AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ
AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

Əlyazması hüququnda

BABULLAZADƏ NURANƏ ASƏF QIZI
ƏLİYEV NƏSİB SÜBHAN OĞLU

"AZƏRPOÇT" MMC-NİN KORPORATİV ŞƏBƏKƏSİNDƏ KRİPTOMUHAFİZƏ ÜSULLARININ TƏDQİQİ

mövzusunda

MAGİSTRLİK DİSSERTASİYASI

İxtisas: 060627 – Elektronika, telekommunikasiya və radiotexnika mühəndisliyi

İxtisaslaşma: **Optik rabitə fizikası və texnikası,**
Radiorabitə radioverlişləri və televiziya

Elmi rəhbər: **t.ü.f.d., dosent R. S. Məmmədov**

BAKI-2023

MÜNDƏRİCAT

GİRİŞ

Mövzunun aktuallığı. Korporasiya termini latıncada “corporatio” sözündən götürülmüş və “birlik” anlamı daşıyır.Korporativ şəbəkə anlamı da müəyyən birliklər,idarə və müəssisələrin informasiya paylaşımı etməsi üçün formalaşdırılmış mürəkkəb strukturlardır.Şəbəkə formalaşdırılarkən əsas olan yüksək əlçatalığın təmini,informasiyanın təhlükəsiz paylaşımının təmini və performansın mümkün olduğu qədər yüksəldilməsidir.Günümüzdə istənilən profilə malik şirkət üçün onun kompüter şəbəkəsinin əhəmiyyəti çox önəmlidir.Çünki hazırda elektron sistemlər idarəetmənin mərkəzləşdirilməsi,ümumi resurslara çıxışı və bu kimi önəmli məsələləri özündə cəmləyir. Ümumiyyətlə, korporativ şəbəkə korporasiyada istifadə edilən müxtəlif tətbiqi proqramlar aralığında məlumat mübadiləsini həyata keçirən bir sistemdir. Korporativ şəbəkə

1. sistem və tətbiqi proqram təminatları,
2. şəbəkə adapterləri,
3. konsentratorlar (qarışdırıcılar),
4. kommutatorlar
5. marşrutlayıcılar,
6. kabel sistemi kimi komponentlərindən ibarət olur.

Müasir dünya iqtisadiyyatına dinamiklik, qeyri–stabillik, rəqabətliliyin artması, elmi –texniki tərəqqinin yüksəlişi, idarəetmə və iqtisadi prinsiplərinin inkişafı xassdır.

Effektivliyin artması ancaq ekstensiv yollarla arta bilməz, yəni ki, investisiya artımı və şöbə və filialları artırmaqla buna nail olmaq mümkün deyil. Əlavə investisiyallar istehsalın artımını və effektivliyin artmasını təmin etmir; eyni zamanda bunlar öz ardınca böyük xərcli əməliyyaları cəlb edir: hazırlıgın təşkilatı və kadrların istifadə olunması, xüsusi avadanlıqların hazırlanması və qurasdırılması və s., hansı ki bunların hər biri böyük bir layihədir; onların icrası üçün isə zaman, əmək və maliyyə vəsaiti tələb edir.

Təskilati strukturun, tərkibin və idarəetmə funksiyalarının düzgün müəyyən edilməsindən sonra təskilatın idarəetmə strukturunun düzgün inkişafa doğru yönəltmək

mümkündür. Bununla yanaşı elə bir model formalasdırmaq lazımdır ki, daim inkisaf etdirmək, xarici və daxili mühiti nəzərə alaraq onda dəyişikliklər etmək mümkün olsun.

Tədqiqatın məqsədi. Dissertasiya işinin əsas məqsədi Azərpoçt MMC-nın korporativ şəbəkəsində istifadə olunan kriptomuhafizə üsullarının tədqiq edilməsi və yeni təhlükəsizlik sisteminin işlənməsidir.

Tədqiqat obyekti. AzərPoçt MMC-nin korporativ şəbəkəsidir.

Tədqiqat predmeti. AzərPoçt MMC-nun korporativ şəbəkəsində kriptomuhafizə üsullarıdır.

Elmi yeniliyi. Disertasiya işində elmi yenilik kimi Azərpoçt MMC-nin korporativ şəbəkəsində istifadə olunan kriptomühafizə üsullarının daha güvənli olması üçün aşağıdakılar təklif edilmişdir.

1. İlkin olaraq daxili şəbəkədə təhlükəsizlik divarında Fortineti tətbiq edilməsi təklif edilmiş və işlənib hazırlanmışdır.
2. Daha sonra isə xarici şəbəkədə isə təhlükəsizlik divarında FG-401F tətbiqi təklif olunmuş işlənib hazırlanmışdır.

Bunun nəticəsi olaraq şəbəkənin layer 7 səviyyəsində də işləmə imkanı,bütün portları bağlayıb və yalnız lazım olan portları açmaq,Firewallda SSL decryption, inspection aktivləşdirmək – gələn və gedən trafiki oxumaq, analiz edilməsi,SD-WAN (Proqram təminatı ilə müəyyən edilmiş geniş sahə şəbəkəsi) dəstəkləməsi,Faylların filtirlənməsi,antivirus,web filtirlənməsi,daxili şəbəkəyə internet üzərindən təhlükəsiz qoşulmaq üçün vpn protokolundan istifadə etmə imkanı və şəbəkənin kriptomühafizəsi prosedurları daha da artırılmışdır. Bu prosedurlar əsasında FortiGate 600F seriyası, kampus və ya filial səviyyəsində yerləşdirilən orta ölçülü və böyük müəssisələr üçün Next Generation Firewall (NGFW) imkanları ilə tətbiq mərkəzli, genişlənə bilən və təhlükəsiz SD-WAN həllini təmin edir. Sadə, sərfəli və tətbiqi asan həlldə system-on-a-chip sürətləndirilməsi və sənayedə aparıcı təhlükəsiz SD-WAN ilə kiber təhlükələrdən qoruyur. Fortinet-in Təhlükəsizliyə əsaslanan şəbəkə yanaşması şəbəkənin yeni nəsil təhlükəsizliklə sıx inteqrasiyasını təmin edir.

Elmi nəşrlər. Dissertasiyanın əsas elmi nəticələri respublika miqyaslı bir elmi-texniki konfrans materiallarında bir məqalə nəşriyyata göndərilmişdir.

Tədqiqat işinin strukturu və quruluşu. Tədqiqat işi girişdən, 4 fəsildən və son olaraq əldə olunmuş nəticələrdən ibarətdir. Tədqiqat işinin sonunda istifadə olunmuş ədəbiyyatların siyahısı qeyd olunmuşdur.

Dissertasiya işində qoyulmuş elmi məsələlər, onun aşağıdakı fəsillərində sistemli şəkildə həlli edilmişdir.

Girişdə dissertasiyasının mövzusunun aktuallığı, məqsədi, qarşıya qoyulan və həll edilən məsələlər, tədqiqat metodları, işin elmi yeniliyi, praktiki dəyəri, müdafiəyə çıxarılan məsələlər, işin strukturu və həcmi işıqlandırılmışdır.

Birinci fəsildə daha çox AzərPoçt MMC-nin tarixi və bu günü haqqda ümumi ətraflı məlumatlar əks olunmuşdur**.**Xidmət göstərdiyi ölkələr, informasiya tamlılığının və məxfiliyinin təmini üsulları qeyd olunmuşdur.

İkinci fəsildə AzərPoçt-un korporativ şəbəkəsinin təhlükəsizliyi vasitələrilə idarəetmə məsələlər , informasiya təhlükəsizliyinin idarə edilməsi qaydaları və ən sonda mərkəzləşdirilimiş korporativ informasiya sistemləri təhlükəsizliyinin idarə edilməsi haqqında danışlmışdır.

Üçüncü fəsildə Azərpoçt MMC-də istifadə olunan şəbəkə avadanlıqları,əməliyyat sistemləri,şəbəkənin qurulması haqqında geniş şəkildə məlumat verilmişdir.Həmçinin korporativ şəbəkənin təsviri,VPN texnologiyasından və b. sistemlərindən də bəhs olunmuşdur.

Dördüncü fəsildə Azərpoçt MMC-nin Korporativ şəbəkəsində istifadə edilən kripmühafizə üsullarından,kriptoqrafiyanın əsaslarından,elktron rəqəmsal imza və həmçinin protokollordan bəhs olunmuşdur.

AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ
AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

Əlyazması hüququnda

BABULLAZADƏ NURANƏ ASƏF QIZI

“AZƏRPOÇT” MMC-nin korporativ şəbəkəsində kriptomuhafizə üsullarının tədqiqi

MAGİSTR DİSSERTASİYASI

İxtisas: 060627 –“Elektronika,telekommunikasiya və radiotexnika Mühəndisliyi”

İxtisaslaşma: Optik rabitə fizikası və texnikası

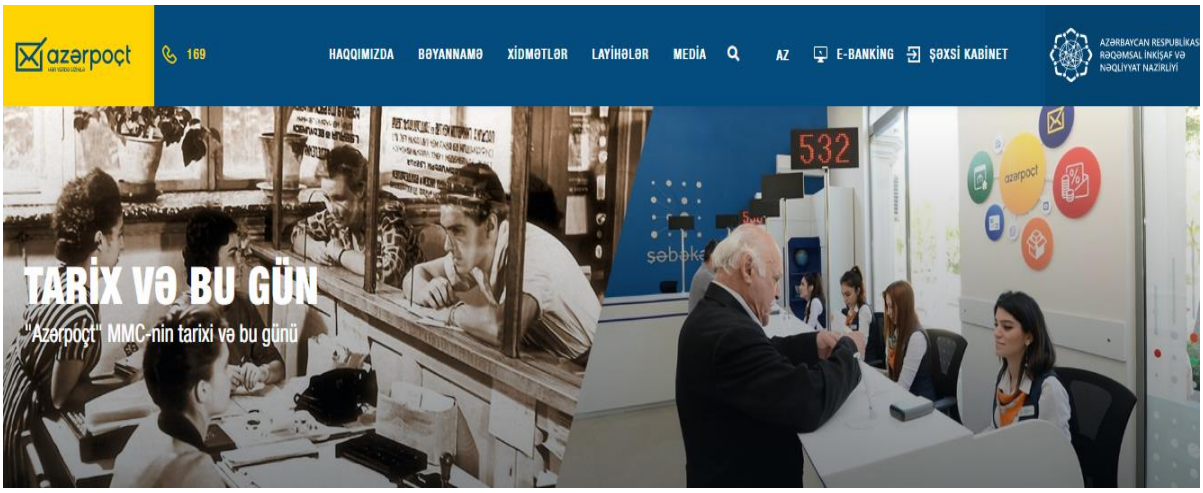
Elmi rəhbər: t.f.d., dos. R.S.Məmmədov

BAKI-2023

I FƏSİL. AzərPoçt MMC-də korporativ şəbəkə sisteminin təhlili

1.1. AzərPoçt MMC- nin tarixi və bu günü.Ümumi strukturu.

Bu dövr Azərbaycan üçün ən ağır və şərəfli dövr olan İkinci Dünya müharibəsinə təsadüf edir. Bu dövrdə poçt göndərişlərinin həcmi artdığından, əsgər məktublarının vaxtında düzgün ünvana çatdırılması böyük məsuliyyət və iradə tələb etdiyindən poçt işçilərinin üzərinə ikili məsuliyyət düşürdü. Belə çətinliklərə baxmayaraq, müharibə illərində poçt işçiləri üzərlərinə düşən bütün vəzifələri sədaqətlə yerinə yetirdilər. 1945-ci ildə Bakıda Beynəlxalq Poçt Xidmətinin yaradılması beynəlxalq poçt göndərişlərinin vaxtında daşınmasına, saxlanmasına və çatdırılmasına nəzarəti təkmilləşdirməyə imkan verdi.



Şəkil 1.1. AzərPoçt MMC-nin tarixi və bu günü

20-ci əsrin sonlarında keçmiş SSRİ-nin dağılması və respublikamızın müstəqillik əldə etməsi nəticəsində "Azərpoçt" rabitəsinin inkişafında yeni dövr başlandı [1,2,3,4].

2002-ci ildə "Azərpoçt" rabitə xidmətlərinin göstərilməsi proseslərini tənzimləyən ilk milli "Poçt Rabitəsi Qaydaları" hazırlanmış, müvafiq qaydada qeydiyyata alınmış və "AzərPoçt"un rabitə müəssisələri tərəfindən istifadəyə göndərilmişdir. Maliyyə xidmətlərinin göstərilməsi ilə bağlı 2004-cü ildə qəbul edilmiş və 2008-ci ildə əlavə və dəyişikliklər edilmiş "Poçt haqqında" Azərbaycan Respublikasının Qanunu Azərpoçt MMC-nin inkişafını daha da sürətləndirmiş və

şəbəkə vasitəsilə yeni xidmətlərin göstərilməsi üçün bir çox imkanlar yaratmışdır. Milli rabitə operatoru Azərpoçt tərəfindən. 2016-cı ildə Azərbaycan Rabitə və Yüksək Texnologiyalar Nazirliyinin qərarına əsasən, "Azərpoçt" üçün telekommunikasiya xidmətlərinin göstərilməsi Qaydaların"da dəyişikliklər edilmiş və "Azərbaycan Respublikasının Dövlət Qanunun"da müvafiq dəyişikliklər edilib reyestrinə daxil edilmişdir.

Ölkənin dövlət poçt operatoru olan "Azərpoçt" Məhdud Məsuliyyətli Cəmiyyəti bu gün respublikada ən böyük xidmət şəbəkəsinə malikdir və eyni zamanda bütün sektorlara münasib qiymətlərlə ənənəvi və qeyri-ənənəvi poçt xidmətləri və maliyyə poçtu xidmətləri göstərməyi bacarır. Əhali və hüquqi şəxslər. "Azərpoçt" filiallarının müasir standartlara uyğun kompüterləşdirilməsi, texniki təchizat və bu sahədə ən son İT nailiyyətlərindən geniş istifadə edilməsi göstərilən xidmətlərin yüksək keyfiyyətinə və etibarlılığına tam zəmanət verir [1,4,5]. Amma respublikamızda fəaliyyət göstərən milli poçt rabitəsi operatoru "Azərpoçt" MMC ilə yanaşı, 60-dan çox özəl poçt operatoru hüquqi və fiziki şəxslərə sürətli poçt və kuryer xidmətləri göstərir.

Azərbaycan Poçt Administrasiyası 1991-ci ildə Regional Rabitə İttifaqına (RRC), 1992-ci ildə İqtisadi Əməkdaşlıq Təşkilatına (ECO), 1993-cü ildə Ümumdünya Poçt İttifaqına (UPI) və 2000-ci ildə Avropa Telekommunikasiya Administrasiyaları Konfransı Komissiyasına (CEPT) qoşulub üzv kimi qəbul edilmişdir. Azərbaycan Poçtunun ən böyük nailiyyətlərindən biri kimi ölkəmiz ilk dəfə 2004-cü ildə Buxarestdə keçirilmiş 23-cü UPİ Konqresində bu qurumun ali orqanı olan İdarə Heyətinə, eləcə də 24-cü Konqresdə təşkilatın ali orqanının hər ikisinə təqdim edilmişdir. 2008-ci ildə Cenevrədə keçirilmiş İnzibati, 2016-cı ildə İstanbulda keçirilən 26-cı Konqresdə yenidən İdarə Heyətinin və Poçt Əməliyyat Şurasının üzvü seçilmişdir.

Bakı poçtalyon (1916) 1925-2021 Poçt xidmətinin çatdırılması

Şəkil 1.2.Tarix boyu poçt xidmətlərinin çatdırılması

Qədim dövrlərdə insanlar çox uzaq məsafələrdə ünsiyyət qurmalı və məlumat yaymalı olurdular. Qədim dövrlərdə insanlar mesajları ötürmək üçün oddan, yüksək təlim keçmiş elçilərdən və göyərçinlərdən istifadə edirdilər. Yazılı mesajlar Azərbaycanda qədim zamanlardan missionerlər tərəfindən ötürülür. Lakin poçt rabitəsi erası 1501-ci ildə başladı. Poçt şöbəsi müasir formada XIX əsrin birinci yarısında yaradılmışdır. 1818-ci il iyunun 1-dən sonra Azərbaycan ərazisində ilk televiziya yaranıb. Ölkənin ikinci böyük şəhəri olan Gəncədə ilk poçt şöbəsi açılıb. Daha sonra Bakı və Naxçıvana poçt səfəri təşkil olunub.

Azərbaycanda dəmir yolu poçtu daşınması 1883-cü il mayın 9-da Bakı ilə Tiflis, 1900-cü ildə isə Bakı ilə Dərbənd arasında başlanmışdır. 2002-ci ilin əvvəlindən etibarən Azərpoçt respublikanın bütün ərazisində marşrutlarda qatarla poçt göndərir.“Azərpoçt”un dünya miqyasında əldə etdiyi nailiyyətlərdən biri də odur ki, “Azərekspresspoçt” RM 160-dan çox qlobal poçt operatorunda EMS “Sürətli Poçt Xidməti” keyfiyyətinə görə keçirilən müsabiqədə ardıcıl 9 dəfə qızıl standart sertifikatına layiq görülüb UPI tərəfindən.

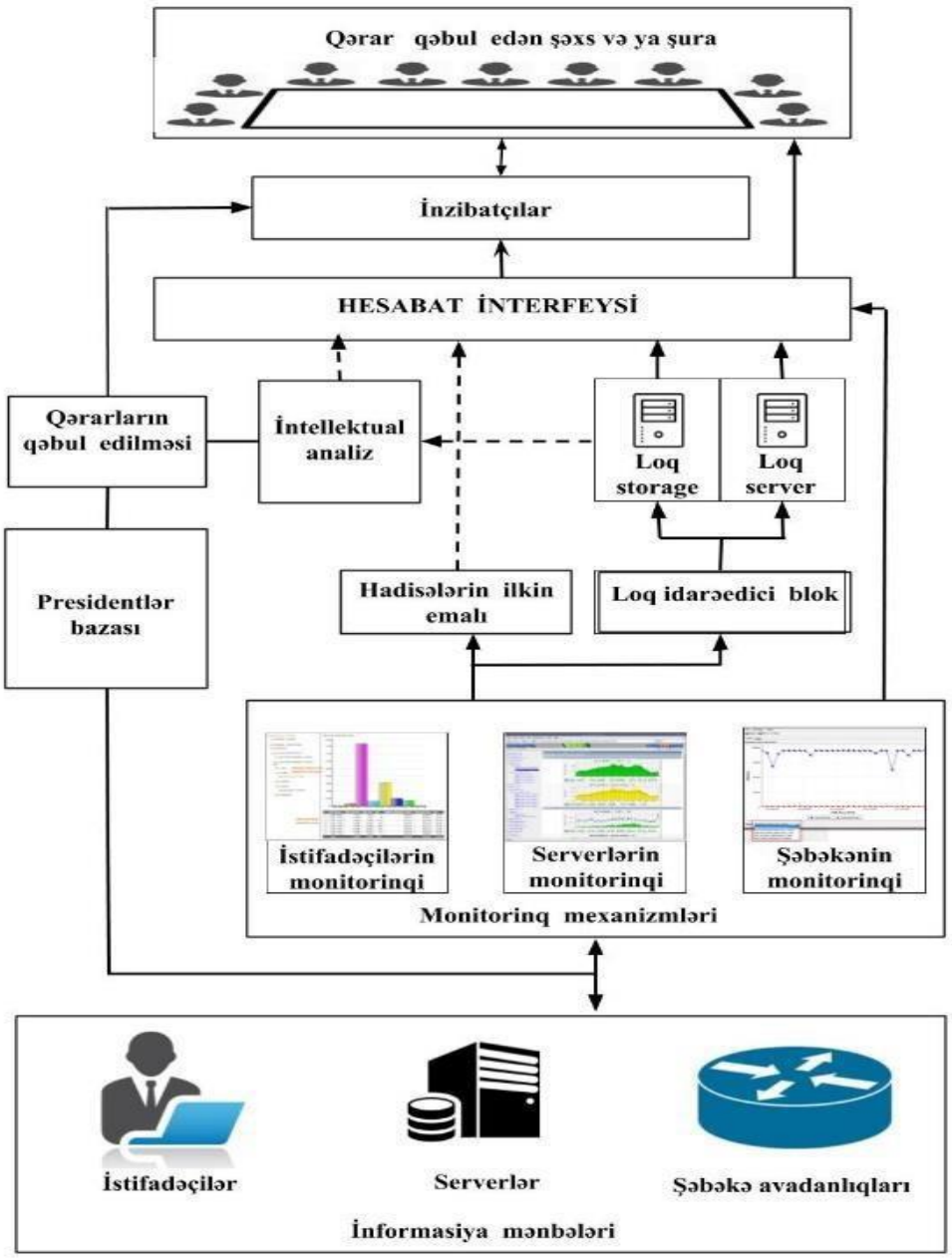
1998-ci ildən “Azərpoçt” MMC Koreyada UPI EMS Hwadong Assosiasiyasının üzvü olub və UPI Poçt Texnologiyaları Mərkəzi bu məhsuldan fəal şəkildə istifadə edir. Ona görə də “Azərpoçt” MMC 2001-ci ildən “IPS.light” izləmə sistemindən, 2005-ci ildən IFS/STEFI beynəlxalq izləmə sistemindən, 2013-cü ildən qlobal izləmə

sistemindən, 2016-cı ildən isə “IPS.Post” izləmə sistemindən istifadə edir. Sistem tətbiqi, bu sistemlərin imkanlarından istifadə edir[6,7].

Azərbaycan son illər sürətlə inkişaf edib və böyük yüksəliş dövrünün şahidi olur. “Azərpoçt” MMC-nin 63 poçt şöbəsi, 7 zəng mərkəzi, 4 filialı, 1496 poçt şöbəsi, 84 poçt şöbəsi var. 202 illik tarixə malik Azərbaycan ölkəsinin ilk və yeganə poçt operatoru olan “Azərpoçt” ildən-ilə böyüyür. Fiziki və texnoloji biliklərin genişlənməsi iqtisadi göstəricilərin də artmasına səbəb olur.

1.2. Şəbəkə təhlükəsizliyi əməliyyat mərkəzinin arxitekturunun sintezi

Kompüter şəbəkələrinin genişlənməsi, onlayn biznesin yayılması və onlayn e-ticarətin meydana çıxması ilə kompüter şəbəkələri hücumlara qarşı həssas oldu. İnternet insanlar və ya işgüzar əlaqələr arasında məlumat mübadiləsini təmin edən və idarə edən ünsiyyət vasitəsinə çevrilmişdir. Məlumat sızdıqda və ya məxfilik onlayn rejimdə pozulduqda, təhlükəsizlik boşluqları istifadəçiləri İnternetdən istifadə edərkən diqqətli olmağa məcbur edir. Bu təhlükəsizlik və ya məxfilik pozuntularına qarşı mübarizə tədbirləri fiziki şəxslər və müəssisələr üçün ortaya çıxır. Naqilsiz və naqilli kompüter şəbəkələri gündəlik istifadə üçün vacibdir,kompüterlərə e-poçt, faylların idarə edilməsi və s. Bu sahədə insanlar müxtəlif funksiyaları yerinə yetirmək üçün kompüterlərdən və şəbəkələrdən istifadə edirlər. Müdaxilə edənlər şəbəkələrə asanlıqla daxil olmaq və güzəştə getmək üçün proqram təminatı zəifliyi kimi texniki üsullardan istifadə edirlər, istifadəçi adı və şifrəni təxmin etmək, fiziki risk [6,7,8,14].



Şəkil 1.3. Şəbəkə təhlükəsizliyi əməliyyat mərkəzinin arxitekturunun sintezi

Burada kibertəhlükəsizlik əməliyyatları mərkəzinin arxitekturasının qurulması hadisələrin intellektual aşkarlanması, təsnifatı və qərarların təhlili metodlarından istifadə etməklə həyata keçirilir. Koqnitiv diaqnostika metodu da tətbiq edildi - İnternet monitor. Trafik həmçinin məzmunun idarə edilməsi və təhlükənin aşkarlanması xüsusiyyətlərinə malikdir. Bu, özlüyündə zərərli proqramlardan hərtərəfli qorunma, İnteqrasiya E-poçt Təhlükəsizliyi adlı anti-spam texnologiyası, şəbəkə profilləri və digər funksiyalar deməkdir[6,7,9].

Şəbəkənin Monitorinqi.Bu proqram Kiber Təhlükəsizlik Əməliyyatları Mərkəzinin düzgün işləməsini təmin etmək üçün istifadə olunur. Bu proqram bu təşkilatın bir hissəsidir. Eyni zamanda, mərkəzləşdirilmiş sistem idarəetmə proqramı hazırlanır. Qabaqcıl proqram onlayn təhdidlər haqqında real vaxt xəbərdarlıq edir. Proqram təminatı şəbəkə üzərində işləyir. Sistem stasionar xidmət operatorları üçün real vaxt rejimində şəbəkə vəziyyətinə nəzarət etmək üçün xüsusi ekrana malikdir. Bu sistemdə məlumat resursları şəbəkənin hər bir təbəqəsinə çatdırılır. Şəbəkə cihazının monitorinqi şəbəkədə işləyən bütün şəbəkə cihazlarının yaddaşının, temperaturunun, yüklənməsinin, kanal vəziyyətinin və trafik axınının monitorinqidir.

Yuxarıda göstərilən sistem şəbəkə monitorinqi funksiyalarını yerinə yetirir və sistemin təhlükəsizliyinin bir hissəsidir.

Başqa bir monitorinq addımı serverin monitorinqidir. Bu server müxtəlif xidmətlər həyata keçirir. Bu xidməti təmin etmək üçün müxtəlif server komponentləri istifadə olunur. Bu server maşınları VMware ESXi, FreeBSD, Ubuntu, RedHat, CentOS, Windows, SUSE Linux və s. Müxtəlif əməliyyat sistemlərində işləyir. Sistem bir və ya bir neçə xidmət üzərində işləyir. İstənilən əməliyyat sisteminin monitorinqi prosesi çoxlu planlaşdırma, işçi qüvvəsi və vaxt tələb edir, ona görə də server avadanlığının işləməsinə ciddi nəzarət edilməlidir.

Nəzarətin yeni formalarından biri də istifadəçilərin izlənməsidir. İstifadəçi nəzarət sistemləri bütün səviyyələrdə onlayn məlumatların elektron şəkildə qeydə alınmasını və dərc edilməsini nəzərdə tutur və çoxlu məlumat mənbəyi tələb edir [2,4].

İstifadəçiləri və səhifələri müəyyən etmək üçün qeydiyyat sistemi yaradılıb. Bu abunə planı bütün kanalı əhatə edir və xidmətdən istifadə etməyə imkan verir.

İstifadəçilərin siyahısı VLAN cədvəlində saxlanılır və aşağıdakı axtarışlarla istifadəçi axtarış funksiyasından istifadə etməklə tapıla bilər:

- ad, soyad;
- VLAN (istiqamət, bina);
- İP ünvan;
- MAC ünvan;
- binanın mərtəbəsi, otağın nömrəsi, kompüterin nömrəsi;

- telefon nömrəsi;
- əlavə qeydlər (vəzifəsi və s.);

Üç monitorinq sistemi tərəfindən toplanan qeydlər təhlil üçün serverə göndərilir. Bu proses aktivdir və hər 24 saatdan bir baş verir. Məntiqi qeydlər hər bir VLAN və hər bir monitorinq rejimi üçün çap olunur. Bu skript istənilən test üçün istifadə edilə bilər. Məsələn, xülasə cədvəlləri, fərdi ev şəbəkəsindən istifadə hesabatları və s. istehsal.

Biz bu qeydləri elmi təhlil və risk təhlili üçün lazım olan müddət ərzində saxlayırıq. Bu fayllar müxtəlif diaqnostik alətlər üçün faydalıdır. Məsələn,

1. Domen zonalar üzrə hesabat;
2. Trafikin veb-saytlar üzrə hesabatı;
3. Həftənin günləri üzrə hesabat;
4. Saatlar üzrə hesabat;
5. Veb-saytların profilinə görə trafikin paylanması;
6. IP ünvan üzrə hesabat;
7. IP qruplar üzrə hesabat;
8. Yaş həddinə görə hesabat;
9. AntiSpam sistemi üzrə hesabatlar.

Bu hesabatlar da bir neçə alt-hesabatlara bölünür:

1. Müraciətlərin həcmi
2. Müraciətlərin sayı

Sorğu şəbəkəyə daxil olan istənilən sorğuya aiddir. Bu anlayış IP ünvanları, URL-lər, istifadəçilər, məzmun və s. soruşa bilər[3,4,5,6].

Qeydiyyat prosesi bütün bağlantılar və istifadəçilər üçün baş verdiyi üçün, bu prosesin ehtiva etdiyi məlumatın nə qədər həssas olduğunu bilmək vacibdir, buna görə də məlumatların saxlanması və idarə edilməsi üçün məlumatların idarə edilməsi modulu yaradılmışdır. Qeydiyyatın idarə edilməsi bölməsi iki hissəyə bölünür:

- Loq server
- Loq storage

Log server saxlama və emal funksiyalarını yerinə yetirir. Bu log faylları bir qovluqda saxlanılır.

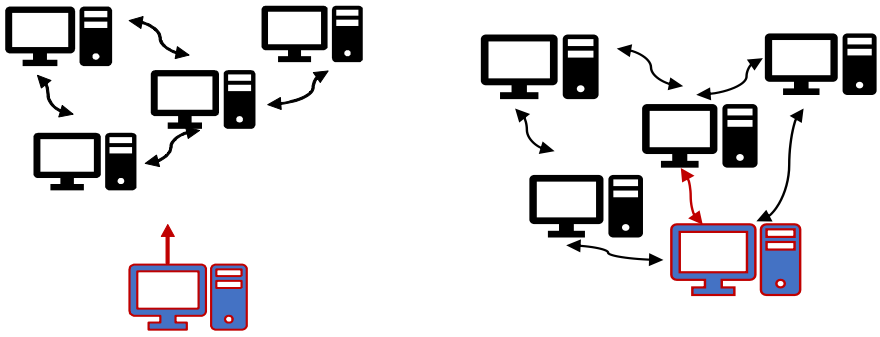
Fayllar həmişə saxlanılan serverdən 24 saat ərzində toplanır və günün sonunda onlar fayl formatında tərtib edilir və qeyd serverinə göndərilir. Bu proses xüsusi hazırlanmış proqram təminatının köməyi ilə baş verir.

Fayl növü qeyd faylını hansı serverin göndərməsindən asılıdır və qeydin növünü müəyyən edir və müvafiq qutuya qoyur. Fayllarda həssas məlumatlar olduğu üçün sistem 24/7 nəzarətdə saxlanılır və sistem hadisələr barədə inzibatçıya məlumat verir. Sistemə və verilənlər bazasına giriş təhlükəsizlik və təhlükəsizliyi təmin etmək üçün xüsusi şifrələmə açarları ilə təmin edilir və bu açarlar mütəmadi olaraq yenilənir.

Məlumat oğurluğu təhlükəsiz şəbəkə məlumatlarını əldə etmək üçün icazəsiz şəbəkə eksfiltrasiyasının baş verdiyi hücum hadisəsidir. Təcavüzkarlar oğurlanmış məlumatdan serverdə və ya kompüterdə özlərini tanımaq, başqalarına göndərmək və fayllarda saxlanan məlumatları oxumağa başlamaq üçün istifadə edə bilərlər. Belə olan halda ölkəmizdə informasiya oğurluğu cinayət sayılır və kompüterlərdən istifadə etməklə qeydə alınmış məlumatları oğurlamaq və ya iqtisadiyyatı, informasiyanı və ya şəbəkələri məhv etmək Azərbaycan Respublikasının qanunları ilə cinayət hesab olunur. İnsan biliyi və razılığı. Şəxsiyyət oğurluğu kredit kartı nömrələrini, sosial təminat nömrələrini, onlayn bank məlumatlarını, e-poçt parollarını, parolları və digər həssas şəxsi məlumatları əldə etmək üçün istifadə edilən qeyri-qanuni və konstitusiyaya zidd fırıldaq formasıdır[5,6].

Kiber Təhlükəsizlik Təhdidləri - İT-nin inkişafı istifadəçilərə böyük rahatlıq gətirməklə yanaşı, şəbəkə üçün bir çox təhlükələr də gətirə bilər. Şəbəkənin idarə edilməsi və şəbəkə təhlükəsizliyi şəbəkə qurulduqdan və quraşdırıldıqdan sonra mühüm əhəmiyyət kəsb edir. Nəticədə, əksər şəbəkə hücumları intranetlərdən qaynaqlanır. Kompüterlərin təqdim etdiyi xidmətlərdən asılı olaraq şəbəkələr müxtəlif hücumlara məruz qala bilər və müxtəlif hücum üsulları təhdid növləri ola bilər. Bu yolla, şəbəkə hücumları sistemləri və proqram təminatını, sistem təhlükəsizliyi hücumları verilənlər bazalarını və şəbəkə cihazlarını, proqram təminatı hücumları isə sistem məlumatlarına girişi hədəfləyə bilər[3,4,5].

Xarici və Daxili təhlükələr: Xarici təhlükələr adətən şəbəkədən kənarda fəaliyyət göstərən istifadəçilərdən gəlir. Kompüter sisteminə və ya şəbəkəyə çıxışı olmayan bu insanlar kənardan pis girişimciyə internet və simsiz şəbəkələr üzərindən kiberhücumlar etməyə icazə verirlər. Bu hücumlar maddi və mənəvi ziyana səbəb ola bilər və onların qarşısını almaq üçün təhlükəsizlik gücləndirilməlidir.



Şəkil 1.4. Xarici və Daxili təhlükələr

Bu, istifadəçi öz hesabı vasitəsilə şəbəkəyə icazəsiz giriş əldə etdikdə və ya şəbəkə avadanlığına fiziki giriş əldə etdikdə baş verir. Bu insanlar hansı məlumatın daha həssas olduğunu ayırd edə bilirlər. Təbii ki, daxili hücumlar həmişə qəsdən olmur. Təhlükəsizlikdən xəbəri olmayan işçilər bəzən internetə daxil olurlar. Müşayiət edən viral infeksiyaya görə xaricdən qaçma riski var.

“AzərPoçt” MMC-nin korporativ şəbəkəsinin mühüm xüsusiyyəti qlobal şəbəkə daxilində korporativ filialların fərdi LAN birləşmələri ilə mərkəzi LAN-dan uzaqda yerləşən şirkətin işçi kompüterlərinin birləşməsidir. Son illərdə bir çox kompüterlərin simsiz rabitə xətlərindən istifadə etməsi adi hala çevrilmişdir.

Şəkil 1.5. AzərPoçt MMC-nin Kompüter şəbəkələri təsvir olunmuşdur

Demək olar ki, “AzərPoçt” kompüter şəbəkəsinin inkişafı standart aparat qaydalarına ciddi nəzarəti və proqram təminatının düzgün seçilməsini əhatə edir. “AzərPoçt”un kompüter şəbəkələri arasında rabitənin yaradılması universal konsensus prinsipinə əsasən kompüterlər arasında məlumat mübadiləsinin həyata keçirilməsini nəzərdə tutur. “AzərPoçt” MMC-nin şəbəkəsi qurarkən əsas məsələ birgə müəssisə avadanlığının elektrik-mexaniki xassələri və informasiya (proqram və verilənlər) kodlaşdırma və məlumatların layihələndirilməsi sistemləri ilə uyğunluğunu təmin etməkdir. Problemin həlli standartlaşdırma sahəsinə aiddir. Müəssisə kompüter şəbəkələrinin standartlaşdırılması üçün “Azərpoçt”un metodoloji əsası bir-biri ilə əlaqəli şəbəkə avadanlığının yaradılmasına çoxmərhələli yanaşmadır. Sürətli maliyyə xidmətlərinin göstərilməsi ilə bağlı 2004-cü ildə qəbul edilmiş və 2008-ci ildə dəyişikliklər edilmiş “Poçt haqqında” Azərbaycan Respublikasının Qanunu. Poçt rabitəsi və poçt rabitəsi şirkətlərinin şəbəkələri sahəsində inkişaflar vasitəsilə ölkə miqyasında yeni xidmətlərin göstərilməsi imkanı da mövcuddur. 2016-cı ildə Azərbaycan Nəqliyyat və Yüksək Texnologiyalar Nazirliyinin qərarı ilə “Poçt rabitəsi xidmətlərinin göstərilməsi haqqında Əsasnamə”də dəyişiklik edilərək Azərbaycan Respublikasının Hüquq reyestrinə daxil edilmişdir [3,4].

Şəkil 1.6. Beynəlxalq yükdaşıma qovşağı olan Çin Xalq Respublikasından e-ticarət sifarişləri ölkədə fəaliyyət göstərən yerli kuryerlər.

Azərbaycanın əlverişli coğrafi mövqeyi, dövlətimizin başçısının məqsədyönlü siyasəti, respublikamızda regional və beynəlxalq nəqliyyat dəhlizlərinin formalaşması, Bakının böyük nəqliyyat və logistika mərkəzinə çevrilməsi yeni imkanlar açmışdır. Ölkəmiz beynəlxalq e-ticarət məhsullarını poçtla göndərir və göndərir. Hazırda Azərbaycan Poçtu sahəsində sərhəd elektron ticarətin həyata keçirilməsi üçün regional poçt qovşağı (HUB) kimi fəaliyyət göstərmək layihəsi həyata keçirilir [3,4,5,6].

Bu layihə çərçivəsində əsas beynəlxalq yükdaşıma qovşağı olan Çin Xalq Respublikasından e-ticarət sifarişləri ölkədə fəaliyyət göstərən yerli kuryerlər tərəfindən qəbul edilərək emal olunmaq üçün "Silkway" aviaşirkətləri vasitəsilə Azərbaycana daşınacaq. "Azərpoçt" MMC-dən MDB və dünyanın 15 ölkəsinə İsrail, İtaliya, ABŞ, Almaniya, Avstriya, Lüksemburq, Hollandiya, Rusiya, Türkiyə, Belarus, Böyük Britaniya, Çexiya, Ukrayna, Fransa, İran poçt çatdırılması və daşınması.

1.3. AzərPoçt Korporativ şəbəkə təhlükəsizliyində hədələrin təhlili edilməsi

Korporativ şəbəkələrdə informasiya təhlükəsizliyinin təmin edilməsi problemi yerli iş stansiyalarına, yerli şəbəkələrə və həmin şəbəkələrin istifadəçilər tərəfindən istifadə edilən ümumi şəbəkələrə çıxışı olan korporativ şəbəkələrə hücumları əhatə edir [1,3,4]. Ümumiyyətlə, sistemlərə hücumlar mürəkkəb ola bilər, bəzən hücumlar

operatorlar tərəfindən həyata keçirilir, digər hallarda isə hücumun mənbəyi bilinmir[8,9,10]. Bu baxımdan, hücumçunun məqsədləri aşağıdakı kimi təsnif edilə bilər:

- Ötürülmüş məlumatın məxfiliyini pozmaq;
- Ötürülmüş məlumatın bütövlüyünün və etibarlılığının pozulması;
- Bütün sistemin və ya sistemin ayrı-ayrı hissələrinin nasazlığı.

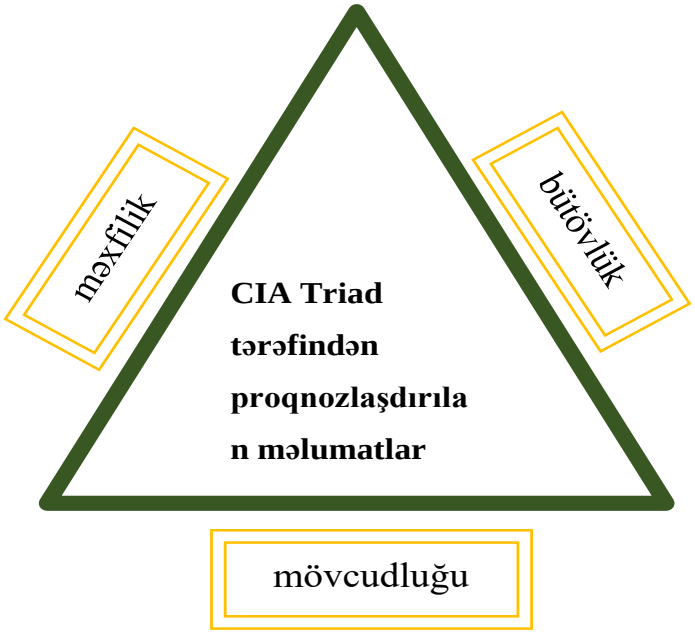
Şəkil 1.7. AzərPoçt Korporativ şəbəkə təhlükəsizliyində hədələr.

Paylanmış sistemlər, ilk növbədə, paylanmış sistemin təşkilatçıları məlumatların ötürülməsi üçün açıq kanallardan istifadə etdiyi üçün uzaqdan hücumlara qarşı həssasdır. Pis adamlar ötürülən məlumatlara passiv təsir etsələr də, çox vaxt kanala və ötürülən məlumatlara aktiv şəkildə müdaxilə edirlər.Xidmət məlumatlarına əsaslanan, istifadəçilər tərəfindən istifadə edilən məlumatlar, eləcə də açıq kanallar vasitəsilə göndərilə bilən məlumatlar həmişə hücuma məruz qalır. Hücumun səbəbini araşdırmaq və müəyyən etmək ağlasığmaz nəticələrə səbəb ola bilər, ona görə də hücumu müəyyən etmək və ciddi şəkildə cavab vermək bizim əsas prioritetimizdir.

1.4. Korporativ şəbəkələrdə informasiya tamlığının və məxviliyinin təmini üsulları

İnformasiya təhlükəsizliyi şirkətin kompüter sistemlərinin təhlükəsiz istifadəsini təmin edən bir sahədir və təşkilatın mühüm sərvəti olan “məlumat” mütəxəssislər tərəfindən qorunur. İnformasiya təhlükəsizliyi şəbəkələr, əsas funksionallıq və

informasiya sistemlərinin kommunikasiya texnologiyaları kimi aspektləri əhatə edir. Həm texniki aspektlər, həm də təşkilatlar informasiya təhlükəsizliyi barədə kifayət qədər məlumatlı olmalı və təhlükəsizlik siyasətlərini müəyyən etməlidirlər və informasiya təhlükəsizliyi informasiya təhlükəsizliyini idarə edən İT mütəxəssisləri tərəfindən təmin edilir.



Şəkil 1.8. CİA üçlüyü

CIA-nın məxfilik, bütövlük və giriş üçlüyü agentlik daxilində informasiya təhlükəsizliyi siyasəti üçün bir modeldir. Modelin qısa forması ABŞ Məxfi Xidməti ilə eyni olduğundan, qarışıqlığın qarşısını almaq üçün bəzən üçlü AIC (availability, integrity, and confidenciality) modeli adlandırılır. Bütövlülük məlumatın etibarlılığını və düzgünlüyünü təmin edir. Mövcudluq o deməkdir ki, səlahiyyətli tərəflər məlumatı etibarlı şəkildə əldə edə bilərlər [13].

Məlumat mövcud olmadıqda baş verə biləcək zərərin həcminə və növünə görə və yalnız məlumatın məxfiliyini məlumatların mühafizəsi üzrə məsul şəxsin xüsusi təlimi vasitəsilə qorumaq mümkün olduqda təsnif edilməlidir. Təlim səlahiyyətli şəxsləri təkcə təhlükələr və onlardan necə qorunmaq barədə deyil, həm də güclü parollar və kriptoqrafik biliklər, sosial mühəndislik texnikalarına dair xəbərdarlıqlar və

istifadəçinin xarici təhdidlər barədə məlumatlılığı kimi digər amillər haqqında maarifləndirməyə kömək edə bilər. Məxfiliyinizi qorumaq üçün istifadə etdiyimiz üsula misal olaraq, AzərPoçtda onlayn olduğunuz zaman hesab nömrənizi ala bilərsiniz. Məlumatların şifrələnməsi məxfiliyi təmin etməyin bir yoludur. İstifadəçi identifikasiyası və parol tələb olunur. İstifadəçilər həmçinin məlumatların harada saxlandığına və tələb olunan tapşırıqları yerinə yetirmək üçün onların nə qədər tez-tez göndərilməsinə əsaslanaraq ehtiyat tədbirləri görə bilərlər, təhlükəsiz məlumat saxlama cihazlarında və ya yalnız kağız formatında saxlama bu cür tədbirlərə misal ola bilər [11,13,14].

İntegrity- Məlumatların dəqiqliyini, tamlığını və etibarlılığını təmin edir. Məlumat tranzit zamanı dəyişdirilməməlidir və icazəsiz şəxslərin məlumatı dəyişdirə bilməməsini təmin etmək üçün tədbirlər görülməlidir (məsələn, məxfiliyin pozulması yolu ilə), o cümlədən, fayl icazələrinin və istifadəçi girişinin yoxlanılması. Versiya nəzarəti istifadəçilər tərəfindən təsadüfi dəyişikliklərin qarşısını almaq üçün istifadə olunur. Həmçinin, elektromaqnit müdaxiləsi və ya server qəzaları kimi qeyri-insani hadisələr nəticəsində baş verə biləcək dəyişiklikləri aşkar etmək üçün bir yol olmalıdır. Şifrələnmiş nəzarətləri daxil edilə bilər.

Əlçatanlıq (istifadəyə yararlılıq) bütün avadanlıqları qorumaqla, lazım olduqda onu tez bir zamanda təmir etməklə və proqram qüsurlarından azad, yaxşı işləyən əməliyyat sistemi mühitini təmin etməklə yaxşı bərpa edilməlidir. Sistemin lazımi sistem yeniləmələrini alması vacibdir. Ehtiyatsızlıq halında, RAID-in yerinə yetirilməsi, hətta hardware problemləri olsa belə, ciddi nəticələrə səbəb ola bilər. Məlumat itkisinə və ya əlaqənin kəsilməsinə qarşı qorunma təbii fəlakətlər və yanğınlar kimi gözlənilməz hadisələri əhatə etməlidir və ehtiyat nüsxələri bu cür hadisələr nəticəsində məlumat itkisinin qarşısını almaq üçün coğrafi cəhətdən təcrid olunmuş yerdə saxlanıla bilər. Aparat və proqram təminatı, həmçinin proksi serverlər kimi əlavə təhlükəsizlik vasitələri sistemi və onun həssas sahələrini xidmətdən imtina hücumları və şəbəkə müdaxilələri kimi zərərli müdaxilələrdən qoruya bilməlidir [7,8,9].

II FƏSİL. Azərpoçt MMC-də korporativ şəbəkə təhlükəsizliyinin idarə edilməsi qaydaları

2.1. Azərpoçt MMC-də korporativ şəbəkə təhlükəsizliyi vasitələrilə idarəetmə məsələləri

AzərPoçt-un müəssisə səviyyəli kibertəhlükəsizlik alətləri ilə əsas idarəetmə problemlərini həll etməyə çalışaq. "AzərPoçt" MMC-nin paylanmış şəbəkə məlumatlarının mühafizəsi idarəetmə sistemi funksional olaraq müəyyən edilmiş problemləri həll etməlidir [7,8,9]:

- Beynəlxalq təhlükəsizlik siyasətinin idarə edilməsi. AzərPoçt şəbəkəsində qlobal təhlükəsizlik siyasətinin idarə edilməsi, yerli təhlükəsizlik siyasətinin formalaşdırılması və məlumatların mühafizəsi ilə bağlı bütün müəyyən edilmiş prosedurların yerli təhlükəsizlik siyasətinə təqdim edilməsi.
- Departament strukturu və potensialın idarə edilməsi məsələləri. Bunlara HR-nin idarə edilməsi, buraxılışlar, proqram təminatına texniki xidmət;
- Kriptoqrafik vasitələrin idarə edilməsi, xüsusən - əsas infrastrukturun əsas idarəsi infrastruktur xidmətləri çərçivəsində müəyyən funksiyaları təmin etməlidir.
- İnformasiya sisteminin təhlükəsizliyinin auditi, informasiya sisteminin mühafizəsinin mövcud vəziyyətinin obyektiv qiymətləndirilməsi, jurnalların təhlili, qanun pozucularının müəyyən edilməsi və s. Xüsusiyyət qeydlərin idarəsi.
- Sistem təhlükəsizliyinin monitorinqi. Monitorinq mümkün cihaz hücumları, cihaz fəaliyyəti və kontekstlə əlaqəli təhlükəsizlik hadisələri haqqında məlumat verir.
- Layihə komandasının performansı necə təmin etməsi və korporativ şəbəkədə təhlükəsizlik nöqtələrini necə müəyyənləşdirməsi.

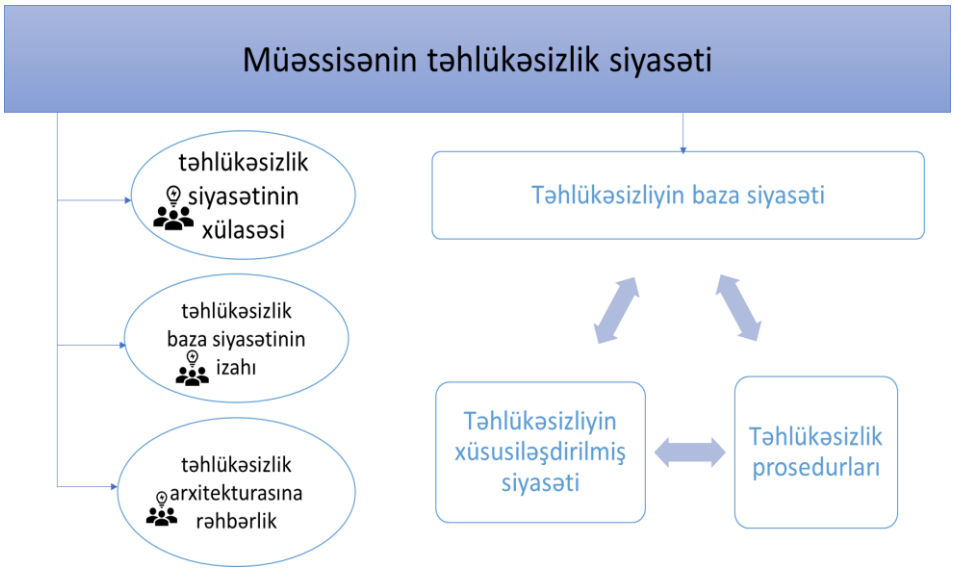
Şirkətin şəbəkəsində informasiya idarəetmə sistemində problemlər var ki, onları iki yolla həll etmək olar. Birinci yanaşma şəbəkə və ya sistem idarəetmə vasitələrini inteqrasiya etməkdir, ikinci yanaşma isə təhlükəsizliyin idarə edilməsi məsələlərini həll etmək üçün mövcud vasitələrdən istifadə etməkdir.

Təhlükəsizlik siyasəti hər bir təşkilat üçün vacibdir, Azərpoçt üçün də eynidir, bu siyasət şirkətin unikal aktivlərinin və resurslarının mühafizəsini təşkil etməyə imkan verir. Azərbaycanda təhlükəsizlik tədbirləri və prosedurlarını, onların rollarını və

işçilərin məsuliyyətlərini müəyyən etmək, yəni təhlükəsizlik qaydalarına uyğunluq baxımından Azərbaycanda bir neçə prosesin həyata keçirilməsi üçün bir sıra təhlükəsizlik siyasəti ümumiyyətlə həyata keçirilir: əsas təhlükəsizlik; xüsusi təhlükəsizlik siyasətləri və təhlükəsizlik prosedurları.

Şirkətin təhlükəsizlik siyasətinin məzmunu aşağıdakı sənədlərdə öz əksini tapmışdır: Təhlükəsizlik siyasətinin xülasəsi – dəyişə biləcək təhlükəsizlik siyasətinin məqsədini və strukturunu izah edir şirkətin ölçüsündən asılı olaraq. Təhlükəsizlik siyasəti bölmələrinə diqqət yetirsək:

- Əsas təhlükəsizlik siyasəti qadağan edilmiş və icazə verilən fəaliyyətlərin qurulmasını, həmçinin təhlükəsizlik arxitekturasının həyata keçirilməsində mülkiyyət siyasətinin mövcudluğunu ehtiva edir;
- Təhlükəsizlik arxitekturasının dizaynı istifadə olunan şəbəkə idarəetmə mexanizminin təhlükəsizlik arxitekturası hissəsinin həyata keçirilməsini təsvir edir.



Şəkil 2.1.Müəssisənin təhlükəsizlik siyasətinin struktur sxemi göstərilmişdir.

Əsas təhlükəsizlik sistemi təşkilatın əsas təhlükəsizlik planıdır. Bu qərar vermə prosesi təşkilatın məlumatları necə təhlil etdiyini təsvir edir. Məlumat əldə etmək və necə tətbiq etmək olar .Təhlükəsizlik sisteminin tətbiqi üçün bütün faydalı tapşırıqlar davamlı və davamlı fəaliyyətə zəmanət vermir. Bundan əlavə, bu plan təhlükəsizlik planı ilə tanış olmaq və təşkilatınızın mövcud təhlükəsizlik vəziyyətini öyrənmək üçün

lazımi şərtləri təmin edir. Demək olar ki, təhlükəsizlik planının strukturu və məzmunu məqsəd və mühitdən asılıdır. İcma bunu təhlükəsizlik tədbirlərinə dəstək verməklə edir [2,3].

"Məlumatların təhlükəsizliyi" sistemi korporativ şəbəkənin əsası hesab olunur. Şəbəkə təhlükəsizliyinin aparıcı aləti olan "Azərpoçt" MMC-ni təcrübədən keçirək. Şirkətlərin paylanmış müəssisə məlumat təhlükəsizliyi planını asanlıqla həyata keçirə biləcəyini göstərir bu səbəbdən əməliyyat sistemindən və bu məqsəd üçün istifadə olunan proqram sistemindən asılı olmayaraq təhlükəsizliyin idarə edilməsi mərkəzləşdirilməlidir. Həmçinin şirkətin informasiya sistemlərində sistem qeydiyyatının nəticələri, icazəsiz giriş, istifadəçi hüquqlarının dəyişməsi və s. Çünki istifadə olunan inzibatçı təşkilatın informasiya sistemində edilən dəyişiklikləri tam təsvir etməlidir [15,16,17,18].

Şirkətin informasiya sisteminin mərkəzləşdirilmiş təhlükəsizlik idarəetməsi GSM (Qlobal Təhlükəsizlik İdarəetmə) qlobal təhlükəsizlik idarəetmə konsepsiyasına əsaslanır. GSM təhlükəsizliyinin idarə edilməsinin qlobal konsepsiyası mürəkkəb sistem qurmağa imkan verir. Şirkətin informasiya resursları bir neçə xüsusiyyətə əsaslanır;

- Şirkətin təhlükəsizlik siyasətinə uyğun olaraq bütün mövcud cihazların təhlükəsizliyini idarə etmək. Şirkətin bütün resurslarını qorumaq üçün qeyri-döyüş qaydalarının bütövlüyü müəyyən edilmişdir. təhlükəsizliyini və təhlükəsizliyini təmin etmək. Bir neçə istehsalçı koordinasiyada avadanlıq təmin edir
- Bir açardan istifadə edərək bütün şirkət məlumat resurslarının xəritələşdirilməsi problemi. Şəxsi cihazlarla pula qənaət edin. Eyni şey birbaşa üçüncü tərəf qovluqlarından istifadəyə də aiddir.
- Təhlükəsizlik mülahizələrinə uyğun olaraq məlumatların mühafizəsi kanallarının yerli idarəetməsinin mərkəzləşdirilməsi prosesi.

Təşkilatın qorunan hər şeyə çıxışının olmasını təmin etmək üçün məxfilik siyasətində qanunlar və ya qadağanedici müddəalar var: xüsusi olaraq icazə verilməyən hər şey qadağandır. Şəbəkədəki cihazlar arasında əlaqəni təmin etmək üçün onlar "ilkin konfiqurasiya" (layout) "yaradırlar" və ümumiyyətlə, əslində istifadə etmədən rabitə

kanalını “təmin edirlər”. Başlanğıc konfiqurasiyası Mərkəzi Cihaz İdarəetməsini konfiqurasiya etmək üçün lazım olan qaydaları ehtiva edir - başlanğıc zamanı təhlükəsizlik siyasətləri. Qlobal təhlükəsizlik siyasəti qarşılıqlı fəaliyyət və sistemin müstəqilliyi və nəzarət funksiyası kimi bütün şəbəkədə tətbiq oluna bilər. Qlobal təhlükəsizlik siyasəti bütün şəbəkənin təhlükəsizlik siyasətinin demək olar ki, tam məntiqi və semantik şərhidir. Buna əsaslanaraq, bir çox fərdi cihaz üçün təhlükəsizlik siyasətlərini konfiqurasiya etmək mümkündür [7,8,9,10].

2.2. İnformasiya mühafizəsi üçün aparat – proqram metodları

Aparat və proqram vasitələri, hardware qorunması kimi problemlərin həlli yollarından biri ola bilər, yəni mühafizə sistemlərində. Həll tərəfindən verilir:

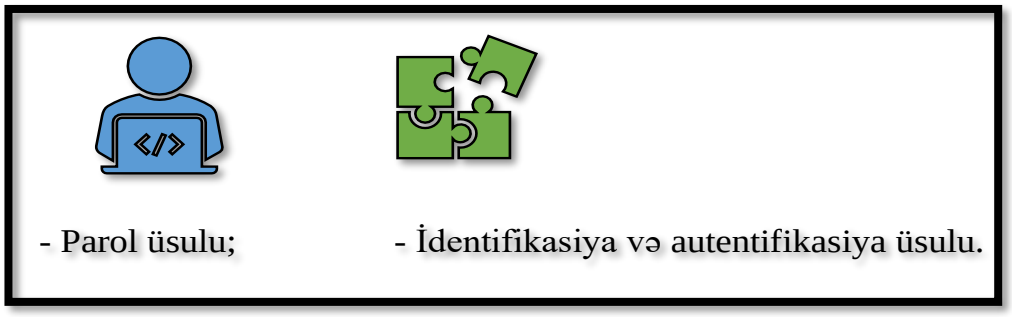
1. İstifadəçilər və proqramlar tərəfindən resurslara və proqramlara icazəsiz girişin qarşısını almaq.

2. Zəruri hallarda ehtiyatlardan icazəsiz istifadənin qarşısının alınması halları

3. Resurslardan sui-istifadəni aşkar edin və qarşısını alın

4. Resurslara icazəsiz girişin qarşısını almaq üçün səmərəli, yüksək keyfiyyətli proqram təminatı hazırlayın Siz istifadəçi və proqrama daxil olmaq cəhdlərini qeyd etməlisiniz. Və dərhal təhlükəsizlik işçisinə xəbər verin.

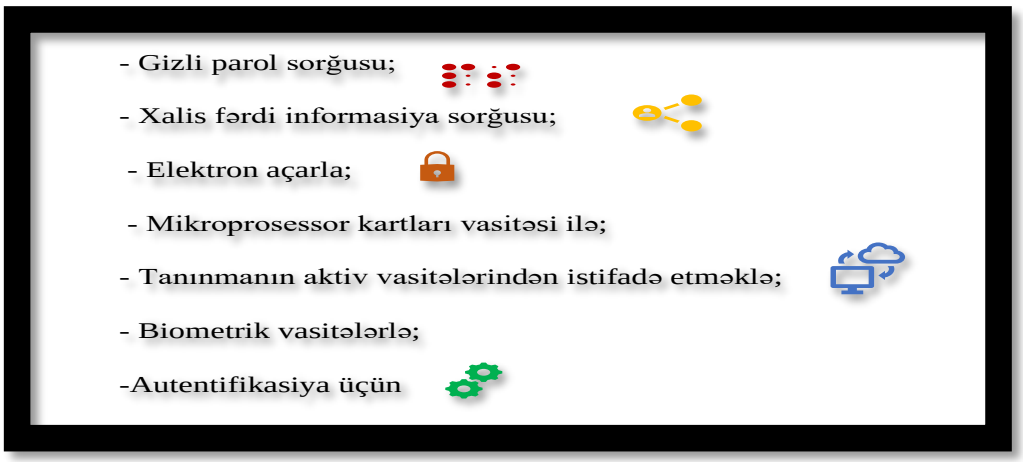
İstifadəçilər tərəfindən resurslardan icazəsiz istifadənin qarşısını almaq. Buna görə iki növ müasir sistem istifadə olunur. Cədvəldə göstərilmişdir:



Cədvəl 1.

Şifrələnməmiş sadə parol qorunması zəif təhlükəsizlik tədbiri hesab olunur. Əsas çatışmazlıq, eyni paroldan istifadə edən bütün istifadəçilərin kompüter sistemi

baxımından fərqlənməməsidir. İstifadəçi üçün parol qorunmasının olmaması əsasən onun yaddaqalanlığı ilə bağlıdır. İstifadəçinin identifikasiyası və autentifikasiyası sistemə girişə nəzarətin daha sərt üsulu hesab olunur. bu zaman sistemə qoşulmaq istəyən bütün istifadəçilər əvvəlcə müəyyən edilir, sonra isə onların eyni istifadəçi olub-olmaması müəyyən edilir. İstifadəçilər parol ilə autentifikasiya edə bilərlər. Doğrulama: İstifadəçinin autentifikasiyası cədvəldə göstərilən üsullardan istifadə etməklə həyata keçirilir:



Cədvəl 2.

Tələb olunan əlavə məlumatda istifadəçinin və ya onun yaxınlarının şəxsi həyatı ilə bağlı hər hansı məlumat və ya təfərrüatlar, məsələn, Azərpoçt hesab nömrəsi, pasport nömrəsi, həyat yoldaşının və ya ərinin soyadı və s. [16,17,18].

Elektron açara misal olaraq maqnit zolaqları olan plastik kartı göstərmək olar. Görünməz parol kimi fəaliyyət göstərən kod kartın yaddaşında saxlanılır. Təsadüfi parol yaradan əsas elektron cihazın xüsusi və daha mürəkkəb versiyası token adlanır. Tokenin çatışmayan xüsusiyyətlərindən biri odur ki, bu istifadəçi sistemə sahib deyilsə, sistemə daxil ola bilməz. Bu halda çıxış yolu bəzi müvəqqəti tokenlərin yaradılmasıdır, bir neçə il əvvəl ABŞ Standartlar və Texnologiyalar İnstitutu tərəfindən hazırlanmış mikroprosessor kartları rəqəmsal imzaların yaradılmasına imkan verir, şifrələmə alqoritmi özü elektron imzaların saxtalaşdırılmasının qarşısını alır. Nəqliyyat vasitəsinə misal olaraq kiçik bir aşağı siqnal radio ötürücüsü və uyğun bir radio qəbuledicisindən ibarət bir sistemdir. Sistemə qoşulduqdan sonra istifadəçi vericini

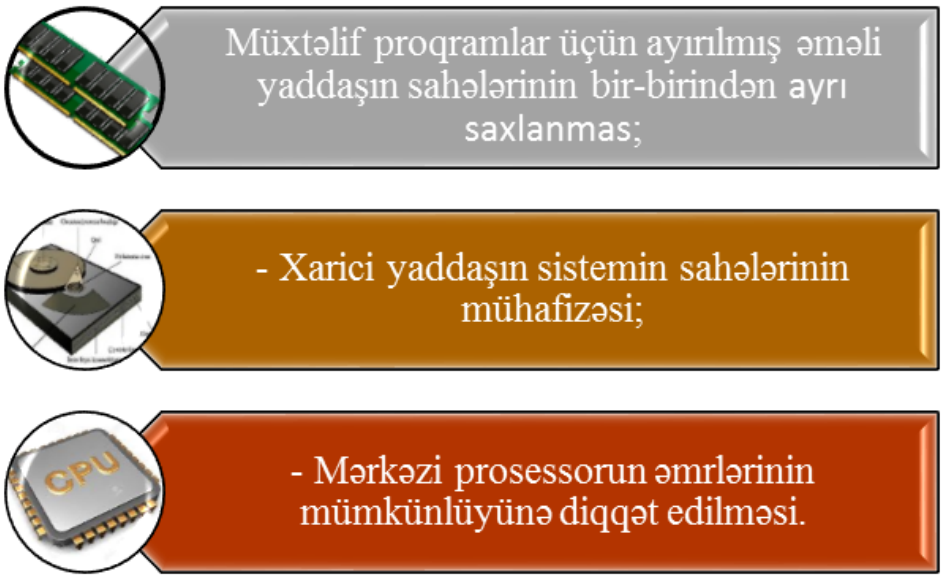
qəbulediciyə yaxınlaşdırmalı və onun işləməsi üçün işə salmalıdır. Qəbuledici siqnalı aşkar etdikdən sonra istifadəçi sistemə qoşula bilər, belə bir sistemin üstünlüyü ondadır ki, fiziki təmas yoxdur. Autentifikasiya üsulları arasında biometrik üsul ən etibarlı hesab edilir, şəxsiyyətin çapı, əl forması, səsi, imzası, tor qişası ilə müəyyən edilməsi isə membran və digər parametrlərdən istifadə etməklə əldə edilə bilər. Təhlükədən qorunma sorğuların qorunan resurslarda qeydiyyatdan keçməsini və icazəsiz giriş cəhdlərini qeyd etməyi tələb edir. İnformasiya və proqram təminatı resurslarının icazəsiz istifadədən necə qorunacağı şəkildə göstərilmişdir:

Şəkil 2.4. İnformasiya - proqram resurslarının icazəsiz istifadədən mühafizəsi sxemi

Məsələn, proqramı icazəsiz surətdən çıxarmaqdan qorumaq üçün icra olunan proqram kodu proqramın aparatında kilidlənə bilər. Bu halda, proqramın bir nüsxəsi başqa bir kompüterdə işləyir və proqramı pozmadan təhlükəsizlik sistemini oxumaq imkanı və ya çətinliyi müəyyən edilməlidir. Hər bir fayl atributunu (məsələn, yoxlama məbləği) məlumatları saxlayan faylları icazəsiz girişdən qoruyan standartla müqayisə

etmək olar. Əgər kimsə faylın məzmununu dəyişdirirsə, yoxlama məbləği dəyişir və bu dərhal aşkar edilir. Checksum alətləri burada faylların redaktəsinə nəzarət edən proqram təminatı və ya sistemi qorumaq və faylların icazəsiz silinməsinin proqramların və məlumatların silinməsinin qarşısını almaq üçün istifadə olunur. Məlumatların şifrəsini açmaq üçün şifrələmə açarını bilməlisiniz, hətta informasiya texnologiyalarının mövcud səviyyəsi ilə belə tapmaq çox çətindir [4,5,6,7].

Məlumatların şifrələnməsi: Şifrələnməmiş verilənlər düz mətn adlanır. Onlar xüsusi şifrələmə alqoritmi ilə şifrələnir, alqoritmin girişi açıq mətn və şifrələmə açarı, çıxışı isə şifrəli mətn adlanan şifrəli mətndir. Şifrələmə alqoritmi gizli olmamalıdır, dərc oluna bilər, lakin şifrələmə açarı gizli olmalıdır. Şifrələmə açarı olmayan birinin şifrəli mətni açа bilməsi ehtimalı azdır. Nəticədə rabitə kanalı ilə göndərilən faktiki məlumatların əvəzinə şifrəli mətn verilənlər bazasında saxlanılır. Resursdan sui-istifadədən qorunma adətən proqram təminatı ilə həyata keçirilir. Onları aşağıdakılar əks etdirir:



Şəkil 2.5. Resursdan sui-istifadədən qorunma adətən proqram təminatı üsulu.

Tətbiq resurslarından (sənədlər, şəkillər, verilənlər və s.) düzgün istifadə əməliyyat sistemlərindən daha çox proqram səviyyəsində təmin edilməlidir. HS səhvlərinin və fasilələrin nəticələrini aradan qaldırmağın və azaltmağın ən vacib

yollarından biri struktur, əməliyyat və İT ehtiyatlarından istifadə etməkdir. hs müxtəlif dərəcəli aparat komponentlərində struktur ehtiyatı: serverlər, müxtəlif qurğular (maqnit disk yaddaşı, prosessorlar və s.), bloklar, mikrosxemlər və s. Buna artıqlıq deyilir. Ehtiyat nüsxələmə zamanı, əsasən, HS-nin sabit və fasiləsiz təchizatının təmin edilməsi, əməliyyat ehtiyatı isə sistemin müxtəlif elementlərinin saxlanma, texniki xidmət və emal funksiyalarını yerinə yetirmək üçün mövcud olmasını təmin edən kompüter prosesinin aparılması deməkdir. Data Redundancy – Dəyərli məlumatların bir dəfə və ya daimi surətdə kopyalanması və arxivləşdirilməsi ilə tam məlumat itkisinin qarşısını almaq üçün istifadə olunur. Belə məlumatlara istifadəçinin tətbiqi proqramları, müxtəlif növ verilənlər (verilənlər bazası faylları, sənədlər və s.), əsas əməliyyat sistemi proqramları və elektron cədvəl, söz və qrafik prosessorlar kimi ümumi proqram paketləri daxildir. Yüksək keyfiyyətli aparat məlumatların təhlükəsizliyi üçün ən vacib ilkin şərtlərdən biridir. Sistemin işləməsi zamanı məlumat itkisinin səbəbləri, eləcə də sistemin nasazlığı və dayanma vaxtı HS planlaması zamanı edilən səhvlər və ya səhvlərlə bağlıdır. HS-nin ümumi təhlükəsizliyinə xələl gətirən qüsurları aradan qaldırmaq və ya azaltmaq üçün aparat və proqram təminatının həyat dövrünün bütün mərhələlərində təhlil, həyata keçirmə, planlaşdırma və monitorinq üçün müasir təhlükəsizlik metodlarından istifadə etmək lazımdır [1,2,3,6].

2.3. AzərPoçt MMC-də informasiya təhlükəsizliyinin idarə edilməsi qaydaları

İnformasiya Təhlükəsizliyi İdarəetmə Siyasətinin məqsədləri üçün istifadə edilən terminlər aşağıdakı mənaları ifadə edir:

1. Audit -audit standartlarına uyğunluq dərəcəsini müəyyən etmək üçün audit sübutlarının əldə edilməsi və obyektiv qiymətləndirilməsi üçün planlaşdırılmış, müstəqil və sənədləşdirilmiş prosesdir.

2. autentifikasiya -xidmət istifadəçisinin şəxsiyyətinin yoxlanılmasına və şəxsən yaradılan təhlükəsizlik məlumatlarının istifadəsinə imkan verən prosesdir;

3. əməliyyat meneceri- informasiya sisteminin idarə edilməsinin biznes proseslərinə və onların sistemdə əks olunmasına yaxşı bələd olan AzərPoçtunun əməkdaşıdır.

4. iş mühiti istifadəçi üçün açıq olan informasiya sisteminin yaradılması üçün real vasitədir.

5. Şəxsi məlumatlar - birbaşa və ya dolayısı ilə şəxsin şəxsiyyətini müəyyən edən məlumatlar;

6. Məlumat - təqdimat formasından və təsnifatından asılı olmayaraq hər hansı fəaliyyətlə bağlı faktlar, fikirlər, məlumatlar, xəbərlər və ya digər məlumatlar.

7. İnformasiya vahidləri Azərpoçt üçün dəyərlidir, fiziki (kağızda, CD və digər daşıyıcılarda) və ya elektron formada (fayllar, fərdi kompüterlərdə saxlanılır), məsələn, Azərpoçta məxsus məlumatlar.

8. İnformasiyanın mövcudluğu - zəruri hallarda məlumat əldə edilə və istifadə edilə bilər;

9. Məlumatların işlənməsi - yaradılması, toplanması, emalı, saxlanması, axtarışı, paylanması və s. məlumatların;

10. İnformasiya sistemi kompüter texnologiyasının tətbiqi də daxil olmaqla, informasiya texnologiyaları və sənədlərin təşkilati və texniki cəhətdən təşkil edilmiş məcmusudur.

11. məlumatın tamlığı - məlumatın düzgünlüyü və tamlığı;

12. İnformasiya təhlükəsizliyi - məxfiliyin və əlçatanlığın qorunması;

13. İnformasiya təhlükəsizliyinin idarə edilməsi sistemi əməliyyat məqsədlərinə nail olmaq üçün "Azərpoçt"un informasiya təhlükəsizliyinin yaradılmasına, dəstəklənməsinə və davamlı olaraq təkmilləşdirilməsinə yönəlmiş tədbirlər və prosedurlar məcmusudur.

14. İnformasiya texnologiyaları - Azərbaycan kompüter və kommunikasiya texnologiyalarının köməyi ilə informasiya proseslərində istifadə olunan üsul və alətlər sistemi.

15. İnkişaf mühiti - informasiya sistemləri üçün proqram təminatının hazırlanmasına aiddir;

16. İstifadəçilər - Azərpoçt əməkdaşları, podratçılar və informasiya sistemində işləmək hüququ olan müştərilər;

17. kriptoqrafik tədbirlər - məlumatların kriptoqrafik transformasiyası yolu ilə məlumatların təhlükəsizliyini təmin etmək üçün istifadə olunan üsullar (avadanlıq, tətbiqi proqramlar və s.);

18. Kritik informasiya sistemləri - Azərpoçtun risklərin idarə edilməsi qaydalarına əsasən risklərin qiymətləndirilməsi əsasında yüksək təsirə malik olan və Azərpoçtun tətbiqi zamanı istifadə olunan informasiya sistemləri, operativ, uçot və avtomatlaşdırılmış idarəetmə sistemləri, məsələn, informasiya və telekommunikasiya şəbəkələri. . işləmək;

19. Test mühiti informasiya sistemi işə salınmazdan əvvəl sınaqdır.

20. Sistem inzibatçısı Azərpoçtun informasiya sistemində dəyişikliklər edən, ehtiyat nüsxələrini çıxaran, onun əməliyyatlarına nəzarət edən və fasiləsiz işləməsinə təminat verən, sistemin funksiyaları üzrə səlahiyyətləri bölüşdürən əməkdaşıdır.

2.3. Mərkəzləşdirilimiş korporativ informasiya sistemləri təhlükəsizliyinin idarə edilməsi

İnformasiya sistemlərinin təhlükəsizliyinin idarə edilməsi işinin təşkili bir neçə prinsipə malikdir:

1. “AzərPoçt” MMC-nin şəbəkə təhlükəsizliyinin idarə edilməsi sistemi qlobal təhlükəsizlik siyasəti səviyyəsində həyata keçirilməlidir. Qlobal siyasət səviyyəsinə müəssisə şəbəkəsi elementləri arasında qarşılıqlı əlaqənin təhlükəsizliyini və müəssisə şəbəkələri ilə xarici aktorlar arasında kommunikasiyaların təhlükəsizliyini dəstəkləyən qaydalar daxildir;

2. mərkəzi biznes şəbəkəsinin təhlükəsizlik və təhlükəsizlik tələbləri biznes strukturuna və əməliyyatlarına uyğunlaşdırılmalıdır;

3. Yerli təhlükəsizlik siyasəti fərdi təhlükəsizlik cihazları üçün konfiqurasiya edilməli və qlobal təhlükəsizlik siyasətinə və qorunan şəbəkə topologiyasına uyğun olaraq avtomatik həyata keçirilməlidir.

Müəssisə informasiya sistemlərinin mərkəzləşdirilmiş mühafizəsinin idarə edilməsi beynəlxalq GSM təhlükəsizliyinin idarə edilməsi konsepsiyasına əsaslanır[3,6,7,8]. GSM-Global Security Management, tərcüməsi qlobal təhlükəsizlik idarəçiliyi deməkdir. Təhlükəsizliyin idarə edilməsinin beynəlxalq konsepsiyası müəyyən xüsusiyyətlərə uyğun olaraq "Azərpoçt"da informasiya ehtiyatlarının kompleks idarə edilməsi və mühafizəsi sistemini yaratmağa imkan verir :

"AzərPoçt" MMC-nin təhlükəsizlik siyasəti əsasında mövcud vəsaitlərin təhlükəsizliyinin idarə edilməsi, şirkət resurslarının mühafizəsi üzrə ziddiyyətli olmayan qaydaların həyata keçirilməsi və müxtəlif istehsalçıların zəmanət fondlarının mühafizəsi siyasətinin həyata keçirilməsi;

- Şəxsi resurslardan istifadə etməklə resurs qeydiyyatı və digər korporativ kataloqlardan birbaşa istifadə;
- "AzərPoçt"un təhlükəsizlik siyasəti əsasında məlumatların mühafizəsi vasitələrinin yerli idarəetməsinin mərkəzləşdirilməsini təmin etmək;
- AzərPoçt alətlərinə giriş qaydalarının seçilməsinə nəzarət, təhlükəsizlik sistemi qaydalarının dolayı seçiminə giriş.

AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ
AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

Əlyazması hüququnda

“Radiotexnika və telekommunikasiya” kafedrası

Əliyev Nəsib Sübhan oğlu

“AZƏRPOÇT” MMC-NİN KORPORATİV ŞƏBƏKƏSİNDƏ KRİPTOMUHAFİZƏ ÜSULLARININ TƏDQİQİ

Mövzusunda

MAGİSTRLİK DİSSERTASİYASI

İxtisas:060627 –“Elektronika,telekommunikasiya və radiotexnika mühendisliyi”
İxtisaslaşma: “Radiorabitə radioverlişləri və televiziya” üzrə

Elmi rəhbər: t.ü.f.d., dos. R.S. Məmmədov

BAKI-2023

III FƏSİL. Azərpoçt MMC-nin korporativ şəbəkəsinin qurulmasında istifadə olunan qurğular haqqında ümumi məlumat.

3.1. Korporativ şəbəkələrin əsasları

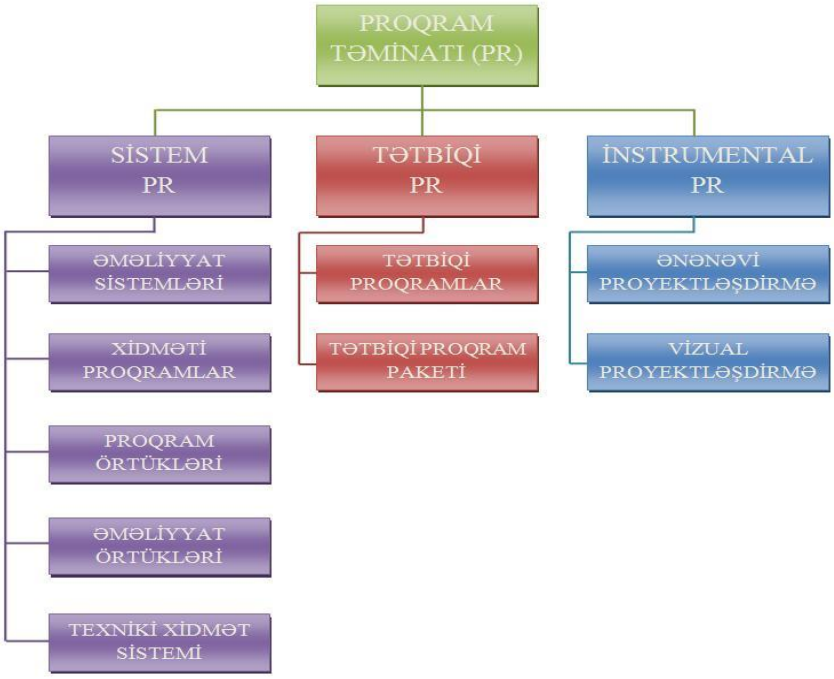
Korporasiya- istifadəçilərin ümumi bir məqsədə çatmaq üçün yaradılmış bir birlikdir. Korporasiyanın subyektləri (istifadəçiləri) arasında informasiya mübadiləsini yeirnə yetirmək üçün korporasi ya daxilində aydın şəkildə başa düşülən, əlaqləndirilmiş və mühafizə olunan kommunikasiya yaradılır[14,15,16,17].

Belə demək olar ki, korporasiyanın yaradılmasında üç əsas elementin:

1. Ümumi məqsədin
2. İnformasiyanın
3. İnformasiya mübadiləsini həyata keçirmək üçün lazım olan vasitələrin olması lazımdır.

Ümumiyyətlə, korporativ şəbək ə korporasiyada istifadə edilən müxtəlif tətbiqi proqramlar aralığında məlumat mübadiləsini həyata keçirən bir sistemdir. Korporativ şəbəkə

7. sistem və tətbiqi proqram təminatları,
8. şəbəkə adapterləri,
9. konsentratorlar,
10. komutatorlar
11. marşrutlayıcılar,
12. kabel sistemi kimi komponentlərindən ibarət olur.



Şəkil 3.1 Proqram təminatının struktur sxemi.

Şəkildən göründüyü kimi sistem proqram təminatı özü də bir neçə alt siniflərə bölünür.Bu alt siniflərə misal olaraq aşağıdakı kimi gösdərmək olar.

- Əməliyyat sistemi: ilkin olaraq kompüteri açdığımız zaman BİOS vasitəsilə RAM-a yüklənir. Kompüterin işini idarə edir,aparat hissəsi, tətbiqi proqram təminatı və istifadəçi arasında interfeys yaradır.

Birməsələli: MS DOS

Çoxməsələli: Unix, Windows, MAC OS, Linux,Solaris,Android,İOS və b.

Şəkil 3.2 Əməliyyat sistemləri

➢ Əməliyyat örtükləri:istifadəçilərə yeni interfeys təqdim etməklə onlara əməliyyat sistemlərinin əmrlərini dərindən bilməkdən azad edir. Yəni istifadəçi yeni qovluq yaradarkən çoxlu kodlardan istifadə etmirdi. Bunun üçün əməliyyat örtükləri yaradıldı ki, bunlara misal olaraq: Norton Commander, Windows Commander,DosNavigator,Windows1.0,Windows3.0,Windows3.1,Windows3.11 və b. göstərmək olar[15,16,17].

➢ Əməliyyat sistemləri: lokal və qlobal informasiyanın emalı,ötürülməsi qəbulu,saxlanılması, şəbəkəyə qoşulmuş kompüterlərin işinə nəzarət və s. funksiyalarını yerinə yetirir. Buna misal olaraq: İBM LAN,Windows Server(2003,2008,2011),Windows NT,Unix Server,Linux Server,Solaris və s.

➢ Servis (xidməti) proqram: istifadəçilərə kompüterlə işləyən zaman əlvə xidmətlər təklif edir. Bu xidmətlərə aşağıdakılar daxildir:

- İstifadəçi interfeysinin təkmilləşdirmək
- Mühafizəsi
- Verilənlərin bərpası
- Xarici yaddaşla əməli yaddaş arasında informasiya mübadiləsini sürətləndirmək

- Arxivləşdirmə-arxiv açma
- Kompüter virusları ilə mübarizə

➢ Tətbiqi proqram təminatı- qısa olaraq konkret məslənin həlli üçün nəzərdə tutulmuşdur.bunlara misal olaraq aşağıdakıları qeyd etmək olar.

- Ümumi təyinatlı
- Üsulyönlü
- Problemyönlü
- Qlobal kompyuter şəbəkələri

2. Şəbəkə adapterləri/kartı

Şəbəkə adapterləri 2 hissəyə bölünür və kompüterə

✓ Daxili-PCI slotuna keçirilir

✓ Xarici-USB portu vasitəsilə qoşulur.

3. Konsentratorların kompüter şəbəkələrində əsasən iki növü istifadə olunur.

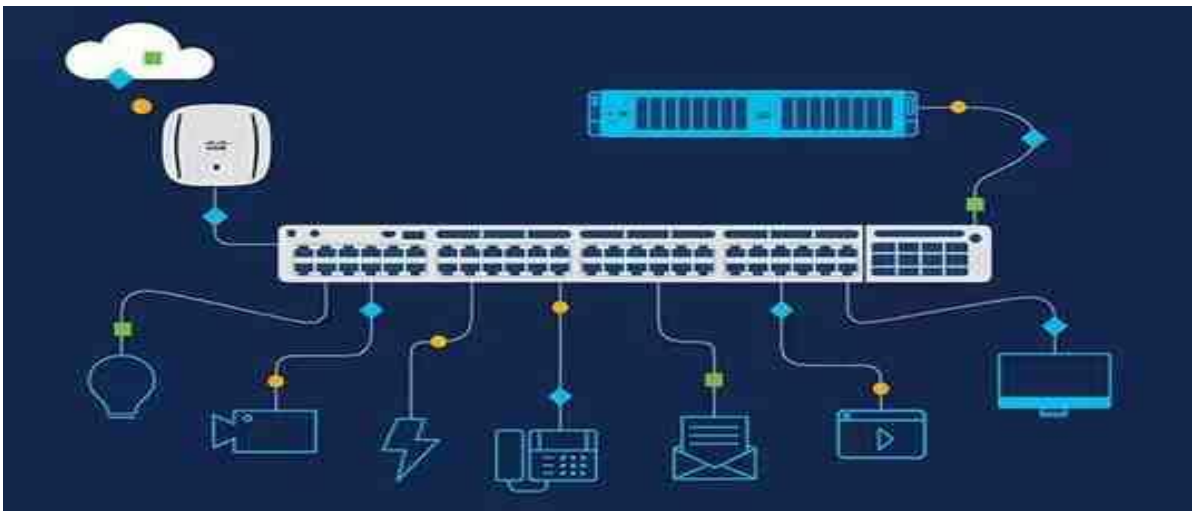
✓ Xab (hub)

✓ Konsentratorlar(consentrator)

Konsentratorlar xabdan fərqli olaraq daha geniş imkanlara malikdir.Bəzən bu cihazlara superxab da deyilir.Bu qurğunun funksiyası ondan ibarətdir ki,müxtəlif şəbəkə qurğularını və seqmentlərini bir-birilə birləşdirir.Üç növü var: passiv,aktiv və intelektual.

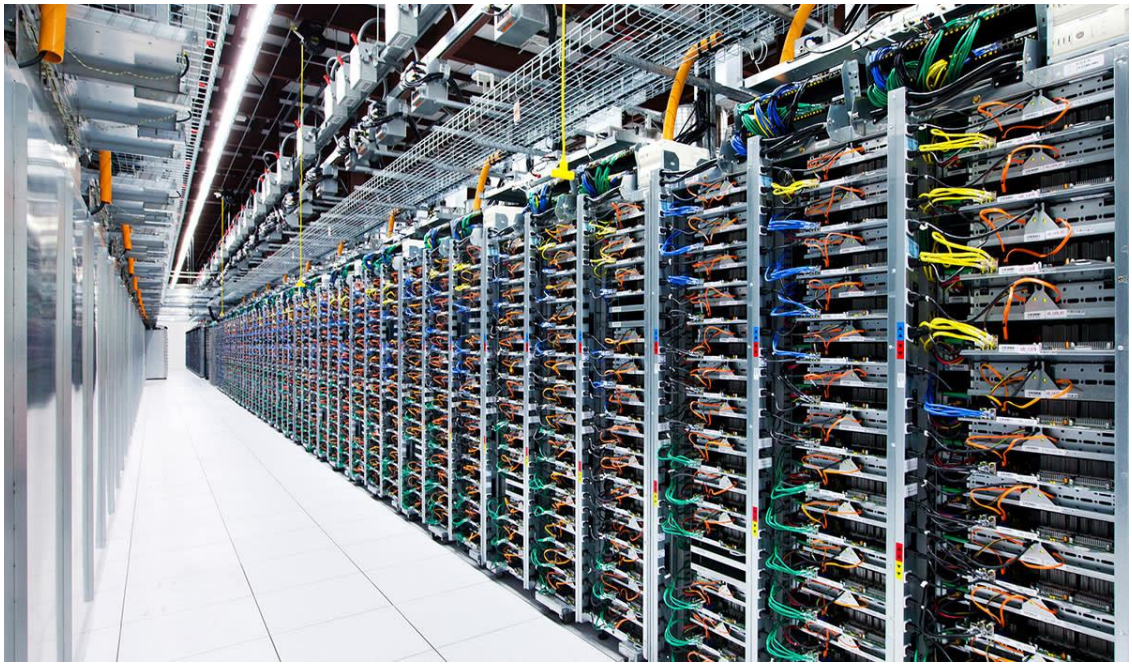
Şək 3.3 Xab

4. Komutatorlar(switch)-qovşaq rolunu yerinə yetirir. Ağıllı qurğudur.MAC ünvanları (local ünvanlar) ilə işləyir.

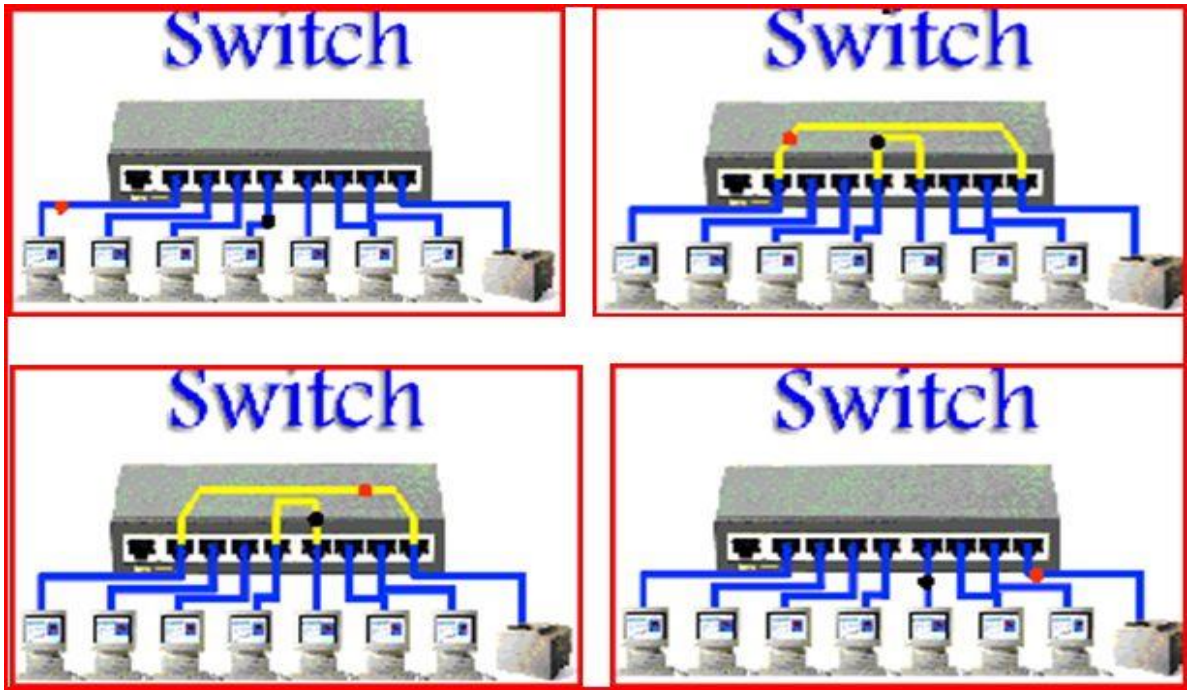


Şək 3.4 Komutatorun (switch) qurulma sxemi.

5. Marşutlayıcılar(router)- informasiya hesablama şəbəkəsində mübadilə olunacaq məlumatın yolunu təyin edir.Router şəbəkə strukturunun seqmentlərə ayrılmasında kompyüterlərin aparat (MAC)ünvanlarından deyil aşkar ədədi ünvandan istifadə olunur[1,2,3,4,5].Bir neçə hissədən ibarət həmin ünvanlarda subnet adlandırılan seqmentlərin nömrələri əks etdirilir və bu nömrələri eyni olan kompüterlərin bir subnet mənsubluğunu bildirir.Buna görə də marşrutlayıcı trafikin lokallaşdırılması üçün daha effektli və etibarlı hesab olunur.



Şək 3.5 Komutatorun visual görünüşü

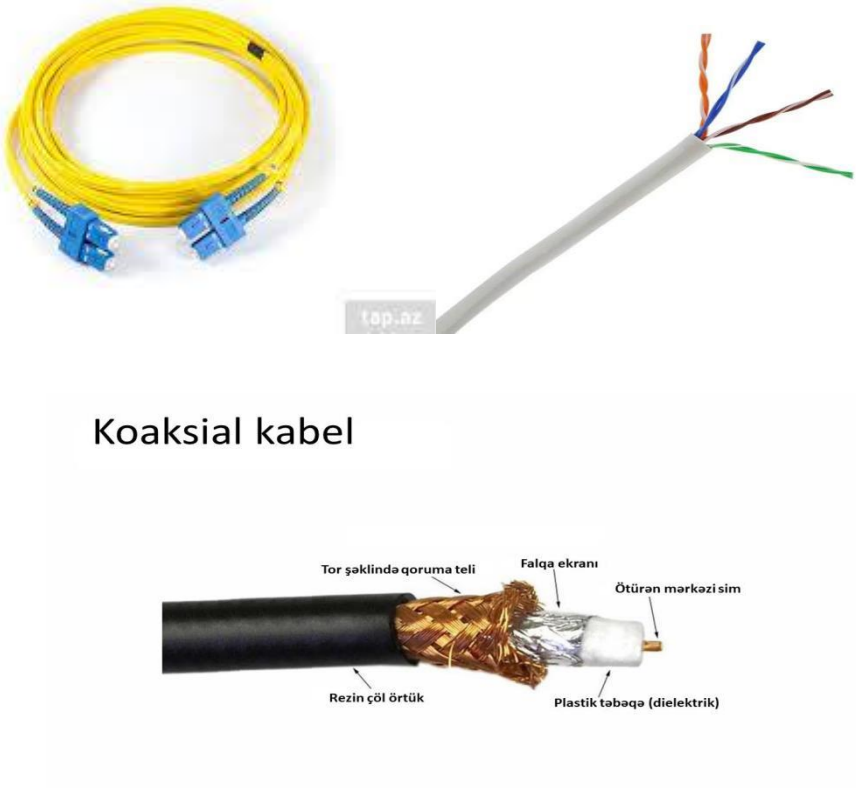


Şək 3.6 Komutatorun işləmə prinsipi

6. Kabel sistemi

Əsasən 3 cür növ kabeldən istifadə olunur ki onlarda aşağıdakı kimi təsnif olunur.

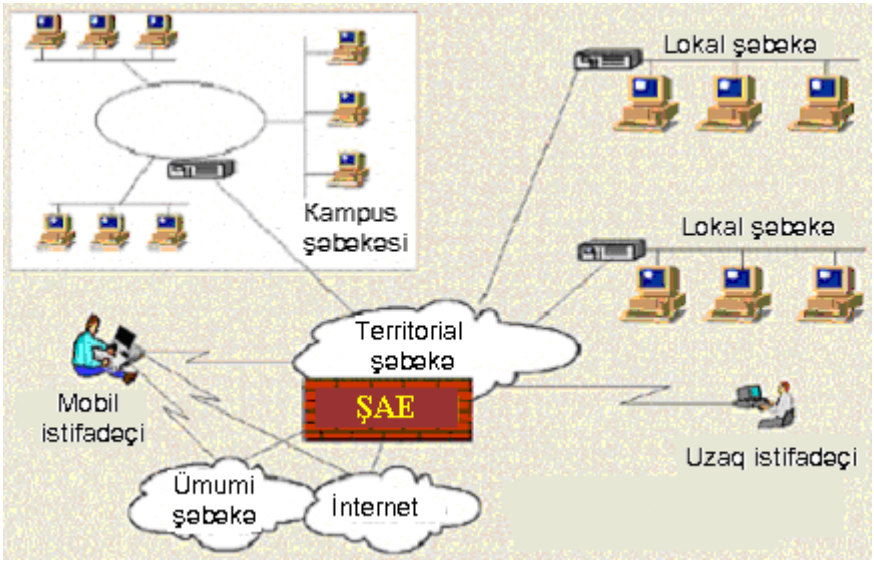
- Burulmuş cüt (mis naqillər)-4cüt (8) naqil
- Koaksial kabellər-əsasən şin topologiyasında istifadə olunur.
- Optik-lifli kabellər-işıq siqnalları



Şəkil 3.7 Kabellərin növləri.

İngilis dilli ədəbiyyatlarda korporativ şəbəkə “enterprise-wide networks” adlandırılır ki bu da tərrcümədə müəssisə miqyaslı şəbəkə kimi adlandırılır. Bu termin özündə birləşmə bərabərlik mənalarını daşıyır,yəni korporativ şəbəkə bir qayda olaraq bir və yaxud daha çox qeyri-bircisli şəbəkələrin (bir şirkətə-firmaya məxsus olan) birləşməsi nəticəsində əmələ gəlir (məs,kampus şəbəkəsi, lokal şəbəkəsi,territorial şəbəkələri internet və b).Yeni nəsil korporativ şəbəkələr müxtəlif cür xidmətləri təchiz edir.Bu cür xidmətlərə verilənlərin ötürülməsi,İP-telefoniya,video və audio konfranslar və videoyayımlar,mühafizə və videonəzarət daxildir[2,3,4,5,6].Korporativ şəbəkənin şirkətdə istifadəsi aşağıdakıları kimi təchiz olunur:

- Kompüter istifadəçilərinin birgə səmərəli işləməsini
- Kompüterlərin,periferiya quğrularının və proqram təminatlarının maksimal effektiv istifadəsi
- Ümumi istifadə olunan verilənlərə daxil olmaların sadəliyi və rahatlığı.



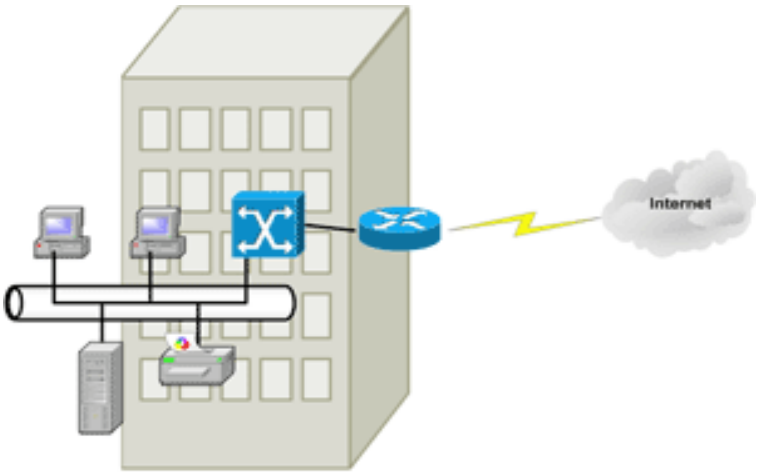
Şək 3.8 Korporativ şəbəkənin stukturu

Korporativ şəbəkələrinin məqsədi şirkət ətrafında vahid informasiyan fəzasının təşkilidir,yəni müxtəlif qovşaqlarda yerləşən sitem və tətbiqi proqramlarının bir-birilə əlaqəsini və onalara uzaqda yerləşən subyektlərin daxil olmalarını təşkil edilməsidir. Şirkətin korporativ informasiya fəzasına həmçinin fayl sistemi vasitəsi ilə informasiya mübadiləsi,təhlükəsiz elektron poçt, çoxsaylı funksiyaları olan telefonlaşdırma,selektor məşvərətləri,videokonfransları və b. kimi ximətlər də aiddir[4,5,7].

Korporativ şəbəkədə başlıca və ən yüksək priortet xidmət əməkdaşların şirkətin korporativ idarəetmə sistemində səmərəli işləməsinin təşkil olunmasıdır.

Korporativ şəbəkənin tarixi lokal və qlobal şəbəkələrin yaranması tarixi ilə çox əlaqəlidir. LAN və WAN şəbəkələrinin yaranması,kompüter istifadəçilərinə, operativ

informasiya mübadiləsində yeni fürsətlər yaradırdı[2,3,4,7].Birinci şirkətlərdə ümumi məsələnin,məs..., mühasibat və yaxud marketinq məsələlərinin həlli üçün nəzərdə tutulmuş amma müəyyən qrup əməkdaşlar tərəfindən istifadə edilən, şabə və yaxud da qrup lokal şəbəkələri yaradılırdı. Sonra bu şəbəkələr şirkət və kampus şəbəkələrinə kimi böyüdülür.



Şək 3.9 Şöbə və yaxud qrup lokal şəbəkəsi

Şlüz(şəbəkə keçidi)-müxtəlif rabitə protokolları ilə işləyən müxtəlif tipli şəbəkələr arasında məlumat mübadiləsini həyata keçirən birləşdirici qurğudur. Eynitipli şəbəkələr arasında mübadilə zamanı məlumatı çevirən körpüdən(BRİDGE) fərqli olaraq,şlüz yalnız ötürməni reallaşdırmır, həmdə verilənlərin formatını təyinat şəbəkəsinin protokoluna uzlaşdırır[2,4,9]. Şlüzün iki növü var:

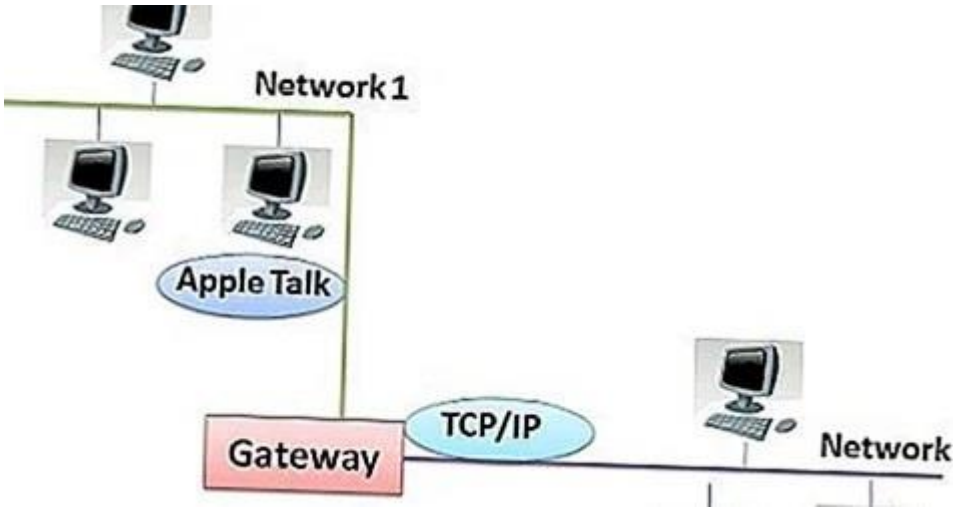
- Daxili
- Xarici

Bir protokolda formatlanmış bir paketi qəbul etdikdə bir şlüz tərəfindən həyata keçirilən proseslər aşağıdakı kimi ifadə olunur: -

- Gateway, göndərən şəbəkəsi tərəfindən istifadə edilən protokol üçün (məsələn, Apple Talk) formatlanmış bir paketi qəbul edir.
- Daha sonra həmin paketi qəbuledicinin şəbəkəsi tərəfindən istifadə edilən başqa bir protokol üçün (məsələn, TCP / IP) formatlaşdırmaq üçün çevirir.

- Paketin formatını emal etdikdən sonra həmin paketi təyinat nöqtəsinə yəni alıcılar şəbəkəsinə ötürür.

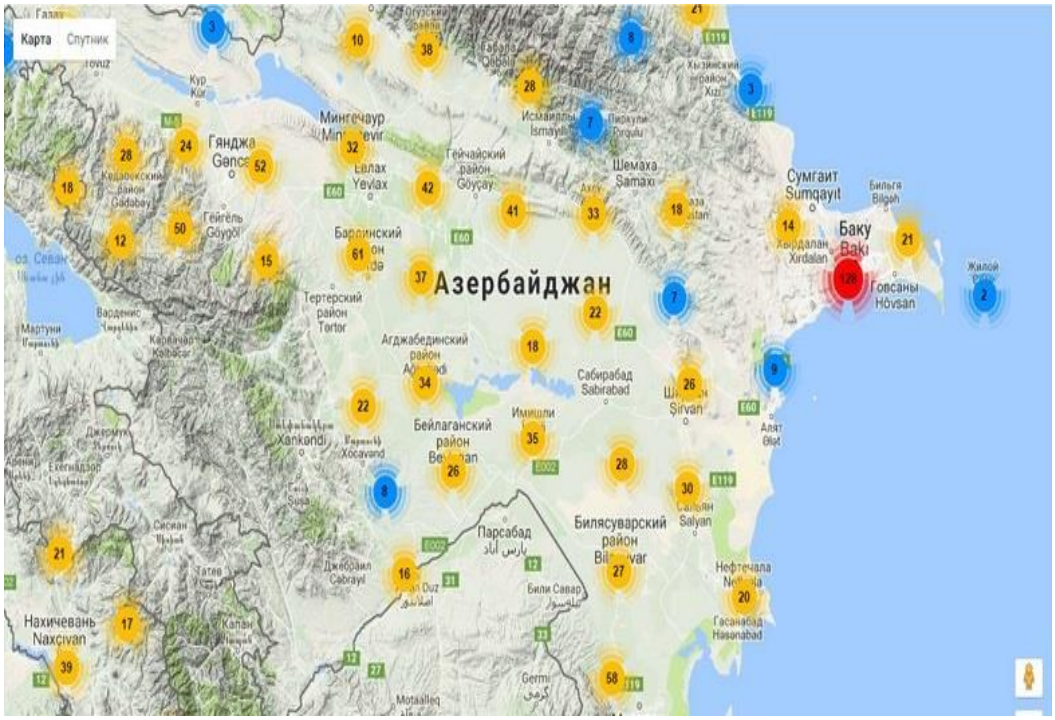
Bəzən modifikasiya yalnız paketin başlığı və qoşqusu üçün tələb olunur və bəzən bir keçid məlumatın sürətini, ölçüsünü və paketin formatını tənzimləməlidir[3,4,5].



Şək 3.10 Şlüz(Gateway) strukturu

Ölçüləri böyük olmadığı üçün bir qayda olaraq şöbə və yaxud qrup şəbəkələri altşəbəkələrə (seqmentlər) bölünmürlər. Şöbələrin lokal şəbəkələri korporativ şəbəkəyə qoşulduqda trafikin böyük hissəsi şöbələrin lokal şəbəkələrində həyata keçirilir. Lokal şəbəkə adətən hər hansı bir şəbəkə texnologiyasının(ethernet,Token Ring) əsasında qurulur.Əgər istifadəçilər arasında böyük həcmli (məs, multimedia fayllarının ötürülməsi və qəbulu) informasiya mübadiləsin yaranarsa, bu vaxt FDDI, Fast Ethernet və yaxud 100VG-AnyLan kimi yuxarı sürətli texnologiyalardan istifadə edilir. Hal hazırda Gigabit Ethernet,10Gigabit Ethernet və 100Gigabit Ethetnet kimi yuxarı surətli texnologiyalar fəaliyyət gösdərir.Gigabit Ethernet avadanlıqları əvəlki nəsil texnologiyalarla(Ethernet,Fast ethernet) daha yaxşı uzlaşırlar. Şöbənin lokal şəbəkələrində bəzən bir və yaxud maksimum iki şəbəkə əməliyat sistemi(ƏS) tətbiq edilir. Ən çox hallarda Lokal Şəbəkədə ayrılmış NetWare 3.x və yaxud Windows NT

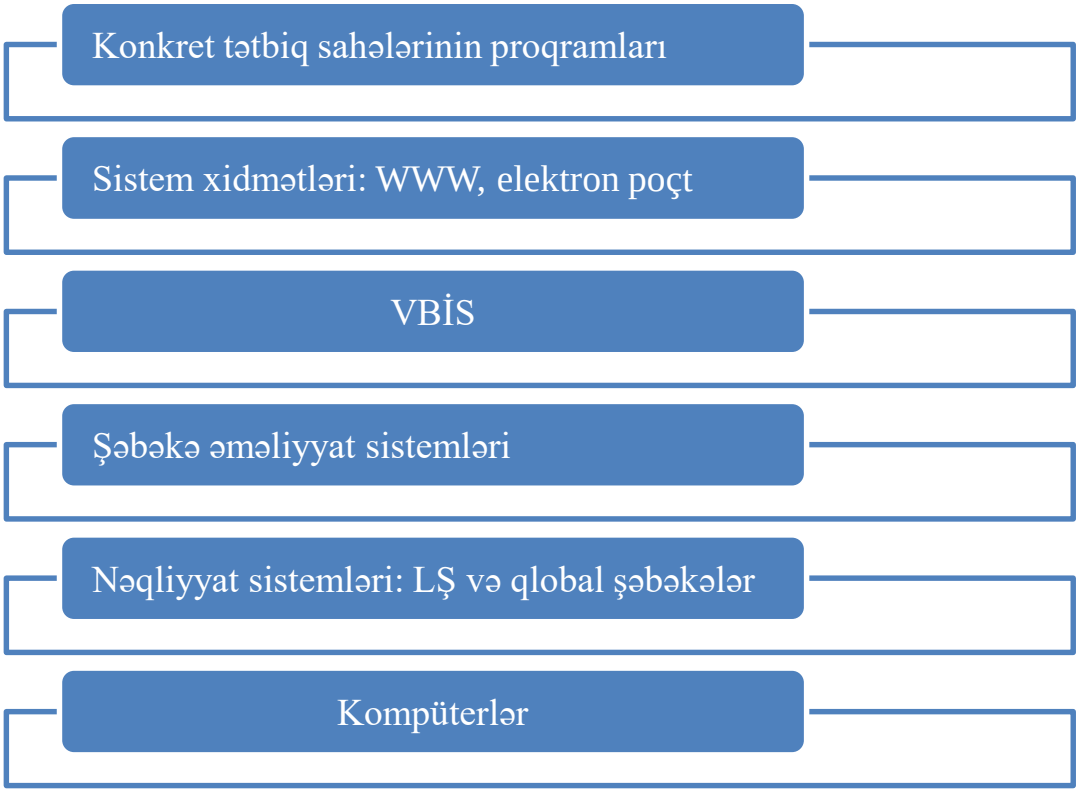
serveri əsasında yaradılır və yaxud bir ranqlı olur. Bir ranqlı şəbəkə dedikdə, Lokal şəbəkədə olan kompüterlərin eyni ranqlı,yəni eyni hüquqlu olması başa düşülür. Bir ranqlı Lokal şəbəkələrə misal üçün Windows for Workgroups şəbəkəsini demək olar. Şöbənin lokal şəbəkələrinin miqyası aşağı olduğu əsasən onu idarə etmək üçün mürəkkəb idarəetmə sistemi zərurət yaranmır. Şöbə səviyyəsində idarəetmə məsələsi nisbətən asandır. Şəbəkə inzibatçısının vəzifəsi yeni istifadəçilərin əlavə edilməsindən, sistem problemlərinin aradan qaldırılmasından, yeni qovşaqların və proqram təminatının yeni versiyalarının quraşdırılmasından ibarətdi[14,16,17].



Şəkil 3.11 Azərpoçtun korporativ şəbəkəsi

3.2. Korporativ şəbəkəsinin xidmətlər

Korporativ şəbəkəni yaxşı anlamaq üçün onu bir neçə təbəqədən ibarət olan piramida şəklində göstərmək olar.



Şəkil 3.12. Koprorativ şəbəkənin iyerarxik təsviri

Korporativ şəbəkəni gösdərən piramidaın əsasında kompüterlər təbəqəsi yerləşir. Kompüterlər məlumatın saxlanılması və emalı mərkəzləri rolunu oynayır. Kompüterlər təbəqəsi üzərində kompüterlər arasında məlumat paketlerinin təhlükəsiz ötürülməsini təşkil etmək üçün nəqliyyat altsistemi yerləşdirilir. Nəqliyyat altsistemiinin bir üst səviyyəsində kompüterlərdə olan tətbiqi proqramların işini həyata keçirən və nəqliyyat sistemi vasitəsi ilə öz kompüterlərinin resurslarını vahid şəkildə istifadəyə verən şəbəkə əməliyyat sistemi işləyir[5,6,7].

Şəbəkə əməliyyat sisteminin üzərində əsas korporativ informasiyanı ardıcıl şəklində saxlayan və onun üstündə isə axtarış əməliyyatını aparmağa şərait yaradan verilənlər bazasını idarəetmə sistemi (VBİS) fəaliyyət gösdərir. Növbəti təbəqədə isə digər sistem xidmətləri işləyir. Buna misal olaraq bu xidmətlərdən, World Wide Web (WWW), elektron poçt sistemini göstərmək olar və sonda korporativ şəbəkənin yuxarı təbəqəsində, verilmiş şirkət və ya verilmiş tipli şirkətlər üçün xüsusi olan problemləri

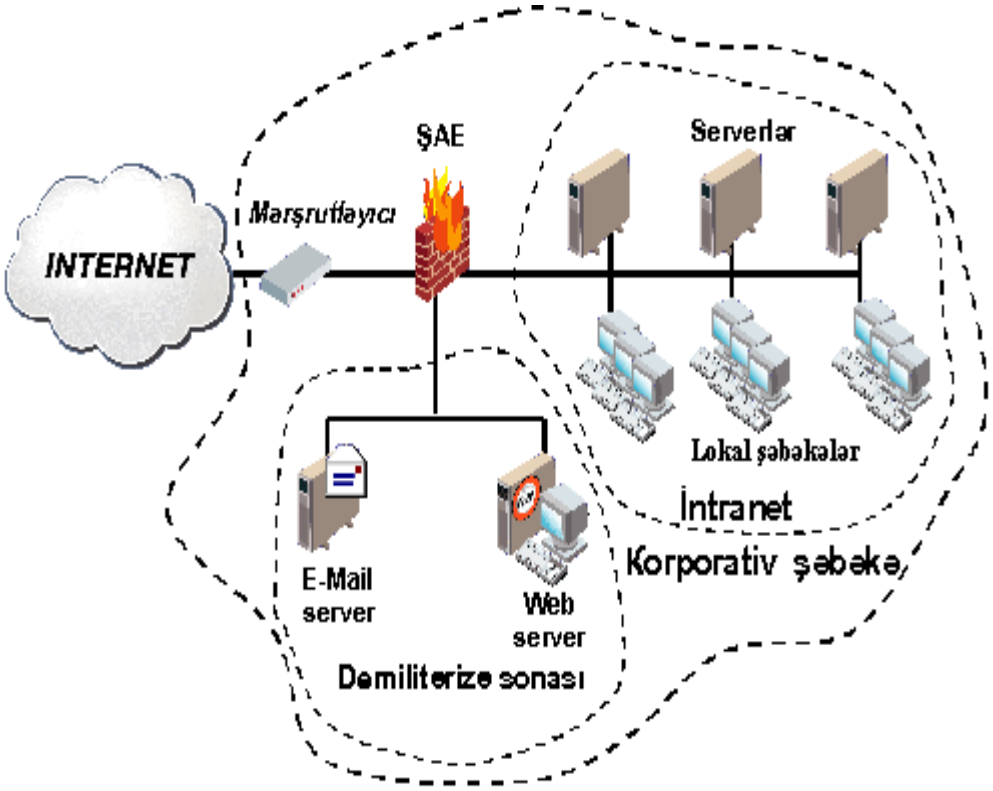
həll edən, konkret tətbiq sahələrinin proqramları işləyir. Buna misal olaraq bankların avtomatlaşdırılması, mühasibat uçotunun təşkili,layihələndirilmənin avtomatlaşdırılması, texnoloji proseslərin idarə edilməsi sistemləri göstərmək olar. Korporativ şəbəkələrin ən son məqsədi konkret tətbiqi sahəsinin proqramlarında nəzərdə tutulub, lakin onların əlverişli işləməsi üçün başqa təbəqlərin altsistemləri öz funksiyalarını icra etməlidirlər[11,12].

Təhlükəsizlik siyasəti informasiyanın və onunla əlaqəli olan resursların mühafizəsinə görə nəzərdə tutulmuş, sənədləşdirilmiş idarəedici qərarlar toplusudur. Korporativ şəbəkənin təhlükəsizlik siyasəti şəbəkə ehtiyatlarına giriş qaydalarına və istifadə şərtlərinə nəzarəti, şəbəkənin idarə olunması qaydalarını,şəbəkənin növbəti inkişafını və s.təsəvvür edir. Praktiki nöqteyi nəzərdən təhlükəsizlik siyasəti 3 mərhələyə ayrılır:

- Şirkət müdirləri tərəfindən verilən,bütövlükdə şirkətə aid olan və son dərəcə vahid xarakter daşıyan qərarlar
- Informasiya təhlükəsizliyinin başqa-başqa tərəflərinə aid olan məsələlər
- Informasiya sisteminin müəyyən xidmətləri

İstənilən korporativ şəbəkənin qurulması zamanı verilənlərin ötürülməsinin təhlükəsizliyi və korporativ informasiyanın icazəsiz daxil olmalardan mühafizəsi məsələlərinə ciddi şəkildə fikir verilməlidir.

Informasiyanın təhlükəsizliyinin yeni üsulları ali səviyyədə mühafizəsini təşkil edir. Şəbəkələrarası ekranlar (ŞAE) virtual xüsusi şəbəkələr(VXŞ) təşkili, icazəsiz daxil olmaların aşkar edilməsi sistemləri və digər vasitələr korporativ şəbəkələrin hər hansı hissəsində informasiyanın xətasız ötürülməsini təşkil etməyə imkan yaradır. Şirkətin informasiya resurlarını kənar müdaxilələrdən qorumaq üçün korporativ şəbəkələrdə demilitərizə zonası (DMZ) yaradılır[16,17,18].



Şəkil 3.13. Korporativ şəbəkənin təhlükəsizliyinin təmin edilməsi sxemi

Bu zona azçıq şəbəkə (məs, İnernet) ilə şirkətin daxili şəbəkələr içərisində bufer rolunu oynayır. Bu zonada adətən WWW server, poçt serveri yerləşdirilir. DMZ-də əlaqlərin və paketlərin idarə edilməsi ŞAE-nın köməyi ilə reallaşdırılır. Korporativ şəbəkənin subyektlərinin İnternetə əv subyektlərin İnternetdən korporativ şəbəkəyə daxilolmalarırını idarə edilməsi sistemi məhz ŞAE və Web-serverin əsasında yaradılır[1,4,5,6].

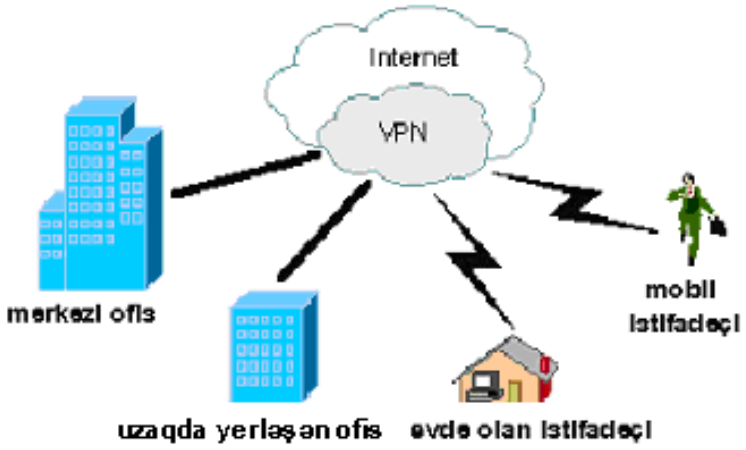
Korporativ şəbəkənin mühafizəsinin təşkil edilməsi dedikdə, onun iş prosesinə icazəsiz daxilolmaların və bununla belə aparat vasitələinin, proqram təminatının və verilənlərin dəyişdirilməsi, oğurlanması, ləğv edilməsi və korlama cəhdlərinə qarşı davamlılığın təmin edilməsi anlaşılır. Korporativ şəbəkənin mühafizə infrrastrukturu bunlar daxildir:

- Daxilolmaya nəzarət
- Autentifikasiya

- Şifrələmə və yaxud elektron- rəqəm imzası (ERİ)
- Kontent analizi

Korporativ şəbəkənin bu infrastrukturu haqqında növbəti fəsildə qeyd ediləcək.

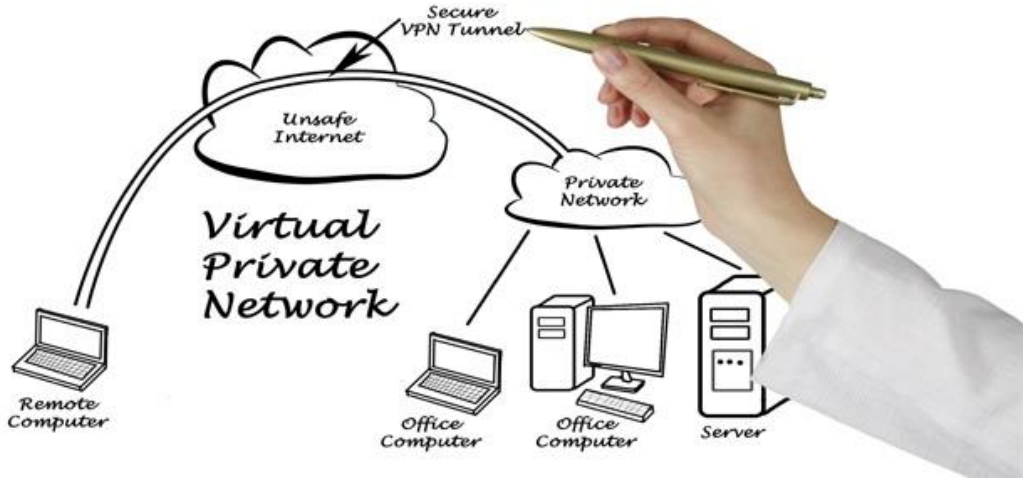
Indi isə son vaxtlar telekommunikasiyanın virtual xüsusi şəbəkələri(VXŞ) haqqında danışaq. Bu şəbəkələrə maraq getdikcə dahada artmaqdadır. Uzaqda yerləşən şöbələrin və subyektlərin İnternet vasitəsilə korporativ şəbəkəyə qoşulmasının maliyyə baxımdan ucuz olması səbəbindən korporativ şəbəkəyə çəkilən xərclərin azaldılması şərti ilə əlaqəlidir.



Şəkil 3.14. Virtual xüsusi şəbəkə.

Virtual xüsusi şəbəkənin gizli verilənləri açıq rabitə kanalları üsulu ilə ötürülməsi üçün təhlükəsiz real şəbəkə qurmağa şərait yaradan texnologiyadır[17,18].

Bu texnologiyaların vacib əhəmiyyəti korporativ IP- trafikinin ötürülməsi üçün internet şəbəkəsinin magistral kimi isttifadə olunmasıdır. Virtual xüsusi şəbəkələr istifadəçilərin uzaqda yerləşən şəbəkələrə və bir neçə lokal şəbəkələrin birləşməsi tapşırıqlarının həlli üçün nəzərdə tutulmuşdur. Virtual xüsusi şəbəkənin strukturu QŞ-nin kanallarını,təhlükəsizlik protokollarını və marşutlayıcıları özündə cəmləşdirir.



Şəkil 3.15. VPN strukturu

Uzaq məsafələrdə yerləşdirilmiş lokal şəbəkələri korporasiya şəbəkəsinə uyğunlaşdırmaq üçün verilmiş virtual kanaldan istifadə edilir. Bu cür birləşmənin quraşdırılması üçün tunelləşdirmə metodundan istifadə edilir. Tunelin təşəbüskarı lokal şəbəkənin paketlərini başlığında tunelin təşəbbüskarının və terminatorunun ünvanları yerləşən yeni IP paketlərə kapsullaşdırır[2,4,5].

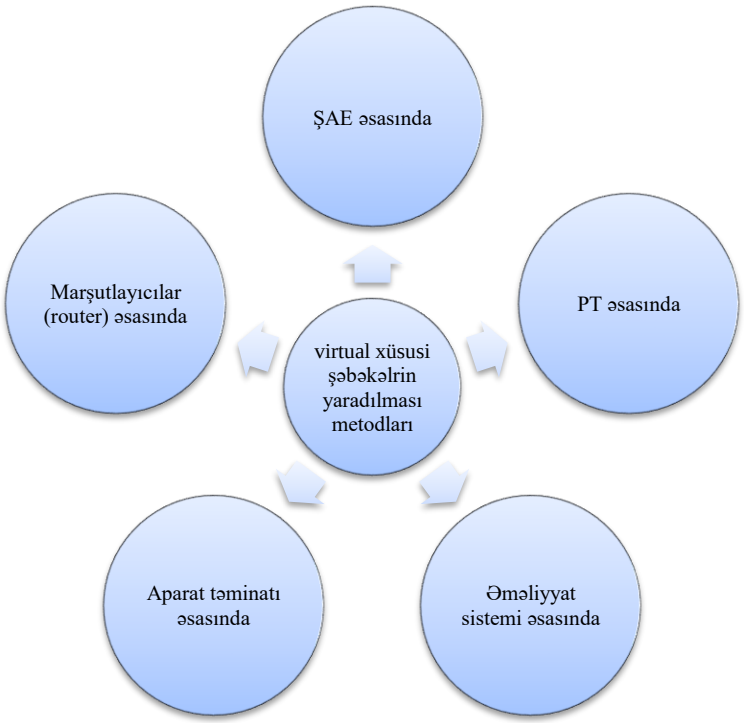
		IP-başlıq	Verilənlər
Yeni IP-başlıq	Təhlükəsizlik başlığı	Şifrlənmiş köhnə IP-paket	

Cədvəl 1.1 IP-paketin yeni IP-paketə kapsullaşdırılması

Tunelin o biri başında bu paketi ayırmaq üçün tunelin terminatoru əks proses həyata keçirir. Qeyd olunduğu kimi, bu cür ötürmələr həyata keçirilən zaman verilənlərin gizliliyi və tamlılığı məsələlərinin diqqət olunması tələb olunur ki, bu prosesləri sadə tunelləşdirmə ilə həyata keçirmək qeyri mümkündür. Göndərilən məlumatın gizliliyini təşkil etmək üçün tunelin hər iki tərəfi üçün eyni olan şifrələmə alqoritmini istifadə etmək vacibdir.

- Ayrı-ayrı avadanlıqlar və proqram təminatları sahəsində virtual xüsusi şəbəkəni qurulması üçün müəyyən standart mexanizmi lazımdır.IPsec (İnternet

Protokol security) protokolu virtual xüsusi şəbəkə qurulmasının belə bir mexanizmidir. IPSec virtual xüsusi şəbəkənin bütün standart üsullarını əks etdirir. Bu protokol tunel qurularkən identifikasiya metodlarını, tunelin əsas nöqtələri içərisində istifadə edilən şifrələmə üsullarını və bu nöqtələr içərisində şifrələmə açarlarının mübadiləsinin və idarə edilməsinin mexanizmlərini təyin edir. Bu protokolun əskik tərəfi ınternet protokolu ilə əlaqəli olmasıdır. Virtual xüsusi şəbəkənin yaradılmasının başqa protokolları Ascend Communication və 3 Com təşkilatları tərəfindən hazırlanmış PPTP (point-topoint tunelling protocol), Cisco Systems şirkətinin qurduğu L2F (Layer 2 Forwarding) və göstərilən protokolların kombinasiyası olan (Layer 2 Tunelling Protocol) protokollarıdır. Lakin bu protokollar IPSec protokolundan fərqli olaraq tam funksiyalı deyil (məs, PPTP protokolu şifrələmə üsulunu təyin etmir). IPSec protokolu IKE (İnternet Key Exchange) protoklu ilə birgə fəaliyyət göstərir. İKE-məlumatların tunel vasitəsilə ötürülməsi müddətində kənar müdaxilələrdən mühafizəsini təşkil edir. Bu protokol kənarda yerləşən qurğular arasında kripoqrafik açarların mühafizəsini idarə olunması və mübadiləsi problemlərini həll edir,IPSec protokolu isə şifrələyir və təsdiq edir. IKE təhlükəsiz əlaqə qurmaq üçün açıq açarlı şifrələmə mexanizmindən tətbiq edərək açarların ötürülməsi prossesini avtomatlaşdırır[2,3,4,5]. Bundan əlavə İKE ilə yaradılmış əlaqənin açarını dəyişməyə imkan yaradır ki, bu da məlumatların gizliliyini gözə çarpacaq dərəcədə artırır. Virtual xüsusi şəbəkələrin yaradılması başqa-başqa üsulların əsasında reallaşdırıla bilər. Bu vasitələr proqram və proqram-aparat əsasında ola bilər.



Şəkil 3.16.

Virtual xüsusi şəbəkələrin yaradılması metodunun seçilməsi zamanı vasitələrin səmərəliliyi faktorunun əsas götürülməsi tələb edilir. Məlәsən əgər marşutlayıcı (router) öz prossesorunun gücünün son həddində işləyirsə,onda vitual xüsusi şəbəkə tunelinin əlavə edilməsi və məlumatların şifrələnməsinin və yaxud deşifrələnməsinin istifadəsi bütün şəbəkənin işini dayandıra bilər. Aparılan təcrübələr əsasında virtual xüsusi şəbəələrin yaradılması üçün xüsusiləşdırılmiş avadanlıqların tətbiqi daha münasibdir,ancaq maddi imkan məhdudiyyəti varsa, onda proqram həlli seçmək olar[4,5,6,7].

3.3. Korporativ şəbəkələrin xüsusiyyətləri

Korporativ şəbəkənin xüsusiyyətlərindən ən vacib cəhətləri bunlardır:

- Böyük əhatəli olması-korporativ şəbəkələr öz aralarında mürəkkəb şəkildə əlaqələnmiş çoxsaylı kompüterləri geniş ərazidə cəmləşdirir

- Qeyri- bircinsliliyi-cihazların, protokolların, əməliyyat sistemlərinin, tətbiqi proqramların qeyri-bircinsliyi

- Qlobal şəbəkənin istifadə edilməsi-korporativ şəbəkələri yaradarkən uzaq məsafədə yerləşən müxtəlif kompüterləri və lokal şəbəkələri uyğunlaşdırmaq üçün bütün növ qlobal əlaqə kanallarından (QƏK) və həmçinin telefon kanallarından,radiokanallarından, peyk rabitəsindən, kanal və paket komutasiyalı şəbəkədən istifadə olunur

- İnteqrasiyalı olması-korporativ şəbəkələrin qeyri-bircins hissələri və altşəbəkələri istifadəçilərə bütün lazımi resurslara mümkün qədər şəffaf müaciət imkanı verərək,birlikdə işləməlidir

- Etibarlılığa yeksək tələb- Korporativ şəbəkələrdə şirkət üçün strateji əhəmiyyətli tətbiqi proqramlar istifadə edilən texniki və proqram təminatlarının etibarlılığına yüksək tələb qoyulmalıdır[7,8,9]

- Şəbəkənin idarə olunmasına yüksək tələb- korporativ şəbəkələrinin böyük miqyaslı olması pmu idarə etmək üçün çox funksiyalı vasitə tələb olur. Əks halda Korporativ şəbəkəni istismar edən çoxlu sayda mütəxəssislərə çəkilən xərclər gəlirdən çox olar. Korporativ şəbəkənin inzibatçılarının baş verən imtinalara operativ reaksiya verən sistemə yox,imtinalar haqqında əvvəlcədən xəbər verən sistemə ehtiyacı olur

- **Həll olunan problemlərin universal xarakterli olması** – LŞ-nin bir qayda olaraq ixtisaslaşdığı halda KŞ üçün müxtəlif məsələlərin olması adi haldır, bunlardan karguzarlıq, texnoloji proseslərin avtomatlaşdırılması, təcrübi proqramların yaradılması, informasiya axtarışı və b.

- **Əhatə olunan texniki problemlərin genişliyi**–Korporativ Şəbəkənin lahiyələndirilməsi zamanı çoxsaylı texniki məsələlər (fərdi kompüterlərin, Əməliyyat Sisteminin, tətbiqi proqramların, Lokal Şəbəkələrin kabel sisteminin, qlobal rabitə növünün seçilməsi,müxtəlif şəbəkə arxitekturlarının

uzlaşdırılması, müxtəlif kommunikasiya avadanlığının əsasında şəbəkənin strukturlaşdırılması məsələləri) meydana çıxır[14,15,16].

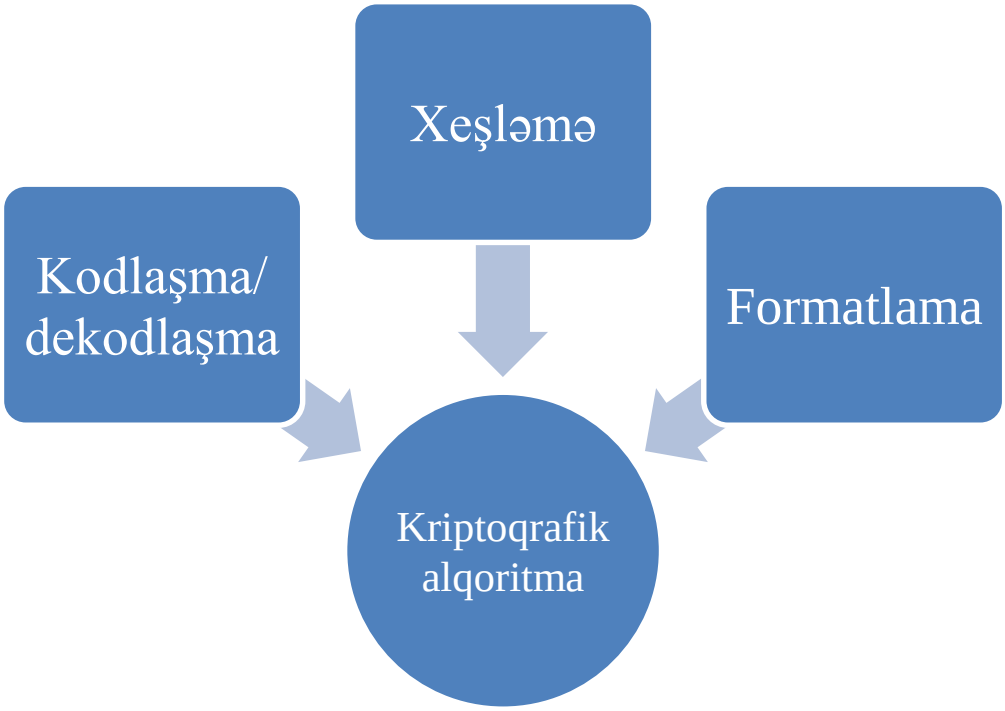
IV FƏSİL.Azərpoçt MMC-nin korporativ şəbəkəsinin "kriptomühafizə" üsullarının tədqiqi

4.1. Kriptoqrafiyanın əsasları

20-ci əsrin 70-ci illərinə kimi ötürülən informasiyanın şifrələnməsi metodlarının yaradılması və öyrənilməsinə aid olan elm sahəsinə və praktiki fəaliyyətinə kriptoqrafiya deyilirdi.Hal-hazrda elm və texnikanın inkişafı , praktiki fəaliyyətin bu sahəsi inkişaf ilə bağlıdır,verilənlərin muhafizə sisteminin kriptoqrafik təhlilini və tətbiqni reallaşdırır[2,3,5].

Kriptoqrafik sistem anlayışı dedikdə kriptoqrafiya üsullarından tətbiq etməklə avtomatlaşdırılmış məlumat sistemlərində və yaxud şəbəkələrdə məlumatın təhlükəsizliyinin təmin olunmasını reallaşdıran sistem başa düşülür.Demək olar ki,bu üsulla alt sistemin kodlanması subyektin identifikasiyası elektron rəqəmsal imza və digərlərindən də tətbiq edilir.

Kriptoqrafiya üsulları dedikdə məlumatın kriptoqrafik dəyişdirilməsindən istifadə olunmaqla məlumat təhlükəsizliyinin təmin olunması üçün faydalı olan imkan və metodlar başa düşülür. Ümumiyyətlə kriptoqrafik vasitələr dedikdə kripto sistem vəzifəsini yerinə yetirən digər qurğular, sənədlər və proqramlar nəzərdə tutulur. Məlumatın kriptoqrafik çevrilməsi dedikdə kriptoqrafik alqoritmlərin birindən tətbiq etməklə məlumatın çevrilməsi anlaşılır.



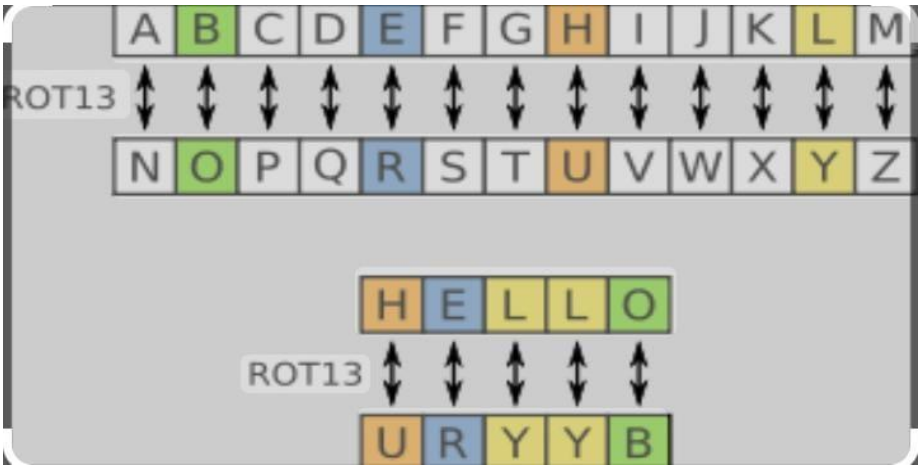
Şəkil 4.1.

Sezar şifrələməsi- tarixdə ilk dəfə Roma sərkərdəsi Yuli Sezar tərəfindən işlədilmiş olan şifrələmə metodudur. Tarixin ilk kriptoloji fikirləri ingilis dilində transposition və substitution cipher adını daşıyır. Yəni yerdəyişdirmə və hərf əvəzetmə şifrələnməsi adlanır. Bu üsullardan birincisi bir yazıdakı hərflərin yerini dəyişdirərək ikincisi isə hərfləri başqa hərflərlə əvəz edərək əldə edilir. Bu şifrələməni istifadə edən ən məşhur şifrələmə üsulu elə Sezar şifrələməsidir. Adını çəkdiyimiz şifrələmə metodikasının işləmə prinsipi belədir:hər hərf özündən bir neçə addım sonra gələn hərfi istifadə etməklə əvəz edilir ki, buna misal olaraq bir neçə hərfdən ibarət olan sözü şifrələyərək sezar metodunun necə işlədiyini göstərmək olar[9,10,11,12].

Sezar şifrələməsini sındırmaq çox asan məsələdir. Bir filoloq bir dildə ən çox istifadə edilən hərfləri tapa bilər. O hərlər ilə mesajlar ən çox istifadə olunan hərfləri qarşılaşdırmaqla hansı hərfin hansı hərf ilə dəyişdirildiyini tapa bilər. Bu isə mətnin deşifrələnməsi adlanır. Sezar şifrələnməsnin riyazi ifadəsi aşağıdakı kimidir:

$$a=(b+c) \bmod k$$

$$b =(a+k-(c \bmod k)) \bmod k$$



Cəvəl 4.1 Sezar şifrələməsi

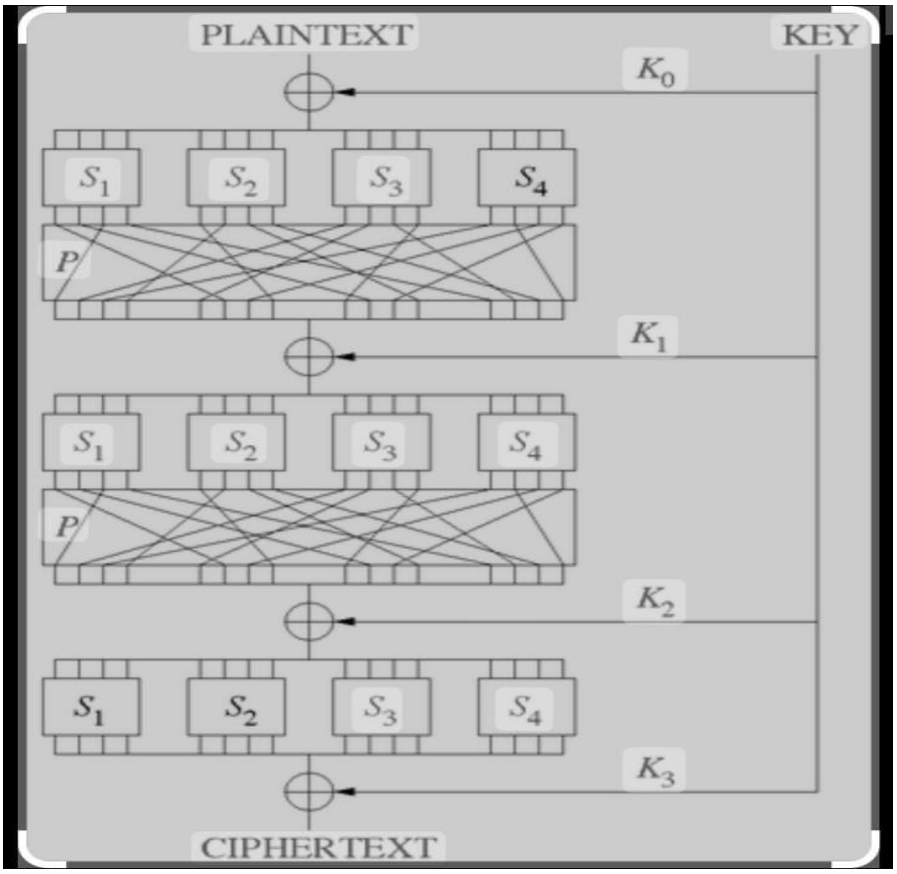
Mətn: Kriptoqrafiya

Şifrələnmiş mətn: Lşksüpmşcğkac

Əvəzləmə (substition)-kriptoqrafiyada SP-şəbəkə və ya yerinə qoyma-əvəzetmə şəbəkəsi (SPN),AES (Rijndael),3-Way, Kuznyechik,PRESENT,SAFER,SHARK və Square kimi blok şifrələmə alqoritmlərində istifadə edilən bir riyazi əməliyyatlar toplusudur.

Əvəzetmə şifrələməsinin məqsədi əlifbadakı hər simvolu eyni əlifbadan fərqli simvolla əvəz etməkdir. Müvafiq olaraq, cədvəl yaradılır və hər simvola uyğun olan alternativ simvol cədvəldə saxlanılır. Mesajı şifrələmək istəyən şəxs bu cədvəlin köməyi ilə hər simvolu bir-bir uyğun simvola çevirir. Şifrələnmiş mesajı açmaq istəyən şəxs eyni cədvəldə bunun əksini edir[11,13,14].

Şifrəni açmaq üçün eyni açarı olan şəxs tərs prosesi tətbiq etməklə cədvəldə hansı hərfin hansı hərfə uyğun olduğunu tapacaq və orijinal "ata və baba" mesajını tapacaq.



Cədvəl 2.2 Əvəzetmə (substitution) şifrələməsi

Bu şifrələmə metodunun məqsədi həndəsədə xəttin tənliyi kimi tanınan y=ax+b xətti funksiyasından şifrələmə prosesində istifadə etməkdir. Müvafiq olaraq, x şifrələnəcək mesajı (sadə mətn), y şifrəli mesajı (şifrə mətni), a və b cütü açarı təşkil edir.

Misal mesaj: “baba baba”

Açar: (3,2) yəni a=3, b=2 kimi verilir

Şifrələnmiş mesajın yaradılması: Əgər onun b hərfi üçün 2-ci hərf olduğu güman edilirsə, o, 3×2 + 2 = 8, yəni əlifbanın 8-ci hərfi kimi tapılır. Bu hərf 'h' hərfidir. Digər hərflər üçün də eyni şəkildə hesablanır. Məsələn, 'e' hərfinə uyğun gələn hərf üçün 3×5 +2 = 17, yəni 'q' hərfi var.

Şifrələnmiş mesaj: “hehe nqnq”

Demək olar ki, bu şifrələmə üsulu əslində əvəzedici şifrədir. Müvafiq olaraq, yalnız hansı simvol bir formulla əlaqəli olan simvolla əvəz olunacaq.

Bu şifrələmə üsuluna hücum etmək üçün tezlik (Frekans) analizi metodundan istifadə edilə bilər.

Encryption: Key Values a=17, b=20

Original Text	T	W	E	N	T	Y		F	I	F	T	E	E	N
x	19	22	4	13	19	24		5	8	5	19	4	4	13
ax+b % 26*	5	4	10	7	5	12		1	0	1	5	10	10	7
Encrypted Text	F	E	K	H	F	M		B	A	B	F	K	K	H

Decryption: a^-1 = 23

Encrypted Text	F	E	K	H	F	M		B	A	B	F	K	K	H
Encrypted Value	5	4	10	7	5	12		1	0	1	5	10	10	7
23 *(x-b) mod 26	19	22	4	13	19	24		5	8	5	19	4	4	13
Decrypted Text	T	W	E	N	T	Y		F	I	F	T	E	E	N

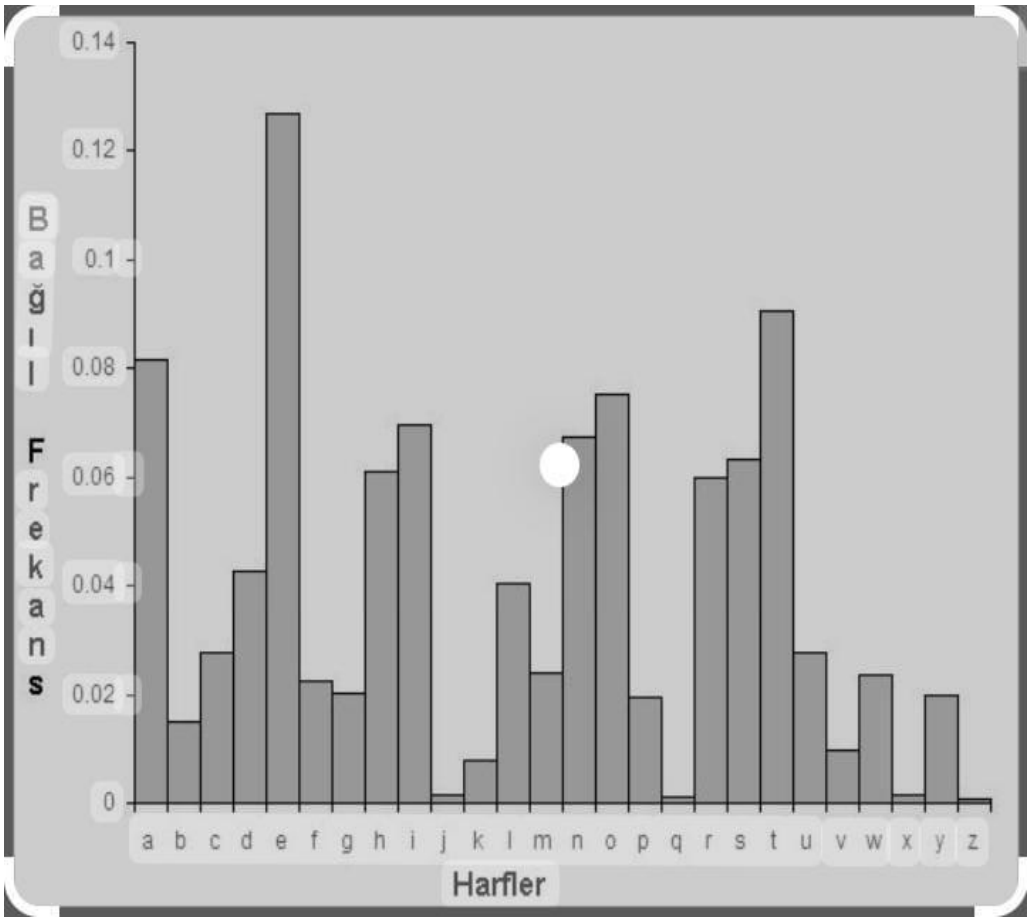
Cədvəl 2.3 Affine cipher tətbiqi

Kriptoanaliz-kriptoqraflar tərəfindən şifrələnmiş mətnlərin təhlili vəŞifrələrin deşifrə edilməsi ilə məşğul olan kriptoqrafiyanın alt bölməsidir.Bu işi görən insanlara kriptoanalitiklər deyilir. Şifrə mətnindəndüz mətnin, yəni orijinal mətnin əldə edilməsi prosesidir[4,6,11].

Frekans analiz-Şifrələnmiş mətnə hücum üsullarından biri tezlik analizinin aparılmasıdır. Bu üsulda mətndəki hərf tezliklərinə uyğun tezlik cədvəli yaradılır. Bu cədvəl orijinal mesajın göndərildiyi tezlik tezlikləri ilə müqayisə edilir və bəzi xarakterik hərfləri təxmin etmək olar.

Məsələn, ingilis dilində e hərfi digər hərflərdən daha çox istifadə olunur. Bu halda şifrlənmiş mətndə ən çox rast gəlinən hərfin yəqin ki, e hərfi olduğunu demək olar.

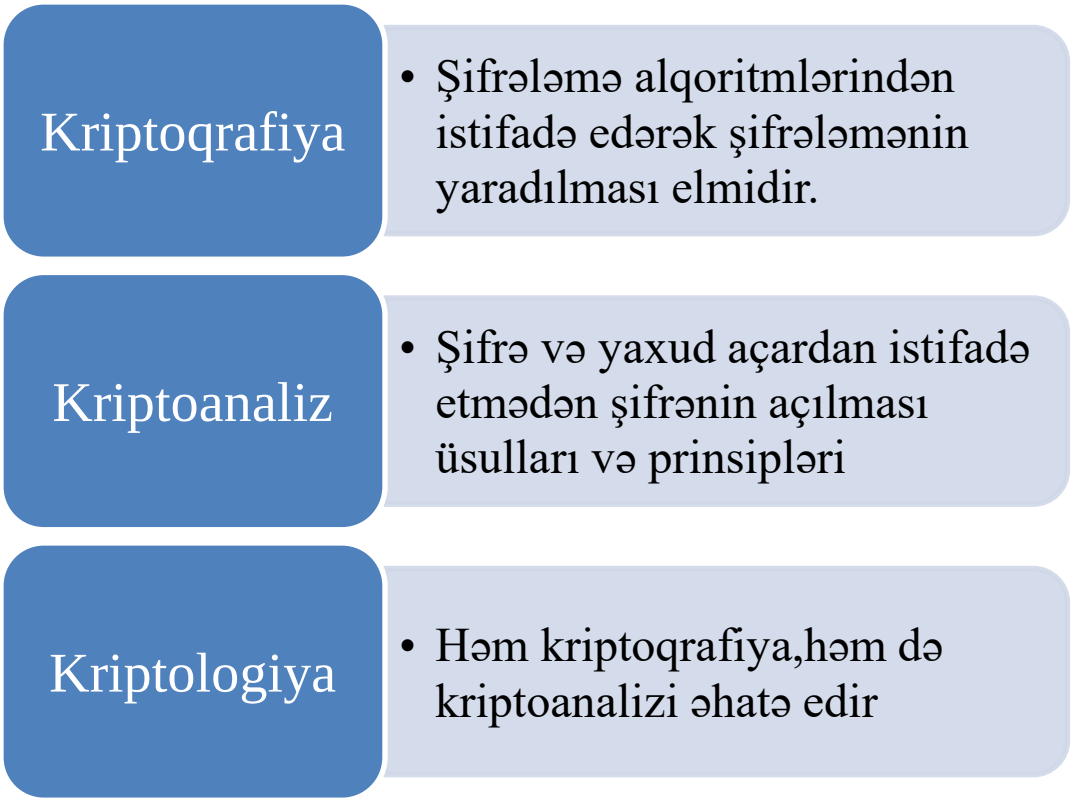
Aşağıdakı cədvəl ingilis dilində hərflərin tezlikləri verilmişdir.



Cədvəl 2.3 Verilənlərin təhlükəsizliyində Frekans analiz

Məlumatların məxfiliyinin təmin edilməsi müasir dövrdə mühüm məsələdir. Bu yazıda məlumatların məxfiliyini (və bütövlüyünü) təmin etmək üçün istifadə edilən ən çox istifadə edilən simmetrik və asimmetrik şifrələmə alqoritmləri araşdırılacaqdır

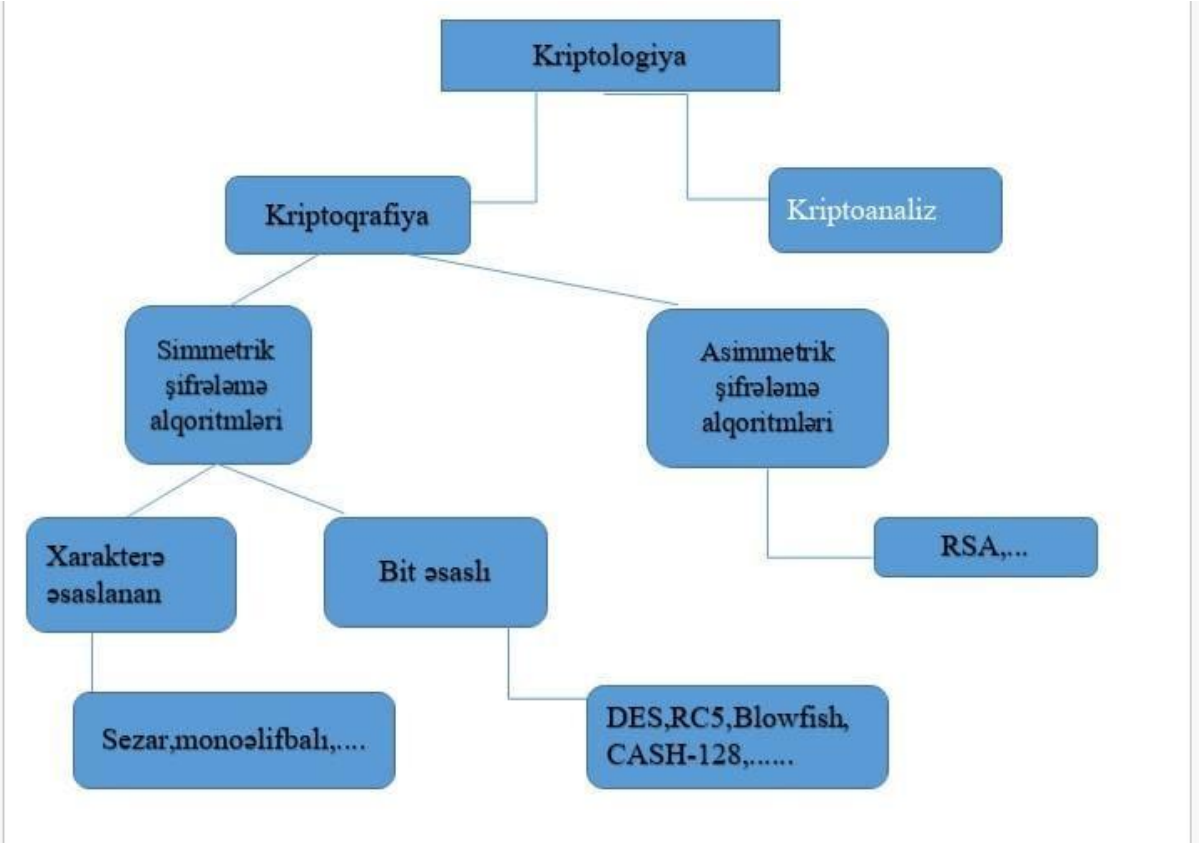
Əsas anlayışlar



Şəkil 4.2.

Kriptoqrafiyada istifadə olunan bəzi əsas anlayışlar aşağıdakılardır:

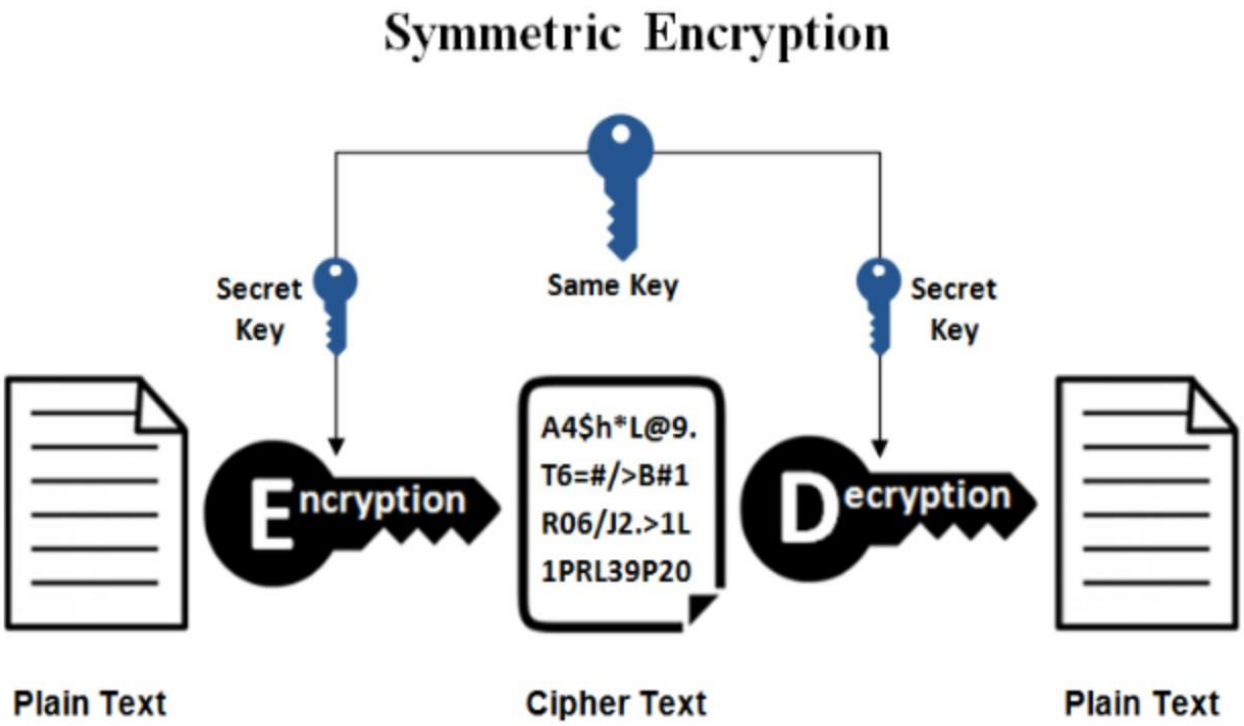
- Plaintext: əsas mətn
- Ciphertext: şifrələnmiş mətn
- Cipher: Əsas mətni şifrələnmiş mətnə çevirən şifrələmə alqoritmi
- Encrypt: Əsas mətni şifrəli mətnə çevrilməsi
- Decrypt: Şifrələnmiş mətnin əsas mətnə çevrilməsi



Şəkil4.3.Kriptologiyanın struktur sxemi

4.2. Açıq açarla şifrələmə. Elektron imza.

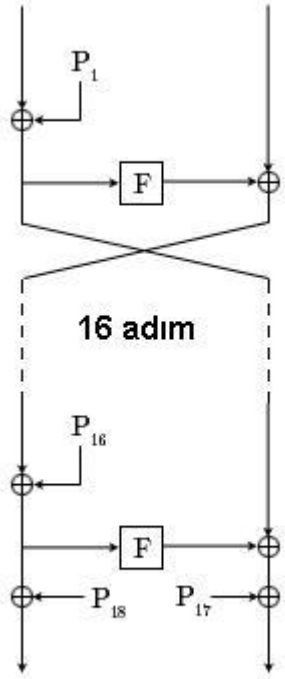
Simmetrik Şifrələmə Alqoritmləri-Simmetrik şifrələmə məlumatı şifrələmək və deşifrə etmək üçün yalnız bir məxfi açarı ehtiva edən ən sadə şifrələmə növüdür. Simmetrik şifrələmə kriptoqrafiya üsulları və şifrələmə alqoritmləri arasında ən qədim və ən yaxşı məlum olan texnikadır. O, nömrə, söz və ya təsadüfi hərflər silsiləsi ola bilən gizli açardan istifadə edir[18,19,20].



Şəkil 4.4.Simmetrik şifrələmə

Blowfish- Feistel şəbəkəsindən istifadə edən blok şifrələmə üsuludur. Bruce Schnider tərəfindən 1993-cü ildə DES-ə alternativ olaraq inkişaf etdirilən metod simmetrik, açarlı, bloklu şifrə üsuludur.Schneier-in bu metodu inkişaf etdirməsinin əsas səbəbi onun DES kimi patentli metodların istifadəsinə alternativ olmasıdır. Bubblefish şifrələməsinin bütün ölkələrdə pulsuz və patentsiz istifadə ediləcəyi arqumenti getdi[18,19].

Blowfish şifrələməsində 16 addımdan ibarət feistel şəbəkəsindən istifadə edilir. Bu şəbəkədə mesaj ölçüsü 64 bitdir və açarın ölçüsü 32 ilə 448 bit arasında dəyişir.Onların işləməsi üçün 4 kilobaytdan çox RAM tələb olunur.Buna görə də, onlar ən kiçik quraşdırılmış sistemlərdə istifadə edilə bilməz.



Şəkil 4.5.Blowfish şifrələməsi

DES-Bu, dünyada ən çox istifadə edilən simmetrik şifrələmə alqoritmlərindən biridir. Feistel şifrələmə metodundan istifadə edir. Blok şifrəsindən istifadə edərək, DES proses zamanı 56 bitlik açardan istifadə edərək 64 bitlik məlumatları şifrələyir. DES alqoritmində 16 raund əvəzetmə və köçürmə əməliyyatları yerinə yetirilir[16,17,19,20].

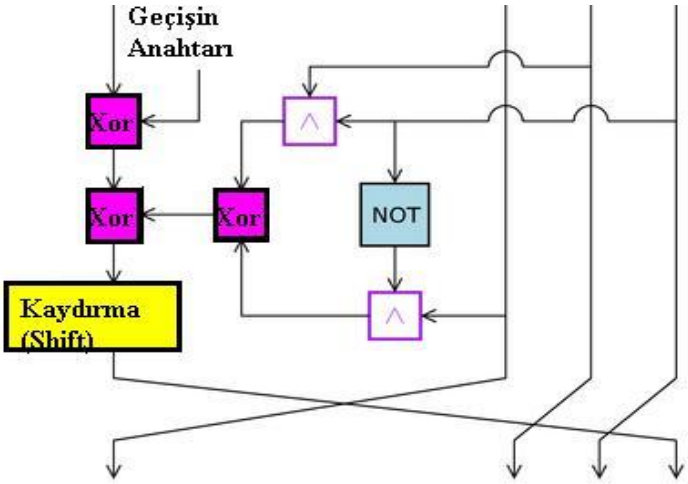
Açarın uzunluğu qısa olduğu üçün qırılıb. Bunun üzərinə Triple-DES (şifrləmə-deşifrə-şifrələmə), yəni 3DES kimi işlənib hazırlanmışdır. 3DES, DES-in ardıcıl 3 dəfə istifadəsidir və açar uzunluğu 168 bitdir. Buna görə standart DES-dən 3 dəfə yavaşdır, lakin bu gün SSH kimi tətbiqlərdə istifadə olunur. AES-in tətbiqi ilə DES populyarlığını itirdi. Çünki AES-dən 6 dəfə yavaşdır.

AES-DES sındırıldıqdan sonra yeni axtarışa başlandı və AES simmetrik şifrələmə alqoritmi yaradıldı. Bu, DES-in gücləndirilmiş versiyasıdır və blok şifrələmə alqoritmindən istifadə edir. AES-də bloklar 128 bitə qədərdir.

AES DES-dən daha sürətlidir. O, 128, 192 və 256 bit uzunluğunda şifrələri dəstəkləyir. Bu gün ən məşhur alqoritmlərdən biridir və güclü hücumlara davamlı hesab olunur.

RC2-Bu, kompüter elmində və məlumat təhlükəsizliyində istifadə edilən şifrələmə alqoritmlərindən biridir. Blok şifrəsinin bir növü olan RC2, RC4, RC5 və RC6 kimi sonrakı şifrələrin primitiv versiyasıdır.

O, sadəcə olaraq 64 bitlik (ikili) feistel şəbəkəsindən istifadə edərək 18 raundda dəyişən uzunluqlu açarla şifrələyir. Bu keçidlərdən 16-sı qarışdırmaq, 2-si isə əzmək üçündür.

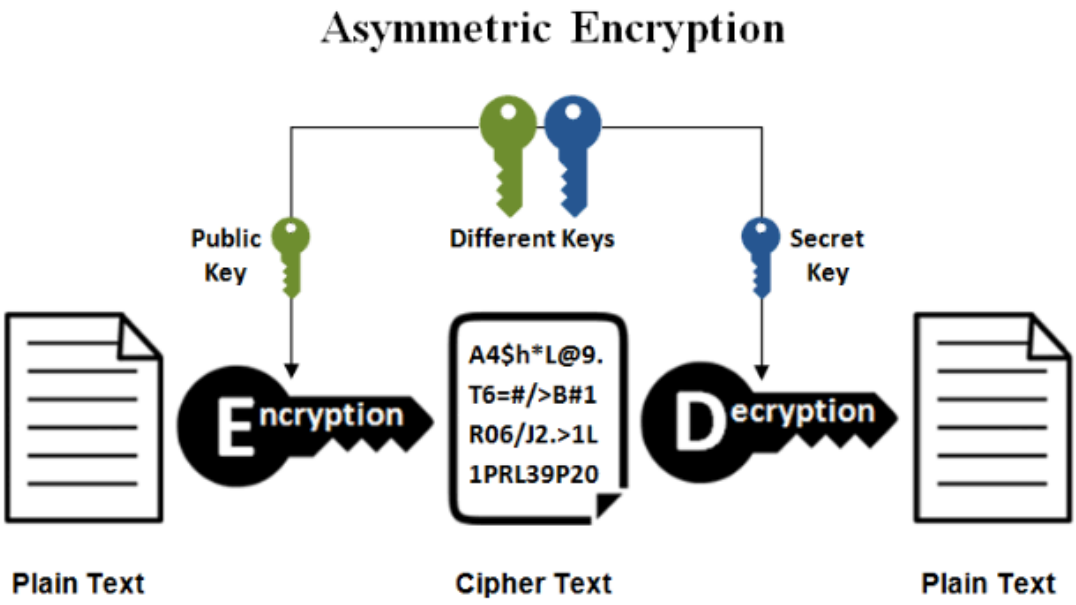


Şəkil 4.6.RC2 üçün feistel şəbəkəsinin keçidi

Bundan əlavə, bloklar arasındakı əlaqələrə uyğun olaraq blok şifrələməsinin müxtəlif rejimləri mövcuddur. Bunlar aşağıda verilmişdir.

Asimmetrik Şifrələmə Alqoritmləri-Şifrələmə və deşifrə əməliyyatları üçün müxtəlif açarların istifadə olunduğu şifrələmə sistemidir[15,18].

Açıq açar infrastrukturu internetdə təhlükəsiz ünsiyyəti təmin edən TLS (SSL-in qabaqcıl versiyası) protokolu, təhlükəsiz e-poçt rabitəsində istifadə edilən PGP protokolu və faylların şifrələnməsi və şifrəsinin açılması üçün istifadə edilən GPG kimi protokollarda istifadə olunur.



Şəkil 4.7.Asimmetrik şifrələmə

Diffie-Hellman (DH)- Diffie və Helman tərəfindən icad edilən ilk asimmetrik şifrələmə alqoritmidir. DH iki iştirakçının əvvəlcədən heç bir məlumat mübadiləsi etmədən təhlükəsiz olmayan kanal vasitəsilə ümumi parol (təhlükəsiz) üzərində razılığa gəlməsi protokoludur. Açar mübadiləsi ilə alqoritmin əsas məqsədi iki istifadəçinin bir-birinə açarı etibarlı şəkildə ötürməsini və sonra bu açarın köməyi ilə bir-birinə şifrələnmiş mesajlar göndərməsini təmin etməkdir. Diffie-Hellman alqoritminin yaradılması ilə simmetrik şifrələmə alqoritmləri üçün əsas problem olan gizli açarın qorunması və paylanması böyük ölçüdə aradan qaldırıldı. Bununla belə, Diffie-hellman alqoritmi yalnız açıq məxfi açarı müəyyən etmək üçün istifadə olunur[13,19].

4.3. Kriptoqrafik protokollar

Protokol-müəyyən məsələlərin bərabər hüquqlu həll olunması üçün iki və daha çox tərəflər arasında qəbul edilən addımlar ardıcıllığına deyilir. Hər bir addım düzgün əməl olunmalı və bir məsələnin həlli üçün ediləcək əməliyyatlar növbəti əməliyyatlarla əvəz edilməlidi.Kriptoqrafik protokollar məlumatın ötürülməsi və qəbulu zamanı qeyd-

şərtsiz əməliyyatların həyata keçirilməsində həyata keçirilir. Bu vaxt kənar şəxs istifadəçilərin bir birinə ötürdüyü məlumata daxil ola bilmir. Kriptoqrafik protokolun yaradılmasında vacib tapşırıq budur ki, məlumatın ötürlməsi və qəbulu zamanı istifadəçilərin bir -birlərinə ötürdükləri məlumatların tamlığı dəqiq olsun[17,18,20].

Kriptoqrafik protokol xüsusiləşdirmədə birtərəfli funksiyalarda təxmini rəqəmlərin generasiyasında geniş tətbiq olunur.

Autentifikasiya protokolu

Autentifikasiya-kompüter sistemi istifadəçisinin şəxsiyyəti kimi bir iddianın sübut edilməsi aktıdır. Şəxsiyyətin və ya əşyanın şəxsiyyətini göstərən identifikasiyadan fərqli olaraq, autentifikasiya həmin şəxsiyyətin yoxlanılması prosesidir.

Autentifikasiya protokolu məlumatı kənar şəxs tərəfindən qorunmalıdır. Autentifikasiya protokolu 3 hissəyə bölünür.

1. Nəyisə əldə etməklə. Ən şox yayılmış üsul şifrənin əldə olunmasıdır.
2. Nəyəsə malik olmaqla(məs;plastik kartlar və s.).
3. Dəyişməyən əlamətlərə görə (barmaq izi, göz rəngi, səs tonu).

Autentifikasiya protokolu şəxsi məlumatların mühafizəsini təmin etmək üçün aşağıdakı səviyyədə təsnif edilir:

- Sadə autentifikasiya
- Ciddi autentifikasiya
- Ilkin səviyyə

Açarların dəyişilmə protokolu.

Açarların dəyişilmə protokolu vasitəsilə hər hansı məxfi açar iki və ya daha çox şəxslər arasında paylaşılır. Açarların dəyişilmə protokolu 3 hissəyə bğlünür:

1. Açarların artıq generasiya olunmuş ötürülmə protokolu
2. Ümumi açarın bərabər hazırlanma protokolu
3. Açarların əvvəlcədən bölüşdürlmə sxemi

Əvvəlcədən açarların bölüşdürlmə sxemi 2 aloqirtmdən ibarətdir: ilkin açarda məlumatın bölüşdürülməsi və açarın formalaşdırılması. Açarların bölüşdürülmə sxemi dayanıqlı olmalıdır.

Açarların dəyişmə protokolları arasında ən çox istifadə olunan Diffi-Hellman alqoritmidir. Alqoritm kanal yolu ilə açarların dəyişdirilməsində yararlı alqoritm olmalıdır.

Özünə məxsus xüsusiyyəti olan protokollar

Açarları dəyişmə protokolu və autentifikasiya protokolu kriptoqrafik protokollar sinifinə aiddir. Bununla bərabər elə protokollar vardır ki, onlar digər xüsusi problemlərin həlli üçün faydalıdırlar. Bu protokollar aşağıdakılardır:

- Səsvermə protokolu
- Eyni zamanda imza atma protokolu
- Qrup şəklində imzalama protokolu
- Danılmaz imzalama
- Kor-koranə imzalama
- Sirrin bölünmə protokolu .

SON NƏTİCƏ

Dissertasiya işinə əsasən Azərpoçt MMC-nin korporativ şəbəkəsində istifadə olunan kriptomühzafizə üsülları haqqında ətraflı məlumat verilmişdir.Bu üsüllar əsasında aşağıdakı işlərə baxılmış və bəzi nəticələr əldə edilmişdir:

1. Korporativ şəbəkədə istifadə olunan cihaz və avadanlıqlara ümumi baxılmış və ətraflı nəzəri analizi aparılmışdır. Bunun nəticəsi olaraq bəzi avadanlıqların yenisi ilə əvəz olunması təklif verilmişdir;

2. Aparılan analiz nəticəsində Azərpoçt MMC korporativ şəbəkənin arxitekturasının qurulması prinsiplərinin xüsusiyyətləri sxemlə təsvir olunmuşdur;

3. Korporativ Şəbəkənin layer 7 səviyyəsində də işləmə imkanı,bütün portları bağlayıb və yalnız lazım olan portları açmaq,Firewallda SSL decryption, inspection aktivləşdirmək – gələn və gedən trafiki oxumaq, analiz edilməsi,SD-WAN (Proqram təminatı ilə müəyyən edilmiş geniş sahə şəbəkəsi) dəstəkləməsi,Faylların filtirlənməsi,antivirus,web filtirlənməsi,daxili şəbəkəyə internet üzərindən təhlükəsiz qoşulmaq üçün vpn protokolundan istifadə etmə imkanı və şəbəkənin kriptomühafizəsi prosedurlarının üstün cəhətləri göstərilmişdir;

4. Sonuncu fəsildə blok şifrələmə alqoritmlərinin korporativ şəbəkədə üstünlükləri haqqında ətraflı geniş izah verilmişdir.Demək olar ki,bu gün blok şifrələmə alqoritmləri şifrələmənin tələb olunduğu bir çox sahələrdə istifadə olunur. Ona görə də bu alqoritmlərin gücü təhlükəsizlik baxımından çox önəmlidir;

5. Blok şifrələmə alqoritmlərinin gücü açarın uzunluğundan və hücumlara qarşı müqavimətindən asılıdır. Bundan əlavə, geniş açar axtarış hücumu da hücumların uğurlu sayılması üçün meyar kimi istifadə edilir. Başqa sözlə, əsas axtarış hücumundan daha ucuz başa gələn hücumlar uğurlu sayılır. Buna görə də alqoritmin dizaynında istifadə olunan açarların idarə edilməsi, yəni əsas açardan açarların alınması üsulu, S qutuları və dövrlərin sayı da alqoritmin hücumlara qarşı müqavimətinə təsir göstərir.

ƏDƏBİYYAT

1. M.H. Həsənov. Optik veriliş sistemləri. - Bakı, Çaşıoğlu. 1998.

2. M.H. Həsənov. Optik veriliş şəbəkəsinin avadanlıqları. Sabah, - Bakı. 2001.

3. T.M.Mansurov. Çoxkanallı telekommunikasiya sistemləri. -Bakı: Təhsil NPM, 2009. – 336 s.

4. T. M. Mansurov, C. Ə. Əliyev, G. İ. Quliyeva, G. Ə. Hüseynova. Optik ölçmələr. Dərs vəsaiti. - Bakı, AzTU, 2017. – 148 s.

5. Aysun Coşkun,Ülkü Ülker. Bilişim teknolojiler dergisi, Gazi Universiteti, Ankara Türkiye cilt 6,sayı 2, mayıs 2013.

6. İsmayıl Calallı (Sadıqov), “İnformatika terminlərinin izahlı lüğəti”, 2017, “Bakı” nəşriyyatı,

7. R.H. Şixəliyev. İnformasiya Texnologiyaları, Bakı 2017.

8. M.N.Əlizadə. İnformasiya təhlükəsizliyi, Dərslik, Bakı, “İqtisad universiteti“ nəşriyyatı, 2016. - 384 səh.

9. Musayev V.H., Qəmbərov M.M., Əliyeva Ş.X., Kompüter təhlükəsizliyinin aparat-proqram vasitələri., Bakı 2015.

10. Партыка Т.Л., Попов И.И. Информационная безопасность. Учебное пособие для студентов учреждений среднего профессионального образования.- М.: ФОРУМ: ИНФРА-М, 2004.

11. Крысин А.В. Информационная безопасность. Практическое руководство. -М.: СПАРРК, К.: ВЕК+,2003.

12. Тарасюк М.В. Защищенные информационные технологии. Проектирование и применение. -М.: СОЛОН-Пресс, 2004.

13. B.A.Nuranə, Ə.S.Nəsib, Q.N.Xeyrulla Korporativ şəbəkələrdə informasiya təhlükəsizliyi . Azərbaycan xalqının ümummilli lideri, görkəmli dövlət xadimi Heydər Əliyevin anadan olmasının 100 illiyinə həsr olunmuş tələbə və gənc tədqiqatçıların "Mütərəqqi texnologiyalar və innovasiyalar" mövzusunda Vll Respublika elmi-texniki konfransın materialları . 25-26may 2023-cü il, AzTU, Bakı, Azərbaycan. -5s (nəşriyyatda).