлатая С.К., Шаханова М.В. Аппаратно-программные средства и методы защиты информации. – Владивосток: Изд-во ДВГТУ, 2007. 318 с.
24. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. — М.: МЦНМО, 2003. -328 с.
25. Галатенко В.А. Стандарты информационной безопасности. –М.: ИНТУИТ.РУ "Интернет-университет ИТ", 2004. – 328 с.
26. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. –М.: Солон-Пресс, 2002. 265 с.
27. Гроувер Д. Защита программного обеспечения. – М.: Радио и связь, 1992. -286 с.
28. Грушо А.А., Тимошина Е.Е. Теоретические основы защиты информации. –М.: Издательство Агенства "Яхтсмент", 1996. -192 с.

29. Губенков А.А., Байбурин В.Б. Информационная безопасность. –М.: ЗАО "Новый издательский дом", 2005. -128 с.
30. Жельников В. Криптография от папируса до компьютера. -М.: ABF, 1996.
31. Зегжды П.Д. Теория и практика обеспечения информационной безопасности. М.: Издательство Агенства "Яхтсмент", 1996. -192 с.
32. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. –СПб.: БХВ-Петербург, 2003. – 368 с.
33. Железняк В.К. Защита информации от утечки по техническим каналам: учебное пособие. ГУАП. – СПб., 2006. – 188 с.
34. Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры: Учебное пособие. –М.: Гелиос АРВ, 2005. – 192 с.
35. Казарин О.В. Безопасность программного обеспечения компьютерных систем. Монография. – М.: МГУЛ, 2003. – 212 с.
36. Кан Д. Взломщики кодов. –М.: Издательство "Центрполиграф", 2000. – 473 с.
37. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. - СПб.: БХВ-Петербург, 2003.
38. Корнюшин П.Н., Костерин С.С. Информационная безопасность. –Владивосток. Издательство Дальневосточного ГУ, 2003. -155 с.

39. Коханович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. – М.: МК-Пресс, 2006. 288 с.
40. Левин Дж., Бароди К. Секреты Интернет. –Киев: Диалектика, Информейши компьютер Энтерпрайз, 1996. -544 с.
41. Левин М. Криптография без секретов: Руководство пользователя. –М.: "Новый издательский дом", 2005. – 320 с.
42. Медведовский И.Д., Семьянов П.В., Леонов Д.Г. Атака на Интернет. – М.: ДМК, 2000. – 336 с.
43. Оков И.Н. Криптографические системы защиты информации. – СПб.:, ВУС, 2001. –236с.
44. Ржавский К.В. Информационная безопасность: практическая защита информационных технологий и телекоммуникационных сетей. Учебное пособие. – Волгоград. Из-во ВолГУ, 2002. -122 с.
45. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. –М.: Радио и связь, 2001. -376 с.
46. Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия. Учебное пособие. –М.: "Дашков и К°", 2005. -336с.
47. Сингх С. Книга кодов: тайная история кодов и их "взлома". –М.: АСТ:Астрель, 2007. -447с.
48. Скляров Д.В. Искусство защиты и взлома информации. –Санкт-Петербург: BHV-Санкт-Петербург, 2004. -288 с.

49. Смарт Н. Криптография. -М.: Техносфера, 2006. – 528 с.
50. Соколов А.В., Степанюк О.М. Защита от компьютерного терроризма. Справочное пособие. – СПб.: БХВ-Петербург; Арлит, 2000. – 496 с.
51. Соколов А.В., Шангин В.Ф. Защита информации в распределенных корпоративных сетях и системах. // ДМК Пресс, 2002. -656 с.
52. Спесивцев А.В., Вегнер В.А,, Крутяков А.Ю. и др. Защита информации в персональных ЭВМ. – М.: Радио и связь, 1992. -192 с.
53. Стенг Д., Мун С. Секреты безопасности сетей. – Киев: Диалектика, Информейшн компьютер Энтерпрайз, 1996. -544 с.
54. Таненбаум Э. Компьютерные сети. –СПб.: Питер, 2006. – 992 с.
55. Торокин А.А. Инженерно-техническая защита информации. –М.: Гелиос АРВ, 2005. -960 с.
56. Уфимцев Е.А., Ерофеев Е.А. Информационная безопасность России. –М.: "Экзамен", 2003. – 560с.
57. Хижняк П.Л. Пишем вирус и … антивирус. –М.: ИНТО, 1991. – 90 с.
58. Хоффман Л.Дж. Современные методы защиты информации. –М.: Советское радио, 1980. 264 с.
59. Шеннон К. Работы по теории информации и Кибернетики / Пер. с англ. –М.: Иностранная литература, 1963. – 829 с.

60. Юсупов Р.М. Наука и национальная безопасность. – СПб.: Наука, 2006. -290.
61. Яковлев В.А. Защита информации на основе кодового зашумления. Часть 1. Теория кодового зашумления. / Под ред. В.И. Коржика.– С.Пб.: ВАС, 1993.–245с.
62. Яковлев А.В., Безбогов А.А., Родин В.В., Шамкин В.Н. Криптографическая защита информации. – Тамбов: Издательство ТГТУ, 2006. -140 с.
63. Ярочкин В.И. Информационная безопасность. – М.: Трикста, 2005. -544 с.

İngilis dilində

64. Abbasov A.M., Gasumov V.A. Construction principles of the security service in the computer systems. // Proceeding of JENC-7. Budapest. 1996. pp.1771-1775.
65. Bender W., Gruhl D., Morimoto N., Lu A. Techniques for data hiding. // IBM Systems Journal, Vol 35, N: 3&4, 1996. pp.313-336.
66. Brassard J. Modern Cryptology. Springer-Verlag, Berlin - Heidelberg, 1988. - 107 p.
67. Building Internet Firewalls, by Brent Chapman. // http://www.greatcircle.com/gca/tutorial/wwwsite.html.
68. Cachin C. An Information-Theoretic Model for Ste-ganography. // In Proceedings of 2nd Workshop on Information Hiding (D. Aucsmith, ed.), Lecture Notes in Computer Science, Springer, 1998.

69. Cheswick W., Bellovin S., Addison W. Firewalls and Internet security. // http://www.anatomy.su.oz.au/danny/book-review/h/Firewals_and_Internet_Security.html.
70. Data Integrity. // LLC. http://www.dintegra.com/.
71. Diffie W., Hellman M.E. New directions in cryptography // IEEE Trans. on Information Theory. 1976. Vol. 22. № 6. P. 644-654.
72. Landwehr C.E. Computer security. // International Journal of Information Security, 2001. №1. pp.3-13.
73. Ranum M., Avolio F. A toolkit and Methods for Internet Firewalls. Trusted Information Systems Inc. // http://www.tis.com/docs/products/gauntlet/Usenix.html/.
74. RSA Data Security. //http://www.rsa.com/.

MÖVZU GÖSTƏRİCİSİ

K

Q

T

Ü

V

Y

Z

Qasımov Vaqif Əlicavad oğlu
Texnika elmləri doktoru

İnformasiya təhlükəsizliyinin əsasları

Dərslik

Bakı – 2009

Redaktor:

Zərif CƏFƏROVA

Kompyuter səhifələyicisi:

Ceyhun MAHMUDOV
Araz AŞUROV

Yığılmağa verilib: 18.05.2009.
Çapa imzalanıb: 12.10.2009.
Fiziki çap vərəqi 21,25. Nəşrin formatı 60x84 $^{1}/_{16,}$
Sifariş 1235. Tiraj 300.

MTN Maddi-texniki Təminat Baş İdarəsinin
Nəşriyyat-Poliqrafiya Mərkəzində
nəşrə hazırlanmış və ofset üsulu ilə çap edilmişdir.