AZƏRBAYCAN RESPUBLİKASI TƏHSİL NAZİRLİYİ

AZƏRBAYCAN DÖVLƏT İQTİSAD UNİVERSİTETİUNEC

MAGİSTRATURA MƏRKƏZİ

Əlyazması hüququnda

Ramazanova Nəzrin Məzahir qızının

"İnternet şəbəkəsində verilənlərin saxlanma təhlükəsizliyinin təmini"

mövzusunda

MAGİSTR DİSSERTASİYASI

İxtisasın şifri və adı: **060509 "Kompüter elmləri'**

İxtisaslaşma: **'İqtisadi İnformasiya sistemləri'**

Elmi rəhbər: **Dos. V.Ş.İBRAHİMOV**

Magistr proqramının rəhbəri: **akad.Ə.M.ABBASOV**

Kafedra müdiri: **akad.Ə.M.ABBASOV**

BAKI – 2020

İxtisar siyahısı:

AİS	Avtomatlaşdırılmış İnformasiya Sistemi
EHM	Elektron Hesablam Maşınları
İHŞ	İnformasiya Hesablama Şəbəkələri
İS	İnformasiya Sistemi
LAN	Local Area Network
MAN	Metropolitan Area Network

MÜNDƏRİCAT

Giriş

Mövzunun aktuallığı

Elmi-texnolojı tərəqqi və bununla əlaqəli olan insan fəaliyyətinin inteqrasiyası günümüzün qlobal problemlərinin yaranmasına səbəb oldu, bu da cəmiyyətdə təhlükəsizlik problemini ortaya qoydu. Məlumat təhlükəsizliyi nədir?

Məlumat təhlükəsizliyi ən vacib iş aktivlərinizi məlumatlarınızı icazəsiz və ya istenməyen istifadədən qorumaqdır. Bu, yalnız düzgün məlumat təhlükəsizliyi məhsullarının yerləşdirilməsini deyil, həm də insanları və prosesləri, məlumatları bütün ömrü boyu qorumaq üçün seçdiyiniz texnologiya ilə birləşdirməyi əhatə edir. Müəssisə məlumatlarının qorunması komandanın idman növünə oxşardır.

Effektiv məlumat təhlükəsizliyi üçün ən yaxşı təcrübələrə, məlumatların qorunması üçün bir riskə əsaslanan bir yanaşma tətbiq etmək, bütün müəssisə daxilində məlumat təhlükəsizliyi məlumatlarını birləşdirən vahid platformadan istifadə etməkdir.

İnsan cəmiyyəti üçün təhlükələri araşdırsaq onun əsas aşağıdakı komponentlərini misal göstərmək olar:ekoloji, siyasi,texnolojı,iqtisadi və s. İnformasiya təhlükəsizliyi bu komponentlər arasında ən əsası sayılır.

Tədqiqatın məqsədi və vəzifələri

Qlobal Şəbəkələrdə işləmək ehtiyyacı yarandıqdan sonra bir sıra tələblər haqda suallar yaranır .Hansı proqram və aparat vasitələri və təşkilati tədbirlər həyata keçirilməlidir? Risk profili nədən ibarətdir? Bu tip suallara cavab almaq üçün təşkilat üçün konseptual təhlükəsizlik siyasəti yaradırlar və tədqiqatın əsas məqsədi bu siyasətin nə dərəcədə əhəmiyyətli olduğunu araşdırmaq və təkliflər irəli sürməkdir.

Təhlükəsizlik siyasətini 2 hissəyə ayırmaq olar:

1. Texniki siyasət -avadanlıqlar və proqram ,aparat vasitələri ilə reallaşdırılır.
2. Administrativ siyasət-aparat və proqramlardan istifadə edən insanlar,insanlara rəhbərlik edən şəxslər vasitəsilə həyata keçirilir.

Uzun illər təşkilatlarda komputerlə printer, skaner və s əlavə cihazlar arasında məlumat mübadiləsi lokal şəbəkə LAN vasitəsilə həyata keçirilirdi.Sonralar lokal şəbəkələrdə bir biri ilə əlaqələndirildi və yeni növ şəbəkə meydana gəldi -regional şəbəkəMAN.Regional şəbəkələr coğrafi hududlar daxilində , hər hansı şəhərin regionun məlumat mübadiləsinə imkan yaradırdı.

Hal hazırda dünyada qlobal şəbəkələr üstünlük təşkil edir onlar arasında ən məşhurları olan Internet, Relcom, Sovintel, bundan başqa ixtisaslaşmış şəbəkələr,Medical Systems və s misal göstərmək olar.

Tədqiqat obyekti və predmenti

Dissertasiya işinin tədqiqat obyekti dövlətin,təşkilatların təhlükəsizlik sistemi,sistemin mühafizə vasitələridir ,predmeti isə təhlükə yaradacaq risklərin aradan qaldırılması ,təhlükəsiz sistemin yaratmaq yollarının öyrənilməsinə yönəlir.

Tədqiqatın informasıya bazası

Azərbaycan Respublikası konstitusiyası , İnternet şəbəkəsinin informasiya ehtiyyatları, mövzunu əhatə edən xarici resusrlar ədəbiyyatları təşkil edir. Tədqiqat prosesində təhlil, analiz,müqayisə, məntiqi ümumiləşdirmə,iqtisadi-riyazi və s. metodlardan istifadə edilmişdir.

Tədqiqatın elmi yeniliyi

Dünya ölkələrində olan müasir avtomatlaşdırılmış informasiya sistemləri üzərində araşdırma aparılmış və elmi nəticələr əldə olunmuşdur,araşdırmalar əsasən aşağıdakı istiqamıtlərdə olmuşdur:

- Müasir informasiya sistemlərinin təşkil ediciləri,elementləri,təminatları araşdırılmış;
- Təhlükələrin növləri tədqiq olunmuş;
- Risklər barədə ətraflı məlumat verilmiş;
- Dayanıqlı sistem və verilənlərin şəbəkədə qorunma yolları göstərilmişdir.

Tədqiqatın praktiki əhəmiyyəti

Tədqiqatın praktiki əhəmiyyəti ondan ibarətdirki araşdırılmış və sadalanmış beynəlxalq təhlükəsizlik standartları,təhlükəsizlik vasitələri,dünya təcrübəsində əldə olumuş nəticələr əsasında Azərbaycanda yəni ölkəmizdə təhlükəsizlik sistemlərini təkmilləşdirmək və tamamilə elektron sistemə keçid etmək olar.

Dissertasiya işinin quruluşu və həcmi

Dissertasiya işi 3 fəsildən ibarətdir.İlk fəsil kompüter və informasiya sistemləri şəbəkəsində təhlükəsizlik məsələlərini əhatə edir,ikinci fəsil şəbəkələrin qorunması ,audit və protokollaşdırma həmçinin proqramların virusdan qorunması məsələlərini əhatə edir .Üçüncü fəsil yeni metodların , informasiya mühafizəsi və kriptoanaliz vasitələrin tətbiqi məsələlərini əhatə edir. Dissertasiya işi ədəbiyyat siyahısının təqdimatı ilə başa çatır.

I FƏSİL. Informasiya Sistemlərinin Təhlükəsizliyinin əsas istiqamətləri.

1.1 İnformasiya Sistemlərinin Təhlükəsizliyi anlayışı

Informasiya Təhlükəsizliyi məsələsi insan cəmiyyətində insanlar arasında informasiya mübadiləsində xüsusi yer tutur və təhlükəsizlik məsələlərinə böyük diqqət ayrılır.Demək olar ki, hər bir fealiyyətdə uğur qazanmaq qiymətli olan informasiya təminatına malik olmaqdan aslıdır .Bir çox dövlətlərin misal olaraq Rusiya Federasiyasının- informasiya,informasiyalaşdırma və informasiyanın qorunması haqda qanununda qeyd olunur ki, informasiya resursları -vətəndaşların,təşkilatların ,korporasiyaların ,dövlətin mülkiyyətidir.

Informasiya Təhlükəsizliyi-kifayət qədər çətin və çoxsəviyyəli problemdir və problemin həlli yalnız sistemli və kompleks yanaşma ilə əldə oluna bilər.

Bu problemi həll etmək üçün qanunvericilik,inzibati ,prosedur və proqram-texniki səviyyədə tədbirlər həyata keçirilir

Gündəlik həyatımızda Elektron Hesablama Maşınından EHM və İnsan-Maşın tərkibli müxtəlif sistemlərdən istifadə İnfromasiya Təhlükəsizliyi problemini qarşıya qoyur.

Bu tip sistemlərin əsas siniflərindən biri Avtomatlaşdırılmış idarəetmə sistemidirAİS -bu tip sitemlərdə informasiyanın toplanması,emalı,saxlanması və idarəetmənin avtomatlaşdırılması hesablama texnologiyalarının avtomatlaşdırılması nəticəsində reallaşdırılır.

Muasir Avtomatlaşdırılmış İdarəetmə sistemləri- coğrafi cəhətdən paylanmış bir çox sahələri vahid dövrədə birləşdirir və özündə ixtisaslaşmış və kompleks Elektron Hesablama Maşınları,terminallar,məlumat ötürmə cihazları digər abuneçi cihazlarını-məlumat hesablama şəbəkələrini əhatə edir.

Avtomatlaşdırılmış idarəetmə sisteminiAİS və İnformasiya Hesablama Şəbəkələrinin İHŞ yaranması beynəlxalq informasiya məkanının dünya sivilizasiya

çərçivəsində formalaşmasına səbəb oldu.Təcrübədə bu tip sitemlərdən istifadə zamanı kompüter cinayətkarlığı iqtisadi və siyasi təxribat, elektron təxribat, şəxsiyyətin hüquq və azadlıqlarının pozulması kimi mənfi hallarla qarşılaşmaq mümkündür.Bütün bunlar informasiya təhlükəsizliyinin bəşəriyyətdə xüsüsi rolu olduğunu vurğulayır.

Mühafizənin predmetinə - Kompüter sistemində saxlanılan ,emal olunan ötürülən məlumatlar daxildir.Bu tip informasiyanın xüsusiyyətləri aşağıdakılardır:

- Fiziki daşıyıcının təbiətindən aslı olmayan ,kompüter sisteminin daxilində ikilik şəkildə saxlanılan məlumatlar
- Avtomatlaşdırmanın yüksək səviyyəsi informasiyanın emalı və ötürülməsi
- Kompüter Şəbəkəsində böyük miqdarda məlumatların konsentarsiyası

İnformasiya Mühafizəsinin obyektinə-İnformasiyanın avtomatlaşdırılmış emalı sistemi və ya kompüter sistemi sayılır.

Murəkkəb idarəetmə sisteminin yaradılmasının və tətbiqinin nəzəri əsaslarının inkişafı informatikanın- informasiyanın EHM və digər texniki vasitələrlə saxlanması,emalı,ötürülməsinin metodlarını öyrənən elmin inkişaf tempindən aslıdır.Eyni zamanda informatika kibernetikanın fundamental əsaslarına söykənən idarəetmə elminin fundamental nəzəri teminatını təşkil edir.

İnformasiyanın nəzəri əsaslarını -informasiya nəzəriyyəsi təşkil edir bu nəzəriyyə kibernetikanın müstəqil bölməsi kimi müxtlif sahələrdə informasiya proseslərinin riyazi təsvirini və tədqiqat ,ötürmə ,emal,informasiyanın çıxarıması metodlarını öyrənir.

Hər hansı avtomatlaşdırılmış idarəetmə sistemini-alqortmik dəstəyinin inkişafı və optimallaşdırlması olmadan qurmaq mümkün deyil.

Alqortmin əsasını-alqoritmlər nəzəriyyəsi və riyaziyyatın -hesablama alqoritmlərini ,riyazi obyektləri oyrənən çoxluqlar nəzəriyyəsi metodları və s oyrənən metodları təşkil edir.

Regional paylanmış idarəetmə sistemlərinin qurulması zamanı yalnız informasiyanın yığılması ,emalı,saxlanması metodlarını və alqoritmlərini deyil həmçinin sistemlər arası məlumatların ötürülməsi metodlarının da öyrənilməsi vacibdir.Bu hal avtomatlaşlaşdırılmış idarə sistemlərinin tətqiqi və təhlilində informasiya nəzəriyyəsinin hissələri olan-informasiya ötürülməsi nəzəriyyələrindən,kodlaşdırma və kriptologiya nəzəriyyələrindən istifadəni lazımi edir.Bu nəzəriyyələrin məcmusu avtomatlaşdırılmış idarə etmə sisteminin daxilində verilənlərin gizli ötürülməsini dəstəkləsədə,informasiya təhlükəsizliyi probleminin strukturunun qurulmasını və sistemin fəaliyyətinin bütün aspektlərini morfoloji, funksional, məlumatverici və praqmatik prosesləri təhlil etməyə imkan vermir.Nəticə olaraq yeni istiqamətin formalaşması-əsasını kompüter texnologiyası təşkil edən idarəetmə sistemlərində - məlumat ötürülməsi nəzəriyyəsini, kodlaşdırma nəzəriyyəsini, kriptologiyanı özündə sistemli şəkildə birləşdirən təsadüfən və ya qəsdən olunan hədələrin , verilənlərin təhrif edilməsinin və ya məhv edilməsinin qarşısını almaq üçün informasiya təhlükəsizliyi nəzəriyysəsinin yaranmasına ehtiyyac yaranır.

Yeni nəzəriyyə kibernetika və informatikanın metodlarının sintezi nəticəsində yaranmasında aslı olaraq təşkilati-texniki sistemlərdə baş verən informasiya prosesslərini tədqiq edir və əsasən informasiyanın avtomatlaşdırılmış emalına yönəlir və bununlada öz predmet sahəsini saxlamaqla öz məzmununa görə informatikaya daxil olur .

Hal hazırda informasiya çox mənalı söz kimi şərh olunur və əsasən müəllifin qarşıya qoyduğu hədəflərdən aslıdır. Beləliklə, V.İ. Şapovalov bu tərifi verir: Bir obyekt haqqında məlumat, müşahidəçinin obyektlə qarşılıqlı təsirindən yaranan müşahidəçi parametrindəki dəyişiklikdir.Digər yanaşma isə Shannon tərəfindən təklif olunan və onun kəmiyyət ölçülməsi ilə əlaqəlidir .

İnformasiya dedikdə müəyyən predmet sahəsi üzrə tədqiq olunan obyekt haqda hadisələr,faktlar,obyektin əsas xüsusiyyətləri xarakteristikaları və həmçinin bu

informasiya elə olmalıdır ki idarə edən şəxs onun vasitəsi ilə optimal qərar qəbul edə bilsin.İnformasiya müxtəlif daşıyıcılarda müxtəlif formada mövcud ola bilər.İnformasiya cəmiyyətinin inkişafı nəticəsində informasiyanın həcmi artır və muasir hesablama texnologiyası və şəbəkələr əsasında yaranan avtomatlaşdırılmış sistemlərdə bu boyük həcmli informasiya qəbul olunur , saxlanılır ,emal olunur və ötürülür.

İnformasiya- təqdimat formasından aslı olmayaraq və fiziki daşıyıcıda saxlanılan bilik və praktiki həll üçün istifadə olunan obyektlər,prosesslər,hadisələr haqda məlumatlardır.

İnfromasiyanın xüsusiyyətləri:

- **Məlumatın dəyərliliyi-**informasiyanın informasiya alıcısına yararlılığı ilə müəyyən olunur yəni informasiya alıcısı bu informasiya vasitəsi ilə qarşıya qoyulmuş məqsədə çatır.
- **Adekvatlıq-** obyektin xüsusiyyətlərini adekvat şəkildə əks etdirmək üçün məlumatların düzgün seçilməsi və formalaşması.
- **İnformasiyanın dolğunluğu-**minimum həcmdə olan informasiyanın qərar qəbulu üçün kifayət olmasıdır.
- **İnformasiyanın əl çatanlığı-**informasiyanın əldə olunması və emalı xüsusi prosedurlar vasitəsi ilə həyata keçirlir.
- **İnformasiyanın aktuallığı-**informasiyanın cari anda dəyərliliyi ilə müəyyən olunur yəni cari anda informasiya problemi həll etməlidir.

Azərbaycan respublikasının konstitusiyasının 32-ci maddəsinin IV maddəsində qeyd edilir ki,<< Hər kəsin yazışma, telefon danışıqları, poçt, teleqraf və digər rabitə vasitələri ilə ötürülən məlumatın sirrini saxlamaq hüququna dövlət təminat verir. Bu hüquq qanunla nəzərdə tutulmuş qaydada cinayətin qarşısını almaqdan və ya cinayət işinin istintaqı zamanı həqiqəti üzə çıxarmaqdan ötrü məhdudlaşdırıla bilər>>beləliklə şəxsiyyətin özünə məxsus informasiyaya digər şəxslərin əl

çatanlığının məhdudlaşdırılması qanunla qorunur [1].Əgər informasiyaya əl çatanlıq məhdudlaşdırılıbsa bu informasiya məxfi informasiya adlanır.Məxfi informasiyaya - dövlət və kommersiya sirləri aiddir.

Dövlət sirri-dövlət üçün əhəmiyyətli məlumatlar daxildir.Dövlət sirrinə aid qanuna əsasən dövlət əhəmiyyətli məxfi məlumatlar üç gizlilik səviyyəsinə bölünür xüsusi əhəmiyyətli,gizli, çox gizli.Dövlət qurumlarında az əhəmiyyətli informasiyanın rəsmi istifadəsi üçün imza-möhürlərdən istifadə olunur.

Kommersiya sirləri-firma ,şirkət,hüquqi şəxsə aid olan informasiya aiddir.Kommersiya sirlərinin məxfilik dəyərini göstərmə üçün 3 yerə ayırırlar:çox məxfi ciddi kommersiya sirlərimuhasibatlıq,məxfi kommersiya sirləri, kommersiya sirləri.

- **Informasiyanın Etibarlığı**- informasiya dünyada baş verən hadisələri,obyektləri haqda məlumatları kifayət qədər dəqiqliklə informasiya alıcısına əks etdirməlidir.
- **İnformasiya Düzgünlüyü**-informasiyanın obyektin həqiqi vəziyyətinə yaxınlıq dərəcəsi ilə müəyyən olunur.
- **Məlumatın Dayanıqlığı**-informasiyanın dəqiqliyini itirmədən , məlumat mənbəsində olan dəyişikliyə cavab vermə qabiliyyəti nəzərdə tutulur. Təhrif olunmuş, həqiqəti əks etdirməyən informasiya informasiya alıcısına maddi və mənəvi zərər verə bilər.Məlumat qəsdən təhrif olunmuşdursa, o yalnış informasiya adlanır.
- **İnformasiyanın cari zamana uyğunluğu**-informasiyanın vaxtında təmin edilməsi yəni informasiya cari anda etibarlılığını və dəyərliliyini qorumalıdır.Misal gətirsək : hal hazırda mənə saat 16:00 üçün hava proqnozu önəmlidir lakin axşam artıq bu informasiya mənə lazimi deyil.Xüsusiyyətləri tənliklə ifadə olunur:

$$Ct=C_{0e}^{-2,3t/\tau}$$

burada C0,-yarandığı anda məlumatın dəyəri, t - məlumatın yaranma anından onun dəyərini təyin edən anadək olan vaxt, τ -məlumatın meydana çıxdığı andan əhəmiyyətini itirən anadək olan vaxtdır.

İnformasiya sistemləri-təşkilatın informasiya ehtiyyatlarını ödəyən və informasiya proseslərini həyata keçirən,informasiya, texniki ,linqvistik təminatdan və insandan ibarət kompleks sistemdir.

İnformasiya sisteminin məhsulu -informsiyadir bu elə informasiyadır ki, informasiya sistemləri və insan tərəfindən texniki proseslər nəticəsinsə xüsusiyyətləri dəyişdirilib.

Texniki proseslər-çıxışda lazimi informasiyanın alınması üçün giriş informasiyası üzərində yerinə yetirilən əməliyyatlardır.

İnformasiya sistemlərindəki məxfi məlumatlara insanlar, sənədlər, nəşrlər, texniki ehtiyyatlar , məlumatları emal edən texniki vasitələr, məhsullar, sənaye və sənaye tullantıları aiddir.

Bir çox hallarda, müharibə edən tərəflərin məlumat toplamaq üçün aktiv hərəkətləri şüurlu və düşünülmüş olur .Bunlara aiddir:

- Məxfi informasiyanın sahibi tərəfindən açıqlanması;
- Müxtəlif texniki kanallardan məlumatların sızması;
- Məxfi məlumatlara müxtəlif yollarla icazəsiz daxil olmaq

İnformasiyanın Avtomatlaşdırılmış Emalı sistemi dedikdə-aşağıdakı komponentlərin birləşməsindən ibarət təşkilati-texniki sistem başa düşülür:

- Məlumatın emalı və ötürülməsinin texniki vasitələrirabitə kanalları;
- Proqram təminatı- proqram və alqoritmlər vasitəsi ilə informasiya emalı;
- İnformasiya təminatı-buraya müxtəlif daşıyıcılarda olan massivlər,sənədlər, verilənlər bazaları və s. daxildir;
- Personal- sistemdən istifadə edənlərin informasiya təminatını ödəmək üçün texniki,proqram ,informasiya ilə yanaşı bu sistemlərdə personalda informasiyanın emalında iştirak edir.

Məlumat sızması - məxfi informasiyanın nəzarətsiz və qanunsuz şəkildə ona əl çatanlığı olan təşkilat,insanların əhatə dairəsindən kənara çıxmasıdır.

Məlumatın sızması məlumatın necə əldə edildiyindən asılı olmayaraq məxfi məlumatların qanunsuz gizli və ya açıq, qəsdən və ya təsadüfi əldə edilməsini əks etdirir.

Qorunan informasiyanın sızması bir neçə hallarda baş verə bilər:

- Bu tip məxfi informasiyanın əldə olunmasına marağı olan insan və ya təşkilat ola bilər ki əldə etmək üçün güc və maddi vasitə sərf edir;
- Elə bir hallar ola bilər ki, düşmən onu maraqlandıran informasiyanı əldə etmək üçün etibar etdiyi şəxslərdən,mənbələrdən istifadə edə bilər.

Məlumat sızıntısının səbəbləri və şərtləri arasında fərqliliklər olduğu kimi oxşarlıqlarda mövcuddur.

Səbəb bir qayda olaraq hərbi və dövlət sirrinin qorunması qaydalarının təkmilləşdirilməməsi, habelə bu qaydaların pozulması, məxfi məlumatları özündə saxlayan sənədlərin məhsul nümunələrinin və digər materialların işlənməsi qaydalarından yayınma ilə əlaqələndirilir.

Məlumatların sızılması şərtlərinə müxtəlif hallar və şərtlər daxildir hansı ki bir başa istehsal,elmi,rəsmi,hesabat məlumatları hazırlanan proselərdə inkişaf edir.

Məsələn bu kimi hallara və şərtlərə aşağıdakılar aid ola bilər:

- Təşkilatda fəaliyyət göstərən işçilər tərəfindən dövlət və hərbi sirlərin qorunması qaydalarının tam anlaşılmaması və bu tip məlumatların daimi izlənməli zərurililiyin dərk edilməməsi;
- məxfi məlumatları emal etmək üçün sertifikatlaşdırılmamış texniki vasitələrdən istifadə;
- informasiyanın qorunmasının hüquqi, təşkilati və mühəndis-texniki tədbirləri qaydalarına əməl olunmasına zəif nəzarət;
- hərbi və dövlət sirri saxlayan məxfi məlumatların rabitə kanallarında tutuması.

Məxfi məlumatların sızmasının və təhrif olunmuş məlumatın alınmasının başlıca səbəblərindən biri təşkilat rəhbərlərinin və işçilərin diqqətsizliyi və məsuliyyətsizliyi səbəbindən olur.

Bundan əlavə məlumat sızmasının səbəblərinə:

- təbii fəlakətlər fırtına sel , qasırğa, zəlzələ,;
- mənfi xarici mühit göy gurultusu, yağış, qar;
- fəlakətlər yanğın, partlayışlar ;
- nasazlıqlar, texniki vasitələrin və avadanlıqların qəzaları və işinin dayandırlması .

İnformasiya Təhlükəsizliyi söz birləşməsi müxtəlif kontekstdə müxtəlif məna kəsb edə bilər.Əsasən fərdin, cəmiyyətin və dövlətin balanslaşdırılmış maraqlarının məcmusundan ibarət informasiya fəzasında , milli maraqların qorunmasını ifadə edir .

İnformasiya Təhlükəsizliyi- bir tərəfdən tədqiq olunan avtomatlaşdırılmış sistemin daxili və xarici təsirlərdən qorumaq , digər tərəfdən avtomatlaşdırımış sistemin mövcudluğu digər sistemlər üçün zərər yetirməməsinin təşkilinə yönəlir.

Rusiya Federasiyasının Beynəlxalq məlumat mübadiləsində iştirak haqqında qanununda informasiya təhlükəsizliyi - cəmiyyətin informasiya mühitinin təhlükəsizliyinə oxşar yəni vətəndaşların, təşkilatların, dövlətin maraqları üçün lazımı olan informasiyanın formalaşmasını, istifadəsini və inkişafını təmin edir.

İnformasiya təhlükəsizliyi dedikdə, informasiya münasibətləri subyektlərinin məlumat sahibləri ,istifadəçiləri ,sistemi dəstəkləyən infrastruktur da daxil olmaqla, yolverilməz ziyan vura biləcək təbii və ya süni xarakterli təsadüfi və ya qəsdən təsirlərdən mühafizəsi başa düşülür.Təhlükə və təhlükəsizlik arasında əlaqə aşağıdakı sxem 1-də göstərilib.

Təşkilatda informasiya təhlükəsizliyi təmin etmək üçün ilk öncə şirkətdə informasiya təhlükəsizliyi mədəniyyəti formalaşmalıdır.İnformasiya Təhlükəsizliyi mədəniyyəti ilk öncə şirkətin işcilərinin bir-birinə davranışı,işçilərin avadanlıqlara

davranışı ilə müəyyən olunur. Mədəniyyət anlayışları təşkilatın müxtəlif seqmentlərinin səmərəli işləməsinə kömək edə bilər . İşçilərin təhlükəsizlik və düşündükləri düşüncə tərzi və gördükləri işlər təşkilatlarda informasiya təhlükəsizliyinə çox təsir edə bilər. Roer & Petrik təşkilatlarda informasiya təhlükəsizliyi mədəniyyətinin yeddi əsas ölçüsünü müəyyənləşdirir:[21]

1 Münasibətlər-Şirkətdə olan işçilərin təşkilatda olan informasiyanın qorunmasına dair hissləri və emossiyaları.

2 Davranışlar- şirkətdə işçilərin dolayı və ya birbaşa yolla informasiya təhlükəsizliyini pozacaq davranışları etmək üçün risk alma dərəcəsi.

3 Dərketmə-İşçilərin informasiya təhlükəsizliyinə dair bilik və təcrübələrinə əsaslanır.Yəni işçi əvəllər işləyibmi,təlükəsizlik təlimatları ilə tanışdırmı.

4 Ünsiyyət- İşçilərin bir-biri ilə ünsiyyət qurma yolları, mənlik hissi, təhlükəsizlik məsələlərinə dəstək və hadisələrin hesabatlandırılması kimi fəaliyyətlər aiddir.

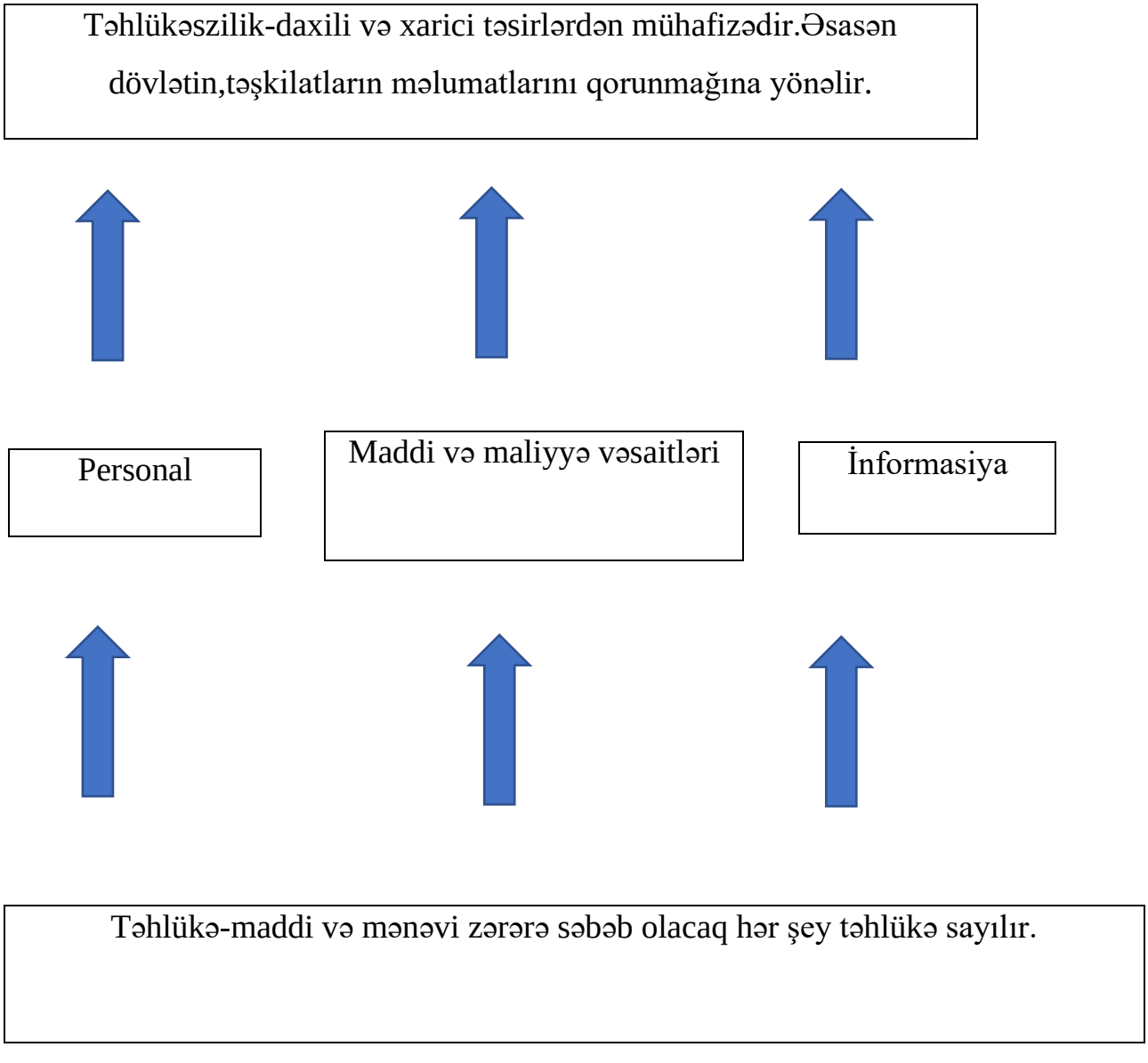
5 Uyğunluq- Təşkilati təhlükəsizlik siyasətinə riayət etmək, bu cür siyasətlərin mövcudluğundan xəbərdar olmaq və bu siyasətlərin mahiyyətininə hər zaman ciddi yanaşmaq vacibdir .

6 Normalar- Təhlükəsizliklə əlaqəli təşkilati davranış və işçilər və həmyaşıdları tərəfindən normal və ya zərər verəbiləcək təcrübələr qeyd olunmalıdır ki yeni gələn işçilər onları təkrar etməsin.

7 Məsuliyyətlər -Təşkilatda çalışan işçilər öz vəzifə və məsuliyyətlərini dərk etməlidirlər və onlar anlamalıdırlar ki informasiya təhlükəsizliyinin vacib elementlərinə aiddirlər.

Lakin tədqiqatlar göstərir ki,işçilər informasiya təhlükəsizliyinin bir hissəsi kimi görmürlər özlərini və informasiya təhlükəsizliyini pozacaq fəaliyyətlər edirlər.Belə hərəkətlərə misal olaraq göstərə bilərik :bildiyimiz kimi şirkətdə rəqiblər haqda informasiyaya çox ehtiyyac duyulur.Başqa rəqib şirkət ,şirkətdə olan işçini satın

ala bilər yəni pul müqavilində məlumat ala bilər və həmin işçi pul müqavilində informasiya sızdıra bilər.Düzdür bunun bir çox səbəbləri ola bilər,işçinin yaşayış səviyyəsi aşağı ola bilər və pula tələbatı ola bilər ,lakin heç bir şey bu hərəkətə bəraət qazandıra bilməz.



Sxem1 [3]

İnformasiya qorunması - informasiya təhlükəsizliyinin təmin edilməsinə yönəlmiş tədbirlər kompleksidir.

İnformasiya təhlükəsizliyi problemlərinə metodoloji cəhətdən düzgün yanaşma

İnformasiya sistemləri İS istifadəçilərinin həmin sistemdən hansı maraqlar üçün istifadə edəcəyini müəyyənləşdirməkdən başlayır.İnformasiya Təhlükəsizliyinə yönələn təhdidlər-informasiya texnologiyalarının istifadəsinə zidd olan tərəfi sayılır.

Bu mövqedən yanaşaraq 2 mühüm nəticə çıxarmaq olar:

1. Müxtəlif təşkilatlar üçün informasiya təhlükəsizliyinə dair atılan addımlar müxtəlif ola bilər.Misal olaraq biz dövlət müəssələri ilə elmi müəssələrin müqayisəsinə baxsaq kifayət eder. Dövlət müəssələrində əsas prinsip budur ki ,onlar sistemin dayanmasının onun hansısa elementinin zəif işləməsi nəticəsinsə məxfi məlumatın sızmasında üstün tuturlar,elmi müəssələrdə isə məxfi məlumatımız yoxdur sistemin dayanmadan işləməyini üstün tuturlar.
2. İnformasiya təhlükəsizliyi yalnız məlumatların icazəsiz əldə edilməsindən mühafizə etməklə məhdudlaşmır, əsaslı şəkildə daha geniş bir anlayışdır. İnformasiya münasibətləri subyektiinformasiya sahibi ,göndərən,informasiyanı qəbul edən şəxlər nəzərdə tutulur yalnız icazəsiz girişdən deyil, həm də işdə fasiləyə səbəb olan sistemin pozulmasından zərər çəkə bilər bu da şirkət rəhbərlərinə maddi və mənəvi ziyan vurur. Bundan başqa, bir çox açıq təşkilatlar üçün məs. təlim, təhsil məlumatların icazəsiz əldə edilməsindən qorunması əhəmiyyət baxımından birinci yerdə dayanmır.

İnformasiya təhlükəsizliyi yalnız EHM-dən aslı deyil həmçinin ,informasiya sisteminin dəstəkləyici infrastrukturunu təşkil edən xidməti personal, elektrik, su və istilik təchizatı sistemləri, kondisionerlər, rabitə vasitələrindən aslıdır. Bu infrastukturun öz vahid dəyəri var lakin bizi maraqlandıran informasiya sistemində təyin olunmuş funksiyanı yerinə yetirərkən sistemə nə kimi təsir edəcəyidir.

Aydındır ki, bütün növ zərərlərdən sığortalanmaq mümkün deyildir,mühafizə vasitələrin və tədbirlərin dəyəri gözlənilən zərərin miqdarından çox olmadıqda, iqtisadi cəhətdən nəticə əldə etmək mümkün olmur.Bu o deməkdir bir çox təhlükələrə qarşı dayanıqlı olmalıdır yəni barışmalıdır,yalnız barışması mümkün olmayan təhlükələrdən qorunmalıdır. Belə yol verilməz zərərlərə insan sağlamlığına və ya ətraf mühitə vurulan zərərlərdir misal olaraq Çernobl-da baş verən hadisə nəticəsində ətraf mühitə və insan sağlamlığına zərər dəymiş habelə dövlət külli miqdarda pul itirmişdir, informasiyanı qorumağın məqsədidə məqbul dəyərlərə zərər vurma dərəcəsini azaltmaqdır.

1.2 İnformasiya Təhlükəsziliyinin əsas hissələri

İnformasiya təhlükəsizliyi çox yönlü, hətta demək olar ki çoxölçülü fəaliyyət sahəsidir, uğur yalnız sistematik, inteqrasiya olunmuş yanaşma ilə mümkündur.

Subyektlərin İnformasiya sistemlərinin istifadəsi ilə əlaqəli maraq dairəsini aşağıdakı kateqoriyalara bölmək olar: informasiya mənbələrinin **əlçatanlğının, tamlığının və məxfiliyinin təmini** və dəstəkləyən infrastrukturun olması .

Əlçatanlıq- tələb olunan informasiyanın lazimi anda çatdırılması xidmətidir.

Tamlıq- İnformasiyanın kənar şəxslərin təhrifindən qorumaq və onun etibarlı şəkildə tam formada məğzinin çatdırlması xidmətidir.

Məxfilikkonfidensiallıq- məlumatın kənar şəxslərin əldə olunmasından qorunmasıdır.

İnformasiya Sistemləri İS-informasiya xidmətləri göstərmək üçün yaradılır. Bu və ya digər səbəbdən istifadəçilərə bu xidmətləri göstərmək mümkün olmadıqda, bütün informasiya münasibətləri subyektləri zərər görə bilər.

Əl çatanlıq informasiya təhlükəsizliyinin ən vacib elementlərindəndir. Əlçatanlığın aparıcı rolu müxtəlif idarəetmə sistemlərində - istehsal, nəqliyyat və s meydana gəlir. Çox sayda insanın istifadə etdiyi məlumat xidmətlərinin uzun müddət

əl çatan olmaması dəmir yolu və aviabilet satmaq, bank xidmətləri və s. nisbətən az dramatik lakin maddi və mənəvi zərərli nəticələri ola bilər.

Tamlığı 2 yere ayırmaq olar : statik- informasiya sistemlərinin dəyişməzliyi halında və dinamik -mürəkkəb tranzaksiyalar yerinə yetirən sitemlər. Dinamik bütövlük nəzarətindən, maliyyə mesajlarının axını təhlil edilərkən istifadə olunur xüsusilə fərdi mesajların oğurlanması,təhrif olunması və ya təkrarlanmasının aşkarlanması üçün istifadə olunur.Tamlıq informasiya təhlükəsizliyinin ən vacib aspektlərindəndir.Məsələn dərmanlar reseptlərinin ,tibbi prosedurların pozulması ölümlə nəticələ bilər.Rəsmi məlumatların: istər qanuni mətnin istər dövlət təşkilatlarının web-səhifələrində olan mətnlərin təhrif olunması xoşa gəlməzdir.

Məxfilik-ölkəmizdə informasiya təhlükəsizliyinin ən geniş yayılmış formasıdır.Təəssüf ki, müasir informasiya sistemlərinin məxfiliyini təmin etmək üçün atılan tədbirlərin praktik icrası bir çox dünya ölkələrində ciddi çətinliklərlə üzləşir. İlkin olaraq məlumat sızmasının texniki kanalları haqqında məlumatlar bağlanır ki, əksər istifadəçilər potensial riskləri anlamaq imkanından məhrum olurlar. İkincisi, çoxsaylı kriptovalyuta maneələri və texniki problemlər məxfiliyin təmin edilməsinin qarşısında durur ,bir çox təşkilatın məxfi problemləri də var yuxarıda göstərilən təhsil müəssisələrində belə, işçilər üçün əmək haqqı məlumatlarını açıqlamamağa çalışırlar və s.

1.3 İnformasiya Təhlükəsizliyinin əhəmiyyəti və mürəkkəbliyi

Hansı səviyyədə milli, sənaye, korporativ və ya fərdi baxmağımızdan aslı olmayaraq ,informasiya təhlükəsizliyi inteqrasiya olunmuş təhlükəsizliyin ən vacib aspektlərindən biridir.

Fikrimizi aydınlaşdırmaq üçün nümunələrə nəzər salaq.

- Rusiya Federasiyasının İnformasiya Təhlükəsizliyi Doktrinasında, məlumat mənbələrini icazəsiz daxil olmaqdan qorumaq informasiya sistemləri və telekommunikasiya sistemlərində məlumatların təhlükəsizliyini təmin etmək Rusiya

Federasiyasının informasiya sahəsindəki milli maraqlarının vacib komponentləri olaraq təyin olunur.

- ABŞ Prezidenti B. Klintonun 15 iyul 1996-cı il, № 13010 sərəncamı ilə infrastrukturu həm fiziki hücumlardan, həm də informasiya silahından istifadə edilən hücumlardan qorumaq üçün bir komissiya yaradıldı.1997-ci il oktyabrın əvvəlində yuxarıda adı çəkilən komissiyanın rəhbəri Robert Marsh, hazırda nə hökumətin, nə də özəl sektorun rabitə şəbəkələrini və enerji təchizatı şəbəkələrini sıradan çıxara biləcək kompüter hücumlarından qorunma vasitələrinə sahib olmadığını bildirdi.
- Amerikan raket kreyseri Yorktown, Windows NT 4.0 platformasında işləyən proqram təminatında baş verən çoxsaylı problemlər üzündən limana dönmək məcburiyyətində qaldı. Bu, kommersiya proqramlarından maksimum istifadə ABŞ Hərbi Dəniz Qüvvələrinin hərbi texnikasının qiymətinin azalmasına səbəb oldu .
- Rusiya Daxili İşlər Nazirliyinin İqtisadi Cinayətlər İdarəsi rəhbərinin müavinin verdiyi məlumata görə 1994-cü ildən 1996-cı ilə qədər Rusiya hakerləri Rusiya Mərkəzi Bankının kompüter şəbəkəsinə sızmaq üçün təxminən 500 cəhd edib. 1995-ci ildə isə 250 milyard rubl oğurlanıb.
- Internet Week jurnalının 23 mart 1998-ci il tarixli məlumatına görə, ən böyük şirkətlərin təhlükəsizlik vasitələrinə xərclədiyi vəsaitlərin qiymətinin artmasına baxmayaraq, kompüter müdaxilələri nəticəsində yaranan itkiləri artmaqda davam edir.
- İnformasiya Təhlükəsizliyi İnstitutu araşdırmasına görə 1997-ci ildə kompüter cinayətlərinə vurulan zərər 137 milyon dollara çatdı ki, bu da 1996-cı ildən 35% çoxdur.Hər bir kompüter cinayəti nəticəsində təxminən 300 min dollar ziyan vurur.
- 1996-cı ilin iyul ayının ortalarında General Motors Corporation, 1996 və 1997-ci illərdəki 292,860 ədəd Pontiak, Oldsmobile və Buick modeli avtomobillərini geri çağırdı, çünki mühərrik proqramında olan bir səhv yanğına səbəb ola bilərdi.
- 2001-ci ilin fevral ayında Commerce One şirkətinin işdən ayrılmış iki işçisi admınistrator şifrəsindən istifadə edərək xarici bir müştəri üçün böyük bir neçə milyon dollar bir layihə təşkil edən serverdəki faylları sildi. Xoşbəxtlikdən, layihənin bir ehtiyat nüsxəsi var idi, buna görə də itkilər istintaq xərcləri və gələcəkdə oxşar

hadisələrin baş verməməsi üçün tədbirlərə ayrılan xərclərlə məhdudlaşdı. 2002-ci ilin avqustunda cinayətkarlar məhkəməyə çıxdılar.

• Miçiqan Universitetində qız tələbə 19 min dollar miqdarında təqaüdünü itirdi, səsbəb isə otaq yoldaşının onların ortaq şəbəkəyə giriş sistemindən istifadə etməsi və onun adından təqaüd ləğv olunması üçün e-poçtu göndərilməsi oldu.

Buna bənzər çox nümunə çəkə bilərik.İnformasiya təhlükəsizliyi probləmlərini analiz edərkən unutmaq lazım deyil ki, hər gün yüksək templə inkişaf edən informasiya texnologiyasının təkibində olur. Burada əhəmiyyət kəsb edən bu günə qədər qəbul edilən fərdi qərarlar qanunlar, təlim kursları, proqram təminatı və aparat məhsulları deyil, texnoloji tərəqqi sürətində rəqabətə imkan verən yeni həllərin yaradılması mexanizmləridir.

Təəssüf ki,müasir proqramlaşdırma texnologiyaları tam təhlükəsiz,səhvsiz proqramlar yaratmır və buda informasiya təhlükəsizliyinin vasitələrinin inkişafını ləngidir.Etibarlı sistemi etibarlı komponentlərdən istifadə etməklə qurmaq mümkündür.Prinsip olaraq bu mümkündür lakin arxitektura prinsiplərinə riayət olunmasını və İS-nin bütün həyat dövrü boyunca təhlükəsizlik vəziyyətinin monitorinqini tələb edir.

Bir neçə ilə nəzər salaq.1999-cu ilin martında sıraca 4 cü olan illik hesabat verildi ,hesabat kompüter təhlükəsizliyi və kompüter cinayətkarlığı -nın problemləri və tendensiyaları mövzusunu əhatə edirdi. Hesabatda kompüter cinayətləri ilə əlaqədar hüquq-mühafizə orqanlarına edilən müraciətlərin sayında kəskin artım qeyd edilmişdir sorğuda iştirak edənlərin 33% -i, rəyi soruşulanların 30% -i məlumat sistemlərinin xarici təcavüzkarlar tərəfindən sındırıldığını bildirdi, sorğuda iştirak edənlərin 57% -i İnternet vasitəsilə hücuma məruz qalıb, 55%-i öz işçiləri tərəfindən . Maraqlıdır ki, son 12 ayda Web-serverləriniz və e-ticarət sistemləriniz pozulubmu? sualına respondentlərin 33% -i bilmirəm deyə cavab verib.

2002-ci ilin aprelində oxşar bir hesabatda saylar dəyişdi, lakin tendensiya eyni olaraq qaldı: respondentlərin 90% -i əsasən iri şirkətlər və dövlət qurumları tərəfindən

son 12 ayda öz təşkilatlarında informasiya təhlükəsizliyi pozuntularının baş verdiyini bildirdi; 80% bu pozuntulardan maliyyə itkisi olduğunu bildirdi; 44% zərərləri kəmiyyətcə qiymətləndirməyi bacardı, ümumi məbləğ 455 milyon dollardan çox oldu.Ən çox zərər oğurluq və saxtakarlıq nəticəsində olub təxminən 170 milyondan çox.

Oxşar göstəricilər İyul 1999 tarixində yayımlanan İnternational Week anketində yer almışdır.Sorğuda iştirak edənlərdən yalnız 22% informasiya təhlükəsizliyinin pozulmaması barədə məlumat vermişdi.Virusların yayılması nəticəsində xarici hücumların sayında kəskin artım olub.

Hücumların sayının artması hələ də böyük narahatçılıq doğurmur.Narahatçılıq doğuran səbəb proqram təminatında zəif yerlərin aşkar olunması və yeni hücüm növlərinin əmələ gəlməsi.

Beləliklə,ABŞ-ın Milli İnfrastruktur Qoruma Mərkəzinin 21 iyul 1999-cu il tarixli məlumat məktubunda bildirilmişdir ki, 3 iyul-16 iyul 1999-cu il tarixləri arasında proqram təmınatında doqquz problemi aşkar edilmişdir və istifadə olunma riski orta və ya yüksək olaraq qiymətləndirilir. Zərər çəkmiş əməliyyat sistemləri arasında Unix, Windows, MacOS-un demək olar ki, bütün növləri var, buna görə bu əməliyyat sistemlərindən istifadə edən heç kim rahat hiss edə bilməz, çünki yeni səhvlər təcavüzkarlar tərəfindən dərhal istifadə olunmağa başlayır.

Belə şəraitdə İnformasiya Təhlükəsizliyi sistemləri həm xarici həm daxili hücumlara qarşı dayanıqlı olmaq üçün əlaqələndirilmiş şəkildə avtomatlaşdırılmalıdır.Bəzən hücümlar bir saniyə də baş verə bilər ,sistemin zəifliklərinin tapılması çox uzun saatlarla davam edə bilər buna görədə gizli fəaliyyətin aşkar olunması çətin olur .Təcavüzkarların məqsədi informasiya təhlükəsizliyinin bütün komponentlərinin – bütövlüyün, əlçatanlığın və ya məxfiliyin pozulmasına yönəlir.

İnformasiya sistemlərinin təhlükəsizliyinin təmininə dair yerinə yetirilən tədbirlərə 3 mərhələdə baxılır.

Qarşıya qoyulmuş tələblərin inkişafı olan birinci mərhələyə aşağıdakılar daxildir:

- İnformasiya Sisteminin tərkibinin müəyyən edilməsi;
- İnformasiya sisteminin zəif hissələrinin təhlili;
- Təhdidlərin qiymətləndirilməsisistem bu təhdidlərə qarşı dayanıqlılığının ölçülməsi;
- Risklərin analizi problemə səbəb olacaq bütün mümkün hadisələrin proqnozlaşdırılması.

İkinci mərhələ mühafizə metodlarının müəyyənləşdirilməsi , aşağıdakı suallara cavabları əhatə edir:

- Hansı təhdidlər aradan qaldırılmalıdır və sistem nə dərəcə qorunur ?;
- Sistemin hansı ehtiyyatları nə dərəcədə qorunur?;
- Mühafizə hansı vasitələrdən istifadə olunaraq həyata keçirilməlidir?;
- Potensial tədidləri nəzərə almaqla mühafizə xərclərinin ümumi dəyəri nə qədər olmalıdır?

Üçüncü mərhələ mühafizə mexanizmi şəklində həyata **keçirilən funsiyaların, prosedurların, vasitələrin** müəyyən olunması.

İnformasiya təhlükəsizliyi sahəsindəki işlərin təhlili göstərir ki,aparıcı ölkələr əsasını aşağıdakılar təşkil edən yaxşı qurulmuş infrastruktura malikdir:

- Sənayə bazarında istehsal olunmuş yüksək inkişaf etmiş mühafizə vasitələrinin məcmusu;
- İnformasiya təhlükəsizliyi barədə kifayət qədər dəqiq ,tədqiq olunmuş konseptual sistem;
- Praktiki təcrübə.

Buna baxmayaraq təcavüzkarlar tərəfindən informasiyaya yönələn hədələr nəinki azalmır,hətta sabit inkişaf tendensiyasına malikdir.

Təcrübə göstərir ki,bu tip hədələrdən qorunmaq üçün informasiya sistemlərində mühafizə sistemi strukturlaşdırlmış və sistemləşdirilmiş şəkildə qurulmalıdır.

Dövlət Komissiyasının rəhbər sənədləri əsasında Avtomatlaşdırılmış emal sistemini qorumaq üçün aşağıdakı müddəalar tərtib edilə bilər.

1. Avtomatlaşdırılmış sistemlərdə informasiya mühafizəsi mövcud qanunların, standartların və normativ-metodiki sənədlərin tələblərinin müddəalarına əsaslanır;

2. Avtomatlaşdırılmış sistemlərdə informasiya mühafizəsi təşkilati-texniki,proqram tədbirlər kompleksinə əsaslanır;

3. Avtomatlaşdırılmış sistemlərdə informasiya mühafizəsi məlumatların emalının bütün texnoloji mərhələlərində və bütün iş rejimlərində, o cümlədən təmir və müntəzəm iş müddətində təmin edilməlidir;

4. Proqram aparat mühafizəsi sistemin funksional imkanlarına məsələn sürətinə mənfi təsir etməməlidir;

5. İnformasiya sisteminin mühafizəsinə yönələn işlərin ayrılmaz hissəsi mühafizə vasitələrinin effektivliyinin ölçülməsidir;

6. AES mühafizəsi qoruyucu vasitələrin səmərəliliyinin monitorinqini əhatə etməlidir.Bu monitorinq dovri və ya lazımi gələrsə Avtomatlaşdırılmış sistemin istifadəçisi və ya tənzimləyici orqan tərəfindən başladıla bilər.

Nəzərdən keçirilən yanaşmalar aşağıdakı əsas prinsiplərin təmin edilməsi ilə həyata keçirilə bilər:

Mürəkkəblik prinsipi

Kompüter təhlükəsizliyi mütəxəssisləri informasiyanın mühafizəsi üçün geniş tədbirlər, metodlar və vasitələrə malikdir.Ayrı-ayrı zəif cəhətləri olmayan mühafizə vasitələri əlaqələndirilmiş vahid mürəkkəb sistem əmələ gətirir və bu sistem bütün giriş kanallrını təhdidlərdən qoruyur.

Qorumanın kəsilməzliyi prinsipi

Məlumatın qorunması bir dəfəlik proses yox davamlı hədəflənmiş prosesdir və avtomatlaşdırılmış informasiya sisteminin AİS bütün həyat tsiklində mövcud olmalıdır.Sistemin mühafizəsi tamamı ilə mühafizə olunmuş sistemə praralel aparılmalıdır.Mühafizəni sistemin arxitekturasını qurarkən nəzərə alsaq daha dayanıqlı mühafizə olunmuş sistem əldə edərik.Mühafizə vasitələrinin funksiyalarının səmərəli yerinə yetirilməsi üçün daimi təşkilati dəstək tələb edir.Mühafizə qurğuların işindəki fasilələr təcavüzkarlara öz zərər yetirən əməllərini yerinə yetirmək üçün şərait yaradır.

Mühfizənin çevikliyi

Bəzən qeyri müəyyən şərtlər daxilində mühafizə sistemi yaratmalı oluruq.İstismarın ilk dövrlərində görülən tədbirlər və qurulan mühafizə vasitələri qorumanı qeyri-kafi yerinə yetirə bilər.Təhlükəsizlik səviyyəsini dəyişilməsini təmin etmək üçün sistem çevik qurulmalıdır.Bu xüsusiyyət əsasən normal işləyən sistemə əlavə mühafizə vasitələri quraşdırmaq lazim gələndə çox vacib olur.

Alqoritmlərin və mühafizə mexanizmlərinin açıqlığı

Alqoritmlərin və mühafizə mexanizmlərinin açıqlığı prinsipinin mahiyyəti ondan ibarətdir ki, mühafizə yalnız təşkilatın strukturunun və alt sistemlərinin alqoritmlərinin işlənməsinin məxfiliyi ilə təmin edilməməlidir.Mühafizə sisteminin alqoritmini bilmək onun işini pozmağa imkan verməməlidir.Lakin bu dəmək deyilki mühafizə sistemi haqda məlumat hamıya açıq olmalıdır təbii ki,sistemin parametrləri təhlükələrdən qorunmaq üçün gizli saxlanılmalıdır.

Mühafizə vasitələrindən istifadənin sadəliyi prinsipi

Mühafizə mexanizmləri sadə və aydın olmalıdır belə ki istifadəçilərdən əlavə dil biliyi,əlavə əmək xərcləri ,başa düşülməyən əməliyyatların icrası tələb olunmamalıdırbir neçə parol və adın daxil edilməsi və s.

İnformasiyanın mühafizəsi anlayışının inkişafını aşağıdakı cədvəl 1-də mərhələri göstərilmişdir:

İnkişaf mərhələləri	Xüsusiyyətləri
1960-1970-ci illər	Əsasən texniki və proqram təminatlarından ibarət mexanizmlər vasitəsi ilə məlumatların təhlükəsizliyini təmin etmək cəhdləri.
1970-1976 -cı illər	Məlumatların qorumasının formal mexanizmlərinin inkişafı,informasiya təhlükəsizliyinə sistemli yanaşma,verilənlərin qorunmasının əsas nüvəsinin müəyyən olunması.
1976-1990-cı illər	İkinci mərhələnin mexanizmlərinin daha da inkişafı. Davamlı bir proses kimi məlumat təhlükəsizliyini təmin etmək barədə bir fikir formalaşdırılması. Məlumatların qorunması üçün standartların işlənməsi. Məlumatların qorunması vasitələrinin aparat tətbiqi tendensiyasının gücləndirilməsi
1990-cı ildən bəri	Üçüncü mərhələ mexanizmlərinin daha da inkişafı. İnformasiya Şəbəkələrində verilənlərin təhlükəsizliyi nəzəriyyəsinin əsaslarının formalaşdırılması və şəbəkədə məlumatların qorunmasını təmin etmək üçün modellərin, metodların və alqoritmlərin işlənməsi

Cədvəl 2

II FƏSİL Etibarlı Şəbəkələrin qurulmasının metodologiyası

2.1 İnformasiya Sistemlərinin idarə edilməsi məsələləri

İdarəetməni komponentlərin və təhlükəsizlik vasitələrinin normal işini təmin edən infraktrusktur servislərinə aid etmək olar. Müassir sistemlərin çətinliyi ondan ibarətdir ki, düzgün qurulmuş idarəetmə sistemi olmadiqda onlar yavaş-yavaş effektivlik azaldığı üçün siradan çıxır və təhlükəsizliyi azalır. İdarəetməyə başqa bir baxış bucağıda mümkündür – informasiya servislərinin və təhlükəsizlik servislərinin inteqrasiyası kimi baxmaq olar hansı ki onların normal və bir-biri ilə uyğunlaşan funksionallığını təmin edir. Bu funksionallıq informasiya sisteminin adminin nəzarəti altında həyata keçirilir

X.700 standartına uyğun idarəetmə aşağıdakı bölmələrə bölünür:

1. komponentlərin monitorinqi;
2. nəzarət yəni nəzarət tədbirlərinin verilməsi və həyata keçirilməsi;
3. sistem komponentlərinin əlaqələndirilməsi.

İSinformasiya sistemi-nin idarəetməsi - seçilmiş insanların hərəkətləridir İS idarəetməsi , İS-nin vəziyyətinin qorunmasını təmin edir və funksional məqsədi yerinə yetirməyə imkan verir.

İdarəetmə sistemləri bunları etməyi bacarmalıdır;

- idarəçiləri planlaşdırmağı, təşkil etməyi, informasiya xidmətlərinin istifadəsinə nəzarət etmək və nəzərdən keçirmək;
- Dəyişən tələblərə cavab vermək imkanı;

- informasiya xidmətlərinin proqnozlaşdırılan davranışını təmin etmək;
- İnformasiyanin müdafiəsini təmin etmək;

Basqa sözle desək idarəetmə mütləq böyük funksional,məqsədyönlü,nəticə verə bilən olmalı, bundan savayı çevik və informasiya baxımından təhlükəsiz olmalıdır.

X.700 beş funksional idarəetmə sahəsinə malikdir :

- Konfiqurasiyanın idarə edilməsi parametrləri normal qəbul etmək , komponentlərin işləməsi,başlanması və dayandırılması, sistemin hazırkı vəziyyəti haqqında məlumat toplanılması, funksionallıq dövründəki əhəmiyyətli dəyişikliklər barədə bildirişlər alınması, sistem konfiqurasiyasının dəyişdirdirilməsi;
- uğursuzluqların idarə edilməsi uğursuzluqların aşkarlanması, sistemin bərpası;
- mühasibat uçotu məlumatlarının idarə edilməsi mənbələrdən istifadə haqqı;
- təhlükəsizliyin idarə edilməsi təhlükəsizlik xidmətləri və mexanizmlərini yaratmaq, silmək və dəyişdirmək, təhlükəsizlik məlumatlarını yaymaq və hadisələrə reaksiya verməklə təhlükəsizlik siyasətini həyata keçirmək;
- performansın idarə edilməsi statistik məlumatların toplanması və təhlili, standart və qeyri-standart şəraitdə sistemin fəaliyyətinin müəyyən edilməsi, sistemin iş rejiminin dəyişdirilməsi.

Menecer və agentlərin qarşılıqlı iyerarxiyası bir neçə səviyyədə ola bilər. Aralıq səviyyələrin elementləri eyni zamanda ikili rol oynayır: ana elementlərinə münasibətdə onlar agent, aşağı hissəyə münasibətdə isə menecerlərdir. Çoxsəviyyəli menecer / agent memarlığı - paylanmış, geniş sistemlərin idarəedilməsinin açarıdır.

idarəetmə konsolu hər hansı bir memarlıq səviyyəsinin məcburi elementidir. İdarəetmə sistemlərinin imkanlarını öyrənmək baxımından aşağıdakı aspektlərə bölünmə nəzərə alınmalıdır:

- məlumatlı atributları, əməliyyatları və obyektlərin bildirişləri;
- funksional nəzarət tədbirləri və onlara lazım olan məlumatlar;

- rabitə idarəetmə məlumatlarının mübadiləsi;
- təşkilati fərqli idarəetmə sahələrinə bölünmə.

Konseptual baxımdan vacib olanlar arasında proaktiv anlayışı aid edilə bilər, yəni. cari məlumatlara və əvvəllər toplanmış məlumatlara əsaslanaraq sistemin davranışını proqnozlaşdırmağa imkan verir. Məsələn, disk bir nece defe taxildiqdan sonra proqram üzre neytrallaşdırılmış olan oxunma/yazma sehvleri haqqinda siqnalin verilmesi. Daha mürəkkəb bir vəziyyətdə, iş yükünün və istifadəçi hərəkətlərinin müəyyən bir hissəsi sistemdə kəskin bir yavaşlamaya sebeb ola bilər; bəzi vəzifələrin prioritetlərini aşağı salmaq və yaxınlaşan böhran barədə idarəçini xəbərdar etmək müvafiq nəzarət tədbiri ola bilər.

2.2 Protokollaşdırma və yoxlama

Şübhəli fəaliyyət dedikdə istifadəçi və ya bir informasiya sisteminin komponentinin zərərli əvvəlcədən müəyyən edilmiş təhlükəsizlik prinsipinə uyğun və ya atipik qəbul edilmiş meyarlara əsasən davranışı başa düşülür.

Protokollaşdırma bir məlumat sistemində baş verən hadisələr haqqında məlumat toplamaq demekdir. Hər bir xidmətin öz mümkün hadisələri var , lakin hər halda onları xarici digər xidmətlərin hərəkətlərindən irəli gələn ,daxili xidmətin hərəkətlərindən irəli gələn və müştəri istifadəçilər və idarəçilərin hərəkətlərindən irəli gələn bölmək olar.

Audit dərhal real vaxtda və ya dövri olaraq həyata keçirilən yığılan məlumatların təhlilidir. Müəyyən edilmiş fövqəladə hallara avtomatik reaksiya verən əməliyyat auditi **aktiv** adlanır

Protokollaşdırma və auditin həyata keçirilməsi aşağıdakı vəzifələri həll edir:

- İstifadəçilər və idarəçilərin hesabatlarının təmin edilməsi;
- Hadisələrin ardıcıllığının yenidən qurulması bacarığını təmin etmək;
- İnformasiya təhlükəsizliyini pozma cəhdlərinin aşkar edilməsi;

- Problemləri müəyyənləşdirmək və təhlil etmək üçün məlumatların verilməsi.

Bir hadisə qeyd edərkən ən azı aşağıdakı məlumatları qeyd etməyiniz tövsiyə olunur:

- tədbirin keçirilmə tarixi və vaxtı;
- hərəkətə başlayan istifadəçinin bənzərsiz identifikatoru;
- hadisə növü;
- hərəkətin nəticəsi uğur və ya uğursuzluq;
- sorğu mənbəyi məsələn, terminal adı ;
- təsirə məruz qalan obyektlərin adları məsələn, açılan və ya silinən fayllar;
- təhlükəsiz məlumat bazalarında edilən dəyişikliklərin təsviri məsələn, bir obyekt üçün yeni təhlükəsizlik etiketi.

Hadisələr ardıcıllığının yenidən qurulması xidmətlərinin qorunmasında zəif cəhətləri üzə çıxarır, işğalda günahkarı tapır, vurulan zərərin dərəcəsini qiymətləndirir və normal işə qayıdır. Problemləri müəyyənləşdirmək və təhlil etmək, əlçatanlıq kimi bir təhlükəsizlik parametrini yaxşılaşdırmağa kömək edə bilər. Çatışmazlıqlar taparsanız, yenidən konfiqurasiya etməyə və ya sistemi yenidən qurmağa, performansın yenidən ölçülməsi və s. cəhd edə bilərsiniz.

Paylanmış heterojen sistemlərdə əlaqələndirilmiş protokollaşdırma və audit təşkil etmək asan deyil. Birincisi, təhlükəsizlik baxımından vacib komponentlər məsələn, marşrutlaşdırıcılar öz protokollaşdırma mənbələrinə malik olmaya bilər; bu vəziyyətdə, protokollaşdırmaları öz üzərinə götürərək, digər xidmətlər tərəfindən qorunmalıdır. İkincisi, müxtəlif xidmətlərdə hadisələri bir-birinə bağlamaq lazımdır.

Təhlükəsizlik siyasətinə uyğun olmayan fəaliyyətlər qanunsuz nüfuz qazanmağa yönəlmiş hücumlara və mövcud səlahiyyət daxilində edilən, lakin təhlükəsizlik siyasətini pozan hərəkətlərə bölünməsi məsləhət görülür.

Hücumlar hər hansı bir mənalı təhlükəsizlik siyasətini pozur. Hücumları təsvir etmək və müəyyən etmək üçün təhlükəsizlik siyasətinə münasibətdə dəyişməz olan

universal metodları, məsələn, ekspert sistemlərinin aparatlarından istifadə etməklə imzalar və hadisələrin giriş axınında aşkarlamaq kimi metodları tətbiq etmək olar.

Hücum imzaları - əvvəlcədən təyin edilmiş bir reaksiyaya səbəb olan bir hücumun baş verəcəyi düşünülən şərtlər toplusudur. imzalara nümunə bir terminaldan sistemə girmək üçün ardıcıl üç uğursuz cəhd , əlaqəli reaksiya nümunəsi, vəziyyət aydınlaşana qədər terminalın bloklanmasıdır.

Aktiv audit vasitələri ilə əlaqədar birinci və ikinci növ səhvləri ayırd etmək:. Birinci növ səhvlərin arzuolunmazlığı göz qabağındadır; kinci növ səhvlər daha az xoşagəlməzdir, çünki təhlükəsizlik idarəçisini əsl vacib məsələlərdən yayındırır, dolayı yolla hücumları atlamağa töhfə verir.

Aktiv audit alətləri IS-nin müdafiəsinin bütün xətlərində ola bilər. Şübhəli fəaliyyəti nəzarət olunan zonanın sərhədində və xarici şəbəkələrə qoşulma nöqtələrində aşkar edə bilərsiniz. Korporativ şəbəkədə aktiv audit xarici və daxili istifadəçilərin şübhəli fəaliyyətlərini aşkarlamağa və dayandırmağa, həm təhlükəsizlik pozuntularından, həm də aparat-proqram səhvlərindən qaynaqlanan xidmətlərin işindəki problemləri aşkar etməyə qadirdir. Aktiv audit mövcud olma hücumlarından qorunmanı da təmin edə bilər.

Funksional komponentlər və memarlıq

Aşağıdakı funksional komponentləri aktiv audit alətlərinin bir hissəsi kimi ayırmaq olar:

- qeydiyyat məlumatları yaratmaq üçün komponentlər. Aktiv audit vasitələri ilə nəzarət olunan obyektlər arasında yerleşir;

- yaradılan qeydiyyat məlumatlarını saxlamaq üçün komponentlər;

- qeydiyyat məlumatları sensorlar çıxarmaq üçün komponentlər.

Şəbəkə və host sensorları ümumiyyətlə fərqlənir, yəni birincisi, şəbəkə kartları dinləmə rejiminə qoyulmuş, ikincisi isə əməliyyat sistemi qeydlərini oxuyan

proqramlardır. Kommutasiya texnologiyalarının inkişafı ilə bu fərq tədricən silinir, çünki şəbəkə sensorları aktiv şəbəkə avadanlıqlarına quraşdırılmalı və onlar şəbəkə OS-nin bir hissəsi olmalıdırlar:

-qeydiyyat məlumatlarına baxmaq üçün komponentlər;

- sensorlardan alınan məlumatların təhlili komponentləri;

- təhlildə iştirak edən məlumatların saxlanması üçün komponentlər;

- qərar qəbul etmə və cavab komponentləri həlledicilər;

- nəzarət edilən obyektlər haqqında məlumatların saxlanması üçün komponentlər;

- analizatorları birləşdirən monitorlar adlanan aktiv audit menecerləri üçün bir təşkilat qabığı rolunu oynayan komponentlər;

- təhlükəsizlik meneceri ilə interfeys komponentləri.

Aktiv audit vasitələri menecer / agent memarlığında qurulmuşdur. Əsas agent komponentləri sensor adlanır. Təhlil, qərar qəbul etmə menecerlərin vəzifələridir. Aydındır ki, menecerlər və agentlər arasında etibarlı kanallar qurulmalıdır.

İndiki vaxtda ən çox istifadə edilən identifikasiya üsulları parol metodlarıdır. Şifrə metodları istifadəçidən sistem yaddaşında saxlanılan istinad parolu ilə müqayisə etmək üçün simvolu parol daxil etməsini tələb edir. Parol şifrə ilə uyğun gəlirsə, istifadəçi sistemlə işləyə bilər. Müxtəlif şifrə metodlarını nəzərdən keçirərkən, aşağıdakı qeydlərdən istifadə edəcəyik: S - sistem mesajı; İ - istifadəçi tərəfindən daxil edilmiş mesaj; OK - düzgün identifikasiya barədə sistem mesajı.

Sadə parol metodu istifadəçi tərəfindən klaviaturadan bir parol daxil edərək giriş etməkdir.

Nümunə 1 Şifrə PASSWORDS sözüdür.

C: Şifrə daxil edin

P: PASSWORD

C: OK

Simvol seçmə metodu, sistemin təsadüfi seçilmiş xüsusi parol simvolları üçün soruşmaqdan ibarətdir.

Nümunə 2. Şifrə PASSWORD sözüdür.

C: Parolu daxil edin: 3, 5

P: AL

C: OK

Simvol seçmə üsulu, giriş edən istifadəçi tərəfindən daxil edilmiş simvolların tək bir müşahidəsi ilə parol dəyərini təyin etməyə imkan vermir.

Nəzərdən keçirilmiş şifrələr təkrar istifadə edilə bilər; onların açıqlanması təcavüzkarın qanuni istifadəçi adından hərəkət etməsinə imkan verir. Şəbəkəni passiv dinləməyə davamlı olan daha bir güclü vasitə birdəfəlik şifrələrdir.

Tək istifadəlik şifrə metodu sistemdə saxlanılan N sayda şifrələrin siyahısını bizə təqdim edir. Sistemə hər dəfə daxil olduqda istifadəçi növbəti parolu daxil edir, iş başa çatdıqdan sonra sistem tərəfindən həmin parol siyahıdan silinir.

Ən məşhur birdəfəlik şifrə generatoru, İnternet standartı RFC 1938 statusuna sahib olan **Bellkore-un S / KEY** sistemidir. Bu sistemin ideyası belədir. Tutaq ki, bir tərəfli f funksiya var yəni, qəbul edilə bilən müddətdə tərsini hesablamaq mümkün olmayan bir funksiya. Bu funksiya həm istifadəçiyə, həm də identifikasiya serverinə məlumdur. Yalnız istifadəçiyə məlum olan K gizli açarın olduğunu düşünək.

Başlanğıc istifadəçi idarəetmə mərhələsində f funksiyası K açarına n dəfə tətbiq edilir, bundan sonra nəticə serverdə saxlanılır. Bundan sonra istifadəçi identifikasiyası proseduru aşağıdakı kimidir:

- server n-1 sayda nömrəni istifadəçi sisteminə göndərir;

- istifadəçi f funksiyasını K şəxsi açarına n-1 dəfə tətbiq edir və nəticəni şəbəkə üzərindən identifikasiya serverinə göndərir;
- server f funksiyasını istifadəçidən alınan dəyərə tətbiq edir və nəticəni əvvəllər saxlanılan dəyərlə müqayisə edir. Təsadüf olduğu təqdirdə istifadəçinin orijinallığı təsdiqlənmiş sayılır, server yeni dəyəri istifadəçi tərəfindən göndərilir xatırlayır və sayğacı n birə endirir.

Etibarlı identifikasiyaya başqa bir yanaşmada , qısa müddət aralığından sonra məsələn, hər 60 saniyədə yeni bir şifrə yaratmaqdır ki, bunun üçün proqramlar və ya xüsusi smart kartlar istifadə olunur.

Şifrə qrupu metodu hər bir istifadəçi üçün sistemin iki qrupdan parol tələb edə biləcəyinə əsaslanır. Birinci qrupa bütün istifadəçilər üçün ümumi suallara cavab verən şifrələr daxildir, məsələn, adı, ünvanı, telefon nömrəsi və s. İkinci qrup şifrələrə - suallara cavablar daxildir, hansı ki istifadəçi qeydiyyatı zamanı sistem idarəçisi tərəfindən sistemlə işləmək üçün təyin olunur. Bu suallar hər bir istifadəçi üçün şəxsən formalaşdırılır, məsələn, sevimli rəng, ananın soyadı və s. Hər dəfə istifadəçi əlaqə quranda sistem təsadüfi olaraq hər qrupdan bir neçə sual seçir. Bu metodun dezavantajı, sistemin çox sayda istifadəçi üçün sual və cavabları saxlamaq üçün əhəmiyyətli bir yaddaş tələb etməsidir.

Funksional çevrilmə metodu, qeydiyyata alınarkən sistemdə işləmək üçün istifadəçiyə ağlında edə biləcəyi bəzi çevrilmələr barədə məlumat verir. Bu vəziyyətdə parol belə bir dönüşün nəticəsində yaranır.

Nümunə 3. Dəyişiklik y = x1 + 2 * x2.

C: Parolu daxil edin: 4, 6

P: 16

C: OK

Şifrələrlə işləyərkən aşağıdakı qaydalara əməl edilməlidir:

parollar yaddaşda yalnız şifrələnmiş formada saxlanılmalıdır;

- İstifadəçi tərəfindən parol daxil edildikdə simvollar açıq görünməməlidir;
- şifrələr vaxtaşırı dəyişdirilməlidir;
- parollar sadə olmamalıdır.

Parolların mürəkkəbliyini yoxlamaq üçün adətən xüsusi parol nəzarətçiləri istifadə olunur.

Hal-hazırda parolların zəifliyini yoxlamağa imkan verən bir parol nəzarətçisi vardır. Nəzarətçi aşağıdakı prosedurdan istifadə edərək parolu sındırmağa çalışır.

1 Giriş istifadəçi adının, başlanğıclarının və birləşmələrinin parol kimi istifadəsinin yoxlanılması. Məsələn, istifadəçi Daniel V. Klein nəzarətçinin müəllifi üçün nəzarətçi DVK, DVKDVK, DKLEIN, LEINK, DVKLEIN, DANIELK, DVKKVD, DANIEL-KLEIN və s. parolları sınayacaqdır.

2 Müxtəlif lüğətlərdən 60.000 söz sözlərin parol kimi istifadəsinin yoxlanılması:

- kişi və qadın adları 16000 ad;
- ölkələrin və şəhərlərin adları;
- cizgi filmlərinin, filmlərin, fantastika əsərlərinin və s. personajların adları;
- idman terminləri komanda adları, idmançıların adları, idman jargonları və s.;
- nömrələrlə ədədlərdə və sözlərdə, məsələn, 2000, TWELVE;
- hərf və nömrələrin xəttləri məsələn, AA, AAA, AAAA və s.;
- müqəddəs adlar və başlıqlar;
- bioloji terminlər;
- jarqon sözləri və lənətlər;
- klaviaturada simvolların ardıcıl yerləşməsi məsələn, QWERTY, ASDF, ZXCVBN və s.;

- kompüter adları Unix-dəki / etc / hostc-dan;
- Şekspirin əsərlərindən personajlar və yerlər;
- tez-tez istifadə olunan xarici sözlər;
- asteroidlərin adları.

3. 2-ci iddiadan müxtəlif sözlərin dəyişdirilməsinin yoxlanılması, o cümlədən:

- ilk hərfin baş hərflə əvəz edilməsi;
- bütün hərflərin böyük hərflərlə əvəzlənməsi;
- bütün sözün çevrilməsi;
- O hərfini 0 sayı ilə və əksinə əvəz etmək 1 hərflə 1 nömrə və s.;
- sözlərin cəm halına çevrilməsi.

Ümumilikdə, nəzarətçi 3-cü iddiaya görə bir təsadüf üçün təxminən 1 milyon söz yoxlayır.

4. 3-cü bənddə nəzərə alınmayan 2-ci iddia sözlərinin müxtəlif dəyişikliklərinin yoxlanılması:

- bir kiçik hərfin böyük hərflə əvəz edilməsi məsələn, michel-miChel və s. - təxminən 400.000 söz;
- iki kiçik hərfin böyük hərflə əvəzlənməsi təxminən 1500.000 söz;
- üç kiçik hərfin böyük hərflə əvəzlənməsi və s.

5. Xarici istifadəçilər üçün istifadəçinin dilindəki sözləri yoxlamaq.

6. Söz cütlüyünün təsdiqlənməsi

Təcrübələr göstərdi ki, bu nəzarətçi beş simvoldan 10% parol, altı simvoldan 35% parol, yeddi simvoldan 25% parol və səkkiz simvoldan 23% parol təyin etməyə imkan verdi. Bunun səbəbi, əksər istifadəçilər sadə şifrələrdən istifadə edir. 1988-ci ildə İnterneti yoluxduran şəbəkə qurdu-nun müəllifi R. Morris bu vəziyyətdən

yararlandı. Morrisin virus ələ keçirmə modulu istifadəçi hesablarını, tərs qaydada istifadəçi adlarını və parol kimi tanınmış 432 sözdən ibarət şablondan parolları sınaqdan keçirdi. Bəzi hallarda, Morris bir sıra sistem şifrələri daxil olmaqla 10% -ə qədər parol əldə edə bildi.

Bununla birlikdə parol qorunması ən təhlükəsiz identifikasiya vasitəsidir. Daxil edilmiş parol casusluq edə bilər. Bəzən hətta optik alətlərdən də istifadə etmək olur. Şifrə, demək ki lüğətdən istifadə edilərək yəni kobud güc metodu ilə də təxmin edilə bilər. Parol faylı şifrələnmiş, lakin oxunaqlıdırsa, onu kompüterinizə yükləyə və tam bir axtarış verərək parolu tapmağa çalışa bilərsiniz.

Aşağıdakı tədbirlər parol qorunmasının etibarlılığını artıra bilər:

- **texniki məhdudiyyətlər** tətbiq etmək parol çox qısa olmamalıdır, hərflər, nömrələr, durğu işarələri ehtiva etməlidir və s.;
- **Parolların etibarlılıq müddətinin** idarə edilməsi, onların dövri dəyişdirilməsi;
- parol faylına girişin məhdudlaşdırılması;
- uğursuz giriş cəhdlərinin **sayının məhdudlaşdırılması** bu, kobud güc metodu -ndan istifadə etməyi çətinləşdirəcək;
- istifadəçi təlimi;
- proqram şifrə generatorlarının istifadəsi sadə qaydalara əsaslanan belə bir proqram yalnız ahəngdar və buna görə yadda qalan şifrələr yarada bilər.

Doğrulama üçün elektron imza istifadə ediləcəksə, sertifikatlardan istifadə tələb olunur. Sertifikatlar ümumiyyətlə bir növ məlumatdan və səlahiyyətli şəxs tərəfindən verilmiş sertifikatın məlumat hissəsinin elektron imzasından ibarətdir. İstifadəçilər müxtəlif səviyyələrdə sertifikatlar ala bilərlər

2.3 Proqram idxalına nəzarət

Kompüterlərdəki məlumatlar nadir hallarda statikdir. Yeni e-poçtlar qəbul edildi. Yeni proqramlar disketlərdən, CD-ROM lardan və ya şəbəkə serverlərindən yüklənir. İnteraktiv veb proqramları kompüterdə işləyən sənədləri yükləyir. Baş vermiş hər hansı bir dəyişiklik virus infeksiyası, kompüter konfiqurasiyasının pozulması və ya proqram lisenziyalarının pozulması riskini daşıyır. Təşkilatlar bu risklərə qarşı həssaslığından asılı olaraq müxtəlif mexanizmlər vasitəsilə qorunmalıdırlar.

Aşağıdakı problemləri həlli yolları proqramların idxalına nəzarət etməyə imkan verir:

- viruslardan və Troyan atlarından qorunma, onların aşkarlanması və çıxarılması;
- interaktiv proqramlara nəzarət Java, Active X;
- proqramın lisenziyalara uyğunluğunun monitorinqi.

Bütün tapşırıqlar aşağıdakı meyarlara görə təsnif edilə bilər:

- nəzarət - prosesin təşəbbüskarı kimdir və proqramın necə idxal edildiyini müəyyən etmək olar;
- təhdid növü - icra olunan proqram, makro, ərizə, lisenziya müqaviləsinin pozulması;
- mübarizə tədbirləri - virusların yoxlanılması, xidmətin dayandırılması, giriş hüquqlarının dəyişdirilməsi, dinləmə, silinmə.

Bir kompüterə proqramları idxal edərkən və onları işə saldıqda, bu proqramların əlavə funksionallığına və ya faktiki funksiyalarının elan olunanlardan fərqli olma riski var. İdxal birbaşa istifadəçi hərəkəti şəklində baş verə bilər və ya digər hərəkətlərin yan təsiri ola bilər ancaq nəzərə çarpan olmaya bilər. Açıq idxal nümunələri: FTP-dən istifadə edərək sənədin PC-yə ötürülməsi, elektron poçtun oxunması, disketdən və ya bir şəbəkədən proqram yüklənməsi və s göstərə bilərik.

Gizli idxal nümunələri: bir Java tətbiqetməsini kompüterinizə yükləyən və ya makro virusa yoluxmuş bir fayl açan veb səhifəni oxumaqdır.

2.4 Viruslardan qorunma.

Əvvəllər disketlər virus infeksiyasının ən çox yayılmış üsulu idi, çünki onların köməyi ilə proqramların kompüterlər arasında ötürülməsi olduqca rahat baş verirdi. BBS-lər yarandıqdan sonra viruslar modem vasitəsilə yayılmağa başladı. İnternet, virusların yayılması üçün başqa bir kanalın meydana gəlməsinə səbəb oldu, bu vasitələrlə tez-tez onlara qarşı mübarizənin ənənəvi üsullarından istifadə etməyə başladılar.

Proqramların qlobal şəbəkələrdən yüklənməsinə imkan verən təşkilatlar üçün elektron poçtlara əlavələr ola bilər, ME-lərdə virusların skan edilməsi yaxşı bir hal ola bilər.

Antivirus təhlükəsizlik siyasətinin üç hissəsi var:

- qarşısının alınması - infeksiyanın qarşısını düzgün almaq qaydaları;
- aşkarlama - verilmiş bir icra olunan faylın, açılış qeydinin və ya məlumat faylında bir virusun olduğunu müəyyənləşdirmək;
- silinməsi - kompüterin virusa yoluxmuş sistemdən çıxarılması ƏS yenidən qurulması, faylların silinməsi, virusa yoluxmuş faylın silinməsi.

Kompüterdə yeni faylların və ya tətbiqlərin görünüşünün tezliyi, həmçinin İnternetdə işləmək, e-poçt oxumaq və xarici mənbələrdən faylları yükləmək üçün konfiqurasiyadakı dəyişikliklər, virusun yoluxma ehtimalı ilə mütənasibdir. Kompüterin və ya içindəki məlumatların əhəmiyyəti nə qədər çox olarsa, viruslara qarşı təhlükəsizlik tədbirlərinə daha çox diqqət yetirilməlidir. Qarşısının alınması siyasəti olaraq , potensial yoluxmuş proqramları və faylları yükləməyinizə qoyulan məhdudiyyətlərə xüsusi diqqət yetirməyiniz başlıca cıxış yoludur. Bundan başqa,

yüksək riskli bir mühitdə, yeni fayllar üçün virus taramasını xüsusilə diqqətlə aparılmasının lazım olduğunu vurğulamalıyıq.

2.5 İnteraktiv proqramlara nəzarət

İnternet nəticəsində proqram mühiti interaktiv bir proqram mühitinə çevrildi, bunların nümunələri Java və Asset X. Bu mühitdə istifadəçi şəbəkə vasitəsilə serverlə qarşılıqlı əlaqə qurur. Server tətbiqi tətbiqetməni istifadəçi kompüterinə yükləyir, sonra onu işlədir. Bu strategiyanı istifadə etmək üçün bir neçə risk var. Əvvəla, yüklənən şeyin tam olaraq nəyi yerinə yetirəcəyini bilməlisiniz.

Daha əvvəl Java kimi dillərdən istifadə edərkən, fayl sisteminə girişə nəzarət etmək və proqramın icrasına nəzarət etmək üçün dildə qurulmuş məhdudiyyətlər səbəbindən bir virusa yoluxmanın mümkün olmadığı iddia edildi. İndi bu ifadələr əvvəlkindən fərqli olaraq tamamilə təkzib olunur. Əhəmiyyətli bir riskə görə, bu texnologiyanı istifadə etməzdən əvvəl istifadəçinin almalı olduğu bir neçə təhlükəsizlik zəmanəti var:

- açılan serverdə appletlərə etibar edilməlidir;
- appletlər yalnız təhlükəsizliyə təsir edən funksiyaları yerinə yetirən fayllara məhdud girmə imkanı olan bir mühitdə işlənməlidir;
- tətbiqetmədən əvvəl appletlərin təhlükəsizliyi yoxlanılmalıdır;
- skriptlər əvvəlcədən hazırlanmır , lakin şərh olunur.

2.6 Proqramın lisenziyası

İnternet bir çox təşkilatlara proqramların yayılmasının yeni yollarından faydalanmağa imkan verdi. Çox sayda şirkət istifadəçilərə məhsullarının test versiyalarını, bəzən demoları və ya məhdud müddət işləyən versiyalarını yükləməyə imkan yaratdı. Bununla birlikdə, bir çox şirkət test proqramlarının tam funksional

versiyalarını yükləyə biləcəyiniz şərtsiz tətbiqetmədən istifadə edir və istifadəçi proqramı kommersiya məqsədləri üçün istifadə edərsə qeydiyyatdan keçməli və müəyyən olunmuş bir məbləğ ödəməlidir.

İstifadəçilər İnternet üzərindən yüklənmiş proqramlar ilə qeydiyyatdan keçmədikdə və ya səhv etdikdə, təşkilat lisenziyalaşdırma qaydalarını pozmuş ola bilər. Bu cür faktların aşkarlanması qanuni tədbirlərə və nəticədə nüfuzun itməsinə səbəb ola bilər.

Aşağı risk - İnternetdən yüklənmiş bütün kommersiya proqramları üçün proqram istehsalçılarının lisenziyaları qaydalarına riayət etməlisiniz. Proqramların test versiyaları sınaq müddətindən sonra çıxarılmalı və ya təşkilat proqramın qanuni versiyasını satın almalıdır.

Orta yüksək risk - kommersiya proqramlarının sistem rəhbərinin icazəsi olmadan yüklənməsinə icazə verilmir. Təşkilatın kompüterlərində istifadə olunan proqramlar yalnız lisenziya qaydalarına uyğun olaraq sistem rəhbərləri tərəfindən quraşdırılır. Şöbə, işçilərin kompüterlərinin lisenziya qaydalarına uyğunluğu və icazəsiz proqramların olmaması üçün avtomatlaşdırılmış vədə vaxtaşırı şəkildə yoxlamalıdır.

III FƏSIL. İnternet Şəbəkədə verilənlərin qorunmasının əsas metodları və vasitələrinin tətbiqi və onların inkişaf tendesiyaları

3.1 Şəbəkədə informasiyanın təhlükəsizliyi və onun mühafizəsi prinsipləri

İnformasiya Təhlükəsizliyinin əsas məqsədi -informasiya münasibəti iştirakçılarının maraqlarının qorunmasına yönəlir.Bu maraqlar çox cəhətli olsa da,əsas diqqət əlyetənlik,tamlıq,məxfiliyin qorunmasına yönəlir.

Təşkilatda informasiya təhlükəsizliyi sisteminin qurulmasına atılan addımlardan ən başlıcası bu aspektlərin təhlilinə və sıralanmasına yönəlir.

İnformasiya təhlükəsizliyi probleminin əhəmiyyəti 2 əsas səbəblə izah olunur.

- Toplanmış informasiya resurslarının dəyərliliyi ilə;
- İnformasiya texnologiyaslndan aslılıq.

Mühüm informasiyanın məhv edilməsi,məxfi verilənlərin oğurlanması,sistemdəki dayanmalar səbəbindən iş yerlərində fasilələrin olması-şirkətin nüfuzuna xələl gətirməklə bərabər böyük maddi itkilərə səbəb olur.İnzibati-idarəetmə və tibbi sistemlərdə baş verən problemlər insan sağlamlığı və həyatına ciddi təhlükələr törədir.

Muasir informasiya sistemləri çox mürəkkəbdir və təcavüzkarlar hesaba almasaq belə sistem özü üçün təhlükədir.Proqram təminatında hər zaman yeni zəifliklər aşkarlanır.Proqram-aparat vasitələri və digər struktur elementlərinin çox saylı əlaqələrini nəzərə almalıyıq.

Korporativ informasiya sistemlərinin yaranması prinsipləri dəyişir.Çoxsaylı xarici informasiya xidmətlərindən istifadə olunur;İnformasiya sistemindən kənarda təmin olunur və autsorsinq adlanır -korporativ informasiya sisteminin bir funksiyasının başqa şirkət tərəfdən reallaşmasıdır.**Aktiv agentlərlə** proqramlaşdırma inkişaf edir.

İnformasiya təhlükəsizliyi probleminin **çətinliyi** informasiyanın mühafizəsi tədbirlərinə xərclənən vəsaitlərin və sistemdəki hər **pozuntunun** yetirdiyi **zərərlə** parallel artır.

İnformasiya təhlükəsizliyi sahəsində uğur yalnız aşağıdakı dörd yanaşmanı nəzərə almaqla əldə olunur:

- Hüquqi-qanunverici;
- İnzibati-administrativ;
- Prosedur;
- Proqram-texniki;

İnformasiya Təhlükəsizliyi problemi yalnız texniki problem deyil;hüquqi məlumat olmadan , rəhbərliyə sin diqqəti olmadan və rəhbərlik lazımi resursları ayırmadan ,kadrların idarə olunması və fiziki mühafizə olmadan problemi həll etmək mümkün deyil.Komplekslikdə öz özlüyündə problemi qəlizləşdirir; müxtəlif sahədən olan mütəxəssislərin bircə fəaliyyətini tələb edir.

Mürəkkəbliyə qarşı mübarizədə əsas alət kimi obyektiv yanaşma tələb olunur.

Qanunverici,inzibati və prosedur səviyyə

Hüquqi səviyyə informasiya təhlükəsizliyinin təmin olunması üçün vacib sayılır.İnformasiya təhlükəsizliyi probleminin əhəmiyyəti hər cəhətdən vurğulanmalıdır; resursları tədqiqatın ən vacib sahələrinə yönəltmək;təhsil fəaliyyətini əlaqələndirmək;zərər yetirənlərə qarşı mənfi münasibət yaratmaq və saxlamaq və s hüquqi təminata aiddir.

Qanunverici səviyyədə əsas rolu qanunlar və aktlar oynayır.İnformasiya və informasiyanın qorunması ilə bağlı qanunlar irəli sürülür.Lisenziyalar və sertifkatlar öz özlüyündə təhlükəsizliyi tam təmin etmir.Bundan əlavə informasiya təhlükəsizliyinin pozulmasına görə dövlət məsuliyyət daşımır.Dünya ölkələrində informasiya təhlükəsizliyinə dair standartlar hazırlanmışdır.Əsasən standartlar

informasiya istehsalçısı,istehlakçısı və ekpert arasında qarşılıqlı mübadiləsini təmin edir.

Standartlar arasına Narıncı Kitab , X.800 tövsiyyələr və informasiya Texnologiyaları Təhlükəsizliyini Qiymətləndirmə meyarları daxildir.

Narıncı Kitab konsepsiyanın əsasını qoydu;təhlükəsizlik tələbinə görə informasiya sistemlərini təsnifləşdirən metodu təklif etdi. Kompüter sistemlərinin təhlükəsizlik kriteriləri adlanan sənəd Amerika Birləşmiş Ştatlarının Müdafiə Nazirliyinə aiddir. Sənəddə təhlükəsizlik pillələrinin – D, C, B və A 4 növü müəyyən olunmuşdur. D səviyyəsindən A səviyyəsinə keçidə sərt tələblər irəli sürülür. C və B səviyyələri siniflərə C1, C2, B1, B2, B3 bölünür. Sistemin sertifikatlaşdırma proseduru nəticəsində müəyyən sinifə aid edilməsi üşün, onun müdafiə edilməsi müəyyən tələbləri ödəməlidir.[2,səh304]

X.800 tövsiyyələr şəbəkə konfiqurasiyasının mühafizəsi suallarını dərindən tədqiq edir və inkişaf etmiş xidmətlər və təhlükəsizlik mexanizmləri təklif edir.

Ümumi meyarlar olaraq bilinən beynəlxalq ISO 15408 standartı daha müasir bir yanaşma tətbiq edir, təhlükəsizlik xidmətlərinin son dərəcə geniş spektrini özündə birləşdirir.Onun dünya standartı kimi qəbul edilməsi yalnız dünya birliyinə inteqrasiya olunmaq üçün deyil həmçinin bu standart informasiya sistemi sahibkarlarına geniş çeşiddə sertifkasiyalaşdırılmış həllər vəd etməklə onların işini asanlaşdırır.Respublikamızda informasiya-kommunkikasiya texnologiyalarının hazırladığı standartlardan istifadə olunur. Bu standartlarla əlavə informasiya təhlükəsizliyinin idarə edilməsi sisteminin tətbiqi üzrə təlimat və s misal göstərə bilərik.Ölkəmizdə bu sahə üzrə beynəlxalq standartlara uyğun addımlar atılır.Standartlar 20 iyun 2012-ci il tədbiq olunmuşdur.

İnzibati səviyyədə əsas məsələ **informasiya təhlükəsizliyi** sahəsində işlərin tərtibi və yerinə yetirilməsinin təmin etmək,və lazimi resurslar ayırmaq və işlərə nəzarət etmək.

Proqramın nüvəsinin əsasını təhlükəsizlik siyasəti təşkil edir və təşkilatda informasiya aktivlərinin mühafizəsinə yönəlir. **İnformasiya təhlükəsizliyi** siyasəti şirkət məlumatlarına, aktivlərinə, sistemlərinə və digər İT qaynaqlarına daxil olan insanların izləməsi lazım olan qaydalar və qaydaların sənədləşdirilmiş bir ifadəsidir. İnformasiya təhlükəsizliyi siyasətinin əsas məqsədi şirkətin kibertəhlükəsizliyi proqramının səmərəli işləməsini təmin etməkdir. Təhlükəsizlik siyasəti canlı sənəddir, lazım olduqda daim yenilənir. Kibertəhlükəsizliyə dair kim, nə və niyə sualları qoyulur.

Təhlükəsizlik siyasətinə nə daxil edilməlidir? İlk başlanğıc üçün, təhlükəsizlik siyasəti məqbul istifadə, məxfi məlumatlar, məlumatların saxlanması, e-poçt istifadəsi, şifrələmə, güclü şifrələr, simsiz giriş və digər təhlükəsizlik siyasətlərindən ibarət ola bilər.[22]

İnformasiya təhlükəsizliyi siyasətinin üstünlükləri nələrdir? Təhlükəsizlik siyasətinə nə üçün ehtiyacımız var? Əsasən beş səbəbi göstərilir:

1. Rol və vəzifələri müəyyən etmək

Yaxşı yazılmış təhlükəsizlik siyasəti sənədi Təhlükəsizlik siyasəti sizə nə etməyə imkan verir? sualına dəqiq cavab verməlidir. Hansı tapşırığa kimin cavabdeh olduğunu, kimin belə bir iş görməyə səlahiyyətli olduğunu, bir işçinin nəyi edə biləcəyini və edə bilməyəcəyini və hər tapşırığın nə vaxt başa çatmalı olduğunu izah etməlidir. Onlar yalnız işçilərin rollarını və məsuliyyətlərini deyil, həm də şirkət mənbələrindən istifadə edən insanların qonaqlar, podratçılar, təchizatçılar və tərəfdaşlar kimi vəzifələrini də müəyyənləşdirirlər.

2. Hesabatlılığı müəyyən etmək

İşçilər səhv edə bilə,üstəlik, bəzi səhvlər baha başa gələ bilər. Bu təhlükəsizlik siyasətinin yararlandığı bir sahədir. Qaydalara əməl etməməyin nəticələri izah olunur. Təhlükəsizlik siyasəti müqavilələr kimidir. Onlar işçilər tərəfindən tanınmalı və imzalanmalıdırlar. Bu o deməkdir ki, heç bir işçi qaydaları pozmağın nəticələrini qaydaları bilməməsi səbəbindən olması istisna edilmir. İşçi qayda pozursa, cəza qeyri-

obyektiv sayılmaz. Təhlükəsizlik siyasətləri məhkəmədə iddianı dəstəkləmək üçün də istifadə edilə bilər.

3. İşçilərin kiber təhlükəsizlik barədə məlumatlılığını artırmaq

Təhlükəsizlik siyasəti təhsil sənədləri kimi çıxış edir. İşçilərə kiber təhlükəsizlik haqqında məlumat verə və kiber təhlükəsizlik barədə məlumatlılığı artıra bilərlər. Təhlükəsizlik siyasəti etibarlı parol seçmək, fayl köçürmələri, məlumatların saxlanması və VPN-lər vasitəsilə şirkət şəbəkələrinə daxil olmaq kimi mövzuları geniş əhatə edir.

4. Təhdidləri aradan qaldırmaq

Təhlükəsizlik siyasəti təhlükəsizlik təhdidlərinin aradan qaldırılması, həmçinin pozuntudan və ya kiber hücumdan qurtulmaqda və zəifliklərin azaldılmasında görülməsi lazım olan işləri həll etməlidir. Təhdidlərin aradan qaldırılması aspekti digər elementlərlə də üst-üstə düşür .Məsələn, təhlükəsizlik tədbirində kim necə hərəkət etməlidir, işçi nə etməli və ya etməməlidir və sonda kim cavabdeh olacaq məsələyə və s sualları cavablandırmalıdır.

5. Qaydalara riayət etmək

Təhlükəsizlik siyasəti beynəlxalq standartların qaydalarına və tələblərinə cavab verməlidir.

Təhlükəsizlik siyasəti niyə hazırlanmalıdır?

Təhlükəsizlik siyasəti bir şirkətin kiber təhlükəsizlik proqramının əsasını təşkil edir. Bu siyasət yalnız şirkət məlumatlarını və İT qaynaqlarını qorumaq və ya işçilərin kiber məlumatlılığını artırmaq üçün deyil; bu siyasət ayrıca şirkətlərin rəqabətdə qalmasına və müştərilərin etibarını qazanmasına kömək edir. Bu barədə düşünün: əgər bank müştərilərin məlumatları hakerlər tərəfindən ələ keçirilirsə , bu banka yenə də etibar ediləcəkmi? Nəticədə şirkətlər itirilmiş istehlakçı etibarını geri ala bilərlər, lakin bunu etmək uzun və çətin bir prosesdir. Təəssüf ki, kiçik ölçülü şirkətlərin ümumiyyətlə kiber təhlükəsizlik proqramına uyğun yaxşı hazırlanmış siyasətləri yoxdur. Bəzi

hallarda, kiçik və ya orta sahibkarlığın məhdud resursları var və ya şirkət rəhbərliyi düzgün düşüncə tərzini qəbul etmir və gecikir qəbul etməyə. Bunun səbəbi isə effektiv kibertəhlükəsizlik proqramının nə qədər vacib olduğunu bilməməsidir. Ama yuxarıda dediyimiz hallarla qarşılaşmamaq üçün təhlükəsizlik siyasətini yaratmağa heç vaxt qeyri ciddi yanaşmaq qəbul edilməməlidir. Təhlükəsizlik siyasətini hazırlayarkən, siyasətçi yuxarıda göstərilən bütün beş faydanı əldə etmək məqsədi ilə bunları yazmalıdır. Şirkət miqyasının kiçik olması şirkətlərin adekvat təhlükəsizlik siyasətinin olmamasına səbəb olmamalıdır.

Təhlükəsizlik siyasətinin və proqramının yaradılmasının ilkin olaraq risklərin təhlili ilə başlayır, birinci mərhələ isə çox yayılmış hədələr ilə tanışlıqdan başlayır.

Əsas təhlükələr- İnformasiya sisteminin öz daxili mürəkkəbliyi və sistemə xidmət edən sistem inzibatçılarının,operatorların,əməliyyatçıların və s şəxslərin səhvlərinə görə yaranır.

Yer baxımından ikinci olaraq saxtakarlıq və oğurluq yer alır.

Real təhlükə isə infrastrukturda olan yanğınlar və qəzalar sayılır. Əsas pozuntuların sayına baxanda daha çox yeri xarici hücumlar alır,lakin əsas zərər daxili hücumlara görə baş verir.

Təşkilatların əksəriyyəti üçün risklə ümumi tanışlıq kifayət edir ki, tədbiq olunmuş həll yolları vasitəsi ilə az intektual və maddi xərclərlə riskə qali gəlsin.

Tipik bir çərçivə təqdim edən İngilis standartı BS 7799: 1995, təhlükəsizlik siyasətinin inkişafında əhəmiyyətli rol oynayır.

Təhlükəsizlik siyasəti və proqramının inkişafı detallı yanaşmaya nümunə ola bilər,belə ki hər sualı əhatə edən səviyyələr mövcuddur.Proqramın vacib xüsusiyyəti informasiya təhlükəsizliyinin saxlanması və inkişafıdır.

Etibarlı və qənaətli təhlükəsizlik sistemini qurulmasının əsas şərti həyat tsiklinin təhlilidir.İnformasiya sisteminin və təhlükəsizliyin sinxronlaşdırılması.Həyat dövrünün aşağıdakı mərhələləri var:

- təşəbbüs;
- alış;
- quraşdırma;
- əməliyyat;
- istismardan çıxarılması.

Təhlükəsizliyi həyat tsiklinə aid etmək olmaz.Təhlükəsizlik təməli əvvəldən qoyulmalı və sonadək qorunmalıdır.

Prosedur səviyyəsi daha çox insanlara yönəlmişdir və aşağıdakı növləri var:

- işçi heyətinin idarəedilməsi;
- fiziki mühafizə;
- iş qüvvəsinin qorunması;
- təhülkəsizlik siyasətinin pozulmasına reaksiyanın verilməsi;
- bərpa işlərinin planlaşdırılması.

Bu səviyyədə vacib təhlükəsizlik prinsipleri qəbul olunub:

- məkan və zaman daxilində mühafizənin kəsilməzliyi;
- Vəzifələrin bölüşdürülməsi;
- Öhdəliklərin minimuma endirilməsi;

Buraya həmçinin həyat tsikli anlayışı və obyektiv yanaşma aiddir.İlk olaraq nəzarət edilən müstəqil vasitələriəşya,ərazi və s və nisbətən müstəqil obyektləri ayrı-ayrlıqda nəzərdən keçirir və onlar arasında qarşılıqlı münasibəti tapır.

Həyat tsikli anlayışını yalnız informasiya sistemləri anlayışına deyil ,həmçinin işçilərə də aid etmek lazım gəlir.Başlanğıc mərhələdə ixtisas və kompüter bilikləri tələbinə aid iş təsvir olunmalıdır,quraşdırma mərhələsində əsasən təhlükəsizlik məsələlərinə aid təlimlər keçirilməlidir,istismardan çıxartma mərhələsində isə diqqetli davranmaq lazımdır ki,incidilmiş işçilər tərəfindən vurulacaq ziyanların qarşısı almaq mümkün olsun.

İnformasiya təhlükəsizliyi cari işin nizamlı aparılmasından çox aslıdır və özünə aşağıdakıları daxil edir:

- İstifadəçilərin dəstəklənməsi;
- Proqram təminatının dəsdəklənməsi;
- İdarəetmənin konfiqurasiyası;
- Ehtiyyat nüsxələrinin yaradılması;
- Daşıyıcıların idarəedilməsi;
- Rəsimləşdirmə;
- Reqlamentli iş.

İnformasiya təhlükəsizliyi sahəsində görülən gündəlik işlərə məlumatların izlənməsidir;ən azı təhlükəsizlik administratoru mühafizə haqda gələn mesajları qəbul etməli və vaxtında həll etməlidir.

Həmçinin fövqəladə vəziyyətlərə informasiya təhlükəsizliyinin pozulmasına sistemi əvvəlcədən hazırlamaq lazımıdır.Təhlükəsizlik pozuntularına qarşı reaksiyalar 3 əsas məqsədə yönəlir:

- İnsidentin lokallaşdırılması və dəymiş zərəri azaldılması;
- Qayda pozanların müəyyənləşdirilməsi;
- Təkrar pozuntular barədə xəbərdarlıq.

Qayda pozanların şəxsiyyətinin müəyyən edilməsi olduqca mürəkkəb prosesdir,lakin birinci və üçüncü məqamlar olduqca düşünülmüş şəkildə hazırlanmalıdır.

Ciddi qəzalar zamanı bərpa işlərinin həyata keçirilməsi olduqca vacibdir.Bu tip işlərin planlaşdırılması aşağıdakı mərhələlərə ayrılır:

- Təşkilatın vacıb funksiyalarının və prioritetlərin müəyyənləşdirilməsi;
- Resurların müəyyənləşdirilməsi təşkilatın kritik funksiyalarının həyata keçirilməsində vacibdir;
- Mümkün qəzaların siyahısını müəyyənləşdirmək;

- Bərpa strategiyalarının hazırlanması;
- Seçilmiş strategiyanın reallaşdırılmasına hazırlıq;
- Strategiyanın yoxlanması.

Proqram-texniki səviyyə

Proqram-texniki tədbirlər əsasən kompüterə- avadanlıq,proqram və məlumata nəzarət etməyə yönəlmiş informasiya təhlükəsizliyinin ən sonuncu və vacib xəttini təşkil edir.

Bu məqamda informasiya sistemlərində olan sürətli tərəqqinin yalnız müsbət yox həçminin mənfi tərəflərida müəyyən olunur.İlkin olaraq əlavə imkanlar yalnız informasiya təhlükəsizliyi mütəxəssisləri üçün yox ,həm də hücüm edən cinayətkarlar üçündə yaranmış olur.İkincisi informasiya sistemləri daimi olaraq yenilənir ,yenidən qurulur həmçinin ən yeni versiya proqram təminatı əlavə olunur və beləliklə informasiya təhlükəsizliyi rejiminə riayət etmək çətinləşir.

Müasir informasiya sistemlərinin mürəkkəbliyini dünya ölkələrində olan ali məhkəmə sistemlərinə nəzər salmaqla müşahidə edə bilərik.

İnformasiya təhlükəsizliyi tətbirlərini aşağıdakı növlərə bölməliyik:

- Profilaktik,informasiya təhlükəsizliyinin pozulmasının qarşısının alınması;
- Pozuntuların aşkar olunması tədbirləri;
- Pozuntuların təsir dairsini lokallaşdırmaq;
- Qaydanı pozan şəxsin müəyyən olunması tədbirləri;
- Təhlükəsizlik rejiminin bərpası tədbirləri.

Düşünülmüş təhlükəsizlik arxitekturasında yuxarıdakı tədbirləri hər biri mövcud olmalıdır.

Praktiki yanaşmadan baxdıqda isə təhlükəsizlik arxitekturasında aşağıdakı prinsiplərin olması çox vacibdir:

- Məkan və zaman daxilində mühafizənin kəsilməzliyi və mühafizə vasitələrindən istifadənin vacibliyi;

- Tanınmış standartlardan və təstiq olunmuş həllərdən istifadə;
- Hər səviyyəsində az təşkil edicisi olmaqla iyerarxik informasiya sisteminin təşkil olunması;
- Sistemin ən zəif elementinin gücləndirilməsi;
- Təhlükəli vəziyyətə keçidin mümkün olmaması;
- İmtiyazların minimumlaşdırılması;
- Vəzifələrin bölüşdürülməsi;
- Çox səviyyəli müdafiə;
- Mühafizə vasitələrinin müxtəlifliyi.
- İnformasiya sisteminin sadə və idarə olunan olması.

Proqram-texniki təmınatın nüvəsini təhlükəsizlik xidmətləri anlayışı təşkil edir.Təhlükəsizlik xidmətlərinə aşağıdakılar aiddir:

- **İdentifikasiya və audentifikasiya;**
- **Girişin idarə olunması;**
- **Protokollaşdırma və audit;**
- **Şifrələmə;**
- **Tamlığa nəzarət;**
- **Ekranlaşdırma;**
- **Təhlükəsizliyin təhlili;**
- **Səhvlərə dözümlülük;**
- **Təhlükəsiz bərpanın təmin olunması;**
- **Tunelləşdirmə-VPN;**
- **İdarəetmə.**

Bu xidmətlər açıq şəbəkədə müxtəlif komponentlərlə işləməlidir,yəni müxtəlid təhdidlərə qarşı dayanıqlı olmalıdır və onun istifadəsi həm istifadıçilər həm də adminlər üçün rahat olmalıdır.Məsələn audentifikasiya\indetifikasiya prosesi şəbəkədə vahid girişi və şəbəkənin passiv və aktiv vəziyyətini dəstəklənməlidir.

Sadalanan təhlükəsizlik xidmətlərindən ən vacib məqamlarını vurğulayırıq.

1. Proqram və aparat metodu ilə tədbiq olunan audentifikasiyanın kriptolojı metoduna ütsünlük verilir.Kriptolojı metodlar anaxronizm halına keçib,biometrik metodların şəbəkə mühitində əlavə yoxlanmasına ehtiyyac olur.

2. Ən etibarlı proqram-təminatı belə keçmişdə qaldıqda anaxronizm dönüşür və ən çox yayılmış hala keçir lakin bir çox yenilikləri dəstəkləmək olmur.Məsələn o tip proqramların terminində troya proqramların nə olduğunu izah etmək mümkün olmur.İdeal olaraq,girişə nəzarət zamanı əməliyyatların semantikası tanıdılmalıdır,lakin bu günə qədər bunun üçün nəzəri bazalar mövcuddur.Başqa bir vacib məqam çox istifadəçi və çoxsaylı resurslar, eyni zamanda konfiqurasiyasının daimi dəyişkənliyi şəritində idarəetmənin asan olmasıdır.

Protokollaşdırma və audit çoxsəviyyəli , geniş və yüksək səviyyəyə keçid zamanı məlumatların filtirlənməsi dəstəkləməlidir.Bu idarəetmənin zəruri şərtləridir.Aktiv audit vasitələrindən istifadə etmək arzuolunandır lakin onların məhdudiyyətlərini bilmək lazımdır belə ki onlar çox da etibarlı deyil.Onları elə konfiqurasiya etmək lazımdır ki,avtomatik cavab zamanı səhvlərin və həyəcan siqnalların sayı az olsun.

Kriptoqrafiya ilə bağlı hər şey həm həm texniki,həm hüquqi baxımdan çətindir və bu şifrələmə üçün ikiqat doğrudur.Baxılan xidmət infrastrukturdur, onun tətbiqi bütün aparat və proqram platformalarında mövcud olmalıdır və yalnız təhlükəsizlik üçün deyil, həm də performans baxımından sərt tələblərə cavab verməlidir.Hələlik ən geniş yayılmış proqram təminatlarından istifadədədir çıxış yolu.

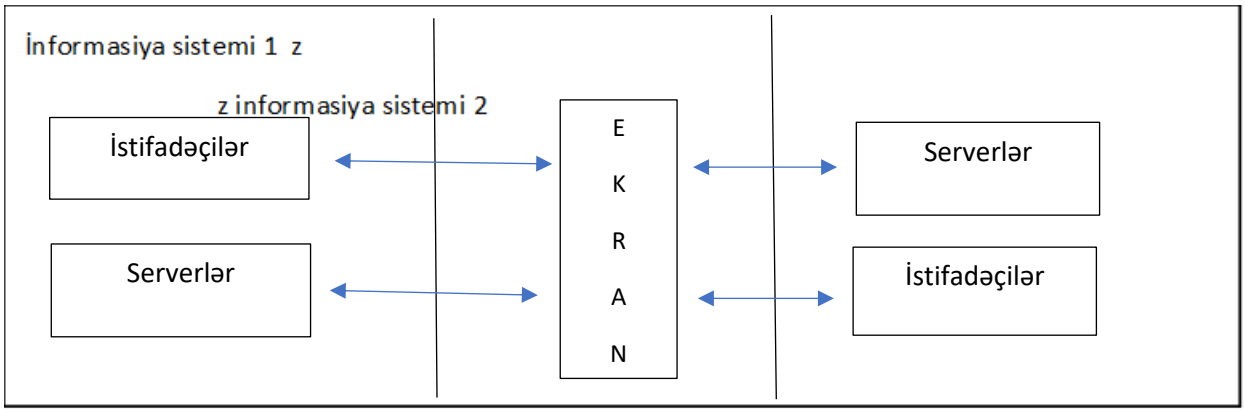
Tamlığa etibarlı nəzarət kriptolojı metodlara əsaslanır və ona oxşar metodlardan istifadə edir. Böyük ehtimalla, Elektron Rəqəmsal İmzalar haqqında qanunun qəbul edilməsi vəziyyəti daha yaxşı bir şəkildə dəyişəcək, tətbiq dairəsi genişlənəcəkdir.Xoşbəxtlikdən,saxlama cihazlarının istifadəsinə əsaslanan statik bütövlüyə dair kriptoqrafik olmayan yanaşmalar mövcuddur, məlumatlar yalnız oxunma üçün istifadə olunur.Oxuma və yazılmanı ayırsaq çox etibarlı sistem əldə edə bilərik.

Ekranlaşdırma- çox zəngin təhlükəsizlik xidmətidir.Onun reallaşması yalnız firewall deyil həmçinin məhdudlaşdırılmış interfeys və vitual lokal şəbəkələr təşkil edir.Ekran obyekti əhatə edir və xarici təqdiminə nəzarət edir. Müasir firewallar çox yüksək səviyyədə təhlükəsizlik, istifadə və idarəetmə rahatlığı şəbəkə mühitində, onlar ilk və çox güclü müdafiə sərhədidir.Hər növ firewalların həm lokal həm korparativ həm daxili ,həm xarici istifadəçilərin hərəkətlərinə nəzarət edir.Əsasən OSİ modelinin filtirlənməsi kimi baxmaq olar

Belə ki,müəyyən IP ünvanları çoxluğu verilir və bu zaman həmin IP çoxluğundan kənarda olan IP ünavanına malik kompüter sistemə giriş edə bilmir.Şəkil 3 -də Ekranlaşmanın iş prinsipi göstərilib

Mühafizənin analizi-həyat tsiklinin mühafizəsini dəstəkləyən elementdir.Aktiv audit everistikdir belə ki,o biliklər bazasının daim yenilənməsini tələb edir.

Dayanıqlığın və təhlükəsiz bərpanın təmin olunması güclü sistemin ən yüksək komponentinəndir.Bunların reallaşdırılmasında əsas diqqət arxitektura suallarına yönəlir -konfiqurasiyayaaparat və proqram yəni aparat və proqram bir-birlərinə uyğun olmalıdır,bundan başqa mümkün təhlükələrin və hansı sahələr daha çox zərər görə bilər onların uçotu aparılır.Təhlükəsizliyin bərpası – layihələndirmə,reallaşdırma və istismar mərhələlərinə xüsusi diqqət tələb edən ən sonunçu sərhəddir.



Cədvəl 3

Tunelləşdirmə-VPN -təhlükəsizlik xidmətləri arasında sadə,lakin ən zəruri elementlərindən biridir.o özü ayrılıqda yox ekranlaşdırma və şifrələmə ilə kombinə olunmuş şəkildə virtual şəbəkənin tətbiqində iştrak edir. Vpn əsasən şəbəkədə verilənləri şifrələnmiş şəkildə ötürür.RDCremote desktop connection məsafədən lokal şəbəkə hüdudları xaricində sistemə,serverə qoşulmaq üçün vpn xidmətlərindən istifadə edir.

İdarə olunma -bu infrastruktur xidmetidir.Təhlükəsiz sistem idarə olunan olmalıdır.Hər zaman informasiya sistemində nə baş verdiyini öyrənmək mümkün olmalıdır ideal olaraq isə vəziyyətin proqnozu barədə məlumat olmalıdır.

3.2 İnternetdə informasiya təhlükəsizliyi protokolları

İnternet adlandırdığımız qlobal şəbəkədən fəal istifadə kompüter cinayətkarlığı problemini qloballaşdırdı.Belə ki istər ölkə daxilində,istər ölkə hüdudlarından kənarda internet üzərindən intensiv məlumat mübadiləsi olur buda verilənləri həmin şəbəkədə qorunmağını zəruri edir. İnternet -müxtəlif kompüter şəbəkələrini əlaqələndirən qlobal informasiya şəbəkəsidir.Əvvəlcə ARPANET şəbəkəsi olaraq yaradıldı ,sonralar ABŞ milli elm fondu beynəlxalq əməkdaşlığı inkişaf etdirmək və tədqiqat müəssələrini birləşdirmək üçün NSFNET layihəsini qurdu.1990-cı ildən etibarən ARPANET öz fəaliyyətini dayandırdi və internet informasiya əlçatanlıq və sürətli əlaqə rabitəsi olmaqla elm dünyasının hüdüdlarından kənardada yayılmağa başladı.Şəbəkəyə qoşulmuş kompüterlər Windows-9X, NT, NetWare, OS/2, Mac OS, UNIX əməliyyat sistemlərindən birini istifadə edə bilər.Məlumat mübadiləsinin sürəti kopüterin konfiqurasiyasından ,şəbəkədən ,istifadəçinin kompüterdən istifadə bacarığı kimi şərtlərdən aslıdır.Məlumat mübadiləsi müştəri tərəfdə veb brauzer,TCP/IP və serverdə HTTP Hyper-Text Transfer Protocol şəbəkə protokolları vasitəsi ilə həyata keçirilir.İnternet yeganə şəbəkədir istənilən insan ondan istifadə edər bu xidmətləri Provayder təmin edir.İnternet üzrə məlumat mübadiləsi zamanı mühafizə təhlükəsizlik protokolları

vasitəsi ilə yerinə yetirilir.İnternet üzərindən verilənlərin təhlükəsiz ötürülməsini təmin edən geniş istifadə olunan protokollarına aşağıdakılar aiddir.

- SSL
- SET
- İPSEC

SSLSecure Socket Layer-verilənləri şifrələnmiş,kriptoqrafik vasitələrdən istifadə edərək ötürür.SSL protokolu məlumatın tamlığına ,etibarlı çatdırılmasına təminat verir.SSl protokolu simmetrik və assimetrik alqoritmlərin birləşməsi zamanı yaranmışdır.SSl protokolunun üstünlüyü onun sadə və rahat olmasındadır.SSl protokolunun çatışmazlığı kimi məlumat alan tərəfin autentifikasiya olmamasıdır belə ki məlumat cinayətkarında əlinə keçirilə bilər.

SETSecurity Electronics Transaction-əsəsən bank sahəsində tranzaksiya əməliyyatları zamanı istifadə olunur.Əsasən müştərilərin plastik kartlardan istifadəsi zamanı təhlükəsiz ödəmələri həyata keçirmək üçün bu kimi standartların istifadəsi əhəmiyyətli olur və əsas üstünlüyü rəqəmsal sertifkatlardan istifadə olunmasıdır.SET protokulu verilənlərin tamlığını,məxfiliyini,etibarlığını qoruyur.Bu protokoldan istifadə etməzdən əvvəl tərəflər sertfikasiya mərkəzlərindən sertifkat əldə etməlidir.

IPSec- protokolu TCP/IP protokoluna əlavə kimi sayılır ,burada əsasən IP v.6 standartından istifadə edilir.Protokol IP şəbəkə səviyyəsində rəqəmsal mübadilə üsulunu dəstəkləyir. Protokol vasitəsi ilə ikitərəfli şifrələmə üsulunu tədbiq etməklə informasiyanın müdafiə olunmasını həyata keçirmək mümkündür. IP paketlərinin həqiqiliyini və şifrələnməsini təsdiq edir. Bundan istifadə edən təşkilatlar İnternetdə özlərinə məxsus xüsusi virtual şəbəkə yaratmışlar.[2,səh-321]

3.3 Şəbəkədə verilənlərin kriptoqrafik qorunması

Kritoqrafiyanın tarixi insan dilinin tarixi ilə eyni yaşdadır.Bundan başqa ilkin olaraq yazı özü özlüyündə kriptoqrafik sistem idi,belə ki yalnızelit insanlar yazı yazmaq qabiliyyətinə malik idi.

Kriptoqrafiyanınməxfi yazı inkişafına müharibələr təkan verdi.Yazılı əmrlər və hesabatlar şifrələnirdi ki,kuryerin düşmənlər tərəfindən ələ keçirilməsi zamanı informasiya əldə oluna bilməsin. Məsələn, Roma imperatoru Sezar hərbi və şəxsi yazışmalarında bir şifrə istifadə etdi, mahiyyəti latın əlifbasında hər hərfi əlifbanın sonrakı hərfi ilə əvəz etmək idi.Sezar Romada şifrələnmiş şəkildə qazandığı qələbə haqda dostuna belə bir məlumat vermişdir: VENI, VIDI, VICI, gəldim, gördüm , qələbə qazandım.

Təxminən kriptoqrafiya ilə eyni zamanda kriptoanalizdəşifrələrin açılması inkişaf etməyə başladı.

Kriptoqrafiyanın tarixini 4 mərhələyə ayırmaq olar:sadə kriptoqrafiya;formal kriptoqrafiya,elmi kriptoqrafiya,elmi kriptoqrafiya.

Sadə kritoqrafiyaya XVI əsrin əvvəlləri əsasən istənilən sadə,elementar şifrələmə mətni aiddir. İlkin mərhələdə məlumatları qorumaq üçün kriptoqrafiya ilə əlaqəli lakin eyni olmayan kodlaşdırma və steganoqrafiya metodlarından istifadə edilmişdir.

İstifadə olunan şifrələrin əksəriyyəti permutasiya və ya mono-əlifba əvəzetmə səviyyəsinə enmişdir.İlk qeydə alınan nümunələrdən biri sezar şifrəsidir hansı ki mənbə mətnin hər hərfini əifba sirasındakı mövqeyinə görə digəri ilə əvəz edilməsidir.Digər bir şifrə, müəllifliyi Yunan yazıçısı Polybiusa aid olan Polybian kvadratıdır, kvadrat əlifba cədvəli ilə təsadüfi doldurulurmaqla Yunan əlifbası üçün 5x5 ölçüdə həyata keçirilən ümumi mono-əlifba əvəzedicisidir.Mənbə mətninin hər bir hərfi altındakı kvadratda olan hərf ilə əvəz olunur.

Formal kriptoqrafiya mərhələsi XV əsrin sonu - XX əsrin əvvəli-formallaşdırılmış və nisbətən şifrələrin mexaniki kriptoanalizinə dayanıqlı olması ilə

bağlıdır. Avropa ölkələrində bu, İntibah dövründə, elmin və ticarətin inkişafı məlumatları qorumağın etibarlı yollarına tələbat yarandığı zaman baş verdi. Bu mərhələdə vacib bir rol, mono-əlifba əvəzetməsini təklif edən birincilərdən olan İtalyan memar Leon Batista Albertiə aiddir. Diplomat Blez Viginerin adını almış bu şifrə, açarla birlikdə mənbə mətninin hərflərini ardıcıl olaraq əlavə etmək dən ibarət idi proseduru xüsusi cədvəldən istifadə etməklə asanlaşdırmaq olar. Onun Şifrə haqqında traktat əsəri kriptologiya üzrə ilk elmi əsər hesab olunur. O dövrdə tanınmış şifrələmə alqoritmlərini ümumiləşdirən ilk nəşrlərdən biri İohann Trisemusun « Poliqrafiya » əsəri idi . Ona iki kiçik, lakin əhəmiyyətli bir kəşfə sahibdir: bir polybian kvadratını doldurmaq yolu və bigrams .

Mono- əlifba ilə əvəzlənmənin sadə, lakin dayanıqlı yolu bigramların dəyişdirilməsi, XIX əsrin əvvəllərində Charles Wheatstone tərəfindən kəşf edilmiş Playfer şifrəsidir.Ona həmçinin cüt kvadrat şifrələməsi inkişafı aiddir.Playfer və Uitston şifrələri birinci dünya müharibəsinə kimi istifadə olunurdu çünki onlar şifrələrin əl ilə açılmasına az dayanıqlı idi.

XIX əsrdə Hollandiyalı Kirkhoff, bu günə qədər aktual olan kriptosistemlərə dair əsas tələbi ifadə etdi: **şifrələrin məxfiliyi alqoritmə deyil, açarın təhlükəsizliyinə əsaslanmalıdır.**

Elmi kriptoqrafiyayadək kriptoqrafiyanın dayanıqlığı və şifrələmə prossesini avtomatlaşdırmağı təmin edən sistem fırlanan kriptoqrafik sistem oldu. İlk belə sistemlərdən biri 1790-cı ildə ABŞ-ın gələcək prezidenti Tomas Jefferson tərəfindən icad edilmiş mexaniki maşındır.

20-ci əsrin əvvəllərində fıralanan maşınlar geniş yayıldı. İlk praktik olaraq istifadə edilən maşınlardan biri 1917-ci ildə Edvard Hebern tərəfindən hazırlanan və Artur Kirş tərəfindən təkmilləşdirilmiş Alman Enigması idi.Bu tip maşınlardan ikinci dünya müharibəsi dövründə aktiv istifadə olunurdu. Alman Enigma maşınından əlavə Sigaba ABŞ, Turex Böyük Britaniya, Qırmızı, Narıncı və Bənövşəyi Yaponiya

cihazlarından da istifadə edilmişdir. Rotor sistemləri rəsmi kriptografiyanın zirvəsidir, çünki çox güclü şifrələri həyata keçirmək nisbətən asandır.

Elmi kriptoqrafiyanın XX əsrin 30-60 cı illəri əsas fərqləndirici xüsusiyyəti kriptoqrafiyanın ciddi riyazi əsaslandırılma ilə kriptosistemlərin ortaya çıxmasıdır. 30-cu illərin əvvəllərində kriptologiyanın elmi əsasını təşkil edən riyaziyyat bölmələri nəhayət formalaşdı: ehtimal nəzəriyyəsi və riyazi statistika, ümumi cəbr, alqoritmlər nəzəriyyəsi, informasiya nəzəriyyəsi, kibernetika fəal inkişaf etməyə başladı. Klod Şennonun Məxfi sistemlərdə ünsiyyət nəzəriyyəsi əsəri kriptoqrafiya və kriptoanalizin elmi bazasını təşkil etdi.O zamandan bəri **KRİPTOLOGİYA** kryptos-məxfi,logos-təlim-məlumatın məxfiliyini qorumaq üçün onun dəyişdiriləsi elmidir.1949-cı ilə dək kriptoqrafiyanın və kriptologiyanın inkişaf mərhələsini qeyri-elmi adlandırırdılar.Şennon dayanıqlı kriptosistem yaratmaq ehtimalını əsaslandırdı. 60-cı illərdə aparıcı kriptoqrafiya məktəbləri rotor kriptosistemləri ilə müqayisədə daha sabit olan blok şifrələrin yaradılmasına yaxınlaşdı, lakin bunlar yalnız rəqəmsal elektron cihaz şəklində həyata keçirilə bilərdi.

Kompüter kriptovalyutası XX əsrin 70-ci illərindən əl və mexaniki şifrələrə nisbətən daha yüksək kriptoqrafik gücə malik bir neçə sifarişlə yüksək kriptoqrafik güc təmin edən kriptosistemləri tətbiq etmək üçün kifayət qədər tutumlu hesablama vasitələrinin yaranması ilə meydana geldi.

Blok şifrələri - güclü və yığcam hesablama vasitələrinin meydana gəlməsi ilə praktik tətbiqi mümkün olan kriptosistemlərin birinci sinifi oldu. 70-ci illərdə Amerikada DES şifrələmə standartı hazırlanmışdır 1978-ci ildə qəbul edilmişdir.

Müəlliflərindən biri Horst Feistel blok şifrələrinin modelini təsvir etdi, bunun əsasında digər daha sabit, simmetrik kriptosistemlər həmçinin milli standart şifrələmə QOST 28147-89 inşa edildi. DES-in meydana gəlməsi ilə kriptoanaliz zənginləşdirildi və Amerikan alqoritminə hücumlar üçün bir neçə yeni növ xətti, diferensial və s. kriptoanaliz yarandı, praktik həyata keçirilməsi yalnız güclü hesablama sistemlərinin yaranması ilə mümkün oldu.

70-ci illərin ortalarında müasir kriptoqrafiyada əsl irəliləyiş oldu - tərəflər arasında gizli açarın ötürülməsini tələb etməyən asimmetrik kriptosistemlərin meydana çıxdı. Burada başlanğıc nöqtəsi, Vitfield Diffie və Martin Hellman tərəfindən 1976-cı ildə Müasir kriptoqrafiya sahəsindəki yeni meyllər adı altında nəşr olunan əsər sayılır. İlkin olaraq əvvəlcə gizli açarı mübadilə etmədən şifrəli məlumat mübadiləsi prinsiplərini formalaşdırdı. Asimmetrik kriptovalyutalar ideyasından asılı olmayaraq, Ralph Merkley yaxınlaşdı. Bir neçə il sonra, Ron Rivest, Adi Şamir və Leonard Adleman, gücü böyük priyomların faktorlaşdırılması probleminə söykənən ilk praktik asimmetrik kriptovalyutası olan RSA sistemini kəşf etdilər. Asimmetrik kriptosistem ideyasından asılı olmayaraq, Ralph Merkley yaxınlaşdı. Bir neçə il sonra, Ron Rivest, Adi Şamir və Leonard Adleman, gücü böyük sadə ədədlərin faktorlaşdırılması probleminə söykənən ilk praktik asimmetrik kriptosistemi olan RSA sistemini kəşf etdilər. Asimmetrik kriptoqrafiya dərhal bir neçə yeni tətbiq sahəsini açdı, xüsusən də elektron rəqəmsal imza sistemləri və elektron pullar.

80-90-cı illərdə kriptoqrafiyanın tamamilə yeni istiqamətləri ortaya çıxdı: ehtimal şifrələmə, kvant kriptoqrafiyası və s. Simmetrik kriptosistemlərin təkmilləşdirilməsi vəzifəsi aktual olaraq qalır. 80-90-cı illərdə SAFER, RC6 və s. hazırlanmış və 2000-ci ildə beynəlxalq konkursdan sonra ABŞ-ın yeni milli şifrələmə standartı AES qəbul edilmişdir.

Kriptoqrafiya məxfiliyin təmin edilməsi və məlumatın bütövlüyünün izlənməsi üçün ən güclü vasitələrdən biridir. Bir çox cəhətdən, proqram və aparat təhlükəsizliyi tənzimləyiciləri arasında mərkəzi yer tutur. Məsələn, fiziki cəhətdən qoruması çox çətin olan kompüterlər üçün yalnız kriptoqrafiya oğurluq halında da məlumatların məxfiliyinə zəmanət verə bilər. [4]

Kriptologiya- məlumatı çevirməklə qorumağın riyazi metodlarını öyrənən bir elmdir,əsasən məlumatları 3-cü tərəfin ələ keçirməsindən qoruyur.Kriptologiyanın 2 istiqaməti var- *Kriptoqrafiya və Kriptoanaliz.*

Kriptoqrafiya məlumatların konfidensiallığını və həqiqiliyini təmin etməklə, çevrilmə üsullarını öyrənir.

Məxfilik dedikdə, əlavə məlumatı açar bilmədən dəyişdirilmiş məlumatı əldə etməyin mümkünsüzlüyü nəzərdə tutulur.

Məlumatın **audentifikasiyası** müəllifliyin həqiqiliyindən və bütövlükdən ibarətdir.

Kriptanaliz açarları bilmədən məlumatların məxfiliyini və həqiqiliyini pozmağın riyazi metodlarını özündə birləşdirir.

Bir çox əlaqəli, lakin kriptoloji olmayan bilik sahələri var.Beləliklə *steganografiya* informasiya massivlərində informasiyanın gizliliyini təmin edir.Təsadüfi təsirlərə məruz qaldıqda informasiyanın tamlığını səhvlərə dayanıqlı şifrələmə nəzəriyyəsi təmin edir. Nəhayət, kriptologiya ilə əlaqəli bir sahə informasiyanın sıxılması riyazi metodları aiddir.

Müasir kriptovalyutaya dörd əsas bölmə daxildir:simmetrik kriptosistem;assimetrik kriptosistem;elektron imza sistemləri;açarların idarə edilməsi sistemi.

Kriptoqrafik metodlardan istifadənin əsas sahələri məxfi məlumatların rabitə kanalları vasitəsilə ötürülməsi, ötürülən mesajların identifikasiyası, məlumatların sənədlər, verilənlər bazaları şifrəli formada bazada saxlanmasıdır.

Şifrələnən və yenidən şifrələnən ,həmçinin elektron imzalara aid informasiya müxtəlif əlifba mətnlərində nəzərdən keçirilir.

Əlifba- məlumat kodlaşdırmaq üçün istifadə olunan məhdud simvollar toplusudur.

Mətn mesaj - əlifba elementlərinin sifariş edilmiş dəsti. Müasir informasiya sistemlərində istifadə olunan əlifbalara misallar:

- Z_{33} əlifbası - Rus əlifbasının 32 hərfi ё istisna olmaqla və boşluq;

- əlifba Z_{256} - standart ASCII və KOI-8 kodlarına daxil edilmiş simvollar;
- ikilik əlifba – $Z_2 = \{0,1\}$;
- səkkizlik və onaltılıq əlifba;

Kodlar və şifrlər elektron hesablama maşınlarının yaranmasından çox əvvəl istifadə edilmişdir. Nəzəriyyə baxımından kodlar və şifrələr arasında dəqiq bir fərq yoxdur. Ancaq praktikada bunlar arasındakı fərq olduqca aydındır. **Kodlar**, şifrəli mətni semantik elementlərə sözlər və hecalar bölərək dil elementləri üzərində işləyir lakin şifrədə həmişə iki element mövcuddur: alqoritm və açar.

Alqoritm, ixtiyari böyük mətni şifrələmək üçün nisbətən qısa açardan istifadə etməyə imkan verir.

Kriptologiyada istifadə olunan bir sıra terminləri müəyyənləşdirək.

Şifrə dedikdə, açıq məlumatlar toplusunun kriptoqrafik dəyişmə alqoritmi ilə təyin edilmiş şifrəli məlumat toplusuna çevrilmə məcmusu kimi başa düşülür.

Şifr -açıq mətn dəstinin ,çevrilmiş mətnlə əlaqəsidir və indexsləşdirilmiş açara malik olur $\{Fk : X \rightarrow S, k \in K\}$.

Kriptoqrafiya sistemi, ya da şifrə, düz mətnin şifrələnmiş T çevrilmiş bir ailəsidir.Bu ailənin üzvləri açar adlandırdığımız k ilə uyğunlaşır.T_k çevrilməsi alqoritm və k açarının dəyəri ilə müəyyən olunur.

Açar-alqoritmin bəzi xüsusi gizli vəziyyətidir,uyğun alqoritmə uyğun olan variantlardan birinin seçilməsidir. Açarın gizliliyi, mənbə mətnini şifrələnmiş vəziyyətdə bərpa etməyin mümkün olmamasını təmin etməlidir.

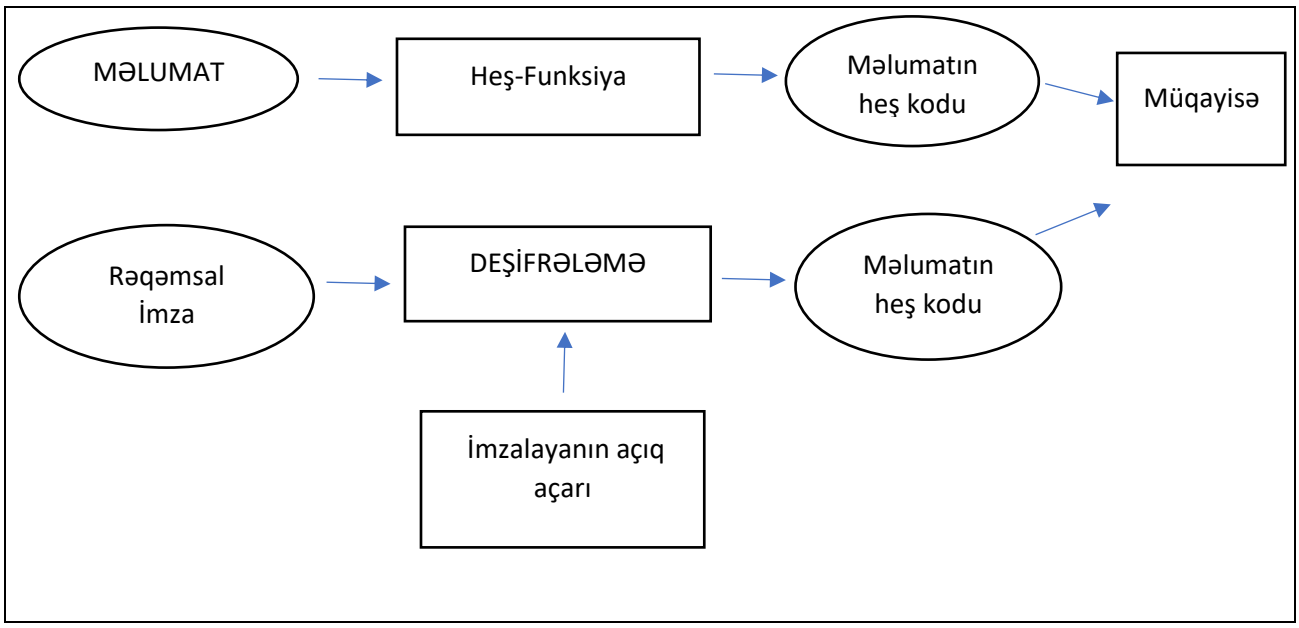
K açarlar çoxluğu-açarın mümkün dəyərlər toplusudur. Tipik olaraq, açar əlifbanın ardıcıl hərflərindən ibarətdir. *Parol* əlifbanın hərflərinin gizli ardıcıllığıdır, lakin şifrələmə açar kimi üçün deyil, subyektlərin identifikasiyası üçün istifadə olunur.

Simmetrik kriptosistemlərdə-açar həm şifrələmə ,həm də deşifrələmə üçün istifadə olunur.

Assimetrik kriptosistemlərdə isə iki bir biri ilə riyazi cəhətdən bağlı olan açıqpublic və qapalıməxfi açarlardan istifadə olunur.İnformasiya açıq hamıya məlum olan açarla şifrələnir,lakin informasiya qapalı yalnız informasiyanı qəbul edənə məlum olan açarla deşifrələnir.

Açar paylama və *açar idarəetmə* terminləri məlumat emalı sisteminin proseslərinə aiddir.

Elektron rəqəmsal imza, mətnə əlavə edilmiş bir kriptoqrafik çevrilmədir ki, bu da başqa istifadəçiyə mətn alarkən məlumatın müəllifliyini və bütövlüyünü yoxlamağa imkan verir.Elektron imzadan əsasən internet banking,elektron portala giriş və s xidmətlərdə istifadə olunur.İnternet banking nümuməsində baxsaq online ödəniş zamanı tərəflərdən biri imzaya uyğun rekvizitləri daxil etməlidir sonra isə adentifikasiya həyata keçirilir.Əsasən elektron imzaya indiki zamanda daha çox ehtiyyac var belə ki Corono virus pandemiyasının yayıldığı zaman ,evdən çıxmaq məhdudiyyətlərinin qoyulması və ticarət mərkəzlərinin işləməməsi ticarət online keçməsinə səbəb oldu.Bu zaman informasiyanın təhlükəsizliyi daha çox qlobal məsələyə çevrilir,beləki odəniş edən zaman kartın rekvizitləri oğurlana bilər bu zaman təhlükəsizlik protokollarından istifadə etmək məqsədə uyğun olur.Bundan başqa elektron mağazalar yaranır vitrini internetde olan mağazalar onlarda təhlükəsizlik problemini həll etməlidirlər.Elektron imzadan istifadə isə müəllifi tam olaraq audentifikasiya etməyə imkan verir.Proses aşağıdakı cədvəldə göstərilib



Cədvəl 4

Məlumatın şifrələməsi açıq məlumatların şifrdən istifadə edərək şifrələnmiş hala çevrilməsi prosesidir,məlumatın şifrədən azad olması isə qapalı mətni şifrədən istifadə edərək açılmasıdır. Açıq məlumatlar termini əvəzinə açıq mətn və mənbə mətnləri, şifrlənmiş məlumatlar əvəzinə qapalı mətni istifadə olunur.

Deşifrələmə- məlumatların qapalı mətndən açıq mətnə qeyri müəyyən açar ,naməlum alqoritm və s vəziyyətdə çevirən kriptoanaliz metodudur.

Şifrələmə məlumatların şifrələnməsi prosesidir. Lakin, kodlaşdırma ifadəsini şifrələməyə sinonim kimi istifadə etmək düzgün deyil və şifrə yerinə kod kodlaşdırma, məlumatları simvol əlifba hərfləri şəklində təmsil etmək kimi başa düşülür.

Qammalaşdırma-açıq məlumatlara qamma şifrə qanununun tədbiq edilməsidir.

Gamma şifrəsi - açıq məlumatların şifrlənməsi və şifrələnmiş məlumatların şifrələnməsi üçün müəyyən bir alqoritm tərəfindən yaradılan təsadüfi ikili ardıcıllıqdır.

İmitasiya mühafizəsi - saxta məlumatların tətbiqindən qorunma. İmitasiya qorumasını təmin etmək üçün şifrəli məlumatlara müəyyən bir qayda ilə açıq məlumatlardan və bir açardan əldə edilmiş sabit uzunluğa aid məlumatlar ardıcıllığı daxil edilir.

Kriptoqrafik qoruma - məlumatların şifrələmə və ya əlavə etmə yolu ilə çevrilməsi kimi başa düşülən kriptoqrafik çevrilmənin köməyi ilə məlumatların qorunmasıdır.

Sinxronizasiya - kriptoqrafik çevrilmə alqoritminin ilkin açıq parametrləri.

Şifrələmə tənliyi – açıq məlumatlardan kriptoqrafik alqoritmlər sayəsində çevrilərək qapalı məlumatların yaranması və əks prosesi izah edən nisbətdir.

İşlədiyim şirkətinin nümunəsində baxsaq məsələyə: belə ki bulud texnologiyasının geniş yayılması ölkəmizdədə onun tədbiqini genişləndirdi və şirkətimizdə bulud texnologiyasının istifadəçilərindəndir.Məlumatların oğurlanmasına risk varmıdır? - Bəli ,çünki tam ideal sistemə malik olmaq mümükün deyildir risklər hər zaman mövcuddur .Lakin dəymiş zərərin miqdarını azaltmaq üçün öncədən tədbirlər görülməlidir.Bu kimi tədbirlədən biri şifrələmədir.Cədvəllərdə saxlanılan vacib məlumatlar,məsələn satış,ambarda olan məhsulların sayı,muhasibat hesabatları,əmək haqqı encrupted-şifrələnmiş şəkildə saxlanılır.Bundan başqa server level səviyyəsində yetkilər vasitəsilə əlçatanlıq nizamlanır.Belə ki əməliyyatçı olan işçinin hesabatlara əl yetənliyi olmur və s.Şəbəkə də qorunma isə firewall,VPN vasitəsilə yerinə yetilir .Beləki şirkətə məxsus lokal şəbəkəyə qoşulmaq uçun userlər açılıb yetki verilir.Şirkətdən kənar şəbəkədən qoşulmaq VPN vasitəsi ilə həyata keçir.Bundan başqa kompüterlərə antiviruslar yazılır və virusun olub olmaması yoxlanılır,çünki lokal kompüterdə virus varsa serverə yoluxması an məsələsi olur.Sosial şəbəkələr və s giriş məhdudlaşır.

Kriptoqrafik sistemlərə olan tələblər

Məlumatların bağlı verilənlərə keçməsinin kriptoqrafik prosesi həm proqram, həm də aparat vasitəsi ilə həyata keçə bilər. Aparatın tətbiqi xeyli bahadır, eyni zamanda yüksək performans, sadəlik, təhlükəsizlik və s. üstünlükləri var.Proqramın tədbiqi daha praktikdir belə ki,istifadə etmək daha rahat olur.

Tədbiq üsulundan asılı olmayaraq, müasir kriptoqrafik məlumat qoruma sistemləri üçün aşağıdakı ümumi tələblər tərtib edilib:

- şifrənin kriptoanalizə qarşı elə dayanıqlı olmalıdır ki, yalnız mətn açarların tam axtarış tapşırığını həll etməklə açıla bilsin və ya müasir kompüterlərin imkanlarından kənara çıxmsın hesablamaların paralelləşməsi nəzərə alınmaqla və ya bahalı hesablama sistemlərinin yaradılmasını tələb etsin;
- kriptoqrafik dayanıqlıq alqoritmin gizliliyi ilə deyil, açarın gizliliyi ilə təmin olunur;
- Şifrəli mətn yalnız açar məlum olduqda oxuna bilən olmalıdır;
- Cinayətkar kifayət qədər böyük miqdarda mənbə məlumatlarını və müvafiq şifrələnmiş məlumatları bilsə belə şifrə dayanıqlı olmalıdır;
- açar və ya mənbə mətnində cüzi bir dəyişiklik şifrələnmiş mətninin görünüşünün əhəmiyyətli dərəcədə dəyişməsinə səbəb olmalıdır;
- şifrələmə alqoritminin struktur elementləri dəyişkən olmamalıdır;
- şifrələnmiş mətn mənbə mətninin miqdarından əhəmiyyətli dərəcədə çox olmamalıdır;
- Şifrələmə prosesində mesaja daxil edilmiş əlavə bitlər tamamilə və etibarlı şəkildə şifrələnmiş mətndə gizlədilməlidir;
- Şifrələmə prosesində baş vermiş səhvlər informasiya itkisinə səbəb olmamalıdır;
- Şifrələmə prosesində istifadə olunan açarlar arasında sadə və asanlıqla qurulan asılılıqlar olmamalıdır;

- Mümkün olan açar çoxluğundan seçilmiş açar digərləri ilə bərabər kriptoqrafik gücü təmin etməlidir ;
- Şifrələmə müddəti çox olmamalıdır.
- şifrələmə dəyəri bağlanacaq məlumatın dəyərinə uyğun olmalıdır.

3.4 İnformasiya kriptoanalizinin nəticələri

Kriptoanalizdə əsas rolu cinayətkar oynayır kimin ki,məqsədi şifrələnmiş mətni oxumaq onu saxtalaşdırmaqdır.

Qayda pozucuları ilə əlaqədar riyazi və digər modellər əsasında qoyulan bir sıra fərziyyələr var:

1. Təcavüzkar şifrələmə alqoritmini və müəyyən bir vəziyyətdə onun reallaşdırmaq yolunu bilir, lakin gizli açarı bilmir.
2. Təcavüzkara şifrəli mətnlər məlumdur,həmçinin bəzi mənbə mətlərinədə girişi ola bilər hansının ki şifrələnmiş varinatını bilir.
3. Təcavüzkarın ixtiyarı hesablama, insan və digər mənbələrə malikdir, həcmi kriptoanaliz nəticəsində əldə ediləcək məlumatın potensial dəyəri ilə əsaslandırılır.

Kriptoanaliz metodlarından istifadə edərək açarı hesablamaq ,şifrəli bir məlumatı oxumaq və ya saxtalaşdırmaq cəhdi *kriptohücum* və ya *şifrəyə hücum* adlanır. Uğurlu bir kripto hücumuna hack-sındırmaq deyilir.**Kriptoqrafik dayanıqlıq**-açarı bilmədən şifrənin açılmasına qarşı dözümlülükdür.

Kriptodayanıqlıq göstəriciləri-istənilən kriptosistemin əsas parametridir.Kriptoqrafik dayanıqlığın göstəricisi kimi bunları göstərə bilərik:

- Bütün mümkün açarların sayı və ya verilən resurslarla müəyyən bir müddətdə açar seçmə ehtimalı;
- əsas açarların və ya mənbə mətninin hesablanması dəyəri.

Bu göstəricilər mümkün kriptoqrafik hücümların səviyyəsini nəzərə almalıdır.

Lakin məlumatların kriptoqrafik üsullarla qorunmasının effektivliyi yalnız şifrənin kriptoqrafik gücünə deyil, həm də bir çox digər amillərə, o cümlədən kriptosistemlərin tətbiqinə və insan amilinə bağlıdır.Məsələn əlində vacib informasiya olan insana rüşvət verib onu almaq ,şifrəni qırmaq üçün yaradılacaq superkompüterlərdən ucuzdur.

Müasir kriptoanaliz ehtimal nəzəriyyəsi və riyazi statistika, cəbr, say nəzəriyyəsi, alqoritmlər nəzəriyyəsi və bir sıra digər nəzəriyyələrə əsaslanır.Kriptoanalizin bütün metodları 4 istiqamətə ayrılır.

1. Statistik kriptoanaliz statistik qanunlara əsaslanan kriptosistemlərin mənbə və şifrəli məlumatlarının hack edilməsi imkanlarını araşdırır. Onun istifadəsi mürəkkəbdir beləki şifrələmədən əvvəl məlumatların əvvəlcədən sıxılması və ya qammalaşdırma halında, böyük uzunluqdakı yalançı təsadüfi ardıcıllıqlar istifadə olunur.
2. Cəbr kriptoanalizi kriptoqrafik alqoritmlərdə riyazi cəhətdən zəif elementləri axtarır. Məsələn, 1997-ci ildə elliptik sistemlərdə kriptoanalizi çox asanlaşdıran açarlar çoxluğu aşkar edilmişdir.
3. Diferensial kriptoanaliz- şifrə mətnindəki dəyişikliklərin mənbə mətnindəki dəyişikliklərdən asılılığının təhlili əsasında yaradılıb və ilk dəfə Murphy tərəfindən istifadə edilmiş, Beham və Shamir tərəfindən DES-ə hücum etmək üçün təkmilləşdirilmişdir.
4. Xətti kriptoanaliz-mənbə və şifrə mətni arasındakı xətti yaxınlaşma axtarışına əsaslanan bir üsuldur. Matsui tərəfindən təklif edilmiş ilk dəfə DES-in sındırmaq üçün istifadə olunmuşdur.

Kriptosistemlərin Hack -sındırılması təcrübəsi göstərir ki,əsas metod frontal hücumdur açarı yoxlayır.

İnformasiya səviyyəsindən aslı olaraq kriprto hücumun bir neçə səviyyəsini fərqləndirirlər.Mürəkkəbliyin artmasına görə kripto hücümların aşağıdakı növləri qeyd olunur.

Şifrəli Mətnə Hücum KA1 Səviyyə - Təcavüzkara bütün və ya bəzi şifrəli məlumatlar əl çatandır .

Mənbə mətni - şifrəli mətn cütlüyünə hücum KA2 səviyyəsi - təcavüz edən şəxs üçün bütün və ya bir neçə şifrəli məlumat və müvafiq mənbə məlumatları əl çatandır.

Seçilmiş cüt mənbə mətni - şifrəli mətn- ə hücum edin. KA3 Səviyyə – Təcavüz edən mənbə mətnini seçmək, bunun üçün şifrəli mətni əldə etmək və aralarındakı asılılıqların təhlilinə əsaslanaraq açarı hesablamaq imkanına malikdir.

Müasir kriptosistemlər KA3 Səviyyəyəyə belə dayanıqlıdır.

Məlumatların bağlanmasının kriptoqrafik metodlarının təsnifatı

Hal-hazırda çox sayda məlumatın kriptoqrafik bağlanması üsulları məlumdur. Şifrələmə metodlarının təsnifatı kriptoqrafik alqoritmlər aşağıdakı meyarlara uyğun olaraq həyata keçirilə bilər:

Açarların tipinə görə: simmetrik kriptoqrafik alqoritmlər; asimmetrik kriptoqrafik alqoritmlər;

İnformasiya blokunun ölçüsünə görə: axın şifrələri; blok şifrə;

Məlumatlarda yaranan zərərlərin təbiəti ilə: dəyişdirmə permutasiya metodu, əvəzetmə metodu; analitik metodlar, aşqar metodları gamming, birləşdirilmiş metodlar.

Kodlaşdırma semantik, simvolik, birləşdirilmişkobinə ola bilər.

Digər yollarla məlumatların bağlanması: steganoqrafiya, sıxılma / genişləndirmə, hissələr ayırma metodlarından istifadə etməklə əldə edilə bilər.

Nəticə

İnformasiyanın qorunmasının inkişaf tarixi, digər elm və texnologiya sahələri ilə əlaqələri nəzərdən keçirilir, informasiyanın qorunmasının əsas anlayışları və tərifləri təqdim olunur, eyni zamanda informasiya təhlükəsizliyi sistemlərinin təşkili prinsipləri və tələbləri əsaslandırılır.

Parol idarəetmə siyasəti, aktiv audit, habelə təhlükəsizlik hadisələrinin həlli və proqramların idxalına nəzarət məsələləri geniş tədqiq olunub .

İnformasiya təhlükəsizliyini təmin etmək missiyası çətindir, bir çox hallarda qeyri-mümkündür, lakin həmişə vacibdir.

Dissertasiya kriptoqrafik məlumatların qorunması məsələlərini araşdırır, əsas anlayışlar və tərifləri təqdim edir, istifadə olunan şifrələrin alqoritmlərini nəzərdən keçirir və müqayisəli təhlil aparır.

Təkliflər bundan ibarətdir ki,əgər bizdə dünya standratlarına uyğun informasiya təhlükəsizliyi sistemi yaratsaq elekton biznesdən daha çox faydalana bilərik.

Prezdentimiz İlham Əliyev cənablarının uğurlu siyasəti nəticəsində son illərdə elektron sistemin inkişafında yüksəliş mövcuddur.Buna misal ASAN xidmət mərkəzlərinin,DOST mərkəzlərinin və s yaradılmasını göstərə bilərik.Yaradılmış elektron sistem digər inkişafda olan ölkərə nümunə oldu.Bu sistemlərdə məxfilik,təhlükəsizlik yüksək səviyyədə təmin olunur.Son illər elektron imzanın tədbiqi nəticəsində bir çox dələduzluq hadisələri kəskin azalmışdır.

ƏDƏBİYYAT SİYAHISI

Azərbaycan dilində

1.Azərbaycan Respublikasının konsitusiyası

2.M.Əlizadə,H.Bayramov,Ə.Məmmədov İnformasiya Təhlükəsizliyi

3.Qasımov V.İnformasiya təhlükəsizliyinin əsasları.Bakı 2009

Rus dilində

4.V. Jelnikov. Papirusdan Kompüterə qədər kriptoqrafiya

5. Галатенко В.А. Основы информационной безопасности.

6. Завгородний В.И. Комплексная защита информации в компьютерных системах

7. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах.

8. Девянин П.Н., Михальский О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности

9. Галатенко В.А. Основы информационной безопасности.

10. Завгородний В.И. Комплексная защита информации в компьютерных системах.

11. Галатенко В.А. Основы информационной безопасности

12 Грибанов В.П., Калмыкова. Основы алгоритмизации и программирования,

13. Руководство по обеспечению безопасности информации от несанкционированного доступа на объектах вычислительной техники ВС.

14. Цветкова М. С., Великович Л. С. Информатика и ИКТ.

15.Иванова ,Пугачёв Объектноориентированное программировани.

16. Н,В.Макарова, В.Б.Волков Информатика

17 .Зегжда Д.П, Ивашко А,М. Основы безопасности информационных систем

Jurnallar və internet resursları

18. https://ks-211.blogspot.com/2015/06/informasiya-thluksizliyi.html

19.İnternet Week

20.Internatinal Week

21. https://en.wikipedia.org/wiki/Information_security#Risk_management

22. https://zeguro.com/blog/what-are-information-security-policies

РЕЗЮМЕ

После получения доступа к глобальной сети, проблема информационной безопасности становится самой глобальной проблемой мира. Сейчас в мире день ото дня увеличивается количество электронных бизнес-площадей. Основная проблема заключается в том, как защитить данные в сети интернет.
В моем исследовании я отметил несколько способов защиты. Наилучшими способами защиты данных в сети являются протоколы безопасности SSL, SET, IPSEC.
С последних лет в Азербайджанской Республике совершенствуются способы обеспечения безопасности. Электронное правительство применяется в Азербайджане. Эффективная координация деятельности субъектов общественных организаций, частного сектора, общественных организаций и граждан, вовлеченных в обеспечение информационной безопасности электронного правительства, зависит от своевременного и качественного обмена информацией между субъектами. Поэтому, основываясь на топологической структуре соответствующих информационных потоков и их анализе, можно перестроить систему координации и повысить ее эффективность. Для этой цели, чтобы смоделировать систему координации информационной безопасности электронного правительства, система разлагается на иерархическую четырехуровневую структуру и строится ее многоагентная сетевая модель.
Для достижения цели в этом направлении создаются координационные центры по кибербезопасности для государственного и частного сектора.

ABSTRACT

After get access to global network , Information security problem get the most global problem of the world. Now in the world increasing day by day amount of electron businees area.The main problem is that how to protect data at internet network.

İn my research case ,I noted some ways of protection.The best ways protect data in network is security protocolsSSL,SET,IPSEC.

Since recent years in Azerbaijan Republic is being improved ways of security. e-government is applied in Azerbaijan. Effective coordination of the activities of actors public organizations, private sector and citizens involved in ensuring the information security of e-government depends on the timely and quality exchange of information between actors. Therefore, based on the topological structure of the relevant information flows and its analysis, it is possible to reengineer the coordination system and increase its efficiency. For this purpose, in order to model the e-government information security coordination system, the system is decomposed into a hierarchical four-level structure and its multi-agent network model is built.

For acihive the goal in this direction, creates cyber security coordination centers for public, private sectors