AZƏRBAYCAN RESPUBLİKASI TƏHSİL NAZİRLİYİ

AZƏRBAYCAN DÖVLƏT İQTİSAD UNİVERSİTETİ

"MAGİSTRATURA MƏRKƏZİ"

Əlyazması hüququnda

Hüseynov Rüfət Qəhrəman oğlu

"Telekommunikasiya sistemlərində informasiya təhlükəsizliyinin təmini"

mövzusunda

MAGİSTR DİSSERTASİYASI

İxtisasın şifri və adı:	060632 "İnformasiya texnologiyaları və sistemləri mühəndisliyi"
İxtisaslaşmanın adı:	"İnformasiya texnologiya və telekommunikasiya sistemləri mühəndisliyi"
Elmi rəhbər:	r.f.d., dos. Həsənova Z.B.
Magistr proqramının rəhbəri:	f.r.e.n., dos. Əliyeva T.Ə
Kafedra müdiri:	tex.e.d., akad. Abbasov Ə.M.

Bakı – 2020

Mündəricat

Giriş

Mövzunun aktuallığı. Bu gün dünyamız demək olar ki, tam olaraq bütövlükdə kompüterləşmə dövrü yaşayır. Həyatımızın istənilən sahəsinə müraciət etsək, artıq proseslərin ənənəvi yollarla həllərinin kənara atılaraq, kompüter, lokal və qlobal şəbəkələr, telekommunikasiya sistemlərindən istifadəyə üz tutduğunu görə bilərik. Əyləncə həyatımızda oyun tətbiqetmələrindən, hökumət işlərində sənədləşmə prosesləri və sənədlərin daşınması işlərindən, adi məişət həyatımızda kommunal ödənişlər də daxil olmaqla bir çox ödənişlərimizin onlayn formada həyata keçirilməsindən ta məlumat mübadiləsində istifadə etdiyimiz səsli, görüntülü zənglərə, sosial şəbəkələrə qədər hər bir sahədə artıq rəqəmsal dünyanın xidmətləri danılmazdır. Ancaq burada qeyd etməli olduğumuz xüsusi bir amil vardır ki, kompüterləşmənin həyatımızdakı hər sahəyə bu qədər geniş bir şəkildə addım atması həyatımızı, işlərimizi nə qədər asanlaşdırdı, nə qədər rahatlaşdırdısa da, bir o qədər də təhlükə mənbəyinə çevirdi. Bu gün hamımız rəqəmsal dünyanın xidmətlərindən kifayət qədər geniş, rahatlıqla istifadə edirik. Amma unutmayaq ki, əksər rəqəmsal proseslərdə bizim şəxsi məlumatlarımız, o cümlədə maliyyə büdcəmiz saxlanılır və ötürülür. Yaxşı bəs, həyatımızı etibar etdiyimiz bu bütün telekommunikasiya xidmətləri, onların güvənliyi nə qədər etibarlıdır? Bəli, bu sualdan da aydın olur ki, bu gün telekommunikasiya sistemlərinin həyata keçirdiyi bizim üçün önəmli proseslərdə, elə o ən az o proseslərin özü qədər əhəmiyyətli olan ən vacib məsələ məhz informasiya təhlükəziliyidir. İnformasiya təhlükəzisliyimizə gələ biləcək hər hansı zərər bizim üçün təhlükədir. Bu təhlükə isə müxtəlif formalarda baş verə bilər. Məsələn: ola bilər ki, telekommunikasiya sistemlərinin özünün informasiyanı təhlükəsiz saxla prinsipləri qaydasında deyil, və yaxud da ola bilər ki, günümüzdə artan xaker hücumları qarşısında dayanmağa qadir deyil. Fərq etməz, hər iki halda da bizimim haqda olan məlumatların itməsi, dəyişilməsi, ələ keçirilməsi, qarışdırılması və sairə kimi məsələlər bizim üçün təhlükə olaraq qalır. Təkcə bu səbəblər deməyə

əsas verir ki, telekommunikasiya sistemlərində informasiya təhlükəsizliyin təmin edilməsi bu gün rəqəmsal dünyada kifayət qədər aktual bir məsələdir.

Mövzunun öyrənilmə səviyyəsi. İndiyədək ayrı-ayrılıqda telekommunikasiya sistemləri və informasiya təhlükəsizliyi xarici alimlər tərəfindən kifayət qədər geniş işıqlandırılsa da, sırf telekommunikasiya sistemlərində informasiya təhlükəsizliyinin necə təmin edilməsi qaydaları çox az müzakirə mövzusu olmuşdur. Yerli mütəxəssislərə baxdıqda isə bu mövzuya ümumiyyətlə yer verimədiyini görürük.

Dissertasiya işinin məqsədi. Dissertasiya işinin məqsədi müxtəlif telekommunikasiya sistemlərində informasiya təhlükəsizliyin necə, hansı üsullarla, hansı prinsiplərlə, hansı qayda-qanun və standartlara əsaslanmaq təmin edildiyini araşdırmaq, onları komplektləşdirmək, mümkün təsnifatını hazırlamaq, fərqli texnologiyaların üstün və mənfi cəhətlərini ayırd etmək və mümkün təklif irəli sürməkdən ibarətdir.

Tədqiqatın predmeti. Tədqiqatın predmetini telekommunikasiya sistemlərində informasiya təhlükəsizliyinin nə qədər önəmli olduğunun ön plana çıxarılması, kompüterləşmənin tarixi boyunca informasiya təhlükəsizliyinin təşkili formalarının hansı istiqamətdə inkişaf etdirilməsi, müasir dövrdə bu məqsədlə hansı texnologiyaların tətbiq olunmasının araşdırılması və mümkün yeni üsulların tətbiqinin nəzərdən keçirilməsi təşkil edir.

Tədqiqatın obyekti. Tədqiqat obyekti kimi müxtəlif telekommunikasiya sistemləri, mobil şəbəkələr, qlobal şəbəkələr, internet dünyası, rəqəmsal aləm seçilmişdir.

Tədqiqatın elmi və nəzəri əsasları. Tədqiqatın elmi-nəzəri əsasını əsasən informasiya-kommunikasiya sahəsindəki xarici mütəxəssislərin kitabları, tədqiqat məqalələri, beynəlxalq standartlar, rəsmi statistikalar və s. təşkil edir.

Tədqiqatın informasiya bazası. Dissertasiya işinin hazırlanmasında əsasən, Beynəlxalq Telekommunikasiya Birliyinin əsas saytı, müasir yenilikləri, müxtəlif illərdəki elmi məqalələri, kitabları istifadə edilmişdir.

Tədqiqatın elmi yeniliyi. Tədqiqat işinin elmi yeniliyini aşağıdakılar göstəricilər müəyyənləşdirir:

- Telekommunikasiya sistemlərinin və informasiya təhlükəsizliyinin ayrı-ayrılıqda və birgə inkişaf xətti nəzərdən keçirilmişdir.
- Telekommunikasiya sistemlərində informasiya təhlükəsizliyinin kifayət qədər aktual və önəmli məsələ olması bu sistemlərin həyatımızdakı rolu və beynəlxalq statistikalar əsasında əsaslandırılmışdır.
- Telekommunikasiya sistemlərində informasiya təhlükəsizliyinin təmin edilməsi ən ali hökumət, qanun səviyyəsindən tutmuş ta adi verilənlərin müxtəlif üsullarla qorunması səviyyəsinə qədər araşdırılmışdır.
- Telekommunikasiya sistemlərində informasiya təhlükəsizliyi prinsipləri, ümumi və xüsusi üsullar, üsullar arasındakı fərqlər, müsbət və mənfi keyfiyyətlər fərqləndirilərək kompleksləşdirilmişdir.

Dissertasiya işinin strukturu. Dissertasiya işi giriş, 3 fəsil, fəsillərin alt kateqoriyaları, nəticə və təkliflərdən ibarət olmaqla ... səhfədir.

Dissertasiya işinin girişində mövzunun aktuallığı əaslandırılmış, onun məqsədi, predmeti və obyekti göstərilmiş, elmi-nəzəri əsasları, elmi yenilikləri və disstertasiya işinin strukturu göstərilmişdir.

Dissertasiya işinin birinci fəslində telekommunikasiya sistemləri və informasiya təhlükəsizliyi sahələrinə giriş edilmiş, dissertasiyanın məqsəd və predmetinə lazım olan ilkin anlayışlar müəyyən edilmiş, onların açıqlamaları verilmiş, telekommunikasiya sistemlərinin və informasiya təhlükəsizliyinin inkişaf tarixinə

qısaca nəzər salınmış, telekommunikasiya sistemlərinin cəmiyyətimiz üçün artan dinamik əhəmiyyətli rolu diqqətə çatdırılmışdır.

İkinci fəsildə telekommunikasiya sistemlərində informasiya təhlükəsizliyinin konseptual modeli təqdim olunmuş, arxitektura, ölçülər, standartlar, tənzimlənmə qaydaları, beynəlxalq təyin olunmuş İTU qaydaları nəzərdən keçirilmişdir.

Üçüncü fəsildə isə telekommunikasiya sistemlərində informasiya təhlükəsizliyinin təmin olunmasının müxtəlif aspektləri, müxtəlif tip kateqoriyalarda əsasən də günümüzdə daha çox yayılan mobil şəbəkələrdə informasiya təhlükəsizliyi ayrılıqda daha dərindən tədqiq edilmişdir.

Nəticə və təkliflər bölməsində isə araşdırmalar nəticəsində əldə edilmiş yekun xülasə, telekommunikasiya sistemlərində informasiya təhlükəsizliyinin gələcək inkişaf xətti proqnozları verilmişdir.

Ümumilikdə dissertasiya işi cəmi 81 səhifədən ibarətdir.

FƏSİL 1. TELEKOMMUNİKASİYA SİSTEMİNİN TƏHLÜKƏSİZLİYİ SAHƏSİNDƏ ƏSAS ANLAYIŞLAR, TELEKOMMUNİKASİYA SİSTEMLƏRİNİN BU GÜNƏ QƏDƏR İNKİŞAF XƏTTİ VƏ TELEKOMMUNİKASİYA SİSTEMLƏRİNİN HAZIRDA İNSAN CƏMİYYƏTİNDƏ ROLU

1.1 Telekommunikasiya nədir?

Telekommunikasiya işarələrin, siqnalların, mesajların, sözlərin, yazıların, şəkillərin, səslərin, videoların və ya hər hansı bir təbiətə aid məlumatların telefon, radio, müxtəlif növ kabellər, simsiz və peyk vasitələri, elektromaqnit sistemləri və sairə kimi müxtəlif texnologiyalar vasitəsilə uzaq məsafəyə ötürülməsidir. Telekommunikasiya hadisəsi o zaman baş verir ki, informasiyanı ötürən tərəflə qəbul edən tərəf arasında informasiyanın ötürülməsi prosesi rabitə texnologiyaları sayəsində həyata keçirilmiş olsun. Bu baxımdan elektrik kabelləri kimi fiziki medianı, eləcə də fəzada

elektromaqnit, radio və yaxudda işıq dalğalarının yayılması nəticəsində verilənlərin ötürülməsi hadisəsini misal göstərmək olar. Latın dilindən tərcümədə “kommunikato” informasiya mübadiləsinin sosial prosesi kimi qəbul edilir. Telekommunikasiya sözü isə 2 sözün (“tele” – uzaq, “kommunikato” – “əlaqə”) birləşməsindən əmələ gəlib uzaq məsafədə yerləşən obyektləri bir-biri ilə informasiya cəhətdən əlaqələndirmək üçün istifadə olunan termin kimi tərif edilir. Telekommunikasiya həmçinin adi kommunikasiya texnologiyalarından özündə bir çox texnologiyanı cəmlədiyinə görə də fərqlənir.

Qədim dövrlərdə, orta əsrlərdə və yaxın keçmişə qədərki zaman ərzində uzaq məsafədən məlumatların qarşı tərəfə çatdırılması üçün işıq mayakları, tonqal işıqları, tüstü siqnalları, bayraqların nümayişi, semafor teleqraf və sairə kimi cürbəcür sadə üsul və vasitələrdən istifadə olunduğu tarixdən bizə məlumdur. XX və XXI əsrlərdə isə artıq insan cəmiyyəti teleqraf, faks, telefon, genişmiqyaslı regional və qlobal kompüter şəbəkələri, mikrodalğalı ötürmə vasitələri, elektromaqnit ötürücülər, optic ötürücülər və peyk rabitə texnologiyaları kimi yüksək səviyyəli və ixtisaslı çox uzaq məsafələrdən məlumat mübadiləsi texnologiyalardan inkişaf həddinə çatdı.

Bu gün telekommunikasiya texnologiyaları arasında simsiz texnologiyalar daha çox üstünlük təşkil edir və gündən-günə də öz tətbiqini və aktuallığını artırmaqdadır. Simsiz rabitənin inkişaf tarixinə nəzər salsaq görərik ki, bu sahədə əsas inqilabi hadisələr XX əsrin ilk ongünlüyünə təsadüf edir. 1909-cu ildə fizika üzrə Nobel mükafatını qazanan Guglielmo Marconi və bu sahənin digər ixtiraçıları radio rabitənin sürətlə inkişafının təməlini qoymuş oldular. Həmin ixtiraçılar arasında teleqrafın ixtiraçıları - Charles Wheatstone və Samuel Morse, telefonun ixtiraçısı - Alexander Graham Bell, radio ixtiraçıları - Edwin Armstrong və Lee de Forest, həmçinin televiziyanın bəzi ixtiraçıları - Vladimir K. Zworykin, John Logie Baird və Philo Farnsworth kimi neçə-neçə öz dövrünün və sahəsinin ən görkəmli nümayəndələrinin adını çəkmək olar.

1.2 Telekommunikasiya vasitələrinin inkişaf tarixi

Uzaq məsafədən informasiya ötürmək üçün tarix boyu ən uzun müddət istifadə olunan vasitələrdən biri xüsusi təlimlərlə öyrədilmiş ev göyərçinləri olmuşdur. İlk dəfə farslar tərəfindən kəşf olunan bu üsulun sonralar Romalılar və digər xalqlar tərəfindən də geniş tətbiqi olunduğu tarixi mənbələrdən məlumdur. Məsələn: eramızın birinci əsrində yaşamış Roma tarixçisi öz əsərlərində Juli Sezarın Gaul adlı şəhərin fəthində göyərçinlərdən elçi kimi bəhrələndiyini qeyd etmişdir. Bundan başqa yunanların olimpiada oyunlarının keçirilməsini, uğur qazanan idmançıların adlarını və nəticələrini ölkə əhalisinə çatdırmaq məqsədilə istifadəsi də bu qədim telekommunikasiya vasitəsinin bir nümunəsi ola bilər.

1792-ci ildə Fransız mühəndisi Klod Chappe Lill və Paris şəhərləri arasında ilk sabit vizual teleqraf sistemini qurdu. Bu semafor teleqraf sistemi cəmiyyətin uzaq məsafəli rabitə sisteminə olan ehtiyaclarının bir çox hissəsini qarşılaya bildi. Amma əsas nüans onda idi ki, həmin semaforların ən çoxu 10-30 kilometr məsafədən bir yüksək ixtisaslı operatorlara və çox bahalı teleqüllələrə ehtiyacı vardı. Nə qədər çətin system olsa da, bu üsul təxminən bir əsr ayaqüstə qala bildi. Ancaq XIX əsrin sonlarında elektrik teleqraflarının informasiya ötürülməsində hökmranlığı tədricən öz əlinə alması nəticəsində 1880-ci ildən etibarən semafor teleqraf sistemlərindən imtina edilməyə başlanıldı.

1837-ci il iyulun 25-də ilk kommersiya elektrik teleqrafı ingilis ixtiraçısı Sir William Fothergill Cooke və ingilis alimi Sir Charles Wheatstone tərəfindən ictimaiyyətə təqdim olundu. Onları birləşdirən əsas cəhət o idi ki, hər ikisi öz cihazlarına yeni bir cihaz kimi deyil, mövcud olan "elektromaqnit teleqrafının inkişafı" kimi baxdılar.

Elə həmin il Samuel Morse sentyabrın 2-də özünün müstəqil olaraq nümayiş etdirdiyi elektrik teleqrafının yeni versiyasını daha da təkmilləşdirdi. Onun bu sahədə

təklif etdiyi kodu “Wheatstone” adlanan siqnalizasiya metodunun inkişafında vacib bir irəliləyiş oldu.

Sonra 1876-cı ildə Aleksander Bell tərəfinfən telefonun ixtirası patentləşdirilmiş oldu. Ancaq hələ bu hadisəyə qədər təxminən otuz il əvvəl Antonio Meucci 1849-cu ildə bir xətt üzərində səsin elektrik siqnalları vasitəsilə ötürülməsinə imkan verən bir cihaz icad etdi. Amma bu cihazın çox zəhmət tələb edən istifadəsi vardı. Belə ki, cihazın iş prinsipi elektrofon effektinə əsaslanırdı və bu səbəbdən də, bu cihazdan istifadə edən şəxslərdən tələb olunurdu ki, qəbul edici tərəfin səsi eşidə bilməsi ötürücü tərəf qəbuledici qurğunu mütləq ağızına sıxmalı idi. Bu isə əlbəttə ki, çox böyük narahatlıq yaradırdı. Ona görə də əhəmiyyəti az oldu və istifadə müddəti də çox uzun çəkmədi. Bu problem aradan qaldırmağı bacaran ilk telefon kommersiya xidmətləri Bell Telefon Şirkəti tərəfindən 1878-1879-cu illərdə Atlantikanın hər iki tərəfində Nyu-Haven və London şəhərlərindən quruldu.

1894-cü ildən başlayaraq, italyan ixtiraçısı Guglielmo Marconi, 1901-ci ilə qədər Atlantik okeanı üzərindən ötürülə biləcəyini iddia etdi və yeni radio dalğalar fenomenindən istifadə edərək simsiz rabitəni inkişaf etdirməyə başladı. Bu radio tezliklə işləyən simsiz teleqrafın başlanğıcı idi. Tezliklə 1900 və 1906-cı illərdə simsiz teleqraf üzərindən səs və musiqinin ötürülməsi də nümayiş olundu, lakin ilkin addımlar o qədər də müvəffəqiyyətli alınmadı.

Millimetr dalğalı rabitə ilk dəfə 1894-1896-cı illərdə benqalalı fizik Jagadish Chandra Bose tərəfindən araşdırıldı və o həyata keçirdiyi təcrübələrindən sonra 60 GHs-dən çox daha yüksək tezliklə işləyən texnologiyanın əsasını qoymağa nail oldu. O, həmçinin 1901-ci ildə radio kristal detektorunu patentləşdirdikdən sonra radio dalğaları daha rahatlıqla aşkar etmək üçün yarımkeçirici qovşaqların istifadəsini təqdim etdi.

Birinci dünya müharibəsi baş verdiyi zaman hərbi rabitənin çox böyük önəm daşıması radio dalğalar vasitəsilə rabitənin təmin edilməsi sahəsində sürətli inkişaf

üçün əlavə bir səbəb oldu. Müharibədən sonra 1920-ci illərdə kommersiya radio AM yayımı başladı və əyləncə, xəbər kimi radio verilişləri tezliklə öz ətrafına böyük bir kütləni toplamağı bacardı. Müharibədən sonra 1920-ci illərdə kommersiya radio AM yayımı başladı və əyləncə və xəbərlər üçün vacib bir kütləvi mühitə çevrildi. Radio stereo FM yayımının inkişafı 1930-cu illərdə ABŞ-da baş vermiş və 1960-cı illərdə və 70-ci illərə qədər Birləşmiş Krallıqda əsas kommersiya standartı olaraq yerdəyişmişdir.

25 Mart 1925-ci ildə John Logie Baird London Selfridges mağazasında şəkillərin hərəkət etdirilməsi ilə hadisənin təsvir edilməsini nümayiş etdirməyi bacardı. Bu ilk mexaniki televiziyanın əsası demək idi. Daha sonra İngilis Yayım Korporasiyası 30 sentyabr 1929-cu ildən başlayaraq təcrübi verilişlərin əsasını qoydu. İkinci Dünya Müharibəsi zamanı televiziya sahəsindəki çalışmalara nisbətən ara verilsə də, müharibədən sonra televiziyanın inkişafı uğurla davam etdirildi.

1.3 Tarixi telekommunikasiya vasitələrinin əsas baza elementləri və iş prinsipləri

Termion boru və ya termion qapaq kimi tanınan cihaz növü, qızdırılan katoddan elektronların termion emissiya fenomenindən istifadə edir və siqnal gücləndirmə və cərəyan rektifikasiyası kimi bir sıra fundamental elektron funksiyalar üçün istifadə olunur. Bir vakuum fotube kimi qeyri-termion tiplər, fotoelektrik effekt sayəsində elektron yayılmasına nail olur və işıq səviyyəsinin aşkarlanması kimi istifadə olunur. Hər iki növdə, elektronlar katoddan anoda boruda olan elektrik sahəsi ilə sürətlənir.

Ən sadə vakuum borusu, 1904-cü ildə John Ambrose Fleming tərəfindən icad edilən diod, yalnız qızdırılan elektron yayan katod və anod ehtiva edirdi. Elektronlar yalnız cihazdan - katoddan anodadək bir istiqamətə axa bilər. Borunun içərisinə bir və ya daha çox nəzarət ızgarasının əlavə edilməsi katod və anod arasındakı cərəyanın şəbəkə və ya ızgaralardakı gərginliklə idarə olunmasına imkan verir. Bu qurğular XX əsrin birinci yarısı üçün elektron sxemlərin əsas komponenti oldu. Bunlar radio, televiziya, radar, səs yazısı və bərpası, şəhərlərarası telefon şəbəkələri və analoq və erkən rəqəmsal kompüterlərin inkişafı üçün çox vacib idi. Bəzi tətbiqlər əvvəllər

hesablama üçün radio və ya mexaniki kompüterlər üçün qığılcım boşluğu ötürücüsü kimi texnologiyalardan istifadə etsə də, bu texnologiyaları geniş yayan və praktik edən və elektronikanın intizamını yaradan termion vakuum borusunun ixtirası idi.

1940-cı illərdə yarımkeçirici cihazların ixtirası daha kiçik, daha səmərəli, etibarlı və davamlı və termion borulara nisbətən daha ucuz olan bərk cisimlərin istehsalına imkan yaratdı. 1960-cı illərin ortalarından etibarən termion borular daha sonra tranzistorla əvəz olunmağa başladı. Termion borular hələ də müəyyən yüksək tezlikli gücləndiricilər üçün bəzi tətbiqlərə malikdir.

1950-ci ildən başlayaraq müasir telekommunikasiya tarixinə telekommunikasiya texnologiyasında yarımkeçirici cihazların geniş tətbiqi səbəbindən həmin period tarixdə "Yarımkeçirici dövr" adı ilə tanınır. Transistor texnologiyasının və yarımkeçirici sənayenin inkişafı telekommunikasiya texnologiyasında əhəmiyyətli irəliləyişlərə imkan verdi və dövlətə məxsus genişzolaqlı dövrəli şəbəkələrdən xüsusi genişzolaqlı paketli şəbəkələrə keçməyə səbəb oldu. Genişmiqyaslı inteqrasiya (LSI) və RF CMOS (radiotezlik tamamlayıcı MOS) kimi metal oksid-yarımkeçirici (MOS) texnologiyaları, məlumat nəzəriyyəsi ilə (məlumatların sıxılması kimi) analoqdan rəqəmsal siqnalın işlənməsinə keçməsinə səbəb oldu. , rəqəmsal telekommunikasiya (rəqəmsal telefon və rəqəmsal media kimi) və simsiz rabitə (mobil şəbəkələr və mobil telefon kimi) tətbiqi ilə telekomunikasiya sənayesinin 20-ci əsrin sonlarına doğru sürətli böyüməsinə səbəb oldu.

Transistor texnologiyasının inkişafı müasir elektron telekommunikasiya üçün əsas olmuşdur. İlk tranzistor, nöqtəli əlaqə tranzistoru 1947-ci ildə Bell Labs-da John Bardeen və Walter Houser Brattain tərəfindən icad edilmişdir. MOS tranzistoru kimi də tanınan MOSFET (metal oksid-silikon sahə effektli tranzistor) sonradan 1959-cu ildə Bell Laboratoriyalarında Məhəmməd M. Atalla və Dawon Kahng tərəfindən icad edilmişdir. MOSFET ən çox istehsal olunan cihaz kimi də tarixə düşümüşdür. MOS texnologiyası, o cümlədən MOS inteqral sxemləri və güc MOSFETləri müasir

telekommunikasiya rabitəsinin infrastrukturunu idarə edir. Kompüterlərlə yanaşı, MOSFET-lərdən qurulan müasir telekommunikasiya digər vacib elementlərinə mobil qurğular, ötürücülər, baza stansiya modulları, marşrutlaşdırıcılar, RF gücləndiriciləri, mikroprosessorlar, yaddaş çipləri və telekommunikasiya sxemləri daxildir.

Edholm qanununa görə, telekomunikasiya şəbəkələrinin bant genişliyi hər 18 ayda bir iki dəfə artır. MOS texnologiyasındakı irəliləyişlər, o cümlədən MOSFET miqyaslılığı (Moore qanununa görə proqnozlaşdırıldığı kimi, ekspansensial tempdə tranzistor sayının artması) telekommunikasiya şəbəkələrində geniş yayılma qabiliyyətini artıran mühüm amil olmuşdur.

1.4 Telekommunikasiyanın inkişafında kompüter şəbəkələri və internet dünyasına keçid

1 sentyabr 1940-cı ildə Corc Stibitz Nyu-Yorkda bir Teletipdən istifadə edərək özünün hazırladığı Kompleks Ədədlər Kalkulyatoru üçün lazım olan giriş verilənlərini ötürdü və hesablanmış nəticələri New Hampshire-dəki Dartmouth Kollecində çıxış dəyərləri olaraq geri aldı. Uzaq "lal" terminalları olan mərkəzləşdirilmiş bir kompüterin (mainframe) bu konfiqurasiyası 1970-ci illərdə məşhur olmuşdur. Lakin, artıq 1960-cı illərdə tədqiqatçılar paket kommutasiyasını, mərkəzləşdirilmiş bir əsas çərçivədən keçmədən asinxron olaraq təyinat yerinə mesaj göndərən texnologiyanı araşdırmağa başladılar. 5 dekabr 1969-cu ildə ARPANET-in başlanğıcını təşkil edən dörd qovşaqlı bir şəbəkə meydana gəldi, 1981-ci ilə qədər bu qovşaqların sayı 213-ə çatdı. ARPANET nəticədə İnterneti yaratmaq üçün digər şəbəkələrlə birləşdi. Bununla da böyük bir insan cəmiyyətinin istənilən iki və daha çox nöqtəsi arasında kommunikasiya yarada bilməsi imkanlarının təməli qoyuldu.

1.5 Lokal şəbəkələr və qlobal şəbəkələr

İnternetin böyüməsinə baxmayaraq, yerli şəbəkələrin (LAN) - bir neçə kilometrə qədər uzanmayan kompüter şəbəkələrinin xüsusiyyətləri fərqlidir. Bunun səbəbi, bu miqyasda olan şəbəkələr daha böyük şəbəkələrlə əlaqəli bütün xüsusiyyətləri tələb

etmir və onlar olmadan daha az xərcli və səmərəlidir. İnternetlə əlaqəli olmadıqda, məxfilik və təhlükəsizlik üstünlüklərinə də malikdirlər. Lakin məqsədyönlü şəkildə İnternetə birbaşa qoşulmanın olmaması, heç də xakerlərdən, hərbi qüvvələrdən və ya iqtisadi güclərdən etibarlı müdafiəni təmin etmiş olmur. Bu təhdidlər yalnız LAN-a uzaqdan qoşulma üsulları olduqda mövcuddur.

Geniş sahə şəbəkələri (WAN) minlərlə kilometrə qədər uzana biləcək özəl kompüter şəbəkələridir. Bir daha, onların üstünlüklərindən bəzilərinə məxfilik və təhlükəsizlik daxildir. Şəxsi LAN və WAN-ların əsas istifadəçilərinə məlumatlarını etibarlı və gizli saxlamalı olan silahlı qüvvələr və kəşfiyyat qurumları daxildir.

1980-ci illərin ortalarında, məlumat bağlantısı təbəqəsi və OSI istinad modelinin tətbiqi təbəqəsi arasındakı boşluqları doldurmaq üçün bir neçə rabitə protokolu dəsti ortaya çıxdı. Bunlara, MS-DOS istifadəçiləri arasında populyarlığına görə, 1990-cı illərin əvvəllərində qurulmuş dominant protokolu olan Appletalk, IPX və NetBIOS daxildir. TCP / IP bu nöqtədə mövcud idi, lakin adətən yalnız böyük hökumət və tədqiqat müəssisələri tərəfindən istifadə olunurdu.

İnternet populyarlaşdıqca və trafikin özəl şəbəkələrə yönəldilməsi tələb olunduğu üçün TCP / IP protokolları mövcud yerli şəbəkə texnologiyalarını əvəz etdi. Əlavə texnologiyalar, məsələn DHCP, TCP/IP əsaslı kompüterlərin şəbəkədə özünü tənzimləməsinə imkan verdi. Bu cür funksiyalar AppleTalk / IPX / NetBIOS protokol dəstlərində də mövcud idi.

Asinxron ötürmə rejimi (ATM) və ya Multiprotokol Etiket Kommutasiyası (MPLS) WAN kimi böyük şəbəkələr üçün tipik məlumat bağlantısı protokollarıdır; Ethernet və Token Ring şəbəkələr üçün tipik məlumat bağlantı protokollardır. Bu protokollar əvvəlki protokollardan daha sadə, məsələn, xidmət zəmanəti keyfiyyəti kimi xüsusiyyətləri buraxır və toqquşmanın qarşısını alır. Bu fərqlərin hər ikisi daha mükəmməl iqtisadi sistemlərə imkan verir.

1980-ci və 1990-cı illərdə IBM Token Ring-in populyarlığına baxmayaraq, demək olar ki, bütün LANlar simli və ya simsiz Ethernet qurğularından istifadə edir. Fiziki təbəqədə, əksər simli Ethernet tətbiqlərində mis bükülmüş cüt kabellərdən istifadə olunur (ümumi 10BASE-T şəbəkələri daxil olmaqla). Bununla birlikdə, bəzi erkən tətbiqlərdə daha ağır koaksial kabellərdən istifadə edilmiş və son tətbiqlərdə (xüsusilə yüksək sürətli olanlar) optik liflərdən istifadə edilmişdir. Optik liflər istifadə edildikdə, multimode liflər və tək rejimli liflər arasında fərq qoyulmalıdır. Multimode lifləri cihazları istehsal etmək daha ucuz olan daha qalın optik liflər kimi düşünmək olar, lakin daha az istifadə olunan bant genişliyi və daha pis aşınma - daha zəif məsafəli performansdan xəbər verir.

1. 6 Analoq siqnallardan rəqəmsal siqnallara keçid

Rabitə siqnalları ya analoq siqnallar, ya da rəqəmsal siqnallarla göndərilə bilər. Bu baxımdan analoq rabitə sistemləri və rəqəmsal rabitə sistemləri olmaqla iki tip rabitə sistemləri var. Analoq siqnal üçün siqnal məlumatla əlaqədar olaraq davamlı olaraq dəyişir. Rəqəmsal siqnallar vasitəsi ilə ötürmə zamanı məlumatlar diskret dəyərlər toplusu olaraq kodlanır (birlərlə və ya sıfırlarla). Siqnalların daxil olması və qəbul zamanı analoq siqnallarda olan məlumatlar yüksək səviyyədə fiziki səs-küylə müşayiət olunur. Ümumiyyətlə, bir rabitə sistemindəki səs-küy, istənilən analoq siqnalın daxil olması və ya xaric olması zamanı tamamilə təsadüfi bir şəkildə müşahidə oluna bilər. Digər tərəfdən analoq siqnallar vasitəsilə informasiyanın ötürülməsi və nümayişi zamanı istifadəçi üçün əlavə problemlər və çətinliklər yaratması da onun əsas əskik əlamətləri hesab olunur.

Digər tərəfdən, əlavə səs-küy pozğunluğu müəyyən bir həddi keçməzsə, rəqəmsal siqnallarda olan məlumatlar təsirsiz qalacaqdır. Onların səs-küyə qarşı müqaviməti rəqəmsal siqnalların analoq siqnallara nisbətən əsas üstünlüyüdür.

Rəqəmsal sistemlərin analoqdan daha bir üstünlüyü, onların çıxışının yaddaşda saxlanması daha asandır, yəni iki gərginlikli vəziyyət (yüksək və aşağı) davamlı bir sıra vəziyyətdən daha asan saxlanılır.

1.7 Simsiz Telekommunikasiya

İnsan cəmiyyətinin telekommunikasiyanın inkişafına sürətlə artan tələbatı qarşısında kabelli kompüter şəbəkələri də davam gətirə bilmədi. Tezliklə kommunikasiyanın növbəti səviyyəsi – simsiz rabitədən istifadə etməklə uzaq məsafələr arasında əlaqə yaratmaq erası başladı. Doğrudur, kabelli, naqilli kompüter şəbəkələri hazırda da istifadə olunmaqdadır. Ancaq simsiz rabitənin ortaya qoyduğu sürət, rahatlıq, keyfiyyət və bir çox amillər baxımından tədricən öz aktuallıqlarını itirməkdə və yalnız local şəbəkələr üçün daha faydalı olmaqdadırlar.

Simsiz inqilab 1990-cı illərdə sosial inqilaba aparan rəqəmsal simsiz şəbəkələrin meydana gəlməsi və simsiz texnologiyalardan paradiqma dəyişməsi, kommersiya simsiz texnologiyaların yayılması da daxil olmaqla başladı. Məsələn: mobil telefonlar və mobil telefoniya, peyjerlər, simsiz kompüter şəbəkələri, mobil şəbəkələr, simsiz İnternet, simsiz bağlantıları olan noutbuk və əl kompüterləri simsiz telekommunikasiyanın ilk və ən geniş yayılmış nümunələridir. Simsiz şəbəkələrin qurulmasındakı inqilab radiotezlik (RF) və mikrodalğalı mühəndislikdəki inkişaflar, eləcə də analoqdan rəqəmsal RF texnologiyasına keçid ilə daha sürətli formada davam etdirilməkdədir. Rəqəmsal simsiz şəbəkələri təmin edən RF texnologiyasının əsas komponenti olan yuxarıda da bəhs etdiyimiz metal oksid-yarımkeçirici sahə effekti tranzistoru (MOSFET və ya MOS tranzistor) texnologiyasındakı avanslar da bu inqilabın mərkəzi nöqtələrindən biri olmuşdur.

1.8 Rəqəmsal media

Praktik rəqəmsal medianın paylanması və axınına artan cəmiyyətin həddən artıq ehtiyacını sıxılmayan medianın yüksək yaddaşı, saxlama və bant genişliyi kimi təklif etdiyi əlavə üstünlüklər sayəsində təmin etmək mümkün oldu. Ən vacib sıxılma

texnikası 1972-ci ildə ilk dəfə görüntü sıxılma texnikası olaraq təklif olunan diskret kosin çevrilməsidir. DCT – demək olar ki, tamamilə itkisiz bir sıxılma alqoritmi.

1.9 Müasir media

Sürətlə artmaqda olan dünya əhalisini bir-biri ilə əlaqələndirməkdə olan müasir media kifayət qədər çeşidə malik olsa da, biz onları daha çox kütləni özündə cəmləyən dörd əsas qrup üzərindən təhlil edəcəyik. Bunlar telefon, radio və televiziya, internet, həmçinin local və qlobal şəbəkələrdir.

1.10 Telefon

Bir telefon şəbəkəsində, zəng edən şəxs müxtəlif telefon stansiyalarındakı açarlar vasitəsilə danışmaq istədikləri şəxsə qoşulur. Həmin açarlar iki istifadəçi arasında bir elektrik bağlantısı meydana gətirir və zəng edən şəxs nömrəni yığdıqda bu açarların tənzimlənməsi elektron olaraq təyin olunur. Bağlantı qurulduqdan sonra zəng edənin səsi zəng edən şəxsin əlindəki kiçik bir mikrofondan istifadə edərək elektrik siqnalına çevrilir. Bu elektrik siqnalı daha sonra şəbəkə vasitəsi ilə istifadəçinin yanına göndərilir və burada o adamın əlindəki kiçik bir dinamik tərəfindən yenidən səsə çevrilir.

2015-ci ildən etibarən əksər yaşayış evlərində şəhər telefonları analoq sistemə əsaslanmaqla qoşulmuşdu, yəni dinamikin səsi siqnalın gərginliyini birbaşa müəyyənləşdirir. Qısa məsafəli zənglər son siqnallardan analoq siqnal kimi idarə olunsa da, getdikcə telefon xidməti təminatçıları siqnalları şəffaf şəkildə ötürmə üçün rəqəmsal siqnallarla əvəz olunmağa başladı. Bunun üstünlüyü ondan ibarətdir ki, rəqəmsal səsli məlumatlar İnternetdən gələn məlumatlarla yan-yana gəzə bilər və uzun məsafəli rabitə şəraitində mükəmməl şəkildə yayıla bilər (səs-küyün təsir etdiyi analoq siqnallardan fərqli olaraq).

Cib telefonları telefon şəbəkələrinə əhəmiyyətli dərəcədə təsir göstərmişdir. Cib telefonu abunəçiləri hazırda bir çox bazarda sabit xətt abunəçilərindən çoxdur. 2005-ci ildə cib telefonlarının satışları 816,6 milyon təşkil etdi və bu rəqəm Asiya / Sakit okean (204 m), Qərbi Avropa (164 m), CEMEA (Mərkəzi Avropa, Orta Şərq və Afrika) (153.5

m) bazarlarında demək olar ki, eyni dərəcədə paylandı. , Şimali Amerika (148 m) və Latın Amerikası (102 m). 1999-cu ildən bəri beş il ərzində yeni abunə baxımından Afrika 58.2% böyümə ilə digər bazarları qabaqladı. Getdikcə bu telefonlar səs məzmununun GSM və ya W-CDMA kimi rəqəmsal şəkildə ötürüldüyü sistemlər tərəfindən xidmət olunur, bir çox bazarlarda AMPS kimi analoq sistemləri ləğv etməyi seçir.

Pərdə arxasında telefon rabitəsində də kəskin dəyişikliklər oldu. TAT-8-in 1988-ci ildə işə başlamasından sonra 1990-cı illərdə optik liflərə əsaslanan sistemlərin geniş yayılması müşahidə edildi. Optik liflərlə əlaqə qurmağın faydası, məlumat ötürmə qabiliyyətinin kəskin şəkildə artmasıdır. TAT-8 özü o dövrdə qoyulmuş son mis kabeldən 10 dəfə çox telefon danışıqlarını həyata keçirə bildi və bugünkü optik lif kabelləri TAT-8-dən 25 dəfə çox telefon danışıqlarını həyata keçirə bilir. Məlumat ötürmə qabiliyyətinin bu artması bir neçə amilə bağlıdır: Birincisi, optik liflər fiziki cəhətdən rəqabət aparan texnologiyalardan daha kiçikdir. İkincisi, onlar crosstalkdan əziyyət çəkmirlər, yəni bir neçə yüzü asanlıqla bir kabeldə birləşdirilə bilər. Nəhayət, multiplekslәşmənin yaxşılaşdırılması tək bir lifin məlumat tutumunun eksponensial böyüməsinə səbəb oldu.

Bir çox müasir optik lif şəbəkələri arasında ünsiyyətə kömək Asinxron ötürmə rejimi (ATM) kimi tanınan bir protokoldur. ATM protokolu ikinci bənddə göstərilən məlumatların yan-yana ötürülməsinə imkan verir. Bu ümumi telefon şəbəkələri üçün uyğundur, çünki şəbəkə vasitəsilə məlumat üçün bir yol yaradır və trafik müqaviləsini bu yola bağlayır. Trafik müqaviləsi, əslində müştəri ilə şəbəkə arasında şəbəkənin məlumatları necə idarə edəcəyi ilə bağlı bir razılaşmadır; şəbəkə trafik müqaviləsinin şərtlərinə cavab verə bilmirsə, əlaqəni qəbul etmir. Bu vacibdir, çünki telefon danışıqları bir müqavilə ilə danışıqlar apara bilər ki, bu da özlərinə sabit bir sürət təmin etsin, zəng edən şəxsin səsi hissələrin gecikməməsini və ya tamamilə kəsilməsini təmin edəcək vacib bir amildir. Bənzər bir işi yerinə yetirən və gələcəkdə ATM-i tamamilə

sıradan çıxartması ehtimal olunan Multiprotocol Label Switching (MPLS) kimi ATM-yə rəqiblər də var.

1.11 Radio və televiziya

Bir yayım sistemində mərkəzi yüksək güclü yayım qülləsi yüksək tezlikli elektromaqnit dalğasını çoxsaylı aşağı güclü alıcılara ötürür. Qüllə tərəfindən göndərilən yüksək tezlikli dalğa vizual və ya audio məlumatları ehtiva edən bir siqnal ilə modulyasiya edilmişdir. Bundan sonra qəbuledici yüksək tezlikli dalğanı almaq üçün tənzimlənir və vizual və ya audio məlumatları daxil edən siqnal almaq üçün bir demodulyator istifadə olunur. Yayım siqnalı ya analoq ola bilər (siqnal məlumatla bağlı davamlı olaraq dəyişir) və ya rəqəmsal (məlumat diskret dəyərlər toplusu olaraq kodlanır).

Yayım mediası sənayesi inkişafında kritik bir dönüş nöqtəsindədir, bir çox ölkə analoqdan rəqəmsal yayıma keçdi. Bu hərəkət daha ucuz, daha sürətli və daha bacarıqlı inteqral sxemlərin istehsalı ilə mümkündür. Rəqəmsal yayımların əsas üstünlüyü ondadır ki, ənənəvi analoq yayımları ilə əlaqəli bir sıra şikayətlərin qarşısını alırlar. Televiziya üçün qarlı şəkillər, xəyal qırıqlığı və digər təhrif kimi problemlərin aradan qaldırılması daxildir. Bunlar analoq ötürülmənin təbiəti səbəbindən baş verir, yəni səs-küy səbəbindən baş verən narahatlıqlar son çıxışda aydın olacaq. Rəqəmsal ötürmə bu problemi aradan qaldırır, çünki rəqəmsal siqnallar qəbul zamanı diskret dəyərlərə endirilir və buna görə kiçik pozuntular son nəticəyə təsir etmir. Sadələşdirilmiş bir misalda, 1011 ikili mesaj siqnal amplitüdləri ilə ötürülərsə və siqnal amplitüdləri ilə qəbul edilirdisə [0.9 0.2 1.1 0.9], yenə də ikili mesaj 1011 - göndərilənlərin mükəmməl bir bərpası ilə həll ediləcəkdir. Bu nümunədən rəqəmsal ötürülmə ilə əlaqədar bir problem də görünə bilər ki, səs-küy kifayət qədər böyükdürsə, şifrəli mesajı əhəmiyyətli dərəcədə dəyişdirə bilər. İrəli səhvlərin düzəldilməsindən istifadə edərək, bir mesaj alıcı bir az səhv səhvini düzəldə bilər, lakin çox səs-küy anlaşılmaz çıxışa və deməli ötürülmənin pozulmasına səbəb olacaqdır.

Rəqəmsal televiziya yayımında, dünyada qəbul edilə biləcəyi üç rəqabətli standart var. Bunlar ATSC, DVB və ISDB standartlarıdır; indiyə qədər bu standartların qəbulu başlıq xəritəsində təqdim edilmişdir. Hər üç standartda video sıxılma üçün MPEG-2 istifadə olunur. ATSC Dolby Digital AC-3-ni səs sıxması üçün istifadə edir, ISDB qabaqcıl səs kodlaşdırmasından istifadə edir (MPEG-2 Hissə 7) və DVB-də səs sıxması üçün standart yoxdur, lakin ümumiyyətlə MPEG-1 Part 3 Layer 2 istifadə edir. Modulyasiya seçimi də sxemlər arasında dəyişir. Rəqəmsal səs yayımında standartlar Rəqəmsal Səs Yayım standartını (həmçinin Eureka 147 standartı kimi tanınır) qəbul etməyi seçən ölkələr ilə daha çox birləşdirilir. İstisna, HD Radio qəbul etməyi seçən ABŞ-dır. HD Radio, Eureka 147-dən fərqli olaraq, rəqəmsal məlumatların normal AM və ya FM analoq ötürmələrində "pərçimləmə" imkanı verən kanaldaxili kanal ötürülməsi kimi tanınan bir ötürmə metoduna əsaslanır.

Bununla birlikdə, rəqəmsal sistemə keçidin gözlənilməsinə baxmayaraq, əksər ölkələrdə analoq televiziya ötürülməkdə qalır. İstisna, keçid müddətini iki dəfə gecikdirdikdən sonra, 12 iyun 2009-cu ildə analoq televiziya ötürülməsini (çox az gücə malik televiziya stansiyaları istisna olmaqla) bitirmiş Amerika Birləşmiş Ştatlarıdır. Keniya da çoxsaylı gecikmələrdən sonra 2014-cü ilin dekabrında analoq televiziya yayımını dayandırdı. Analoq televiziya üçün rəngli televiziya yayımı üçün üç standart mövcud idi (burada övladlığa götürmə xəritəsinə baxın). Bunlar PAL (Alman dizaynlı), NTSC (Amerika dizaynlı) və SECAM (Fransız dizaynlı) kimi tanınır. Analoq radio üçün rəqəmsal radioya keçid rəqəmsal qəbuledicilərin baha olması ilə çətinləşir. Analoq radio üçün modulyasiya seçimi adətən amplitüd (AM) və ya tezlik modulyasiyası (FM) arasındadır. Stereo səsləndirməyə nail olmaq üçün stereo FM üçün bir amplituda modulyasiya edilmiş subcarrier istifadə olunur və stereo AM və ya C-QUAM üçün kvadrat kvadrat amplituda modulyasiyasından istifadə olunur.

1.12 İnternet

İnternet, İnternet Protokolundan (IP) istifadə edərək bir-biri ilə əlaqə quran dünya miqyasında kompüterlər və kompüter şəbəkələri şəbəkəsidir. İnternetdəki hər hansı bir kompüter, məlumatları ona yönəltmək üçün digər kompüterlər tərəfindən istifadə edilə bilən unikal bir IP ünvanına malikdir. Beləliklə, İnternetdəki hər hansı bir kompüter öz IP ünvanından istifadə edərək hər hansı digər kompüterə mesaj göndərə bilər. Bu mesajlar, ikitərəfli əlaqə yaratmağa imkan verən kompüterin IP ünvanını özləri ilə aparır. Beləliklə İnternet kompüterlər arasında mesaj mübadiləsidir.

2000-ci ildə ikitərəfli telekommunikasiya şəbəkələri vasitəsilə axan məlumatların 51% -nin İnternetdən (qalan hissəsinin (42%) sabit telefondan) axdığı təxmin edilir. 2007-ci ilə qədər internet açıq şəkildə üstünlük təşkil etdi və telekommunikasiya şəbəkələrindəki bütün məlumatların 97% -ni (qalan hissəsi (2%) mobil telefonlar vasitəsilə) tutdu. 2008-ci ildəki məlumata görə, dünya əhalisinin təxminən 21.9% -i Şimali Amerikada (73.6%), Okeaniya / Avstraliya (59.5%) və Avropada (48.1) ən yüksək giriş nisbəti ilə (əhalinin faizi ilə ölçülür) İnternetə çıxışı var. %). Genişzolaqlı çıxış baxımından dünyada İslandiya (26.7%), Cənubi Koreya (25.4%) və Hollandiya (25.3%) liderlik etdilər.

Kompüterlər və marşrutlaşdırıcıların bir-birləri ilə necə əlaqə qurmalarını tənzimləyən protokollar səbəbindən İnternet qismən işləyir. Kompüter şəbəkəsi ünsiyyətinin təbiəti, protokol yığımındakı fərdi protokollar digər protokollardan daha az və ya az müstəqil işlədildiyi bir qatlı bir yanaşma ilə uzanır. Bu, daha yüksək səviyyəli protokolların işləmə tərzini dəyişdirmədən, aşağı səviyyəli protokolların şəbəkə vəziyyəti üçün özelleştirilməsinə imkan verir. Bunun nə üçün vacib olduğuna dair praktik bir nümunədir, çünki işlədiyi kompüterin Ethernet və ya Wi-Fi bağlantısı vasitəsilə İnternetə qoşulub-qoşulmadığından asılı olmayaraq İnternet brauzerinə eyni kodu işlətməyə imkan verir. Protokollar, ümumiyyətlə qəbul edilmiş şəbəkə protokolu

paketini qurmaq üçün uğursuz bir cəhddə 1983-cü ildə ortaya çıxan OSI istinad modelindəki yerləri baxımından çox danışılır.

nternet üçün, fiziki mühit və məlumat bağlantısı protokolu paketlərin dünyanı keçdiyi üçün bir neçə dəfə dəyişə bilər. Bunun səbəbi, İnternet hansı fiziki vasitə və ya məlumat bağlantısı protokolunun istifadə olunduğuna heç bir məhdudiyyət qoymur. Bu, yerli şəbəkə vəziyyətinə ən uyğun olan media və protokolların qəbuluna səbəb olur. Praktikada əksər qitələrarası rabitə optik lifin üstündəki Asynchronous Transfer Mode (ATM) protokolunu (və ya müasir bir ekvivalent) istifadə edəcəkdir. Bu, əksər qitələrarası rabitə üçün İnternetin ümumi kommutasiya telefon şəbəkəsi ilə eyni infrastrukturu paylaşdığına görədir.

Şəbəkə təbəqəsində, İnternet Protokolu (İP) məntiqi ünvana müraciət etmək üçün standart hala gəlir. World Wide Web üçün bu "IP adreslər" Domain Ad Sistemindən istifadə etməklə insanın oxunan formasından əldə edilmişdir (məs: 72.14.207.99 www.google.com saytından götürülmüşdür). Hazırda İnternet Protokolunun ən çox istifadə olunan versiyası dördüncü versiyadır, lakin altıncı versiyaya keçmək yaxınlaşır.

Nəqliyyat qatında ən çox rabitə ya Transmissiya Nəzarət Protokolunu (TCP) və ya İstifadəçi Datagram Protokolunu (UDP) qəbul edir. TCP, göndərilən hər bir mesajın digər kompüter tərəfindən qəbul edilməsi vacibdirsə, UDP sadəcə istədiyi zaman istifadə olunur. TCP ilə paketlər itirildikdə və daha yüksək qatlara təqdim edilmədən əvvəl qaydada yerləşdirildikdə geri göndərilir. UDP ilə paketlər itirilmədiyi təqdirdə sifariş verilmir və geri göndərilmir. Həm TCP, həm də UDP paketləri paketin hansı tətbiqi və ya emal edilməsini təyin etmək üçün onlarla port nömrələri daşıyır. Müəyyən tətbiq səviyyəli protokollar müəyyən limanlardan istifadə etdiyinə görə, şəbəkə rəhbərləri xüsusi tələblərə uyğun trafiklə manipulyasiya edə bilərlər. Nümunələr üçün misal göstərə bilərik ki, müəyyən bir liman üçün nəzərdə tutulmuş trafikin qarşısını almaqla İnternetə girişi məhdudlaşdırmaq və ya prioritet təyin etməklə müəyyən tətbiqlərin işinə təsir göstərməkdir.

Nəqliyyat qatının üstündə bəzən istifadə olunan və sessiya və təqdimat təbəqələrinə sərbəst uyğunlaşan müəyyən protokollar mövcuddur, ən əsası Təhlükəsiz Sockets Layer (SSL) və Nəqliyyat Layer Təhlükəsizlik (TLS) protokolları. Bu protokollar iki tərəf arasında ötürülən məlumatların tamamilə məxfi qalmasını təmin edir. Nəhayət, tətbiq qatında İnternet istifadəçilərinin HTTP (veb gəzən), POP3 (e-poçt), FTP (fayl ötürülməsi), IRC (İnternet sohbeti), BitTorrent (fayl paylaşma) XMPP (dərhal mesajlaşma) kimi protokollardan gələcəkdə daha çox faydalanacağı güman edilməkdədir.

Səs üzərindən İnternet Protokolu (VoIP) məlumat paketlərini sinxron səsli rabitə üçün istifadə etməyə imkan verir. Məlumat paketləri səs tipli paket kimi qeyd olunur və şəbəkə rəhbərləri tərəfindən prioritet sayıla bilər ki, real vaxt, sinxron söhbət digər məlumat trafiki növləri ilə mübahisəyə daha az məruz qala bilər (məsələn, fayl ötürülməsi və ya e-poçt) və ya buferləşdirilir əvvəlcədən (yəni audio və video) zərər vermədən. Şəbəkə eyni anda baş verən bütün VoIP zənglər üçün kifayət qədər tutuma sahib olduqda və şəbəkə prioritetləşdirmə üçün, yəni özəl bir korporativ stil şəbəkəsinə sahib olduqda bu prioritetləşdirmə yaxşıdır, lakin İnternet ümumiyyətlə bu şəkildə idarə olunmur və bu səbəblərdən da ola bilər ki, şəxsi şəbəkə və ictimai İnternet üzərindən VoIP zənglərinin keyfiyyətində hiss olunacaq səviyyədə böyük fərqlər əmələ gəlmiş olsun.

1.13 Telekommunikasiya sistemlərinin cəmiyyətə təsiri

Telekommunikasiya müasir cəmiyyətə əhəmiyyətli bir sosial, mədəni və iqtisadi təsir göstərir. Əhəmiyyətini anlamaq üçün sadəcə bunu qeyd etmək bəs edər ki, 2008-ci ildə hesablamalar telekommunikasiya sektorunun gəlirlərini 4.7 trilyon dollar olduğunu və bunun ümumi dünya məhsulunun (rəsmi məzənnə) 3 faizindən daha çox olmasını müəyyənləşdirdi. Aşağıdakı hissədə isə telekommunikasiyanın cəmiyyətimizə böyük miqdarda və əhəmiyyətli təsirlərini daha ətraflı şəkildə göstərilmişdir.

1.13.1 İqtisadi təsirlər. Mikroiqtisadiyyat səviyyəsində

Mikroiqtisadi miqyasda şirkətlər qlobal biznes imperiyalarının qurulmasına kömək etmək üçün telekommunikasiya vasitələrindən istifadə etdilər. Bu amil Amazon.com onlayn pərakəndə satıcısının işində özünü açıq-aşkar şəkildə göstərir. Amma bununla belə akademik Edvard Lenertə görə, hətta şərti pərakəndə satıcı Walmart, rəqibləri ilə müqayisədə daha yaxşı telekommunikasiya infrastrukturundan faydalanmışdır. Dünyadakı şəhərlərdə ev sahibləri pizza çatdırılmasından tutmuş elektrikçilərə qədər müxtəlif ev xidmətləri sifariş etmək və təşkil etmək üçün telefonlarından istifadə edirlər. Hətta nisbətən yoxsul icmaların da telekomunikasiyadan öz üstünlükləri üçün istifadə etdikləri hamımıza məlumdur. Banqladeşin Narshingdi bölgəsində, təcrid olunmuş kəndlilər birbaşa toptancılarla danışmaq və mallarına daha yaxşı qiymət vermək üçün mobil telefondan istifadə edirlər. Kot-d'İvuarda qəhvə yetişdiriciləri qəhvə qiymətlərindəki hər saat dəyişikliyini izləmək və ən yaxşı qiymətə satmaq üçün mobil telefonların tətbiqindən faydalanırlar.

1.13.2 İqtisadi təsirlər. Makroiqtisadiyyat səviyyəsində

Makroiqtisadi miqyasda Lars-Hendrik Röller və Leonard Waverman yaxşı telekommunikasiya infrastrukturu ilə iqtisadi böyümə arasında səbəbli əlaqə təklif etdilər. Bəziləri əlaqəni səbəb kimi görmək düzgün olmadığını iddia etsələr də, mütəxəssislərin əksəriyyəti bir əlaqənin mövcudluğu barədə həmfikir oldular.

Bununla belə, yaxşı telekommunikasiya infrastrukturunun iqtisadi faydaları səbəbindən dünyanın müxtəlif ölkələri arasında telekommunikasiya xidmətlərinə qeyri-bərabər çıxışı ilə əlaqədar narahatlıq artmaqdadır. Bu hadisə rəqəmsal boşluq kimi tanınır. Beynəlxalq Telekommunikasiya İttifaqının (BTİ) 2003-cü ildə apardığı bir araşdırma, ölkələrin təxminən üçdə birinin hər 20 nəfərə birdən çox mobil abunə, ölkələrin üçdə birində hər 20 nəfər üçün bir dənə də olsun quru telefon abunəçiliyinə sahib olduğunu göstərdi. İnternetə çıxışı baxımından, bütün ölkələrin təxminən yarısı İnternetə çıxışı olan 20 nəfərdən birinə düşən hissədən daha aşağı göstəriciyə malikdir.

Bu məlumatlardan, eləcə də təhsil məlumatlarından BTİ, vətəndaşların informasiya və rabitə texnologiyalarından istifadə və istifadə etmək qabiliyyətlərini ölçən bir indeks tərtib edə bildi. Statistikaya görə İsveç, Danimarka və İslandiya ən yüksək, Afrika ölkələri Nigeriya, Burkina Faso və Mali ən aşağı göstəricilərə sahib oldu.

1.13.3 Sosial təsirlər

Telekommunikasiya sosial münasibətlərdə də mühüm rol oynamışdır. Bununla belə, telefon sistemi kimi qurğular əvvəlcə sosial ölçülərdən fərqli olaraq cihazın praktik ölçülərinə görə (məsələn, iş aparmaq və ya ev xidmətləri sifariş etmək qabiliyyəti) reklam edildi. Yalnız 1920-ci illərin sonu və 1930-cu illərə qədər cihazın sosial ölçüləri telefon reklamlarında görkəmli bir mövzu oldu. Yeni promosyonlar, sosial söhbətlərin cəmiyyətdə insanların ailəsi və dostları ilə əlaqədə olmağın vacibliyini vurğulayaraq, istehlakçıların emosiyalarına müraciət etməyə başladılar.

O vaxtdan bəri telekomunasiyanın sosial münasibətlərdə oynadığı rol getdikcə daha çox əhəmiyyət kəsb etməyə başladı. Son illərdə sosial şəbəkə saytlarının populyarlığı kəskin artdı. Bu saytlar istifadəçilərə bir-biri ilə ünsiyyət qurmaq, başqalarının görmək üçün fotoşəkillər, hadisələr və profillər göndərmək imkanı verir. Profillər bir insanın yaşını, maraqlarını, cinsi üstünlüklərini və münasibət statuslarını sadalaya bilər. Bu baxımdan bu saytlar sosial əlaqələrin qurulmasından tutmuş məhkəmə görüşünə qədər hər şeydə mühüm rol oynaya bilər.

Sosial şəbəkə saytlarından əvvəl qısa mesaj xidməti (SMS) və telefon kimi texnologiyalar da sosial qarşılıqlı əlaqələrə ciddi təsir göstərmişdir. 2000-ci ildə İpsos MORI bazar araşdırma qrupu, İngiltərədəki 15-24 yaşındakı SMS istifadəçilərinin 81% -nin, sosial tənzimləmələri əlaqələndirmək üçün xidmətdən istifadə etdiyini və 42% -inin cəmiyyətin ən ümumi və ortaq məişət problemləri məqsədilə istifadə etdiyini bildirdi.

1.13.4 Digər təsirlər

Mədəni baxımdan telekommunikasiya ən azı cəmiyyətin musiqi və filmə giriş imkanlarını artırdı. Məsələn: televiziya ilə insanlar video mağazasına və ya kinoya getmədən əvvəl öz evlərində görmədikləri filmlərə baxa bilərlər. Yaxud radio və internet ilə insanlar musiqi mağazasına getmədən arzuladıqları musiqiləri dinləyə bilərlər.

Telekommunikasiya həm də insanların öz xəbərlərini alma tərzini dəyişdirdi. 2006-cı ildə ABŞ-da qeyri-kommersiya Pew İnternet və Amerika Həyatı Layihəsi tərəfindən 3000-dən çox amerikalıdan ibarət bir araşdırma aparıldı. Araşdırma nəticəsində insanların xəbər alma üsulları arasında televiziya və ya radio kimi telekommunikasiya vasitələrindən istifadənin qəzet və digər üsullardan istifadəni aşkar fərqlə qabaqladığı məlum oldu.

Telekommunikasiya, reklamlara da eyni dərəcədə əhəmiyyətli təsir göstərmişdir. TNS Media Intelligence, 2007-ci ildə ABŞ-da reklam xərclərinin 58% -ni telekommunikasiya sahəsindən asılı olan KİV-lərə xərclədiyini bildirmişdir.

1.13.5 Telekommunikasiyanın hökumət səviyyəsində təsirləri

Bir çox ölkələr "BMT-nin informasiya və rabitə texnologiyaları məsələləri üzrə aparıcı agentliyi" olan Beynəlxalq Telekommunikasiya İttifaqı (İTU) tərəfindən qurulmuş Beynəlxalq Telekommunikasiya Qaydalarına uyğun qanun qəbul etdi. 1947-ci ildə, Atlantic City konfransında, BTİ "yeni bir beynəlxalq tezlik siyahısında qeydiyyata alınan və Radio Qaydalarına uyğun olaraq istifadə edilən bütün tezliklərə beynəlxalq müdafiəni təmin etmək" qərarına gəldi. BTİ-nin Atlantik şəhərində qəbul etdiyi Radio Qaydalarına əsasən, Beynəlxalq Frekans Qeydiyyatı Şurasında istinad edilən, idarə heyəti tərəfindən araşdırılmış və Beynəlxalq Tezlik Siyahısında qeydiyyata alınan bütün tezliklər "zərərli müdaxilədən beynəlxalq qorunma hüququna malikdir".

Qlobal baxımdan telekommunikasiya və yayımın idarə olunması ilə bağlı siyasi mübahisələr və qanunvericilik mövcuddur. Yayımın tarixi, radio yayımı kimi çap və telekommunikasiya kimi şərti rabitə ilə əlaqəli bəzi mübahisələri müzakirə edir. İkinci Dünya Müharibəsinin başlanması beynəlxalq yayım təbliğatının ilk partlamasına səbəb oldu. Ölkələr, onların hökumətləri, qiyamçılar, terrorçular və milislər təbliğatı təşviq etmək üçün hamısı telekommunikasiya və yayım texnikasından istifadə etdilər. Siyasi hərəkatlar və müstəmləkəçilik üçün vətənpərvərlik təbliğatı 1930-cu illərin ortalarından başladı. 1936-cı ildə BBC, Şimali Afrikada da müstəmləkə maraqlarına sahib olan İtaliyadan bənzər verilişlərə qarşı çıxmaq üçün Ərəb dünyasına təbliğat yayımladı.

Son İraq müharibəsindəki kimi müasir üsyançılar, əməliyyatdan bir neçə saat sonra qorxuducu telefon danışıqları, SMS və koalisiya qoşunlarına edilən hücumun mürəkkəb videolarından istifadə edirlər. "Sünni üsyançıların hətta öz televiziya stansiyası var. Əl-Zavraa, İraq hökuməti tərəfindən qadağan edilsə də, koalisiya təzyiqi onu bir neçə dəfə peyk aparatlarını dəyişdirməyə məcbur etdiyi kimi, İraq Kürdüstanının Ərbil şəhərindən də yayımlayır."

1.14 İnformasiya təhlükəsizliyinə tələbat

Təhlükəsizlik mühəndisliyi pislik, səhv və uyğunsuzluq qarşısında etibarlı qalacaq sistemlərin qurulması ilə məşğul olur. Tam sistemlərin dizaynı, tətbiqi və sınaqdan keçirilməsi, habelə ətraf mühitin dəyişməsi ilə mövcud sistemlərin uyğunlaşdırılması üçün tələb olunan alətlər, proseslər və metodlar üzərində cəmlənir. Bunlara kriptovalyutası, kompüter təhlükəsizliyi, aparat istiliyinə davamlılıq, iqtisadiyyat, tətbiqi psixologiya, təşkilatlar və qanunları əhatə edən çarpaz intizam ekspertizası tələb olunur. Müasir kriptovalyutası riyaziyyat, kompüterşünaslıq və elektrik mühəndisliyi fənlərini kəsişdirir. Beləliklə, yaxşı təhlükəsizlik mühəndisliyi dörd elementin birləşməsini tələb edir. Siyasətə ehtiyac var; nail olmaq üçün qarşıya qoyulan məqsədlər. Sonra mexanizm; siyasəti həyata keçirmək üçün toplanacaq şifrlər, giriş kontrolları, aparat dəyişdiricilərinə müqavimət və digər maşınlar kimi. Həm də

əminliyə ehtiyacımız var; hər bir mexanizmə yerləşdiriləcək etibar dərəcəsi. Nəhayət, təşviq var; Sistemi qoruyan və qoruyan insanların optimal performansını artıran motivləri, təcavüzkarların siyasəti məğlub etməyə çalışdıqları motivləri.

FƏSIL 2. KOMMUNİKASİYA SİSTEMLƏRİNİN TƏHLÜKƏSİZLİYİNİN KONSEPTUAL MODELI

2.1 Müasir telekommunikasiya sistemlərinin əsas elementləri

Müasir telekommunikasiya bir əsrdən çox müddət ərzində mütərəqqi inkişaf yaşamış bir sıra əsas konsepsiyalara əsaslanır. Telekommunikasiya texnologiyaları ilk növbədə simli və simsiz metodlara bölünə bilər. Ümumilikdə əsas telekommunikasiya sistemi hər zaman bu və ya digər şəkildə mövcud olan üç əsas hissədən ibarətdir:

1. Məlumat alaraq onu bir siqnala çevirən ötürücü qurğu
2. Siqnal daşıyan tez-tez “fiziki kanal” olaraq da adlanan ötürücü vasitə. Nümunə olaraq "boş yer kanalı"nı misal göstərmək olar.
3. Kanaldan siqnal götürən və onu alıcı üçün lazımlı məlumatlara çevirən qəbuledici.

Məsələn, bir radio yayım stansiyasında stansiyanın böyük gücləndiricisi ötürücüdür; və yayım antenası güc gücləndiricisi və "boş yer kanalı" arasındakı interfeysdir. Boş yer kanalını ötürmə mühiti kimi düşünmək olar və bu zaman alıcının antenası boş yer kanalı ilə qəbuledici arasında interfeys kimi çıxış edir. Son olaraq, radio qəbuledici radio siqnalının təyin olunduğu nöqtədir və insanların qulaq asması üçün elektrik enerjisindən səsə çevrildiyi yerdir.

Bəzən telekommunikasiya sistemləri həm ötürücü, həm də qəbuledici, və yaxud da həm də ötürücü kimi işləyən tək elektron qutusundan ibarət olan amma "dupleks" (iki tərəfli sistemlər) olur. Məsələn, mobil telefon ötürücüdür. Bir ötürücü elektron və qəbuledicinin içərisində olan elektronika əslində bir-birlərindən olduqca müstəqildir. Bunu asanlıqla izah etmək olar ki, radio ötürücülərdə vatt və ya kilovatla ölçülən elektrik gücləri ilə işləyən gücləndiricilər var, lakin radio qəbuledicilər mikrodalğalarda

və ya nanovattlarda ölçülən radio güclər vasitəsilə işləyirlər. Beləliklə, ötürücülər yüksək güclü dövrə və aşağı gücə malik dövriyyələrin işləməsi zamanı bir-birinə müdaxilələrin qarşısını almaq üçün diqqətlə hazırlanmalı və qurulmalıdırlar.

Sabit xətlər üzərindəki telekommunikasiya yalnız bir ötürücü və yalnız bir qəbuledici arasında olduğu üçün nöqtədən nöqtəyə əlaqəsi adlanır.

Çoxsaylı ötürücü və çox sayda qəbuledicinin eyni fiziki kanal vasitəsilə əməkdaşlıq etmək və qəbuledicilər arasında palaşmaq üçün hazırlanmış telekommunikasiya multipleks sistemlər adlanır. Multipleksinq üsulundan istifadə edərək fiziki kanalların paylaşımı çox vaxt xərclərdə çox böyük azalmalara səbəb olur. Çoxtərəfli sistemlər telekommunikasiya şəbəkələri daxilində qurulur və multipleks siqnallar qovşaqlarda düzgün təyinat terminal qəbuledicisinə keçir.

2.2 Əsas təhlükəsizlik arxitekturası və ölçüləri

ITU-T təlimatlarında göstərildiyi kimi Tövsiyə X.805, paylanmış tətbiqlərin son təhlükəsizliyinə nail olmaq üçün memarlıq və ölçüləri müəyyənləşdirir. Ümumi prinsiplər və təriflər bütün tətbiqlərə tətbiq olunur, baxmayaraq ki, təhdid və həssaslıq kimi təfərrüatlar və onların qarşısını almaq və ya qarşısını almaq tədbirləri bir tətbiq ehtiyaclarına görə dəyişir.

Təhlükəsizlik arxitekturası iki əsas konsepsiya təbəqəsi baxımından müəyyən edilmişdir. Təhlükəsizlik təbəqələri şəbəkə elementlərinə və son şəbəkəni təşkil edən sistemlərə tətbiq olunan tələbləri ünvanlayır. Üç qat infrastruktur təbəqəsi, xidmətlər qatı və tətbiqlər təbəqəsidir. Qatları müəyyənləşdirməyin üstünlüklərindən biri də sona çatan təhlükəsizliyi təmin etmək üçün fərqli tətbiqlər arasında təkrar istifadəyə imkan verməkdir. Hər bir təbəqədəki zəifliklər fərqlidir və beləliklə hər təbəqənin ehtiyaclarını ödəmək üçün əks tədbirlər təyin edilməlidir.

İnfrastruktur təbəqəsi ayrıca şəbəkə elementlərindən əlavə şəbəkə ötürmə qurğularından ibarətdir. İnfrastruktur qatına aid olan komponentlərin nümunələri fərdi marşrutlaşdırıcılar, açarlar və serverlər, eləcə də aralarındakı rabitə əlaqələrini yaradır.

Xidmətlər təbəqəsi müştərilərə təklif olunan şəbəkə xidmətlərinin təhlükəsizliyini təmin edir. Bu xidmətlər icarəyə verilən xətt xidmətləri kimi əsas əlaqə təkliflərindən tutmuş sürətli mesajlaşma kimi əlavə dəyər xidmətləri arasındadır.

Tətbiqlər təbəqəsi müştərilərin istifadə etdiyi şəbəkə əsaslı tətbiqlərin tələblərinə cavab verir. Bu tətbiqlər e-poçt kimi sadə və ya çox yüksək səviyyəli video köçürmələrin neft kəşfiyyatında və ya avtomobillər dizaynında istifadə edildiyi bir yerdə görüntülənən qədər mürəkkəb ola bilər.

2.3 Təhlükəsizlik konteksti

Əsasən, kriptovalyutaya ehtiyac, məlumatın saxlanması və ya ötürülməsi ilə bağlı tələblərə cavab olaraq ortaya çıxdı. Təmin etmək üçün müəyyən etdiyi ən əsas təhlükəsizlik ehtiyacları məxfilik, bütövlük, mövcudluq və orijinallıqdır.

Doğrulama simmetrik (şəxsi açar) kriptoqrafiya üçün istifadə edilsə də, onun asimmetrik (açıq açar) kriptovalyutada ekvivalenti rəqəmsal imzadır. Doğrulama göndərən tərəfindən qəbul edilən və qəbuledici tərəfindən paylaşılan bir təsdiqləmə açarı ilə göndərən tərəfindən yaradılan Mesaj Doğrulama Kodu (MAC) vasitəsi ilə həyata keçirilir. Digər tərəfdən, hər bir iştirakçının açıq açarının sertifikatlaşdırılması Sertifikat Orqanının (CA) Açıq Açar İnfrastrukturu (PKI) sxemində rəqəmsal imza vasitəsilə həyata keçirilir.

Bir sistemdəki təhlükəsizlik problemlərini qiymətləndirərkən, sistemin təhlükəsizlik vəziyyətinin bir neçə xüsusiyyətini qiymətləndirmək lazımdır. Bunlara təhdidlər, zəifliklər və risklər daxil edilməlidir. Təhdidlər sistemin təhlükəsizliyinə potensial zərər verə biləcək hadisələr, məsələlər və ya varlıqlardır; bunlar təbii fəlakətlər də daxil olmaqla qəsdən və ya başqa şəkildə ola bilər. Zəifliklər, sistemə zərər

vurmaq üçün potensial bir qabiliyyəti təmin edən və ya cəlb edən kanallar və ya vasitələrdir; zərərin meydana gəlməsi üçün fürsətdir. Məsələn, balanslaşdırılmış diyetlərin olmaması insanı xəstəliklərə qarşı həssas edir və ya qapısını kiliddən buraxmaq evin fiziki təhlükəsizliyindəki bir zəifliyə səbəb olur. Nəhayət, həm təhdidlərin, həm də zəifliklərin birlikdə olduğu yerlərdə risklərin mövcud olduğu deyilir. Başqa sözlə, sistemin təhlükəsizliyini pozmaq üçün onsuz da mövcud olan bir zəifliyi istifadə edə biləcək bir sistem üçün təhlükə yaradır. Məsələn, tamamilə savadsız bir düşmənlə qarşı-qarşıya qalan bir orduda əmrləri ümumiyyətlə, düz mətnlə yazmaq, həssaslığı meydana gətirir, lakin uyğun bir təhlükə olmadığı üçün əlaqəli bir risk yoxdur, çünki düşmənin oxumaq qabiliyyəti yoxdur. mesaj. Adətən, sistemin təhlükəsizliyindəki potensial problemləri müəyyən etmək üçün sistematik bir risk analizində sistemlə əlaqəli müxtəlif təhdid və zəifliklərin bir matrisini yaratmaq faydalıdır (Risk Qiymətləndirmə Matrix).

2.4 Telekommunikasiya şəbəkəsinin əsas mahiyyəti

Bir telekommunikasiya şəbəkəsi bir-birinə mesaj göndərən ötürücülərin, qəbuledicilərin və rabitə kanallarının toplusudur. Bəzi rəqəmsal rabitə şəbəkələrində istifadəçiyə məlumatı düzgün ötürmək üçün birlikdə işləyən bir və ya daha çox marşrutlaşdırıcı yerləşdirilir. Analoq rabitə şəbəkəsi iki və ya daha çox istifadəçi arasında əlaqə quran bir və ya daha çox açardan (çeviricidən) ibarətdir. Hər iki şəbəkə növü üçün uzun məsafələrə ötürüldükdə siqnalın gücləndirilməsi və ya yenidən qurulması üçün təkrarlayıcılara ehtiyac ola bilər.

2.4.1 Əlaqə kanalları

"Kanal" termini iki fərqli mənaya malikdir. Bir mənada kanal ötürücü və qəbuledici arasında siqnal daşıyan fiziki mühitdir. Buna misal olaraq səsli rabitə üçün atmosfer, bəzi növ optik rabitə üçün şüşə optik liflər, voltaj və elektrik cərəyanları vasitəsilə rabitə yaratmaq üçün istifadə olunan koaksial kabellər, görünən işıq, infraqırmızı dalğalar, ultrabənövşəyi işıq, radio dalğaları və sairə nümunə gətirmək

olar. Bu kanal "boş yer kanalı" adlanır. Radio dalğalarının bir yerdən digərinə göndərilməsinin ikisi arasında bir atmosferin olması və ya olmaması ilə heç bir əlaqəsi yoxdur. Radio dalğalar hava, duman, bulud və ya hər hansı digər bir qazın təsirindən asılı olmayaraq istənilən mühitdən keçərək öz ünvanına çata bilmək kimi mükəmməl bir xarakteristikası vardır.

Telekomunikasiyada "kanal" ifadəsinin digər mənası, birdən çox məlumat axınını eyni anda göndərmək üçün istifadə edilə bilməsi məqsədilə bir ötürücü mühitin bir hissəsi olan rabitə kanalı mənasında anlaşılmaqdadır. Məsələn, bir radio stansiyası 94.5 MHz (megahertz) qonşuluqdakı frekanslarda radio dalğaları boş yerə sərbəst yayımlaya bilər, digər bir radio stansiyası isə eyni vaxtda 96.1 MHz ətrafındakı tezliklərdə radio dalğalarını yayımlaya bilər. Hər bir radio stansiyası, "daşıyıcı tezlikləri" adlanan yuxarıdakı kimi tezliklərdə mərkəzləşdirilmiş qaydada təxminən 180 kHz (kilohertz) tezlik bantı üzərində radio dalğaları ötürür. Bu nümunədəki hər bir stansiya, bitişik stansiyalarından 200 kHz ilə ayrılır.

Yuxarıdakı nümunədə, "boş yer kanalı" tezliklərə görə rabitə kanallarına bölünmüş və hər bir kanala radio dalğalarının yayımlanacağı ayrı bir tezlik diapazonu verilmişdir. Orta mühitin tezliyə görə kanallara bölünməsi sistemi "tezlik-bölmə multipleksasiyası" adlanır. Eyni konsepsiya üçün başqa bir termin, "çox dalğa uzunluğunda bölmə multipleksləşməsi" dir, bu, çox ötürücü eyni fiziki mühiti bölüşdükdə daha çox istifadə olunur.

Bir rabitə mühitini kanallara ayırmağın başqa bir yolu, hər bir göndərənə təkrarlanan vaxt seqmentini (bir "zaman yuvası", məsələn, hər saniyədən 20 millisaniyəlik) ayırmaq və hər göndərənə yalnız öz vaxtı ərzində mesaj göndərməsinə imkan verməkdir. Orta hissəni rabitə kanallarına ayırmağın bu üsulu "vaxt bölmə multipleksasiyası" (TDM) adlanır və optik lif rabitəsində istifadə olunur. Bəzi radio rabitə sistemləri ayrılmış FDM kanalı daxilində TDM istifadə edir. Beləliklə, bu sistemlər TDM və FDM hibridindən istifadə etmiş olurlar.

2.4.2 Moldulyasiya

Məlumat ötürmək üçün bir siqnalın formalaşması modulyasiya kimi tanınır. Rəqəmsal bir mesajı analoq dalğa şəklində təmsil etmək üçün modulyasiya istifadə edilə bilər. Buna ümumi halda "açarlama" deyilir. Morse Kodunun telekommunikasiya sahəsində daha köhnə tətbiqlərdən yararlandığı bir neçə açarlama üsulu mövcuddur. Bunlara faza-növbə açarlığı, tezlik dəyişməsi açarlığı və amplituda dəyişmə düymələri daxildir. Məsələn, "Bluetooth" sistemi müxtəlif qurğular arasında məlumat mübadiləsi üçün faza növbəli düymələrdən istifadə edir. Bundan əlavə, yüksək tutumlu rəqəmsal radio rabitə sistemlərində istifadə olunan "kvadrat kvadrat amplituda modulyasiyası" (QAM) adlanan faza-növbəli açarlama və amplitüd-növbəli açarlama birləşmələri mövcuddur.

Modulyasiya həmçinin aşağı tezlikli analoq siqnalların məlumatlarını daha yüksək tezliklərdə ötürmək məqsədilə də istifadə edilə bilər. Bu, aşağı tezlikli analoq siqnalların boş yer üzərində effektiv şəkildə ötürülə bilməməsi səbəbindən çox faydalıdır. Beləliklə, aşağı tezlikli analoq siqnaldan gələn məlumat ötürülməzdən əvvəl daha yüksək tezlikli bir siqnala ("daşıyıcı dalğa" kimi tanınır) təsir etməlidir. Buna nail olmaq üçün bir neçə müxtəlif modulyasiya sxemləri mövcuddur. ən əsas olan iki amplituda modulyasiyası (AM) və tezlik modulyasiyası (FM). Bu prosesə bir nümunə, bir frekans modulyasiyasından istifadə edərək 96 MHz-lik bir daşıyıcı dalğasına təsir edən bir disk jokeyinin səsini göstərmək olar. Bu zaman səs daha sonra "96 FM" kanalı kimi bir radioda qəbul edilir. Bundan əlavə, modulyasiya, tezlik bölünməsi multiplexing (FDM) istifadə edə biləcək bir üstünlüyə malikdir.

2.5 İnformasiya təhlükəsizliyi prinsiplərini tənzimləyən ümumi qanun və qaydalar

Aşağıda, dünyanın müxtəlif yerlərində məlumatların emalı və informasiya təhlükəsizliyinə əhəmiyyətli təsir göstərən və ya olacaq hökumət qanunlarının və qaydaların qismən siyahısı verilmişdir. Həmçini İnformasiya təhlükəsizliyinə

əhəmiyyətli dərəcədə təsir göstərdikdə mühüm sənaye sektoru qaydaları da daxil edilmişdir.

1. Böyük Britaniyanın Məlumatların Mühafizəsi Qanunu 1998-ci ildə bu cür məlumatların əldə edilməsi, saxlanılması, istifadəsi və ya açıqlanması da daxil olmaqla ayrı-ayrı şəxslərə aid məlumatların emalının tənzimlənməsi üçün yeni müddəalar verir. Avropa Birliyi Məlumat Qoruma Direktivi (EUDPD), bütün E.U. tələb edir. üzvləri E.U. ərzində vətəndaşlar üçün məlumat məxfiliyinin qorunmasını standartlaşdırmaq üçün milli qaydalar qəbul edirlər.
2. Kompüterdən sui-istifadə aktı 1990-cı il ABŞ Parlamentinin kompüter cinayətini (məsələn, hack etmə) cinayət törətməsi aktıdır. Bu akt bir sıra digər ölkələrin, o cümlədən Kanada və İrlandiya Respublikasının informasiya təhlükəsizliyi qanunlarını hazırladıqları zaman ilham aldıqları bir modelə çevrildi.
3. E.U.-nun Məlumatların Saxlanılması Direktivi (ləğv olundu), internet xidməti təminatçılarından və telefon şirkətlərindən altı aydan iki ilədək edilən hər bir elektron mesaj və telefon danışığında məlumatların saxlanmasını tələb etdi.
4. Ailənin Təhsil Hüquqları və Məxfilik Qanunu (FERPA) (20 ABŞ § 1232 g; 34 CFR Hissə 99) tələbə təhsili qeydlərinin məxfiliyini qoruyan ABŞ Federal Qanunudur. Qanun ABŞ Təhsil İdarəsinin tətbiq olunan bir proqramı çərçivəsində vəsait alan bütün məktəblərə şamil olunur. Ümumiyyətlə, məktəblərdə bir şagirdin təhsil rekordundan hər hansı bir məlumat çıxarmaq üçün valideyndən və ya uyğun tələbədən yazılı icazə alınmalıdır
5. Federal Maliyyə Təşkilatları İmtahan Şurasının (FFIEC) auditorlar üçün təhlükəsizlik qaydaları, onlayn bank təhlükəsizliyinə dair tələbləri müəyyənləşdirir.
6. 1996-cı il tarixli Tibbi Sığorta Daşınması və Hesabatlılıq Qanunu (HIPAA) elektron səhiyyə əməliyyatları üçün milli standartların və provayderlər, tibbi sığorta planları və işəgötürənlər üçün milli identifikatorların qəbul edilməsini

tələb edir. Əlavə olaraq, sağlamlıq məlumatları təhlükəsizliyini və məxfiliyini qorumaq üçün tibb işçilərindən, sığorta təminatçılarından və işəgötürənlərdən tələb olunur.

7. 1999-cu il Gramm-Leach-Bliley Aktı (GLBA), 1999-cu il Maliyyə Xidmətlərinin Müasirləşdirilməsi Qanunu olaraq da tanınır, maliyyə qurumlarının topladığı, saxladığı və işlədiyi fərdi maliyyə məlumatlarının məxfiliyini və təhlükəsizliyini qoruyur.
8. 2002-ci il Sarbanes-Oxley Qanununun (SOX) 404-cü bölməsi, açıq şəkildə satılan şirkətlərdən hər maliyyə ilinin sonunda təqdim etdikləri illik hesabatlarda maliyyə hesabatları üçün daxili nəzarətlərinin səmərəliliyini qiymətləndirmələrini tələb edir. Baş məlumat işçiləri maliyyə məlumatlarını idarə edən və hesabat verən sistemlərin təhlükəsizliyinə, dəqiqliyinə və etibarlılığına cavabdehdirlər. Bu akt, həmçinin açıq şəkildə satılan şirkətlərdən qiymətləndirmələrinin doğruluğunu təsdiq etməli və hesabat verməli olan müstəqil auditorlarla əlaqə yaratmağı tələb edir.
9. Ödəniş Kartı Sənaye Məlumat Təhlükəsizliyi Standartı (PCI DSS) ödəniş hesabı məlumatları təhlükəsizliyinin artırılması üçün hərtərəfli tələbləri müəyyən edir. PCI Təhlükəsizlik Standartları Şurasının qurucu ödəmə markaları, o cümlədən American Express, Discover Financial Services, JCB, MasterCard Worldwide və Visa International - qlobal əsasda ardıcıl məlumat təhlükəsizliyi tədbirlərinin geniş tətbiqini asanlaşdırmaq üçün hazırlanmışdır. PCI DSS, təhlükəsizlik idarəetmə, siyasət, prosedur, şəbəkə arxitekturası, proqram dizaynı və digər kritik qoruyucu tədbirlər tələblərini özündə cəmləşdirən çoxşaxəli təhlükəsizlik standartıdır.
10. Dövlət təhlükəsizliyinin pozulması barədə bildiriş qanunları (Kaliforniya və bir çoxu) şifrələnməmiş "şəxsi məlumatların" pozulduğu, itirildiyi və ya oğurlandığı zaman istehlakçılara xəbərdarlıq etmələrini tələb edir.

11. Kanadanın Şəxsi Məlumatların Mühafizəsi və Elektron Sənəd Qanunu (PIPEDA), müəyyən şərtlərdə toplanmış, istifadə edilən və ya açıqlanmış şəxsi məlumatları qorumaqla, məlumat və ya əməliyyatları çatdırmaq və ya qeyd etmək üçün elektron vasitələrdən istifadəni təmin etməklə elektron ticarəti dəstəkləyir və təbliğ edir. Kanada Sübut Qanununa, Qanuni Sənədlər Qanununa və Əsasnamə Yenidən İştirak Qanununa düzəlişlər.
12. Yunanıstanın Rabitə Təhlükəsizliyi və Məxfilik üzrə Yunan Orqanlığı (ADAE) (Qanun 165/2011), müştərilərin məxfiliyini qorumaq üçün Yunanıstanda elektron rabitə şəbəkələri və / və ya xidmətlər təqdim edən hər bir şirkət tərəfindən tətbiq ediləcək minimum məlumat təhlükəsizliyi nəzarətlərini yaradır və təsvir edir. . Bunlara həm idarəetmə, həm də texniki nəzarət daxildir (məsələn, qeyd qeydləri iki il ərzində saxlanılmalıdır).
13. Yunanıstanın Rabitə Təhlükəsizliyi və Məxfiliyi üzrə Yunan Orqanlığı Təşkilatı (ADAE) (Qanun 205/2013) Yunanıstan telekommunikasiya şirkətləri tərəfindən təqdim olunan xidmətlərin və məlumatların bütövlüyünün və əlçatanlığının qorunması ətrafında cəmləşir. Qanun bu və digər əlaqəli şirkətləri müvafiq iş planları və lazımsız infrastrukturları qurmağa, yerləşdirməyə və sınaqdan keçirməyə məcbur edir.

2.6 İnformasiya təhlükəsizliyi mədəniyyəti

Təhlükəsizliyə bələd olan işçilərin nə dərəcədə olduğunu izah etməklə, informasiya təhlükəsizliyi mədəniyyəti, məlumat təhlükəsizliyinə həm müsbət, həm də mənfi istiqamətdə təsir edən bir təşkilatın fikirləri, adətləri və sosial davranışlarıdır. Mədəni anlayışlar təşkilatın müxtəlif seqmentlərinin səmərəli işləməsinə kömək edə bilər və ya bir təşkilat daxilində məlumat təhlükəsizliyinə qarşı işləyir. İşçilərin təhlükəsizlik və düşündükləri düşüncə tərzi və gördükləri işlər təşkilatlarda informasiya təhlükəsizliyinə çox təsir edə bilər. Roer & Petric (2017) təşkilatlarda informasiya təhlükəsizliyi mədəniyyətinin yeddi əsas ölçüsünü müəyyənləşdirir:

- Münasibətlər: İşçilərin məlumatların təşkilati təhlükəsizliyinə aid müxtəlif fəaliyyətlərlə bağlı hissləri və duyğuları.
- Davranışlar: Məlumat təhlükəsizliyinə birbaşa və ya dolayı təsir göstərən aktual və ya nəzərdə tutulan fəaliyyətlər və işçilərin risk alma hərəkətləri.
- Tanıma: İşçilərin məlumat təhlükəsizliyi ilə əlaqəli olan təcrübə, fəaliyyət və öz effektivliyi ilə əlaqəli məlumatlandırma, yoxlanıla bilən məlumat və inanclar.
- Ünsiyyət: İşçilərin bir-biri ilə ünsiyyət qurma yolları, mənlik hissi, təhlükəsizlik məsələlərinə dəstək və hadisələrin hesabatlandırılması.
- Uyğunluq: Təşkilati təhlükəsizlik siyasətinə riayət etmək, bu cür siyasətlərin mövcudluğundan xəbərdar olmaq və bu siyasətlərin mahiyyətini geri çağırmaq bacarığı.
- Normalar: Təhlükəsizliklə əlaqəli təşkilati davranış və işçilər və həmyaşıdları tərəfindən normal və ya sapma hesab olunan təcrübələr, məsələn, təhlükəsizlik təhlükəsizlik davranışları ilə bağlı gizli gözləntilər və informasiya-kommunikasiya texnologiyalarının istifadəsinə dair yazılmamış qaydalar.
- Məsuliyyətlər: İşçilərin, məlumatların təhlükəsizliyini qorumaq və ya təhlükə altına almaq üçün kritik bir amil olaraq aldıqları rol və vəzifələri dərk etməsi və bununla da təşkilat.

Andersson və Reimers (2014), işçilərin özlərini təşkilatın Təhlükəsizlik Təhlükəsizliyi "səyləri" nin bir hissəsi olaraq görmədiklərini və tez-tez təşkilati informasiya təhlükəsizliyini ən yaxşı maraqlarına məhəl qoymayan hərəkətlər etdiklərini tapdılar. Tədqiqatlar göstərir ki, informasiya təhlükəsizliyi mədəniyyəti davamlı inkişaf etdirilməlidir. Təhlildən Dəyişməyə qədər İnformasiya Təhlükəsizliyi Mədəniyyətində müəlliflər, "Bu bitməyən bir proses, qiymətləndirmə və dəyişiklik və ya təmir dövrüdür." İnformasiya təhlükəsizliyi mədəniyyətini idarə etmək üçün beş addım atılmalıdır: əvvəlcədən qiymətləndirmə, strateji planlaşdırma, operativ planlaşdırma, həyata keçirmə və qiymətləndirmədən sonra.

- Əvvəlcədən qiymətləndirmə: işçilərin daxilində informasiya təhlükəsizliyi barədə məlumatlılığı müəyyən etmək və mövcud təhlükəsizlik siyasətini təhlil etmək
- Strateji Planlaşdırma: Daha yaxşı bir məlumatlandırma proqramı hazırlamaq üçün aydın hədəflər təyin etməliyik. Buna nail olmaq üçün insanları qruplaşdırmaq faydalıdır
- Əməliyyat Planlaşdırma: daxili ünsiyyət, idarəetmə alışı, təhlükəsizlik maarifləndirmə və təlim proqramlarına əsaslanan yaxşı bir təhlükəsizlik mədəniyyətini yaratmaq
- İcra: rəhbərliyin öhdəliyi, təşkilat üzvləri ilə ünsiyyət, bütün təşkilat üzvləri üçün kurslar və işçilərin öhdəlikləri olmalıdır
- Qiymətləndirmədən sonrakı dövr: Əvvəlki addımların effektivliyini daha yaxşı qiymətləndirmək və davamlı təkmilləşmə üzərində qurulmaq

2.7 Standartların mənbələri

Beynəlxalq Standartlaşdırma Təşkilatı (İSO), İsveçrənin Cenevrə şəhərində bir katiblik tərəfindən əlaqələndirilən 157 ölkənin milli standartları institutlarının konsorsiumudur. ISO dünyanın ən böyük standartlar tərtibatçısıdır. İSO 15443: "İnformasiya texnologiyası - Təhlükəsizlik texnikası - İT təhlükəsizliyinin təminatı üçün bir çərçivə", ISO / IEC 27002: "İnformasiya texnologiyası - Təhlükəsizlik texnikası - İnformasiya təhlükəsizliyinin idarə olunması üçün təcrübə kodu", İSO-20000: "İnformasiya texnologiyası - Xidmətin idarə edilməsi" və ISO / IEC 27001: "İnformasiya texnologiyaları - Təhlükəsizlik texnikası - İnformasiya təhlükəsizliyini idarəetmə sistemləri - Tələblər" informasiya təhlükəsizliyi mütəxəssisləri üçün xüsusi maraq doğurur.

ABŞ Milli Standartlar və Texnologiya İnstitutu (NİST), ABŞ Ticarət Departamentində tənzimlənməyən bir federal agentlikdir. NIST Kompüter Təhlükəsizliyi Bölməsi standartlar, ölçülər, testlər və qiymətləndirmə proqramlarını

inkişaf etdirir, təhlükəsiz İT planlamasını, tətbiqini, idarə edilməsini və istismarını artırmaq üçün standart və qaydaları dərc edir. NIST eyni zamanda ABŞ Federal İnformasiya Qenerasiya Standart nəşrlərinin (FIPS) qəyyumudur.

İnternet Cəmiyyəti, 180-dən çox ölkədə 100-dən çox təşkilat və 20 mindən çox fərdi üzvü olan peşəkar bir cəmiyyətdir. İnternetin gələcəyi ilə qarşılaşan məsələlərin həllində liderliyi təmin edir və İnternet Mühəndisliyi Tapşırıq Qüvvələri (IETF) və İnternet Memarlıq Şurası (IAB) daxil olmaqla, İnfrastruktur standartlarına cavab verən qruplar üçün təşkilati evdir. ISOC, rəsmi İnternet Protokol Standartlarını və RFC-2196 Sayt Təhlükəsizliyi Təlimatını ehtiva edən Şərhlər üçün İstəkləri (RFC) qəbul edir.

Məlumat Təhlükəsizliyi Forumu (ISF) maliyyə xidmətləri, istehsal, telekommunikasiya, istehlak malları, hökumət və digər sahələrdə bir neçə yüz aparıcı təşkilatın qlobal qeyri-kommersiya təşkilatıdır. İnformasiya təhlükəsizliyi təcrübələri üzərində araşdırma aparır və illik iki illik Təcrübə Standartında və üzvlər üçün daha ətraflı tövsiyələr təklif edir.

İnformasiya Təhlükəsizliyi Peşəkarları İnstitutu (IISP), əsas məqsədi, informasiya təhlükəsizliyi üzrə mütəxəssislərin peşəkarlığını və bununla da bütövlükdə bu sahənin peşəkarlığını inkişaf etdirmək məqsədi ilə, üzvləri tərəfindən idarə olunan müstəqil, qeyri-kommersiya təşkilatıdır. İnstitut IISP Bacarıqları Çərçivəsini inkişaf etdirdi. Bu çərçivə, öz rollarının effektiv yerinə yetirilməsində informasiya təhlükəsizliyi və məlumat təminatı mütəxəssislərindən gözlənilən bir sıra səlahiyyətləri təsvir edir. Həm özəl, həm də dövlət sektoru təşkilatları və dünyaca məşhur alimlər və təhlükəsizlik liderləri arasında əməkdaşlıq yolu ilə hazırlanmışdır.

Almaniyanın Təhlükəsizlik Təhlükəsizliyi Federal İdarəsi (Alman Bundesamt für Sicherheit in Məlumat İnformasiya Texnologiyaları (BSI) -də) 100-1-100-4 BSI-Standartları "məlumat təhlükəsizliyinə aid metodlar, proseslər, prosedurlar, yanaşmalar və tədbirlər" daxil olmaqla bir sıra tövsiyələrdir. ". [86] BSI-Standard 100-2 IT-Grundschutz Metodologiyası, informasiya təhlükəsizliyi idarəetməsinin necə

qurulacağını və işlənməsini izah edir. Standart çox spesifik bir bələdçini, İT Əsas Qoruma Kataloqlarını (İT-Grundschutz Kataloqları kimi də tanınır) əhatə edir. 2005-ci ilə qədər əvvəllər kataloqlar əvvəllər "İT Əsas Qoruma Təlimatı" kimi tanınırdı. Kataloqlar İT mühitində təhlükəsizliklə əlaqəli zəif nöqtələri aşkar etmək və onlarla mübarizə aparmaq üçün faydalı sənədlər toplusudur. Kolleksiya, sentyabr 2013-cü il tarixinə giriş və kataloqlarla birlikdə 4,400 səhifəni əhatə edir. IT-Grundschutz yanaşması ISO / IEC 2700x ailəsinə uyğundur.

Avropa Telekommunikasiya Standartları İnstitutu Sənaye Xüsusiyyətləri Qrupunun (ISG) ISI başçılıq etdiyi informasiya təhlükəsizliyi göstəricilərinin bir siyahısını standartlaşdırdı.

2.8 Telekommunikasiya sistemlərinin ötürmə qabiliyyəti

İkitərəfli telekommunikasiya şəbəkələri vasitəsi ilə dünya miqyasında məlumat mübadiləsi üçün effektiv gücü 1986-cı ildə 281 petabayt (optimal sıxılmış) məlumatdan 1993-cü ildə 471 petabitə, 2000-ci ildə 2,2 (optimal sıxılmış) eksabayta və 2007-ci ildə 65 ekzabitə (optimal şəkildə sıxılmış halda) qədər artdı. Bu, 1986-cı ildə gündə adambaşına iki qəzet səhifəsinin, 2007-ci ilə qədər hər adam başına altı qəzetin məlumat ekvivalentidir. Bu böyüməni nəzərə alaraq, telekommunikasiya dünya iqtisadiyyatında getdikcə əhəmiyyətli rol oynayır və qlobal telekommunikasiya sənayesi 2012-ci ildə təxminən 4,7 trilyon dollara yaxın bir sektor təşkil etdi. Qlobal telekommunikasiya sənayesinin xidmət gəlirləri 2010-cu ildə dünyanın ümumi daxili məhsulunun (ÜDM) 2,4% -ə uyğun olaraq 1,5 trilyon dollar olduğu təxmin edildi.

FƏSİL 3. KOMMUNİKASİYA SİSTEMLƏRİNİN TƏHLÜKƏSİZLİYİNİN TƏMİN EDİLMƏSİNDƏ ƏSAS ASPEKTLƏR

3.1 Təhlükəsizlik anlayışı

Təhlükəsizlik başqalarının yaratdığı potensial zərərdən (və ya digər istənməyən məcburi dəyişikliklərdən) azadlıq və ya müqavimətdir. Təhlükəsizlikdən faydalananlar

(texniki istinadlar) insanlar və sosial qruplar, obyektlər və təşkilatlar, ekosistemlər və ya arzuolunmaz dəyişikliyə həssas olan hər hansı digər qurum və ya fenomen ola bilər.

Təhlükəsizlik əsasən düşmən qüvvələrdən qorunmağa aiddir, lakin digər hisslərin geniş dairəsinə malikdir: məsələn, zərərin olmaması kimi (məsələn, istəkdən azadlıq); vacib bir malın olması (məsələn, ərzaq təhlükəsizliyi); potensial zərər və ya zərərə qarşı müqavimət kimi (məsələn, etibarlı təməllər); məxfilik kimi (məsələn, etibarlı telefon xətti); ehtiyat kimi (məsələn, təhlükəsiz otaq və ya hücrə); və ruhi vəziyyət kimi (məsələn, emosional təhlükəsizlik).

Termin kimi təhlükəsizlik anlayışı onu təmin etmək məqsədi güdən akt və sistemləri (məsələn, təhlükəsizlik qüvvələri; təhlükəsizlik xidməti; kiber təhlükəsizlik sistemləri; təhlükəsizlik kameraları uzaq mühafizə) də öz əhatəsinə götürür.

Təhlükəsizliyin təmin edilməsi proseslərinin üç müxtəlif və vacib səviyyələrini bir-birindən fərqləndirmək olar.

1. Siyasi səviyyədə təhlükəsizliyin təmin edilməsi
2. Fiziki səviyyədə təhlükəsizliyin təmin edilməsi
3. İnformasiya texnologiyaları səviyyəsində təhlükəsizliyin təmin edilməsi

Siyasi səviyyədə təhlükəsizliyin təmin edilməsi milli təhlükəsizlik, ictimai təhlükəsizlik, vətəni qoruma təhlükəsizliyi, ölkədaxili təhlükəsizlik, beynəlxalq təhlükəsizlik, insan təhlükəsizliyi və başqa bu kimi dövlət səviyyəli təhlükəsizlik amillərini özündə ehtiva edir.

Fiziki səviyyədə təşkil olunan təhlükəsizlik tədbirlərinə aşağıdakıları misal göstərmək olar. Məsələn: hava limanındakı təhlükəsizlik tədbirləri, korporativ təhlükəsizlik tədbirləri, qida təhlükəsizliyi, ətraf-mühit təhlükəsizliyi, şəxsi əmlak təhlükəsizliyi, infrastruktur təhlükəsizliyi, fiziki avadanlıqların təhlükəsizliyi və sairə.

XXI əsr informasiya və texnologiya əsri olduğundan son dövrlərdə əsas diqqət yuxarıda adlarını çəkdiyimiz siyasi və fiziki səviyyədə təhlükəsizliyin təmin

edilməsindən daha çox məhz informasiya texnologiyaları səviyyəsində təhlükəsizliyin təmin edilməsi prinsiplərinə yönəldilmişdir. Bunun da nəticəsi olaraq bu sahədə təhlükəsizlik tədbirlərinin görülməsi çeşidləri son onilliklərdə kifayət qədər artmışdır. Kommunikasiya təhlükəsizliyi, kompüter təhlükəsizliyi, internet təhlükəsizliyi, tətbiqetmə proqramları və proqram təminatı təhlükəsizliyi, informasiya təhlükəsizliyi, rəqəmsal təhlükəsizlik, şəbəkə təhlükəsizliyi kimi günümüzdə çox vacib və actual rol oynayan bu təhlükəsizlik prinsipləri sırf informasiya texnologiyaları səviyyəsində təşkil olunan təhlükəsizlik tədbirləri siyahısın yalnızca bir hissəsidir.

Digər təhlükəsizlik prinsipləri də günümüz üçün kifayət qədər əsas rol oynasa da, mən mövzu ilə əlaqədar olaraq əsas etibarilə məhz informasiya təhlükəsizliyi prinsiplərinin həyata keçirilməsinin üzərində dayanacağam.

3.2 İnformasiya təhlükəsizliyi

İnformasiya təhlükəsizliyi, məlumat risklərini azaltmaqla məlumatın qorunması praktikasıdır. Məlumat risklərinin idarə edilməsinin bir hissəsidir. Bu, adətən icazəsiz / yersiz giriş, istifadə, açıqlama, kəsilmə, silinmə / məhv, korrupsiya, dəyişiklik, yoxlama, qeyd və ya devalvasiya ehtimalının qarşısını almaq və ya ən azı azaltmağı əhatə edir. hadisələrin mənfi təsirlərinin azaldılması halları da bura daxildir. Məlumat istənilən formada ola bilər, məs. elektron və ya fiziki. Yaxud da maddi (məsələn, sənəd işi) və ya qeyri-maddi (məsələn, bilik). İnformasiya təhlükəsizliyinin əsas istiqaməti təşkilatın məhsuldarlığını əngəlləmədən səmərəli siyasətin həyata keçirilməsinə diqqət yetirməklə məlumatların məxfiliyinin, bütövlüyünün və mövcudluğunun balanslı qorunmasıdır. Buna əsasən aşağıdakıları əhatə edən strukturlaşdırılmış risk idarəetmə prosesi vasitəsilə nail olunur.

- Məlumat və əlaqəli aktivlərin, həmçinin potensial təhdidlərin, zəifliklərin və təsirlərin müəyyən edilməsi;
- Risklərin qiymətləndirilməsi;

- Risklərin qarşısının alınması, azaldılması, bölüşülməsi və ya qəbul edilməməsi üçün risklərin necə həll ediləcəyi və ya necə müalicə ediləcəyi barədə qərar vermək;
- Risklərin azaldılması tələb olunduğu təqdirdə, müvafiq təhlükəsizlik idarəetmələrini seçmək və ya hazırlamaq və tətbiq etmək;
- Fəaliyyətləri izləmək, hər hansı bir problemi, dəyişiklikləri və inkişaf imkanlarını həll etmək üçün lazımi düzəlişlər etmək.

Bu intizamı standartlaşdırmaq üçün alimlər və mütəxəssislər parol, antivirus proqram təminatı, firewall, şifrələmə proqramı, hüquqi məsuliyyət, təhlükəsizlik şüuru və təlim və sairə kimi qabaqlayıcı tədbirlərin həyata keçirilməsini məsləhət görürlər. Bu standartlaşdırma, məlumatların əldə edilməsinə, işlənməsinə, saxlanmasına, ötürülməsinə və məhv edilməsinə təsir edən müxtəlif qanunlar və qaydalar tərəfindən irəli sürülə bilər. Bununla birlikdə, hər hansı bir standartın və rəhbərliyin müəssisə daxilində tətbiqi davamlı inkişaf mədəniyyəti qəbul edilmədiyi təqdirdə məhdud təsir göstərməsi hallarının da baş verməsi mümkündür.

İnformasiya təhlükəsizliyinin əsasını məlumat təminatı, məlumatın məxfiliyini, bütövlüyünü və mövcudluğunu (CİA) qorumaq, kritik problemlər yarandıqda məlumatın heç bir şəkildə pozulmamasını təmin edən aktdır. Bu məsələlərə təbii fəlakətlər, kompüter / server nasazlığı və fiziki oğurluq daxildir. Kağıza əsaslanan iş əməliyyatları hələ də yayılsa da, özünün informasiya təhlükəsizliyi praktikasını tələb edir, müəssisənin rəqəmsal təşəbbüsləri getdikcə daha çox vurğulanır və bunun nəticəsi olaraq da indi informasiya texnologiyaları (İT) təhlükəsizlik mütəxəssisləri tərəfindən həyata keçirilir. Bu mütəxəssislər informasiya təhlükəsizliyini texnologiyaya tətbiq edirlər (əksər hallarda kompüter sisteminin hansısa bir forması). Bir kompüterin mütləq bir ev masası demək olmadığını qeyd etmək lazımdır. Kompüter bir prosessoru və bəzi yaddaşı olan hər hansı bir cihazdır. Bu cür qurğular şəbəkə olmayan müstəqil qurğulardan kalkulyator kimi sadə, ağıllı telefon və planşet kompüterləri kimi şəbəkəli

mobil hesablama cihazlarına qədər ola bilər. İT təhlükəsizlik mütəxəssisləri demək olar ki, həmişə daha böyük müəssisələrdəki məlumatların xarakteri və dəyəri səbəbindən hər hansı bir böyük müəssisə / müəssisədə tapılır. Onlar şirkətdəki bütün texnologiyaları tez-tez tənqidi şəxsi məlumat əldə etməyə və ya daxili sistemlərə nəzarəti əldə etməyə çalışan zərərli kiberhücumlardan etibarlı şəkildə qorunmaq üçün məsuliyyət daşıyırlar.

İnformasiya təhlükəsizliyi sahəsi son illərdə əhəmiyyətli dərəcədə böyüdü və inkişaf etdi. Şəbəkə və müttəfiq infrastrukturun etibarlılığı, tətbiqetmələrin və məlumat bazalarının təmin edilməsi, təhlükəsizlik testi, məlumat sistemlərinin auditi, işin davamlılığının planlaşdırılması, elektron qeydlərin aşkarlanması və rəqəmsal məhkəmə ekspertizası da daxil olmaqla ixtisaslaşma üçün bir çox sahə təklif edir.

3.3 İnformasiya təhlükəsizliyinin qısa tarixi

Rabitə quruluşunun ilk günlərindən etibarən diplomatlar və hərbi komandirlər yazışmaların məxfiliyini qorumaq üçün müəyyən bir mexanizm təmin etməyi və pozğunluqları aşkarlamaq üçün bəzi vasitələrin olmasının lazım olduğunu başa düşdülər. Bu məqsədlə ilk dəfə eramızdan əvvəl 50-ci ildə Julius Sezar, Sezar şifrələnməsi vasitəsilə informasiya təhlükəsizliyinin, başqa sözlə desək, günümüzdəki kriptoqrafiyanın əsasını qoydu. Daha sonra isə, əksər hallarda prosedur idarəetmə vasitələrinin tətbiqi ilə qorunma təmin edildi. Həssas məlumatlar, etibarlı şəxslər tərəfindən qorunmalı və daşınmalı, qorunan və etibarlı bir mühitdə və ya güclü bir qutuda saxlanılmalı olduğuna işarə edildi. Poçt xidmətləri genişləndikcə hökumətlər məktubları tutmaq, deşifrə etmək, oxumaq və yenidən satmaq üçün rəsmi təşkilatlar yaratdılar.

XIX əsrin ortalarında hökumətlərə həssaslıq dərəcəsinə görə məlumatlarını idarə etməyə imkan verən daha mürəkkəb təsnifat sistemləri hazırlanmışdır. Məsələn, İngiltərə hökuməti bunu müəyyən dərəcədə 1889-cu ildə rəsmi sirlər qanununun dərc edilməsi ilə kodlaşdırdı. Birinci Dünya Müharibəsi illərində, müxtəlif cəbhələrə və

oradan məlumat ötürmək üçün çox səviyyəli təsnifat sistemlərindən istifadə olunurdu ki, bu da diplomatik və hərbi qərargahlarda kodların hazırlanması və bölmələrin daha çox istifadəsini təşviq edirdi. Kodlar müharibələr arasında daha mürəkkəb hala gəldi, çünki məlumatları dolandırmaq və səhv etmək üçün maşınlar işə salındı. Müttəfiq ölkələrin İkinci Dünya Müharibəsi dövründə paylaşdığı məlumatların həcmi təsnifat sistemlərinin və prosedur nəzarətlərinin rəsmi şəkildə uyğunlaşdırılmasını zəruri etdi. Sənədləri kimin idarə edə biləcəyini (adətən çağırılmış qoşunların əvəzinə zabitlərin) və harada getdikcə daha mürəkkəb seyflərin və anbar yerlərinin inkişaf etdirildiyi üçün harada saxlamağın lazım olduğunu göstərmək üçün işarələnmiş bir nişan aralığı meydana gəldi. Almanların müharibə məlumatlarını şifrələməsi üçün istifadə etdiyi və Alan Turing tərəfindən müvəffəqiyyətlə şəkildə şifrələnmiş Enigma Maşın, təmin edilmiş məlumatların yaradılmasının və istifadəsinin parlaq nümunəsi kimi qəbul edilə bilər. Sənədlərin düzgün şəkildə məhv edilməsini təmin etmək üçün prosedurlar inkişaf etdi və bu prosedurlara əməl edilməməsi müharibənin ən böyük kəşfiyyat zərbələrinə səbəb oldu.

XX əsrin sonu və iyirmi birinci əsrin ilk illərində telekommunikasiya, hesablama aparatı və proqram təminatı və məlumat şifrələməsi sahəsində sürətli inkişaf müşahidə olundu. Kiçik, daha güclü və daha az bahalı hesablama texnikasının olması kiçik biznes və ev istifadəçisinin əli ilə elektron məlumatları emal etməyə imkan verdi.

İnternet vasitəsilə aparılan elektron məlumatların emalı və elektron işlərin sürətli böyüməsi və geniş yayılması, beynəlxalq terrorizmin çoxsaylı hadisələri ilə yanaşı, kompüterlərin və onların saxladıqları, emal etdikləri və ötürdükləri məlumatların qorunmasının daha yaxşı üsullarına ehtiyac yaratdı. Kompüter təhlükəsizliyi və məlumat təminatı ilə əlaqəli akademik fənlər çoxsaylı peşəkar təşkilatlarla birlikdə ortaya çıxdı, hamısı informasiya sistemlərinin təhlükəsizliyini və etibarlılığını təmin etmək üçün ortaq məqsədləri bölüşdülər.

3.4 İnformasiya təhlükəsizliyinə müxtəlif yanaşmalar

Yaşadığımız informasiya əsrində informasiya saxlanmasına və ya mübadiləsinə yönəlmiş hücumlar çoxsaylı çeşidliyinə görə fərqləndiyindən mütəxəssislər tərəfindən informasiya təhlükəsizliyi amili birmənalı olaraq qəbul edilmir. Nəticədə informasiya təhlükəsizliyi anlayışına fərqli yanaşmalar mövcuddur. Həmin yanaşmalardan bəziləri aşağıdakılardır:

- Məlumatların məxfiliyinin, bütövlüyünün və əlçatanlığının qorunması. Qeyd: Bundan əlavə, orijinallıq, hesabatlılıq, rədd etmə və etibarlılıq kimi digər xüsusiyyətlər də cəlb edilə bilər.
- Məlumat və məlumat sistemlərinin məxfiliyini, bütövlüyünü və mövcudluğunu təmin etmək üçün icazəsiz giriş, istifadə, açıqlama, pozulma, dəyişdirmə və ya məhv olmaqdan qorunması.
- Yalnız səlahiyyətli istifadəçilərin (məxfiliyin) zəruri olduqda dəqiqliyi və tam məlumatı (bütövlüyü) əldə etməsininin təmin edilməsi (mövcudluğu).
- İnformasiya Təhlükəsizliyi bir təşkilatın əqli mülkiyyətini qorumaqdır.
- informasiya təhlükəsizliyi, iş üçün məlumat riskinin dəyərini idarə etmək olan bir risk idarəetmə intizamıdır.
- İnformasiya riskləri və nəzarətlərinin balansda olmasına dair yaxşı məlumatlı bir əminlik hissi.
- İnformasiya təhlükəsizliyi məlumatın qorunmasıdır və məlumatı icazəsiz tərəflərə yayma riskini minimuma endirir.
- Telekommunikasiya sistemindən və ya cihazlarından istifadə etməklə informasiya və informasiya ehtiyatının təhlükəsizliyi məlumat, informasiya sistemləri və ya kitabları icazəsiz giriş, ziyan, oğurluq və ya məhv olmaqdan qorumaq deməkdir.

İstənilən halda informasiya təhlükəsizliyi anlayışının tərifini əksər mütəxəssislər tərəfindən qəbul olunan aşağıdakı kimi vahid formada ümumiləşdirmək olar.

İnformasiya Təhlükəsizliyi, məlumatların bütün yerlərdə (daxilində və xaricində) saxlanması üçün mövcud olan bütün növ (texniki, təşkilati, insan yönümlü və qanuni) təhlükəsizlik mexanizmlərinin inkişafı və tətbiqi ilə əlaqəli bir çox istiqamətli təhsil və peşə sahəsidir. təşkilatın perimetri) və nəticədə məlumatların yaradıldığı, işləndiyi, saxlanıldığı, ötürüldüyü və məhv edildiyi, təhdidlərdən azad olduğu məlumat sistemləri. İnformasiya və informasiya sistemlərinə olan təhlükələr təsnif edilə bilər və təhdidlərin hər bir kateqoriyası üçün müvafiq təhlükəsizlik məqsədi müəyyən edilə bilər. . Təhlükənin təhlili nəticəsində müəyyən edilmiş təhlükəsizlik məqsədləri dəsti, adekvatlığını və inkişaf edən mühitə uyğunluğunu təmin etmək üçün vaxtaşırı yenidən nəzərdən keçirilməlidir. Hal-hazırda müvafiq təhlükəsizlik hədəflərinə aşağıdakılar aid edilə bilər: məxfilik, bütövlük, mövcudluq, məxfilik, orijinallıq və etibarlılıq, rədd etmə, hesabatlılıq və audit.

3.5 İnformasiya təhlükəsizliyinin təmin olunmasına səbəb olan təhdidlər

İnformasiya təhlükəsizliyinə təhdidlər müxtəlif formalarda olur. Bu gün ən çox görülən təhdidlərdən bəziləri proqram hücumları, intellektual mülkiyyət oğurluğu, şəxsiyyət oğurluğu, avadanlıq və ya məlumat oğurluğu, təxribat və məlumat qəsbidir. Çoxu bir növ proqram hücumlarına məruz qalmışdır. Viruslar, qurdlar, fişlənmə hücumları və Trojan atları, proqram hücumlarının bir neçə ümumi nümunəsidir. İntellektual mülkiyyətin oğurlanması da informasiya texnologiyaları (İT) sahəsində bir çox müəssisə üçün geniş problem olmuşdur. Şəxsiyyət oğurluğu, adətən həmin şəxsin şəxsi məlumatlarını əldə etmək və ya sosial mühəndislik yolu ilə həyati əhəmiyyətli məlumatlardan istifadə etmək üçün başqası kimi davranmaqdır. Avadanlıqların və ya məlumatların oğurlanması bu gün əksər cihazların mobil olması səbəbindən geniş yayılmışdır, oğurluğa meyllidir və məlumat tutumunun həcmi artdıqca daha arzuolunmaz hala gəlmişdir. Sabotaj, bir qayda olaraq, müştərilərin etimadını itirməyə çalışan bir təşkilatın veb saytının məhv edilməsindən ibarətdir. Məlumat qəsb etməsi, şirkətin əmlakının və ya məlumatlarının oğurlanmasından ibarətdir ki, dolayı dillə

şantaj ilə olduğu kimi, məlumatı və ya əmlakı sahibinə geri qaytarması müqabilində ödəniş almaq cəhdi kimi. Bu hücumların bəzilərindən özünüzü qorumağa kömək edəcək bir çox yol var, lakin ən funksional tədbirlərdən biri istifadəçinin vaxtaşırı məlumatlandırılmasıdır. Hər hansı bir təşkilat üçün bir nömrəli təhdid istifadəçilər və ya daxili işçilərdir, onlara daxili təhdidlər də deyilir.

Hökumətlər, hərbi qurumlar, maliyyə qurumları, xəstəxanalar, qeyri-kommersiya təşkilatları və özəl müəssisələr işçiləri, müştəriləri, məhsulları, araşdırmaları və maliyyə vəziyyəti haqqında çoxlu məxfi məlumatlar toplayırlar. Bir işin müştəriləri və ya maliyyəsi və ya yeni məhsul xətti haqqında məxfi məlumatlar bir rəqibin və ya qara şapka hakerinin əlinə düşərsə, bir iş və onun müştəriləri geniş yayılmış, düzəlməz maliyyə itkisi ilə yanaşı şirkətin nüfuzuna xələl gətirə bilər. Bir iş baxımından, informasiya təhlükəsizliyi xərclərə qarşı balanslaşdırılmış olmalıdır; Gordon-Loeb Model bu problemi həll etmək üçün riyazi iqtisadi yanaşma təmin edir. Şəxs üçün məlumat təhlükəsizliyi, müxtəlif mədəniyyətlərdə çox fərqli baxılan məxfiliyə əhəmiyyətli təsir göstərir.

3.6 Təhdidlərin qarşısının alınması tədbirləri

Təhlükəsizlik təhdidi və ya riski ilə mümkün cavablar aşağıdakılardır.

- həssaslığı aradan qaldırmaq və ya təhdidləri qarşısını almaq üçün təhlükəsizlik tədbirləri və əks tədbirləri həyata keçirmək
- təhdidin dəyərini sığorta və ya autsorsinq almaq kimi başqa bir müəssisə və ya təşkilatın üzərinə qoymaq
- əks tədbirin dəyəri təhlükə səbəbindən mümkün itki dəyərindən yüksək olub olmadığını qiymətləndirmək

3.7 İnformasiya təhlükəsizliyinin əsas prinsipləri (CİA üçbucağı)

CIA məxfilik, bütövlük və əlçatanlıq üçlüyü informasiya təhlükəsizliyinin mərkəzində dayanır. (Klassik InfoSec üçlüyünün üzvləri - məxfilik, bütövlük və mövcudluq - ədəbiyyatda təhlükəsizlik atributları, xassələri, təhlükəsizlik məqsədləri,

fundamental aspektlər, məlumat meyarları, kritik məlumat xüsusiyyətləri və əsas bina blokları olaraq bir-birinə istinad olunur.) Bununla belə, mübahisələr davam edir CIA-nin bu üçlüyünün sürətlə dəyişən texnologiya və iş tələblərini həll etmək üçün yetərli olub olmaması ilə əlaqədar mövcudluq və məxfilik arasındakı kəsişmələrdə genişlənmənin, habelə təhlükəsizlik və məxfilik arasındakı əlaqələrin genişləndirilməsini nəzərdən keçirmək üçün tövsiyələr verilir. Bəzən "hesabatlılıq" kimi digər prinsiplər təklif edilmişdir; rədd edilməməsi kimi məsələlərin üç əsas konsepsiya içərisində uyğun olmadığına işarə edildi.

Məxfilik (confidentiality – CİA-nın birinci bucağı) - İnformasiya təhlükəsizliyində məxfilik "məlumat, icazəsiz şəxslərə, təşkilatlara və ya proseslərə təqdim edilməməsi və ya açıqlanmamasıdır." Əksinə, məxfilik məlumatlarımızı icazəsiz izləyicilərdən qorumaq üçün tətbiq olunan məxfilik hissəsidir. Elektron məlumatların məxfiliyinə misal olaraq, laptop oğurluğu, parol oğurluğu və ya səhv şəxslərə göndərilən həssas elektron poçtlar daxildir.

Bütövlük (İntegrity – CİA-nın ikinci bucağı) - Məlumat təhlükəsizliyində, məlumatın bütövlüyü, bütün ömrü boyu məlumatların düzgünlüyünü və tamlığını qorumaq və təmin etmək deməkdir. Bu, məlumatların icazəsiz və ya təyin olunmamış bir şəkildə dəyişdirilə bilməyəcəyi deməkdir. Bu verilənlər bazasında istinad bütövlüyü ilə eyni deyil, buna baxmayaraq əməliyyatın emalının klassik ACID modelində başa düşüldüyü kimi xüsusi bir tutarlılıq hadisəsi kimi baxıla bilər. İnformasiya təhlükəsizlik sistemləri adətən məxfiliklə yanaşı mesaj bütövlüyünü təmin edir.

Əlçatanlıq (Avialability – CİA-nın üçüncü bucağı) - Hər hansı bir informasiya sisteminin məqsədinə xidmət etməsi üçün məlumat lazım olduqda mövcud olmalıdır. Bu, məlumatın saxlanması və işlənməsi üçün istifadə olunan hesablama sistemlərinin, qorunması üçün istifadə olunan təhlükəsizlik nəzarət vasitələrinin və daxil olmaq üçün istifadə olunan rabitə kanallarının düzgün işləməsi deməkdir. Yüksək mövcudluq sistemləri elektrik enerjisinin kəsilməsi, aparat çatışmazlığı və sistem yeniləmələri

səbəbindən xidmətdə kəsilmələrin qarşısını alaraq hər zaman mövcud olmağı hədəfləyir. Mövcudluğu təmin etmək, hədəf sisteminə gələn mesajların seli kimi əsassız olaraq onu bağlamağa məcbur etmək kimi xidmətdən yayınma hücumlarının qarşısını alır.

İnformasiya təhlükəsizliyi sahəsində mövcudluğa bir çox hallarda uğurlu bir informasiya təhlükəsizliyi proqramının ən vacib hissələrindən biri kimi baxmaq olar. Nəticədə son istifadəçilərin iş funksiyalarını yerinə yetirə bilmələri lazımdır; mövcudluğu təmin etməklə bir təşkilatın bir təşkilatın maraqlı tərəflərinin gözlədiyi standartları yerinə yetirə bilməsi. Buraya proxy konfiqurasiyaları, xaricdən veb girişi, ortaq sürücülərə giriş imkanı və e-poçt göndərmə imkanı kimi mövzular daxil ola bilər. Çox vaxt icra məmurları informasiya təhlükəsizliyinin texniki tərəflərini başa düşmürlər və mövcudluğa asan bir düzəliş kimi baxırlar, lakin bu, çox vaxt şəbəkə əməliyyatları, inkişaf əməliyyatları, insidentlərə reaksiya və siyasət / dəyişikliklərin idarə olunması kimi bir çox təşkilati qrupun əməkdaşlığını tələb edir. Uğurlu bir informasiya təhlükəsizliyi qrupu, CIA üçlüyünün effektiv şəkildə təmin edilməsi üçün düzəldilməsi və uyğunlaşdırılması üçün bir çox fərqli rolu özündə cəmləşdirir.

Təxirə salınmazlıq (Non-repudiation) - Qanunvericilikdə rədd edilməməsi, birinin müqavilə üzərindəki öhdəliklərini yerinə yetirmək niyyətini ifadə edir. Bu da bir əməliyyatın bir tərəfinin bir əməliyyatın alınmasını inkar edə bilməyəcəyini və digər tərəfin bir əməliyyatın göndərilməsini inkar edə bilməməsini nəzərdə tutur.

Qeyd etmək vacibdir ki, kriptoqrafik sistemlər kimi texnologiya rədd etmə səylərinə kömək edə bilsə də, konsepsiya əsas məqamda texnologiya aləmini aşan bir qanun konsepsiyasındadır. Məsələn, mesajın göndəricinin şəxsi açarı ilə imzalanmış bir rəqəmsal imza ilə uyğun olduğunu göstərmək kifayət deyil və beləliklə yalnız göndərən mesajı göndərə bilərdi və heç kəs onu ötürmə (məlumat bütövlüyü) ilə dəyişdirə bilməzdi. İddia edilən göndərici bunun qarşılığında rəqəmsal imza alqoritminin həssas və ya qüsurlu olduğunu nümayiş etdirə bilər, ya da imza açarının pozulduğunu iddia

edə və ya sübut edə bilər. Bu pozuntulara görə günah göndəricinin üzərinə düşə bilər və ya olmaya bilər və bu cür təsdiqlər göndəricini məsuliyyətdən azad edə bilər və ya azad edə bilməz, lakin iddia imzanın mütləq həqiqiliyini və bütövlüyünü sübut etməsi iddiasını yalnışdır. Belə olduqda, göndərən mesajı rədd edə bilər (çünki orijinallığı və bütövlüyü rədd edilməməsi üçün vacib şərtdir).

3.8 İnformasiya təhlükəsizliyi zamanı risklərin idarə edilməsi

Sertifikatlaşdırılmış İnformasiya Sistemləri Auditoru (CISA) Təlimatı 2006, risk menecmentinin aşağıdakı tərifini təqdim edir. Bura adları çəkilən proseslər aiddir: "Risklərin idarə edilməsi, bir təşkilatın iş məqsədlərinə çatmasında istifadə etdiyi məlumat mənbələrinə olan həssaslıqların və təhdidlərin müəyyən edilməsi və qarşısıalınmaz tədbirlərin görülməsi prosesidir. , təşkilat üçün məlumat qaynağının dəyərinə əsaslanaraq riskin məqbul səviyyəyə endirilməsini həyata keçirmək."

Bu tərifdə bəzi dəqiqləşdirməyə ehtiyac ola biləcək iki şey var. Birincisi, risklərin idarə edilməsi prosesi davamlı, təkrarlanan bir prosesdir. Qeyri-müəyyən təkrarlanmalıdır. İş mühiti daim dəyişir və hər gün yeni təhlükələr və həssaslıqlar yaranır. İkincisi, riskləri idarə etmək üçün istifadə olunan əks tədbirlərin (nəzarət vasitələrinin) seçimi məhsuldarlıq, maya dəyəri, əks tədbirin effektivliyi və qorunan informasiya aktivinin dəyəri arasında balans yaratmalıdır.

Risklərin təhlili və risklərin qiymətləndirilməsi proseslərində məhdudiyyətlər mövcuddur, çünki təhlükəsizlik hadisələri baş verdikdə onlar bir kontekstdə meydana çıxır və nadir və unikallığı gözlənilməz təhdidlərə səbəb olur. Böhranlar, sürprizlər və yan təsirləri ilə xarakterizə olunan bu hadisələrin təhlili, hər hadisənin təfərrüatlarını subyektiv olaraq araşdırıb şərh edə bilən nəzəri bir yanaşma tələb edir.

Risk, məlumatverici aktivə (və ya aktivin itirilməsinə) ziyan vuran pis bir şeyin baş vermə ehtimalı. Zəiflik dedikdə məlumat verən bir şəxsə zərər verə və ya zərər verə biləcək bir amil nəzərdə tutulur. Təhdid, zərər verə biləcək bir şeydir (texnoloji və ya təbiət hərəkəti).

Təhdidin zəifliyə zərər vurmaq üçün istifadə etmə ehtimalı risk yaradır. Təhdid zərər vermək üçün bir həssaslıqdan istifadə edərsə, təsiri olur. İnformasiya təhlükəsizliyi kontekstində təsir mövcudluğun, bütövlüyün və məxfiliyin itirilməsi və bəlkə də digər itkilərdir (itirilmiş gəlir, həyat itkisi, daşınmaz əmlak itkisi). Bütün riskləri müəyyən etmək mümkün deyil və bütün riski aradan qaldırmaq da mümkün deyil. Qalan riskə "qalıq risk" deyilir.

Risk qiymətləndirməsi işin müəyyən sahələri haqqında məlumatı olan bir qrup tərəfindən həyata keçirilir. Komandanın üzvlüyü zaman keçdikcə dəyişə bilər, çünki işin müxtəlif hissələri qiymətləndirilir. Qiymətləndirmə, məlumatlı rəy əsasında subyektiv keyfiyyət analizindən istifadə edə bilər və ya etibarlı dollar rəqəmləri və tarixi məlumatlar olduqda təhlil kəmiyyət analizindən istifadə edə bilər.

Tədqiqatlar göstərir ki, əksər informasiya sistemlərində ən həssas məqam insan istifadəçisi, operator, dizayner və ya digər insan olur. İSO / IEC 27002: 2005 Məlumat təhlükəsizliyinin idarə olunması üçün Təcrübə Kodeksi risk qiymətləndirilməsi zamanı aşağıdakıların araşdırılmasını tövsiyə edir:

- təhlükəsizlik siyasəti
- informasiya təhlükəsizliyinin təşkili
- aktivlərin idarə olunması
- insan resurslarının təhlükəsizliyi
- fiziki və ekoloji təhlükəsizlik
- rabitə və əməliyyatların idarə edilməsi
- girişə nəzarət
- informasiya sistemlərinin alınması, inkişafı və texniki xidməti
- informasiya təhlükəsizliyi hadisələrinin idarə edilməsi
- iş davamlılığının idarə edilməsi
- tənzimləmə uyğunluğu.

Geniş mənada risklərin idarə edilməsi prosesi aşağıdakılardan ibarətdir:

1. Aktivlərin müəyyənləşdirilməsi və dəyərinin qiymətləndirilməsi. Daxildir: insanlar, binalar, hardware, proqram təminatı, məlumatlar (elektron, çap, digər), təchizat.
2. Təhdid qiymətləndirməsini aparılması. Daxildir: Təbiət aktları, müharibə aktları, qəzalar, təşkilat daxilində və ya xaricində meydana gələn zərərli hərəkətlər.
3. Bir həssaslıq qiymətləndirməsini aparılması və hər bir zəiflik üçün onun istifadəsi ehtimalını hesablanılması. Siyasətləri, prosedurları, standartları, təlim, fiziki təhlükəsizlik, keyfiyyətə nəzarət, texniki təhlükəsizliyi qiymətləndirilməsi.
4. Hər bir təhlükənin hər bir aktivə təsirini hesablayın. Keyfiyyətli analiz və ya kəmiyyət təhlili istifadə edilməsi
5. Müvafiq idarələri müəyyənləşdirin, seçin və tətbiq edin. Mütənasib cavab verin. Məhsuldarlığı, maya dəyəri və aktivin dəyərini nəzərdən keçirilməsi
6. Nəzarət tədbirlərinin səmərəliliyini qiymətləndirilməsi. Nəzarət tələb olunan məhsuldarlığı itirmədən tələb olunan maya dəyəri ilə qorunmasını təmin edilməsi

Hər hansı bir risk üçün rəhbərlik, aktivin nisbi aşağı dəyəri, meydana çıxma nisbi aşağı tezliyi və biznesə nisbətən aşağı təsirə əsaslanaraq riskin qəbul edilməsini seçə bilər. Və ya rəhbərlik riskin azaldılması üçün müvafiq nəzarət tədbirlərini seçərək həyata keçirərək riskin azaldılmasını seçə bilər. Bəzi hallarda risk sığorta almaq və ya başqa bir işə autsorsinq etməklə başqa bir işə ötürülə bilər. Bəzi risklərin reallığı mübahisələndirilə bilər. Belə hallarda rəhbərlik riskdən imtina etməyi seçə bilər.

3.9 İnformasiya təhlükəsizliyinin idarə edilməsi

Düzgün təhlükəsizlik nəzarətini seçmək və həyata keçirmək əvvəlcə bir təşkilata riskləri məqbul səviyyələrə endirməyə kömək edəcəkdir. Nəzarət seçimi riskin qiymətləndirilməsinə əsaslanmalı və onun əsasında müəyyənləşdirilməlidir. Nəzarətlər təbiətdə dəyişə bilər, lakin əsas etibarilə məlumatların məxfiliyini, bütövlüyünü və ya mövcudluğunu qorumaq informasiya təhlükəsizliyinin bir nömrəli qanunu hesab edilir. İSO / IEC 27001 müxtəlif sahələrdə nəzarət prinsiplərini təyin etmişdir. Təşkilatlar öz

tələbinə uyğun olaraq əlavə nəzarət funksiyaları tətbiq edə bilərlər. İstənilən halda, ISO / IEC 27002 vahid təşkilatı məlumat təhlükəsizliyi standartlarına dair bir təlimat təklif edir. Həmin təlimatın tərkib hissələri aşağıdakılardan ibarətdir:

İnzibati nəzarət. İnzibati nəzarət təsdiq edilmiş yazılı siyasət, prosedur, standart və təlimatlardan ibarətdir. İnzibati nəzarət biznesi idarə etmək və insanları idarə etmək üçün çərçivə təşkil edir. İnsanlara işin necə aparılacağı və gündəlik əməliyyatların necə aparılacağı barədə məlumat verirlər. Hökumət orqanları tərəfindən yaradılan qanun və qaydalar da müəssisəni məlumatlandırdıqları üçün inzibati nəzarət növüdür. Bəzi sənaye sektorlarında tətbiq edilməli olan siyasət, prosedur, standart və qaydalar var - Visa və MasterCard tərəfindən tələb olunan Ödəniş Kartı Sənayesi Məlumat Təhlükəsizliyi Standartı (PCI DSS) buna misaldır. İnzibati nəzarətin digər nümunələrinə korporativ təhlükəsizlik siyasəti, parol siyasəti, işə götürmə siyasəti və intizam qaydaları daxildir.

Ümumi halda desək, inzibati nəzarət məntiqi və fiziki nəzarətin seçilməsi və həyata keçirilməsi üçün əsas təşkil edir. Məntiqi və fiziki nəzarət çox vacib olan inzibati nəzarətin təzahürləridir.

Məntiqi nəzarət. Məntiqi nəzarət (texniki nəzarət də deyilir) məlumat və hesablama sistemlərinə girişi izləmək və idarə etmək üçün proqram və məlumatlardan istifadə edir. Şifrələr, şəbəkə və host əsaslı təhlükəsizlik duvarı, şəbəkə müdaxiləsini aşkaretmə sistemləri, girişə nəzarət siyahıları və məlumat şifrələməsi məntiqi nəzarət nümunələridir.

Tez-tez gözdən qaçırılan vacib bir məntiqi nəzarət, ən az imtiyaz prinsipidir ki, bu da fərdi, proqram və ya sistem prosesinə tapşırığı yerinə yetirmək üçün lazım olduğundan daha çox güzəşt verilməməsini tələb edir. Ən az imtiyaz prinsipinə əməl edilməməsinin açıq bir nümunəsi, e-poçtu oxumaq və internetdə gəzmək üçün istifadəçi Administrator olaraq Windows-a daxil olmaqdır. Bu prinsipin pozulması ayrı-ayrı şəxs zamanla əlavə giriş imtiyazları toplayanda da baş verə bilər. Bu, işçilərin iş vəzifələri

dəyişdikdə, işçilər yeni bir vəzifəyə yüksəldildikdə və ya işçilər başqa bir şöbəyə köçürüldükdə olur. Yeni vəzifələri ilə tələb olunan giriş imtiyazları, artıq ehtiyac duyulmayan və ya uyğun olmaya biləcək mövcud imtiyazlara tez-tez əlavə olunur.

Fiziki təhlükəsizlik. Fiziki nəzarət iş yerinin və hesablama qurğularının mühitini izləyir və idarə edir. Bu cür qurğulara giriş və daxil olmağı da nəzarət edir və qapılar, kilidlər, istilik və kondisioner, tüstü və yanğın həyəcan siqnalları, yanğın söndürmə sistemləri, kameralar, barrikadalar, çitlər, təhlükəsizlik işçiləri, kabel kilidləri və s. Şəbəkəni və iş yerini funksional sahələrə ayırmaq da fiziki nəzarət daxildir.

Tez-tez gözdən qaçırılan vacib bir fiziki nəzarət vəzifələrin ayrılmasıdır ki, bu da fərdin özü tərəfindən vacib bir işi yerinə yetirə bilməməsini təmin edir. Məsələn, kompensasiya tələbi ilə müraciət edən bir işçi ödəniş üçün icazə verə və ya çeki çap edə bilməməlidir. Bir tətbiq proqramçısı eyni zamanda server idarəçisi və ya verilənlər bazası administratoru olmamalıdır; bu rol və vəzifələr bir-birindən ayrılmalıdır.

Dərinlikdə müdafiə

İnformasiya təhlükəsizliyi, məlumatın ilkin yaradılmasından tutmuş sonuncu istifadəsinə qədər bütün ömrü boyu məlumatı qorumalıdır. Məlumat hərəkətdə və istirahət zamanı qorunmalıdır. Həyatı boyunca, məlumatlar bir çox fərqli məlumat emal sistemlərindən və ya bir məlumat emal sisteminin müxtəlif hissələrindən keçə bilər. Məlumat və informasiya sistemlərinin təhdid edilə biləcəyi bir çox fərqli yol var. Məlumatın ömrü boyunca tam qorunması üçün, məlumat emal sisteminin hər bir komponentinin öz mühafizə mexanizmləri olmalıdır. Təhlükəsizlik tədbirlərinin qurulması, üst-üstə qoyulması və üst-üstə düşməsi "dərin müdafiə" adlanır. Yalnızca ən zəif bağlantısı qədər güclü olan metal bir zəncirdən fərqli olaraq, dərin strategiya müdafiəsi, bir müdafiə tədbiri uğursuz olduğu təqdirdə, digər tədbirlər qorunmasını təmin etməyə davam edəcəkdir.

İnzibati nəzarət, məntiqi nəzarət və fiziki nəzarət haqqında bir az əvvəl yuxarıda məlumat verdik. Hər üç növ nəzarət birgə olaraq dərinlik strategiyasında bir müdafiə qurma əsasını yaratmaq üçün istifadə edilə bilər. Bu yanaşma ilə dərinlikdəki müdafiə üç fərqli təbəqə və ya birinin digərinin üstünə qoyulmuş təyyarə kimi konseptual hala gətirilə bilər. Dərinlik müdafiəsinin bu konseptual modelini bəzən üst-üstə qatlarla örtülmüş soğanı xatırlatdığına görə "soğan modeli" də adlandırırlar. Soğanın əsasını təşkil edən məlumatlar, soğanın sonrakı xarici təbəqəsi və şəbəkə təhlükəsizliyi, ev sahibliyi əsaslı təhlükəsizlik və tətbiqi təhlükəsizliyi olan bir soğan təbəqəsini meydana gətirdiyini düşünməklə dərinliyə dair əlavə məlumat əldə etmək olar. soğanın ən xarici təbəqələrini meydana gətirir. Hər iki perspektiv eyni dərəcədə etibarlıdır və hər biri dərin strategiyada yaxşı bir müdafiənin həyata keçirilməsinə dəyərli fikir verir.

3.10 İnformasiya təhlükəsizliyinin təsnifatı

İnformasiya təhlükəsizliyi və risklərin idarə edilməsinin vacib bir istiqaməti məlumatın dəyərini tanımaq və məlumat üçün müvafiq prosedurları və qorunma tələblərini müəyyən etməkdir. Bütün məlumatlar bərabər deyil və buna görə də bütün məlumatlar eyni dərəcədə qorunma tələb etmir. Bunun üçün təhlükəsizlik təsnifatı təyin edilməsi tələb olunur. Məlumat təsnifatında ilk addım yüksək rəhbərliyin üzvünün təsnif ediləcək xüsusi məlumatın sahibi kimi müəyyənləşdirilməsidir. Sonra, bir təsnifat siyasətinin inkişaf etdirilməsi vacib şərtlərdəndir. Siyasət fərqli təsnifat etiketlərini təsvir etməli, müəyyən bir etiket təyin ediləcək məlumatın meyarlarını müəyyənləşdirməli və hər bir təsnifat üçün tələb olunan təhlükəsizlik tədbirlərini sadalamalıdır.

Hansı təsnifat məlumatının təyin edilməsinə təsir edən bəzi amillər məlumatın təşkilat üçün nə qədər dəyərinə, məlumatın nə qədər köhnəldiyinə və ya köhnəlmiş olub-olmamasına aiddir. Qanunlar və digər tənzimləmə tələbləri də məlumatları təsnif edərkən vacib mülahizələrdir. İnformasiya Sistemlərinin Auditi və Nəzarət Birliyi (ISACA) və İnformasiya Təhlükəsizliyi üçün İş Modeli, təhlükəsizlik mütəxəssislərinin

təhlükəsizliyi sistem baxımından araşdırması, təhlükəsizliyin bütöv bir şəkildə idarə oluna biləcəyi bir mühit yaratması, həqiqi risklərin həll edilməsinə imkan yaradan bir vasitə kimi xidmət edir.

Seçilən və istifadə olunan informasiya təhlükəsizliyi təsnifatı etiketlərinin növü, təşkilatın xarakterindən asılı olacaqdır, nümunələr:

- İş sektorunda: İctimai, həssas, özəl, məxfi kimi etiketlər.
- Hökumət sektorunda: Təsnif edilməmiş, Qeyri-rəsmi, Qorunan, Məxfi, Gizli, Top Gizli və onların İngilis dilində olmayan ekvivalentləri kimi etiketlər.
- Sahələrarası birləşmələrdə, Ağ, Yaşıl, Kəhrəba və Qırmızıdan ibarət olan "İşıqfor" Protokolu.

Təşkilatdakı bütün işçilər, habelə iş ortaqları təsnifat sxemi üzrə təlim keçməli və hər təsnifat üçün tələb olunan təhlükəsizlik nəzarəti və istifadə qaydalarını başa düşməlidirlər. Təyin edilmiş müəyyən bir informasiya aktivinin təsnifatı məlumat üçün hələ təsnifatın uyğun olmasını və təsnifat tələb olunan təhlükəsizlik nəzarətinin mövcudluğunu və onların düzgün prosedurlarına əməl edilməsini təmin etmək üçün vaxtaşırı nəzərdən keçirilməlidir.

Giriş nəzarəti. Qorunan məlumatlara daxil olmaq, məlumat əldə etmək səlahiyyəti olan insanlar üçün məhdudlaşdırılmalıdır. Kompüter proqramları və bir çox hallarda məlumatı emal edən kompüterlər də icazə verilməlidir. Bunun üçün qorunan məlumatlara girişi idarə etmək üçün mexanizmlərin olmasını tələb edir. Giriş idarəetmə mexanizmlərinin incəliyi qorunan məlumatın dəyəri ilə paralel olmalıdır; məlumatların nə qədər həssas və ya dəyərli olduğu təqdirdə idarəetmə mexanizmlərinin daha güclü olması lazımdır. Giriş idarəetmə mexanizmlərinin qurulduğu təməl şəxsiyyət və identifikasiya ilə başlayır.

Giriş nəzarəti ümumiyyətlə üç mərhələdə nəzərdən keçirilir: identifikasiya, audentifikasiya və təsdiqləmə. İndi isə onların hər birini ayrılıqda nəzərdən keçirək.

İdentifikasiya (eyniləşdirmə). Şəxsiyyət kiminsə kim olduğunu və ya nəyinsə nə olduğunu təsdiq edir. Bir şəxs "Salam, mənim adım Con Doe" ifadəsi verərsə, kim olduqlarını iddia edirlər. Ancaq onların iddiası həqiqətə uyğun olmaya bilər. John Doe'nin qorunan məlumat əldə etməsinə icazə verilməzdən əvvəl John Doe olduğunu iddia edən şəxsin John Doe olduğunu təsdiqləmək lazımdır. Adətən iddia istifadəçi adı şəklindədir. Bu istifadəçi adını daxil etməklə "istifadəçi adının mənsub olduğum adamam" iddiasını edirsiniz.

Audentifikasiya (Mənsubluq, Doğrulama). Doğrulama şəxsiyyət iddiasının təsdiqlənməsi aktıdır. John Doe pul çıxarmaq üçün bir banka girəndə, bank kassasına şəxsiyyət iddiası olan John Doe olduğunu söyləyir. Bank kassiri foto şəxsiyyət sənədini görməyi xahiş edir, buna görə də kassaya sürücülük vəsiqəsini verir. Bank kassiri lisenziyanın John Doe'nin çap olunduğuna əmin olmaq üçün yoxlayır və lisenziyadakı fotoşəkili John Doe olduğunu iddia edən şəxsə qarşı müqayisə edir. Şəkil və ad şəxslə uyğun gəlirsə, kassir John Doe'nin iddia etdiyi adam olduğunu təsdiq etdi. Eynilə, düzgün şifrə daxil etməklə istifadəçi istifadəçi adının mənsub olduğu şəxs olduğunu sübut edir.Doğrulama üçün istifadə edilə bilən üç müxtəlif məlumat növü var:

- Bildiyiniz verilənlər: PİN, şifrə və ya ananın qız adı
- Sahibi olduğunuz əşyalar: sürücülük vəsiqəsi və ya maqnit oxuyucu kartlar
- Sizi bütün digər insanlardan fərqləndirən özəlliklərinizdir: barmaq izləri, səs izləri və retina (göz) taramaları daxil olmaqla biometrikdir.

Güclü identifikasiya birdən çox identifikasiya məlumatını (iki amil identifikasiya) təmin etməyi tələb edir. İstifadəçi adı, bu gün kompüter sistemlərində ən çox yayılmış şəxsiyyət formasıdır və parol autentifikasiyanın ən yaygın formasıdır. İstifadəçi adları və şifrələr öz məqsədlərinə xidmət etdi, lakin onlar getdikcə artıq uyğun olmayan təhlükəsizlik üsulları hesab olunurlar. İstifadəçi adları və şifrələr yavaş-yavaş dəyişdirilir və ya vaxta əsaslanan birdəfəlik parol alqoritmləri kimi daha mürəkkəb identifikasiya mexanizmləri də əlavə olunmaqla zənginləşdirillir.

Təsdiqləmə (İcazə). Bir şəxs, proqram və ya kompüter müvəffəqiyyətlə müəyyənləşdirildikdən və təsdiq edildikdən sonra hansı məlumat mənbələrinə daxil olmalarına icazə verildiyi və hansı hərəkətlərin yerinə yetirilməsinə icazə veriləcəyi müəyyənləşdirilməlidir (işə salmaq, görmək, yaratmaq, silmək və ya dəyişdirmək). Buna icazə deyilir. Məlumat və digər hesablama xidmətlərinə giriş icazəsi inzibati siyasət və prosedurlardan başlayır. Siyasətlər hansı məlumat və hesablama xidmətlərinə, kim tərəfindən və hansı şərtlərlə əldə edilə biləcəyini göstərir. Bundan sonra girişə nəzarət mexanizmləri bu siyasəti tətbiq etmək üçün konfiqurasiya olunur. Fərqli hesablama sistemləri müxtəlif növ giriş idarəetmə mexanizmləri ilə təchiz edilmişdir. Bəziləri hətta fərqli girişə nəzarət mexanizmlərinin seçimi təklif edə bilər. Sistem təklif etdiyi giriş nəzarəti mexanizmi, çıxışa nəzarət üçün üç yanaşmadan birinə əsaslanacaq və ya üç yanaşmanın birləşməsindən əldə edilə bilər.

Qeyri-ixtiyari yanaşma bütün giriş nəzarətini mərkəzləşdirilmiş bir idarə altında birləşdirir. Məlumat və digər mənbələrə çıxış, ümumiyyətlə, təşkilatdakı şəxslərin fəaliyyətinə (roluna) və ya şəxsin yerinə yetirəcəyi vəzifələrə əsaslanır. Diskresional yanaşma informasiya mənbəyinin yaradıcısına və ya sahibinə həmin mənbələrə girişi idarə etmək imkanı verir. Məcburi girişə nəzarət yanaşmasında, informasiya mənbəyinə verilən təhlükəsizlik təsnifatı əsasında giriş verilir və ya rədd edilir.

Bu gün istifadə edilən ümumi giriş nəzarəti mexanizmlərinə misal olaraq bir çox qabaqcıl verilənlər bazası idarəetmə sistemlərində mövcud olan rol əsaslı giriş nəzarəti daxildir; UNIX və Windows əməliyyat sistemlərində verilən sadə sənəd icazələri; Windows şəbəkə sistemlərində təqdim olunan qrup siyasət obyektləri; və Kerberos, RADIUS, TACACS və bir çox firewall və marşrutlaşdırıcılarda istifadə olunan sadə giriş siyahıları və sairə.

Effektiv olmaq üçün siyasətlər və digər təhlükəsizlik nəzarəti qüvvəyə minməlidir. Effektiv siyasət insanların hərəkətləri üçün cavabdeh olmasını təmin edir. ABŞ Xəzinədarlığının həssas və ya mülkiyyət məlumatlarını emal edən sistemlərə dair

təlimatları, məsələn, bütün uğursuz və müvəffəqiyyətli identifikasiya və giriş cəhdlərinin qeydiyyata alınmalı olduğunu və bütün məlumatlara girişin müəyyən bir növ iz buraxmalı olduğunu bildirir.

Ayrıca, ehtiyacı bilmək prinsipi, giriş nəzarətindən danışarkən təsirli olmalıdır. Bu prinsip bir insana iş funksiyalarını yerinə yetirmək imkanı verir. Bu prinsip fərqlərin təmizlənməsi ilə məşğul olduqda hökumətdə istifadə olunur. Fərqli şöbələrdə olan iki işçinin gizli rəsmiləşdirilməsinə baxmayaraq, məlumat mübadiləsi üçün bilmək ehtiyacı var. Bilmək lazım olan prinsipə əsasən, şəbəkə rəhbərləri işçilərə nəzərdə tutulduqlarından daha çox imkan verməmələri üçün işçiyə ən az miqdarda imtiyazlar verirlər. Bilmək lazım olan şey məxfilik-bütövlük-mövcudluq üçlüyünün tətbiqinə kömək edir. Bilmək lazım olan şey üçlüyün məxfi sahəsinə birbaşa təsir göstərir.

3.11 Kriptoqrafiya

İnformasiya təhlükəsizliyi istifadə edilə bilən məlumatları səlahiyyətli istifadəçidən başqa hər kəs tərəfindən istifadə edilə bilməyən bir formaya çevirmək üçün kriptoqrafiyadan istifadə edir; bu proses şifrələmə adlanır. Şifrələnmiş (yararsız hala salınmış) məlumat, şifrələmə prosesi vasitəsilə kriptoqrafik açara sahib olan səlahiyyətli bir istifadəçi tərəfindən yenidən orijinal istifadəyə yararlı formaya çevrilə bilər. Kriptoqrafiya, məlumat ötürülmə zamanı (elektron və ya fiziki olaraq) və məlumat saxlandıqda, icazəsiz və ya təsadüfi açıqlanmadan qorunmaq üçün informasiya təhlükəsizliyində istifadə olunur.

Kriptoqrafiya, təkmilləşdirilmiş identifikasiya metodları, mesajın həzm edilməsi, rəqəmsal imzalar, rədd etmə və şifrələnmiş şəbəkə əlaqələri daxil olmaqla digər faydalı tətbiqlərlə informasiya təhlükəsizliyini təmin edir. Köhnə, daha az etibarlı olan Telnet və Fayl Köçürmə Protokolu (FTP), yavaş-yavaş şifrəli şəbəkə əlaqələrini istifadə edən Secure Shell (SSH) kimi daha etibarlı tətbiqlərlə əvəz olunur. Simsiz rabitə WPA / WPA2 və ya daha yaşlı (və daha az etibarlı) WEP kimi protokollardan istifadə edərək şifrələnə bilər. Simli rabitə (məsələn, ITU - T G.hn) şifrələmə üçün AES

və autentifikasiya və açar mübadiləsi üçün X.1035 istifadə edərək təmin edilir. GnuPG və ya PGP kimi proqram tətbiqləri, məlumat fayllarını və e-poçtu şifrələmək üçün istifadə edilə bilər.

Kriptoqrafiya düzgün tətbiq edilmədiyi zaman təhlükəsizlik problemlərini ortaya qoya bilər. Kriptoqrafik həllərin kriptoqrafiya üzrə müstəqil ekspertlər tərəfindən ciddi nəzərdən keçirilmiş sənaye tərəfindən qəbul edilmiş həllərdən istifadə edilməklə həyata keçirilməlidir. Şifrələmə açarının uzunluğu və gücü də vacib bir məqamdır. Zəif və ya çox qısa bir açar zəif şifrələmə yaradacaqdır. Şifrələmə və şifrəni açmaq üçün istifadə olunan düymələr hər hansı digər məxfi məlumatlarla eyni dərəcədə qorunmalıdır. İcazəsiz açıqlanmadan və məhv edilmədən qorunmalı və lazım olduqda mövcud olmalıdırlar. İctimai açar infrastrukturun (PKI) həlləri açar idarəetmə ilə əlaqəli bir çox problemi həll edir.

3.12 Məlumatların ötürülməsi zamanı baş verə biləcək qəzaların qarşısının alınması planları.

Bir insidentə cavab planı bir təşkilatın kiber hücumuna reaksiyasını diktə edən bir qrup siyasətdir. Bir təhlükəsizlik pozuntusu aşkar edildikdən sonra plana başlanılır. Məlumatların pozulmasına hüquqi təsir göstərə biləcəyini qeyd etmək vacibdir. Yerli və federal qanunları bilmək çox vacibdir. Hər plan, təşkilatın ehtiyacları üçün unikaldır və İT komandasının bir hissəsi olmayan bacarıq dəstini özündə cəmləşdirə bilər. Məsələn, bir məlumat pozuntusundakı hüquqi təsirləri idarə etməyə kömək etmək üçün bir vəkil cavab planına daxil edilə bilər. Yuxarıda qeyd edildiyi kimi hər plan unikaldır, lakin əksər planlara aşağıdakılar daxildir:

Əvvəlcədən hazırlıq. Yaxşı bir hazırlıq insidentlərə cavab vermə qrupunun inkişafını əhatə edir. Bu komanda tərəfindən istifadə ediləcək bacarıqlar, nüfuz testi, kompüter mühakiməsi, şəbəkə təhlükəsizliyi və s. Bu komanda kiber təhlükəsizlik və müasir hücum strategiyalarındakı tendensiyaları da diqqətdə saxlamalıdır. Son

istifadəçilər üçün bir təlim proqramı vacibdir, həm də ən müasir hücum strategiyaları şəbəkədəki istifadəçiləri hədəfə alır.

Eyniləşdirmə. Hadisəyə cavab planının bu hissəsi təhlükəsizlik hadisəsinin olub olmadığını müəyyənləşdirir. Son istifadəçi məlumat verdikdə və ya bir idarəçi pozuntular barədə xəbərdarlıq verdikdə, istintaq başlayır. İnsident qeydləri bu addımın vacib hissəsidir. Komandanın bütün üzvləri məlumat axınının mümkün qədər sürətli olmasını təmin etmək üçün bu qeydi yeniləməlidirlər. Bir təhlükəsizlik pozuntusunun baş verdiyi müəyyən edilərsə, növbəti addım aktivləşdirilməlidir.

Minimum zərər. Bu mərhələdə, IRT təhlükəsizlik tədbirinin əhatə dairəsini məhdudlaşdırmaq üçün pozuntunun baş verdiyi əraziləri təcrid etmək üçün işləyir. Bu mərhələdə məlumatın məhkəmə qaydasında qorunması vacibdir ki, sonradan prosesdə təhlil olunsun. Çirklənmə fiziki olaraq bir server otağı olan və ya bir virusun yayılmasına imkan verməmək üçün bir şəbəkəni seqmentləşdirmək qədər sadə ola bilər.

Zərərin aradan qaldırılması. Müəyyən olunmuş təhlükənin təsirlənmiş sistemlərdən silindiyi yerdir. Buraya zərərli faylları silmək, güzəştli hesabları ləğv etmək və ya digər komponentləri silmək daxil ola bilər. Bəzi hadisələr bu addımı tələb etmir, lakin bu addıma keçməzdən əvvəl hadisəni tam başa düşmək vacibdir. Bu, təhdidin tamamilə aradan qaldırılmasını təmin etməyə kömək edəcəkdir.

Məlumat axınının bərpa edilməsi. Bu mərhələ sistemlərin orijinal işə bərpa olunduğu yerdir. Bu mərhələ məlumatların bərpası, istifadəçi giriş məlumatlarının dəyişdirilməsi və ya gələcəkdə pozuntuların qarşısını almaq üçün təhlükəsizlik duvarı qaydaları və ya siyasətinin yenilənməsi ola bilər. Bu addımı icra etmədən sistem gələcək təhlükəsizlik təhdidlərinə qarşı hələ də həssas ola bilər.

Əvvəldən konfiqurasiya. Bu addımda bu müddət ərzində toplanmış məlumatlar təhlükəsizliklə bağlı gələcək qərarlar qəbul etmək üçün istifadə olunur. Bu addım gələcək hadisələrin qarşısını almaq üçün vacibdir. Bu məlumatları idarəçiləri daha da

təlimləndirmək üçün istifadə etmək proses üçün vacibdir. Bu addım, təhlükəsizlik hadisəsi yaşamış digər qurumlardan yayılan məlumatların işlənməsi üçün də istifadə edilə bilər.

Dəyişikliklərin idarə olunması. Dəyişikliklərin idarə edilməsi, məlumatların emalı mühitində dəyişikliklərin yönləndirilməsi və nəzarət edilməsi üçün rəsmi bir prosesdir. Bura masaüstü kompüterlər, şəbəkə, serverlər və proqram təminatlarında dəyişikliklər daxildir. Dəyişikliklərin idarə edilməsinin məqsədi məlumatların emalı mühitində baş verən dəyişikliklər nəticəsində yaranan riskləri azaltmaq və dəyişikliklər edildikdə emal mühitinin sabitliyini və etibarlılığını artırmaqdır. Lazımi dəyişikliklərin həyata keçirilməsinin qarşısını almaq və ya maneə törətmək dəyişiklik rəhbərliyinin məqsədi deyil.

İnformasiya emalı mühitində hər hansı bir dəyişiklik risk elementini təqdim edir. Görünür sadə dəyişikliklər də gözlənilməz təsir göstərə bilər. Rəhbərliyin bir çox vəzifələrindən biri risklərin idarə olunmasıdır. Dəyişikliklərin idarə edilməsi, məlumatların emalı mühitində baş verən dəyişikliklərlə daxil edilən risklərin idarə olunması üçün bir vasitədir. Dəyişikliklərin idarə edilməsi prosesinin bir hissəsi dəyişikliklərin qeyri-müəyyən vaxtlarda həyata keçirilməməsini, kritik iş proseslərini poza və ya digər dəyişikliklərə müdaxilə edə biləcəyini təmin edir.

Hər dəyişikliyi idarə etmək lazım deyil. Bəzi dəyişikliklər, gündəlik məlumatların işlənməsinin bir hissəsidir və əvvəlcədən müəyyən edilmiş prosedura riayət edir, bu da emal mühitində ümumi risk səviyyəsini azaldır. Yeni bir istifadəçi hesabı yaratmaq və ya yeni bir masaüstü kompüterin yerləşdirilməsi ümumiyyətlə dəyişiklik idarə etməyi tələb etməyən dəyişikliklərə misaldır. Bununla birlikdə, istifadəçi sənəd paylaşımlarını köçürmək və ya E-poçt serverini təkmilləşdirmək emal mühitinə daha yüksək risk yaradır və normal gündəlik fəaliyyət deyildir. Dəyişikliklərin idarə edilməsində kritik ilk addımlar (a) dəyişikliyin müəyyən edilməsi

(və bu tərifin ötürülməsi) və (b) dəyişiklik sisteminin əhatə dairəsinin müəyyənləşdirilməsidir.

Dəyişikliklərin idarə edilməsi, ümumiyyətlə, əsas iş sahələri, təhlükəsizlik, şəbəkə, sistem administratorları, verilənlər bazası administrasiyası, tətbiq inkişaf etdiriciləri, masaüstü dəstəyi və kömək masası nümayəndələrindən ibarət bir dəyişiklik icmal heyəti tərəfindən nəzarət olunur. Dəyişiklik nəzərdən keçirmə şurasının vəzifələri avtomatlaşdırılmış iş axını tətbiqinin köməyi ilə asanlaşdırıla bilər. Dəyişiklik nəzərdən keçirmə şurasının məsuliyyəti təşkilatın sənədləşdirilmiş dəyişiklik idarəetmə prosedurlarına əməl edilməsini təmin etməkdir. Dəyişikliklərin idarə edilməsi prosesi aşağıdakı kimidir.

Dəyişiklik tələbinin göndərilməsi. Hər kəs dəyişiklik tələb edə bilər. Dəyişiklik sorğusunu verən şəxs, təhlili həyata keçirən və ya dəyişikliyi həyata keçirən eyni şəxs ola bilər. Dəyişiklik tələbi alındıqda, tələb olunan dəyişikliyin təşkilatların iş modelinə və təcrübəsinə uyğun olub olmadığını və dəyişikliyin həyata keçirilməsi üçün lazım olan mənbələrin miqdarını müəyyənləşdirmək üçün ilkin baxışdan keçə bilər.

Tələbin təsdiqlənməsi. Rəhbərlik işi idarə edir və resursların bölüşdürülməsinə nəzarət edir, rəhbərlik dəyişikliklərə dair tələbləri təsdiqləməli və hər dəyişiklik üçün prioritet təyin etməlidir. Rəhbərlik dəyişikliyin iş modelinə, sənaye standartlarına və ya ən yaxşı təcrübələrə uyğun olmadığı təqdirdə dəyişiklik tələbini rədd etməyi seçə bilər. Rəhbərlik dəyişiklik üçün ayrıla biləndən daha çox vəsait tələb edərsə dəyişiklik tələbini rədd etməyi də seçə bilər.

Planın tərtib olunması. Dəyişikliyin planlaşdırılması təklif olunan dəyişikliyin əhatə dairəsini və təsirini aşkar etmək; dəyişikliyin mürəkkəbliyini təhlil etmək; Resursların bölüşdürülməsi və həm icra, həm də geri planların hazırlanması, sınaqdan keçirilməsi və sənədləşdirilməsi. Geri göndərmə qərarı veriləcək meyarları müəyyənləşdirmək lazımdır.

Testləşdirmə və monitorinq. Dəyişiklik istehsal mühitinə tətbiq edilməzdən əvvəl, həqiqi istehsal mühitini yaxından əks etdirən təhlükəsiz bir sınaq mühitində sınaqdan keçirilməlidir. Planın geri qalan hissəsi də mütləq sınaqdan keçirilməlidir.

Proses cədvəlinin hazırlanması. Dəyişiklik nəzərdən keçirmə şurasının məsuliyyətinin bir hissəsi digər planlaşdırılan dəyişikliklər və ya kritik iş fəaliyyətləri ilə potensial qarşıdurmalar üçün təklif olunan icra tarixini nəzərdən keçirməklə dəyişikliklərin planlaşdırılmasına kömək etməkdir.

Dəyişikliklər arası əlaqə. Bir dəyişiklik planlaşdırıldıqdan sonra məlumat verilməlidir. Rabitə dəyişiklikləri planlaşdırma zamanı gözdən yayınan ola biləcək digər dəyişikliklər və ya kritik iş fəaliyyəti barədə başqalarına dəyişiklik nəzərdən keçirmə lövhəsini xatırlatmaq imkanı verməkdir. Rabitə də kömək masası və istifadəçilərə bir dəyişiklik baş verdiyini bilmək üçün xidmət edir. Dəyişiklik nəzərdən keçirmə şurasının başqa bir məsuliyyəti planlaşdırılan dəyişikliklərin dəyişiklikdən təsirlənən və ya dəyişikliyə marağı olanlara düzgün şəkildə çatdırılmasını təmin etməkdir.

Planların həyata keçirilməsi. Təyin edilmiş tarix və vaxtda dəyişikliklər həyata keçirilməlidir. Planlaşdırma prosesinin bir hissəsi həyata keçirmə planını, sınaq planını və geriyə planı hazırlamaq idi. Dəyişikliyin həyata keçirilməməsi və ya yerinə yetirilməsindən sonrakı sınaq testi uğursuz olarsa və ya digər "ölmüş" meyarlar yerinə yetirilərsə, geriyə plan yerinə yetirilməlidir.

Dəyişikliklərin sənədləşdirilməsi. Bütün dəyişikliklər sənədləşdirilməlidir. Sənədlərə dəyişiklik üçün ilkin sorğu, onun təsdiqlənməsi, ona verilən prioritet, həyata keçirilmə, sınaq və geri planlar, dəyişiklik nəzərdən keçirmə şurası tənqidinin nəticələri, dəyişikliyin həyata keçirildiyi tarix / vaxt, kim tərəfindən həyata keçirildiyi və Dəyişiklik uğurla həyata keçirildi, uğursuz oldu və ya təxirə salındı.

Dəyişikliklərin sonda nəzərdən keçirilməsi. Dəyişikliklərin nəzərdən keçirilmə heyəti dəyişikliklərin sonrakı icmalını keçirməlidir. Uğursuz və dəstəklənən dəyişiklikləri nəzərdən keçirmək xüsusilə vacibdir. İcmal heyəti qarşılaşdığı problemləri anlamağa çalışmalı və inkişaf üçün sahələr axtarmalıdır.

Sadə və istifadəsi asan olan dəyişikliklərin idarə edilməsi prosedurları, məlumat emalı mühitində dəyişiklik edildikdə yaranan ümumi riskləri xeyli azalda bilər. Dəyişikliklərin idarə edilməsi prosedurları həyata keçirildikcə dəyişikliklərin ümumi keyfiyyətini və uğurunu artırır. Bu planlaşdırma, araşdırma, sənədləşmə və rabitə ilə həyata keçirilir.

İSO / IEC 20000, Görünən OPS kitabçası: İTİL-in 4 Praktik və Yoxlanılan addımlarda yerinə yetirilməsi (Tam kitabın xülasəsi), və İnformasiya Texnologiyaları İnfrastruktur Kitabxanası, hamısı dəyişikliklərin idarə edilməsi proqramının məlumat təhlükəsizliyini təmin etmək üçün dəyərli rəhbərliyi təmin edir.

İşin davamlılığı. İş davamlılığının idarə edilməsi (BCM), təşkilatın kritik iş funksiyalarını hadisələr səbəbindən kəsilmədən qorumaq və ya ən azı təsirləri minimuma endirmək məqsədi daşıyır. BCM hər hansı bir təşkilat üçün texnologiyanın və işin hər zamanki kimi davam etməsi üçün mövcud təhdidlərə uyğun olması üçün vacibdir. BCM, bütün zəruri iş funksiyalarının hər hansı bir iş funksiyası üçün hər hansı bir təhdid olduğu təqdirdə davam etməsi üçün lazım olanı təmin etməsi üçün bir təşkilatın təhlili planına daxil edilməlidir. Bütün bunlar aşağıdakıları əhatə edir.

Tələblərin təhlili, məsələn, kritik iş funksiyalarının, asılılıqların və potensial uğursuzluq nöqtələrinin, potensial təhdidlərin və buna görə insana aid hadisələrin və ya təşkilatın narahatlıq risklərinin müəyyən edilməsi;

Spesifikasiya, məsələn, maksimum yol verilə bilən kəsilmə dövrləri; bərpa nöqtələrinin məqsədləri (məlumat itkisinin maksimum məqbul dövrləri);

Memarlıq və dizayn, məsələn, uyğunlaşma (məsələn, mühəndislik İT sistemləri və yüksək mövcudluğu üçün proseslər, işi dayandıra biləcək halların qarşısını almaq və ya qarşısını almaq), hadisə və fövqəladə halların idarə edilməsi (məsələn, binaların boşaldılması, təcili yardım xidmətləri, triage / vəziyyətin qiymətləndirilməsi və bərpa planlarının istifadəsi), bərpa (məsələn, yenidən qurulması) və fövqəladə halların idarə edilməsi (mövcud olan hər hansı bir resursdan istifadə edərək baş verən hər hansı bir şeyə müsbət yanaşmaq üçün ümumi imkanlar);

Həyata keçirmə, məsələn, ehtiyat nüsxələrin qurulması və planlaşdırılması, məlumat ötürülməsi və s., Kritik elementlərin çoxalması və gücləndirilməsi; xidmət və avadanlıq tədarükçüləri ilə müqavilə bağlamaq;

Sınaq, məsələn, müxtəlif növ, xərclər və təminat səviyyələrində iş davamlılığı üçün təlimlər;

İdarəetmə, məsələn, strategiyaları müəyyənləşdirmək, məqsəd və hədəfləri təyin etmək; işi planlaşdırmaq və istiqamətləndirmək; vəsait, insanlar və digər mənbələr ayırmaq; digər fəaliyyətlərə nisbətən prioritetləşdirmə; komanda quruculuğu, liderlik, nəzarət, motivasiya və digər iş funksiyaları və fəaliyyətləri ilə əlaqələndirmə (məsələn, İT, qurğular, insan resursları, risklərin idarə edilməsi, məlumat riski və təhlükəsizlik, əməliyyatlar); vəziyyəti izləmək, işlər dəyişdikdə tənzimləmələri yoxlamaq və yeniləmək; davamlı inkişaf, öyrənmə və müvafiq investisiya yolu ilə yanaşmanın yetişməsi;

Təminat, məsələn, müəyyən edilmiş tələblərə qarşı sınaq; əsas parametrləri ölçmək, təhlil etmək və hesabat vermək; tənzimləmələrin istəniləcəyi təqdirdə plana keçəcəyinə daha çox əmin olmaq üçün əlavə testlər, rəylər və auditlər aparmaq.

BCM həm hadisələrin ehtimalını, həm də şiddətini azaltmaqla fəlakətlə əlaqəli riskləri minimuma endirmək üçün geniş bir yanaşma tətbiq etsə də, fəlakətdən xilasetmə planı (DRP) fəlakətdən sonra mümkün qədər tez iş əməliyyatlarını bərpa

etməyə yönəlmişdir. Bir fəlakət baş verdikdən dərhal sonra istifadə edilən fəlakətlərin bərpa planı kritik informasiya və kommunikasiya texnologiyaları (İKT) infrastrukturunun bərpası üçün zəruri addımları əks etdirir. Fəlakətlərin bərpası planlamasına planlaşdırma qrupunun yaradılması, risk qiymətləndirməsinin aparılması, prioritetlərin müəyyən edilməsi, bərpa strategiyasının hazırlanması, ehtiyatların və planın sənədlərinin hazırlanması, yoxlama meyarları və prosedurlarının hazırlanması və sonuncu planın həyata keçirilməsi daxildir.

3.13 Ən çox yayılan telekommunikasiya sistemlərində - mobil şəbəkələrdə müasir dövrdə informasiya təhlükəsizliyinin təmin olunması

Son bir neçə ildə artan şəbəkə genişliyi, yetkin virtualizasiya texnikası və yaranan bulud əsaslı iş tələbləri sayəsində bulud hesablanması sürətlə böyüdü. Bundan əlavə, 2013-cü ilə qədər mobil qurğular, Gartner-in proqnozlaşdırdığı kimi, dünyada ən çox yayılmış veb giriş müəssisələri kimi PC-ləri qabaqlayacaqdır. Beləliklə, mobil texnologiyalarla bulud hesablamasının qarışığı çox gözlənilir. Mobil Bulud Hesablama (MCC), həm məlumatların saxlanması, həm də məlumatların işlənməsinin tətbiqi başladıldığı mobil cihazlardan kənarda həyata keçirildiyi bir infrastruktura aiddir. Bundan əlavə, mobil bir qurum yalnız bir mobil cihazla məhdudlaşmır; daha əhəmiyyətlisi, bulud qaynaqları, infrastruktur, xidmətlər və insan ola bilər. Beləliklə, bu anlayışla MCC daha sonra infrastrukturda, mənbələrdə, xidmətlərdə, istifadəçi cihazlarında və hətta insanlarda hərəkətliliyin olduğu bir bulud sisteminə aiddir. MCC sisteminin tendensiyası yalnız müəyyən ərazilərdə istifadəçilərə sabit xidmətlər göstərmək məqsədi daşımır, xüsusən də bütün dünyada mobil istifadəçilər arasında əlaqə yaratmağı gözləyir. MCC istifadəçilərinin hərəkətliliyi səbəbindən coğrafi olaraq paylanmış bir bulud sistemi istifadəçilərə mobil cihazlarına coğrafi olaraq "yaxın" olan bulud qaynaqlarına qoşulmağa imkan verən təbii bir seçimdir ki, bu da ümumiyyətlə mərkəzləşdirilmiş yanaşma ilə müqayisədə daha az rabitə gecikməsi deməkdir. MobiCloud ənənəvi MANETləri yeni bir xidmət yönümlü rabitə memarlığına çevirir. MobiCloud-da bir mobil cihaz hesablama və saxlama xidmətlərini müvafiq ESSI və

Təhlükəsiz Saxlama (SS) ilə təmin edə bilər. Üstəlik, cihaz buludlara hərəkət trayektoriyası kimi həssas məlumatlarını göndərəcəkdir. Qayıdış olaraq, bulud mobil cihaz tərəfindən verilən hərəkətlilik məlumatlarına görə daha yaxşı bir yer mərkəzli xidmətlər təqdim edə bilər. MobiCloud-da, mobil istifadəçilər mobil cihazlardan alınan məlumatları qorumaq üçün bulud xidməti təminatçısına etibar etməlidirlər. Bununla birlikdə, gizlilik mövzusunda həssas məlumatları ictimai bir buludda saxlamaq böyük narahatlıq doğurur. Bu sənəd bu məxfilik məsələsini həll etmək məqsədi daşıyır. Yeni təhlükəsiz mobil bulud çərçivəsi. Mobil bulud üç əsas sahədən ibarətdir: bulud mobil və hissedici domen, bulud etibarlı domeni və bulud ictimai xidməti və saxlama sahəsi.

Mobil şəbəkələrdə təhlükəsiz informasiya platformasının təşkilinin qarşısında dayanan əsas problemlər. Təhlükəsizlik sistemi istifadəçi identifikasiya kodunun daxil olduğu hər hansı bir sistemdə vacib bir rol oynayır, təhlükəsizlik sistemləri hər hansı bir kompüterli və ya rəqəmsal girişə nəzarət üçün vacibdir. Mobil qurğular, ehtiyat, təhlükəsizlik, rabitə və sair kimi qaynaqlarında bir çox mübarizə ilə qarşılaşır. Çox sayda təhlükəsizlik həssaslığı və zərərli kodlar kimi müxtəlif mobil cihazlara, məsələn mobil telefonlara, smartfonlara, noutbuklara və s. təsir göstərir. Bu problemlər xidmət keyfiyyətlərinin yaxşılaşdırılmasına böyük təsir göstərir. Bulud, mobil, veb və API idarəetmə kimi komponentlər tərəfindən istifadə edilə bilər ki, bu da REST texnologiyasından istifadə etməklə sadə kəşf və OS biznesinə və infrastruktur aktivlərinə təhlükəsiz giriş imkanı verir .İnfrastruktur təminatçıları (bulud əsaslı IaaS və SaaS provayderi) və mobil xidmətlər qeydləri (yəni API) idarəetmə) kəşf, tədarük, məlumatların dəyişdirilməsi və xidmətlərin istifadəsi üçün orta proqram təminatı ilə qarşılıqlı əlaqə yaratmaq üçün vahid bir yol tələb olunur.

Sürətlə inkişaf edən mobil və bulud hesablama aləmləri tətbiqlərə və işgüzar logistikalara getdikcə daha çox təzyiq göstərir. Burada qeyd etmək vacib olan amil, rəqəmsal şifrələrin serverdə saxlanılmamasıdır, lakin hashingdan sonra şifrəli formada saxlanılır. Sonralar identifikasiya sistemi üzərində bir çox tədqiqat aparıldı və

tədqiqatçılar sonradan mətn əsaslı parollara ən yaxşı alternativ kimi təsdiqlənən qrafik parol identifikasiya sistemini kəşf etdilər.

Bu məqsədlə Susan Wiedenbeck Jim Waters, Jean-Camille Birget və Alex Brodskiy Nasir Memon "Qrafik parollardan istifadə edərək təsdiqləmə: Əsas nəticələr" adlı əsərində PassPoints adlı yeni və daha etibarlı qrafik parol sistemi hazırlamışlar. Bu işdə PassPoints sistemi, təhlükəsizlik xüsusiyyətləri və PassPoints-i alfasayısal şifrələrlə müqayisə etdiyimiz empirik araşdırma təsvir olunur. Empirik araşdırmada iştirakçılar ya bir alfasayısal və ya qrafik bir şifrə öyrənmişlər və beş həftə ərzində şifrələrini daxil etmək üçün üç uzununa sınaq keçirmişlər. Təhlükəsizlik və gizliliklə əlaqəli risklər səbəbindən gözləntilərdən çox-çox aşağı nəticələr əldə olunmuşdur. Bu araşdırma mövcud ədəbiyyatlara əsaslanaraq, mobil bulud hesablama infrastrukturunu təmin etmək üçün işin hazırkı vəziyyətini vurğulayırdı. Nəticədə bir mobil mesaj identifikasiya kodunu istifadə edərək bir bulud serverində saxlanan sənədlərin bütövlüyünü yoxlamaq üçün mobil müştərilərə enerji səmərəliliyini yoxlamaq sxemini təklif olundu. Təqdim olunan sxem bütövlükdə yoxlanış işlərinin çoxunu bir bulud xidməti təminatçısına yükləyir və mobil müştəri üzərində işləmə işlərini minimuma endirmək üçün etibarlı üçüncü tərəfə. Bulud xidməti provayderi, mobil müştəri tərəfindən göstəriş verildikdə saxlanılan faylları koprosessor tərəfə yönləndirir. Koprosessor, bütövlüyü yoxlamaq üçün alınan sənədlərdə artan MAC hesablayır.

Proxy yenidən şifrələmə və şəxsiyyət əsaslı şifrələmə sxemlərinin köməyi ilə istifadəçi məlumatlarını açıqlamadan bulud üzərindəki məlumatları və təhlükəsizlik idarəçiliyini təmin edən etibarlı bir məlumat xidməti təklif etdi. Təqdim olunan etibarlı məlumat xidməti təhlükəsizlik idarəçiliyini mobil istifadəçilərdən uzaqlaşdırsa da, mobil istifadəçilər buludda bir fayl yükləməzdən əvvəl kriptoqrafik əməliyyatlar aparmalı olurlar. Kriptoqrafik əməliyyatlar kütləvi cütləşmə qiymətləndirmələri və eksponensial hesablamaları əhatə edir. Kriptoqrafik əməliyyatlar, mobil bulud hesablamaları üçün etibarlı bir çərçivə hazırlayarkən nəzərə alınması lazım olan xeyli

miqdarda enerji istehlak edir. İkincisi, bulud mobil istifadəçi adından təhlükəsizlik idarəçiliyini və yenidən şifrələməni yerinə yetirmək üçün məsuliyyət daşıyır. Mobil istifadəçi məlumatlarının təhlükəsizliyini, bütövlüyünü və identifikasiyasını təmin edən ağıllı telefonlar üçün bir sxem təklif etdi. Mobil istifadəçi ənənəvi asimmetrik şifrələmə üsullarından istifadə edərək faylları şifrələyir. Şifrələnmiş fayllar mobil istifadəçi adı, imza və şifrə ilə birlikdə bulud serverlərində saxlanılır. İstifadəçi etimadnaməsi ilə birlikdə şifrələnmiş fayllar bir rəqibin ev sahibliyi etdiyi bulud serverində saxlanıla bilər. Düşmən sonradan istifadəçini təqlid etmək üçün etimadnaməsini istifadə edə bilər. İkincisi, təklif olunan sxem cihazın emal və saxlama məhdudiyyətlərinə məhəl qoymadı. Şifrələmə və deşifrləmə və bütün bir fayl üzərində tətbiq olunan hash funksiyası mobil cihazda yerinə yetirilir. Məxfiliyi və məxfiliyi təmin edən bir resurs məhdud mobil cihaz üçün açıq məlumat əldə etmə sxemini təklif etdi. Etibarlı üçüncü tərəf, mobil istifadəçi adından kodlaşdırma / deşifrləmə, şifrələmə / şifrəni açmaq, imza yaratmaq və yoxlama üçün məsuliyyət daşıyır. Mobil istifadəçinin işlərini etibarlı üçüncü tərəfə endirməsi enerjiyə qənaət etsə də, mobil istifadəçilərin sayının artması performansın pozulmasına səbəb olur. Yeni mobil bulud hesablama çərçivəsini təklif etdi ki, bu da yalnız adi hesablama xidmətləri təqdim etmir, eyni zamanda risklərin idarə edilməsi, etibarlı idarəetmə və etibarlı marşrutlaşdırma baxımından MANET-in funksionallığını yaxşılaşdırır. MobiCloud-un MANET-ə verdiyi üstünlüklərə baxmayaraq, MobiCloud çərçivəsi bulud qovluğunun etibarına yararlı olduğunu nəzərə almadı. Mobil istifadəçi məlumatlarını bulud serverlərində etibarlı bir şəkildə saxlamaq üçün bir mexanizm olmalıdır. Rənglərdən istifadə edərək təkmilləşdirilmiş mətn əsaslı çiyin sörfünə davamlı qrafik parol sxemini müzakirə edir. Təklif olunan sxemdə istifadəçi asanlıqla və effektiv şəkildə sistemə daxil ola bilər.

3.14 Telekommunikasiya sistemlərində şəbəkə təhlükəsizliyi

İndiki vaxtda bir siçan istifadə etməklə, elektrik şəbəkələri və trafik sistemləri daxil olan sistemlər yerlərindən və tarazlıq vəziyyətindən asılı olmayaraq istifadəçilər

üçün əlçatandır. Fərqi yoxdur, statik və ya mobil olsun. Dəfələrlə elmi tədqiqatlar sübut etdi ki, belə qarşılıqlı əlaqə nəticəsiz deyildir. Kabel modemlərinin əksəriyyətində mövcud olan genişlik sayəsində istənilən bir peşəkar xaker böyük şəhərlərdə mobil telekommunikasiya şəbəkələrindəki səs xidmətini passivləşdirə biləcək hücumlara başlaya bilər. Fövqəladə vəziyyətlərdə belə şəbəkələr insanların həyatını xilas etmək üçün vacib olduqda, bu cür hücumlar olduqca təhlükəli ola bilər.

Telekommunikasiya mənbələri səs və məlumat şəbəkələri, simsiz xidmətlər, yüksək sürətli məlumat rabitə, telefon, şəbəkə serverləri, açarlar və ya elektron rabitə ötürmələrində istifadə olunan hər hansı digər cihaz, xidmət və ya sistem ola bilər. Telekommunikasiya sistemlərinin yeri / xarakteri eyni dərəcədə müxtəlifdir: yerli və ya tikinti şəbəkələrindən qlobal şəbəkələrə qədər; tək telefon aparatlarından rabitə peyklərinə; və ya müəyyən bir tətbiqə həsr edilmiş və ya bir çox istifadəçi, proqram və tətbiq tərəfindən paylaşılan olub-olmaması.

Ümumiyyətlə telekommunikasiya üçün təhlükəsizlik tələbləri təcrid olunmuş bir fenomen kimi görülməməlidir. Əksinə, telekommunikasiya mənbələri üçün təhlükəsizlik mülahizələri hər zaman nəzərə almalıdır ki, telekommunikasiya müasir dövrdə İnformasiya Cəmiyyəti kontekstində İnformasiya Texnologiyaları (İT) ilə əlaqəli sənaye sahələri üzrə müəssisələrin fəaliyyət göstərməsi üçün vacib və kritik bir mənbədir.

Bundan əlavə, telekomunikasiya resursları üzərindəki tətbiqlər və ötürmələr də vacib və kritik olduğu başa düşülməlidir. Məlumat və ya kompüterə əsaslanan şəbəkə müvafiq təhlükəsizliyə sahib olduğu kimi, çox vaxt eyni şəbəkə ola bilən bir telekommunikasiya şəbəkəsi də ekvivalent təhlükəsizliyə sahib olmalıdır. Məsələn, telekommunikasiya mənbələri üçün Şifrə Təhlükəsizliyi tələbləri, standart səs sökmə vahidləri (telefonlar) kimi şifrə ilə qorunma imkanına malik olmayan telekommunikasiya cihazları və mənbələri istisna olmaqla, digər İT mənbələri ilə eynidir.

Davam edənləri nəzərə alaraq, bu fəsildə əvvəlcə təhlükəsizlik kontekstini və təhdid ölçüsünü qiymətləndirərək mövzuya qısa bir yer veriləcəkdir. Bunun ardınca telekommunikasiya sisteminin təhlükəsizlik tələbləri; telekommunikasiya şəbəkələri üçün təhlükəsizlik təhdidlərinin müəyyən edilməsi, ehtimal olunan əks və ya yumşaldıcı tədbirlər və bu tədbirlərin həyata keçirilməsi və s. nəzərdən keçiriləcəkdir.

3.15 Kriptologiyanın qısa icmalı

Şifrə sistemi və ya kriptosistem mesajları arzu olunmayan alıcılardan qorunmaq üçün istifadə olunan bir texnikadır. Bir alqoritm və bütün mümkün mətnlər, şifrə mətnləri və açarlardan ibarətdir. Kriptoqrafik bir alqoritm şifrələmə və şifrənin açılması üçün istifadə olunan riyazi funksiyadır. Kriptoqrafiya, kriptovalyutası bu cür sistemləri sındırma sənətidir, kriptosistemlər yaradan sənət və elmdir.

Kriptologiya termini həm kriptovalyutanı, həm də kriptoanalizi əhatə etmək üçün istifadə olunur. Göndəriləcək orijinal mesaj düz mətn adlanır, şifrəli mesaj isə şifrəli mətn. Şifrələmə - alqoritm və açardan istifadə etməklə düz mətnin şifrə mətninə çevrilməsi prosesidir. Açarı mesajla qanuni əlaqəsi olanlar tərəfindən gizli və ya açıq şəkildə paylaşıla bilən və bir mesajdan digərinə fərqli ola bilən komponentdir. Açar tez-tez kriptovalyuta adlanır. Şifrəni açmaq şifrə mətnini orijinal düz mətnə çevirmək prosesidir. Bu tərs proses şifrələmə alqoritmi və açarı haqqında biliklərdən irəli gəlir.

Kerckhoffun prinsipi ilə təmin edildiyi kimi, açardan başqa sistem haqqında hər şey ictimaiyyətin məlumatı olsa da kriptosistem etibarlı olmalıdır. Eyni fikir Shannon'un maksimində "düşmən qarışıqlığı ilə təhlükəsizlikdən" fərqli olaraq "düşmən sistemi tanıyır" kimi ifadə edilir.

Bir nümunə olaraq, 786 nömrəsinin kriptosistemdən istifadə edərək göndəriləcəyini düşünün və hər iki tərəf 019-un açar dəyəri barədə razılığa gəldilər. Mesajın (786) və açarın (019) əlavə olunduğu şifrələmə alqoritmindən istifadə edərək şifrə mətni 805. Alıcının açarını (019) və şifrələmə alqoritmini (əlavə) bildiyindən, mesajı tərs əməliyyatı etməklə şifrəni mətndən çıxarmaq olar, düz mətn mesajı 786

almaq üçün 805-dən 019-u çıxmaq olur. rabitə, şifrələmə texnikası məlum olsa belə, şifrə mətnindən düz mətni tapmaqda çətinlik çəkməlidir.

3.16 Kriptoqrafiya konteksti

Kriptoqrafiya mesajların etibarlı saxlanılması sənəti və elmidir; burada şifrələmə əsas məqsəddir. Məlumatların şifrələnməsi və şifrəsinin açılması üçün riyaziyyatdan istifadə etməklə, həssas məlumatları saxlamağı və ya təhlükəli şəbəkələr (məsələn, İnternet) üzərindən ötürməyi, beləliklə nəzərdə tutulan alıcının xaricində hər kəs tərəfindən oxuna bilməyəcəyini təmin edən bir elmdir. Söhbət, qulaq asmaçı, haker və kiber döyüşçüləri daxil edən düşmənlərin təsirini dəf edən protokol və alqoritmlərin qurulması və təhlilindən gedir. Bunlar məlumatların məxfiliyi, məlumatların bütövlüyü və autentifikasiya / rəqəmsal imza kimi informasiya təhlükəsizliyindəki müxtəlif aspektlərlə əlaqədardır.

Nəticə və təkliflər

BTİ 1865-ci ildə Beynəlxalq Teleqraf Birliyi olaraq təsis edilmişdir. İlk təcrübə sahəsi teleqraf olsa da, ITU-nun işi rəqəmsal yayımdan İnternetə və mobil texnologiyalardan üçölçülü televiziyaya qədər bütün İKT sektorunu əhatə edir. İKT təhlükəsizlik standartlarının inkişafı son illərdə İnternet və digər şəbəkələrin istifadəsinin sürətlə artması və artan sayına və müxtəlif təhlükələrə qarşı istifadəçi və sistemlərin qorunması ehtiyacının tanınması ilə çox sürətlənmişdir.

Müvafiq və effektiv təhlükəsizlik müddəalarının sistem dizayn prosesinin vacib və ayrılmaz hissəsi olması çoxdan qəbul edilmişdir. Dizaynla təhlükəsizlik, yeni gəlir və tələsik istehsal olunan əks tədbirlərlə qarşı-qarşıya gəlməyə çalışan İKT aktivlərini qorumaqda daha təsirli olur. ITU-T tərəfindən hazırlanan təhlükəsizlik tövsiyələri, təhlükəsiz sistem dizaynını dəstəkləmək üçün sağlam bir əsas verir.

Gələcəyə baxaraq, telekommunikasiya şəbəkələri və kompüter şəbəkələri birləşməyə davam edəcəkdir. Həm də əminliklə bilirik ki, şəbəkələr və veb əsaslı xidmətlər və tətbiqlər sürətlə böyüməyə davam edəcək və əksər insanlar üçün, habelə dövlət və özəl sektor təşkilatları üçün gündəlik həyatın vacib bir hissəsinə çevriləcəkdir. Artıq bir neçə ildir gördüyümüz kimi, təhdid və hücumlar getdikcə yenilikçi yollarla inkişaf etməyə davam edir. Bu təhdidlərə qarşı vaxtında və effektiv cavab tədbirləri hazırlamaq və inkişaf etdirmək üçün davamlı problem olaraq qalacaqdır. Xüsusi zəifliklərin azaldılması üçün sistemlərin və şəbəkələrin daha yaxşı, daha etibarlı dizaynına və həyata keçirilməsinə nail olmaq çətin olacaq. Və yeni təhlükələrə, təhlükəsiz dizayn və həyata keçirilməsinin vacibliyini bir daha vurğulayan bir vəziyyətə qarşı sürətli reaksiya əldə etmək getdikcə daha çətin olacaq. Müsbət addımlardan biri, kiber təhlükəsizlik mübadiləsi işimizdə sübut olunan təhdidlər haqqında məlumat mübadiləsidir. Bu, qlobal telekommunikasiya / İKT cəmiyyətinin təhdidlərə cavab vermək və təsirini azaltmaq qabiliyyətini artıracaqdır.

Təhlükəsizliyin aktual olduğu bir sıra sahələri müəyyən etmək mümkündür. Əşyalar İnterneti (IoT) xüsusi maraq doğuran sahələrdən biridir, çünki istehlakçı cihazları və sensor cihazları da daxil olmaqla gündəlik cihazların bağlantısında kütləvi artım nəzərdə tutulur ki, bu da bir çox hallarda istehlakçının xəbərdar olmaması və ya ona aidiyyəti olmamasıdır. Qısacası bir təhlükəsizlik pozuntusudur. Təhlükəsizliyin qeyri-kafi olmasının nəticələrinin bəzi dramatik nümunələri nümayiş etdirilib. Bunlara hal-hazırda quraşdırılmış avtomobil idarəetmə sistemlərinin təhlükəsizlik parametrlərinin aşkara çıxarılması və qaçırılması və avtomatlaşdırılmış səhiyyə çatdırılması mexanizmlərində icazəsiz dəyişikliklər daxildir. SG17, IoT üçün təhlükəsizlik çərçivəsini inkişaf etdirir və ITU-T, ağıllı şəhərlər və icmalara ilkin diqqət yetirərək, IoT və tətbiqlərini öyrənmək üçün yeni bir İş Qrupu (SG20) qurdu.

Kritik infrastrukturun qorunması (CIP) effektiv təhlükəsizliyin tamamilə vacib olduğu digər bir sahədir. Bununla birlikdə, bu sahə üçün standartların inkişafı bir sıra amillərlə mürəkkəbdir, o cümlədən müxtəlif ölkələrdə kritik infrastrukturun nədən ibarət olduğu və lazımi standartların işlənib hazırlanması təşkilatının SDO-larının mövcud olub-olmaması ilə bağlı fikir ayrılıqları). . Bununla birlikdə, CIP təhlükəsizlik ehtiyaclarını ödəmək üçün artıq hazırlanmış və ya inkişaf etdirilən bir çox təhlükəsizlik standartları qəbul edilə bilər. Smart Grid-in təhlükəsizliyi SDO-ların diqqətini çəkən başqa bir sahədir. Smart Grid təhlükəsizlik tələbləri SG17 tərəfindən nəzərdən keçirilir.

193 Üzv Dövlət və BTİ-nin təxminən 700 Sektor Üzvü və şərikləri, üzvlərin ehtiyaclarını nəzərə alaraq idarə olunan və təcavüzkar bir iş proqramında təhlükəsizlik mövzusunda texniki tövsiyələr və təlimatlar hazırlamağa davam edərək bu problemlərə cavab verməyə davam edəcəklər. Ümumdünya Telekommunikasiya Standartlaşdırma Assambleyası tərəfindən qurulmuş təşkilati quruluş. Mümkün olduğu təqdirdə, ITU-T səylərin təkrarlanmasını minimuma endirmək və uyğunlaşdırılmış həllərə mümkün qədər səmərəli və sürətli şəkildə nail olmaq üçün digər standartların inkişafı təşkilatları ilə əməkdaşlıq edəcəkdir.

Ədəbiyyat

1. Aliquluyev R. və Adıgözəlova N., (2016), "İnformasiya təhlükəsizliyi üzrə aparılan tədqiqatların bibliometrik analizi", Azərnəşr, 311 səh.

2. Əliquliyev R.M. və İmamverdiyev Y.N, (2003), "Rəqəm imzası texnologiyası", Azərnəşr, 372 səh.

3. Həşimov M., (2013), "Əşyalar internetinin təhlükəsizlik məsələləri", Bakı, 194 səh.

4. İmamverdiyev Y., (2014), "İnformasiya təhlükəsizliyi sahəsində beynəlxalq koalisiyaların formalaşdırılması problemləri", Bakı, 242 səh.

5. Qasımov V.Ə., (2009), "İnformasiya təhlükəsizliyinin əsasları", Bakı, 412 səh.

6. Qasımov V.Ə, (2007), "İnformasiya təhlükəsizliyi: kompüter cinəyatkarlığı və kiberterrorçuluq", Elm, 263 səh.

7. Nəbiyev B., (2017) "Şəbəkə təhlükəsizliyi əməliyyat mərkəzinin arxitektur modeli", Elm, 355 səh.

8. Aceituno V., "On İnformation Security Paradigms", İSSA Journal, 2005, p.22-26

9. Anderson K., "İT Security Professionals Must Evolve for Changing Market", SC Magazine, 2006, p.121-127

10. Blechman A., (2008), "Chronology: Reuters from pigeons to multimedia merger". Nature America, 201 p.

11. Calvert J.B., (2004), "The Electromagnetic Telegraph". Scholastic, 312 p.

12. Chaesub L., (2015), “Security in Telecommunications and Information Technology”, Bloomsbury, 525 p.

13. Cybersecurity Information Exchange Techniques – www.itu.int

14. Dhillon G., (2007), “Principles of İnformation Systems Security”, John Wiley & Sons, 442 p.

15. Dustin D., (2017), “Awareness of How Your Data is Being Used and What to Do About It”, CDR Blog, 542 p.

16. Easttom C., (2011), “Computer Security Fundamentals”, Pearson Education, 291 p.

17. Gaudin S., (2019), “The transistor: The most important invention of the 20th century”, John Wiley & Sons, 552 p.

18. George A. J., (1955), “Jamming and Protection of Frequency Assignments”, 388 p.

19. Haykin E., (2010), “Worldwide Telecommunications Industry Revenues”, Reuters, 243 p.

20. Hoddeson L., (2012), “The Vacuum Tube”. Random House, 684 p.

21. Hurdeman A.A., (2003), “The Worldwide History of Telecommunication”. Simon & Schuster, 531 p.

22. İnternational Telecommunication Union. “İTU Radio Regulations”, Journal of HarperCollins Publishers. 2015, p.150-158

23. Lambo T., “İSO/İEC 27001: The future of infosec certification”, İSSA Journal, 2006, p.120-127.

24. Jakubowski A., “History of Semiconductors”, Journal of Geneva. 2010, p.52-55

25. Julia H., (2001), “The Cert Guide to System and Network Security Practices”, Boston, 315 p.

26. Kerry R., (2019), “The Wireless Revolution”, Queensland 645 p.

27. Malcolm J., (2009), “Security in Telecommunications and Information Technology”, Wayback Machine, 367 p.

28. Martin H. & Priscila L., (2011), “The World’s Technological Capacity to store, Communicate and Compute Information”, Timeline, 605 p.

29. Mireeille S., (2007), “The Effect of Income Inequality on Mobile Phone Penetration”, 171 p.

30. Ronald L., (2003), “The CİSSP Prep Guide”, Wiley & Sons, 574 p.

31. Saleem B., (2006), “Optical fibre waveguide”, Britain Express, 356 p.

32. Thomas R., (2001), “İnformation Security Risc Analysis”, Auerbach publications, 456 p.

33. Thomas R., (2002), “İnformation Security Policies, Procedures, and Standards”, Auerbach, 527 p.

34. Timothy P., (2018), “İnformation Security: Design, İmplementation and Compliance”, Auerbach publications, 372 p.

35. White G., (2003), “All in One Security”, Osborne, 252 p.

36. William S., (2004), “Data and Computer Communications”, Wayback Machine, 366 p.

Xülasə

Beləliklə, “Telekommunikasiya sistemlərində informasiya təhlükəsizliyinin təmin edilməsi” mövzusunun tədqiqi həyatımızın hər sahəsində böyük rol oynayan, eləcə də şəxsi məlumatlarımız, büdcələrimiz də daxil olmaqla bizim üçün böyük əhəmiyyət kəsb edən çox önəmli məlumatlarımızı daşıyan telekommunikasiya sistemləri və vasitələrinin informasiya təhlükəsizliyinin təmin edilməsinin necə vacib olduğunu göstərdi. Tədqiqatın elmi yeniliyinin əsasında telekommunikasiya sistemlərinin həm tarixi inkişafı boyunca, həm də gələcəyə baxan yönündə informasiya təhlükəsizliyinin necə və hansı üsullara dayanaraq təmin edilməsi, həmçinin hansı perspektivli sahələrdə istifadə olunması zəruriliyinin müqayisə, analiz, statistik və digər tədqiqat metodları sayəsində aşkara çıxarılması və ümumiləşdirilməsi dayanır. Tədqiqatın informasiya bazasının əsası birbaşa olaraq “Beynəlxalq Telekommunikasiya Birliyi” təşkilatının rəsmi saytı, eləcə də, həmin birlik tərəfindən müxtəlif illərdə çap edilmiş elmi məqalələr və kitablar təşkil edir. Tədqiqatın nəticələrini aşağıdakı kimi ümumiləşdirmək olar.

- Telekommunikasiya sistemlərində informasiya təhlükəsizliyi birbaşa olaraq Beynəlxalq Telekommunikasiya Birliyinin tövsiyələrin əsasında təmin edilir.
- Birliyin son tövsiyələrinə əsasən müasir dövr üçün Dizaynla təhlükəsizlik, yeni gəlir və tələsik istehsal olunan əks tədbirlərlə qarşı-qarşıya gəlməyə çalışan İKT aktivlərini qorumaqda daha təsirli hesab edilir.
- Müsbət addımlardan biri kiber təhlükəsizlik mübadiləsi sahəsində sübut olunmuş təhdidlər haqqında informasiya mübadiləsidir.
- Gələcəyin ən perspektiv sahələrindən biri olan Əşyalar İnternetinə informasiya təhlükəsizliyinin daha da gücləndirilmiş formasının tətbiqi ən vacib məsələlərdən biridir.
- Kritik infrastrukturların qorunması telekommunikasiya sistemlərində informasiya təhlükəsizliyinin tətbiqinin növbəti çox önəmli bir sahəsidir.

Summary

Thus, the study of "Information Security in Telecommunication Systems" showed how important it is to ensure the information security of telecommunications systems and facilities that play an important role in all areas of our lives, as well as our personal data, including our budgets. The scientific novelty of the research is based on the identification and generalization of the need for how and in what ways to ensure information security of telecommunication systems both historically and in the future, as well as in what promising areas through comparison, analysis, statistics and other research methods. The research database is based directly on the official website of the International Telecommunication Union, as well as scientific articles and books published by the union in different years. The results of the study can be summarized as follows.

- Information security in telecommunication systems is provided directly on the basis of the recommendations of the International Telecommunication Union.
- According to the latest recommendations of the Association, Design is considered to be more effective in protecting ICT assets for the modern era, trying to deal with security, new income and countermeasures produced in a hurry.
- One of the positive steps is the exchange of information on proven threats in the field of cyber security.
- One of the most important issues is the application of a more strengthened form of information security to the Internet of Things, one of the most promising areas of the future.
- Protection of critical infrastructures is another very important area of application of information security in telecommunication systems.

Резюме

Таким образом, исследование «Информационная безопасность в телекоммуникационных системах» показало, насколько важно обеспечить информационную безопасность телекоммуникационных систем и средств, которые играют важную роль во всех сферах нашей жизни, а также в наших личных данных, включая наши бюджеты. Научная новизна исследования основана на выявлении и обобщении необходимости того, как и каким образом обеспечить информационную безопасность телекоммуникационных систем как исторически, так и в будущем, а также в каких перспективных областях путем сравнения, анализа, статистики и другие методы исследования. База данных исследований основана непосредственно на официальном веб-сайте Международного союза электросвязи, а также на научных статьях и книгах, опубликованных профсоюзом в разные годы. Результаты исследования можно обобщить следующим образом.

- Информационная безопасность в телекоммуникационных системах обеспечивается непосредственно на основе рекомендаций Международного союза электросвязи.
- Согласно последним рекомендациям Ассоциации, дизайн считается более эффективным для защиты активов ИКТ в современную эпоху, пытаясь справиться с безопасностью, новыми доходами и контрмерами, созданными в спешном порядке.
- Одним из положительных шагов является обмен информацией о проверенных угрозах в области кибербезопасности.
- Одним из наиболее важных вопросов является применение более усиленной формы информационной безопасности к Интернету вещей, одной из наиболее перспективных областей будущего.
- Одним из наиболее важных вопросов является применение более усиленной формы информационной безопасности к Интернету вещей, одной из наиболее перспективных областей будущего.