O’ZBEKISTON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI VA KOMMUNIKATSIYALARINI RIVOJLANTIRISH VAZIRLIGI
TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

H i m o y a g a
kafedra mudiri
Irgasheva D.Y._____
«___»_____2015 y.

BAKALAVR BITIRUV ISHI

Mavzu: **“Korporativ tarmoqlarning himoyalanganlik darajasi va samaradorligini baholash”**

Bitiruvchi	_____ (imzo)	Kunarov Q.S. (F.I.O.)
Rahbar	_____ (imzo)	Tashev K.A. (F.I.O.)
Taqrizchi	_____ (imzo)	Abdullaev M.M. (F.I.O.)
HFX maslahatchisi	_____ (imzo)	Abdullaeva S.M. (F.I.O.)

Toshkent - 2015

O’ZBEKISTON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI VA KOMMUNIKATSIYALARINI RIVOJLANTIRISH VAZIRLIGI
TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

Fakultet *Kompyuter injiniringi*
Kafedra *Axborot xavfsizligi*
Yo’nalish (mutahasislik) *5330300 – Axborot xavfsizligi*

«TASDIQLAYMAN»
«AX» kafedra mudiri
*Irgasheva D.Y.*_____
«_____» _____ 2015 y.

Bitiruv malakaviy ishini bajarishga

TOPSHIRIQ

Kunarov Qobil Sobirovich

(familyasi, ismi, otasini ismi)

1. BMI mavzu: Korporativ tarmoqlarni himoyalanganlik darajasi va samaradorligini baholash

2. Universitet qarori bilan tasdiqlangan: «*17*» *yanvar 2015* y. № *59-15*

3. Ishini to’liq bajarish uchun berilgan vaqt: *20.03.2015*

4. Ishning boshlang’ich ma’lumotlari: *Mavzuga doir ilmiy - texnik adabiyotlar, Internet ma’lumotlari, Microsoft Visio 2010*

5. Hisob tushuntirish matni mundarijasi (ishni bajarilishdagi masalalar ro’yxati) *Mazmunnoma, kirish, nazariy qism, asosiy qism, hayot faoliyati xavfsizligi, xulosa, foydlanilgan adabiyotlar.*

6. Grafik materiallar ro’yxati: *Microsoft Office Power Point 2010 ilovasida tayyorlangan prezentatsiya slaydlari*

7. Topshiriq berilgan kun *20.01.2015 y.*

Rahbar _____
(imzo)

Topshiriqni oldi
_____
(imzo)

8. BIning har bir bo’limida bajariladigan ishlarga maslahatlar:

Bo’lim	Rahbar F.I.O	Imzo	
		Topshiriq berdi	Topshiriq oldi
Kirish	*Tashev K.A.*		
1-bo’lim	*Tashev K.A.*		
2-bo’lim	*Tashev K.A.*		
3-bo’lim	*Abdullaeva S.M.*		
Xulosa	*Tashev K.A.*		

9. Ishni bajarish grafigi:

	BMI bo’limlarining nomlari	Bajarish muddati	Bajarilganligi haqida rahbar imzosi
1.	*Kirish, masalaning qo’yilishi*	*23.01.15-28.01.15*	
2.	*Masalaning qo’yilishi, fan soxasining tahlili*	*29.01.15-14.02.15*	
3.	*Tahlil qilingan usullarni tadbiq etish*	*17.02.15-01.03.15*	
4.	*Hayot faoliyati xavfsizligi*	*17.03.15-27.03.15*	
5.	*Xulosa*	*28.03.15-29.03.15*	
6.	*Prezentatsiya slaydlarini ishlab chiqish*	*01.04.15-18.04.15*	
7.	*Dastlabki himoya*	*02.06.2015*	

Bitiruvchi _____ «_____» _____ 2015 y.
(imzo)

Rahbar _____ «_____» _____ 2015 y.
(imzo)

MUNDARIJA

Ushbu bitiruv ishi Korporativ tarmoqlarni arxitekturasi, ularni qurish texnologiyalari, xavfsizligiga bo’ladigan tahdidlar, hujumlarni tahlil etib, samarali chora-tadbirlar ishlab chiqish, hamda himoyalanganlik darajasini samaradorligini baholashga bag’ishlangan.

В данной выпускной работе рассматриваются архитектуры корпоративные сети, анализируется угрозы безопасности и мероприятий от атак, оцениваются уровень и эффективност безопасности.

This final qualifying work devoted to a corporate network architecture, it’s creation methods, vulnerabilities, threads and protection methods against it and calculating protection degree.

Kirish

Shiddat bilan rivojlanib borayotgan axborot texnologiyalari insoniyat hayotiga katta o’zgarishlarni olib kirdi. Deyarli barcha sohalarni qamrab olayotgan axborot texnologiyalari, insonlarning ajralmas bir qismiga aylanib ulgurdi. Rivojlangan davlatlar bilan hamkorlik qilish bozor iqtsodiyotining muhim talablaridan hisoblanadi. Bu borada korporativ tarmoqlarning sohada qo’llanilishi, elektron tijorat, ta’lim, sog’liqni saqlash hattoki qishliq xo’jaligi kabi tarmoqlarni qamrab oldi. Har bir sohani o’ziga yarasha ijobiy va salbiy tomonlari bo’lgani kabi, korporativ tarmoqlarning ham, o’ziga yarasha afzallik va kamchiliklari mavjud. 2015 yil 4 fevraldagi O’zbekiston Respublikasi Prezidentining ПФ-4702-sonli qarori, O’zbekiston Respublikasi axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligining tashkil etilishi sohaga bo’lgan etiborni muhimliligidan dalolat beradi.

Bakalavr bitiruv ishining maqsadi: Korporativ tarmoqlarning xavfsizligiga qaratilgan. Korporativ tarmoqlardagi zaifliklar va ularga bo’ladigan tahdid hamda hujumlarni tahlil etib samarali chora tadbirlarni ishlab chiqish va ulardan foydalanish. Himoyalangan korporativ tarmoqlarni monitoring qilish orqali himoyalanganlik darajasi va samaradorligini baholashdan iborat.

Bitiruv malakaviy ishi kirish, 3 ta qism, xulosa va foydalanilgan adabiyotlar ro’yhatidan iborat.

1-qism nazariy qism: Korporativ tarmoqlarni himoyalash muammolari, kompyuter tarmoqlarining ta’rifi, texnologiyalari va ularning topologiyalari. Korporativ tarmoqlarni qurish texnologiyalari, arxitekturasi hamda korporativ tarmoqlarga bo’ladigan tahdid, hujumlar va ulardagi zaifliklar keltirilgan.

2-qism amaliy qism: Himoyalangan korporativ tarmoq arxitekturasi, korporativ tarmoqda ma’lumotlar uzatish va qayta ishlash qismini himoyalash, WhatsUp-Gold dasturiy ta’minoti yordamida, korporativ tarmoqning himoyalanganlik darajasi va samaradorligini baholash ko’rib chiqilgan.

3-qismda hayot faoliyati xavfsizligi muammolari keltirilgan.

I.bob. Korporativ tarmoqlarni himoyalash muammolari

1.1. Komyuter tarmoqlari, tarmoq texnologiyasi va ularning topologiyalari

Kompyuter tarmoqlarining o’zaro aloqalari asosini tarmoq texnologiyalari tashkil etadi. Bu texnologiyalar tarmoqning o’lchami, uni shakillantirish qoidalari va tarmoqda ko’rsatiladigan xizmatlarga bog’liq ravishda xilma-xil bo’ladi. Cheklangan hududlarda ishlaydigan uncha katta bo’lmagan tarmoqlarda Ethernet, Token Ring, FDDI texnologiyalari ko’p tarqalgan. Shaharlar va mintaqaviy chegaralarda, katta masofalarda ishlaydigan tarmoqlarda Frame Relay, ATM kabi olisdan o’zaro aloqa texnologiyalari ishlatiladi. Komyuter tarmoqlarining kommunikatsion jihozlari passiv (kabellar, ulovchi razyomlar, kommutatsion panellar) va aktiv (tarmoq adapterlari, konsentratorlar, kommutatorlar, ko’priklar, mashrutizatorlar) kabi turlarga bo’linadi. Yordamchi turdagi jihozlarga uzluksiz elektr ta’minot qurilmalari, montaj uskunalari, kommutatsion jihozlarni joylashtirish shkaflari kiradi. Komyuter tarmoqlarining asosiy komponentalari serverlar, ishchi stansiyalar, terminallar, printerlar, tarmoq interfeysi bilan ta’minlangan audio va video aloqa vositalari hisoblanadi. Terminallar tarmoqning oxirgi elementlari hisoblanadi va ular orqali foydalanuvchilar kopyuter tizimining apparat, dasturiy yoki axborot resurslariga murojat etadilar. Bular grafik va alfavit raqamli qurilmalar va ish joylarida bo’lgan printerlar, skanerlar hisoblanadi. Ishchi stansiyalar ko’pincha shaxsiy kompyuterlar ko’rinishida tarmoqning resurslariga va tarmoq xizmatlarini foydalanuvchilarga murojat etish imkoniyatini ta’minlaydi. Ishchi stansiya ish joyining vazifalarini ta’minlash uchun dasturiy vositalarga (operatsion tizimlar), tarmoqning boshqa kompyuterlar bilan o’zaro aloqasi uchun tarmoq dasturiy komponentalari, shuningdek aloqa liniyalari bilan moslashtirish va ma’lumotlarni uzatishni ta’minlash uchun apparat kommunikatsion vositalariga (modemlar, tarmoq adapterlari) kiradi. Serverlar tarmoqlarning ishini boshqarish funksiyasini bajaradigan, axborot resurslarini saqlaydigan va foydalanishga beradigan, umuman tarmoqning ajratiladigan resurslariga ishchi stansiyalar

tomonidan murojat etishni ta’minlaydigan quvvatli kopyuterlardir. Tarmoqning ishlash jarayonida tarmoq bo’yicha uzatiladigan axborotlar oqimi trafik deyiladi. Trafik tushunchasiga ham oxirgi qurilmalar orasida uzatildigan foydali axborot hamda qabul qilingan protokollarga mos ravishda bog’lamalarining o’zaro aloqasini ta’minlaydigan xizmat axboroti kiradi. Tarmoqlarni qurishda muxim muammolardan biri axborotlar va paketlarini tezkor etkazish maqsadida kommutatsiyalash hisoblanadi. Trafikning tranzitli uzatilishini bajaradigan tarmoqning har bir bog’lamasi oxirgi foydalanuvchilar orasida trafikni kommutatsiyalashni bilishi kerak. Kommutatsiyalash texnologiyasiga tarmoq orqali axborot oqimlarini uzatish marshrutini tanlash prinsipi bevosita ta’sir qiladi. Marshrut bu ma'lumotlar belgilangan manzilga etib borishi uchun ular o'tishi kerak bo'lgan tarmoqning tranzit bog’lamalarining ketma-ketligidir. Axborot oqimlari foydalanuvchiga qisqa vaqtda minimal o'zgarish bilan yetkazilishi kerak. Kompyuter tarmog’ining dasturiy ta’minoti tarmoq operatsion tizimlari va ishlov berish amaliy dasturlari foydalanuvchiga tarmoqning apparat, dasturiy va axborot resurslariga murojat etish imkoniyatini beradi. Kompyuter tarmoqlari rivojlanib katta hududlarni egalladi, keng xizmat turlarini ko'rsatadigan bo'ldi, o'z tarkibiga yuqori unumli kompyuter va kommunikatsion vositalarini oldi. Egallangan hudud va xizmat ko'rsatiladigan abonentlar soni nuqtai nazaridan barcha kompyuter tarmoqlari shartli ravishda lokal (LAN-Local Area Network), mintaqaviy yoki shahar (MAN-Metropolitan Area Network) va global (WAN-Wide Area Network) tarmoqlarga bo'linadi[2].

Korxonalar, davlat muassasalari, kompaniyalar, ofislar, banklar, universitet binolarida va inshootlar doirasida ishlaydigan tarmoqlar lokal tarmoqlar deyiladi. Ularning asosiy vazifasi funksional bir xil foydalanuvchilarni (tarmoq abonentlarini) tarmoq orqali birlashtirishdan iborat. Odatda bular bugalteriya, kadrlar bo'limi, marketing xizmatlari, o'quv guruhlari, doimo qo'shma faoliyat olib boradigan tadqiqot laboratoriyalari hisoblanadi. Lokal tarmoqlar ma’lumotlarni uzatishning eng yuqori tezligini ta’minlaydi, chunki tarmoq bo'yicha uzatiladigan paketlar dastlabki ulanishning o'rnatilishini talab etmaydi. Lokal tarmoqlarda har

bir kompyuter o'zining tarmoq adapteriga ega bo'ladi, u ma’lumotlarni uzatish muhiti bilan bog’lashga xizmat qiladi.

Mintaqaviy yoki shahar tarmoqlari o'nlab va yuzlab kilometr masofalarga tarqalgan, uncha katta bo'lmagan ma’muriy hududiy bo'linmalarini qamrab oladi. Bunday tarmoqlar lokal tarmoqlarni bir-birlari bilan tejamkor ulanishini ta’minlaydi va global tarmoqlar bilan tezkor almashtirish magistrallariga ulanishlarga ega. Mintaqaviy tarmoqlarda foydalanuvchilarni ulash uchun aktiv kommunikatsion qurilmalar ishlatiladi.

Global tarmoqqa butun dunyo Internet tarmog’i misol bo'ladi. Bunday tarmoqlarda ma’lumotlarni uzatish tezligidagi farqdan tashqari boshqa mavjud farqlar bor. Global tarmoqlarda masofadan ma'lumotlarni uzatish uchun tezkor aloqa kanallari bilan birlashtirilgan marshrutizatorlar ishlatiladi [13]. Tarmoqning masshtabiga bog’liq bo'lmagan holda texnik va dasturiy komponentlarni majmualashtirib, tarmoqni yagona axborot tizimi sifatida ishlatishda bir necha majburiy shartlar bajarilishi kerak:

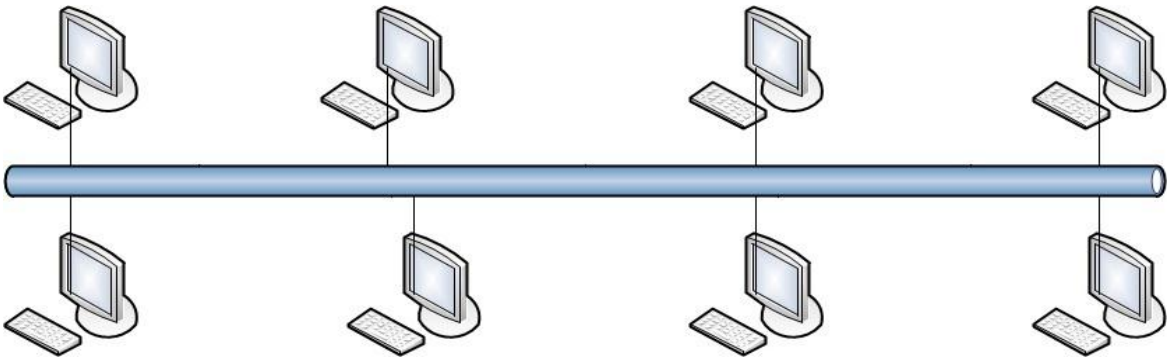
- tarmoq strukturasi, uning ish tartiblari va ma’lumotlar formatlari bilan mos ravishda funksional komponentlarning axborot moslashuvchanligi;
- qabul qilish-uzatish elementi turlari, signallarning chastota va dinamik diapazonlari, aloqa liniyalari bo'yicha uzatiladigan signallarning statik va dinamik parametrlarining elektr moslashuvchanligi;
- ulovchi elementlar interfeys qurilmalarining barcha turlarini konstruktiv moslashuvchanligi;
- kompyuterlarning dasturiy ta'minoti va kommunikatsion komponentlari pog’onasida interfeysning mavjudligi;
- foydalanuvchilar o'zaro ishlaganda yoki ularning umumiy resurslarga murojat qilishda almashtirish proseduralari va ma’lumotlar formatlarini aniqlaydigan qabul qilingan protokollar, standart qoidalar to'plamiga rioya etilishi.

Kompyuter tarmog’ining serverlari va ishchi stansiyalarining bir-birlariga nisbatan fizik joylashishi, ularni aloqa liniyalar bilan ulanish usuli va geometrik chizmasi topologiya deb tushuniladi. Topologiya tarmoqqa qo'yiladigan

talablardan qo'yidagilarga, ya'ni foydalanuvchilarga operativ va to'liq xizmat ko'rsatishga bog'liq bo'ladi. Kompyuter tarmoqlarini qurishda asosiy vazifalardan biri qurilmalarni elektrik va mexanik xarakteristikalari mosligini va kodlashtirish tizimlari, ma'lumotlar formati mosligini ta'minlash. Bu masalani yechish standartizatsiyalashtirish sohasiga tegishli [2]. Asosiy topologiyalar quydagilar:

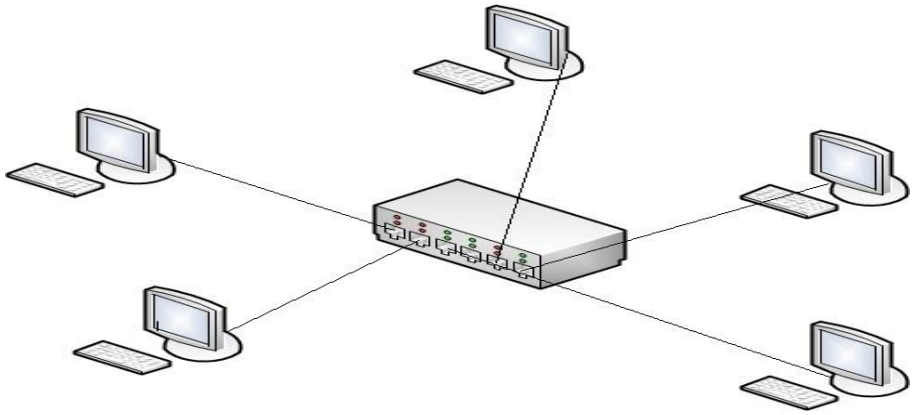
- Shina (*bus*);
- Yulduz (*star*);
- Halqa (*ring*).

Agar kompyuterlar bir kabel (segment) bo'ylab ulangan bo'lsa, bunday topologiya shina deb ataladi. Bu topologiya 1.1 rasmda keltirilgan.



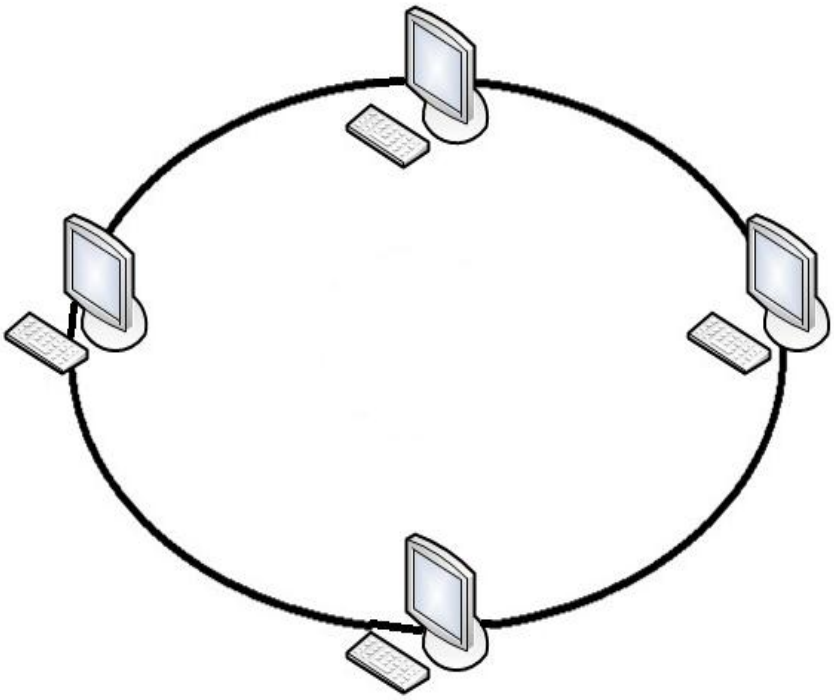
1.1 rasm. Shina topologiyasi

Agar kompyuterlar bir nuqtadan chiqqan segmentlarga yoki to'plagichga ulangan bo'lsalar, bunday topologiya yulduz deb ataladi. Bu topologiya 1.2 rasmda keltirilgan.



1.2 rasm. Yulduz topologiyasi

Agar kompyuterlar ulangan kabel halqa qilib ulangan bo’lsa, bunday topologiya halqa deb ataladi. Bu topologiya 1.3 rasmda keltirilgan.



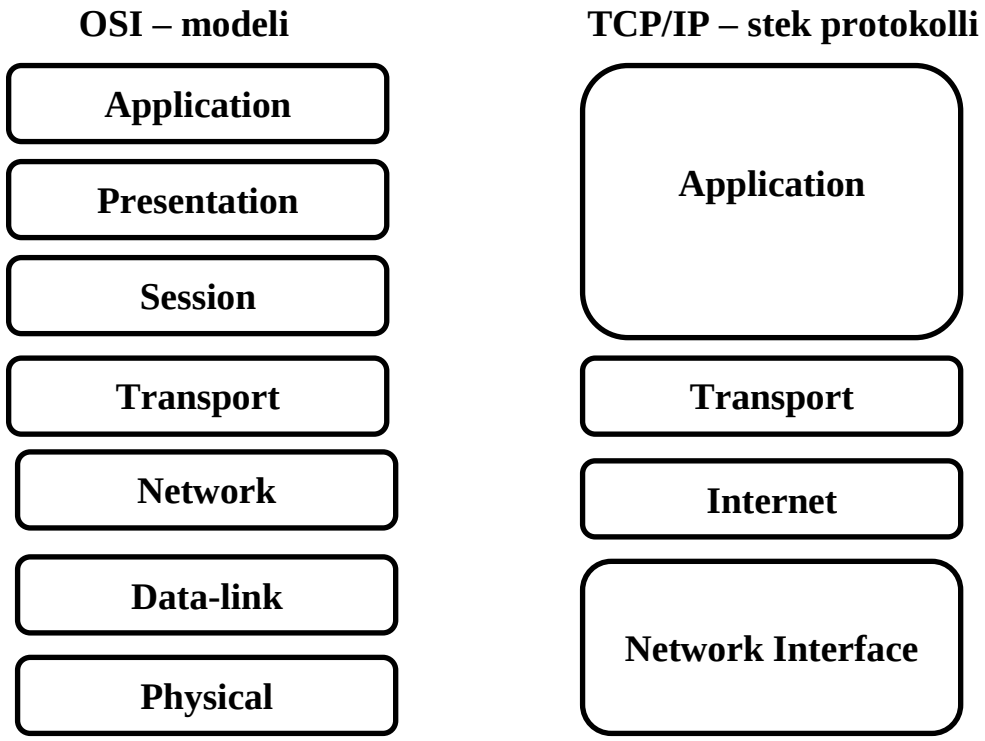
1.3 rasm. Halqa topologiyasi

1.1 - jadval

Topologiyalarning xususiyatlari

Topologiya	**Qulayligi**	**Kamchiligi**
Shina	- kabel tajaladi; - oson kengaytiriladi; - sodda va kafolatli.	- kabelni ishdan chiqishi, tarmoq ishini to’xtatadi; - ma’lumotlarni ko’pligi, o’tkazish qobilyatini pasaytiradi.
Yulduz	- kopyuterlar sonini oson ko’paytirish; - markazdan boshqarish va nazorat qilish; - biror kompyuterning ishdan chiqishi tarmoqqa ta’sir qilmaydi.	- markaziy konsentratorning ishdan chiqishi, tarmoqni ish faoliyatini to’xtatib qo’yadi.
Halqa	- barcha kopyuterlar bir xil mavqega ega; - foydalanuvchilar soni katta ahamiyatga ega mas.	- biror kompyuterning ishdan chiqishi, tarmoq faoliyatini to’xtatib qo’yadi; -tarmoq sozlanmalarini o’zgartirish, tarmoq ishini to’xtatadi.

Kompyuter tarmoqlarida asosiy metodik standartizatsiyalash, tarmoqlararo vositalarni ishlab chiqarishda ko’p darajali usulda yondashish. Bunday yondashuvlar va xalqaro standartlashtirish instituti ISO (International Standarts Organization) ning texnik takliflari asosida ochiq tizimlar o’zaro aloqasi standart modeli OSI (Open Systems Interconnection) TCP/IP stek protokolli ishlab chiqildi. Bu model satxlari 1.4 rasmda keltirilgan.



1.4 rasm. OSI modeli va TCP/IP stek protokolli

ISO/OSI modeli kompyuter tarmoqlari rivojida asosiy rol o’ynadi. OSI modelida o’zaro aloqa vositalari yettita sathga bo’linadi:

- ilova (Application);
- taqdim etish (Presentation);
- seans (Session);
- transport (Transport);
- tarmoq (Network);
- kanal (Data Link);
- fizik (Physical).

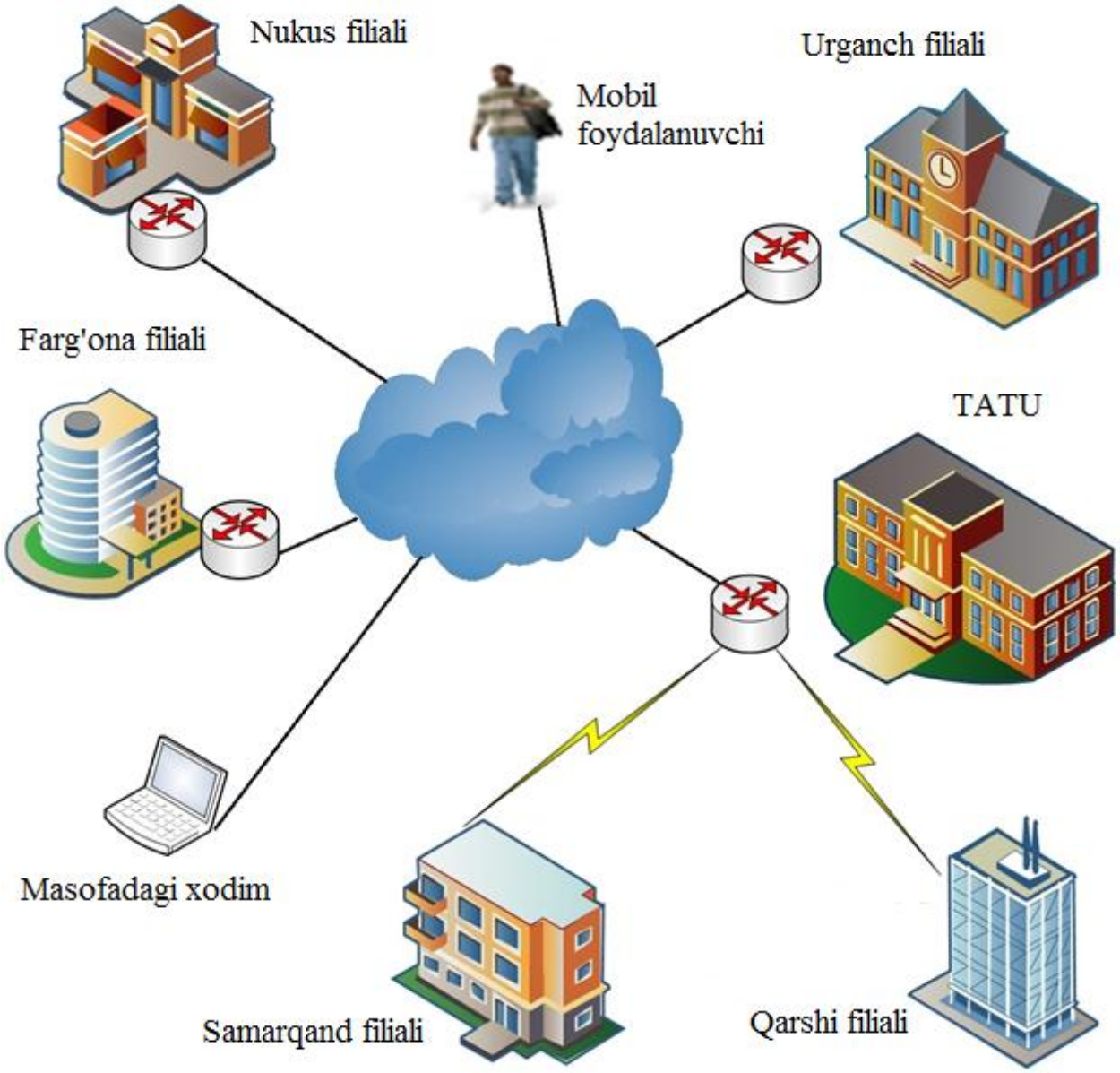
Eng yuqori daraja ilova darajasi hisoblanib, bunda foydalanuvchi dasturlar bilan ma’lumot almashadi. Eng quyi daraja esa, fizik daraja hisoblanadi. Bu darajada qurilmalar o’rtasidagi signal almashinuvini ta’minlaydi. Aloqa kanallari orqali ma’lumot almashinuvi ma’lumotning yuqori darajadan pastki darajaga uzatish, keyin aloqa liniyalari orqali transportirivka qilish va nihoyat mijoz kompyuterida ma’lumotni quyi darajadan yuqori darajaga uzatish orqali amalga oshiriladi.

TCP/IP protokolli maxsus global tarmoq uchun va tarmoqlar o'rtasidagi muloqotni olib borish uchun loyihalashtirilgan. U past sifatli aloqa kanallariga va xatolikka yo'l qo'yish ehtimoli katta tarmoqlarga mo'ljallangan. Bu protokoll dunyo kompyuter tarmog’i internetda qabul qilingan, abonentlarning ko'p qismi oddiy telefon aloqa yo'llariga ulanadilar. Uning asosida yuqoriroq bosqich protokollari ishlaydi, jumladan SMTP, FTP, SNMP protokollari. TCP/IP protkollarining kamchiligi kichik tezlikda ishlashi. Internet kabi katta tarmoqlarda tarmoqlararo axborot almashinuvi TCP/IP protokollar steki orqali amalga oshiriladi. TCP/IP protokollar stekining asosiy afzalligi uning har xil unumdorlikka ega bo'lgan tarmoq qurilmalari o'rtasida ishonchli aloqani ta'minlashida. TCP/IP protokollari xabarlarni uzatish mexanizmini taqdim qiladi, xabar formatini tavsiflaydi va xatoliklarga qanday ishlov berish kerakligini ko'rsatadi. Bu protokollar qurilma turiga bog’liq bo'lmagan holda ma'lumotlarni uzatish jarayonini tavsiflash va tushunish imkonini beradi [4].

1.2 Korporativ tarmoqlarni qurish texnologiyalari va ularning arxitekturasi.

Korporativ tarmoq bu xususiy firmalar ichidagi yoki firmalar o’rtasidagi kompyuter (Intranet) tarmog’idir. U internet tarmog’iga murojat qilishi mumkin, unda internet texnologiyasini ishlatilishi tufayli kengaytirilgan imkoniyatlarga ega, lekin tashqi foydalanuvchilar tomonidan punktlardagi resurslariga murojat qilishdan himoyalangandir. Uni lokal tarmoqlarni va internet tarmog’i vositalarini ishlatib, firmalar o’rtasidagi va firmalar ichidagi ma’lumotlarni saqlash, uzatish va

qayta ishlashni bajaradigan tizim kabi qarash mumkin. Korporativ tarmoq arxitekturasi 1.5 rasmda keltirilgan.



1.5 rasm. Korporativ tarmoq arxitekturasi.

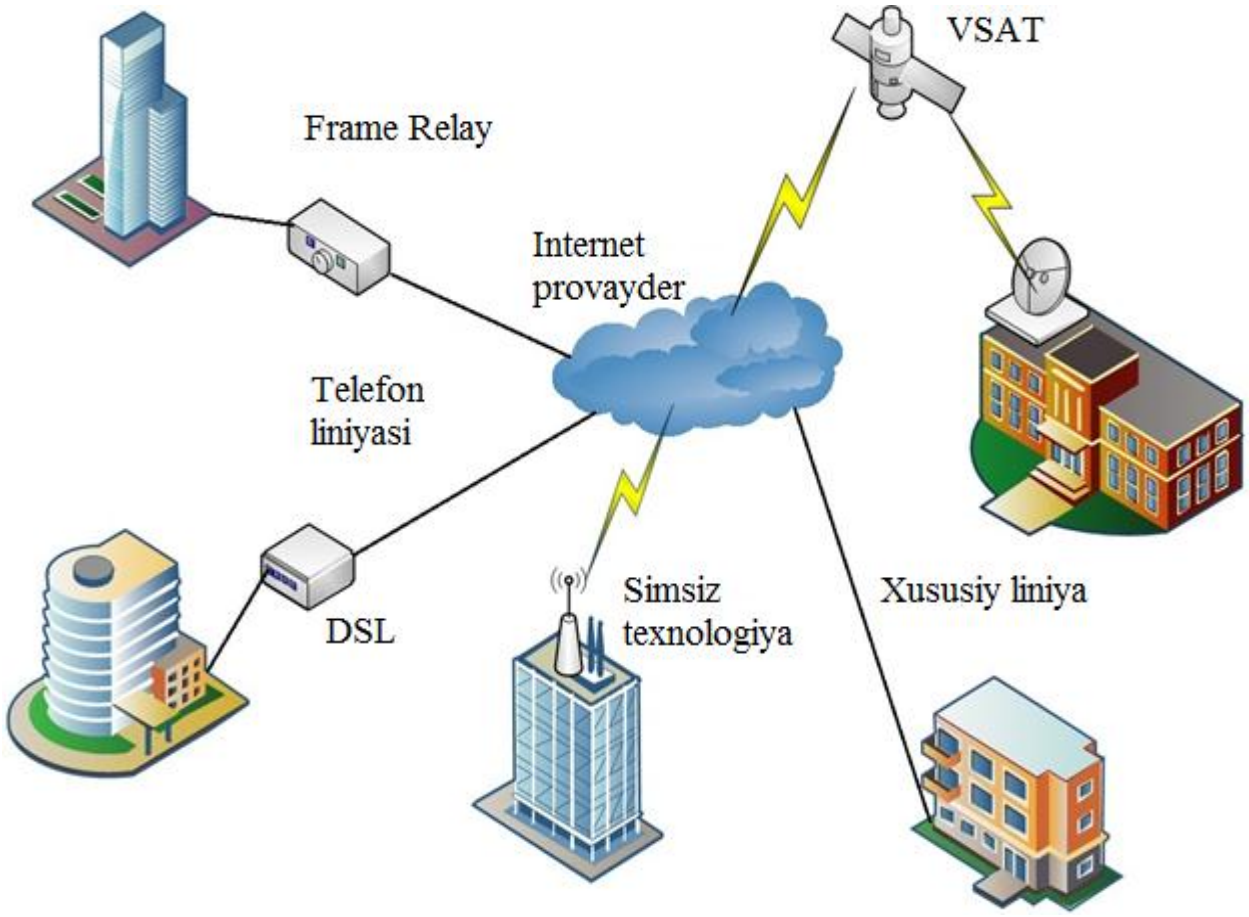
Intranet tarmog’i eng kamida quyidagi asosiy tarmoq texnologiyalarining bajarilishini ta’minlashi kerak:

- tarmoqni boshqarish;
- qolgan hamma xizmatlarni va resurslarni o’zida aks ettiruvchi tarmoq katalogi;
- tarmoqning fayl tizimi;

- axborotlarni integrallashgan uzatish (elektron pochta, faks, telekonferensiyalar va boshqalar);
- World Wide Web da ishlash;
- ma’lumotlarni ruxsat etilmagan murojat qilishdan himoya qilish.

Korporativ tarmoqlarni qurishda foydalaniladigan texnologiyalar va mexanizmlarga quydagilar kiradi:

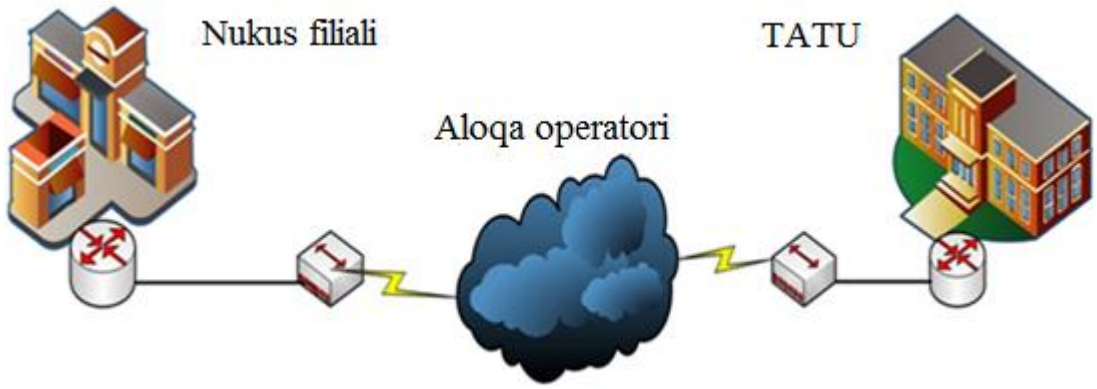
- xususiy yani alohida ajratilgan yoki ijaraga olingan liniyalar;
- internet - DSL simli va simsiz texnologiyalar ;
- kommutatsiyalangan tarmoq – Frame Relay, ATM, ISDN;
- VSAT-texnologiyasi. Bu texnologiyalar arxitekturasi 1.6 rasmda keltirilgan.



1.6 rasm. Korporativ tarmoqlarni qurish texnologiyalari

Xususiy yani alohida ajratilgan yoki ijaraga olingan liniyalar, optimal xavfsiz echim bo’lib xisoblanadi. Bu texnologiya o’tgan asrning 50-yillari

boshidan mavjud bo’lib nuqta – nuqta yoki ketma – ketlik deb ham atalgan. O’z nomi bilan ko’rinib turuibdiki ijaraga olingan liniya yoki kanaldan foydalangani uchun tashkilot aloqa operatoriga oylik to’lovlarni to’lab boradi. Bu kanallarning qiymati o’tkazuvchanlik qobilyati yani sifati va bog’lanadigan nuqtalar orasidagi masofaga qarab belgilanadi. Bu texnologiya arxitekturasi 1.7 rasmda keltirilgan.



1.7 rasm. Nuqta – nuqta texnologiyasi

Bu texnologiya asosida korporativ tarmoqlarni qurishda PPP yoki HDLC protokollaridan foydalaniladi.

Ajratilgan liniyalar afzalliklari:

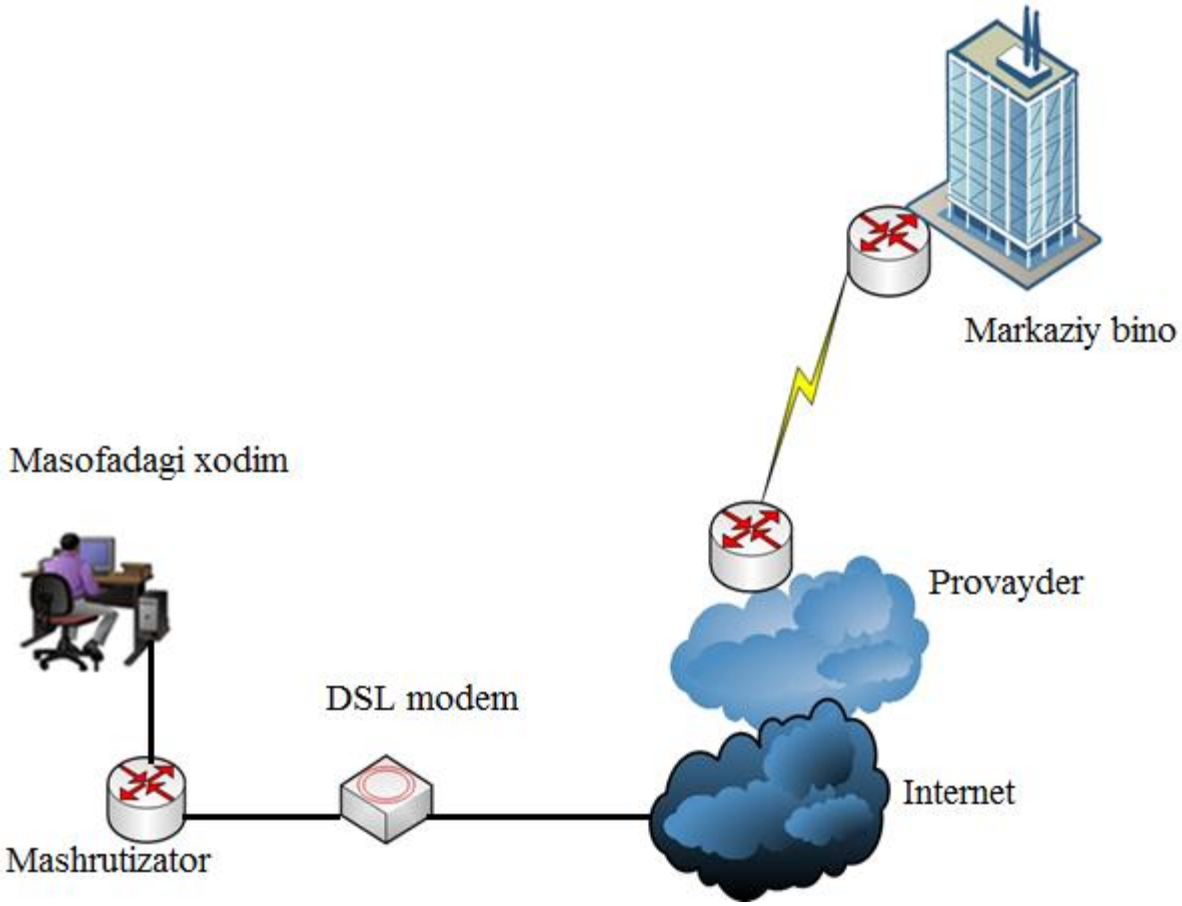
- oddiyligi, tarmoqlar montaji va bunday "nuqta-nuqta" kabi aloqa kanallarini ta'mirlash minimal tajriba talab qiladi;
- sifati yuqori ma’lumotlarni uzatishda kechikish va xatoliklarni bartaraf etilganligi;
- qulay har doim aloqani mavjudligi, muhim ahamiyatga ega bo’lib IP orqali VoIP yoki video uzatish uchun doimiy hisoblanadi.

Ajratilgan liniyalar kamchiliklri:

- qiymati jixatdan qimmat xisoblanadi, chunki xar bir nuqtani ulash uchun uskuna va yo’riqnoma bo’yicha interfeys talab qilinadi.

DSL (domain specific language) – texnologiyasi doimiy aloqani ta’minlsh uchun telefon liniyalari asosida ishlaydi. DSL modemi Ethernet tarmog’idan kelgan signalni o’zgartirib bog’langan nuqtaga uzatadi. Bu texnologiya juda qulay

xisoblanib korxona yoki tashkilotlar o’z xodimlarini uy sharoitida, masofadan turib ishlashlarini qo’llab quvatlaydi. Bu texnologiya 1.8 rasmda keltirilgan.



1.8 rasm. DSL texnologiyasining arxitekturasi

Masofadagi xodim to’gridan to’g’ri korporativ tarmoqqa ulana olmaydi. Birinchi novbatda alqa operatori orqali internet provayderiga, undan so’ng internet orqali IP adresdan foydalangan holda korporativ tarmoqqa ulanishi mumkin. Bu jarayon xavfli xisoblanib, xavfni bartaraf etish uchun xavfsizlik chora tadbirlardan foydalaniladi.

DSL texnologiyasi afzalliklari:

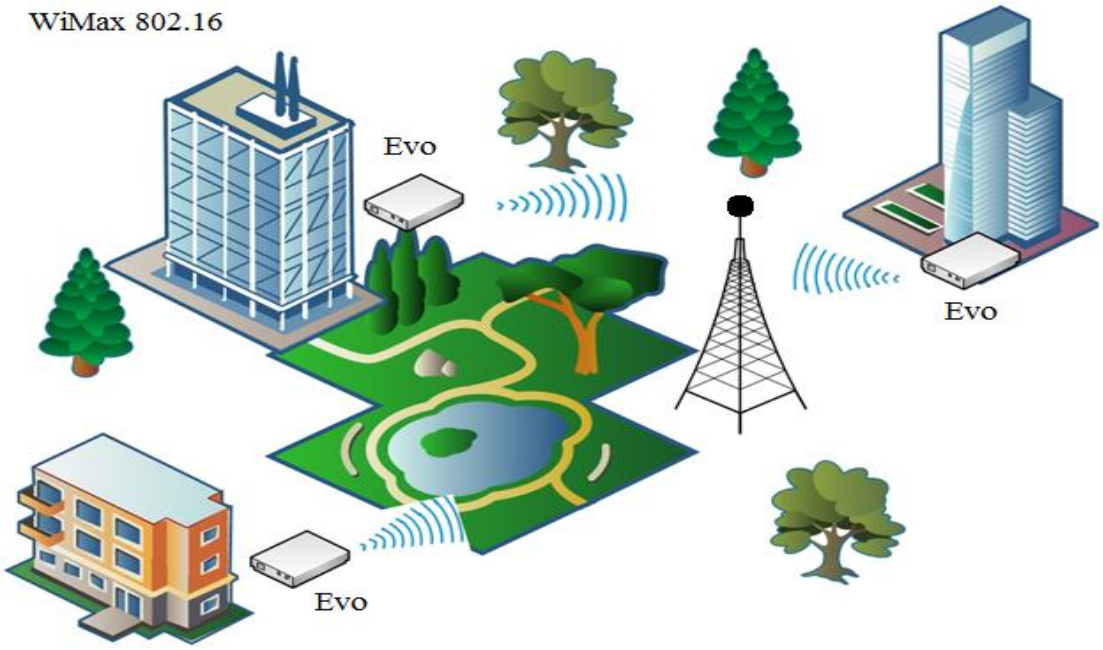
- qulay tarmoqni qurishda yuqori tajriba talab etmaydi;
- arzon DSL modem ishlatiladi, qo’shimcha interfeyslar talab etilmaydi;

DSL texnologiyasi kamchiliklri:

- xavfsiz hisoblanadi chunki o’rtada internet vositasidan foydalaniladi;
- ma’lumotlarni uzatishda kechikish va xatoliklarning mavjudlig.

Simsiz texnologiyalar ma’lumot uzatishda qulay echimlardan hisoblanib, ma’lumot va axborotlarni uzatishda radio chastotalardan foydalaniladi. Bu texnologiya 1.9 rasmda keltirilgan bo’lib, quydagi versiyalari mavjud:

- Bluetooth – 802.15, xizmat ko’rsatish masoofasi 100 metr;
- Wifi – 802.11a/b/g/n, xizmat ko’rsatish masofasi 300 mert;
- WiMax – 802.16, xizmat ko’rsatish masofasi 50 kilomert.



1.9 rasm. WiMax texnologiyasi asosida qurilgan topologiya

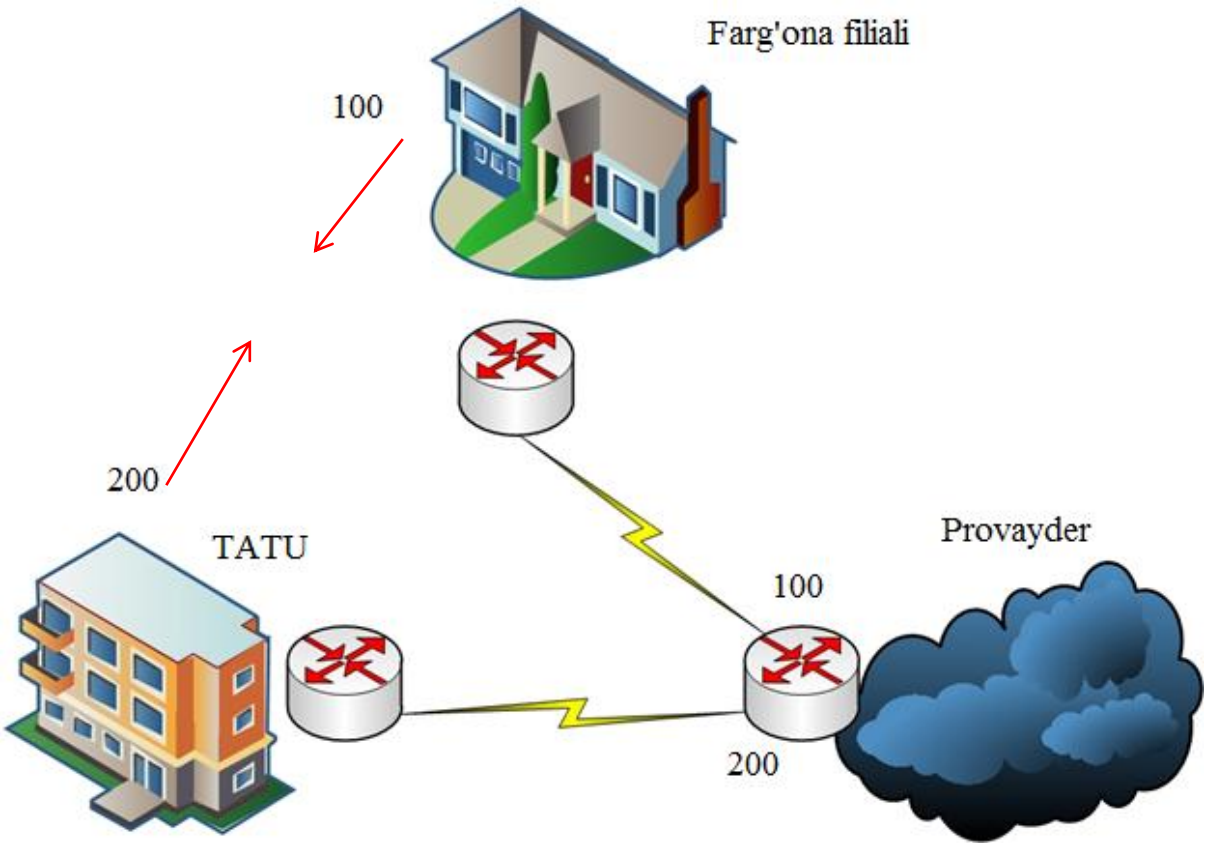
Quydagi rasmda keltirilgan topologiyada WiMax 802.16 texnologiyasidan foydalanilgan. Bu texnologiya samarali xisoblanib ma’lumotlarni uzatishda kechikishlar yo’qligi, tezlikning yuqoriligi, xizmat ko’rsatish polosasining kengligi, uy sharoitidagi xodimlarning korporativ tarmoqqa ulanishlarini qo’llab quvataydi. Simsiz texnologiyasi afzalliklari:

- tarmoq qurishda kabellardan foydalanilmaydi, tog’li hududlarda aloqani o’rnatish qulayligi;

Simsiz texnologiyasi kamchiliklri:

- ma’lumot yoki axborotlar ochiq nazoratlanmaydigan hududlar orqali yuborilishi xavfsiz hisoblanadi va noqulay ob – havoning ta’sir etishi.

Frame Relay texnologiyasi tashkilot yoki korxonalarni filialari bilan bog’lanishlari uchun internet povayderi orqali amalga oshiriluvchi texnologiya hisoblanadi. Yani bu tarmoq qurishdagi OSI modelining kanal satxida amalga oshiriladi. Bu texnologiya 1.10 rasmda keltirilgan.



1.10 - rasm. Frame – Relay topologiyasi

Bu topologiyada TATU o’z filiali bilan bog’lanishi uchun internet provayderga murojat qiladi, o’zi va filliali uchun belgilangan identifikatori orqali bog’lanishni amalga oshiradi.

Frame Relay texnologiyasi afzalliklari:

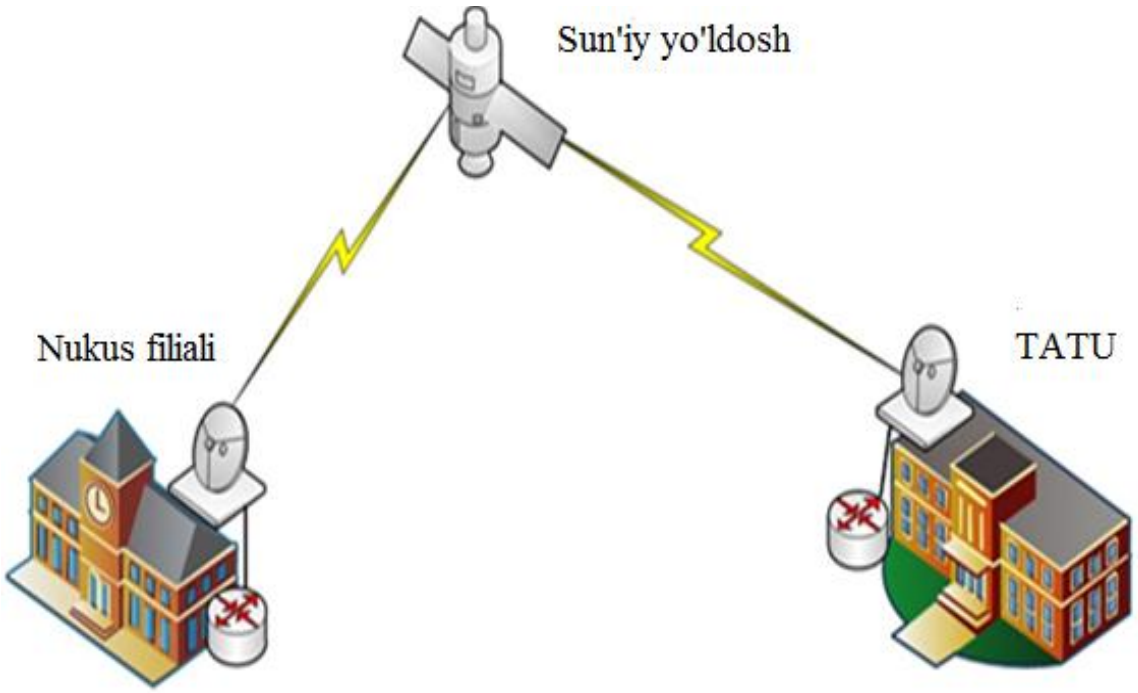
- korporativ tarmoqlarni bir – biri bilan bog’lashda qulay yoki oddiy usullardan xisoblanadi;
- yuqori tajriba va amallarni talab qilmaydi;
- qo’shimcha qurilma yoki interfeyslarni talab etmasligi.

Frame Relay texnologiyasi kamchiliklari:

- ma’lumot yoki axborotlar almashishagi kechikish, tezlikning pastligi;

- qiymati jixatdan qimmatroq hisoblanadi chunki xar bir filial uchun aloxida identifikator ishlatiladi.

VSAT (Very Small Aperture Terminal) - texnologiyasi uzoq masofada joylashgan filliallarni bog'lashda samarali hisoblanadi. Bunda yerning sun'iy yo'ldoshidan foydalanilgan holda uzoq masofada joylashgan korporativ tarmoqlar orasida o'zaro aloqani hosil qilishimiz mumkin. Bu texnologiya 1.11 rasmda keltirilgan.



1.11 rasm.VSAT texnologiyasi

Mashrutizatorlar antennaga ulangan holda orbitada joylashgan yerning su'niy yo'ldoshi orqali minglab kilometr uzoqlikda joylashgan filiallari bilan o'zaro aloqani ta'minlaydilar. Bu texnologiya juda samarili hisoblanib o'z o'rnida qiymati jihatidan juda qimmat hisoblanadi [12].

1.3 Korporativ tarmoqlarga bo'ladigan tahdid, hujumlar va ulardagi zaifliklar

Korporativ tarmoq yoki axborot tizimi doirasidagi axborotlrga ta'sir qiluvchi xavfsizlik tahdidlari 4 xil obyektlarga qaratiladi. Bu obyektlarga qaratilgan tahdidlar 1.2 jadvalda keltirilgan:

1.2 jadval

Axborot tizimi tarkibidagi axborotlar va axborot resurslariga bo’ladigan xavfsizlik tahdidlari

Axborot tizimi doirasidagi xavfsizlik tahdidlari ta’sir qiladigan obyektlar	Axborot tizimi tarkibidagi axborot resurslari, jarayonlar va dasturiy ta’minot.	va ularning turlari:	- axborotlarning obro’sizlantirilishi; - ma’lumotlar va dasturlarning ruxsatsiz o’zgartirilishi; - ishlash qobilyatiga salbiy ta’sirlar; - dasturiy (virusli) tahdidlar.
	Axborot tizimi ichida uzatilayotgan ma’lumotlar.		- axborot tizimidagi ma’lumotlar oqimining ochilishi; - axborot tizimidagi ma’lumotlar oqimining almashtirilishi.
	Kommunikatsiya qurilmalari(KQ).		- KQ ichidagi dasturiy ta’minotning buzilishi hamda KQ va unga ulangan kompyuterlarning ishdan chiqarilishi; - Paketlarni noto’g’ri manzilga jo’natilishi, ularning yo’qotilishi, hamda almashib qolishi; - KQ uzatayotgan paketlarga viruslarning joylashtrilishi; - tarmoq foydalanuvchilari almashayotgan ma’lumotlarning xususiyatlarini aniqlash maqsadida foydalanuvchilar faolligini nazorat qilish.
	Tizimlararo axborot almshish tizimlari (electron pochta).		- jo’natuvchilarning yolg’on manzillari; - xatlar va jo’natmalarni kuzatib o’qib boorish; - pochta bombalari.

Eng xavfli insidentlar:

- atayin (g‘arazli maqsadlarda) kompyuter viruslarini tarqatish;
- milliy axborot tarmoqlari va hostlarini skanerlash;

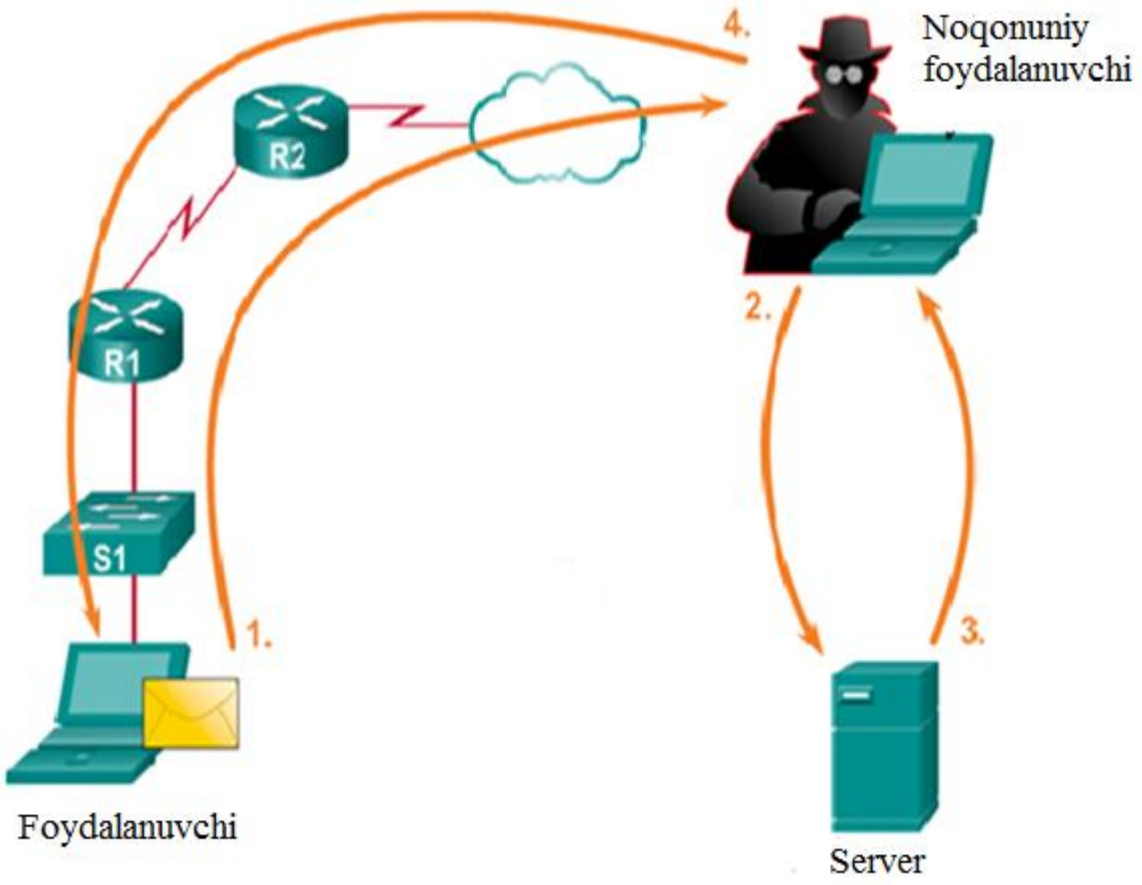
- tarmoqning asosiy tugunlari va yirik server resurslariga ularning faoliyatini izdan chiqarish, buzib kirish yoki tizim ma'lumotlarni sifatsizlantirishga qaratilgan xavf-xatarlar;
- tarmoq boshqaruvidagi ustuvorliklarni qo‘lga kiritishga yo‘naltirilgan turli tahdidlar; milliy axborot resurslari va ayrim hostlarga DoS (Denial of Service) va DDoS (Distributed Denial of Service) tahdidlari;
- axborot tarmoqlari xavfsizlik tizimini buzib kirish, shu jumladan, zararli dasturlarni xufiyona "joriy etish" yo‘li bilan;
- parol va boshqa autentifikatsiya ma'lumotlarini tanlash hamda qo‘lga kiritish;

Kompyuter tizimi yoki tarmog’i himoyasini buzishga urinishlarni kompyuter tizimini axborotni ta'minlovchi ob'ekt sifatida ko'rish orqali klassifikatsiyalash mumkin. Umumiy holda qandaydir manbadan(masalan, fayl yoki xotira qismi) axborot oqimining adresiga(masalan, boshqa fayl yoki bevosita foydalanuvchi) uzatilishi kuzatiladi. Shu nuqtai nazardan quyidagi hujumlarni farqlash mumkin:

- Uzish;
- Ushlab qolish;
- Turlash;
- Soxtalashtirish.

Ushlab qolish - resursdan ruhsat berilmagan foydalanishga yo'l ochiladi. Natijada axborotning maxfiyligi (konfidensialligi) buziladi. Bunday foydalanuvchilar fizik shaxs, programma yoki kompyuter bo'lishi mumkin.

Turlash - resursdan nafaqat noqonuniy foydalanishga yo'l ochiladi, balki resurs buzgunchi tomonidan o'zgartiriladi. Natijada axborotning yaxlitligi buziladi. Bunday uzilishlarga misol tariqasida fayldagi ma'lumotlar mazmunini o'zgartirilishini, programmaning vazifalari va xarakteristikalarini o'zgartirish maqsadida uni modifikatsiyalashni, tarmoq orqali uzatilayotgan axborotlar mazmunini o'zgartirilishini ko'rsatish mumkin. Bu tarmoq hujumlari haqida quyidagi 1.12 rasmda ko’rsatib o’tilgan.

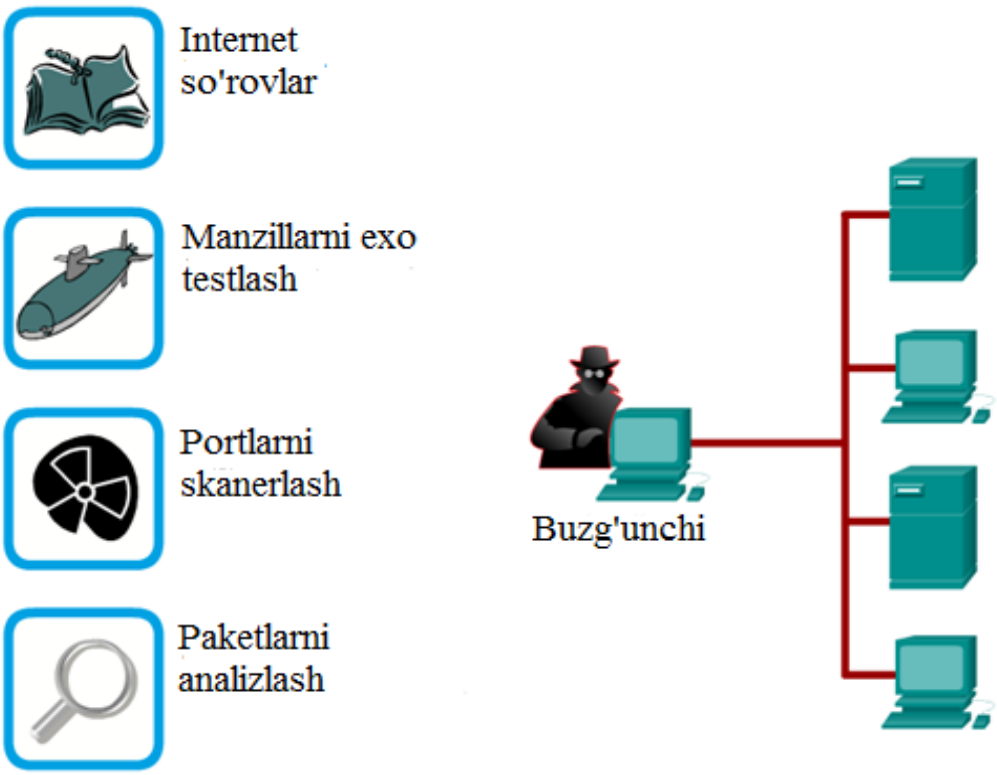


1.12 rasm. Ushlab qolish, turlash va soxtalashtirish

Soxtalashtirish - tizimga soxta ob'ekt kiritiladi. Natijada axborotning asliga to'griligi buziladi. Bunday buzilishlarga misol tariqasida tarmoq orqali yasama ma'lumotlarni uzatish yoki faylga yozuvlarni qo'shishni ko'rsatish mumkin. Yuqorida keltirilgan buzilishlar passiv va aktiv hujum atamalari bo'yicha klassifikatsiyalanganida passiv tahdidga ushlab qolish mansub bo'lsa, uzish, turlash va soxtalashtirish aktiv tahdidga mansub ekanligini ko'rishimiz mumkin.

Tarmoq razvedkasi - umumfoydalaniladigan ma’lumot va ilovalar yordamida axborot to’plashdir. Odatda buzg’unchi biror bir tarmoqqa hujum qilisdan oldin u xaqida iloji boricha ko’proq axborot to’plashga xarakat qiladi. Tarmoq razvedkasidan butunlay qutulib bo’lmaydi. Masalan exo icmp va pereferiya mashrutizatoridagi exo javobni uzib qo’ysa, siz exo testlashdan xalos bo’lasiz, ammo tarmoqda ro’y beradigan nosozliklarni diagnostika qilish uchun

zarur bo’lgan ma’lumotlarni yo’qotasiz [3]. Bu tarmoq hujumlari haqida quyidagi 1.13 rasmda ko’rsatib o’tilgan.

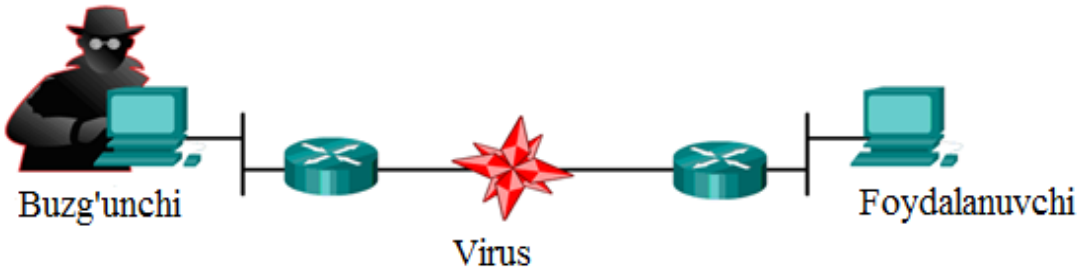


1.13 rasm.Tarmoq razvedkasi

Tarmoq razvedkasi DNS so’rov exo testlash, paketlarni maxsus analizator dasturlar yordamida analiz qilish va portlarni skanerlash natijasida bajariladi. DNS so’rovlar u yoki bu domenning egasi kimligi va bu domenga qaysi adreslar berilganligini tushinishga yordam beradi. DNS yordamida fosh etilgan manzillarni exo testlash ushbu muhitda qaysi hostlar real ishlayotganligini real ko’rishga imkon beradi. Hostlar ro’yxatini qo’lga kiritib, ushbu hostlar madatlaydigan xizmatlarning to’liq ro’yxatini tuzish maqsadida buzg’unchi portlarni skanerlash vositaaridan foydalanadi. Natijada buzish uchun foydalanish mumkin bo’lgan axborot qo’lga kiritiladi [3].

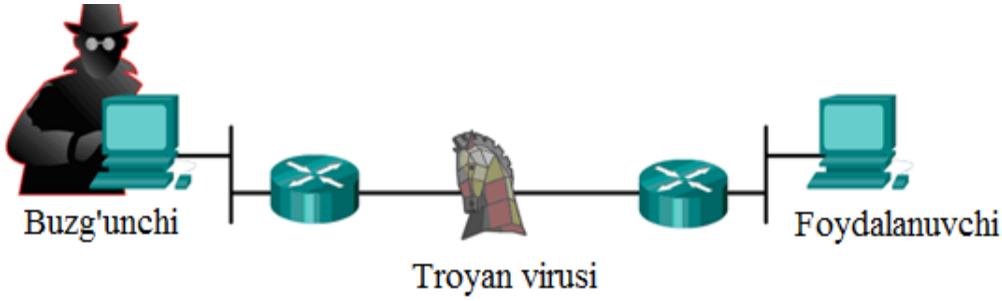
Virus – bu dasturchi tomonidan tuzilgan, kompyuter ish faoliyatini tekis ishlashiga halaqit beradigan, oqibatda kompyuterni yoqilishini ham taqiqlab qo’yadigan dasturdir. Bu dasturlar asosan internet tarmog’i orqali foydalanuvchi komyuteriga tushadi. Albatta, bu dastur, internet foydalanuvchisi bilmagan holda

o’z komyuterida paydo bo’ladi. Viruslar, troyanlar va qurtlarni zararli kod yordamida tarmoqqa tarqatadilar. Bu hujum 1.14 rasmda keltirilgan.



1.14 rasm. Virus hujumi

Troyanlar (Trojan Horses) – Qadimgi yunonlarning Troyaga yurishlari davrida qo’llagan hiylasi, ya’ni troyaliklarni otga ishqiboz ekanligidan foydalanib, ularga katta yog’och ot sovg’a qilishlari va bu otning troyaliklar mag’lubiyatiga olib kelishi voqeasidan olingan nom. Bu hujum 1.15 rasmda keltirilgan.

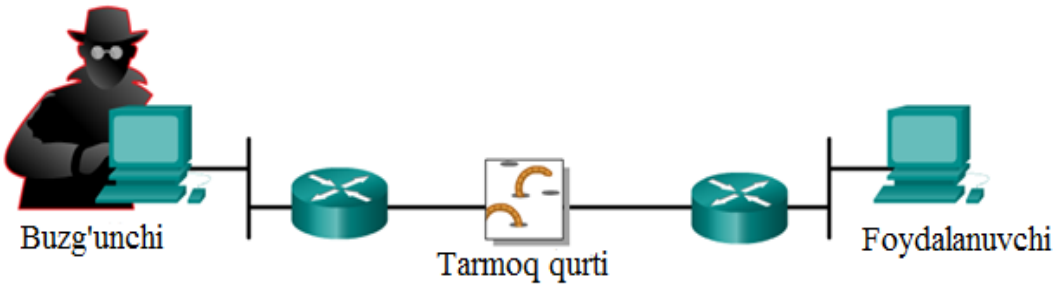


1.15 rasm. Troyan virusi

Troyanlar odatda internet orqali tarqaladi. Troyanlar kompyuteringizga o’rnashib olib, dastlab foydali programma sifatida o’zlarini tanishtiradilar, lekin ularning asl vazifasi foydalanuvchiga noma’lumligicha qoladi. Yashirin ravishda ular o’zlarining yaratuvchisi **(**cracker – yovuz haker**)** tomonidan belgilangan harakatlarni amalga oshiradilar.

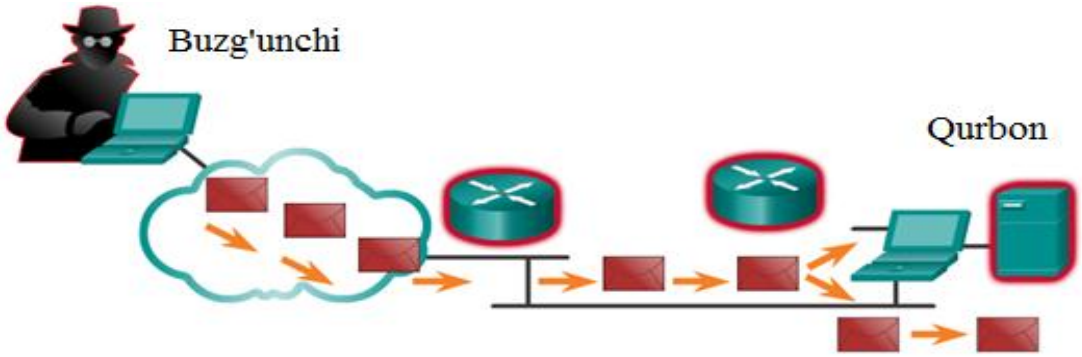
Tarmoq qurtlari (Worms) – o’z nomiga mos ravishda juda tez o’z-o’zidan ko’payadigan viruslardir. Odatda bu viruslar internet yo’li intranet tarmoqlari orasida tarqaladi. Tarqalish usuli sifatida elektron xatlar yoki boshqa tez tarqaluvchi mexanizmlardan foydalanadi. Ular haqiqatan ham kompyuteringizdagi ma’lumotlar va kompyuter xavfsizligiga katta ziyon yetkazadi. Tarmoq qurtlari

operatsion tizimning nozik joylaridan foydalanish yoki zararlangan elektron xatlarni ochish yo'li bilan kompyuteringizga o'rnashib olishi mumkin. Bu hujum 1.16 rasmda keltirilgan.



1.16 rasm. Tarmoq qurti virusi

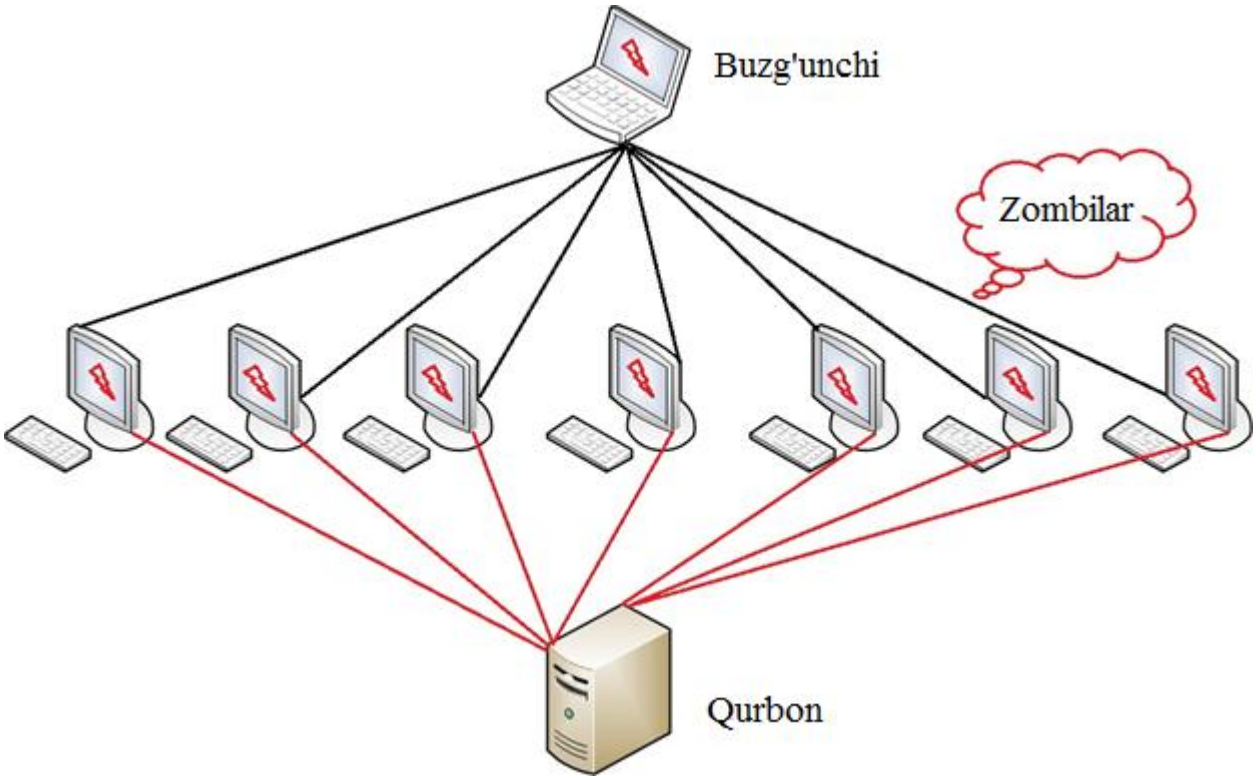
Xizmat ko'rsatishdan voz kechishga undaydigan hujumlar DOS (Denial of Service) hujumlar dab ham yuritiladi. Bu turdagi hujum boshqalaridan farq qiladi. Uning maqsadi qandaydir ruxsatsiz foydalanish yoki nusxa olish emas. Bu turdagi hujumlar operatsion tizimlar, ilovalarni va tarmoqni ishlashini ruxsat etilgan chegaralaridan oshib ketishi hisobiga tashkilot tarmog'idan oddiy foydalanuvchilarni foydalana olmaydigan qilib qo'yadi. Bu hujum 1.17 rasmda keltirilgan.



1.17 rasm. DOS hujumi

Ko'p hollarda tizim arxitekturasining zaif joylaridan foydalaniladi. DOS – hujumlarni oldini olish juda qiyin. Buning uchun xarakatlarni provayder bilan muvofiqlashtirish zarur. Agar sizni tarmog'ingiz to'lib toshishiga mo'ljallangan trafikni provayderda to'xtatilmasa, tarmoqning kirishida uni to'xtatib bo'lmaydi. Chunki hamma o'tkazish polosasi band bo'ladi. Agar hujum bir vaqtda ko'plab

qurilmalar orqali xizmat ko’rsatishga voz kechishga undaydigan taqsimlangan hujumlar DDOS (Distributed Denial of Service) deb yuritiladi. Bu hujum 1.18 rasmda keltirilgan.



1.18 rasm. DDOS xujumi

Bu hujum, hujum qilinayotgan tizim ishdan chiqunga qadar unga kema – ket ko’p sondagi so’rovlar jo’natilaveradi. Ishdan chiqish turi severning turi, texnik ko’rsatkichlari va imkoniyatlariga bog’liq bo’ladi [4].

Korporativ tarmoqlarda quydagi zaifliklar mavjud bo’lganda hujumlar amalga oshirilishi mumkin:

- axborot tizimi va ma’lumot uzatish tarmog’i qurilmalarining himoyasi mavjud tahdidlarga mos emasigi;
- ma’lumotlarning tizim doirasida ochiq holda uzatilishi;
- ma’lumotlarning tizim doirasida keng qamrovli etkazish protokollari yordamida tarqalishi;
- foydalanish imkoniyatlarini boshqarish dasturlardagi sozlanmalar hamda texnik ko’rsatmalardagi xatoliklar;

- shifrlash uchun etarli darajada muhim bo’lsada, shifrlanmagan holda saqlanuvchi ma’lumotlar;
- dasturlarning shifrlanmagan holda saqlanuvchi birlamchi matnlari;
- tarmoq qurimalari sozlanmalaridagi xatoliklar va ochiq qoldirilgan portlar;
- ochiq xonalarda saqlanuvchi ma’lumotlar va dasturiy ta’minotning zaxira nusxalari.

Ma’lumotlar va dasturlarning ruxsatsiz o’zgartirilishi axborot tizimida quydagi zaifliklar mavjud bo’lganda amalga oshirilishi mumkin:

- ma’lumotlarni faqatgina o’qishga ruxsati bor foydalanuvchilarga o’zgartirish imkoniyati berilganligi;
- dasturuy ta’minotga aniqlanmagan o’zgartirishlarning shu jumladan, “troya otlari” ni yaratuvchi dasturlarning kiritilganligi;
- ortiqcha yozuvlarga ruxsat beruvchi imtiyozlar mexanizimining mzvjudligi va viruslarni aniqlash hamda ulardan himoyalanish vositalarining yo’qligi [5].

II.bob. Himoyalangan korporativ tarmoq arxitekturasi

2.1. Himoyalangan korporativ tarmoqlarni qurishda yondoshishlar

Himoyalangan korporativ tarmoq va uni xavfsizlik tizimini saqlab qolish tizimli yani kompleks yondashuvni talab qiladi. Bu yondashishga muvofiq, siz birinchi alohida tarmoqda mumkin bo’lgan tahdidlarni to'liq tahlil qilib va bu tahdidlarning har biri uchun, himoyalanish taktikasini ishlab chiqishingiz lozim. Bu tahdidlarga qarshi kurashishda eng samarali usullar va ishonchli vositalardan foydalanish bular:

- dasturiy va apparat;
- tashkiliy va qonun chiqaruvchi;
- ma'muriy va psixologik mudofa hisoblanadi.

Qonunchilik himoya vositalari - qonunlar, hukumat qarorlari va Prezident farmonlari, foydalanish va cheklangan ma'lumotlar tashish qoidalarini boshqarishni, shuningdek, ushbu qoidalarni buzganlik uchun javobgarlik va jarimalar solish orqali.

Ma'muriy choralar - kompaniya yoki tashkilot rahbariyati tomonidan qabul qilingan umumiy ish hisoblanadi. Korxonada tashkil etilgan axborot xavfsizligi siyosati, quydagilarni o’z ichiga olishi kerak:

- ma'lumotlarni muhofaza qilish ishlarini to’g’ri tashkil etish;
- qanaqa ma'lumot va uni kimdan himoya qilish kerak;
- kimga va qanday ma'lumotdan foydalanish huquqini, vazifalarini taqsimlash;
- ma'lumotlarning har bir turi uchun talab qilinadigan himoyalash vositalari.

Tashkiliy (yoki protsessual) xavfsizlik choralari, masalan, xodimlar uchun maxsus qoidalar, kompyuteringizda maxfiy axborotni tashishning aniq tartibi.
Ma'naviy va axloqiy qoidalar muayyan bir mamlakatda hisoblash resurslarini tarqalishi bilan tashkil etildigan barcha turdagi qoidalar. Axborot xavfsizligi texnik va dasturiy vositalari tasniflanishiga ko’ra quydagilarga bo’linadi:

- auditorlik vositalari;

- axborotlarni shifrlash;
- identifikatsiya, autentifikatsiya va avtorizatsiya shu jumladan erkin foydalanishni nazorat qilish tizimlari;
- hujjatlarni hisobga olish aniqlash uchun ishlatiladigan raqamli imzo tizimi;
- hujjatlarni yaxlitligini isbotlash vositalari;
- anti-virus vositalari;
- xavfsizlik devorlari.

Yuqoridagi xavfsizlik chora-tadbirlari barcha tizim dastur va tarmoq aloqa qurilmalari, axborotlarni, operatsion tizimlarni himoyalsh uchun mo'ljallangan yondoshishlar hisoblanadi. Tashkilotlarda himoyalash bilan bog'liq bo'lgan muammolarni echish uchun aksariyat hollarda qisman yondashishlardan foydalanishadi.

Bu yondoshishlar, odatda, avvalo foydalana oluvchi resurslarning joriy darajasi orqali reaksiya ko'rsatishadi. Aslida xavf-xatarlar juda ko'p bo'lishi mumkin. Undan tashqari, xavfsizlik ma'murlari ko'pincha o'zlariga tushunarli bo'lgan xavfsizlik, xavf-xatarlariga qat'iy joriy nazorati va xavfsizlikning umumiy siyosatini ta'minlovchi kompleks yondashish xavf-xatarlarini anchagina kamaytirishi mumkin.

Oxirgi vaqtda turli kompaniyalar tomonidan qator yondoshishlar ishalab chiqildiki, bu yondashishlar nafaqat mavjud zaifliklarni aniqlashga, balki o'zgargan eski yoki paydo bo'lgan yangi zaifliklarni aniqlashga va ularga mos himoyalash vositalarini qarshi qo'yishga imkon beradi. Xususan, ISS (Internet Security Systems) kompaniyasi tomonidan xavfsizlikni adaptiv boshqarish modeli ANS (Adaptive Network Security) ishlab chiqildi. Xavfsizlikka adaptiv yondashish, to'g'ri loyihalangan va yaxshi boshqariluvchi jarayon va vositalar yordamida xavfsizlik xavf-xatarlarini real vaqt rejimida nazoratlash, aniqlash va ularga reaksiya ko'rsatishga imkon beradi. Tarmoqning adaptiv xavfsizligi quyidagi asosiy uchta element orqali ta'minlanadi:

- xavf-xatarlarni baholash;

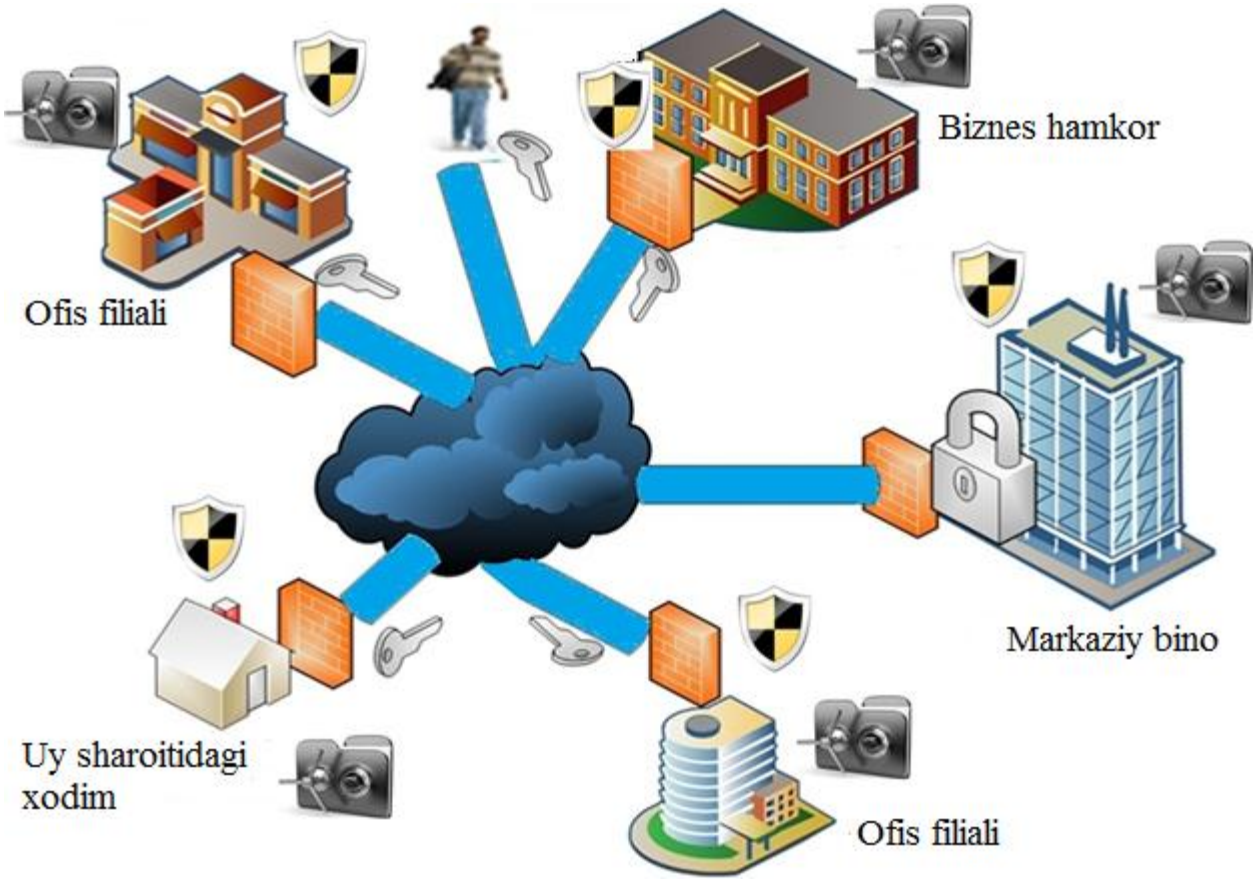
- himoyalanishni taxlillash;
- hujumlarni aniqlash.

Xavf-xatarlarni baholash (keltiradigan zararning jiddiylik darajasi bo'yicha), tarmoq kism tizimlarini (jiddiylik darajasi bo'yicha), tahdidlarni (ularning amalga oshirilishi ehtimolligi bo'yicha) aniqlash va rutbalashdan iborat. Tarmoq konfiguratsiyam muttasil o'zgarishi sababli, xavf-xatarlarni baholash jarayoni ham uzluksiz o'tkazilishi lozim. Korporativ axborot tizimining himoyalash tizimini qurish xavf-xatarlarni baholashdan boshlanishi lozim.

Himoyalanishni taxlillash - tarmoqning zaif joylarini qidirish. Tarmoq ulanishlardan, uzellardan, hostlardan, ishchi stansiyalardan, ilovalardan va ma'lumot bazalaridan tarkib topgan. Bularning barchasi himoyalanishlar samaradorligining hamda no'malum zaifliklarining aniqlanishiga muxtoj.

Xavfsizlikni adaptiv boshqarish modeli komponenti, yangi zaifliklar xususidagi eng oxirgi axborotni taqsim qilgan holda, himoyalanishni taxlillash jarayonini modifikatsiyalashga javob beradi. U xujumlarni aniqlash komponentini ham, uni hujumlar xususidagi oxirgi axborot bilan to'ldirish orqali, modifikatsiyalaydi. Adaptiv komponentalarga misol sifatida yangi viruslarni aniqlash uchun virusga qarshi dasturning ma'lumotlar bazasini yangilash mexanizmini ko'rsatish mumkin. Barcha tahdidlarni nazoratlash va ularga o'z vaqtida samarali reaksiya ko'rsatish imkonini beradi. Bu esa o'z navbatida, nafaqat taxdidlarning amalga oshirilishiga sabab bo'luvchi zaifliklarni bartaraf qilishga, balki zaifliklar paydo bo'lish sharoitlarini tahlillashga imkon beradi. Tarmoq xavfsizligini adaptiv boshqarish modeli tarmoqni suiste'mol qilishni kamaytirishga, tarmoqdagi xodisalardan foydalanuvchilar, ma'murlar va kompaniya rahbariyatining xabardorlik darajasini oshishiga ham imkon beradi. Ta'kidlash lozimki, ushbu model oldin ishlatiluvchi himoyalash mexanizmlaridan voz kechmaydi. Ularning funksionalligini yangi texnologiyalar evaziga kengaytiradi. O'zlarining axborot xavfsizligini ta'minlash tizimlarini zamonaviy talablarga mos kelishini xoxlovchi tashkilotlar mavjud echimlarni uchta yangi komponent himoyalanishni tahlillash, xujumlarni aniqlash va xavf-xatarni

baholash bilan to’ldirishi lozim. Himoyalangan korporativ tarmoq arxitekturasi 2.1 rasmda keltirilgan.



2.1 rasm. Himoyalangan korporativ tarmoq arxitekturasi.

Axborot xavfsizligini ta’minlashning asosiy konsepsiyasini turli aloqa va xavfsizlikni ta’minlash tizimlari, umumiy texnik vositalar, aloqa kanallari, dasturiy ta’minot va ma’lumotlar bazalariga ega yagona tizimga integrasiyasiga asoslangan kompleks yondashuv tashkil etadi. Kompleks xavfsizlik vujudga kelishi mumkin bo‘lgan barcha turdagi tahdidlar (noqonuniy foydalanish, ma’lumotlarni tutib olish, terrorizm, yong‘in, tabiiy ofatlar va hokazolar)ni majburiy hisobga olib, zamon va makon (faoliyatning barcha texnologik sikllari) bo‘yicha xavfsizlikni ta’minlashning majburiy bo‘lgan uzluksiz jarayonini nazarda tutadi. Kompleks yondashuv qanday shaklda qo‘llanilishidan qat’iy nazar, u murakkab va turli yo‘nalishdagi xususiy masalalarni, ularning o‘zaro chambarchas bog‘liqlikdagi yechimi bilan hal etiladi. Bunday masalalar eng dolzarblari bo‘lib, axborotlardan

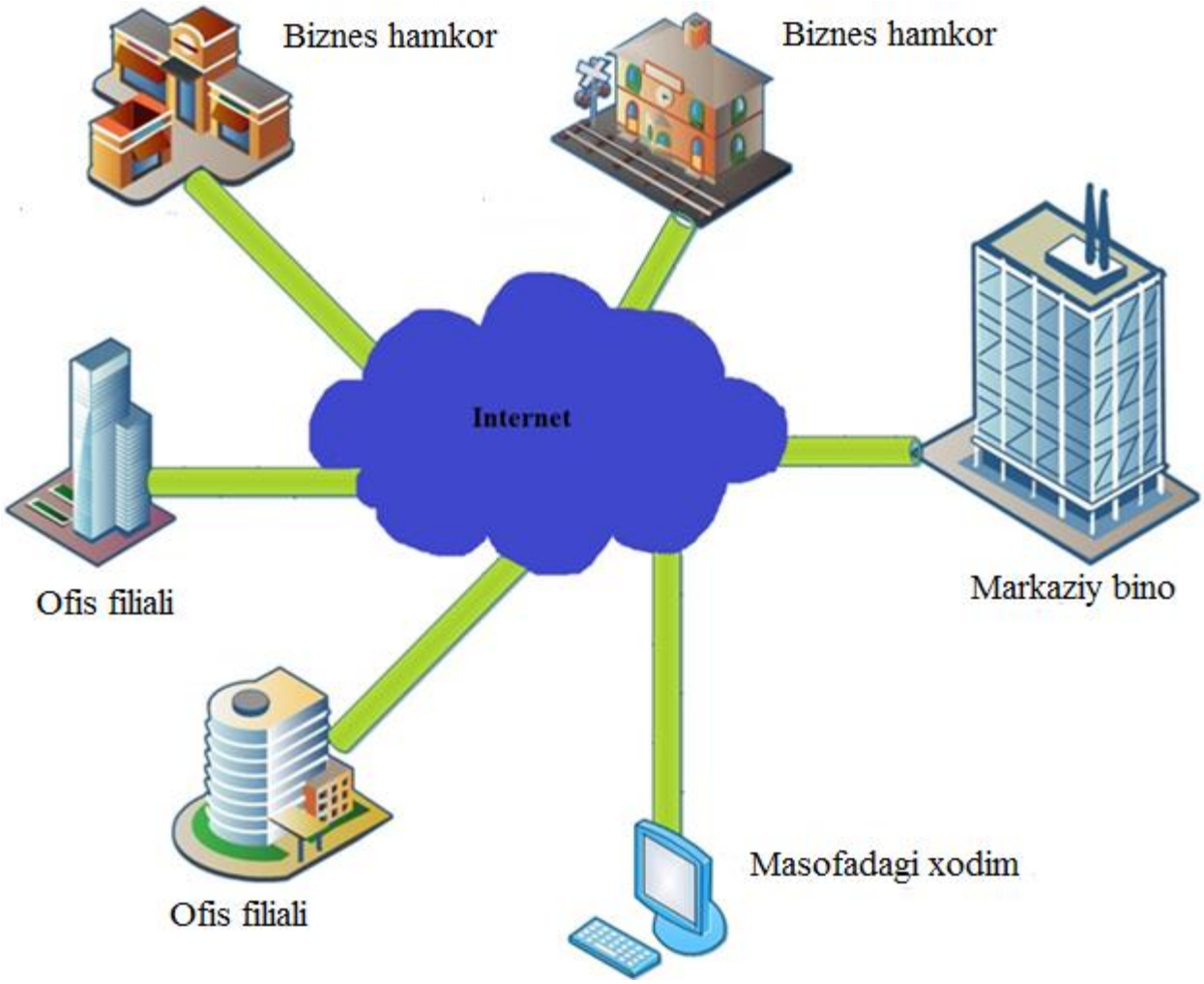
foydalanishni cheklash, axborotlarni texnik va kriptografik himoyalash, texnik vositalarning yondosh turlanishlari darajasini kamaytirish, obyektlarning texnik mustahkamlanganligi, ularning qo‘riqlash va tahlikadan xabardor qilish (signalizatsiya) qurilmalari bilan jihozlanganligi hisoblanadi [11].

2.2 Himoyalangan korporativ tarmoqda ma’lumotlar uzatish qismini himoyalash

Kompyuter tarmoqlarining ochiq kanallari orqali axborotni uzatish jaroyanidagi axborot xafvsizligi kripto himoyalangan tunellar yoki VPN tunellar deb nomlanuvchi himoyalangan virtual kanallarni qurishga asoslangan. Bu tunnellarning har biri shunday ulanishni nazarda tutadiki, bunday ulanish ochiq tarmoq orqali o’tkaziladi va u orqali virtual tarmoqning kriptografik himoyalangan paket xabarlari uzatiladi.

VPN (Virtual Private Network) — virtual xususiy tarmoq mantiqiy tarmoq bo‘lib, o‘zidan yuqoridagi boshqa tarmoq, masalan, internet asosida quriladi. Bu tarmoqda kommunikatsiyalardan umumiy xavfsiz bo‘lmagan tarmoq protokollaridan foydalanilishiga qaramay, shifrlashdan foydalangan holda, axborot almashinishda begonalarga berk bo‘lgan kanallar tashkil qilinadi. VPN tashkilotning bir necha ofislarini ular o‘rtasida nazorat qilinmaydigan kanallardan foydalangan holda, yagona tarmoqqa birlashtirish imkonini beradi. Har qaysi «ma’lumot jo‘natuvchi, qabul qiluvchi» juftligi o‘rtasida ma’lumotlarni bir protokoldan ikkinchi protokolga inkapsulyatsiya qilish imkonini beruvchi o‘ziga hos tunnel xavfsiz mantiqiy bog‘lanish o‘rnatiladi. Tunnellashtirish metodi yordamida ma’lumotlar paketi umumiy foydalanish tarmog‘i orqali xuddi oddiy ikki nuqtali bog‘lanishdagi kabi translyatsiya qilinadi. VPN tarmog’i arxitekturasi 2.2 rasmda keltirilgan. VPN ning uchta asosiy ko‘rinishi qabul qilingan:

- masofadan turib foydalanish imkoniyati mavjud bo‘lgan VPN (Remote Access VPN);
- tashkilot ichidagi VPN (Intranet VPN);
- tashkilotlararo VPN (Extranet VPN).



2.2 rasm. VPN tarmog’i arxitekturasi

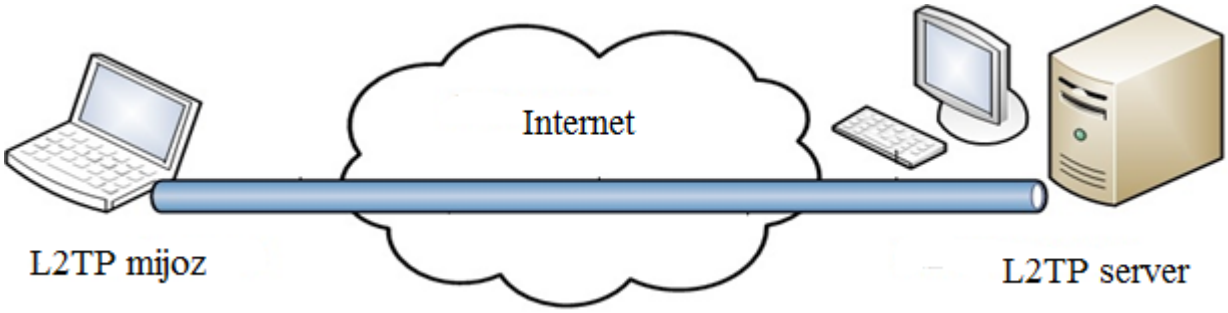
O‘z novbatida, VPN alohida tarmoq xususiyatlarini qamrab olgan, lekin bu tarmoq umumiy foydalanish tarmog‘i, masalan, internet orqali amalga oshiriladi. Shunday qilib VPN bu:

- kriptografiyaga asoslangan trafik himoyasi;
- dunyoning istalgan nuqtasidan ichki resurslardan foydalanish imkonini beruvchi kafolatlangan himoyalovchi kommunikatsiya vositasi;
- korporatsiyaning kommunikatsiya tizimini alohida ajratilgan liniya qurishga sarf etiladigan vositalarni ishlatmasdan rivojlanishidir.

Korporatsiyaning mavjud tarmoq infratuzilmasi VPN dan foydalanishga dasturiy ta’minot yordamida yoki qurilma ta’minoti yordamida tayyorlangan bo‘lishi mumkin. Foydalanuvchi dasturiy vositalari odatda masofadan turib ulanishda kanal darajasidagi standart PPP (Point-to-Point Protocol) protokolidan

foydalanadi. PPTP va L2TP protokollari PPP protokoli asosida qurilgan bo'lib, uning kengaytirilgan variantlari hisoblanadi.

L2TP protokoli esa tunnellashtiruvchi protokol hisoblanadi, chunki faqatgina tunnellashtirish funksiyasini qo'llab – quvvatlaydi. Ma'lumotlarni himoyalash (shifrlash, butunlik, autentifikatsiya) funksiyalari bu protokolda qo'llab – quvvatlanmaydi. L2TP protokolida tunnellashtiriladigan ma'lumotlarni himoyalash uchun qo'shimcha IPSec protokolini ishlatish kerak. L2TP protokolli asosidagi tarmoq 2.3 rasmda keltirigan.



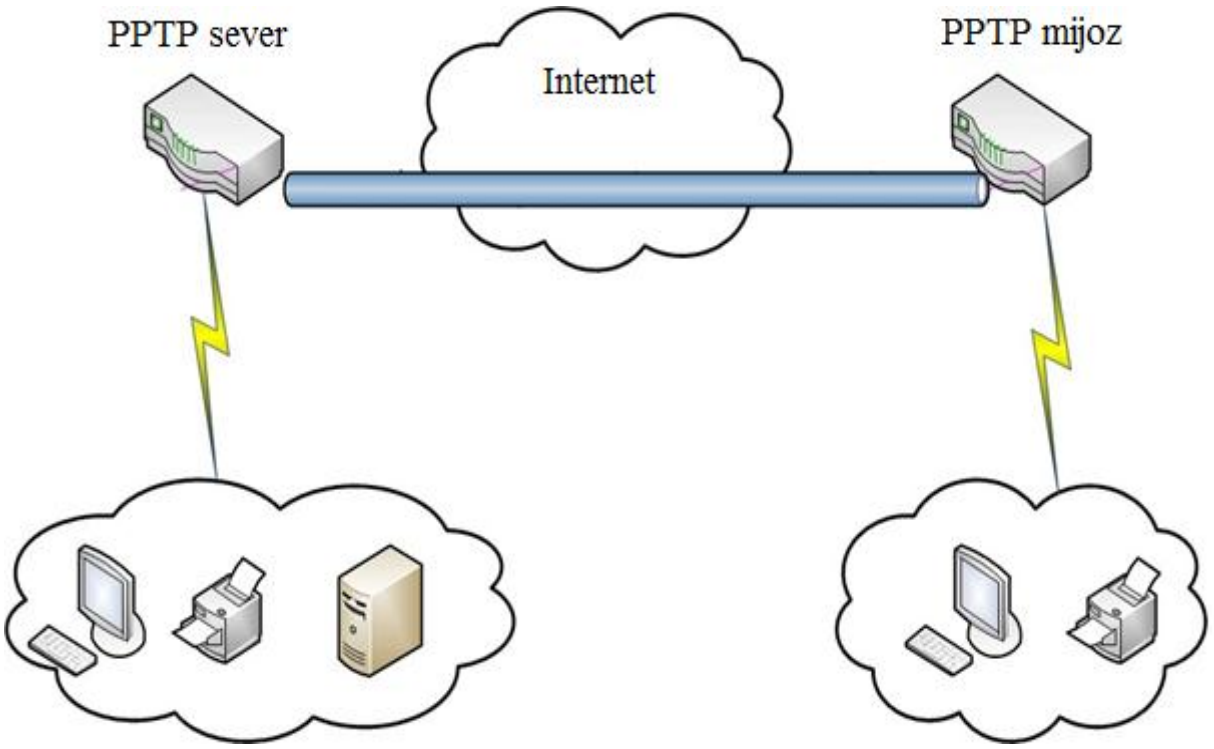
2.3 rasm. L2TP-protokolli asosidagi tarmoq arxitekturasi

Konfidensial ma'lumotlarni bir nuqtadan ikkinchisiga umumiy foydalaniladigan tarmoq orqali yetkazish uchun dastlab ma'lumotlar PPP protokoli yordamida inkapsulyatsiya qilinadi, keyin esa PPTP va L2TP protokollari ma'lumotlarni shifrlashadi va xususiy inkapsulyatsiyalarini amalga oshiradilar. Tunnel protokoli paketlarni tunnelling chiquvchi nuqtasidan yakuniy nuqtasiga yetkazib bo'lganidan so'ng deinkapsulyatsiya amalga oshiriladi.

PPTP (Point-to-Point Tunneling Protocol) protokoli va L2TP (Layer-2 Tunneling Protocol) OSI modeli kanal darajasining tunnellashtiruvchi protokollari hisoblanadi. Bu protokollarning umumiy xususiyati shundan iboratki, ular korporativ tarmoq resurslariga, himoyalangan ko'p protokolli masofadan turib, ochiq tarmoq orqali, masalan, internet orqali, ulanishni tashkil etish uchun ishlatiladi.

PPTP protokolida quyidagi autentifikatsiya protokollari qo'llab quvvatlanadi:

- PAP (Password Authentication Protocol) parol bo'yicha protokolli ishlatiladigan identifikatorlar va parollar aloqa liniyalari shifrlanmagan holda uzatiladi, va faqat sever mijoz autentifikatsiyasini amalga oshiradi;
- CHAP (Challenge Handshaking Authentication Protocol) ikki tomonlama qo'l siqish protokoli;
- EAP-TLS (Extensible Authentication Protokol – Transport Layer Security) protokoli. CHAP, EAP va TLS protokollari ishlatilganda yovuz niyatli shaxslar tomonidan qo'lga kiritilgan shifrlangan paketlarning qayta ishlatilishidan himoya, mijoz va VPN server o'rtasida ikki tomonlama autentifikatsiya ta'minlanadi. PPTP protokolli asosida qurilgan tarmoq 2.4 rasmda keltirilgan.



2.4 rasm. PPTP-protokolli asosida qurilgan tarmoq arxitekturasi

Ikkala protokol ham PPTP va L2TP odatda himoyalangan kanalni yaratish protokollariga kiritiladi, ammo bunday aniqlanishga faqat PPTP protokoli to'gri keladi, chunki u uzatiladigan ma'lumotlarni tunnellashtirish va shifrlashni ta'minlaydi.

Ma’lumotlarni uzatish qismini himoyalashda yana bir protokoll IPSec (Internet Protokol Security) protokollar steki ishlatiladi.Bu protokoll ma’lumot almashinuv jarayonida qtnashadigan ishtirokchilar autentifikatsiyasi, trafikni tunnellashtirish va IP paketlarni shifrlash uchun ishlatiladi. IPSec protokolining asosiy vazifasi IP tarmoq bo’yicha ma’lumotlarni xavfsiz yetkazishni ta’minlash. IPSec protokolli trafik himoyasini joriy IPv4 protokolida, shuningdek hozirgi kunda internet texnologiyasida keng tarqalayotgan IPv6 protokoli versiyasida ham ta’minlay oladi. IPSec protokollarining asosiy vazifasi IP tarmoqlar bo’yicha xavfsiz ma’lumot almashinuvini ta’minlash. IPSec ni qo’llash quyidagilarni kafolatlaydi:

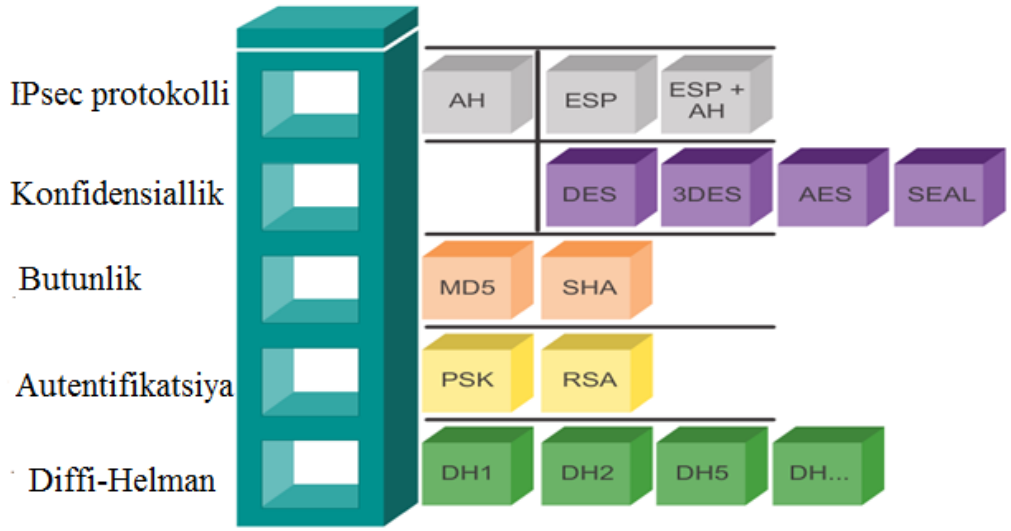
- uzatiladigan ma’lumotlar butunligini, ya’ni ma’lumot uzatilishda hech qanday buzulishlar, yo’qitishlar va qaytarilishlar bo’lmasligi;
- uzatuvchi autentifikatsiyalanganligi, ya’ni ma’lumotlar haqiqatdan ham aniq va to’g’ri manzilga uzatilishi;
- uzatiladigan ma’lumotlar konfidensialligi, ya’ni ruxsat etilmagan hollarda ma’lumotni o’qiy olmaslik.

IPSec protokolli asosan quyidagi komponentalardan tashkil topgan bo’ladi:

- asosiy protokol, ESP (Encapsulating Security Payload) va AH (Authentication Header);
- IKE (Internet Key Exchange);
- SPD (Security Policy Database);
- SAD (Security Association Database).

IPSec protokolida ma’lumotlarni shifrlash uchun maxfiy kalitlarni ishlatadigan istalgan simmetrik shifrlash algoritmi qo’llanilishi mumkin. Himoyalangan virtual kanallarni tashkil etish mumkin bo’lgan OSI modelining eng yuqori darajasi bu seans darajasi bo’lib hisoblanadi. Seans darajasidagi tashkil etiladigan himoyalangan virtual kanallar protokollari himoyaning amaliy protokollari, shningdek, turli xil xizmatlarni ko’rsatuvchi yuqori darajali protokollar:

- HTTP;
- FTP;
- POP3;
- SMTP va boshqa protokollar uchun shaffof. IPSec protokolli strukturasi 2.5 rasmda keltirilgan.



2.5 rasm. IPSec protokolli strukturasi

Ma’lumotlarning butunligi va autentligini ta’minlash uchun (AH va ESP protokollarida) shifrlashning bir turidan foydalaniladi. Bir tomonlama shifrlovchi funksiya (One way function), xesh funksiya (Hash function) deb ham yuritiladi, yoki dayjest – funksiya (Digest Function). Ma’lumotlarni bu funksiya yordami bilan shifrlaganda katta bo’lmagan chegaralangan baytlardan iborat dayjest qiymat qaytaradi. Ayni vaqtda AH va ESP protokollari uchun ikkita autentifikatsiyalash algoritmlari HMAC-MD5 va HMAC-SHA-1 qabul qilingan. HMAC (Keyed-Hashing for Message Authentication Code) algoritmi RFC 2104 standartida aniqlangan. MD5 (Message Digest version 5, RFC 1321 standarti) va SHA-1 (Secure Hash Algorith version 1, standart FIPS 180-1) funksiyalari umumiy maxfiy kalitli xesh funksiyalar hisoblanadi. IPSec quyidagi himoya funksiyalarini ta’minlaydi:

- autentifikatsiya;

- ma’lumotlar butunligi;
- konfidensiallik;
- kalitlarni ishonchli boshqarish;
- tunnellashtirish.

Sarlavhani autentifikatsiyalaydigan AH protokoli autentlik tekshiruvini va IP paketlar butunligin ta’minlaydi. AH protokoli qabul qiluvchi quyidagilarga ishonch hosil qilishiga imkon beradi:

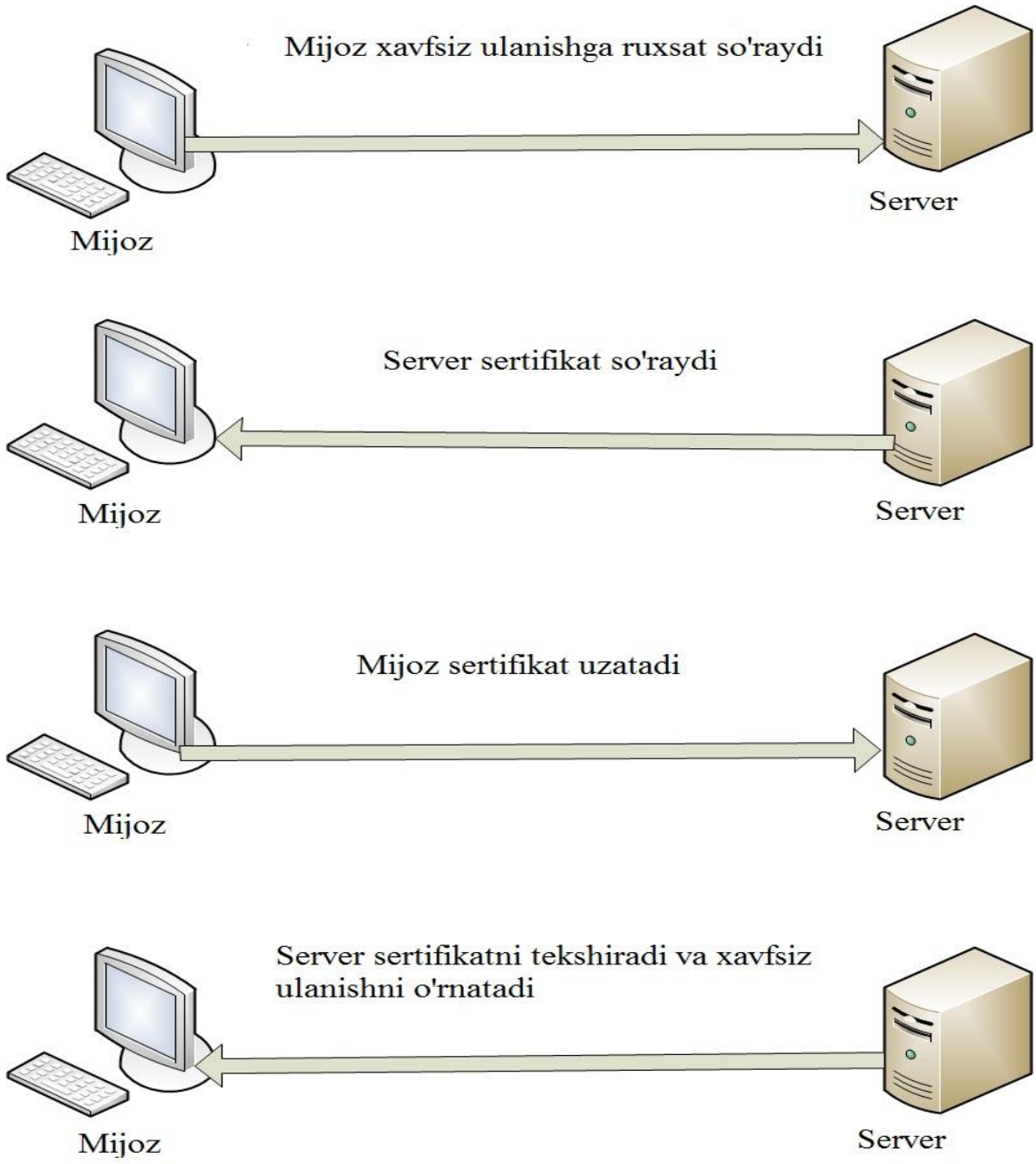
- paket aynan kerakli, ya’ni joriy ulanish o’rnatilgan tomondan uzatilgan;
- paket ma’lumotlari tarmoq orqali uzatish vaqtida hech qanday buzilishlarga uchramagan;
- paket oldinroq qabul qilingan biror–bir paketning dublikati emas.

Ammo, seans darajasida yuqori darajali protokollar amalga oshiradigan dasturlar bilan bevosita bo’gliqligi boshlanadi. Shuning uchun ushbu darajaga tegishli ma’lumot almashinuvi himoya protokollarini tashkil etish, odatda yuqori darajalardagi tarmoq dasturlariga o’zgartirishlar kiritishni talab qiladi. Seans darajasidagi ma’lumot almashinuvi himoyasi uchun SSL protokoli keng ko’lamda qo’llaniladi. SSL (Secure Socket Layer – himoyalangan soketlar protokollari) protokoli Netscape Communications tashkiloti tomonidan va RSA Data Security tashkiloti hamkorligida mijoz/server dasturlarida himoyalangan ma’lumot almashinuvini tashkil etish uchun ishlab chiqarilgan. SSL protokolining yadrosini assimmetrik va simmetrik kriptosistema texnologiyalarining kompleks ishlatilishi tashkil qiladi. SSL protokolida ikkala tomon autentifikatsiyasi foydalanuvchilarning (mijoz va server) maxsus sertifikatlash markazlari tomonidan raqamli imzolar bilan tasdiqlangan ochiq kalitlar sertifikatlari almashinuvi yo’li bilan bajariladi. Serverning SSL autentifikatsiyasi mijozga serverning haqiqiyligini tekshirish imkonini beradi. SSL-sessiyasi o’rnatilganda quyidagi masalalar yechiladi:

- tomonlar autentifikatsiyasi;

- tomonlarning himoyalangan ma’lumot almashinuvida ishlatiladigan kriptografik algoritmlar va siqish algoritmlari mosligi va kelishuvi;
- umumiy maxfiy maxsus kalitni tashkillashtirish;
- umumiy maxfiy maxsus kalit asosida ma’lumot almashinuvining kripto himoyasi uchun umumiy maxfiy seans kalitlarni generatsiyalash.

Mijoz va sever orasidagi xavfsiz ulanishni tashkil etilishi va ular orasidagi autentifikatsiya jarayoni 2.6 rasmda keltirilgan.



2.6 rasm. Mijoz va sever orasidagi xavfsiz ulanishni tashkil etilishi

Hozirgi vaqtda SSL protokoli OSI modelining seans darajasidagi himoyalangan kanal protokoli sifatida qo'llaniladi. SSL protokoliga asosan kripto himoyalangan tunnellar virtual tarmoqning yakuniy nuqtalari orasida yasaladi. Ulanishnig bir tomonida server, ikkinchi tomonida mijoz faoliyat ko'rsatadi.

SSL protokolida autentifikatsiyaning ikki xil usuli mavjud:

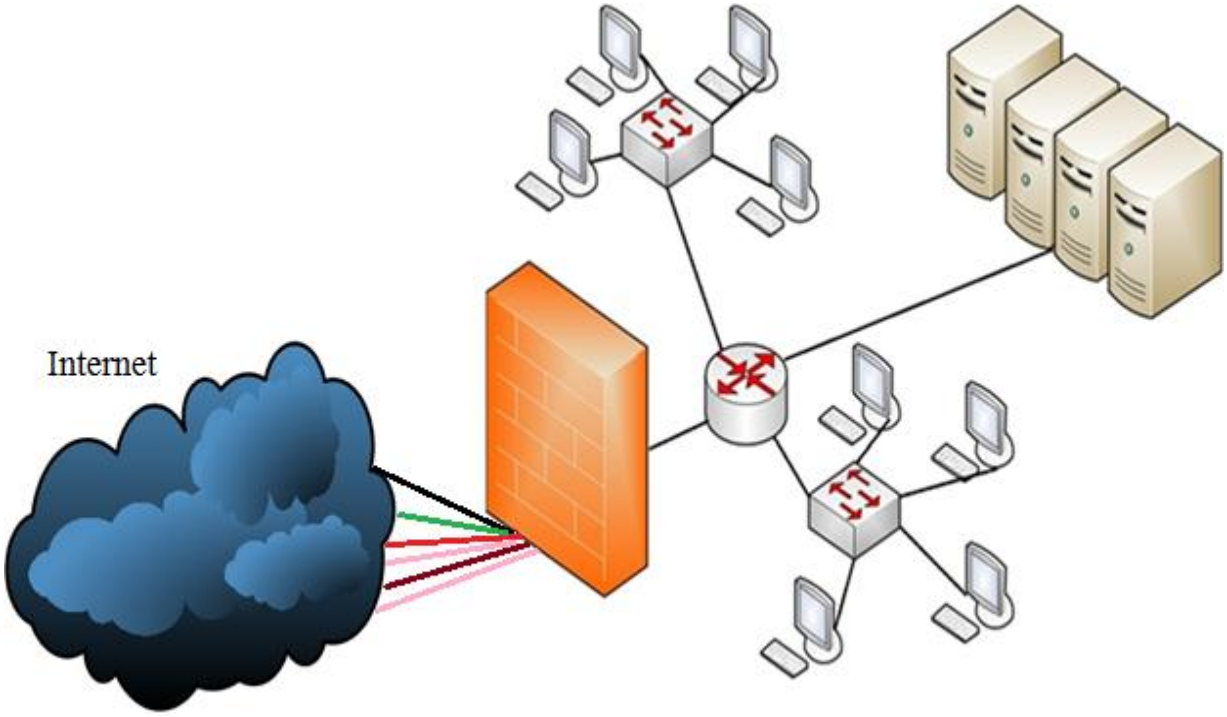
- serverning mijoz bilan autentifikatsiyasi;
- mijozning server bilan autentifikatsiyasi.

SSL protokoli X.509 standartiga mos keluvchi sertifikatlarni, shuningdek ochiq kalitlar infrastrukturasi standarti PKI (Public Key Infrastructure) ni qo'llab quvvatlaydi. Bu standartlar yordamida sertifikatlarning yetkazilishi va haqiqiyligini tekshirish amalga oshiriladi [3].

2.3. Himoyalangan korporativ tarmoqda ma'lumotlar sqaqlash va qayta ishlash qismini himoyalsh

Himoyalangan korporativ tarmoqda ma'lumotlar sqaqlanadigan va qayta ishlanadigan qismi bu tashkilot yoki korxonanaing ichki qismidagi kopmyuterlar serverlar va ulardagi ma'lumotlar bazalari hisoblanadi. Birinchi novbatda himoyalanadigan qism bu tarmoqning kirish qismi hisoblanadi. Kirish va chiqishlarni nazorat qilish, hamma foydalanayotgan tarmoqdan kelib chiqayotgan tahdidlarni blokirovkalash uchun «tarmoqlararo ekran» (Firewall) deb nomlanuvchi dasturiy va apparat-dasturiy vositalaridan foydalaniladi. Odatda, alohida ajratilgan va himoyalangan KT «tarmoqlararo ekran» orqali hamma foydalanadigan tarmoqqa ulanadi. Tarmoqlararo ekran himoyalangan KTga kelib tushayotgan va undan chiqib ketayotgan axborotlarni nazorat qilish uchun qo'llaniladi.

Tarmoqlararo ekranning asosiy vazifasi (kirayotgan yoki chiqayotgan) trafikni filtrlashdan iborat. Korporativ tarmoqning himoyalanganlik darajasiga qarab filtrlashning turli qoidalari o'rnatilishi mumkin. Filtrlash qoidalari filtrlar ketma-ketligini tanlash orqali amalga oshiriladi. Tarmoqlararo ekran texnologiysi 2.7 rasmda keltirilgan.



2.7 rasm. Tarmoqlararo ekran texnologiysi

Tarmoqlararo ekran filtrlashni kanallar, tarmoqlar, transport va amaliy sathlarda amalga oshiradi. Ekran qancha ko‘p sathni o‘z ichiga olsa, shuncha takomillashgan hisoblanadi. Tarmoqlararo ekranda, dasturiy vositachi vazifani bajaruvchi va subyekt va obyekt orasida ulanishni ta’minlovchi, so‘ngra axborotni qayd qilish va nazoratini amalga oshirib jo‘natuvchi, ekranlovchi agentlardan (proxy-serverlar) foydalaniladi. Ekranlovchi agentlarning qo‘shimcha vazifasi foydalanishga ruxsat berilgan subyektdan haqiqiy obyektni yashirishdan iborat.

Ekranlovchi agentlarning o‘zaro aloqa ishtirokchilariga ta’siri yo‘q. Tarmoqlararo ekranning manzillarni translatsiyalash funksiyasi haqiqiy ichki manzillarni tashqi abonentlardan yashirish uchun mo‘ljallangan. Bu tarmoq topologiyasini yashirish va agar himoyalangan tarmoq uchun yetarli miqdorda manzillar ajratilmagan bo‘lsa, yanada ko‘proq sondagi manzillardan foydalanishga imkon yaratadi.

Tarmoqlararo ekran maxsus jurnallarda hodisalarni qayd qilib boradi. Biror aniq talab bo‘yicha ekranni sozlash orqali jurnallarni yuritish imkoniyati nazarda tutilgan.

Yozuvlar tahlili o‘rnatilgan qoidalarni buzishga bo‘lgan buzg‘unchilarning urinishlarini qayd qilish va ularni aniqlash imkonini beradi.

Ekran simmetrik emas. Tarmoqlararo ekran quyidagi to‘rtta funksiyani bajaradi:

- ma’lumotlarni filtrlash;
- ekranlovchi agentlardan foydalanish;
- manzillarni translatsiyalash;
- hodisalarni qayd qilish.

U “tashqi” va “ichki” tushunchalarini farqlay oladi. Ekran ichki sohani nazoratsiz va adovatli bo‘lgan tashqi muhitdan himoyasini ta’minlab beradi. Shu bilan birga ekran himoyalangan tarmoq subyektlari tomonidan ommaviy tarmoq obyektlaridan foydalanishni cheklashni ham ta’minlaydi. Foydalanishga ruxsat berilgan subyektning vakolatlari buzilgan holatda uning ish faoliyati blokirovka qilinadi va barcha kerakli ma’lumotlar jurnalga yozib qo‘yiladi. Tarmoqlararo ekranlarga quyidagi zamonaviy talablar qo‘yiladi:

- Asosiy talablar bu ichki tarmoqning xavfsizlikni ta’minlash va tashqaridan ulanishlar va aloqa seanslarini to‘liq nazorat qilish;
- Ekranlovchi tizim tashkilotning xavfsizlik siyosatini oddiy va to‘liq yuritish uchun quvvatli va moslanuvchan boshqarish vositalariga ega bo‘lmog‘i darkor;
- Tarmoqlararo ekran lokal tarmoq foydalanuvchilariga sezdirmasdan ishlashi va ular tomonidan ruxsat etilgan amallarni bajarishlariga xalaqit bermasligi lozim;
- Tarmoqlararo ekran ko‘p miqdordagi murojatlarni blokirovka qilib qo‘yishni va ishdan chiqishining oldini olish uchun, uning protsessori tez ishlay olish, pik rejimlarida kiruvchi va chiquvchi oqimlarni yetarli darajada samarali qayta ishlay olishga ulgurishi lozim;
- Xavfsizlikni ta’minlash tizimi har qanday tashqi noqonuniy ta’sirlardan himoyalangan bo‘lishi lozim, chunki bu ta’sirlar tashkilotning konfedensial ma’lumotlarini ochish kaliti bo‘lishi mumkin;

- Ekranni boshqaruv tizimi olisdagi filiallar uchun ham yagona xavfsizlik siyosatini yuritishni markazlashgan holda ta’minlash imkoniyatiga ega bo‘lmog‘i lozim;
- Tarmoqlararo ekran foydalanuvchilarning tashqi ulanishlari orqali foydalanishga ruxsat berishning mualliflashtirish vositalariga ega bo‘lmog‘i, tashkilot xodimlarini xizmat safarida ham tarmoqdan foydalanishlariga imkon yaratadi.

Ma’lumotlar korporativ tarmoqdagi foydalanuvchilar komyuterlarida ham saqlanadi va qayta ishlanadi. Shuning uchun ham kompyuter viruslaridan va boshqa dasturlar ta’siridan va o‘zgartirishlardan himoyalanish, kompyuter tizimlarida axborotlarni qayta ishlash jarayonini himoyalashning mustaqil yo‘nalishlaridan hisoblanadi. Ushbu xavfga yetarlicha baho bermaslik foydalanuvchilarning axborotlari uchun jiddiy salbiy oqibatlarni keltirib chiqarishi mumkin. Kompyuter viruslaridan va boshqa dasturlar ta’siridan va o‘zgartirishlardan himoyalanish, kompyuter tizimlarida axborotlarni qayta ishlash jarayonini himoyalashning mustaqil yo‘nalishlaridan hisoblanadi. Viruslarning ta’sir mexanizmlarini, ularga qarshi kurash usullari va vositalarini bilish viruslanishga qarshi harakatlarni samarali tashkil etish, ularning ta’siridan zararlanish ehtimolligini va talofatlarni minimumga keltirish imkonini beradi. Viruslarning ommaviy tarqalib ketishi va ularning KT resurslariga ta’siri oqibatlarining jiddiyligi, maxsus antivirus vositalarini va ularni qo‘llash usullarini yaratish va foydalanish zaruriyatini keltirib chiqardi. Antivirus vositalari quyidagi masalalarni hal etish uchun qo‘llaniladi:

- viruslarni topish va ularni yo’q qilish;
- virus dasturlar ishini blokirovka qilish;
- viruslar ta’sirining oqibatlarini bartaraf qilish.

Viruslarni topishni, ularni joylashib olish bosqichida yoki hech bo‘lmaganda virusning buzg‘unchilik funksiyalarini boshlagunga qadar amalga oshirgan maqsadga muvofiq. Shuni ta’kidlash joizki, barcha turdagi viruslarni topishni kafolatlovchi antivirus vositalari mavjud emas. Virus topilgan holatda, uning

tizimga keltirishi mumkin bo‘lgan zararli ta’sirini minimallashtirish maqsadida darhol virus dasturning ishini to‘xtatilish lozim. Virusning ta’sir oqibatlarini bartaraf qilish ikki yo‘nalishda olib boriladi:

- virusni o‘chirish;
- fayllarni xotira sohalarini tiklash.

Tizimni qayta tiklash virus turiga, uni aniqlangan hamda zararlovchi ta’sirini boshlagan vaqtiga bog‘liq. Viruslar tizimga kirish jarayonida, o‘zini saqlaydigan joydagi ma’lumotlarni o‘chirib yuborsa, hamda zararlovchi ta’siri natijasida ma’lumotlarni o‘zgartirish nazarda tutilgan bo‘lsa, zaxiraga olingan ma’lumotlarsiz yo‘qolgan ma’lumotlarni tiklab bo‘lmaydi. Viruslarga qarshi kurashda aniq bir ketma-ketlik va kombinatsiyada qo‘llaniluvchi, viruslarga qarshi kurashish usullarini hosil qiluvchi dasturiy va apparat-dasturiy vositalardan foydalaniladi.

KTning xavfsiz ishlashining asosiy shartlaridan biri, amalda sinovdan o‘tkazilgan va o‘zining yuqori samara berishini ko‘rsatgan bir qator qoidalarga rioya qilish hisoblanadi.

Birinchi qoida – qonuniy rasmiy yo‘l bilan olingan dasturiy mahsulotlardan foydalanish. Dasturiy ta’minotning qaroqchilik yo‘li bilan ko‘paytirilgan nusxalarida, rasmiy yo‘l bilan olinganlariga nisbatan viruslarning mavjudlik ehtimoli juda yuqori.

Ikkinchi qoida – axborotlar zaxirasini hosil qilish. Avvalo dasturiy ta’minotning distributivlari yozilgan tashuvchilarni saqlash zarur. Bunda tashuvchilarga ma’lumotlarni yozish imkoni berilgan bo‘lsa, imkon qadar uni blokirovka qilish zarur. Ishga talluqli ma’lumotlarni saqlanishiga jiddiy yondashishi zarur. Muntazam ishga taalluqli fayllarning zaxira nusxalarini yaratib borish va ularni yozishdan himoyalangan yechib olinuvchi tashuvchilarda saqlash kerak. Agar bunday nusxalar yechib olinmaydigan tashuvchilarda yaratilayotgan bo‘lsa, ularni butunlay boshqa kompyuterning doimiy xotirasida yaratish maqsadga muvofiq.

Uchinchi qoida – antivirus vositalaridan muntazam foydalanish. Antivirus vositalari muntazam yangilanib turilishi lozim.

To‘rtinchi qoida – yangi yechib olinadigan axborot tashuvchilardan va yangi fayllardan foydalanilganda ehtiyotkorlikka rioya qilish. Yangi yechib olinadigan tashuvchilar olinganda, albatta, yuklanuvchi va fayl viruslari mavjudligiga, olingan fayllar esa fayl viruslari mavjudligiga tekshirilishi lozim. Tekshiruv, skanerlovchi dasturlar va evristik tahlilni amalga oshiruvchi dasturlar yordamida amalga oshirilishi kerak.

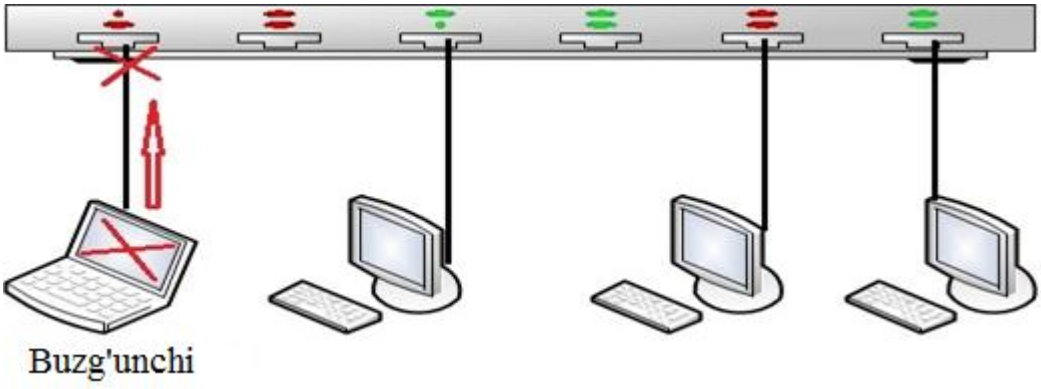
Beshinchi qoida – tizimga, ayniqsa taqsimlangan tizimlarga yoki jamoa bo‘lib foydalaniladigan tizimlarga, kiritilayotgan fayllarni va yechiladigan axborot tashuvchilarni maxsus ajratilgan kompyuterlarda tekshirish. Uni tizim administratori yoki ma’lumotlar xavfsizligiga mas’ul bo‘lgan shaxsning avtomatlashtirilgan ish joyidan amalga oshirilishi maqsadga muvofiq. Disk va fayllarni har tomonlama antivirus tekshiruvidan o‘tkazilgandan so‘ng ularni tizimdan foydalanuvchilarga taqdim etish mumkin.

Oltinchi qoida – agar axborotlarni tashuvchilarga yozish nazarda tutilmagan bo‘lsa, bunday amallarni bajarilishini blokirovka qilish. Yuqorida keltirilgan tavsiyalarga doimiy rioya qilinishi virus dasturlar bilan zararlanish ehtimolini ancha kamaytiradi va foydalanuvchini axborotlarni qaytib tiklab bo‘lmaydigan yo‘qotishlardan saqlaydi.

Ma’lumotlarni saqlash va qayta ishlash qurilmalari tarmoq qurilmalari ya’ni, kommutator va mashrutizatorlaga ulanadi. Bu tarmoq qurilmalarida xavfsizlik choralarini qo’llash orqali ichki tarmoqdan bo’ladigan hujumlarni oldini olish, hamda ularni bartaraf etishda, foydalaniladi.

Kommutatorda asosiy xavfsizlik choralarini qo'llanilishi. Port security kommutatorda hostlarning MAC-adreslarini ko'rsatishga imkon yaratuvchi va port orqali ko'rsatilgan manzilga ma’lumotlarni uzatishga ruhsat beradigan funksiyasi hisoblanadi. Ruxsatsiz ulanishdan himoyalanish 2.8 rasmda keltirilgan. Bu xavfsilik chorasi yordamida quyidagilarni bartaraf qilish mumkin:

- tarmoqqa ruhsatsiz ulanish va tarmoq qurilmasining MAC-adresini ruxsatsiz o'zgartirishdan;
- kommutatsiya jadvalini to'lib toshishiga qaratilgan hujumlardan.



2.8 rasm. Ruxsatsiz ulanishdan himoyalanish

Agar yuboruvchining MAC-adresiga ruxsat berilmagan bo'lsa, port paketlarni uzatmaydi. Bundan tashqari port orqali trafikni uzatishga ruxsat beradigan MAC-adreslar miqdorini cheklab qo'yish mumkin.

Masrutizatorlarda asosiy xavfsizlik choralarini qo'llanilishi ACL (Access Control List) ruhsat berishlar ro'yhati bo'lib, bu orqali tarmoq paketlariga ruhsat berish yoki ularni ta'qiqlash mumkin. Odatda ACL IP paketlarga ruxsat beradi yoki taqiqlaydi, lekin bundan tashqari u IP paket tarkibini tekshirishi, paket turini aniqlashi va TCP yoki UDP portlarni tekshirishi mumkin. Ruhsat berishlar ro'yhati xizmati asosan tarmoq qurilmalari (marshrutizator, kommutator, tarmoqlararo ekran) da mavjud bo'lib, ichki tarmoq va internet o'rtasidagi keraksiz bo'lgan trafikni filtrlashda ishlatiladi. ACL da trafikni klassifikatsiyalash funksiyasi uni tekshirish va qaerda qo'llanilishiga qarab aniqlanadi.

ACL turli xolatlarda qo'llanilishi mumkin, masalan:

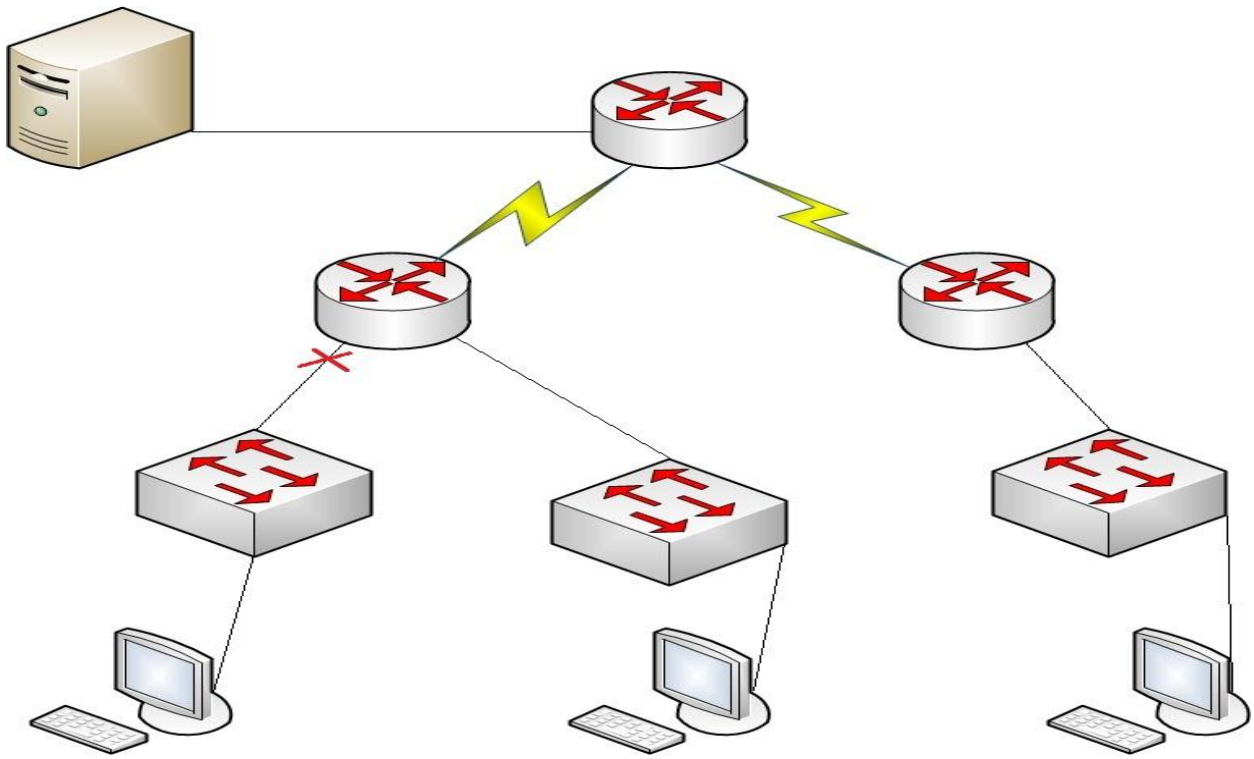
- interfeysda, paketlarni filtrlash;
- telnet tarmog’ida, marshrutizatorga ruhsat berishni chelkash;
- VPN trafikni qaysi qismini shifrlash lozim;
- QOS trafikni muqimlilik darajasini aniqlash;
- NAT qaysi adreslarni translyatsiyalash lozim.

ACL xizmati o'zida permit (ruxsat berish) yoki deny (taqiqlash) matnlardan iborat qoidalar to'plamini qamrab oladi va shu qoidalar asosida tarmoqda

paketlarni qayta ishlanish jarayonini tartibga solib turadi. ACL xizmatining ikki hil toifasi mavjud:

- Standart (Standart): 1-99 gacha faqatgina manbaning manzilini tekshira oladi;
- Kengaytirilgan (Extended): 100-199 gacha nafaqat manbaning balki qabul qiluvchining manzilini, balki IP holatida foydalanuvchilarning TCP/UDP portlarini ham tekshira oladi;

Shuni yodda tutish lozimki interfeysga, protokolga yoki yo'nalishga 1tadan ortiq ruhsat berishlar ro'yhatini qo'llash mumkin emas. Manzillarni filtrlash uchun ACL xizmatida WildCard maska ishlatiladi. Bu teskari maska hisoblanadi. Bunga quyidagi andozani misol qilib keltirishimiz mumkin: 255.255.255.255 oddiy maskadan 255.255.255.0 maskani hosil qilamiz, va bunga teskari bo'lib 0.0.0.255 maskasi olinadi. Ruxsat berishlar ro'yhati o'zi alohida global konfigda yaratiladi va interfeysga bog’lanadi. Shundan so'ngra ruhsat berishlar ro'yhati ishlashni boshlaydi. ACL ni ishlash prinspi 2.9 rasmda keltirilgan.



2.9 rasm. ACL orqali cheklovlarni o’rnatish

Ruxsat berishlar ro'yxatini to'g’ri sozlash uchun quyidagi jarayonlarni yodda tutish lozim:

- paketlarni qayta ishlash jarayoni belgilangan qoidalarga muvofiq qatiy tartibda olib boriladi;
- agar paket qoidaga to'g’ri kelsa u qayta ishlanmaydi;
- har bir ruxsat berishlar ro'yhatining oxirida ko’rinmaydigan deny any (hammasini taqiqlash) turadi;
- kengaytirilgan ACL ni iloji boricha manbaga yaqinroq, standart ACL ni esa qabul qiluvchiga yaqinroq joylashtirish lozim;
- interfeysga, protokolga va yo'nalishga 1tadan ortiq ro'yhatni joylashtirish mumkin emas;
- ACL marshrutizator tomonidan generatsiya qilingan trafikka tasir qilmaydi;
- tarmoq manzillarini filtrlash uchun WildCard maska ishlatiladi; [6]

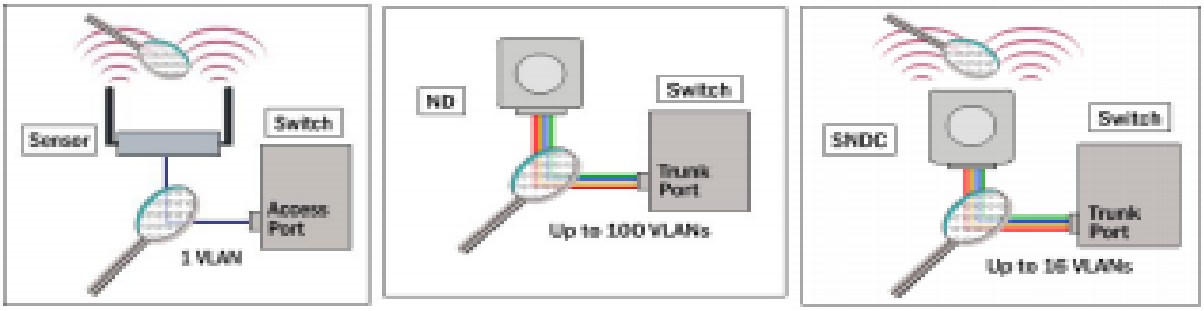
Himoyalangan korporativ tarmoqlarda simsiz texnologiyalar qo’llanilgan, hamda vlanlarga ajratilgan qisimlarini himoyalash, doimiy nazorat qilib turishda HP Mobility Xavfsizlik IDS / IPS tizimi RF menejeri va MSM415 Sensoridan foydalanish, korporativ tarmoq xavfsizligini ta’minlashning samarali usullaridan hisoblanadi. MSM415 Sensor bilan birga HP RF Manager barcha IEEE 802.11 WLAN tarmoqlari uchun to'liq qo'llab-quvvatlash bilan avtomatik siyosatga asoslangan xavfsizlik va manzil-kuzatish imkoniyatlari bilan simsiz tahdidlar oldini oladi. Tahdidlar bo'yicha harakatlanish uchun avtomatik ravishda bitta sensori bir vaqtning o'zida Denial of service (DOS) hujumlar va 20 dan ortiq tahdidlarni oldini oladi. HP IDS/IPS va MSM415 sensori 2.10 va 2.11 rasmlarda keltirilgan.

2.10 rasm. HP IDS/IPS xavfsizlik qurilmasi

2.11 rasm. HP MSM415 RF Xavfsizlik Sensori

HP MSM415 RF Xavfsizlik Sensori doimiy simsiz tahdidlar uchun IEEE 802.11a / b / g / n tarmoqlarini ko'zdan kechiradi. Doimiy tarmoqni skanerlash, RF Manager avtomatik ravishda simsiz tarmoq orqali ma'lumot oqishni nazorat qiladi.Sensor 3 xil rejimga sozlanadi:

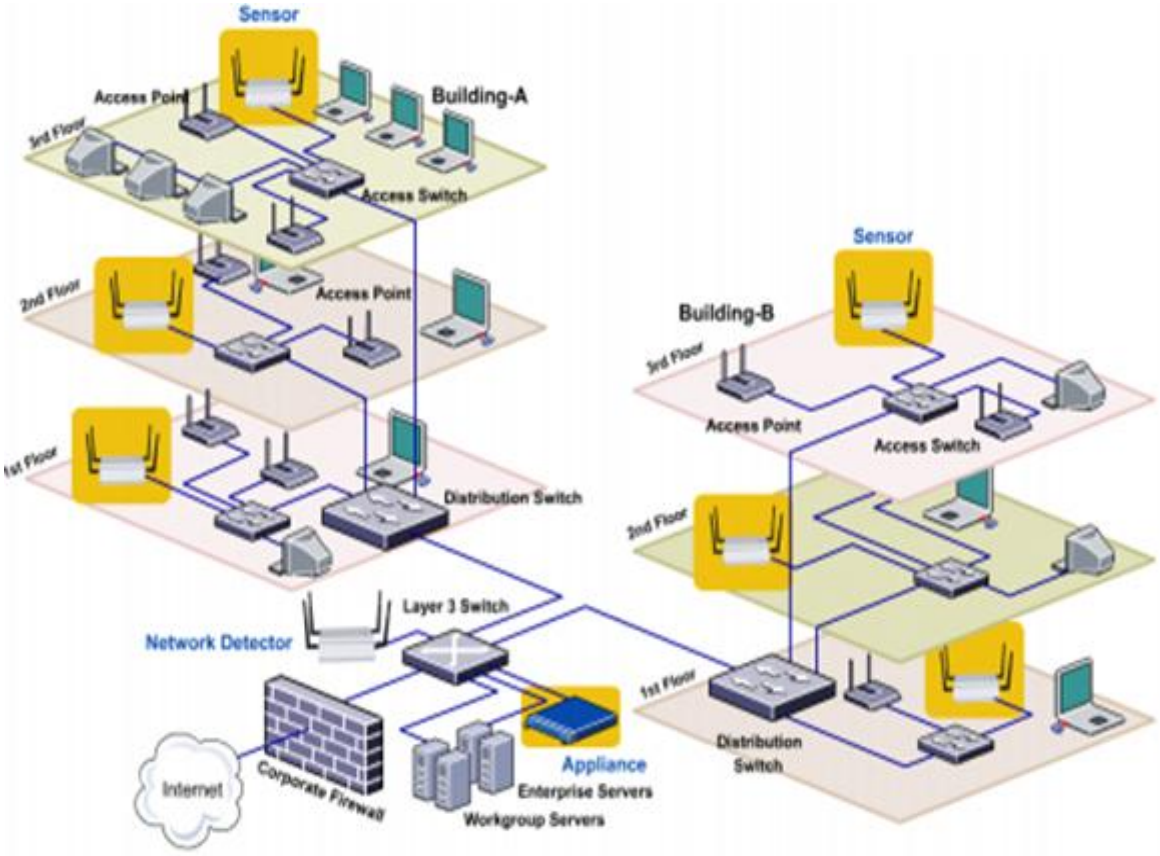
- sensor faqatgina simsiz interfeyslarni boshqarish uhun;
- ko’p karrali VLAN lar faqat Ethernet interfeyslari uchun;
- sensor ham simsiz interfeyslarni va cheklangan miqdordagi VLAN lar Ethernet interfeyslarni boshqarish uchun sozlanadi. Sozlanmalar rejimi 2.12 rasmda ko’rsatilgan.



2.12 rasm. Sozlanmalar rejimi

HP Mobility Xavfsizlik IDS/IPS tizimi RF menejeri va MSM415 sensori yordamida:

- avtomatik tajovuz tahdidlarni aniqlash va oldini olish;
- xavfsizlik siyosati va markaziy boshqaruv;
- kompleks hisobot;
- rollarga asoslangan ma'muriy huquqlar;
- auto mdix;
- simsiz trafik ichini 360 daraja ko‘ra olish kabi qulytliklarga ega [11].



2.13 rasm. HP Mobility Xavfsizlik IDS / IPS tizimi RF menejeri va MSM415 sensoridan iborat korporativ tarmoq

Axborotning butunligi va foydalanishga qulayligi apparat vositalar zaxirasini yaratish, foydalanuvchilarning xato harakatlarini blokirovka qilish, kompyuter tizimlarining ishonchli elementlaridan va barqaror ishlovchi tizimlardan foydalanish yo‘li bilan amalga oshiriladi. Tizim elementlarini qasddan ortiqcha ishlatish tahdidlari bartaraf etiladi. Buning uchun bajariladigan dasturlarga buyurtmalarni kelib tushish intensivligini o‘lchash mexanizmlaridan va bunday buyurtmalarni berishni cheklash yoki blokirovka qilish mexanizmlaridan foydalaniladi. Bunday hollarda ma’lumotlarni uzatish yoki dasturlarni bajartirishga bo‘lgan buyurtmalar oqimining birdaniga keskin oshib ketishini aniqlash imkoni ham oldindan nazarda tutilgan bo‘lishi kerak. Korporativ tarmoqlarda axborotlarning butunligi va foydalanishga qulayligini ta’minlashning asosiy shartlaridan biri ularning zaxiralarini hosil qilishdan iborat. Axborotlar zaxirasini

yaratish strategiyasi axborotning muhimligini, korporativ tarmoqning uzluksiz ishlashiga bo‘lgan talablarni, ma’lumotlarni tiklashdagi qiyinchiliklarni hisobga olgan holda tanlanadi. Himoyalangan korporativ tarmoqlarda faqatgina ruxsat etilgan dasturiy ta’minotdan foydalanilishi lozim. Foydalanishiga rasman ruxsat etilgan dasturlarning ro‘yxati, ularning butunligini nazorat qilishning usullari va davriyligi korporativ tarmoqni ekspluatatsiya qilinishidan oldin aniqlanishi kerak.

2.4 Himoyalangan korporativ tarmoqning himoyalanganlik darajasi va samaradorligini baholashda WhatsUp-Gold dasturiy ta’minoti

Himoyalanishni tahlillash texnologiyasi tarmoqni nozik joylarini topish, bu ma’lumotlarni umumlashtirish va ular bo’yicha hisobot berish imkoniyatiga ega. Agar bu texnologiyani amalga oshiruvchi tizim adaptiv komponentga ham ega bo’lsa, aniqlangan zaifliklarni avtomatik tarzda bartaraf etish mumkin. Himoyalanishni taxlillash texnologiyasi tarmoq xavfsizligi siyosatini, uni tashkilot tashqarisidan yoki ichkarisidan buzishga urinishlardan oldin, amalga oshirishga imkon beruvchi ta’sirchan usul hisoblanadi. Xujumlarni aniqlash korporativ tarmoqdagi shubhali xarakatlarni baholash jarayoni. Xujumlarni aniqlash operatsion tizim va ilovalarqni qaydlash jurnallarini yoki real vaqtdagi trafikni taxlillash orqali amalga oshiriladi. Tarmoq uzellari yoki segmentlarida joylashtirilgan xujumlarni aniqlash komponentlari turli hodisalarni, xususan, ma’lum zaifliklardan foydalanuvchi harakatlarni ham baholaydi. Asosiy vazifalari:

- kompyuter va axborot texnologiyalaridan foydalanishda ular bilan g‘ayriqonuniy munosabatda bo‘lishga yo‘l qo‘ymaslik masalalari bo‘yicha operatorlar hamda provayderlarning kompyuter xavfsizligi bo‘linmalari hamda milliy axborot tizimining boshqa sub'yektlari sa'y harakatlarini muvofiqlashtirish;
- foydalanuvchilar, kompyuter texnikasi va dasturiy ta'minot ishlab chiqaruvchilar tomonidan kompyuter tarmoqlari xavfsizligiga bugungi kunda mavjud tahdidlar to‘g‘risidagi axborotlarni, shuningdek, muayyan kompyuter hodisalari va kompyuter tizimlarini muhofaza qilishda qo‘llanilayotgan texnik-

dasturiy vositalarning samaradorligiga oid materiallarni yig‘ish, ularni tegishli ma'lumotlar bazasida jamlash va tahlil qilish;

- foydalanuvchilarga xatarlarni baholashda konsultativ xizmat va texnik yordam ko‘rsatish, ularni ro‘y berishi mumkin bo‘lgan xavf-xatarlardan o‘z vaqtida xabardor qilish, kompyuter xavfsizligini ta'minlash borasidagi huquqiy-normativ bazani takomillashtirish bo‘yicha takliflar berish va boshqalar. Xizmat turlari:
- korporativ tarmoq xavfsizligi auditi;
- web-saytlarning texnologik auditi;
- serverlar axborot xavfsizligi holatining tahlili;
- korporativ tarmoqqa texnik yordamdan keyingi ko‘maklashuv va monitoring.

Korporativ tarmoq xavfsizligi auditi deganda, mustaqil auditorlik xizmati tomonidan kompaniya axborot resurslarining xavfsizligini har tomonlama tahlil qilish tushuniladi. Bunda kompaniya xavfsizlik tizimidagi zaifliklar aniqlanib, tarmoqning muhofaza qilinganlik darajasini oshirish bo‘yicha qator chora-tadbirlar belgilanadi. Ma'lum bo‘lishicha, "buzib ochish"larning 80 foizi kompaniyaning o‘zida, uning xodimlari ishtirokida sodir etilar ekan. Aynan, shu narsa mustaqil auditorlik xizmati tahlili o‘tkazilishi kerakligini belgilovchi bosh omillardan biridir. Zotan, faqat mohir va yuqori malakali mutaxassislargina xavfsizlik tizimining barcha zaif jihatlarini aniqlab, muhofazaning strategiyasi, siyosati hamda arxitekturasini ishlab chiqish hamda joriy etishga qodir.

Kompyuter tarmoqlarining qay darajada muhofaza qilinganligini baholash uchun turli testlar o‘tkaziladi. Bular: skanerlash, "yengil" hamda "og‘ir" test va boshqalardir. Ruxsatsiz, xufiyona kirib olishni aniqlash testlarini o‘tkazish ishonchli muhofaza tizimini yaratish borasidagi eng kerakli dastlabki qadam deyish mumkin [11].

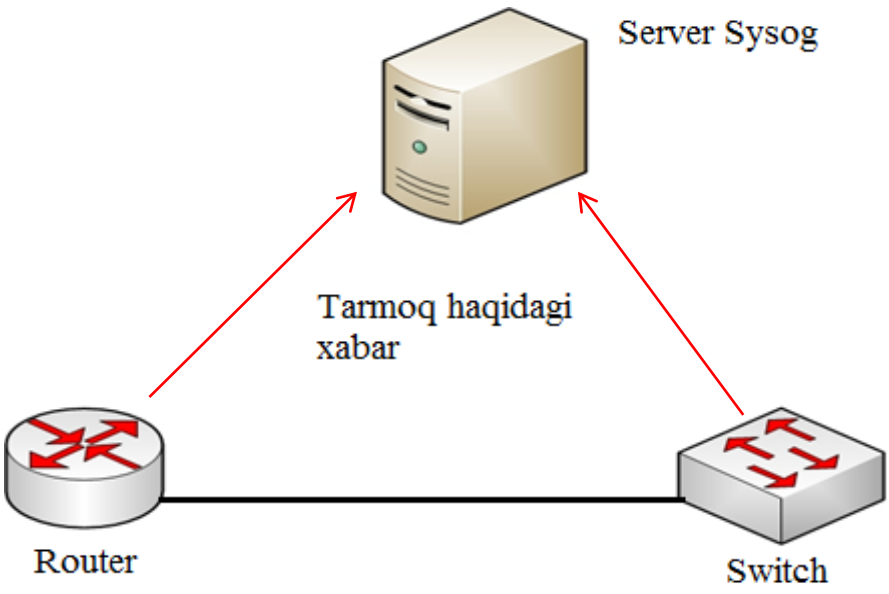
Korporativ tarmoqning himoyalanganlik darajasini aniqlash tarmoqni tahlil qilish va undagi jarayonlarni monitoringi tarmoqni samarali boshqarish uchun ma'lumot va boshqa mutaxassislar uchun tarmoqdan foydalanish bo'yicha statistik

hisobotlarni yaratish imkonini beradi. Shu bilan bir qatorda aktiv ulanishlardagi xatolik darajasini aniqlash va kanallarning holati undan foydalanishni darajasini aniqlashda bir necha omillar bor. Ma’lumotlarni to'plash va uzoq vaqt davomida saqlash bu ma'lumot tarmoq mamuri tomonidan tahlil qilish va undagi vujudga kelgan yoki kelishi mumkin bo’lgan xatolik kamchiliklarni oldindan aniqlash va shu qismini o'zgartirish uchun loyihalash, shuningdek, taxmin qilish imkonini beradi.

Tarmoq mamurlarining o’z tarmog'ini kuzatib tahlil qilib borishlari uchun foydalanishi mumkin bo’lgan quydagi protokollar mavjud:

- Syslog
- SNMP
- NetFlow

Bu protokollarning o’ziga yarasha kuchli va zaif tomonlari bor, har biri mashhur protokollar hisoblanadi. Ular birgalikda tarmoqni tahlil qilish uchun samarali vosita hisoblanib Protokol NTP (tarmoq vaqt bayonnomasi) turli qurilmalar log fayllarni solishtirish uchun harakat, ayniqsa, muhim ahamiyatga ega bo'lgan barcha qurilmalar uchun vaqtni sinxronlashtirish uchun ishlatiladi. Syslog ishlash prinspi 2.14 rasmda keltirilgan.

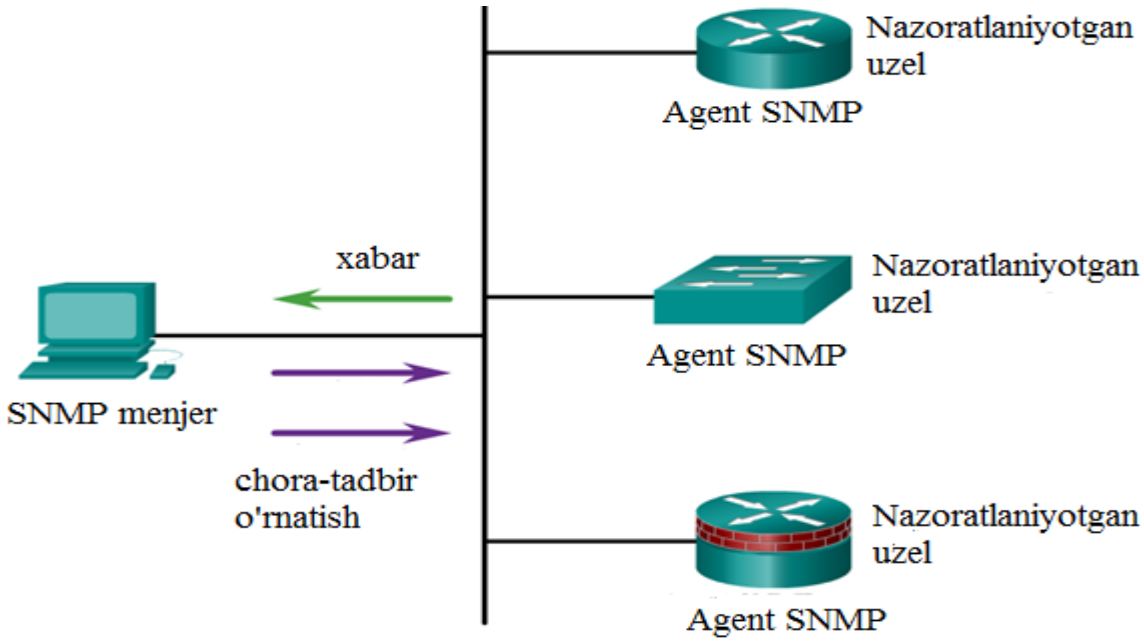


2.14 rasm. Syslog protokolli strukturasi

Tarmoq mamurlari tarmoq infratuzilmasi va qurilmalar holati haqidagi xabarlar haqida xabardor bo'lib turishlari uchun, syslog protokollini tarmoq qurimalariga sozlaydilar va qurilmalar protokoll yordamida belgilangan vaqt davomida o’zlari va tarmoqdagi bo’layotgan jarayonlarni belgilangan manzil bo’yicha log fayl ko’rinishida muntazam yuborib turishadi.

Rasmda ko’rsatilgaidek tarmoq serveri bir ish stansiyasidagi syslog xabarlarni ko'rish uchun syslog interfeysi o'rnatilgan bo'lishi kerak. Iterfeys orqali tarmoq mamuri syslog to’plagan ma’lumotlardagi voqea jarayonlar qiymati sana vaqti va shu kabi xabarlarga asoslanib aniq xarakatlanishi mumkin. Syslog protokolli IP tarmoqlari orqali voqealar bildirishnoma yuborish uchun UDP-514 porti foydalaniladi.

SNMP (Simple Network Management Protocol) protokolli orqali tarmoq ma’murlari tarmoq qurilmalari mashrutizatorlar, kommutatorlar, ishchi stansiyalar, tugunlar yani uzellarni nazorat qilish imokonini beradi. Bu tarmoq operatsiyalarini kuzatib qidirish va tarmoq muammolarni hal etish, hamda tarmoq o'sishi uchun rejalar ishlab chiqish uchun samarali hisoblanadi. SNMP ishlash strukturasi 2.15 rasmda keltirilgan.



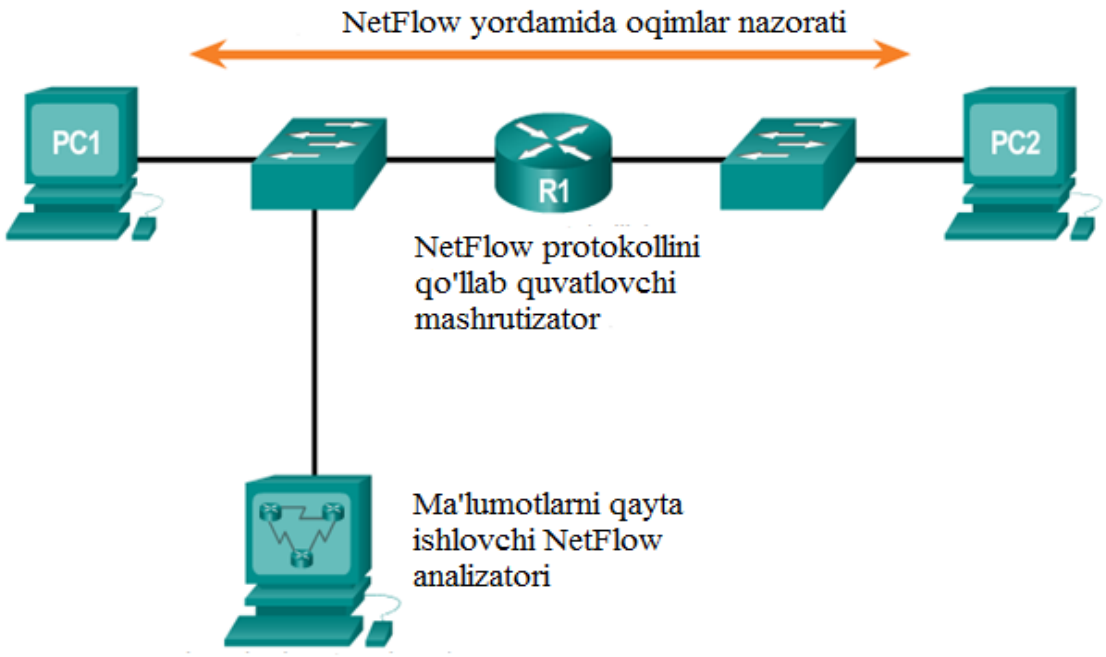
2.15 rasm. SNMP protokolli stukturasi

SNMP agent mijoz tarmoq qurilmasiga joylashtiriladi. Tarmoq qurilmalari bunday dasturiy moduli agent SMNP bilan jihozlangan marshrutizatorlar, serverlar, xavfsizlik devorlari va ishchi stantsiyalarini nazorat qilinishini ta’minlaydi. SNMP qabul qilish va xabar yuborish uchun, UDP-162 portidan foydalanadi. SNMP tizimi uch unsurdan iborat:

- menejer SNMP (tarmoq menejeri);
- agent SNMP (boshqariladigan tugun);
- boshqaruv ma'lumotlar bazasi (MIB).

SNMP interfeysli dasturiy ta’minot orqali boshqariladi. Rasmda ko'rsatilgandek, biri SNMP menejer bo'lsin muzokara tomonidan SNMP agenti ma'lumotlarni to'plash va SNMP menejeriga yuboradi, olingan xabardan foydalanib tarmoq qurilmalardagi sozlanmalarini o'zgartirishingiz, yoki xatoliklarni bartaraf etishingiz mumkin.

NetFlow texnologiyasi korporativ tarmoq qurilmalari qismlariga konfiguratsiya yordamida transport satxidagi patok yani oqimlarni tahlil qilish va eksport ma'lumotlar uchun yanada murakkab parametrlarini yaratish uchun imkon beradi. NetFlow protokoli ishlash stukturasi 2.16 rasmda keltirilgan.



2.16 rasm. NetFlow protokoli

NetFlow protokoli bu oqim uchun bayt va paketlar sonini kuzatib, ular ustidan nazoratni amalga oshiradi, ma'lumotlar yig'uvchi (kollektor) NetFlow deyiladi. NetFlow protokoli monitoring uchun standartga aylangan va hozirda keng tarmoq sanoatini qo’llab quvvatlanadi.

WhatsUp Gold – dasturi Cisco kompaniyasi tomonidan tarmoqni kompleks nazorat qilish va tarmoqdagi xatoliklar, kamchiliklar, yuzaga kelishi mumkin bo’lgan noxush holatlarni monitoring, ularni eksplutatsiya qilish uchun ishlab chiqilgan dasturiy ta’minot hisoblanadi. Markazlashgan boshqaruvni tashkil etish hamda kompleks monitoring, tarmoqni tahlil qilishda SNMP, SYSLOG, NETFLOW protokollari yordamida tarmoq holati, unda ro’y berayotgan jarayonlar haqida ma’lumot to’plash, jurnalga qayd qilish va hisobot ko’rinishida tayorlashni amalgam oshiradi.

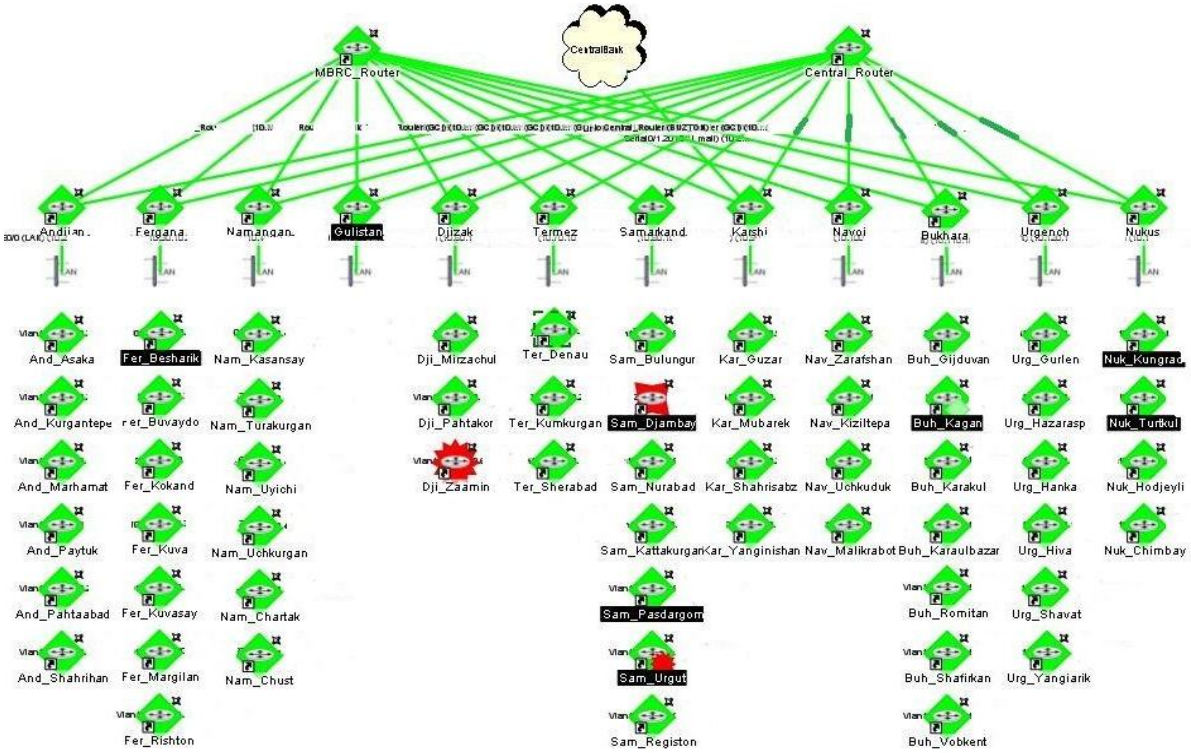
WhatsUp Gold dasturiy ta’minoti orqali korporativ tarmoqlardagi qurilmalarni, 25-25000 tagacha foydalanuvchilarni monitoring qilish imkoniyatiga ega bo’lib korporativ tarmoqda joylashgan tarmoq qurilmalari va uning filialaridagi qurilmalarni doimiy ravishda nazorat qilish va ularga virtual bog’lanib nosozliklarni bartaraf etish imkoniyatining mavjudligi. Dastur inerfeysi 2.17 rasmda ko’rsatilgan.

2.17 rasm. WhatsUP- Gold dasturi interfeysi

WhatsUP- Gold dasturi interfeysi quydagi bo’limlardan iborat:

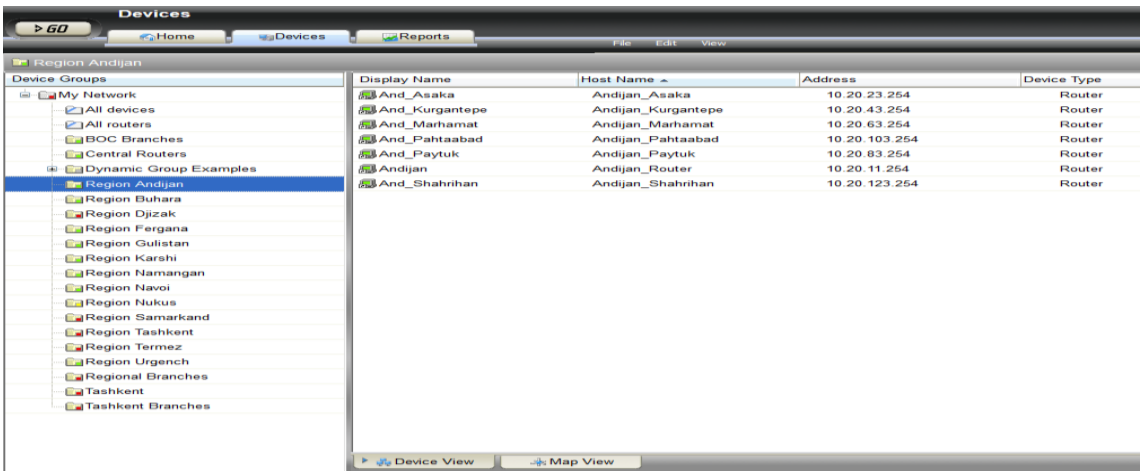
- Home;
- Devices;
- Reports.

O’zbekiston Respublikasi “Milliy banki” korporativ tarmoqlarini yani o’zidagi ichki lokal tarmog’i, shaxar, viloyat, tumanlardagi filiallarini monitoring qilish va doimiy nazorat qilib boorish uchun WhatsUp Gold dasturiy ta’minotidan foydalanar ekan. Bu dasturiy ta’minot juda qulay hisoblanib foydalanuvchi uchun sodda interfeysli ko’rinishda ishlab chiqilgan. Banknig filialari orasidagi tarmoq 2.18 rasmda ko’rsatilgan.



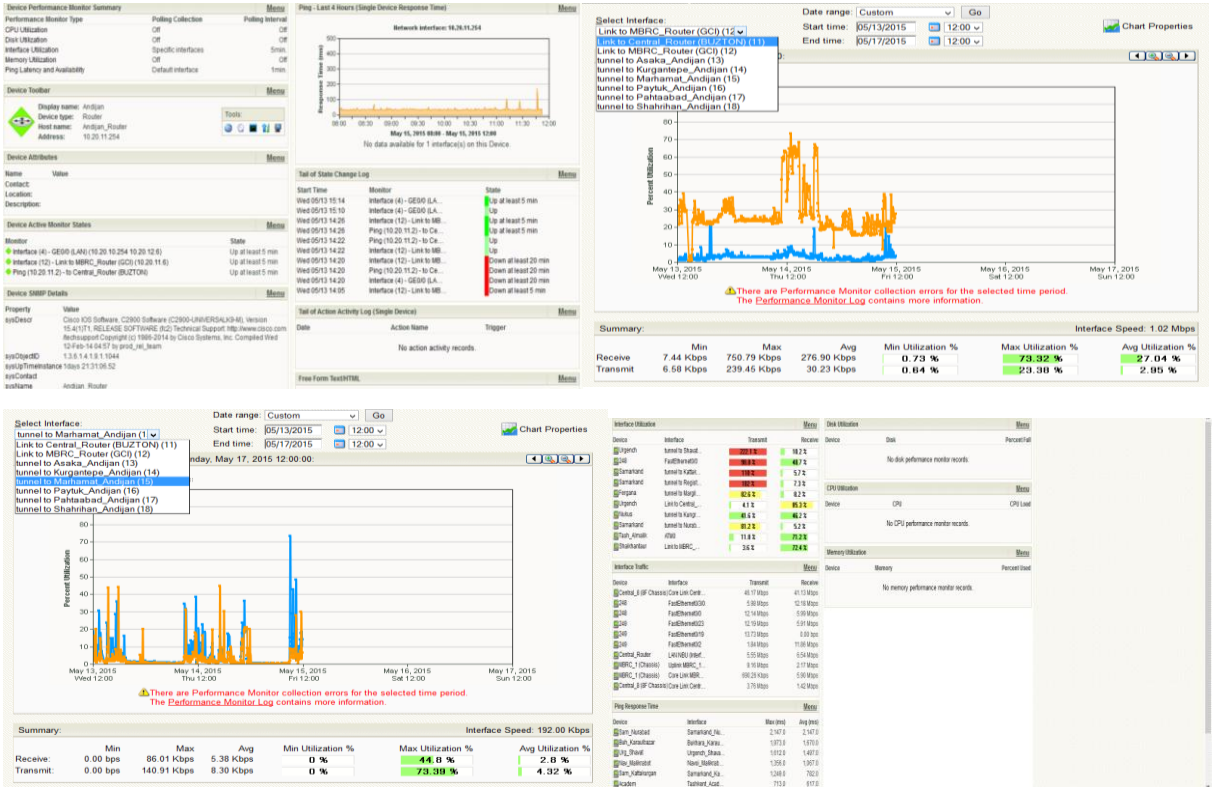
2.18 rasm. Milliy bankning fillialari orasidagi tarmoq

Dastur yordamida tarmoqdagi ro’y berayotgan barcha holatlarni kuzatib borish imkoniyatlarning mavjudligi va bu holatlar, jarayonlar to’g’risida hisobot tayorlash kabi qulayliklarga egaligi, korporativ tarmoqni himoyalanganlik darajasi va samaradorligi haqida yetarlicha ma’lumotga ega bo’lish imkoniyatini beradi.



2.19 rasm. Bankning fillialari

Dastur orqali bankning Andijon viloyati va tumanlarida joylashgan fillialarini monitoringini ko’rip chiqamiz.



2.20 rasm. Tarmoq monitoringi

Mazkur rasmda Andijon viloyati Marhamat tumanidagi bankning tarmog’i holati, traffik tahlili, nosozliklar va shu kabi boshqa ko’plab ma’lumotlar keltirilgan. Bu ma’lumotlar yordamida tarmoq ma’muri bu nosozliklarni bartaraf etishi noxush holatlarni oldini olish imkoniyatiga ega bo’ladi [11].

III.bob. Hayot faoliyati xavfsizligi

3.1. Hayot faoliyati xavfsizligini ta’minlashni huquqiy me'yoriy va tashkiliy asoslari

Mehnat muhofazasi huquqiy, ijtimoiy-iqtisodiy texnologik va sanitariya me'yorlari sistemasi bo'lib, mehnatkashlarni ishlash sharoiti va hayot faoliyati xavfsizligini ta'minlaydi. Mehnat muhofazasi hayot faoliyat xavfsizligi fanining mutaxassislikka tegishli asosiy qismini o'rganadi. Aniq muammolar, transport vositalari, texnologik jarayonlar, ish turlari, bino va inshootlar uchun xavfsizlikni ta’minlash har bir fanning mutaxassislik kursida beriladi.

1992 yilning 8-dekabrida O'zbekiston Respublikasi Konstitutsiyasining qabul qilinishi mamlakatimiz hayotida ulkan siyosiy voqea bo'ldi. Hech bir davlat o'zining asosiy qonunida davlat va jamiyat qurilishining tamoyillarini, fuqaroning huquq va erkinliklarini, jamiyat taraqqiyotining iqtisodiy asoslari hamda strategik yo'nalishlarini mustahkamlamasdan turib, demokratik, huquqiy suveren davlat bo'la olmaydi. Respublikamiz konstitusiyasi demokratik, xalqaro miqyosida etibor berilgan meyor va talablarga javob beradi deyishga to'la asosimiz bor. Bozor iqtisodiyotiga o'tish va ijtimoiy barqarorlikni yetarli emasligi ishchilarni ishlash bo'yicha huquqlariga, ularning mehnatini muhofazalash, talab darajasidagi ish sharoitlarini yaratishga oid muammolarni ko'payishiga sabab bo'ldi. Barcha hamdo'stlik mamlakatlaridagi kabi O'zbekistonda ham so'ngi yillarda deyarli ko'pchilik xalq xo'jaligi soxalarida mehnat sharoiti yomonlashuvi tendentsiyasi kuzatildi. Ishlab chiqarishda yangi tashkil etilayotgan xususiy sektorlarning unumini ortishi bu soxadagi ko'rsatkichlarni yanada pasayishiga sabab bo'ldi. Bunday ishlab chiqarishda band bo'lgan ishchilar mehnatini muxofazalash, ularga talab darajasida mehnat sharoitini yaratish haqida ushbu soxa mas'ullari turli sabablarga ko'ra etarlicha e'tibor qarata olmayapti deb bo'lmaydi. Ularning ayrimlari bu soxada etarli bilim va tajribaga ega bo'lmasa, ayrimlari bu haqda umuman tushunchaga ega emas desak mubolag’a bo'lmaydi. Chunki, bunday ishlab chiqarish sub'ektlarini chiqarish raxbarlari, ish yurituvchilar, ish boshliqlarining ichida o'rta ma'lumotli, o'rta maxsus ma'lumotli raxbarlar ham

etarli. Ba'zan mutaxassisliklari ishlab chiqarish yo'nalishiga to'g’ri kelmaydigan xodimlar ham ular ichida uchrab turadi. Yuqorida aytilgan kamchiliklardan tashqari muttasaddi tashkilotlar tomonidan bunday ishlab chiqarish korxonalarining faoliyatlari yetarlicha, samarali nazorat qilinayapti deyish qiyin. Ishchilarni ishlab chiqarishda hayot faoliyati xavfsizligini ta’minlash bo'yicha asosiy me'yoriy qonunchilik aktlarining qabul qilinishi bilan hozirgi vaqtda bu muammolar holati birmuncha ijobiy tomonga o'zgarmoqda.

Xavfsiz mehnat qilish huquqi O'zbekiston Respublikasi Konstitusiyasining 37-moddasida mustaxkamlab qo'yilgan. Mehnat muxofazasi bo'yicha koronalardagi, muassasalardagi asosiy qonunchilik aktlari O'zbekiston Respublikasining mehnat kodeksi, fuqarolik kodeksi va mehnatni muxofaza qilish to'g’risidagi qonunlari hisoblanadi.

O'zbekiston Ruspublikasining 1993-yil 6-maydan kuchga kiritilgan Mehnatni muhofaza qilish to'g’risidagi qonuni ishchilar va ish beruvchilar o'rtasidagi mehnatni muxofaza qilishga oid munosabatlarni tartibga solishni huquqiy asoslarini belgilaydi.

O'zbekistonda birinchi marta ish beruvchilar bilan mehnat munosabatlariga kirishayotgan jismoniy shaxslar mehnatini muhofazasi muammolarini aniq echimiga bog’liq har xil savollar qonunchilik darajasida ko'rilmoqda. Bu qonunlar ish bajaruvchilarga ham ular bilan mehnat munosabatlarida bo'ladigan ishlovchilarga ham, hamda ta'lim muassasalarini, ishlab chiqarish amaliyotlarini o'tayotgan o'quvchi va talabalarga ham bir xil ta'sirga egadir. Qonunchilik mehnat munosabatlarida bo'lgan barcha ishtirokchilarni, ular xox jismoniy, xox xuquqiy shaxs bo'lishidan va qanday shaklda faoliyat yuritayotganidan qat'iy nazar mehnat muxofazasi talablarini so'zsiz bajarilishi shart ekanligiga urg’u beradi. Ushbu qonun ish beruvchilar va ishlovchilar munosabatidagi mehnat muxofazasi sistemalari rolini aniqlaydi. Agar korxona va tashkilotda mehnat muxofazasi bo'yicha xizmat yoki mutaxassis bo'lmasa, ish beruvchi mehnat muxofazasi bo'yicha xizmat ko'rsatadigan mutaxassis yoki tashkilot bilan tegishli shartnomani tuzishi shart. Ish beruvchi ishlovchilarni mehnat muxofazasi talablari bilan

tanishtirishi va har bir ish joyida mehnat muxofazasi talablariga mos keladigan sharoitni yaratishi, ish joylarini mehnat sharoiti bo'yicha attestatsiyadan o'tkazishga burchlidir. Ish beruvchi ishlovchi bilan mehnat shartnomasini tuzishda ishchini o'z xisobidan tibbiy ko'rikdan o'tkazishi lozimligi qonunda belgilangan. Ish beruvchi ishchilarni faoliyati davomida ham quyidagi hollarda tibbiy ko'rikdan o'tkazish ishlarini tashkil etishi shart:

- 18 yoshga to'lmaganlar;
- 60 yoshga to'lgan erkaklar, 55 yoshga to'lgan ayollar;
- nogironlar;
- mehnat sharoiti noqulay ishlarda, tungi ishlarda, shuningdek transport xarakati bilan bog’liq ishlarda band bo'lganlar;
- oziq-ovqat sanoatida, savdo va bevosita axoliga xizmat ko'rsatish bilan bog’liq bo'lgan boshqa tarmoqlardagi ishlarda band bo'lganlar;
- umumta'lim maktablari, maktabgacha tarbiya va boshqa muassasalarning bolalarga ta'lim yoki tarbiya berish bilan mashg’ul bo'lgan pedagog va boshqa xodimlari.

Tibbiy ko'riklardan o'tishdan bo'yin tovlashga xodim haqli emas. Tibbiy komissiyalarning tekshiruvlar natijasida bergan tavsiyalarini bajarishdan bo'yin tovlagan xodimlarni ish beruvchi ishga qo'ymaslikka haqlidir. Agar ishchining sog’ligi ish sharoitining salbiy ta'sirida yomonlashgan bo'lsa u navbatdan tashqari tibbiy ko'rikdan o'tkazishni talab qilishga haqli.

Tibbiy ko'riklardan o'tkazish qayd etilgan hollarda korxona (ish beruvchi) mablag’i hisobiga amalga oshiriladi. Ish joylarida to'liq, zararsiz va xavfsiz ish sharoitini yaratish amalda mumkin emas. Shu sababli mehnat muxofazasining vazifasi zararli va xavfli ishlab chiqarish omillarinining ishlovchilarga zararli ta'sirini eng kam darajaga keltirishga imkon beradigan chora-tadbirlarni amalga oshirishdan, ishlovchilarni shikastlanishlarini oldini olishdan, yuqori mehnat unumdorligiga erishishga yordam beradigan qulay sharoitlarni yaratishdan iborat.

Texnika xavfsizligi - ishlovchilarga ishlab chiqarishda texnika xavfsizligini, uning oldini oladigan tashkiliy chora-tadbirlar va texnika vositalari sistemasi.

Yong’in xavfsizligi - ob'ektda yong’in paydo bo'lish xavfini oldini olish, shuningdek moddiy boyliklarni muxofaza qilishdan iborat. Ishlab chiqarish sanitariyasi, ishlab chiqarishdagi zararli omillar ta'sirini oldini oladigan chora-tadbirlar va texnika vositalari sistemasi. Ishlab chiqarishdagi xavfli omil ishlab chiqarishda ishlovchilarga muayyan sharoitlarda ta'sir yetganda shikastlanishga yoki sog’liqning keskin yomonlashuviga olib keladigan omil. Xarakatlanayotgan mashina, mexanizm, yuk ko'tarish vositalari bilan ko'tariladigan yuk, mashina va mexanizmlarning muxofazalanmagan aylanuvchi, ilgarilanma, qaytma harakat qiluvchi qismlar (kardanli, zanjirli, tishli, tasmali, friksion uzatma) ning harakati xavfli omillar qatoriga kiradi. Ishlab chiqarishdagi zararli omil, ishchilarga ish vaqtida ta'sir etib kasallanishga yoki ish qobiliyatining pasayishiga olib keladigan omil. Zararli omillarga neft maxsulotlari (benzin, dizel yoqilg’isi bug’lari, pestisidlar, mineral o'g’itlar, chang, shovqin, titrash, tebranish), ish joyida namlikni ortishi yoki kuchli yoritilganligi, iqlim sharoitlari va boshqalar kiradi.

Elektr xavfsizligi - kishilarni elektr toki, elektr yoyi, elektrmagnit maydonining zararli va havfli ta'siridan muxofaza qilishni ta'minlaydigan tashkiliy va texnik chora-tadbirlar sistemasi.

Shikastlanish - ishlab chiqarishdagi zararli yoki xavfli ta'sirlar natijasida inson organlari yoki teri qoplamasi fiziologik butunligini buzilishi.

Mehnat sharoiti - mehnat jarayonida insonning salomatligi va ish qobiliyatiga ta'sir etadigan omillar majmui.

Shaxsiy himoyalanish vositalari - bir xodimni muxofaza qilish uchun xizmat qiladigan vositalar. Shaxsiy himoya vositalariga - ish kiyimi, poyafzal, gaz niqoblar, respiratorlar, niqoblar, shlemlar, himoya ko'zoynaklari, quloqchinlar va boshqalar kiradi. Ishlab chiqarishdagi baxtsiz hodisa - ish vaqtida yuz beradigan hodisa.

Kasb kasalligi - kishi organizmiga ish sharoitlarining zararli ta'siri natijasida kelib chiqqan (surunkali changli bronxitlar, titrash kasalligi, har xil kimyoviy

preparatlar bilan zaxarlanish) kasalliklardir. Ruxsat etilgan konsentratsiya (daraja, miqdor) (REK, RED, REM) - 8 soatli yoki boshqa ish kuni, shuningdek haftasiga 40 soatdan ortiq bo'lmagan, ishlashi davomida kasallik yohud sog'ligida o'zgarishlar keltirib chiqarmaydigan konsentratsiya (daraja, miqdor) [10].

3.2. O'zbekiston Respublikasida mehnat muxofazasini nazorat qiluvchi tashkilotlar

Mehnat muxofazasi bo'yicha qonunlarning bajarilishini nazorat qilib turish quyidagi davlat tashkilotlariga yuklatilgan:

- O'zbekiston Respublikasi Mehnat va aholini ijtimoiy muxofaza qilish vazirligi;
- "Sanoatkontexnazorat" agentligi;
- O'zbekiston Respublikasi Sog'liqni saqlash vazirligining sanitariya epidemiologiya nazorati;
- Respublika Ichki ishlar vazirligining yong'indan muxofaza qilish Bosh boshqarmasi;
- O'zbekiston Respublikasi energetika va elektrlashtirish Davlat aksionerlik jamiyati.

Mehnat va aholini ijtimoiy muxofaza qilish vazirligi korxonalarda xavfsiz ishlash, texnika xavfsizligi bo'yicha me'yor qoidalariga, sanoat sanitariyasi va mehnat gigienasiga hamda mehnat qonunchiligiga rioya qilish masalalarini nazorat qiladi. har bir tarmoq o'z texnik inspektoriga ega. "Sanoatkontexnazorat" agentligi bug' qozonlarining to'g'ri ishlashini, bosim ostida ishlaydigan idishlarni, yuk ko'tarish mashinalari (ko'tarma kranlar, liftlar), ekskovatorlar, gaz uskunalari magistral quvurlari ishini va portlovchi moddalarni ishlatish, saqlash va tashish ishlarini nazorat qiladi [10].

Respublika sanitariya-epidemiologiya nazorati havo, suv va tuproqni ifloslanishdan ogohlantirish, shovqin va titrashni yo'qotish, sexlarning sanitariya holatlarini yaxshilash (harorat, nisbiy namlik, yoritilganlik va x.k.) ishlarini nazorat qiladi.

Davlat yong’in nazorati yong’inga qarshi tadbirlarni, o’t o'chirish vositalarining holatini, yong’in haqida xabar berish vositalarining ishini nazorat qiladi.

O'zbekiston Respublikasi energetika va elektrlashtirish Davlat aksionerlik jamiyati korxonalardagi energiya tizimlarining texnik ekspluatasiyasini va xavfsizlik texnikasi qoidalariga rioya qilishni nazorat qiladi. Barcha ishlab chiqarish korxonalarida uch pog’onali nazorat amalga oshiriladi.

- pog’ona - har kuni usta jamoatchi-nazoratchi birgalikda sexdagi ish joylarini aylanib chiqib, uchragan kamchiliklarni tuzatish choralarini ko'radilar.
- pog’ona - har hafta sex boshlig’i katta jamoatchi nazoratchi bilan birgalikda sexdagi ish joylarini aylanib chiqib, uchragan kamchiliklarni tuzatish choralarini ko'radi.
- pog’ona - oyda bir marta korxona bosh muxandisi mehnat muxofazasi muxandisi bilan birgalikda ish joylarini aylanib chiqadilar. Bu nazorat bo'yicha korxonada qaror chiqariladi.

Barcha korxona, tashkilot, muassasa, vazirliklar va tarmoqlarda mehnat muxofazasi qonunlari bajarilishining oliy nazorati. Mehnat va aholini ijtimoiy muhofaza qilish vazirligiga yuklatilgan.

3.3. Elektromagnit maydonining inson organizmga ta'siri

Elektromagnit maydonining inson organizmiga ta'siri elektr va magnit maydonlarining kuchlanishi, energiya oqimining intensivligi tebranish chastotasi, nurlanishning tananing ma'lum yuzasida to'planishi va inson organizmining shaxsiy xususiyatlariga bog’liq bo'ladi. Elektromagnit maydonining inson organizmiga ta'sir ko'rsatishining asosiy sababi inson tanasi tarkibidagi atom va molekulalar bu maydon ta'sirida musbat va manfiy qutblarga bo'lina boshlaydi. qutblangan molekulalar elektromagnit maydoni tarqalayotgan yo'nalishga qarab xarakatlana boshlaydi. Elektromagnit maydonining inson organizmiga ta'siri natijasida qon, xujayralar oraliqidagi suyuqliklar tarkibida tashqi maydon ta'siridan ionlashgan toklar hosil qiladi. O'zgaruvchan elektr maydoni inson tanasi

xujayralarini o'zgaruvchan dielektrik qutblanish, shuningdek, o'tkazuvchi toklar hosil bo'lishi xisobiga qizdiradi. Issiqlik samarasi elektromagnit maydonlarining energiya yutishi xisobiga bo'ladi. Energiya yutilishi va ionlashgan toklarning hosil bo'lishi biologik xujayralarga maxsus ta'sir ko'rsatishi bilan kechadi, bu ta'sir inson ichki organlari va xujayralaridagi nozik elektr patensiallari ishini buzish va suyuqlik aylanish funksiyalarining o'zgarishi xisobiga bo'ladi. O'zgaruvchi magnit maydoni atom va molekulalarning magnit momentlari yo'nalishlarining o'zgarishiga olib keladi. Bu effekt inson organizmiga ta'sir ko'rsatish jixatidan kuchsiz bo'lsada, lekin organizm uchun befarq deb bo'lmaydi. Maydonning kuchlanishi qancha ko'p bo'lib uning ta'sir davri davomli bo'lsa, organizmga ko'rsatuvchi ta'siri shuncha ko'p bo'ladi [9].

Tebranish chastotasining ortishi tana o'tkazuvchanligi va energiya yutish nisbatini oshiradi, ammo kirib borish chuqurligini kamaytiradi. Uzunligi 10 sm dan qisqa bo'lgan to'lqinlarning asosiy qismi teri xujayralarida yutilishi tajriba asosida tasdiqlangan. 10-30 sm diapazondagi nurlanishlar teri xujayralarida kam yutiladi (30-40%) va asosan ularning yutilishi insonning ichki organlariga to'g’ri keladi. Bunday nurlanishlar nihoyatda xavfli hisoblanadi. Organizmda hosil bo'lgan ortiqcha issiqlik ma'lum chegaragacha inson organizmining termoregulyatsiyasi hisobiga yo'qotilishi mumkin. Issiqlik chegarasi deb ataluvchi ma'lum miqdordan boshlab (I>10 mVt/sm2), inson organizmda hosil bo'layotgan issiqlikni chiqarib tashlash imkoniyatiga ega bo'lmay qoladi va tana harorati ko'tariladi, bu esa o'z navbatida organizmga katta zarar etkazadi. Issiqlik yutilishi inson organizmining suvga serob qismlarida yaxshi kechadi (qon, muskullar, o'pka, jigar va x.k). Ammo issiqlik ajralishi qon tomirlari sust rivojlangan va termoregulyatsiya ta'siri kam bo'lgan organlar uchun juda zararlidir. Bularga ko'z, bosh miya, buyrak, ovqat xazm qilish organlari, o't va siydik xaltalari kiradi. Ko'zning nurlanishi ko'z korachig’ining xiralashishiga (kataraktaga) olib keladi. Odatda ko'z qorachig’ining xiralashishi birdaniga rivojlanmasdan, nurlangandan keyin bir necha kun yoki bir necha haftadan keyin paydo bo'ladi.

Elektromagnit maydoni inson organizmiga ma'lum o'tkazuvchanlikka ega bo'lgan dielektrik moddiy sifatida xujayralarga issiqlik ta'sirini ko'rsatibgina qolmasdan, balki bu xujayralarga biologik ob'ekt sifatida ham ta'sir ko'rsatadi. Ular to'g’ridan-to'g’ri markaziy nerv sistemasiga ta'sir ko'rsatadi, xujayralarning yo'nalishini o'zgartiradi yoki molekula zanjirini elektr maydoni kuchlanish chiziqlari yo'nalishiga aylantiradi, qon tarkibi oqsil molekulalari biokimyo faoliyatiga ta'sir ko'rsatadi. Qon tomir sistemasining funksiyasi buziladi. Organizmdagi uglevod, oqsil va mineral moddalar almashinuvini o'zgartiradi. Ammo bu o'zgarishlar funksional xarakterda bo'lib, nurlanish ta'siri to'xtatilishi bilan ularning zararli ta'siri va og’riq sezgilari yo'qoladi. Elektromagnit maydonini normalash va undan himoyalanish Respublikamizda yo'lga qo'yilgan nurlanishning ruxsat etilgan darajalari juda kam birlikni tashkil qiladi. Shuning uchun organizm uzoq vaqt nurlanish ta'sirida bo'lgan taqdirda ham hech qanday o'zgarish bo'lmasligi mumkin [8].

Sanitar me'yorlar bo'yicha ko'zda tutilgan “Yuqori, o'ta yuqori va xaddan tashqari yuqori chastotadagi elektromagnit maydonlari manbalarida ishlaganlar uchun sanitar norma va qoidalar” quyidagicha ruxsat etilgan norma va chegaralarni belgilaydi: ish joylarida elektromagnit maydoni radiochastota kuchlanishi elektr tarkibi bo'yicha 100 kGc-30 MGc chastota diapazonida 20 V/m, 30-300 MGc chastota diapazonida 5 V/m dan oshmasligi kerak. Magnit tarkibi bo'yicha esa 100 kGc- 1,5 MGc chastota diapazonida 5 V/m bo'lishi kerak. SVCH 30-300 000 MGc diapazonida ish kuni davomida ruxsat etiladigan maksimal nurlanish oqim kuchlanishi 10 mk Vt/sm2 , ish kunining 2 soatidan ortiq bo'lmagan vaqtdagi nurlanish 100 mk V/sm2 dan oshmasligi kerak. Bunda albatta muxofaza ko'zoynagi taqilishi kerak. qolgan ish vaqti davomida nurlanish intensivligi 10 mk Vt/sm2 dan oshmasligi kerak. SVCH diapazonida kabi nurlanish bilan bog’lanmagan kishilar va doimiy yashovchilar uchun nurlanish oqimi zichligi 1mk Vt/sm2 dan oshmasligi kerak. Yuqorida keltirib o'tilgan formulalarni tahlil qilish, elektromagnit maydonidan ish joylarini uzoqroq joylashtirish va elektromagnit maydonlari oqimlarini yo'naltiruvchi antennalar bilan ish joylari orasidagi

masofani o'zgartirish, generatorning nurlanish kuchlanishini kamaytirish, ish joylari bilan nurlanish oqimlari uzatilayotgan antennalar orasiga yutuvchi va kamaytiruvchi ekranlar o'rnatish, shuningdek, shaxsiy muhofaza aslaxalaridan foydalanish ish joylaridagi elektromagnit maydonlaridan muhofazalashning asosiy vositalari hisoblanadi. Oraliqni uzaytirish yo'li bilan erishiladigan muhofaza usuli eng oddiy va eng samarali xisoblanadi. Bu usuldan ish joylari elektromagnit maydonlaridan tashqarida bo'lgan ishchilar va shuningdek, nurlanuvchi qurilmalarni uzoqdan turib boshqarish imkoniyatini beradigan hollarda foydalanish mumkin. Bu usuldan foydalanish imkoniyati ish bajarilayotgan xona yetarlicha kattalikda bo'lgandagina muvoffaqiyatli chiqadi. Nurlanishni kamaytirishning yana boshqa usuli kuchli nurlanish generatorini, kuchsizroq nurlanish generatori bilan almashtirishdir. Lekin bu usulda texnologik jarayonni hisobga olish zarur. Nurlanish kuchini kamaytirishning boshqa usuli sifatida antennaga ekvivalent bo'lgan nurlanishni yutuvchi yoki kamaytiruvchi qurilmalarni antenyuatorlarni qo'llash, generatordan nurlanish tarqayotgan qurilmagacha bo'lgan oraliqdagi nurlanish kuchini yo'qotishi yoki kamaytirishi mumkin [10].

Xulosa

Ushbu bitiruv malakaviy ishini bajarish jarayonida, korporativ tarmoqlarning tarixi, rivojlanish bosqichlari, arxitekturasi, qurish texnologiyalari, tarmoq texnologiyalari va ularning topologiyalari, korporativ tarmoqlarga bo’ladigan tahdidlar, zaifliklar, hujumlar hamda ularga qarshi chora-tadbirlar keltirib o’tildi. Tarmoqni monitoring qilishda SYSLOG, SNMP, NETFLOW, protokollari hamda WhatsUP Gold dasturiy ta ‘minotidan foydalanildi. WhatsUP Gold dasturi quydagi protokollar yordamida korporativ tarmoqning himoyalanganlik darajasini aniqlash tarmoqni tahlil qilish va undagi jarayonlarni monitoringi tarmoqni samarali boshqarish uchun ma'lumot va boshqa mutaxassislar uchun tarmoqdan foydalanish bo'yicha statistik hisobotlarni yaratish imkonini beradi. Bu hisobot yordamida tarmoq ma’muri o’z tarmoqlarini qay holatdaligini va tarmoq ishlashidagi affzallik, kamchilik va xatoliklarini vaqtida qayd etib ularni oldini olish bartaraf etish, oldindan chora-tadbirlar ishlab chiqish, himoyalanganlik darajasi va samaradorligini baholash kabi qulayliklarga erishishlariga yordam beradi.

Foydalanilgan adabiyotlar ro‘yhati

1. Ўзбекистон Республикаси Президентининг қарори «Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигини ташкил этиш тўғрисида» 2015 йил 4 февралдаги ПФ-4702-сонли
2. Ахборот хавфсизлиги асослари: Маърузалар курси / физика-математика фанлари номзоди, катта илмий ходим И.М.Каримовнинг умумий таҳрири остида, Ўзбекистон Республикаси ИИВ Академияси, 2013. – 131 б.
3. Ғаниев. С.К, Каримов. М.М, Ташев К.А, Ахборот хавфсизлиги. Ахборот коммуникацион тизимлари хавфсизлиги. Тошкент “Алоқачи” 2008.
4. В.Ф Шаньгин Информационная безопасность копьютерных систем и сетей. 2011. - 416 с
5. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3.
6. K.A Tashev, N.B Nasrullaev, “Komyuter tizimlari va tarmoqlarida axborot xavfsizligi” fanidan lobaratoriya ishlarini bajarish uchun uslubiy ko’rsatmalar. Toshkent 2013 y.
7. Левин М. Безопасность в сетях Internet и Intranet. – М., 2001.
8. А.В Луковников, “Меҳнат мухофазаси”, Тошкент, Ўқитувчи 1984 й.
9. G.E G’oipov “Mehnat muxofazasi”, Toshkent, Mehnat 2000 y.
10. O. Qudratov, T. G’aniev, “Favqulotda vaziyatlarda fuqaro muxofazasi” Toshkent 2005 y.
11. http://www. Intuit.ru
12. http://www. Netacad.com
13. http://www. Ziyonet.uz
14. http://www. My.gov.uz