O’ZBEKISTON RESPUBLIKASI OLIY VA O’RTA MAXSUS TA’LIM VAZIRLIGI

BUXORO MUHANDISLIK TEXNOLOGIYA INSTITUTI

«Informatika va axborot texnologiyalari» kafedrasi

5140900 – Kasb ta’limi(«Informatika va axborotlar texnologiyalasi») ta’lim yo’nalishi bo’yicha

««Axborot xavfsizligining usul va vositalari » fanidan “Kompyuter tarmog`ida informatsiya himoyasi” moduli bo`yicha laboratoriya ishlarini bajarish uchun elektron qo`llanma yaratish » mavzusidagi

BITIRUV MALAKAVIY ISH

Bajardi: **14-09 MIIT guruhi talabasi Ibragimov Nusratilloxon**

Rahbar: **kat.o`qt. Ibragimov U.M.**

Himoyaga ruxsat etildi

“____”_____2013y.

Kafedra mudiri: _____ dots. Razzoqov Sh.I.

BUXORO - 2013

14-09MIITguruxitalabasiIbragimov Nusratning ««Axborot xavfsizligining usul va vositalari » fanidan “Kompyuter tarmog`ida informatsiya himoyasi” moduli bo`yicha laboratoriya ishlarini bajarish uchun elektron qo`llanma yaratish» mavzusidagibitiruvmalakaviyishiga

ANNOTATSIYa

Hammaga ma`lumki hozirgikundazamoniyinformatsiontexnologiyalarrivojlanganpaytdaInternet tarmog`idan nafaqat mutaxassislar balki ixtiyoriy sohadagi mutaxassislar ham keng ma`noda foydalanib kelmoqda. Bugungi kunda korxona va tashkilotlarda simsiz kompyuter tarmoqlarining roli juda oshib ketdi. Shu uchun O`zbekistonda ham simsiz kompyuter tarmoqlari rivojlanmoqda. Endilikda korxonalar o`z ishlarini avtomatlashtirishda ham simsiz kompyuter tarmoqlaridan dasturlardan keng foydalanib kelishmoqda, shuninguchunKasbiyta`lim (Informatikavaaxborottexnologiyalari) yo’nalishitalabalarigazamonaviyinformatsiontexnologiyalarniqo’llashdakompy uter tarmoqlaridan foydalanib ma`lumotlarni almashinish uchun dasturiy vositalardan foydalanish talabimuhimo’rinlardanbiriniegallaydi. Buyo’nalishdatalabalargakompyuter tarmoqlaridan ma`lumot almashinishjarayonida ularda uchrab turadigan hujumlarni bartaraf etish ko’nikmalarnishakllantirishmaqsadidaushbu elektron qo`llanma yaratildi.Kompyuter tarmoqlarida himoya elektron qo`llanmasi ixtiyoriy kompyuter tarmoqlarida uchraydigan hujumlarni ko`rsatib beradi. Kompyuter tarmoqlarida himoya elektron qo`llanmasidan foydalanib talabalar kompyuter tarmoqlarida qanday hujumlarni amalga oshirish mumkinligini ko`rishlari va bajarib ko`rishlari uchun ushbubitiruvmalakaviyishiqo’yildi. Bitiruvmalakaviyishiningyanabiryutug’ishundaki, undanafaqatAxborot xavfsizligining usul va vositalari faniningo’rganishda, kompyuter tarmoqlari va tizimlari faninio’zlashtirishdahamqo’lkeladi.

UshbuBMIningtarkibi: Kirish, Nazariyqism, Asosiyqism, Pedagogikqism, Hayotfaoliyatixavfsizligiqismi, Ilova, Xulosa, Adabiyotlarro’yxati.

Kirishqismidamavzuningqo`yilishi, dolzarbligi, ahamiyativakutilayotgannatijalarhaqidagapboradi.

Nazariyqismdakompyuter tarmoqlari, ayniqsa simsiz tarmoqlarning turlari va ularda bo`ladigan hujumlar to`g`risida zaruriy ma`lumotlarkeltirilgan. Mavzugadoirtayanchma`lumotlarnazariyqismdakiritilgan.

Asosiyqismdaslax va wireshark dasturimuhitidahujumlarni qanday amalga oshirish usullariniqo’llashmumkinligi vaularni bajarish ketma-ketligi haqidama`lumotkeltirilgan, shubilanbirgalikdadasturiy maxsulotni o`rnatish ketma-ketligito’liqtushunarliqilibyoritilgan.

Hayotfaoliyatixavfsizligiqismidakompyuter xonalarida kompyuterdan foydalanish tartiblari va elektr toki haqida ma`lumot keltirilgan.

Xulosaqismidabuelektron qo`llanmaning ahamiyati, undanfoydalanishvayutuqlarikeltirilgan.

Ilova. Asosiyqismtarkibigakiritilganbo'libdasturiy vosita valistingiko'rsatilgan.

AdabiyotlarroʼyxatidaBMInitayyorlashdakerakbo'lganbarchaadabiyotlarro'yxatikiritilgan.

Mundarija

KIRISH

Mening bitiruv malakaviy ishim mavzusi ““Axborot xavfsizligining usul va vositalari” fanidan “Kompyuter tarmog’ida informatsiya himoyasi” moduli bo’yicha laboratoriya ishlarini bajarish uchun elektron qo’llanma” yaratish deb nomlanadi.

Informatsion texnologiyalar va Internet global tarmog’ining juda ham tez rivojlanishi inson faoliyatining barcha yo’nalishlariga ta’sir o’tkazuvchi informatsion sohaning paydo bo’lishiga olib keldi. Korporativ information tarmoqlar hozirgi kunda har bir zamonaviy tashkilotning eng asosiy vositalaridan biri bo’lib kelmoqda.Ular an’anaviy biznes ko’rinishini elektron biznesga aylantirishga imkon beradi.

Elektron biznes tashkilot faoliyatining har tomonlama effektivligini oshirish uchun global Internet tarmog’i va zamonaviy informatsion texnologiyalarini ishlatadi, masalan, ishlab chiqarish, reklama, marketing, savdo-sotiq, soliq va bank tizimi, moliya tizimi, ishchilarni qidirish, mijozlarni qo’llab – quvvatlash va hamkorlik aloqalari uchun.

Masalaning qo’yilishi. Kompyuter taqmoqlarida informatsiya himoyasining asosiy tushunchalarini yoritib berish va kompyuter tarmoqlarida uchraydiganhujumlarni ko`rsatuvchi elektron elektron qo`llanma yaratish. Yaratiluvchi elektron elektron qo`llanmada nafaqat kompyuter tarmoqlari hujumlari haqida ma’lumot berishilishi, balki, talabaning o`zi ham bajarib ko`rishi uchun ketma-ketlikda ko’rgazmali namoyish etib talabalarga tushunarli bo’lishi ta`minlashi kerak.

Bitiruv malakaviy ishning maqsadi. “Axborot xavfsizligining usul va vositalari” fanidan “Kompyuter tarmog’ida informatsiya himoyasi” moduli bo’yicha laboratoriya ishlarini bajarish uchun elektron qo’llanma yaratish.

Mavzuning dolzarbligi. Elektron biznesni yaratishda ma’lumot xavfsizligi eng muhim omillardan biri hisoblanadi. Buning ostida korporativ ma’lumotlarning va tashkil etilgan infrastrukturaning tashkilot yoki uning mijozlariga zarar keltirishi mumkin bo’lgan tasodifiy va uyushtirilgan hujumlardan himoyalanganligi tushuniladi.

Ma’lumotlar xavfsizligining buzilishi kompaniyaga juda ham katta zarar keltirishi, hatto uning to’la-to’kis yopilishiga ham olib kelishi mumkin. shuning uchun ma’lomotlar xavfsizligini ta’minlash nafaqat kompyuter tarmoqlari va tizimlari sohasidagi mutaxassislar, bundan tashqari elektron biznes bilan shug’ullanuvchi judako’plab foydalanuvchilar va tashkilotlar ham muhim hisoblanadi.

Kutilayotgan natijalar. Yaratilgan elektron elektron qo`llanma xohlagan dasturchi va ayniqsa informatika va axborot texnologiyadari yo’nalishida tahsil oluvchi talabalar hamda bo’lajak tarmoq administratorlari kompyuter tarmoqlarini yaratishda uchraydigan hujumlar va ularni bartaraf etish usullarini oson tushunishlari va Kasb ta`limi (Informatika va axborot texnologiyalari) yo’nalishi talabalariga “Axborot xavfsizligining usul va vositalari” fanidan tajriba mashg’ulotlarini bajarishda ma`lumotnoma sifatida foydalanilishi mumkin.

Bitiruv malakaviy ish Kirish,Mavzu bo’yicha nazariy ma`lumotlar, Asosiy qism, Pedagogik qism, Hayot faoliyati havfsizligi, Xulosa, Foydalanilgan adabiyotlar ro’yxati va dastur ilovalari kabi qismlardan iborat.

Kompyuter tarmog’ida informatsiya himoyasi

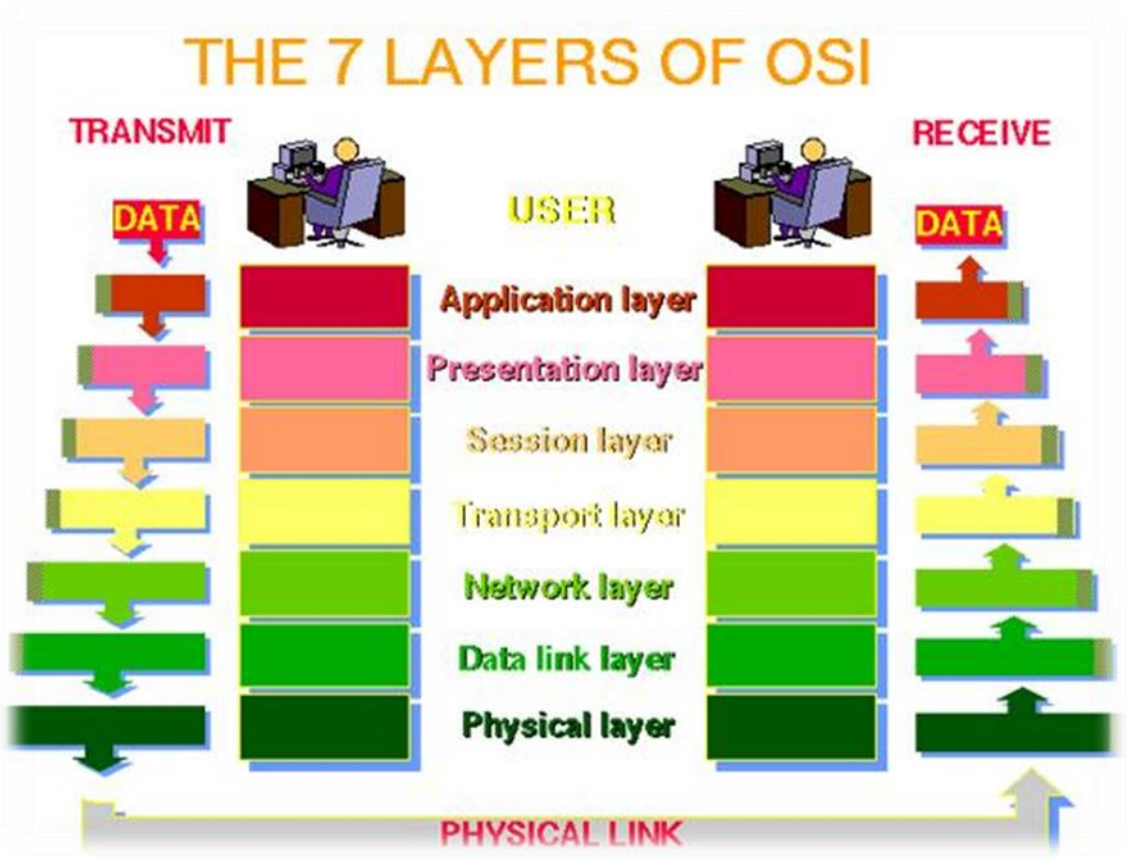
Kompyuter tarmoqlarini qurishda asosiy vazifalardan biri qurilmalarni elektrik va mexanik xarakteristikalari mosligini va kodlashtirish tizimlari va ma’lumotlar formatlari mosligini ta’minlash. Bu masalani yechish standartizatsiyalashtirish sohasiga tegishli.Kompyuter tarmoqlarida asosiy metodik standartizatsiyalash - tarmoqlararo vositalarni ishlab chiqarishda ko’p darajali usulda yondashish. Bunday yondashuvlar va Xalqaro standartlashtirish instituti ISO (International Standarts Organization) ning texnik takliflari asosida 1980-yillar boshida ochiq tizimlar o’zaro aloqasi standart modeli OSI (Open Systems Interconnection) ishlab chiqildi. ISO/OSI modeli kompyuter tarmoqlari rivojida asosiy rol o’ynadi.

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.

Ochiq tizimar o’zaro aloqasi ISO/OSI va TCP/IP stek protokollari

ISO/OSI modeli tizimlar o’zaro aloqasining turli darajalarini aniqlaydi va har qaysi daraja qaysi funksiyani amalga oshirishini ko’rsatib beradi.

OSI modelida o’zaro aloqa vositalari yettita darajaga bo’linishadi: dasturiy (Application), taqdim etish (Presentation), seans (Session), transport (Transport), tarmoq (Network), kanal (Data Link) va fizik (Physical). Eng yuqori daraja – dasturiy.Bu darajada foydalanuvchi dasturlar bilan ma’lumot almashadi.Eng quyi daraja esa – fizik. Bu daraja 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.

Kerakli moslikni ta’minlash uchun kompyuter tarmoqlari arxitekturasining har bir darajasida maxsus standart protokollar mavjud. Ular bitta darajada turgan, lekin tarmoqning turli xil uzellarida joylashgan tarmoq komponentlari o’zaro almashinadigan xabarlar ketma-ketligi va formatini aniqlaydigan tartiblangan qoidalar to’plamini o’zida mujassamlashtiradi.

Tarmoqda uzellar o’zaro aloqasini tashkil etish uchun yetarli bo’lgan ierarxik tashkil etilgan protokollar to’plami *kommunikatsion protokollar steki* deb aytiladi. ISO/OSI modeli va ISO/OSI protokollar stekini aniq ajrata olish kerak. ISO/OSI modeli ochiq tizimlar o’zaro aloqasining konseptual sxemasi hisoblanadi, ISO/OSI protokollar steki esa ISO/OSI modelida aniqlangan yettita daraja uchun aniq va konkret bo’lgan protokollar spetsifikatsiyasini o’zida akslantiradi.

Kommunikatsion protokollar ham dasturiy ham apparat vositalar yordamida tashkil etilishlari mumkin. Quyi daraja protokollari odatda dasturiy va apparat vositalar kombinatsiyasi orqali, yuqori daraja protokollari esa – qabul qilinganidek faqat dasturiy vositalar yordamida tashkil etiladi.

Qo’shni daraja protokollarini tashkil etuvchi va tarmoqning bir uzelida joylashgan modullar bir - birlari bilan ham mos ravishda qat’iy aniqlangan qoidalar va standartlashtirilgan xabarlar asosida o’zaro aloqa qilishlari zarur. Bu qoidalarni *darajalararo interfeys* deb atash qabul qilingan.Darajalararo interfeys bir darajadan qo’shni darajaga ma’lumot yetkazib beradigan xizmatlar to’plamini aniqlaydi. Umuman olganda, protocol va interfeys bir – biriga yaqin tushuncha hisoblanadi, ammo tarmoqlarda ularga turli sohalardagi vazifalar yuklatilgan: protokollar bitta darajadagi, ammo turli tarmoq uzellaridagi modullar o’zaro aloqasi qoidalarini aniqlashadi, interfeyslar esa bir uzeldagi qo’shni darajalar orasidagi modullar o’zaro aloqasi qoidalarini aniqlashadi.

TCP/IP steki o’zaro aloqa qiluvchi protokollarninig butun bir to’plamini o’zida mujassamlashtiradi. Ulardan eng muhimi internetda bir kompyuterdan ko’plab oraliq tarmoqlar, shyluzlar va marshrutizatorlar orqali boshqa kompyuterga marshrut (yoki marshrutlar) qidirish va shu marshrutlar bo’yicha ma’lumotlar bloklarini uzatish uchun javob beradigan IP protokoli va ma’lumotni ishonchli yetkazib berish, xatosizlik va uzatilgan ma’lumotni to’gri tartibda qabul qilib olish uchun javob beradigan TCP protokollari hisoblanadi.

TCP/IP steki rivojiga o’zining UNIX operatsion tizimi versiyasida steklar protokolini tashkil etgan, dasturlar va ularning boshlang’ich kodlarini ommabop va bepul tarzda tarqatgan Berklidagi Kaliforniya universiteti katta hissa qo’shdi.

Ushbu operatsion tizimning mashhur bo'lishi IP, TCP va boshqa stek protokollarining keng tarqalishiga sabab bo'ldi. Hozirgi kunda bu stek butun jahon axborot tizimi Internet tarmog'ida kompyuterlar orasidagi aloqani ta'minlashda, hamda juda ko'plab korporativ tarmoqlarda ishlatilmoqda.TCP/IP steki tarmoqlarni tashkil etishdagi eng keng tarqalgan vosita hisoblanadi.

TCP/IP stekining keng qamrovda qo'llanilishining asosiy sabablari uning quyidagi xususiyatlari bilan tushuntiriladi:

- ancha tugatilgan standartlangan va shu bilan birga ko'p yillik tarixga ega bo'lgan keng tarqalgan tarmoq protokollari steki;
- qariyb barcha katta hajmdagi tarmoqlar o'zining asosiy trafigini TCP/IP protokoli orqali uzatadi;
- barcha zamonaviy operatsion tizimlar TCP/IP stekini qo'llab – quvvatlaydi;
- Internet tarmog'iga ulanish usuli;
- turli xil tizimlarni ham transportli tizimostilar darajasida, ham amaliy servislar darajasida tarmoqni tashkil etishda juda keng imkoniyatlarga egaligi;
- Internetda ishlab chiqarilgan Internetning transportiv xizmatlarini va WWW gipermatn texnologiyasini ishlatadigan korporativ intranet – tarmoqlar yaratish uchun asos;
- mijoz – server dasturlari uchun mustahkam kengayuvchi platforma-aro muhit.

Kanal darajasidagi xafvsizlik – PPTP va L2TP protokollari

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.

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. 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.

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. Dastlab, kanal darajasida joylashgan PPP protokoli ma'lumotlarni inkapsulyatsiyalashtirish va ularni nuqta – nuqta ulanishida yetkazib berish uchun ishlab chiqilgan edi. Bu protokol asinxron ulanishlarni tashkil etishda ham ishlatiladi.

PPP to'plamiga ulanishni boshqaruvchi protokol LCP (Link Control Protocol) va tarmoqni boshqaruvchi protokol NCP (Network Control Protokol) kiradi. LCP protokoli nuqta – nuqta ulanish konfiguryatsiyasi, o'rnatilishi, ishlashi va tugatilsihiga javobgar. NCP protokoli esa nuqta – nuqta ulanishi orqali transportirovkani amalga uchun tarmoq darajasini PPP protokoliga inkapsulyatsiya qila oladi. Bu esa bir vaqtning o'zida bitta ulanish orqali Novell IPX va Microsoft IP paketlarini uzatishga imkon beradi.

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.

Fizik va kanal darajalarida PPTP va L2TP protokollari bir xil ishlaydi, lekin shu bilan ularning o’xshashligi tugaydi va farqlanishlar boshlanadi.

PPTP protokoli

Microsoft kompaniyasi boshchiligida va boshqa bir qator kompaniyalar hamkorligida ishlab chiqilgan PPTP (Point-to-Point Tunneling protokol) protokoli masofadan turib ulanuvchi foydalanuvchilarning mahalliy tarmoqqa Internet tarmog'i orqali ulanish imkoniyati bo'lganda himoyalangan virtual kanallar yaratish uchun mo'ljallangan.

Microsoft kompaniyasi o'zining operatsion tizimlarida PPTP protokolini keng qo'llaganligi uning tez tarqalishiga sabab bo'ldi. Ba'zi bir tarmoqlararo ekran va VPN shlyuzlar ishlab chiqaruvchilar ham PPTP protokolini qo'llab – quvvatlaydilar. PPTP protokoli himoyalangan kanallarni yaratishda ma'lumot almashinuvi uchun IP, IPX va NetBEUI protokollarini qo'llashga imkon beradi. Bu protokollar ma'lumotlari PPP kadrlariga joylashtiriladi va PPTP protokoli yordamida IP protokoli paketlariga inkapsulyatsiya qilinadi va bu paketlar istalgan TCP/IP tarmog'i orqali shifrlangan holatda ko'chiriladi.

PPTP sessiyasida uzatiladigan paketlar quyidagi strukturaga ega bo'lishadi:

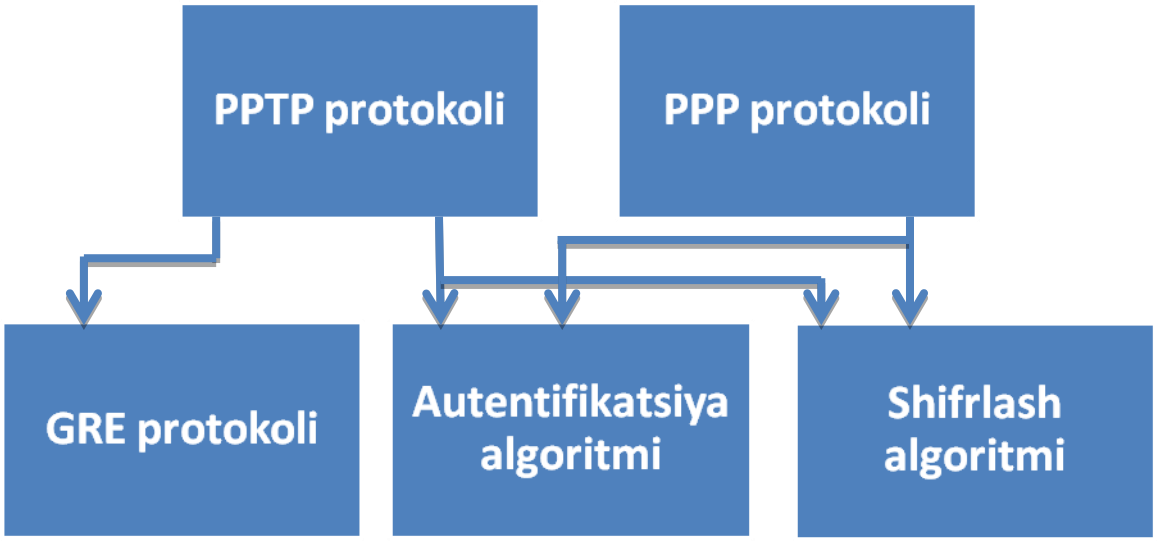
- Internet tarmog'i ichida ishlatiladigan kanal daraja sarlavhasi, masalan Ethernet kadri sarlavhasi;
- uzatuvchi va paket qabul qiluvchi manzilini saqlaydigan IP sarlavha;
- GRE (Generic Routing Encapsulation) marshrutizatsiyasi uchun inkapsulyatsiyaning umumiy metodi sarlavhasi;
- o'zida IP, IPX va NetBEUI paketlarini saqlovchi dastlabki PPP paket.

Uzatish kadri sarlavhasi	IP sarlavhasi	GRE sarlavhasi	PPP sarlavhasi	Shifrlangan PPP ma'lumotlar	Kadr uzatishning oxiri

Qabul qiluvchi uzel IP paketlardan PPP kadrlarni ajratib oladi, keyin esa PPP kadrdan dastlabki IP, IPX va NetBEUI paketni ajratib oladi va uni lokal tarmoq orqali konkret adresatga jo'natadi. Kanal darajasidagi inkapsulyatsiyalanadigan protokollar turiga kiruvchi PPTP protokoli kabi protokollarning ko'p – protokolligi, yuqoriroq darajadagi himoyalangan kanal protokollaridan afzal jihati bo'lib hisoblanadi. Masalan, agar korporativ tarmoqda IPX yoki NetBEUI ishlatilayotgan bo'lsa, IPSec yoki SSL protokollarini qo'llab bo'lmaydi, chunki ular tarmoq darajasi IP protokolining faqat bittasini qo'llab – quvvatlay oladi.

Inkapsulyatsiyaning ushbu usuli OSI modeli tarmoq darajasi protokollaridan mustaqillikni ta'minlaydi va ochiq IP – tarmoqlar orqali istalgan mahalliy (IP, IPX va

NetBEUI) tarmoqlarga masofadan turib ulanishni amalga oshirishga imkon beradi. PPTP protokoliga asosan himoyalangan virtual tarmoq yaratishda masofadan turib ulanuvchi autentifikatsiyalanadi va uzatiladigan ma’lumotlar shifrlanadi.



Masofadan turib ulanuvchi foydalanuvchi autentifakatsiyasi uchun PPP da qo’llaniladigan turli xil protokollar ishlatilishi mumkin. Microsoft kompaniyasi tomonidan Windows operatsion tizimlarida yo’lga qo’yilgan PPTP protokolida quyidagi autentifikatsiya protokollari qo’llab – quvvatlanadi:

- PAP (Password Authentication Protocol) parol bo’yicha protokoli;
- ikki tomonlama qo’l siqish MSCHAP (Microsoft Challenge – Handshaking Authentication Protocol) protokoli;
- EAP - TLS (Extensible Authentication Protokol – Transport Layer Security) protokoli.

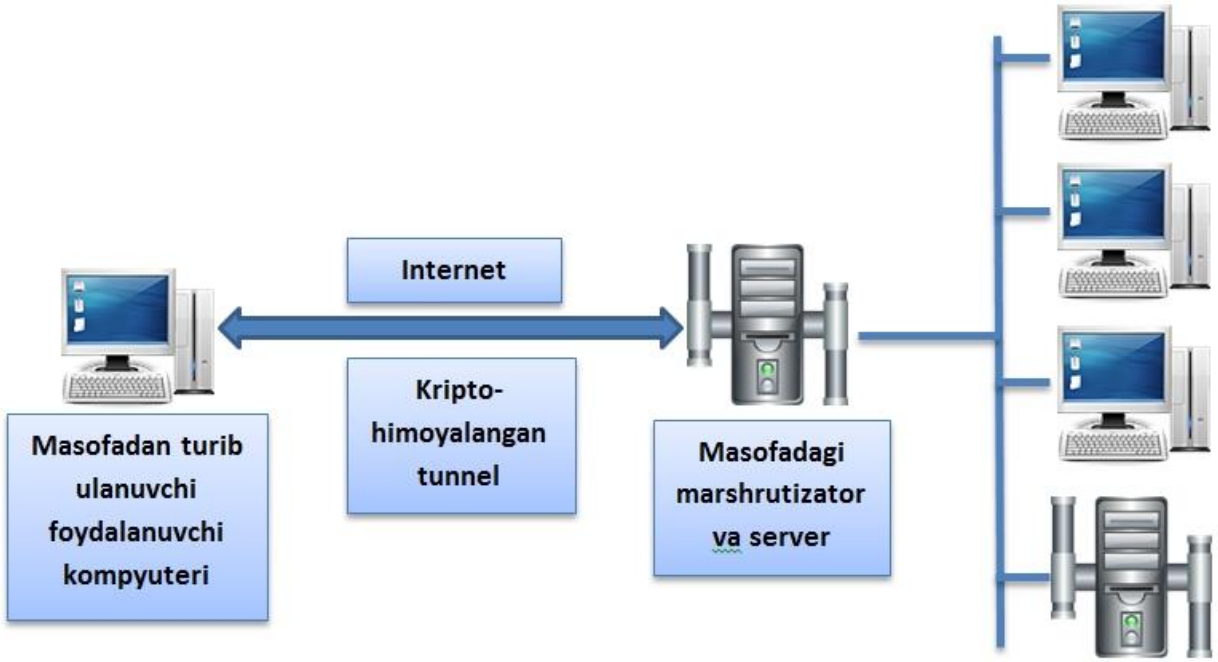
PAP protokoli ishlatilganda identifikatorlar va parollar aloqa liniyalari orqali shifrlanmagan holda uzatiladi, va faqat server mijoz autentifikatsiyasini amalga oshiradi.

MSCHAP va EAP – TLS protokollari ishlatilganda yovuz niyatli shaxslar tomonidan qo’lga kiritilgan shifrlangan paketlarning qayta ishlatilishidan himoya va mijoz va VPN – server o’rtasida ikki tomonlama autentifikatsiya ta’minlanadi.

PPTP yordamida shifrlash Interner orqali ma’lumot almashinuivda hech kim ushbu ma’lumotlarni qo’lga kirita olmasligini ta’minlaydi.MPPE (Microsoft Point – to – Point Encryption) shifrlash faqat MSCHAP (1 va 2 - versiyalar) va EAP – TLS

bilan mos keladi va mijoz va server o’rtasidagi parametrlar mosligi ta’minlangan holda shifrlash kaliti uzunligini avtomatik tanlay oladi. MPPE shifrlash 40, 56 va 128 bit uzunlikdagi kalitlar bilan ishlay oladi. PPTP protokoli shifrlash kaliti qiymatini har bir paket qabul qilinganidan keyin o’zgartiradi.

PPTP protokoli masofadan turib ulanuvchi foydalanuvchi kompyuterining to’g’ridan – to’g’ri Internetga ulanishini tunnellashtirish sxemasida qo’llaniladi. Bu tunnellashtirish sxemasini ko’rib chiqamiz.



Masofadan turib ulanuvchi foydalanuvchi mahalliy tarmoq bilan ulanishni masofadan turib ulanish xizmati RAS (Remote Access Service) ning mijoz qismi yordamida o’rnatadi; RAS Windows tarkibiga kiradi. Keyin esa foydalanuvchi masofadagi mahallit tarmoq serveriga uning IP – adresini ko’rsatib murojaat qiladi, va u bilan PPTP protokoli orqali aloqa o’rnatadi. Masofdagi server vazifasini lokal tarmoqning chetki marshrutizatori bajarishi mumkin.

Masofadan turib ulanuvchi foydalanuvchi kompyuterida Windows NT tarkibiga kiruvchi RAS xizmatining mijoz qismi va PPTP drayveri, masofadagi serverda esa Windows NT Server tarkibiga kiruvchi RAS serveri va PPTP drayveri o’rnatilgan bo’lishi kerak. PPTP protokoli ikki tomon o’zaro almashinadigan bir nechta xizmatchi xabarlarni aniqlaydi. Xizmatchi xabarlar TCP protokoli orqali uzatiladi.

Muvaffaqiyatli autentifikatsiyadan so’ng himoyalangan ma’lumot almashinuvi jarayoni boshlanadi. Lokal tarmoq ichki serverlari PPTP protokolini qo’llab – quvvatlamasliklari mumkin, chunki tashqi marshrutizator IP paketlardan

PPP kadrlarni ajratib oladi va uarni kerakli IP, IPX yoki NetBIOS formatida lokal tarmoq orqali jo’natadi.

L2TP protokoli

OSI modelining kanal darajasidagi himoyalangan virtual tarmoqlarni qurish uchun Cisco Systems kompaniyasi tomonidan PPP protokoliga alternativ L2F (Layer-2 Forwarding) protokoli ishlab chiqilgan. L2F protokoli PPTP protokolidan turli xil tarmoq protokollarini qo'llashi va Internet provayderlar uchun qulayligi bilan farq qiladi. Masofadan turib ulanuvchi foydalanuvchi kompyuteri va server aloqasini ta'minlash uchun L2F protokoli turli xil masofadan turib ulanish protokollarini qo'llay oladi, masalan, PPP, SLIP. Ammo, L2F protokoli quyidagi kamchiliklarga ega:

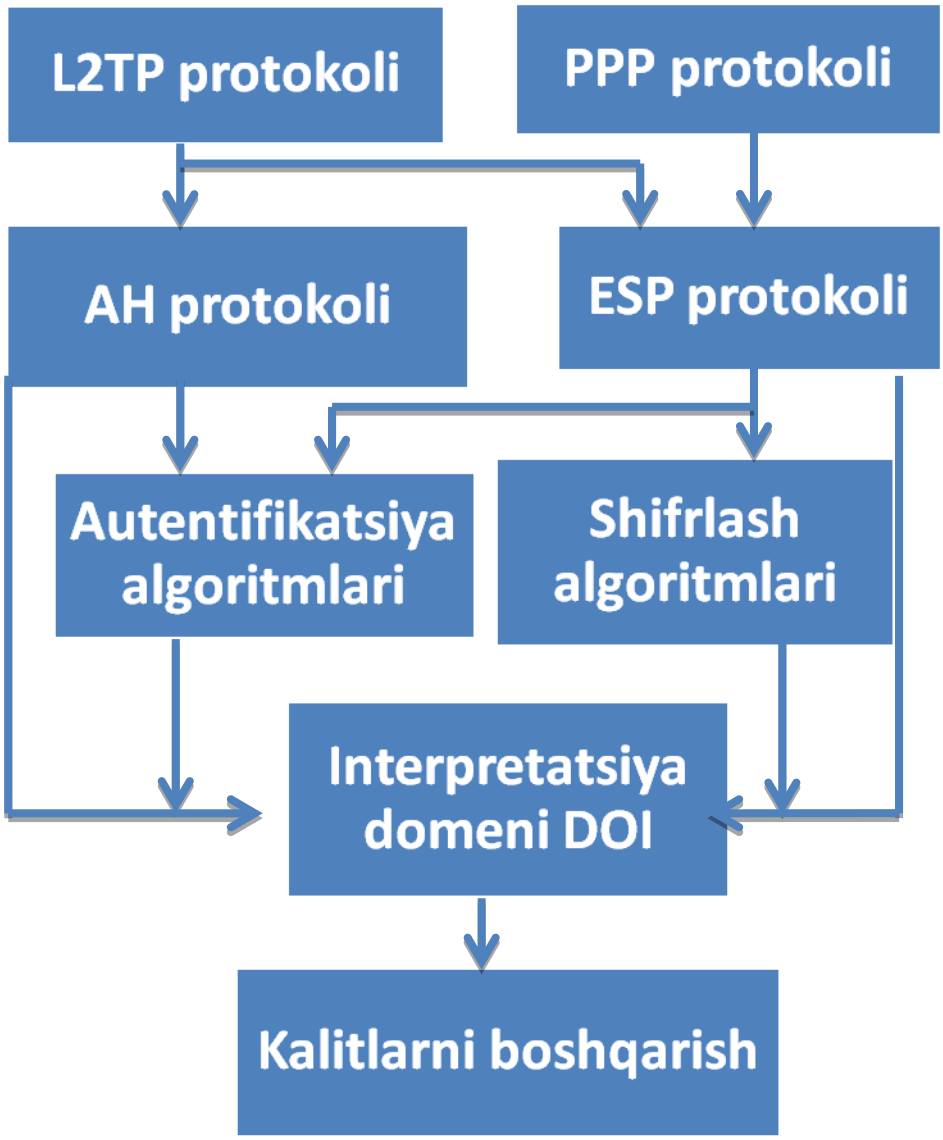
- L2F protokolida IP protokolining joriy versiyasi uchun information almashinuvning yakuniy nuqtalari orasida kripto – himoyalangan tunnel qurish ko'zda tutilmagan;
- himoyalangan virtual kanal faqatgina provayder serveri va mahalliy tarmoqning chetki marshrutizatori orasida qurilishi mumkin, bunda masofadagi foydalanuvchi kompyuteri va provayder server o'rtasidagi soha ochiq qoladi.

Shuning uchun L2F protokoli o'rnini Internet proyekti standarti hisoblanadigan L2TP protokoli butunlay egalladi.

L2TP (Layer-2 Tunneling Protocol) protokoli Microsoft va Cisco Systems kompaniyalari hamkorligida IETF organizatsiyasida ishlab chiqilgan. L2TP protokoli PPP – trafikni istalgan muhitli ommabop tarmoqlar orqali himoyalangan tunnellashtiruvchi protokoli sifatida ishlab chiqilgan. Bu protokol ustidagi ishlar PPTP va L2F protokollari asosida olib borilgan, va natijada u har ikkala protokolning afzal tomonlarini o'zida aks ettirdi.

PPTP protokolidan farqli, L2TP protokoli IP protokoliga bog'lanmagan, shuning uchun u paketlar kommutatsiyalanadigan tarmoqlarda ishlatilishi mumkin, masalan, ATM (Asynchronus Transfer Mode) yoki kadrlar retranslyatsiyalanadigan tarqmoqlarda (Frame Relay).Bundan tashqari, L2TP protokoliga muhim funksiyalardan hisoblangan ma'lumotlar oqimini boshqarish kiritilgan.

L2TP protokoliga PPTP protokoli spetsifikatsiyasida bo'lmagan bir qator himoya funksiyalari ham kiritilgan, xususan IPSec protokollar steki AH va ESP protokollari bilan ishlash yo'lga qo'yilgan. Quyida L2TP protokoli arxitekturasi keltirilgan.



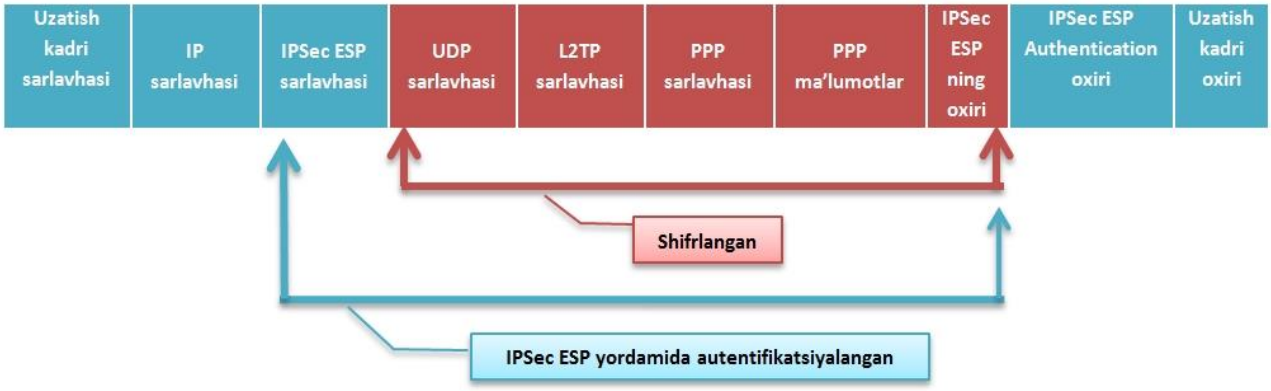
AH va ESP protokollari IPSec protokollar stekining asosiy komponentlari hisoblanadilar. Bu protokollar foydalanuvchilarga ularning tanlovlari bo'yicha turli xil shifrlash va autentifikatsiyaning kriptografik algoritmlarini qo'llashga imkon beradilar. Interpretatsiya domeni DOI (Domain of Interpretation) ga foydalaniladigan protokol va algoritmlar birgalikda ishlashining ta'minot funksiyalari joylashtirilgan. Himoyalangan kanallarni qurishda IPSec protokollar stekining qo'llanilishini keying bo'limlarda ko'rib o'tamiz.

Umuman olganda, gibrid protokol hisoblangan L2TP protokoli PPP protokolining masofadagi foydalanuvchilarni autentifikatsiyalash, himoyalangan virtual ulanish yasash va ma'lumotlar oqimini boshqasrish funksiyalari bilan kengaytirilgan ko'rinishi hisoblanadi.

L2TP protokoli transport sifatida UDP protokolini qo'llaydi va tunnelni boshqarish uchun ham, ma'lumotlar almashinuvi uchun ham bir xil formatdagi xabarlarni ishlatadi. Microsoft dasturiy ta'minotlarida L2TP protokoli

boshqaruvchi xabarlar sifatida shifrlangan PPP paketlarni o'zida saqlovchi UDP paketlarni ishlatadi. Yetkazib berishning ishonchliligi paketlar ketma – ketligi boshqaruvini kafolatlaydi.

L2TP protokoli ham PPTP protokoli singari paketni tunnel orqali jo'natish uchun PPP ma'lumotlar maydoniga dastlab PPP sarlavhasi, keyin esa L2TP sarlavhasini qo'shishdan boshlaydi.Shu yo'sinda yasalgan paket UDP protokoli yordamida inlapsulyatsiyalanadi. Uzatuvchi va qabul qiluvchi porti sifatida L2TP protokoli 1701 UDP – portni ishlaradi. L2TP tunneli orqali almashiniladigan paket strukturasini ko'rib chiqamiz.



TanlanganIPSecprotokollarstekixafvsizliksiyosatigabinoanL2TPUDP – xabarlarnishifrlashivaulargaESP (EncapsulationSecurityPayload) boshlanishvaoxiri, shuningdek, IPSecESPAuthenticationoxirisarlavhalariniqo'shishimumkin. So'ngraIPinkapsulyatsiyaamalgaoshiriladi.IPSecESPAuthenticationyordamidaIPinformatsionmayadoniautentifikatsiyasio'tkaziladi, ESPIPSecprotokoliesapaketshifriniochishdayordamberadi.KeyinkompyuterUDPsarlavhaniqaytaishlaydivaL2TPsarlavhasinitunnelniidentifikatsiyalashuchunishlatadi. EndiPPPpaketqaytaishlanadiganvako'rsatilganfoydalanuvchigajo'natiladiganfoydali ma'lumotlarnisaqlaydi.

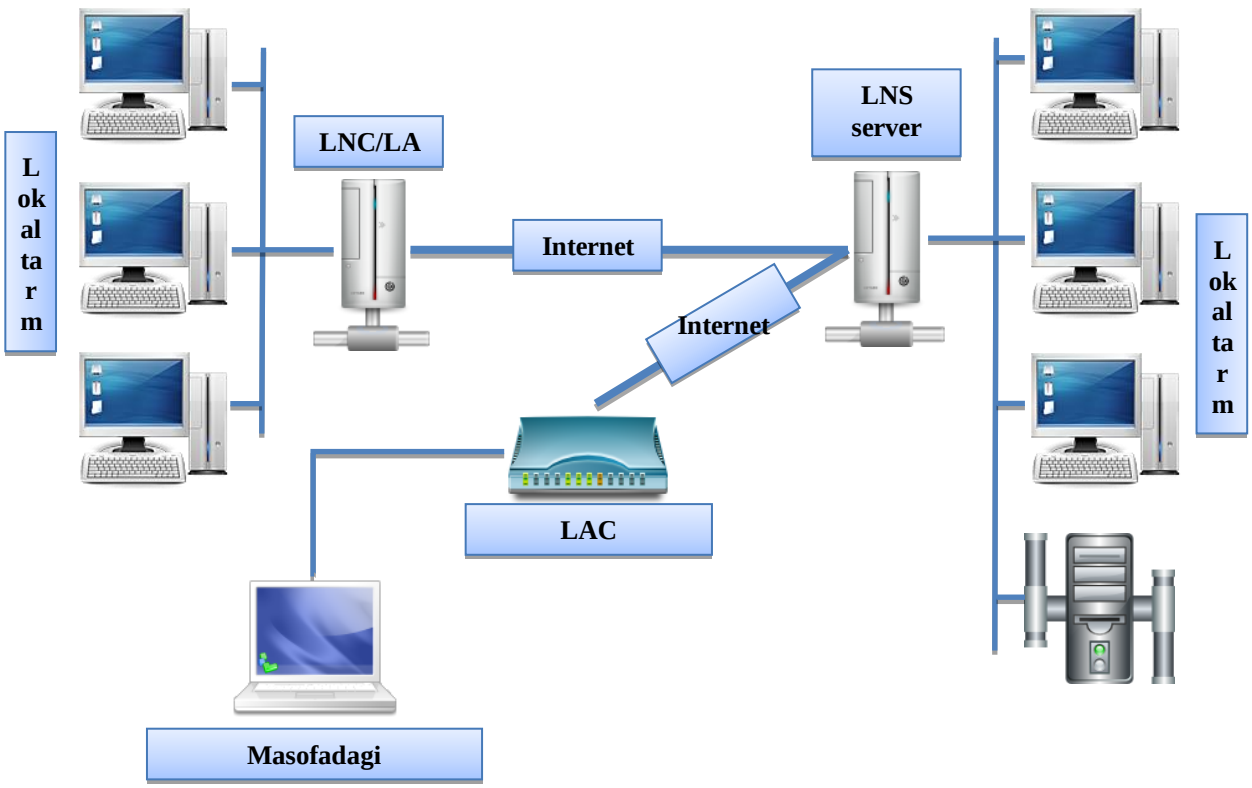
PPTPprotokoliyetarlihimoyadarajasinita'minlasada, baribirL2TPprotokoli (IPsecustidaqurilgan) ishonchliroq.IPSecustidaqurilganL2TPprotokoli "foydalanuvchi" va "kompyuter" darajalaridaautentifikatsiyanita'minlaydimshuningdekma'lumotlarautentifikatsiyasivashifrlashinibajaradi. Mijoz va VPN serverlar autentifikatsiyasining birinchi bosqichida L2TP protokoli sertifikatlash xizmatidan olingan lokal sertifikatlarni ishlatadi. Mijoz va server sertifikatlar bilan almashinishadi va himoyalangan ESP PA (Securoty Assocation) aloqa qurishadi.

L2TP (IPSec ustida qurilgan) kompyuter autentifikatsiyani yakunlagandan so'ng mijoz darajasidagi autentifikatsiya amalga oshiriladi. Bu autentifikatsiya uchun istalgan protokol, hattoki foydalanuvchi nomi va parolini ochiq tarzda uzatuvchi PAP, to'g'ri keladi. Bu hech qanday xafv – xatar tug'dirmaydi, chunki L2TP (IPSec ustida qurilgan) butun sessiyani shifrlaydi. Kompyuter va

foydalanuvchi autentifikatsiyasi uchun turli xil shifrlash kalitlarni qo'llaydigan MSCHAP yordamida foydalanuvchini autentifikatsiyalsh xafvsizlikni yanada mustahkamlashi mumkin.

L2TP protokoli masofadagi provayder serveri va korporativ tarmoq marshrutizatori orasida vujudga keladigan sxemadan foydalanishni mo'ljallaydi. O'zidan oldingi protokollar – PPTP va L2F dan farqli, - L2TP protokoli yakuniy abonentlar o'rtasida bir vaqtning o'zida har biri alhida dastur uchun ajratilishi mumkin bo'lgan bir nechta tunnellar ochish imkonini beradi. Bu xususiyatlar tunnellashtirish imkoniyatlarini kengaytiradi va xafvsizligini ta'minotini kuchaytiradi.

L2TP spetsifikatsiyasiga asosan masofadagi provayderning server vazifasini LAC (L2TP Access Concentrator) konsentratori bajarishi kerak. U L2TP protokolining mijoz qismini tashkillashtiradi va masofadagi foydalanuvchiga uning lokal tarmog'iga Internet orqali tarmoq darajasidagi ulanishni ta'minlaydi. Masofadagi lokal tarmoq serveri sifatida PPP protokoli bilan mos keladigan platformalarda ishlaydigan LNS (L2TP Network Server) tarmoq serveri ish yuritishi kerak.



Xuddi PPTP va L2F protokollaridegidek L2TP protokolida ham himoyalangan virtual kanal uch bosqichda tashkil etiladi:

- lokal tarmoqning masofadagi serveri bilan ulanishni o’rnatish;
- foydalanuvchi autentifikatsiyasi;
- himoyalangan tunnel konfiguryatsiyasi.

Birinchi bosqichda foydalanuvchi masofadagi lokal tarmoq serveri bilan ulanishni o’rnatish uchun ISP provayderi bilan PPP – ulanishni o’rnatadi. ISP provayderi serverida ishlaydigan LAC konsentratori bu ulanishni qabul qiladi va PPP lanalni o’rnatadi. So’ngra LAC konsentratori yakuniy uzel va foydalanuvchi qisman autentifikatsiyasini amalga oshiradi. Faqat foydalanuvchi nomini ishlatgan holda ISP provayderi foydalanuvchiga L2TP tunnellashtirish xizmati kerakliligini aniqlaydi.Agar bunday xizmat kerak bo’lsa, LAC konsentratorining keyingi qadami tarmoq LNS serveri manzilini aniqlash bo’ladi, keyinchalik shu manzil bilan tunnelli ulanish amalga oshiriladi. Foydalanuvchi tarmog’iga xizmat ko’rsatuvchi foydalanivchi va LNS server o’rtasidagi moslikni aniqlashni qulaylashtirish uchun ISP provayder qo’llab – quvvatlaydigan ma’lumotlar bazasi ishlatilishi mumkin.

LNS serverning IP – adresi aniqlangandan so’ng shu server bilan oldinroq yaratilgan tunnel bor yoki yo’qligi tekshiriladi.Agar bunday tunnel mavjud bo’lmasa, u o’rnatiladi. Provayder LAC konsentratori va lokal tarmoq LNS serveri o’rtasida L2TP protokoli bo’yicha sessiya o’rnatiladi.

LAC va LNS o’rtasida tunnel yaratishda yangi ulanishga shu tunnel sohasida identifikator beriladi, va u Call ID chaqirish identifikatori deb nomlanadi. LAC konsentratori tarmoq LNS serveriga Call ID ma’lumotlari bilan chaqirish xabarini uzatadi.LNS serveri bu chaqiruvni qabul qilishi yoki rad etishi mumkin.

Ikkinchi bosqichda L2TP sessitasi o’rnatilgandan so’ng tarmoq LNS serveri foydalanuvchi autentifikatsiyasini amalga oshiradi.Buning uchun autentifikatsiyalashning standart algoritmlaridan biri, xususan CHAP, ishlatilishi mumkin. Autentifikatsiya protokoli CHAP ishlatilgan holda xabar paketi chaqiruvchi – so’z, foydalanuvchi nomi va shifrlanmagan paroldan tashkil topgan bo’ladi. PAP protokoli uchun bu ma’lumot foydalanuvchi nomi va shifrlanmagan paroldan tashkil topgan bo’ladi. Tarmoq LNS serveri bu ma’limotni autentifikatsiyani amalga oshirish uchun avtomatik tarzda ishlatishi mumkin, bunda masofadagi foydalanuvchi bu ma’lumotlarni qayta kiritib o’tirmaydi va qo’shimcha autentufukatsiya sikli hosil qilinmaydi.

LNS server autentifikatsiya natijasini uzatgan vaqtda LAC konsentratoriga foydalanuvchi uzel IP – adresi haqida ma’lumotni ham uzatishi mumkin. Umuman

olganda, LAC konsentratori masofadagi foydalanuvchi uzeli va tarmoq LNS serveri orasidagi vositachi kabi ishlaydi.

Uchinchi bosqichda foydalanuvchining muvaffaqiyatli autentifikatsiyasida provayder LAC konsentratori va tarmoq LNS serveri orasida har ikki tomonlama himoyalangan tunnel yaratiladi. Masofadagi foydalanuvchidan PPP kadr kelgan vaqtda LAC konsentratori undan kadrni o'rovchi baytlarni, kontrol summa baytlarini olib tashlaydi, so'ngra L2TP protkoli yordamida uni tarmoq protokoliga inkapsulyatsiyalaydi va tunnel orqali LNS serveriga uzatadi. LNS serveri L2TP protokolini ishlatgan holda yetib kelgan paketdan PPP kadrni ajratib oladi va uni standart ko'rinishda qayta ishlaydi.

Tunnelning zaruriy parametrlar qiymati nastroykasi boshqaruvchi xabarlar yordamida amalga oshiriladi. L2TP protokoli paketlar kommunikatsiyali istalgan transport ustida ishlay oladi. Umumiy holda bu transport, masalan UDP protokoli, paketlarni kafolatlangan darajada yetkazib berilishini ta'minlamaydi.Shuning uchun L2TP protkoli bunday savollarni har bir masofadagi foydalanuvchi uchun tunnel ichidagi ulanish o'rnatmalari protseduralarini ishlatgan holda o'zi mustaqil yechadi.

Shuni ta'kidlab o'tish kerakki, L2TP protokoli kripto – himoyaning konkret bir usullarini aniqlamaydi va turli xil shifrlash standartlari ishlatilish imkoniyatini nazarda tutadi. Agar himoyalangan tunnel IP – tarmoqlarda yaratilishi kerak bo'lsa, kripto – himoyani tashkillashtirish uchun IPSec protokoli ishlatiladi. PPTP protokoliga qaraganda IPSec ustida qurilgan L2TP ma'lumotlar himoyasini kuchliroq darajada ta'minlaydi, chunki u 3-DES (Triple Dara Encryption Standart) va AES shiflrash algoritmlaridan foydalanadi. Bundan tashqari, HMAC (Hash Message Authentication Code) algoritmi yordamida L2TP protokoli ma'lumotlar autentifikatsiyasini ta'minlaydi.Ma'lumotlar autentifikatsiyasi uchun bu algoritm 128 razryad uzunlikdagi xesh yasaydi.

Shu tarzda, PPTP va L2TP protokollarining funksional imkonayatlari turlicha. PPTP protokoli faqat IP – tarmoqlarda qo'llanilishi mumkin, va tunnel yaratish va foydalanishda unga alohida TCP ulanish zarur. L2TP protkoli faqat IP – tarmoqlardan tashqari, boshqa turli tarmoqlarda ham ishlay oladi, tunnel yaratish uchun xizmatchi xabarlar va u orqali ma'lumot almashinishda bir xil formatdan va protokollardan foydalaniladi, va ma'lumotlarni tashkillashtirishda muhim bo'lgan qariyb 100 foizli xafvsizlikni kafotlashi mumkin.

L2TP protokolining ijobiy sifatlari uni himoyalangan virtual tarmoqlar yarstishda eng qulay protokollar safiga kiritadi. Shunga qaramasdan, L2TP protokoli kanal darajasidagi tunnel orqali ma'lumot almashinuvida bir qator kamchiliklarni yengib o'ta olmaydi:

- L2TP protokolini tashkil etish uchun ISP provayderlar qo’llab – quvvatlanishi zarur;
- L2TP protokoli trafikni tanlangan tunnel miqyosida chegaralaydi va foydalanuvchilarni Internetning boshqa qismlariga chiqishlaridan mahrum qiladi;
- taklif etilgan L2TP spetsifikatsiyasi faqat IP – tarmoqlarda IPSec protokoli yordamida standart shifrlashni ta’minlaydi.

Tarmoq darajasidagi xavfsizlik – IPSec protokoli

Kompyuter tarmoqlari kamchiliklarini radikal bartaraf etish uchun ma’lum bir alohida dasturlar sinfi himoya tizimini emas, balki, butun tizim himoyasini tashkil qilish kerak. Xususan IP – tarmoqlar uchun bu shuni anglatadiki, himoya tizimlari OSI modelining tarmoq darajasida amal qilishlari kerak. Bunday tanlovning ustunligi shundan iboratki, IP – tarmoqlarda aynan tarmoq darajasi o’zining yuqori gomogenligi bilan farq qiladi: yuqori darajadagi protokollar, ma’lumot almashinshning fizik muhiti va kanal darajasi texnoligiyasidan qat’iy nazar ma’lumotlar transportirovkasini IP protokolisiz amalga oshirib bo’lmaydi. Shuning uchun uchinchi darajada tarmoq himoyasini tashkil etish boshqa darajalarda ham hech qanday o’zgartirishlar kiritilmay turib, kamida xuddi shunday himoyani ta’minlaydi.

OSI modelining tarmoq darajasida himoyalangan virtual kanallarni tashkil etsihda himiya shaffofligi va sifati o’rtasidagi optimal mutanosiblikka erishiladi. Tarmoq darajasida himoya vositalarini qo’llash ularni dasturlar uchun shaffoflashtiradi, chunki tarmoq darajasi va dastur o’rtasida transport darajasi protokoli joylashgan. Foydalanuvchi uchun himoya protseduralari qariyb sezilirmas bo’ladi, xuddi IP protokolining o’zidek. Tarmoq darajasida trafik himoyasi va kalitlarni boshqarishning yetarli to’liq darajada tashkil etish imkoniyati mavjud, chunki aynan tarmoq darajasida xabarlar paketi marshrutizatsiyasi amalga oshiriladi.

IPSec (Internet Protokol Security) protokollar steki ma’lumot almashinuv ishtirokchilari autentifikatsiyasi, trafikni tunnellashtirish va IP – paketlarni shifrlash uchun ishlatiladi. IPSec protokolining asosiy vazifasi – IP tarmoq bo’yicha ma’lumotlarni xavfsiz yetkazishni ta’minlash.IPSec protokoli trafik himoyasini joriy IPv4 protokolida, shuningdek hozirgi kunda Internet texnologiyasida keng tarqalayotgan IPv6 protokoli versiyasida ham ta’minlay oladi.

IPSec himoya vositalari arxitekturasi

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 uzatilishida 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.

Shuni ta'kidlab o'tish kerakki, ma'lumotlar xavfsizligi tushunchasi yana bir talabni o'z ichiga oladi - bu ma'lumotlar mavjudligi (доступность). Bu ma'lumotlar uzatilishi va yetib kelishnini kafolatlaydi. IPSec protokllari bu vazifa bilan shug'ullanmaydi, va uni transport darajasi TCP protokoliga qoldiradi. Shuning uchun odatda TCP va IP protokollari birgalikda TCP/IP protokollari deb yuritiladi.

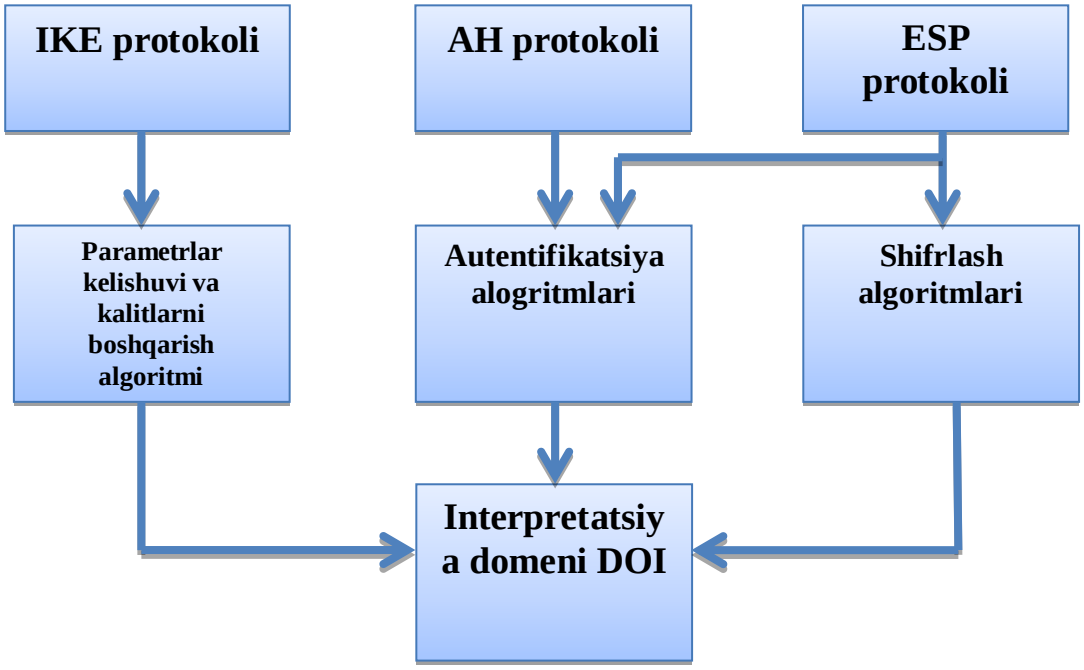
IP – tarmoqlarda kommunikatsiyaning asosiy birligi IP – paket hisoblanadi.

IP sarlavha		**TCP yoki UDP transport sarlavha**	**Ma'lumotlar**
S - manzil	**D - manzil**		

IP – paket S – manzil (Source address) – uzatuvchi adresi, D – manzil (Destination address) – qabul qiluvchi adresi, transport sarlavhasi, ma'lumot tipi haqidagi axborot va ma'lumotning o'zidan tashkil topadi.

IPSec protokoli asosan quyidagi komponentlardan 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).



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’tnatilgan tomondan uzatilgan;
- paket ma’lumotlari tarmoq orqali uzatish vaqtida hech qanday buzilishlarga uchramagan;
- paket oldinroq qabul qilingan biror – bir paketning dublikati emas.

AH protokoli uzatiladigan ma’lumotlarning konfidensialligini ta’minlamaydi, u shifrlash uchun mo’ljallanmagan. Ma’lumotlar oraliq uzellar tomonidan o’qilishi mumkin, lekin ularni o’zgartirib bo’lmaydi. Ma’lumotlarning butunligi va autentligiga IP – sarvalha oldidan va transport darajasi (TCP/UDP) sarlavhasi oldidan autentifikatsiyalaydigan sarlavha qo’shish orqali erishiladi.

0 **16** **31**

Keyingi sarlavha	**Uzunlik**	**Ajratib qo’yilgan**
Himoya paremetlari indeksi SPI		
Tartib raqam SN		
Autentifikatsiyalanadigan ma’lumotlar (o’zgaruvchi uzunlik)		

Inkapsulyatsiyalovchi himoya ESP protokoli

ESP protokoli ma’lumotlar paketlarining konfidensialligi, autentligi, butunligi va takrorlardan himoyalanganligini ta’minlaydi. Shuni ta’kidlab o’tish kerakki, ma’lumotlar konfidensialligini ESP protokoli har doim ta’minlaydi, lekin ma’lumotlar butunligi va autentligi u uchun umumiy talab bo’lib hisoblanadi. Ma’lumotlar konfidensialligi alohida paketlarni shifrlash yo’li bilan ta’minlanadi. Butunlik va autentifikatsiya esa dayjestning hisoblanishi asosida ta’minlanadi.

ESP protokolida autentifikatsiya va konfidensiallik funksiyalari birgalikda yoki alohida ishlatilishlari mumkin. Konfidensiallik funksiyalari ishlatilmaganda tarmoq manzillarini translyatsiyalovchi NAT mexanizmini qo’llash mumkin.Chunki bu vaqtda IP – paketlar sarlavhasidagi manzillarni o’zgartirish imkoni vujudga keladi.

0 **16** **31**

<table>
<tr><td colspan="3">Himoya paremetlari indeksi SPI</td></tr>
<tr><td colspan="3">Tartib raqam SN</td></tr>
<tr><td colspan="3">Ma’lumotlar (o’zgaruvchi uzunlik)</td></tr>
<tr><td></td><td colspan="2">Pad to’ldiruvchi</td></tr>
<tr><td>Pad to’ldiruvchi</td><td>To’ldiruvchi uzunligi</td><td>Keying sarlavha</td></tr>
<tr><td colspan="3">Autentifikatsiyalanadigan ma’lumotlar (o’zgaruvchi uzunlik)</td></tr>
</table>

ESP protokoli AH protkoli bilan birgalikda yoki alohida qo’llanilishi mumkin. ESP va AH protokollari birgalikda qo’llangan holda ular turli xil usullar bilan kombinatsiyalashishlari mumkin. Agar transport darajasi ishlatilayotgan bo’lsa, ESP protokoli sohasida shifrlash ketidan autentifikatsiya amalga oshiriladi, AH protokoli esa ESP protokolidan so’ng qo’llanilishi kerak. Tunnel darajasida AH va ESP protokollari turli xil qism paketlarga qo’llaniladi va, bundan tashqari, turli xil boshlang’ich va/yoki yakuniy nuqtali ko’p marta ichma – ich tunnellashtirishga ruxsat beriladi.

IPSec protokoli autentifikatsiya va shifrlash algoritmlari

IPSec (ESP) protokolida ma’lumotlarni shifrlash uchun maxfiy kalitlarni ishlatadigan istalgan simmetrik shifrlash algoritmi qo’llanilishi mumkin.

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 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 hisoblanishadi.

ESP protokoli uchun bir nechta shifrlash algoritmlari qabul qilingan. Odatda ESP uchun shifrlash algoritmi sifatida DES (Data Encryption Standart), 3-DES (uch karrali DES) va yangi shifrlash standarti AES (Advanced Encryption Standart) ishlatiladi.

Kripto-kalitlarni boshqarish protokoli IKE

ESP va AH protokollari aloqa konfidensialligi, tomonlar autentifikatsiyasi va ma’lumotlar butunligi kabi eng asosiy himoya atributlarini tashkil etishni ta’minlaydilar. Ammo barcha bu funsiyalar kalitlarni taqsimlovchi va ma’lumot almashinuv ishtirolchilari o’rtasida protokollar mosligini ta’minlovchi kuchli yordamchi infrastrukturasiz o’zining har qanday ma’nosini yo’qotadi.

IPSec protokolida bunday infrastruktura rolini IKE (Internet KeyExchange) protokollar guruhi o’ynaydi.Bu nom 1988-yilda eskicha ISAKMP/Oakley o’rniga keldi.

RFC 2408 hujjatida keltirilgan ISAKMP (Internet Security Association and Key Management Protocol) protokoli Diffi – Hellman kalitlar almashinuvi protsedurasi, shuningdek, autentifikatsiya protseslari uchun algoritm va matematik strukturalarni birgalikda ishlashini ta’minlaydi. RFC 2412 da keltirilgan Oakley protokoli Difii – Hellman algoritmiga asoslangan va kalitlarning bevosita almashinuvini tashkil qilish uchun xizmat qiladi.

IKE protokollari uchta masalani yechishadi:

- tomonlar autentifikatsiyasini amalga oshirishadi, himoyalangan ma’lumot almashinuv seansida ishlatiladigan shifrlash algoritmlari va kalitlar xarakteristikalari mosligini aniqlashadi;
- ulanishning kalit ma’lumotini yaratishni va ularni boshqarishni ta’minlashadi, kalitlarning bevosita almashinuvi (shuningdek, ularning tez-tez yangilanishini);
- ulanish parametrlari va ba’zi bir hujun turlaridan himoyani boshqarishadi, barcha qabul qilingan kelishuvlar amalga oshishini boshqarishadi.

IPSec protokolini ishlab chiqargan guruh o’zining faoliyatini oxirgi sanab o’tilgan masalalarni yechishdan boshladi.Natijada himoyalangan virtual ulanishlar konsepsiyasi vujudga keldi, yoki xavfsiz assotsiatsiyalar SA (Security Associations) konsepsiyasi.

IPsec xavfsizlik vositalari afzalliklari

IPSec tizimi standartlari tarmoq xavfsizligi sohasida progressiv metodika va yutuqlarga erishdi, mutaxassislar o’rtasida IP – tarmoqlar uchun ishonchli va oson moslashadigan himoya tizimi sifatida mashhur bo’ldi.

IPSec tizimi VPN qurish standartlari orasida yetakchi o’rinlarni mustahlam egallagan.Bunga uning ochiq arxitekturasi, kriptografiya sohasidagi barcha yangiliklarni qo’llay olishi kabi omillar sababchi.IPSec tarmoqni ko’plab hujunlardan himoyalash imkonini beradi.Himoyalangan kompyuter yoki tarmoqqa faqatgina ro’yxatdan o’tgan tomonlardan paketlar kirishi mumkin.

IPSec quyidagi himoya funksiyalarini ta’minlaydi:

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

Seans darajasida xavfsizlik – SSL, TLS, SOCKS protokollari

Himoyalangan virtual kanallarni tashkil etish mumkin bo'lgan OSI modelining eng yuqori darajasi – bu seans darajasi bo'lib hisoblanadi. Himoyalangan virtual tarmoqlarni seans darajasida yaratishda ma'lumot almashinuvini kriptografik himoyalash, shuningdek, autentifikatsiya va bir qator boshqa funksiyalarni amalga oshirish imkoniyati vujudga keladi.

Haqiqatdan ham, OSI modelining seans darajasi mantiqiy ulanishlarni o'rnatish va ularni boshqarish funksiyalariga javob beradi. shuning uchun bu darajada vositachi – dasturlarni qo'llash imkoniyati mavjud.

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 b. protokollar) uchun shaffof. 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. Seans darajasidagi oraliq funksiyalarni amalga oshirish uchun standart tariqasida IETF (Internet Engineering Task Force) tashkiloti tomonidan SOCKS protokolini ishlatish qabul qilingan.

SSL va TLS protokollari

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. Hozirgi vaqtda SSL protokoli OSI modelining seans darajasidagi himoyalangan kanal protokoli sifatida qo’llaniladi.

SSL protokoli ma’lumot almashinuvining himoyasini ta’minlash uchun ma’lumot himoyasining kriptografik usullarini ishlatadi. Bu protokol tarmoqning har ikkala abonentlari orasida himoyalangan kanal yaratishning barcha funksiyalarini bajaradi, ularning autentifikatsiyasini, konfidensialligini, uzatiladigan ma’lumotlar butunligi va autentligini ta’minlaydi. SSL protokolining yadrosini assimmetrik va simmetrik kriptosistema texnologiyalarining kompleks ishlatilishi tashkil qiladi.

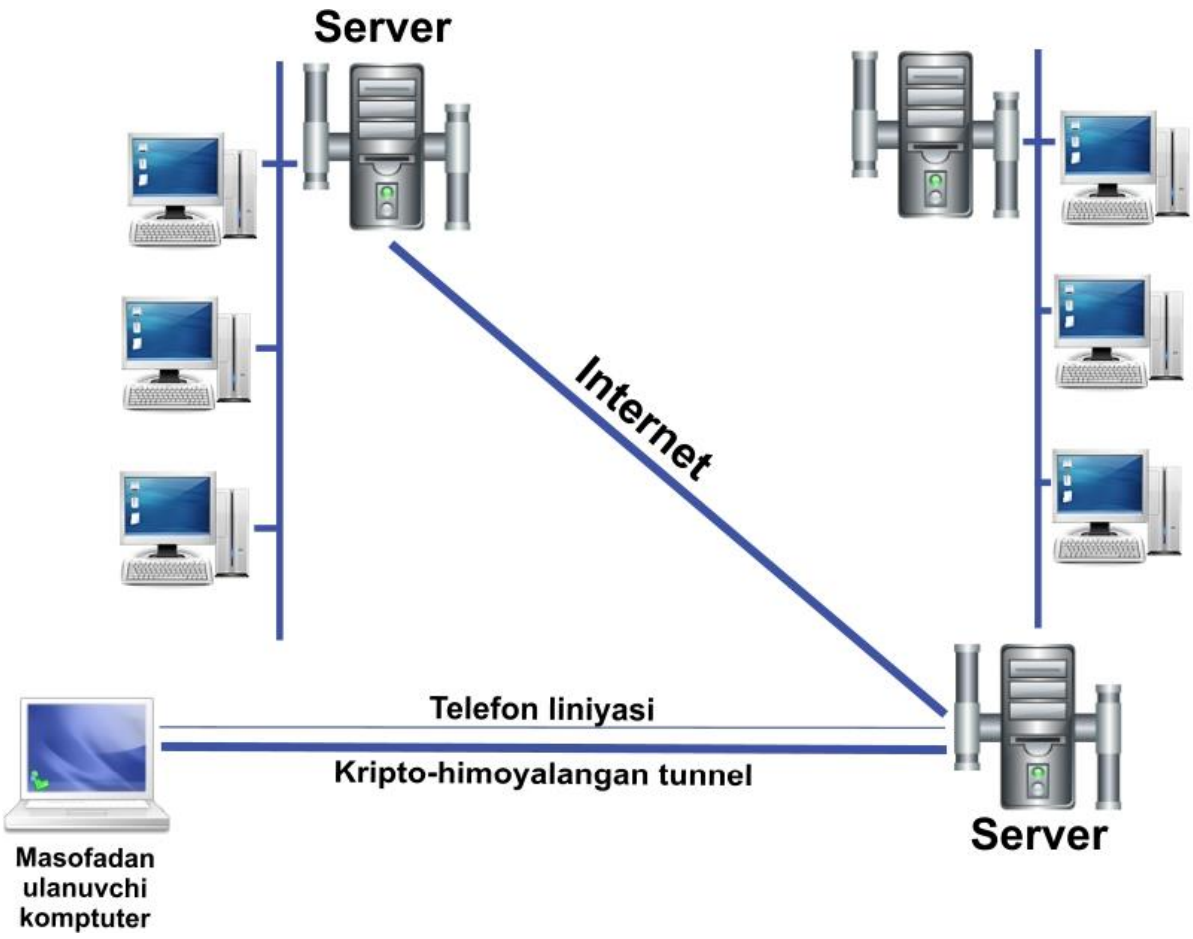
SSL protokolida ikkala tomon autentifikatsiyasi foydalanuvchilarning (mijoz va server) maxsus sertifikatlash markazlari tomonidan raqamli imzolar bilan tasdiqlangan ochiq kalitlar sertifikatlari almashinuvi yo’li bilan bajariladi. SSL protokoli X.509 standartiga mos keluvchi sertifikatlarni, shuningdek ochiq kalitlar infrastrukturasi standarti PKI (Public Key Infrastructure) ni qo’llab – quvvatlaydi. Bu standartlar yordamida sertifikatlarning yetkazilishi va haqiqiyligini tekshirish amalga oshiriladi.

Konfidensiallik uzatiladigan xabarlarni tomonlar ulanishi o’rnatilganda o’zaro almashiniladigan simmetrik session kalitlarni shifrlash orqali ta’minlanadi.Session kalitlar shifrlangan ko’rinishda ham uzatiladi, bunday holda ular abonentlarning sertifikatlaridan olingan ochiq kalitlar yordamida shifrlanadi. Simmetrik kalitlarning assimmetrik kalitlardan afzalligi shundaki, ularning shifrlanish tezliklari assimmetrik kalitlarning shifrlanish tezligidan ancha katta va shuning uchun ular xabarlarning himoyasi uchun ishlatiladi.

Almashiniladigan ma’lumotlarning aslligi va butunligi elektron raqamli imzolarni tashkil etish va ularni tekshirish hisobiga ta’minladani. Raqamli imzolar va shifrlash kaliti almashinuvi uchun ochiq kalitli algoritm ishlatiladi.

Assimmetrik shifrlash algoritmi sifatida RSA, shuningdek Diffi – Hellman algoritmi ishlatiladi. Simmetrik shifrlashda esa RC2, RC4, DES, 3-DES va AES algoritmlarini ishlatish imkoniyati mavjud. Hesh – funksiyalarni hisoblashda esa MD5 va SHA-1 standartlarini qo’llash mumkin. SSL protokolining 3.0 versiyasida kriptografik algoritmlar to’plamiga qo’shimcha va yangi algoritmlar kiritish mumkin.

SSL protokoliga asosan kripto-himoyalangan tunnellar virtual tarmoqning yakuniy nuqtalari orasida yasaladi.Ulanishnig bir tomonida server, ikkinchi tomonida mijoz faoliyat ko’rsatadi.



SSL-sessiyasi o’rnatilganda quyidagi masalalar yechiladi:

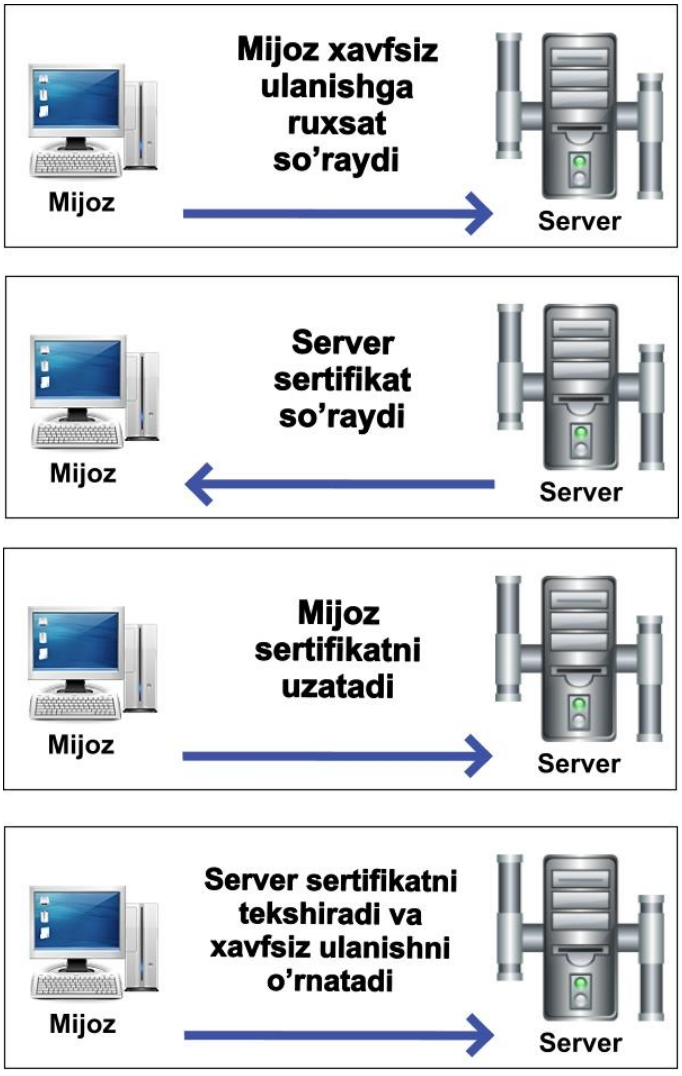
- tomonlar autentifikatsiyasi;
- tomonlarning himoyalangan ma’lumot almashinuvida ishlatiladigan kriptografik algoritmlar va siqish algoritmlari mosligi va kelishuvi;
- umumiy maxfiy maxsus-kalitni kalitni tashkillashtirish;
- umumiy maxfiy maxsus-kalit asosida ma’lumot almashinuvining kripto-himoyasi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

SSL protokolida autentifikatsiyaning ikki xil usuli mavjud:

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

Serverning SSL - autentifikatsiyasi mijozga serverning haqiqiyligini tekshirish imkonini beradi. SSL protokolini qo'llab – quvvatlovchi mijoz dasturiy ta'minoti standart kriptografik usullar yordamida ochiq kalit bilan serverning sertifikati va ochiq kaliti haqiqatdan ham shu mijozning ishonchli sertifikatlar ro'yxatida mavjud bo'lgan manbadan kelganligini tekshiradi. Bunday tekshirish juda muhim bo'lishi mumkin, masalan, agar foydalanuvchi kredit kartasi raqamini tarmoq orqali uzatmoqchi va qabul qiluvchi serverning haqiqiyligini tekshirmoqchi bo'lsa.

Mijozning SSL – autentifikatsiyasi serverga mijozning haqiqiyligini tekshirishga imkon beradi. Xuddi server autentifikatsiyasidagidek kabi, bu holda ham server mijoz sertifikati haqiqiyligini tekshiradi.Masalan, bank konfidensial ma'lumotlarni mijozga uzatayotgan vaqtda.



1999 – yilda SSL protokoliga asoslangan TLS (Transport Layer Security) protokoli vujudga keldi va u hozirda Internet standarti hisoblanadi. SSL 3.0 va TLS 1.0 protokollari o'rtasidagi farq unchalik ham katta emas.

SOCKS protokoli

SOCKS (SOCKet Secure) protokoli server – vositachi yoki proksi – server orqali OSI modelining seans darajasida mijoz/server dasturlarning o'zaro munosabatini tashkillashtiradi.

Dastlab SOCKS protokoli faqatgina mijoz dasturlari tomonidan keladigan so'rovlarni serverlarga qayta yo'llash, shuningdek olingan javoblarni qayta mijozga uzatish uchun ishlab chiqilgan. Mijoz/server dasturlari o'rtasida so'rov va javoblarni qayta yo'llash NAT (Network Address Translation) IP – adreslarini translyatsiyalash funksiyalarini qo'llash imkonini yaratadi. NAT texnologiyasini qo'llash ichqi tarmoq topologiyasi yashirishga yordam beradi, bu esa o'z navbatida tashqaridan uyushtiriladigan hujumlarni amalga oshirishni qiyinlashtiradi.Tarmoq manzillarini translyatsiyalash himoyani kuchaytirishdan tashqari, o'zining shaxsiy adresatsiyasini amalga oshira olish imkoniyati tufayli ichki adres sohasini kengaytirishga imkon beradi.

SOCKS v.5 protokoli IETF (Internet Enfineering Task Force) tashkiloti tomonidan Internet standarti sifatida tasdiqlangan bo'lib, RFC 1928 (Request for Comments) ga kiritilgan.

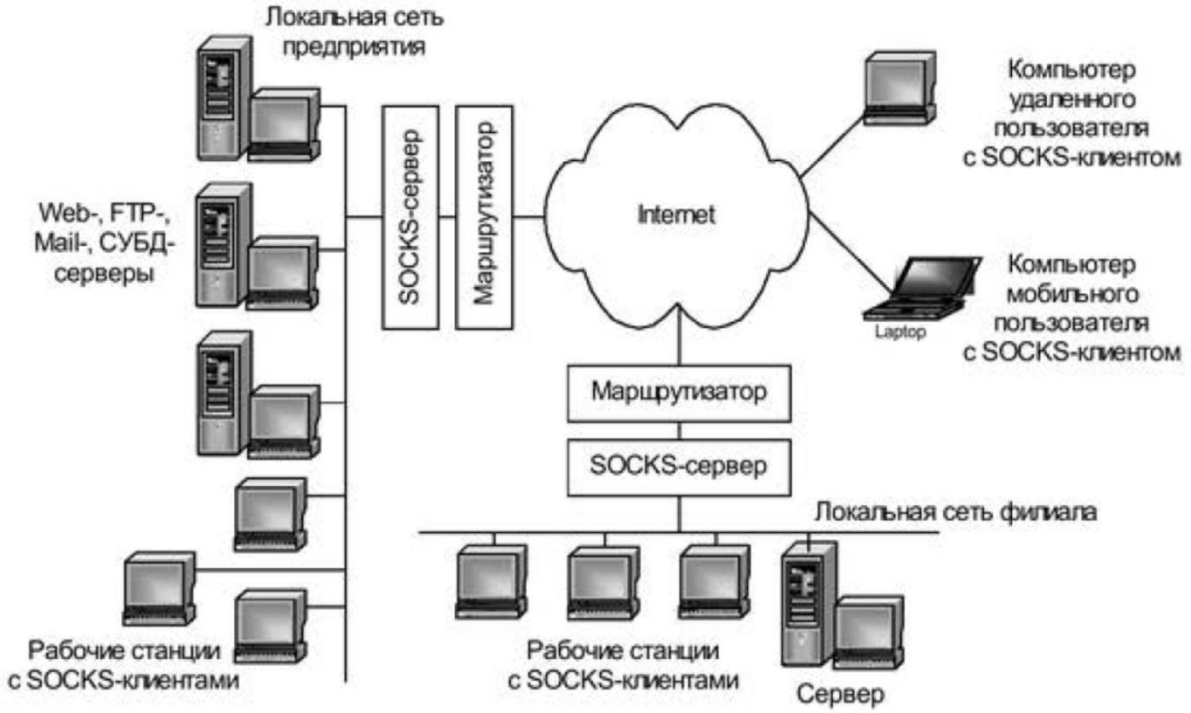
SOCKS v.5 protokoli asosida quriladigan ulanishning umumiy sxemasini quyidagicha tasvirlash mumkin:

- tarmoqdagi biror – bir amaliy server bilan ulanish o'rnatmoqchi bo'lgan mijoz so'rovi shu kompyuterda o'rnatilgan SOCKS – mijozga murojaat qiladi;
- SOCKS – server bilan ulangan SOCKS – mijoz o'zi qo'llab – quvvatlaydigan barcha autentifikatsiya usullarining identifikatorlarini uzatadi;
- SOCKS – server autentifikatsiyaning qaysi usulidan foydalanishni hal qiladi (agar SOCKS – server SOCKS – mijoz tomonidan taklif etilgan autentifikatsiya turlaridan birortasini ham qo'llab – quvvatlamasa, ulanish uziladi);
- tanlangan usul yordamida server mijozni autentifikatsiyalaydi; muvaffaqiyatsiz autentifikatsiyada SOCKS – server ulanishni uzadi;
- muvaffaqiyatli autentifikatsiyadan so'ng SOCKS – mijoz SOCKS – serverga tarmoqdagi so'ralayotgan amaliy serverning DNS – nomi yoki IP – adresini uzatadi, va keyin SOCKS – server oldindan aniqlangan qoidalar asosida ushbu amaliy server bilan ulanishni o'rnatish haqida qaror qabul qiladi;

- ulanish o’rnatilgan holda, mijoz va amaliy server bir – birlari bilan ulanishlar zanjiri orqali aloqa qilishadi, bu zanjirda SOCKS – server ma’lumotlarni qayta translyatsiyalaydi, shuningdek tarmoq orqali o’zaro aloqa himoyasida vositachi funksiyasini ham bajarishi mumkin: masalan, agar autentifikatsiya vaqtida SOCKS – server va SOCKS – mijoz o’zaro seans kalitlari bilan almashinishgan bo’lsa, ular o’rtasidagi butun trafik shifrlanadi.

Bundan tashqari SOCKS – server quyidagi qo’shimcha funksiyalarni ham bajarishi mumkin:

- ichki tarmoq resurslariga ruxsatni chegaralash;
- tashqi tarmoq resurslariga ruxsatni chegaralash;
- xabarlar oqimi filtratsiyasi, masalan viruslarni dinamik axtarish;
- hodisalar registratsiyasi va belgilangan hodisalarga ta’sir;
- tashqi tarmoqdan so’raladigan ma’lumotlarni keshlash.



Simsiz tarmoqlar xavfsizligi

Simsiz tarmoqlar butun dunyo bo'ylab kundan kunga keng tarqalmoqda. Bunga sabab bu texnologiyaning qulayligi, keng ko'lamligi va nisbatan arzonligidadir. Simsiz tarmoqlar tezlik, tarqalish radiusi, aloqa sifati va himoyalanganlik kabi parametrlar bilan xarakteristikalanadi.

Ma'lumki, simsiz tarmoqlar xafvsizligini ta'minlash ancha qiyin.Agar simli tarmoqlarda hujumlar uyushtirish uchun avval shu tarmoq kabel sistemasi yoki ma'lum bir qurilmalariga fizik ruxsatga ega bo'lish kerak bo'lsa, simsiz tarmoqlarda bunga hech qanday hojat yo'q.chunki simsiz tarmoqlarning tarqalish muhiti bu havo. Istalgan shaxs shu tarmoq tarqalish radiusida turib ushbu tarmoqqa hujum uyushtirishi mumkin.

LAN (Lokal Area Network) va MAN (Metropolitan Area Network) tarmoqlari standartlar oilasi IEEE 802 tarkibiga kiruvchi IEEE 802.11 standarti simsiz tarmoqlar standarti hisoblanadi. Bu standart hali to'liqligicha yakunlanmagan bo'lib, uning istida izchil izlanishlar olib borilmoqda va yangi yutuqlarga erishilmoqda.

- 802.11 – dastlabki 1 Mbit/s va 2 Mbit/s, 2.4 GHz (1997-yil);
- 802.11a – 54 Mbit/s, 5 GHz (1999-yil);
- 802.11b – yangilangan standart, 5.5 va 11 Mbit/s (1999-yil);
- 802.11g – 54 Mbit/s, 2.4 GHz (b versiya bilan moslik) (2003);
- 802.11n – yangi standart, 600 Mbit/s, 2.4-2.5 yoki 5 GHz; 802.11a/b/g lar bilan moslik (2009);
- 802.11ac – yangi ishlab chiqarilayotgan IEEE standarti. Tezlik 1.3 Gbit/s gacha, energiya iste'moli 802.11n ga qaraganda olti barobar kam. 802.11 a/b/g/n lar bilan moslik. 2013-yil 1-fevral holatida 95% ga tayyor. Yangi standartda ishlovchi qurilmalar ishlab chiqilgan.
- 802.11ad – qo'shimcha diapazonli yangi standart, 60 GHz, 7 Gbit/s.
- 802.11as (taxminan) – yangi turdagi antennalardan foydalanishi nazarda tutuilgan yangi standart, 135 GHz, 20 Gbit/s.

Simsiz tarmoqlari xavfsizligini ta'minlash uchun dastlab ishlab chiqilgan WEP (Wired Equivalent Privacy) standarti bir qator kamchiliklarga ega edi.Shuning uchun uning o'rnini WPA (Wi-Fi Protected Access) standarti egalladi. Simsiz tarmoq xavfsizligini ta'minlash uchun quyidagi talablar ham bajarilishi kerak:

Fizik himoya. Wi-Fi tarmog'ini qurishda ulanish nuqtalarini tashqi fizik ta'sirdan himoyalash.

To'gri sozlash. Tavsiya etilgan shifrlash va autentufikatsiya standartlaridan foydalanish.

Qo'shimcha himoya vositalari. Faqatgina standart himoya vositalariga tayanmasdan, keng ko'lamdagi xavfsizlik dastur va vositalaridan foydalanish. Masalan trafik analizatorlar, tarmoqlararo ekran, monitoring va h.

VPN-agentlar. Ko'plab ulanish nuqtalari ochiq tarzda ishlaydilar.Shuning uchun ma'lumot almashinuvi xavfsizligini ta'minlash uchun VPN kanallarni tashkil etsih.

Wi-Fi tarmog’i xavfsizligini tekshirish

Buning uchun kerak bo’ladigan vositalar:

1) Wi-Fi ulanish nuqtasi; bizning misolda bu TP-LINK D7D91D Wi-Fi ulanish nuqtsiga ega modem-router,

2) mijoz – Wi-Fi standartida ishlay oladigan istalgan qurilma, kompyuter yoki mobil telefon;

3) hujum uyushtiriladigan kompyuter – Wi-Fi tarmoq platasi va CD/DVD-ROM ga ega bo’lishi kerak;

4) AirSlax 3.2 operatsion tizimi (CD yoki DVD distributivda); distributiv va u haqidagi qo’shimcha ma’lumotni http://airslax.ru/ saytidan olish mumkin.

WPA standarti yordamida himoyalangan Wi-Fi tarmog’i paroloni topish

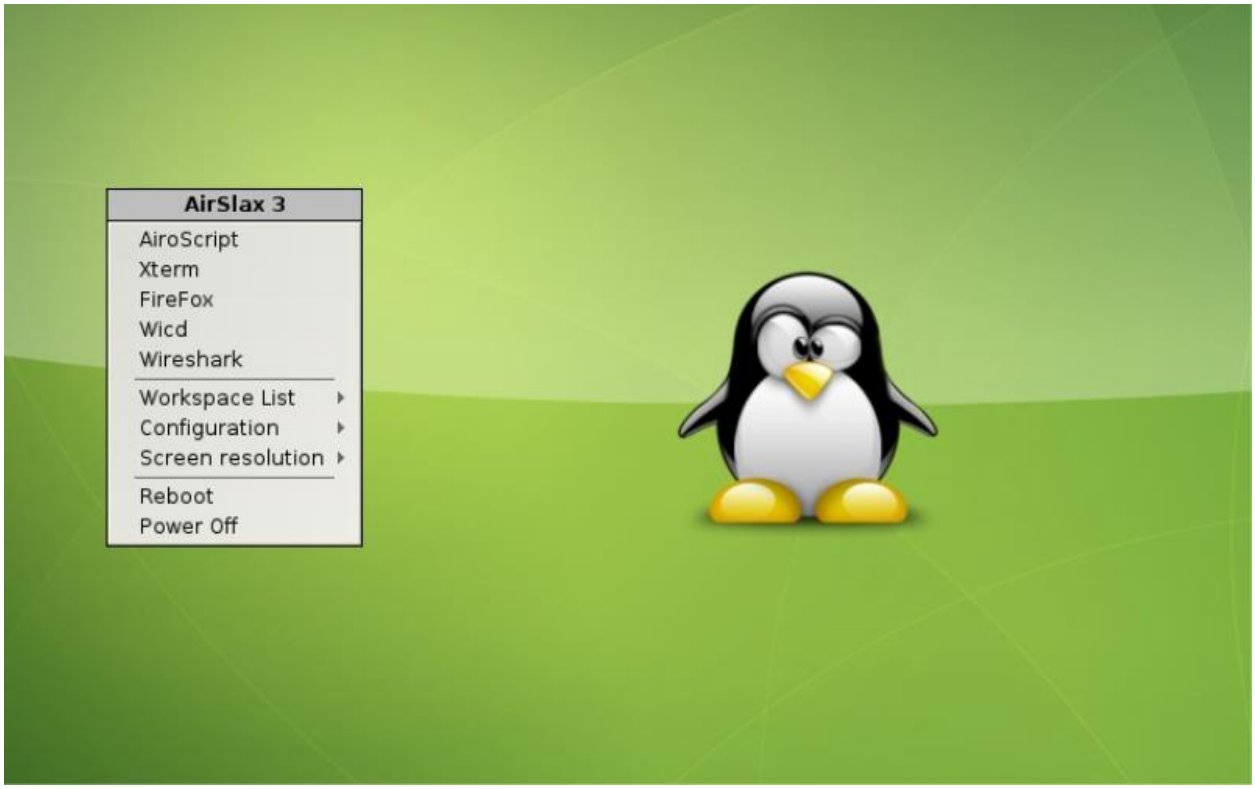
1. Kompyuterning CD/DVD-ROM qurilmasiga AirSlax distributivini qo’yamiz va BIOS da dastlab CD/DVD-ROM dan yuklanish kerakliligini ko’rsatamiz. Bizda AirSlax operatsion tizimining quyidagi menyusi chiqadi:

2. Run Slax komandasini tanlaymiz va yuklanish boshlanadi:

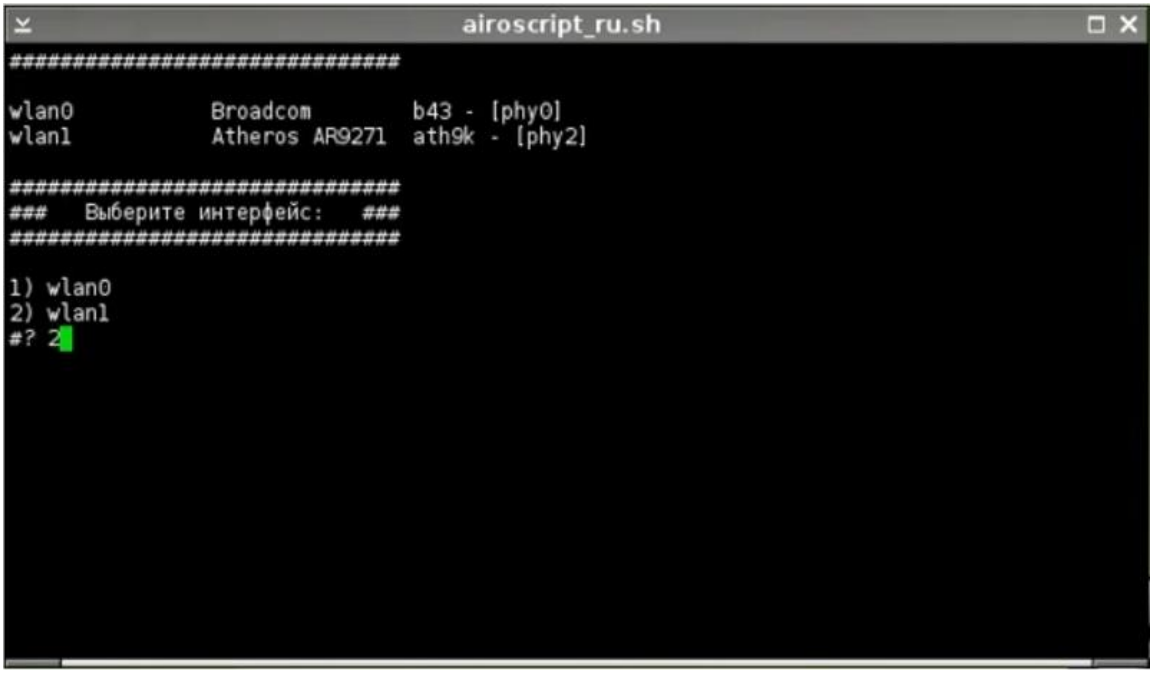
```
vmlinuz
PID hash table entries: 2048 (order: 1, 8192 bytes)
Dentry cache hash table entries: 65536 (order: 6, 262144 bytes)
Inode-cache hash table entries: 32768 (order: 5, 131072 bytes)
__ex_table already sorted, skipping sort
Initializing CPU#0
Initializing HighMem for node 0 (00000000:00000000)
Memory: 505216k/524224k available (8408k kernel code, 18556k reserved, 3364k dat
a, 636k init, 0k highmem)
virtual kernel memory layout:
    fixmap  : 0xffd36000 - 0xffff000   (2852 kB)
    pkmap   : 0xff800000 - 0xffc00000   (4096 kB)
    vmalloc : 0xe07f0000 - 0xff7fe000   ( 496 MB)
    lowmem  : 0xc0000000 - 0xdfff0000   ( 511 MB)
      .init : 0xc1b80000 - 0xc1c1f000   ( 636 kB)
      .data : 0xc18361c1 - 0xc1b7f240   (3364 kB)
      .text : 0xc1000000 - 0xc18361c1   (8408 kB)
Checking if this processor honours the WP bit even in supervisor mode...Ok.
SLUB: Genslabs=15, HWalign=64, Order=0-3, MinObjects=0, CPUs=1, Nodes=1
Hierarchical RCU implementation.
 RCU restricting CPUs from NR_CPUS=32 to nr_cpu_ids=1.
NR_IRQS:2304 nr_irqs:256 16
Console: colour VGA+ 80x25
console [tty0] enabled
```

3. Operatsion tizim to’liq yulklanib bo’lganidan so’ng AirSlax ishchi stolini ko’rishimiz mumkin:

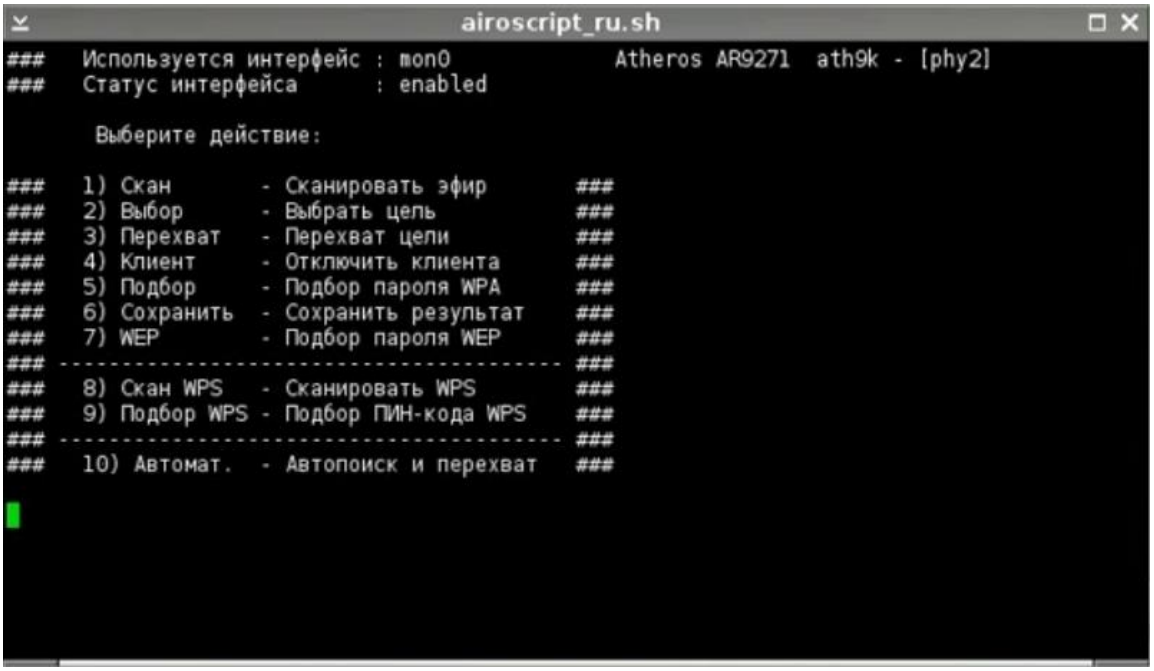
4. Sichqonchaning o’ng tugmasini bosamiz va paydo bo’lgan menyudan AiroScript dasturini ishga tushiramiz:



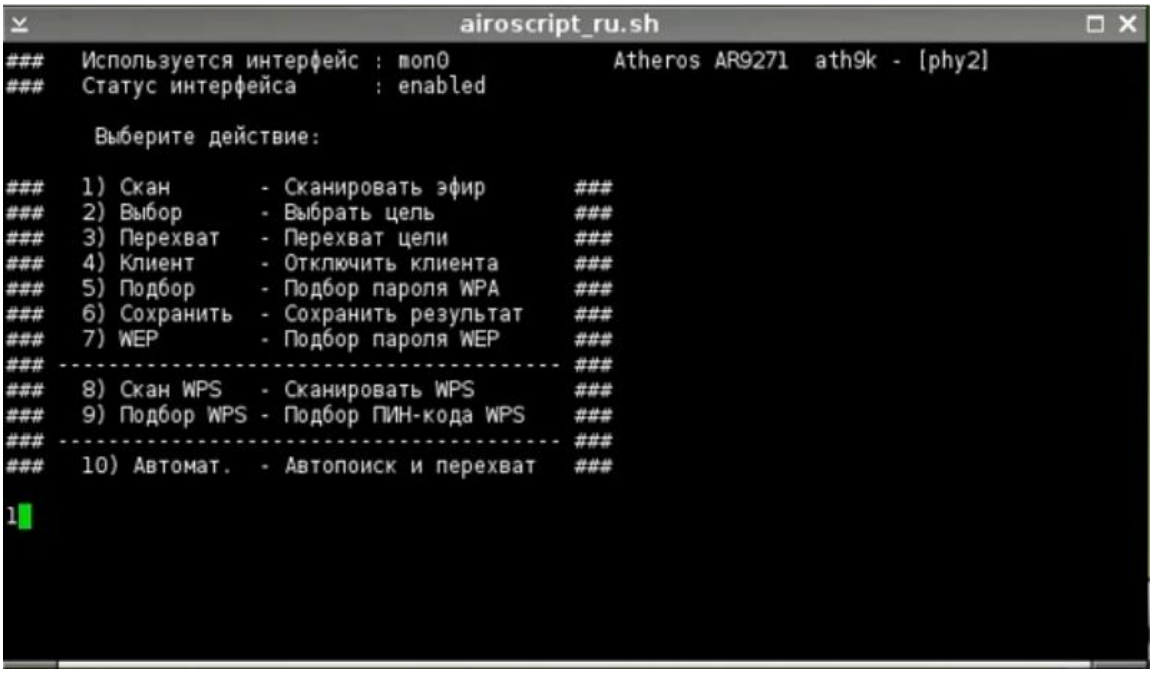
5. Kompyuterimizda mavjud bo’lgan tarmoq platalari ro’yxati ochiladi, ulardan bizga keraklisini tanlaymiz, bizning misolda bu 2 raqam ostidagi Wi-Fi tarmoq platasi:

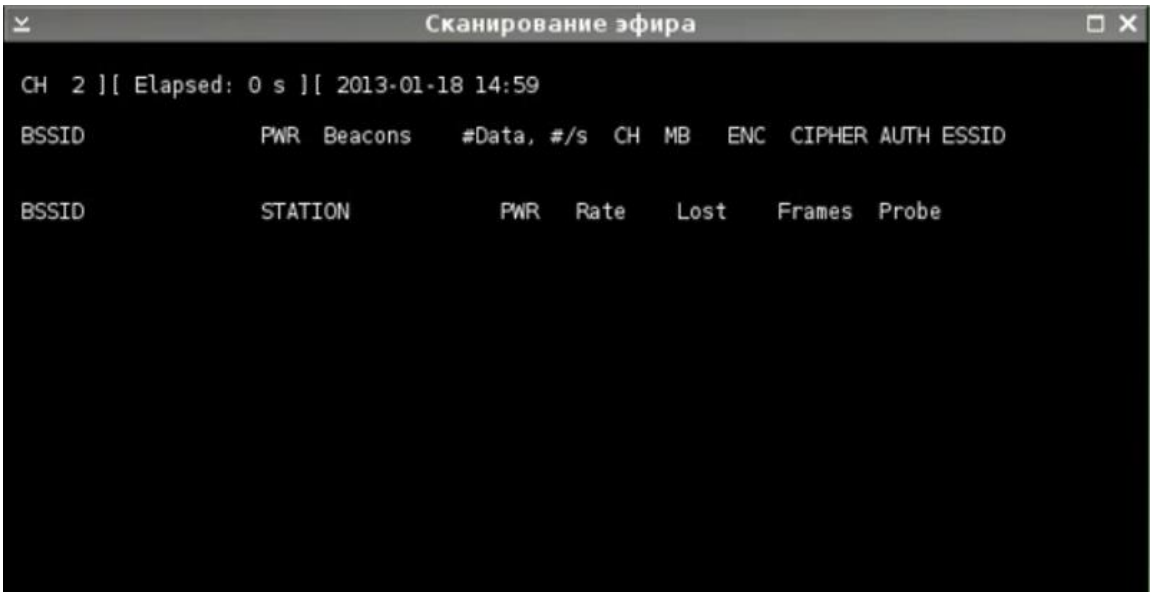


6. Shundan keyin AiroScript dasturining bosh menyusi ochiladi. Bunda «Статусинтерфейса» sohasida «enabled» qiymati turgan bo'lishi kerak. Aks holda tanlagan tarmoq platamizni ishlatish imkoniyati mavjud emas:

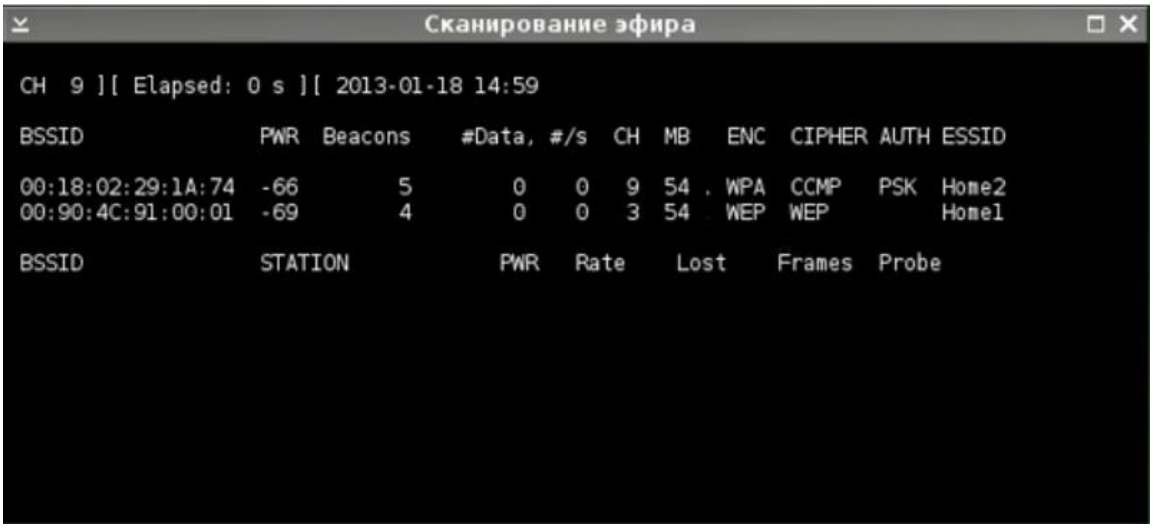


7. 1-bo'lim orqali efirni skanerlaymiz va ulanish nuqtasini qidiramiz:

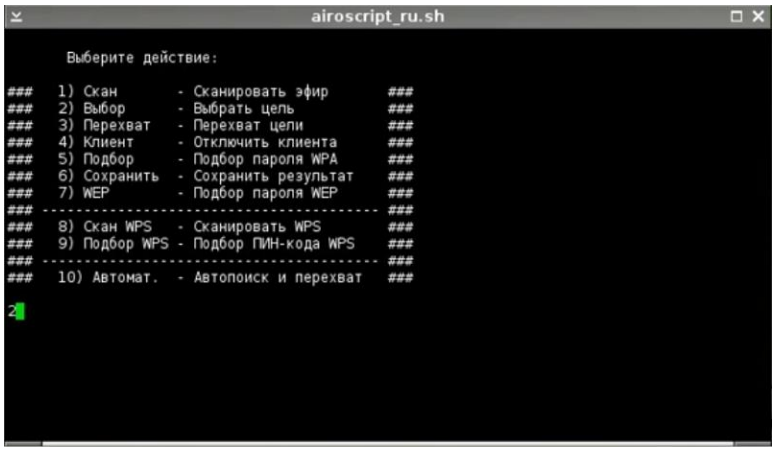


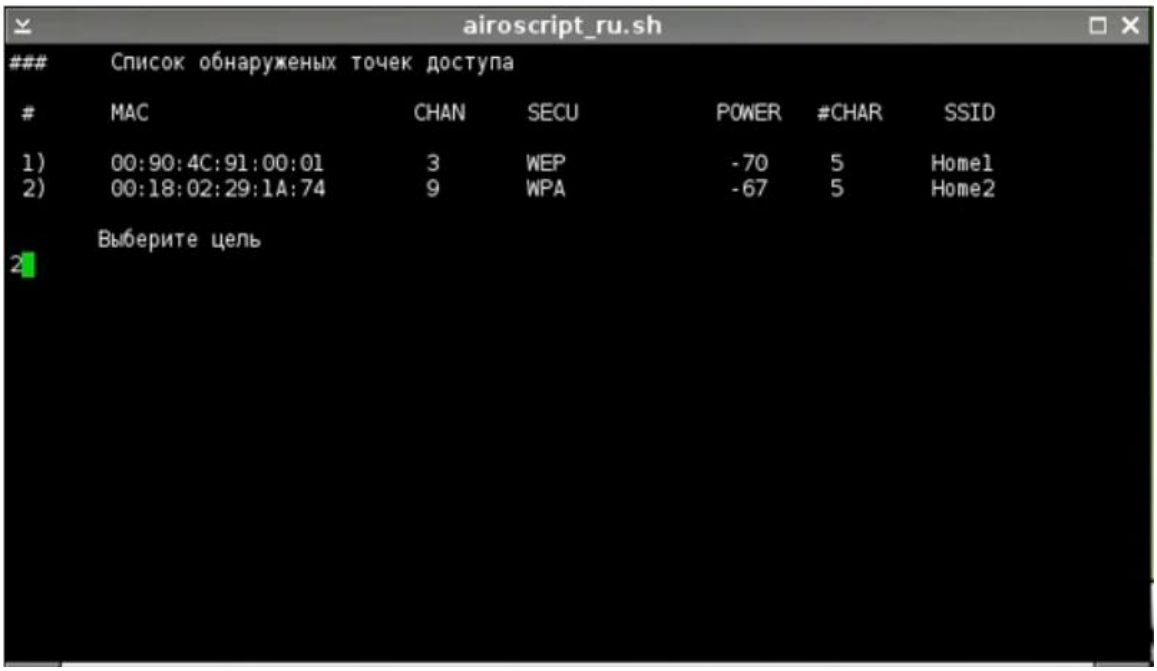


8. Ulanish nuqtalari topilganda so’ng:

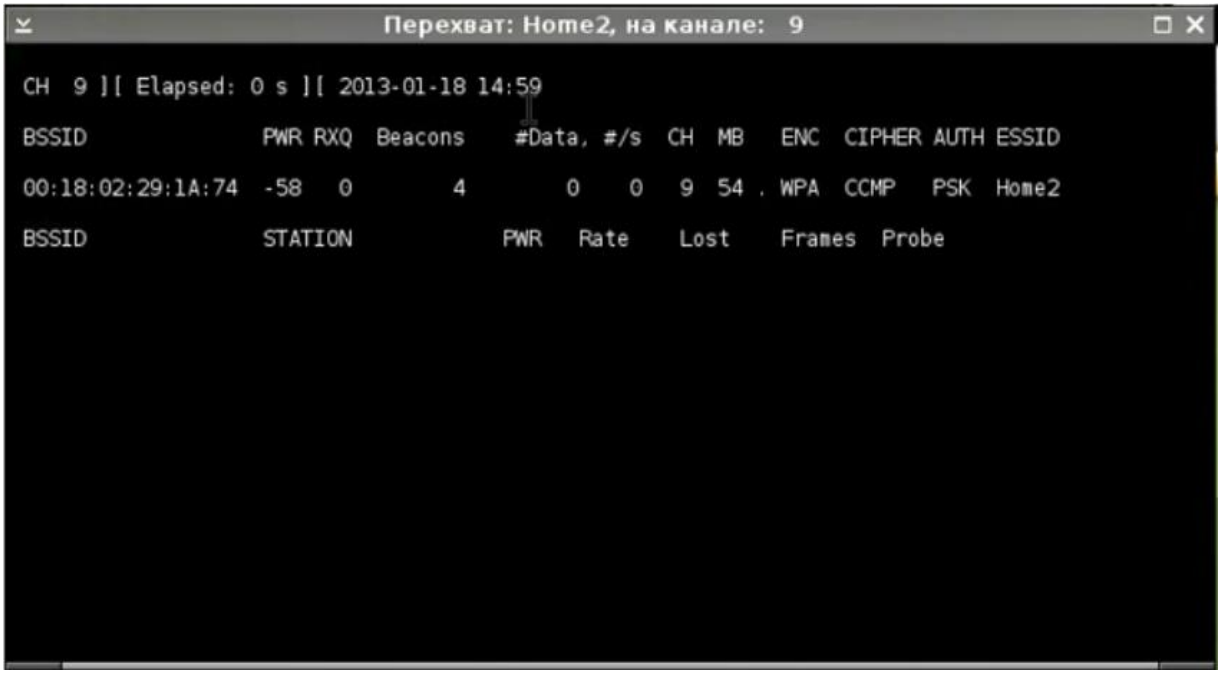


9. 2-bo’lim orqali bizga kerakli ulanish nuqtasini tanlaymiz, bizning misolda bu 2-raqam ostidagi ulanish nuqtasi:

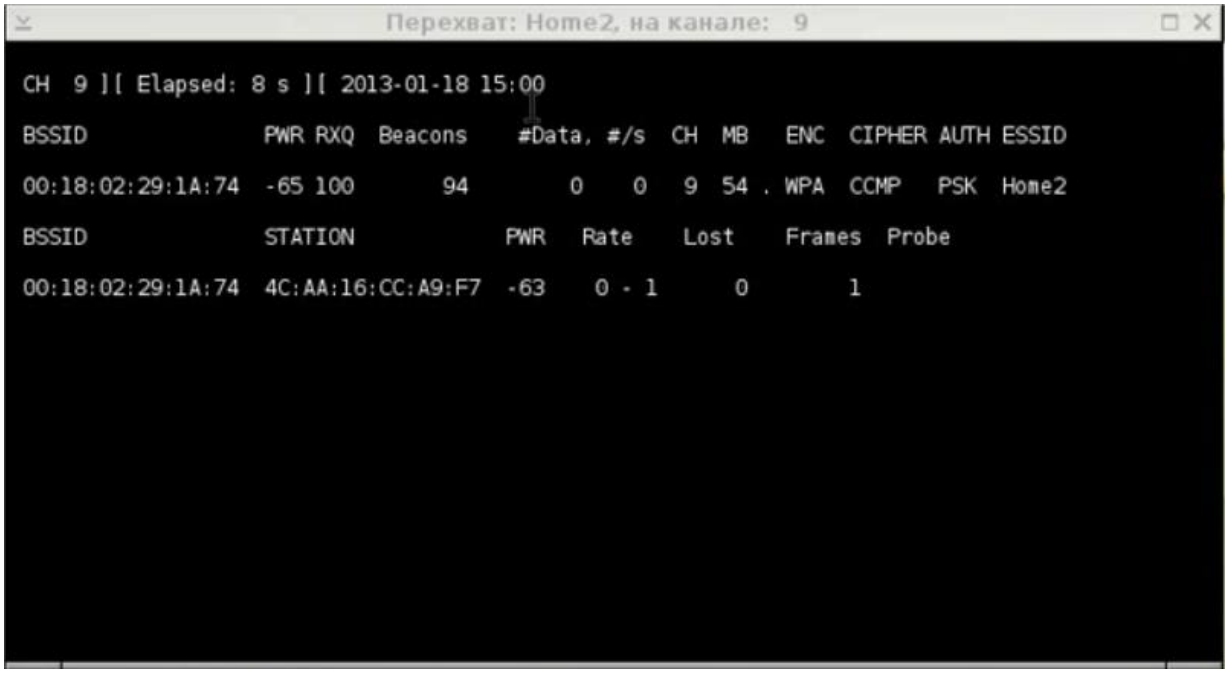




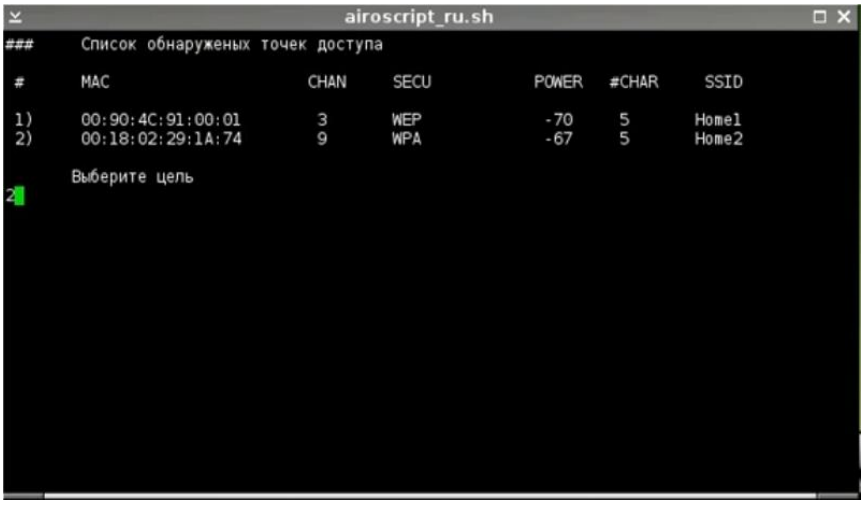
10. 3-bo’lim orqali paketlarni ushlab olish bosqichiga o’tamiz:

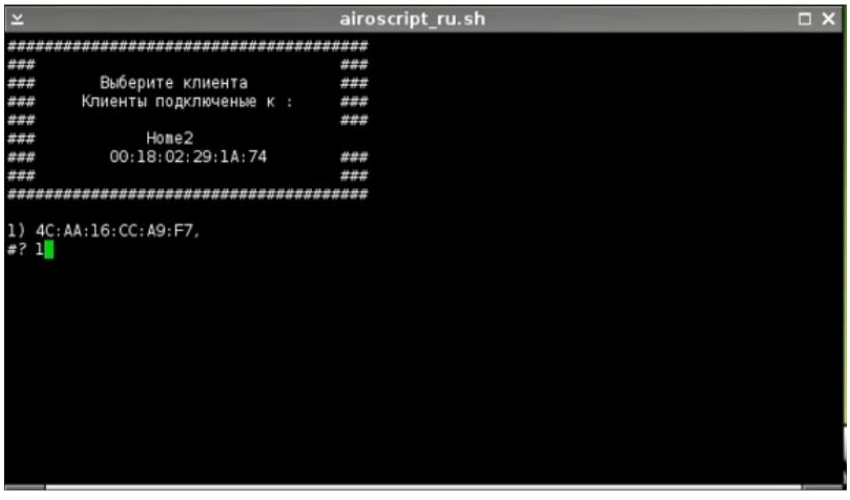


11. Mijozning paydo bo’lishini kutamiz. Bizga kerakli bo’lgan ulanish nuqtasi mijozi paydo bo’lganidan keyin keying qadamga o’tamiz:

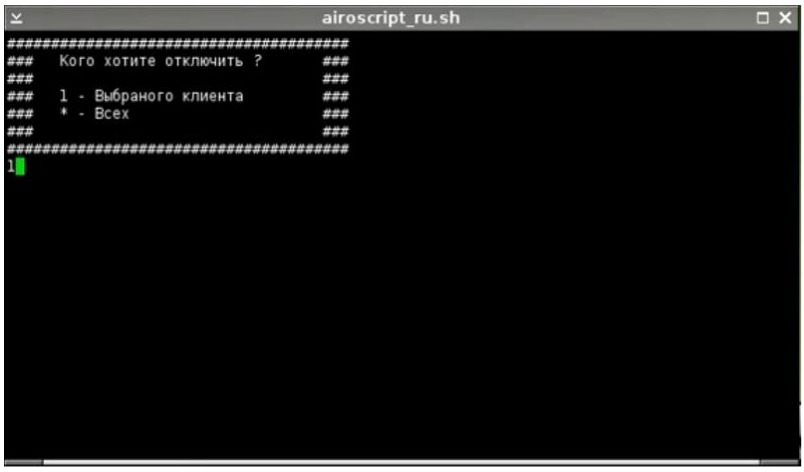


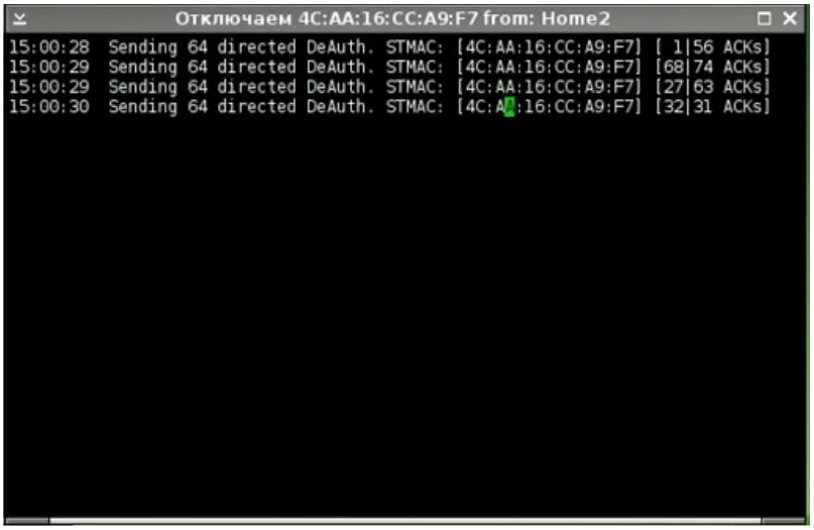
12. Endi 2-bo’limga qaytib paydo bo’lgan mijozni tanlaymiz:



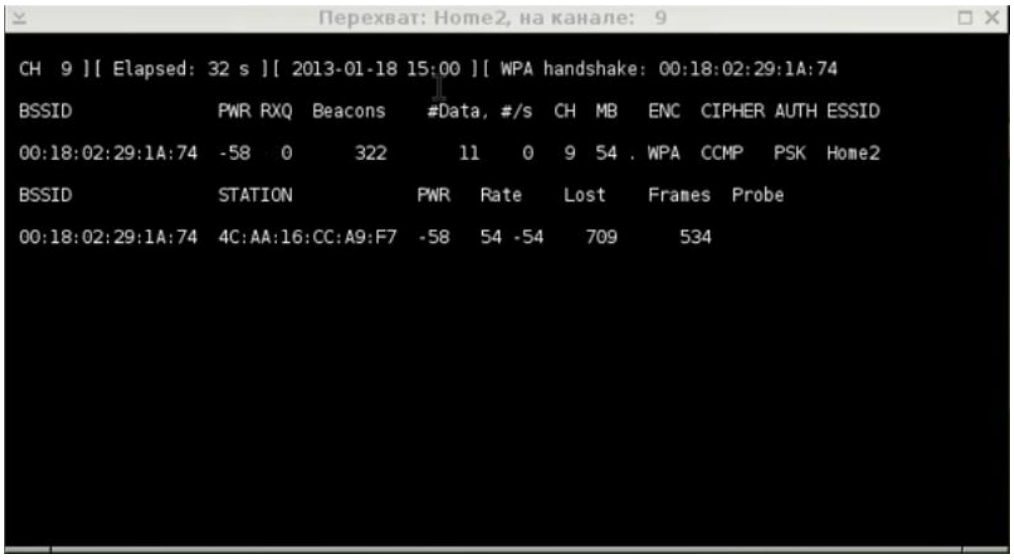


13. 4-bo’lim yordamida tanlangan mijozni o’chiramiz:

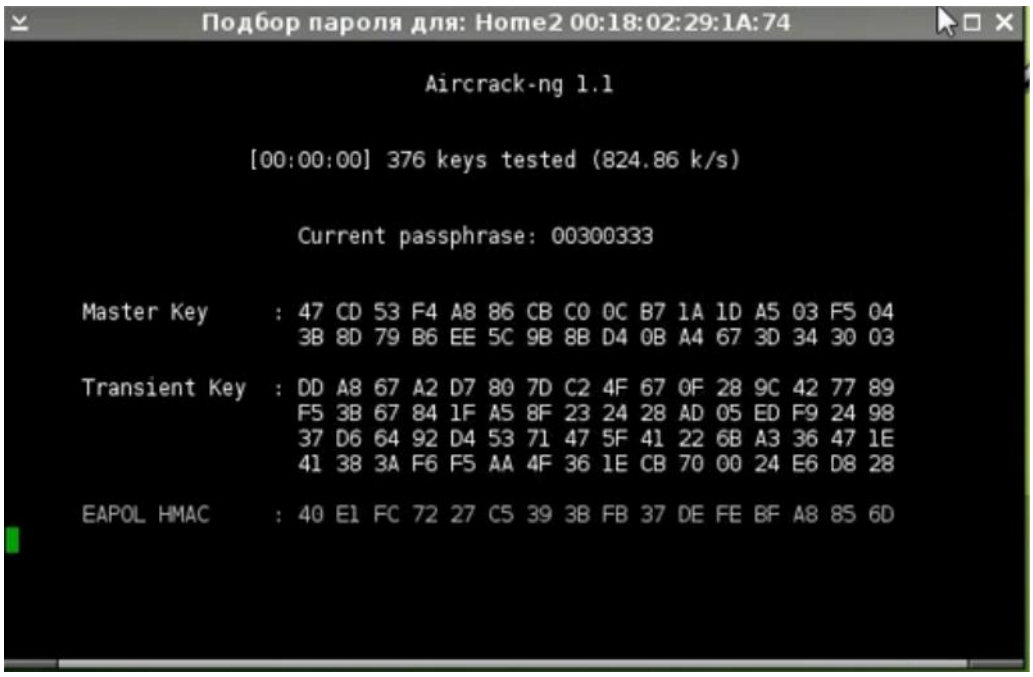




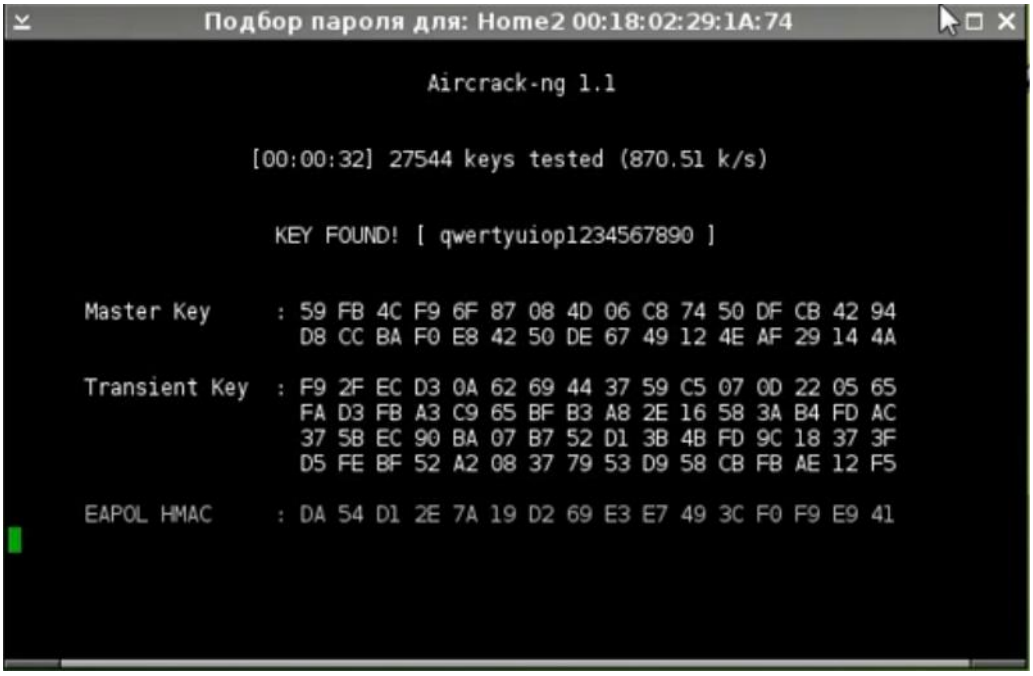
14. Paketlarni ushlab olish oydasida ulanish nuqtasi bilan Handshake ga erishilishini kutamiz:



15. Handshake ga erishilgandan so’ng bosh menyudan 5-bo’limga o’tamiz va parolni qidirishni boshlaymiz:



16. Agar parol topilsa “KEY FOUND!” yozuvi chiqadi va qavs ichida parol keltiriladi:



WEP standarti yordamida himoyalangan Wi-Fi tarmog'i paroloni topish

WEP standarti yordamida himoyalangan Wi-Fi tarmog'i parolini topish uchun 3-bo'limdan so'ng 7-bo'limga o'tish kerak.Muvaffaqiyatli hujumda WEP paroli qariyb 100% holatlarda topiladi.Parolni qidirish o'rtacha 5-10 daqiqa davom etadi.

Endi ushbu hujumlardan qanday qilib himoyalanish haqida qisqacha ma'lumot berib o'tsak.Ma'lumki, WEP standart allaqachon amaldan chiqqan.Lekin shunga qaramasdan, ishlab chiqarilayotgan ko'plab qurilmalar hali ham WEP standartini qo'llab – quvvatlashni davom ettirmoqda.Agar sizning Wi-Fi tarmog'ingizga tashqi tomondan ruxsat etilmagan kirishlar ro'y berishini xohlamasangiz, unda Wi-Fi tarmoqni yaratishda WEP texnologiyasidan foydalanmaslik tavsiya etadi.

WPA standartiga keladigan bo'lsak, u ancha vaqt WEP standarti o'rnini ishonchli egallab keldi.Lekin WPA standartining ham bir qator kamchiliklari topib, himoyasini yorib o'tish usullari ishlab chiqildi.Shunga qaramasdan, WPA standartini sindirish tanlangan parolga bo'gliq.WPA standarti orqali ishonchli himoyani tanlash uchun "qiyin" parollar ishlatilishi kerak.

"Tog'ri" parol yaratish uchun quyidagi tavsiyalarga rioya qilish kerak:

- faqat sonlarning kombinatsiyasidan iborat bo'lgan parolni hech qachon ishlatmaslik kerak, masalan, 123456789, 12345, 44444 va h.;
- ruxsat etilgan standartga binoan parolni iloji boricha maksimal uzunlikda yaratish;
- ishlatilayotgan standartda ruxsat etilgan barcha simvollar to'plami (harflar, raqamlar, ayrim belgilar) elementlaridan foydalanish, masalan, "password" o'rniga "pa$$w0rd-1wrrq";
- harflarning ham yuqori ham pastki registrlarini ishlatish.

WPS texnologiyasi haqida

WPS (Wi-Fi Protected Setup) standarti (va protokoli) ham Wi-Fi tarmoqlarda keng qo'llaniladi. 2007 – yilda Wi-Fi Alliance tomonidan ishlab chiqilgan bo'lib, Wi-Fi tarmoqlarini yaratishda yarim-avtomat standart hisoblanadi.

WPS protokolining asosiy maqsadi Wi-Fi tarmog'ini yaratish jaroyonini osonlashtirishdan iborat, shuning uchun u dastlab Wi-Fi Simple Config deb atalgan. Ushbu protokol kompyuter simsiz tarmoqlari xavfsizligi haqida yetarli bilim va tushunchaga ega bo'lmagan foydalanuvchilarga yordam berish maqsadida ishlab chiqilgan. WPS protokoli Wi-Fi tarmoqni yaratishda tarmoq nomi va shifrlash turini o'zi avtomatik tanlaydi.

TP-Link firmasi routerlarida WPS protokoli anologi QSS (Quick Security Setup) funksiyasi mavjud.

2011 – yilning dekabrida Stefan Fibyok va Kreyg Xeffner WPS protokolining kamchiligini ko'rsatib berishdi. Agar Wi-Fi ulanish nuqtasida WPS standarti aktivlashtirilgan (ya'ni, ishlayotgan) bo'lsa, tarmoq parolini bir necha soatlar ichida topilsh mumkinligi ma'lum bo'ldi.

Tarmoq PIN-kodi 8 xonali raqamlardan iborat bo'lib, mos ravishda PIN-kodning 100 mln.ta variant mavjud. Oxirgi 8-raqam esa oldingi yettita raqamdan keltirib chiqariladigan kontrol summa asosida yaratiladi.Demak, variantlar 10 mln.gacha qisqaradi. Bundan tashqari, WPS protokolining zaifligi PIN-kodni ikki qismga, 4 va 3 tadan raqamga, bo'lib tekshirishga imkon beradi. Bu esa o'z navbatida birinchi qism uchun 10 mingta, ikkinchi qism uchun mingta variant degani.Umumiy holda bor-yog'i 11 mingta variant qoladi.Bu esa 100 mln.dan qariyb 9100 barobar kichik.

Tarmoq xavfsizligini ta'minlash uchun routerning parametrlarida WPS funksiyasini o'chirib qo'yish tavsiya etiladi.

Tarmoq trafigi analizi va hujumlari asoslari

Tarmoq trafigi monitoringi va analizi kompyuter tarmog'ini boshqarish jarayonining ajralmas qismi bo'lib hisoblanadi va diagnostika, testlash va buzilishlarni qidirish, information oqimlar strukturasini optimallashtirish, shuningdek, kompyuter tarmoqlari uzellari va informatsiya xavfsizligini ta'minlash muammolarini aniqlash va yechishda ishlatiladi.

Ushbu bo'limda lokal tarmoq segmentida tarmoq trafigi analizi va protokollar dasturiy analizatori Ethereal bilan ishlash ko'rib chiqiladi.

Tajribalarni bajarish uchun tarmoq kompyuterlari Windows 2000/XP operatsion tizimlari ostida tarmoqqa sozlangan bo'lishlari, va ba'zi bir hollarda Internet tarmog'iga ulanish talab etiladi. Bundan tashqari WinPCap (2.3 versiyasidan yuqori) kutubxonasi va Ethereal (0.10.11 versiyasidan yuqori) analizatori kerak bo'ladi.

1.1. Dastur haqida umumiy ma'lumotlar.

Tarmoq monitoringgi va tarmoq trafigini analiz qiluvchi ko'plab instrumental vositalar mavjud. Bunday vositalardan biri Ethereal paketi, u protokollarning dasturiy analizatori bo'lib hisoblanadi. Protokollar analizatori tarmoq adapterini kadrlar qabul qilishning "tartibsiz" rejimiga o'tkazadi, oz'ining buferiga tarmoq trafigining filtrlangan kadrlarini yozib qo'yadi, foydalanuvchi so'roviga asosan ekaranga u yoki bu kadrlarni chiqaradi va protokollar dekoderi yordamida protokol sarlavhasidagi sohalar qiymati va ma'lumotlar bloki haqidagi ma'lumotlarni foydalanuvchiga yetkazib beradi.

Shu turdagi ko'pchilik dasturlar singari, Ethereal quyidagi komponentlardan iborat:

- hujum filtri;
- kadrlar buferi;
- protokollar dekoderi;
- kadrlar nomoyishi filtri;
- statistika moduli (eksert tizim elementlari bilan).

Ethereal ning shubhasiz afzalliklariga quyidagilar kiradi:

- Unix va Windows operatsion tizimlarida ishlay olishi;
- dastur kodi ochiqligi;

- turli xil texnologiyalar tarmoq segmentlarida trafikni ushlab olish imkoniyati;
- juda ko’plab protokollarni (700 dan ortiq) analiz qilish imkoniyati;
- natijalarni o’ndan ortiq formatlarga eksport qilish;
- juda qulay qidirish va filtrlash tizimi;
- ekspert tizimi elementlari mavjudligi;
- ajratilgan paketlar fragmentini diskda saqlab qo’yish;
- va boshqa bir qator qulayliklar.

1.2. Dasturni o’rnatish va hujumga tayyorlanish.

1. WinPCap kutubxonasi va Ethereal analizatorini o’rnating.

2. Ethereal dasturini oching va dastur bosh oynasini butun ekranga yoying.

Hujumnu uyushtirishdan oldin, kerakli parametrlarni to’g’irlab chiqish kerak.

3. Menyudan ***Capture => Options*** qismiga kiring.

Ochilgan oyna yordamida quyidagi parametrlarni o’rnating (1.1 - rasm):

- Interface – ro’yxatdan kompyuteringizning tarmoq adapterini tanlang;

- Buffer size – buffer hajmi (jimlikda 1 MB);

- Capture packets in promiscuous mode – tartribsiz rejimni ishlatish.

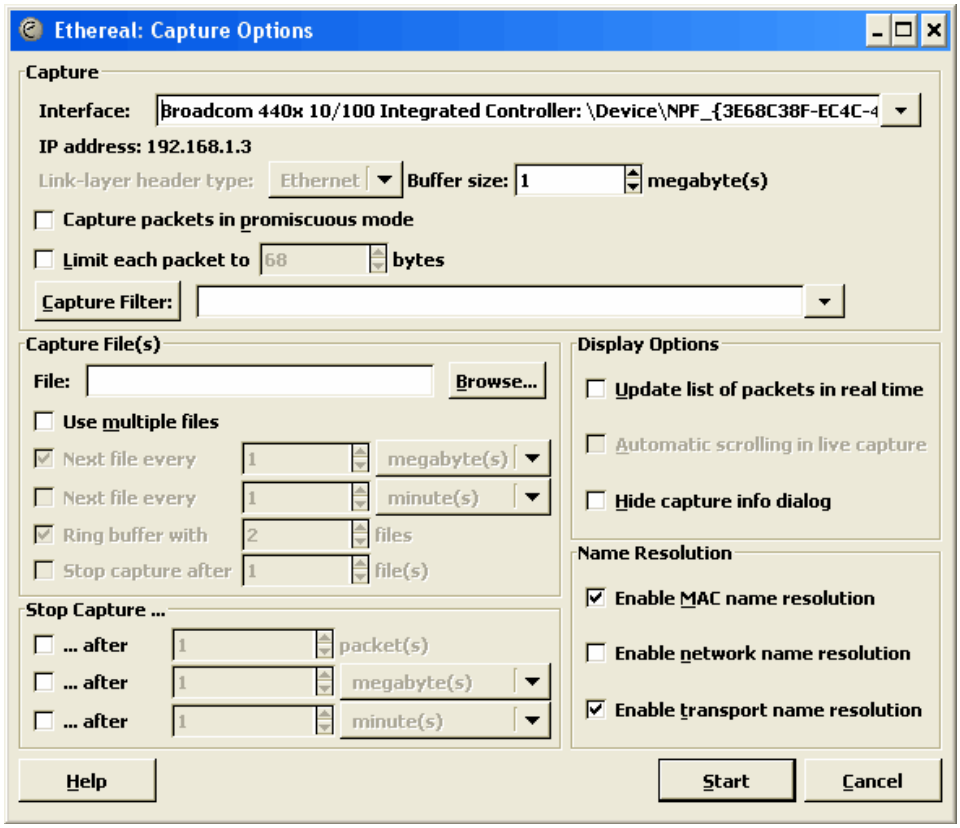
4. “Capture packets in promiscuous mode” rejimini o’chirib qo’ying. Bu holda faqat o’zingizning kadrlaringizni ushlab olasiz. Paketlar soni ancha kamayadi va ishlashni yengillashtiradi.

1.3. Dasturning foydalanuvchi interfeysi.

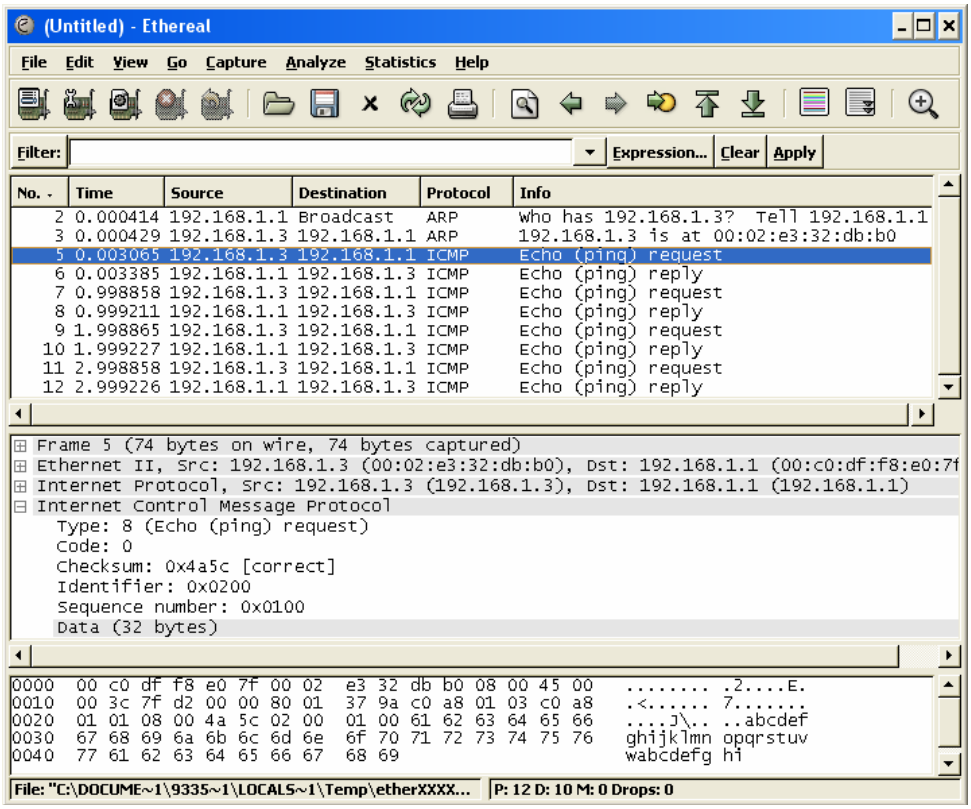
5. ARP protokoli kesh xotirasin tozalash uchun MS-DOS buyruqlar yordamchisini chaqirib, arp –d buyrug’ini bajaring. Ethereal da jarayonni boshlash uchun “Capture” tugmachasini bosing. Buyruqlar yordamchisida ping <server_nomi> (server nomi o’rnida uning IP – manzilini ham ishlatish mumkin) buyrug’ini bajaring. Ping buyrug’i yakuniga yetgandan so’ng “Stop” tugmachasini bosing.

Ethereal dasturi ekrani monitorida hozirgina buferga yozilgan tarmoq paketlarini ko’rsatuvchi bir nechta panelni ko’rishimiz mumkin.dastur oynasining umumiy ko’rinishi 1.2. – rasmda keltirilgan.

Paketlar ro’yxati paneli har qatorda u yoki bu paket xarakteristikalarini ko’rsatadi.



(1.1. – rasm)



(1.2. – rasm)

1.4. Paketlar ko’rsatilish filtri.

Paketlar namoyishini qulaylashtirish uchun filtrlarndan foydalanish mumkin.

6. Faqat ICMP paketlarini ajratib olish uchun “Filter” sohasiga “icmp” kalit so’zini kiriting va “Apply” tugmachasini bosing.

Filtrlar va ularni ishlatish misollari	
frame.marked	Маркированный кадр `frame.marked == true`
frame.number	Номер кадра `frame.number == 150`
frame.time	Время захвата кадра `frame.time == "Feb 1, 2006 09:00:00"`
frame.pkt_len	Длина кадра `frame.pkt_len == 48`
eth.dst	Заголовок Ethernet: MAC-адрес назначения `eth.dst == 01:00:5e:00:00:02`
eth.src	Заголовок Ethernet: MAC-адресисточника `eth.src == 00:a0:cc:30:c8:db`
eth.type	Заголовок Ethernet: тип вложенного протокола `eth.type == 0x0800`
arp.hw.type	Заголовок протокола ARP: тип протокола канального уровня `arp.hw.type == 0x0001`
arp.proto.type	Заголовок протокола ARP: тип протокола сетевого уровня `arp.proto.type == 0x0800`

arp.opcode	Заголовок протокола ARP: MAC-адрес источника `arp.src.hw_mac == 00:10:4b:30:c4:4a`
arp.src.proto_ipv4	Заголовок протокола ARP: IP-адрес источника `arp.src.proto_ipv4 == 10.1.0.1`
arp.dst.hw_mac	Заголовок протокола ARP: MAC-адрес назначения `arp.dst.hw_mac == 00:00:00:00:00:00`
arp.dst.proto_ipv4	Заголовок протокола ARP: IP-адрес назначения `arp.dst.proto_ipv4 == 10.1.0.2`
ip.version	Заголовок протокола IP: версия протокола IP `ip.version == 4`
ip.hdr_len	Заголовок протокола IP: длина заголовка `ip.hdr_len == 24`
ip.flags.df	Заголовок протокола IP: флаг фрагментации `ip.flags.df == 0`
ip.flags.mf	Заголовок протокола IP: флаг не последнего фрагмента `ip.flags.mf == 0`
ip.frag_offset	Заголовок протокола IP: смещение фрагмента `ip.frag_offset == 0`
ip.ttl	Заголовок протокола IP: время жизни пакета `ip.ttl == 1`

ip.proto	Заголовок протокола IP: протокол вышестоящего уровня `ip.proto == 0x01`
ip.dst	Заголовок протокола IP: IP-адрес назначения `ip.dst == 224.0.0.2`
ip.addr	Заголовок протокола IP: IP-адрес `ip.addr == 10.2.0.0/16`
tcp.srcport	Заголовок протокола IP: порт источника `tcp.srcport == 1054`
tcp.dstport	Заголовок протокола IP: порт назначения `tcp.dstport == 21`
tcp.seq	Заголовок протокола IP: последовательный номер `tcp.seq == 4856133`
tcp.ack	Заголовок протокола IP: номер подтверждения `tcp.ack == 4856134`
tcp.flags.urg	Заголовок протокола IP: бит присутствия срочных данных `tcp.flags.urg == 0`
tcp.flags.ack	Заголовок протокола IP: бит присутствия подтверждения `tcp.flags.ack == 1`
tcp.flags.push	Заголовок протокола IP: бит выталкивания данных `tcp.flags.push == 0`

tcp.flags.reset	Заголовок протокола IP: бит сброса соединения `tcp.flags.reset == 0`
tcp.flags.syn	Заголовок протокола IP: бит синхронизации сессии `tcp.flags.syn == 1`
tcp.flags.fin	Заголовок протокола IP: бит завершения сессии `tcp.flags.fin == 0`
tcp.window_size	Заголовок протокола IP: размер приемного окна `tcp.window_size == 8760`
udp.srcport	Заголовок протокола UDP: порт источника `udp.srcport == 2364`
udp.dstport	Заголовок протокола UDP: порт назначения `udp.dstport == 53`
icmp.type	Заголовок протокола ICMP: тип сообщения `icmp.type == 8`
icmp.code	Заголовок протокола ICMP: уточняющий код сообщения `icmp.code == 0x00`

Ishlatiladigan taqqoslash amallari:

- == (eq) – teng, masalan, icmp.type == 8;
- != (ne) – teng emas, masalan, eth.type != 0x0800;
- > (gt) – katta, masalan, tcp.srcport > 1023;
- < (lt) – kichik, masalan, frame.pkt_len lt 60;
- >= (ge) – katta yoki teng, masalan, frame.pkt_len ge 60;
- <= (le) – kichik yoki teng, masalan, tcp.dstport <=1023.

7. Yuqorida keltirilgan filtrlarni ishlatib ko'ring va ular qanday natija berishini tekshirib ko'ring.

8. `!(ip.addr == X.X.X.X)` va`ip.addr !== X.X.X.X`. misollari orasidagi farqni tushuntirib bering.

Filtrlash amallari sifatida quyidagilarni ham ishlatish mumkin:

- && (AND) – mantiqiy "va",

masalan: `(ip.dst==10.0.0.1) AND tcp.flags.syn`;

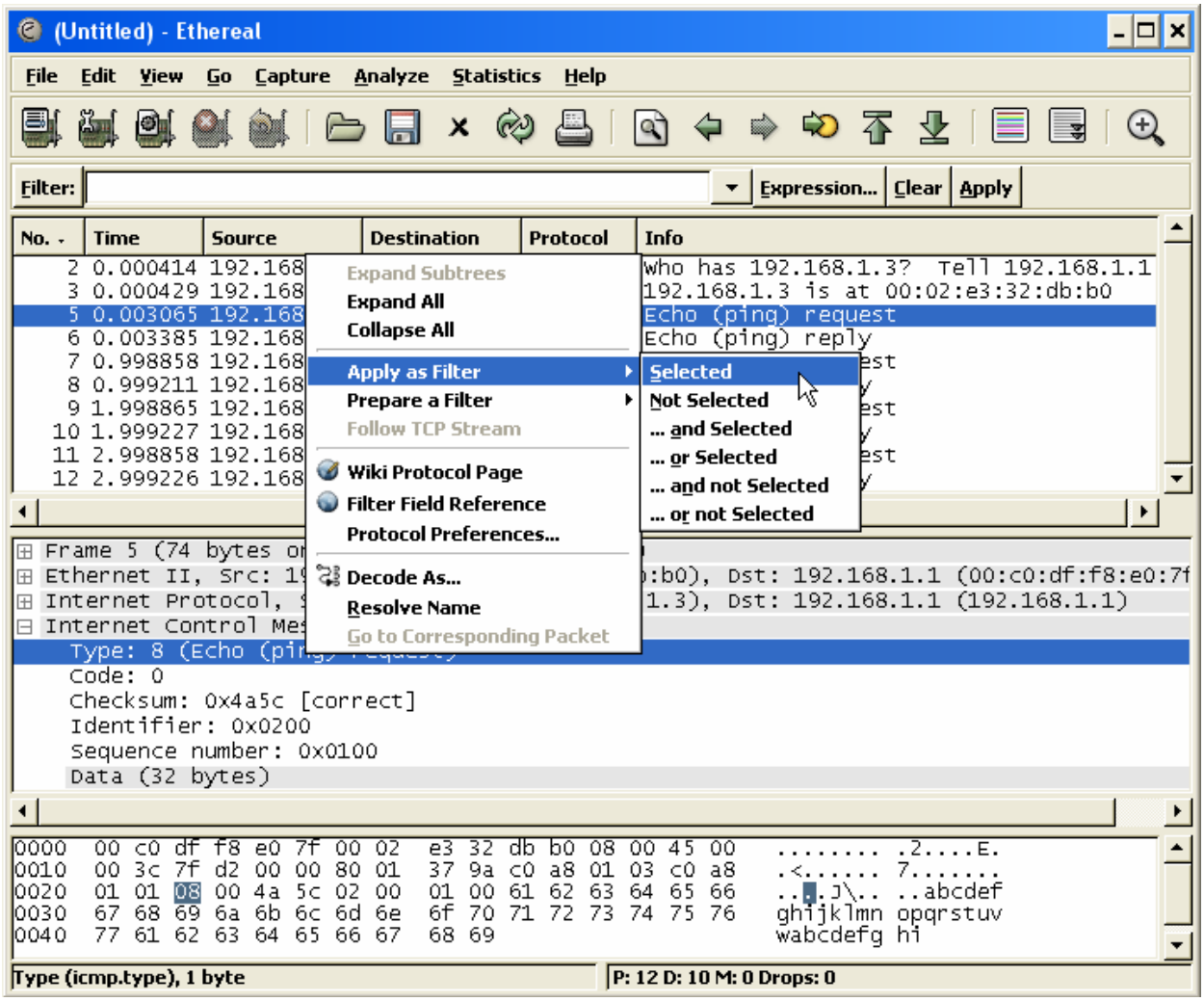
- || (OR) – mantiqiy "yoki",

masalan:`(ip.addr==10.0.0.1) OR (ip.addr==10.0.0.2).`

9. Faqat ICMP – so'rovlarini ajratib oling.

10. ICMP kadrlaridan tashqari barcha kadrlarni ajratib oling.

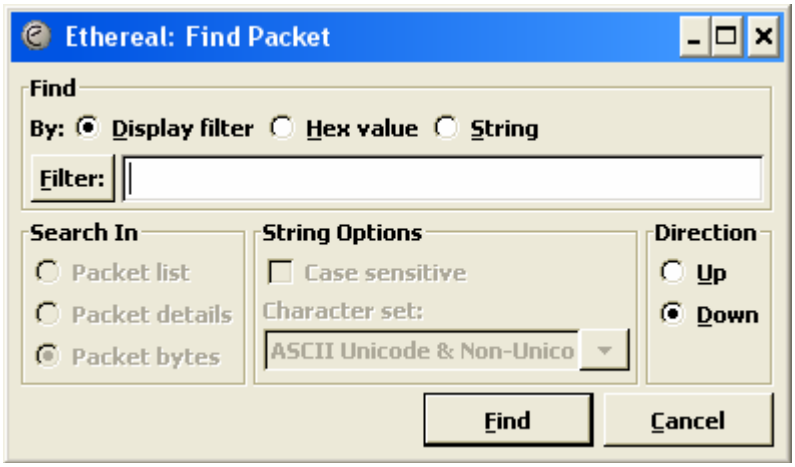
Filtrlash parametrlarini tozalash uchun "Clear" tugmachasini bosing.



(1.4. – rasm. Paketlarni qidirish kriteriylarini aniqlash oynasi)

1.5. Kadrlarni qidirish.

U yoki bu kriteriylarni qoniqtiradigan kadrlarni buferdan qidirish menyuning ***Edit => Find*** komandaso orqalo amalga oshiriladi.Paketlarni qidirish kriteriylarini aniqlash oynasi 1.4. – rasmda ko'rsatilgan.



1.6. Kalit kadrlarni ajratish.

Bufer ro'yxatida analiz uchun muhimroq va kalit paketlarni asosiy menyuning ***Edit => Mark Packet*** (toogle) buyrug'i yoki kontekst menyuning **Mark Packet (toogle)** buyrug'i orqali belgilab olish mumkin. Bu imkoniyat ayniqsa, katta buferlar bilan ishlashda kerak bo'ladi, kerakli ajratib qo'yilgan paketlar boshqa rangga bo'yaladi, shuningdek saqlab qo'yish, eksport qilish va chop qilishda ham bu ranglar saqalanadi.

1.7. Natijalarni saqlab qo'yish.

Ma'lumotlarni faylga saqlash menyuning ***File =>Save*** yoki ***File => Save As*** buyruqlari orqali amalga oshiriladi. Ma'lumotlarni saqlash oynasi 1.5. – rasmda keltirilgan.

Ma'lumotlarni saqlashda biz bir necha xil saqlash variantlaridan foydalanishimiz mumkin:

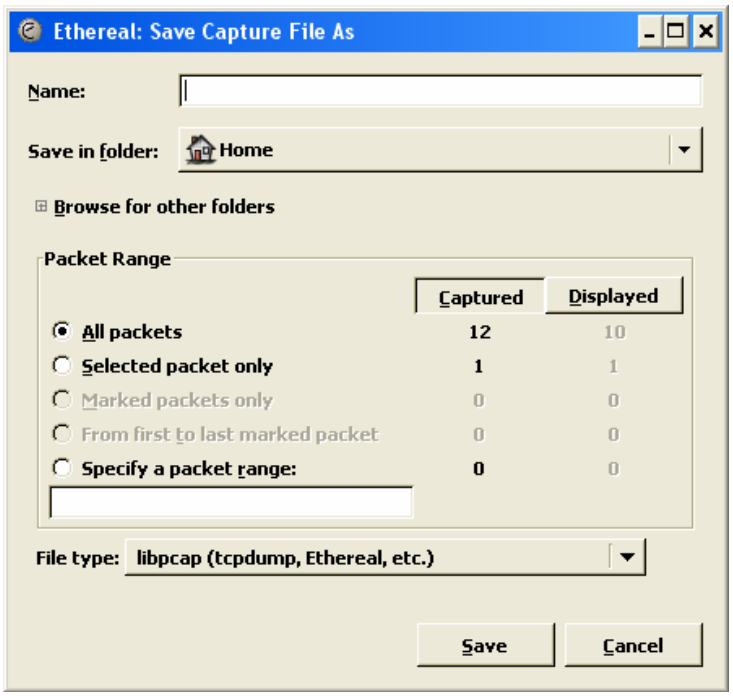
All packets – barcha paketlar;

Displayed – faqat namoyish etilayotganlar;

Selected packet only – tanlangan paket;

Marked packet onlyva***From list to last marked packet*** – oldin belgilab qo'yilgan paketlar;

Specif a packet range – ko'rsatilgan paketlar diapazoni.



(1.5 – rasm)

Jimlikda Ethereal ma’lumotlarni Libpcap tipida saqlaydi, bu format TcpDump dasturi fayllari bilan mos keladi. Ma’lumotni saqlashda **File type** ro’yxatidan boshqa, 20 dan ortiq, formatlarga ham eksport mumkin. Shuni sedan chiqarmaslik kerakki, yangi seans boshlashdan oldin olingan natijalarni albatta saqlab qo’yish kerak.

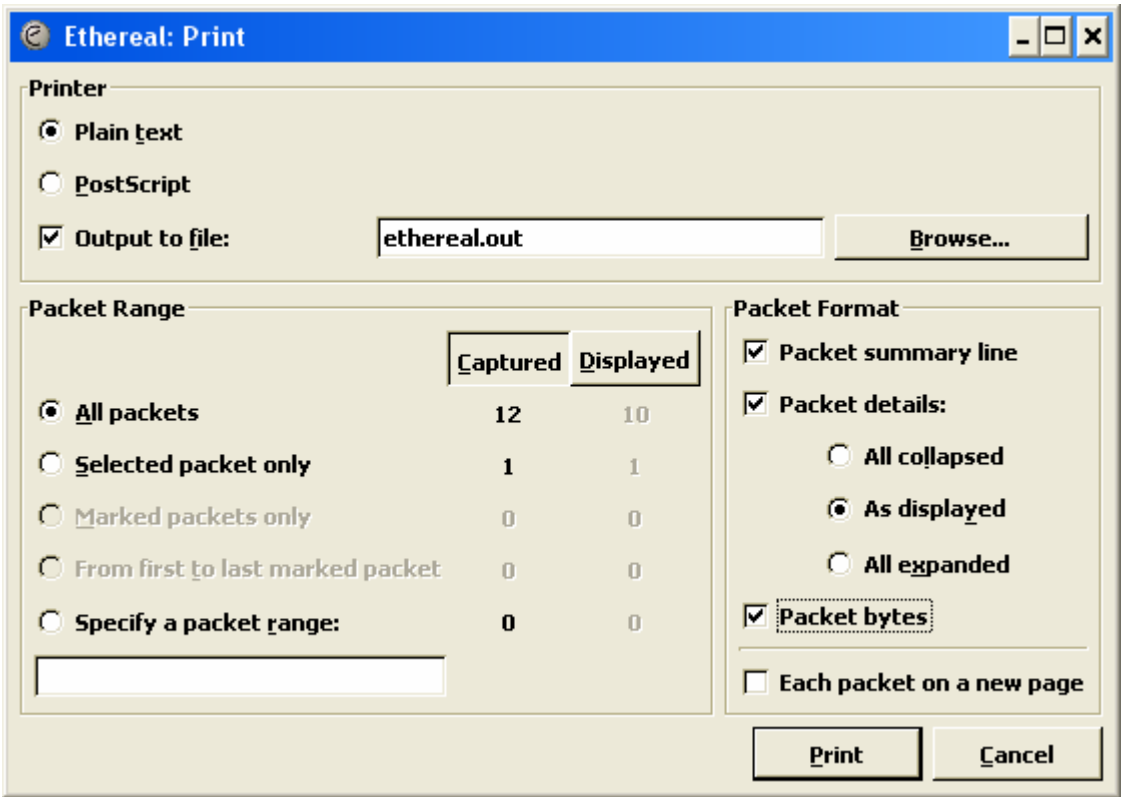
1.8. Ma’lumotlarni chop qilish.

Paketlar haqidagi ma’lumotlarni chop qilish uchun **Print** buyrug’idan foydalaniladi. Chop etish oynasining umumiy ko’rinishi 1.6. – rasmda keltirilgan.

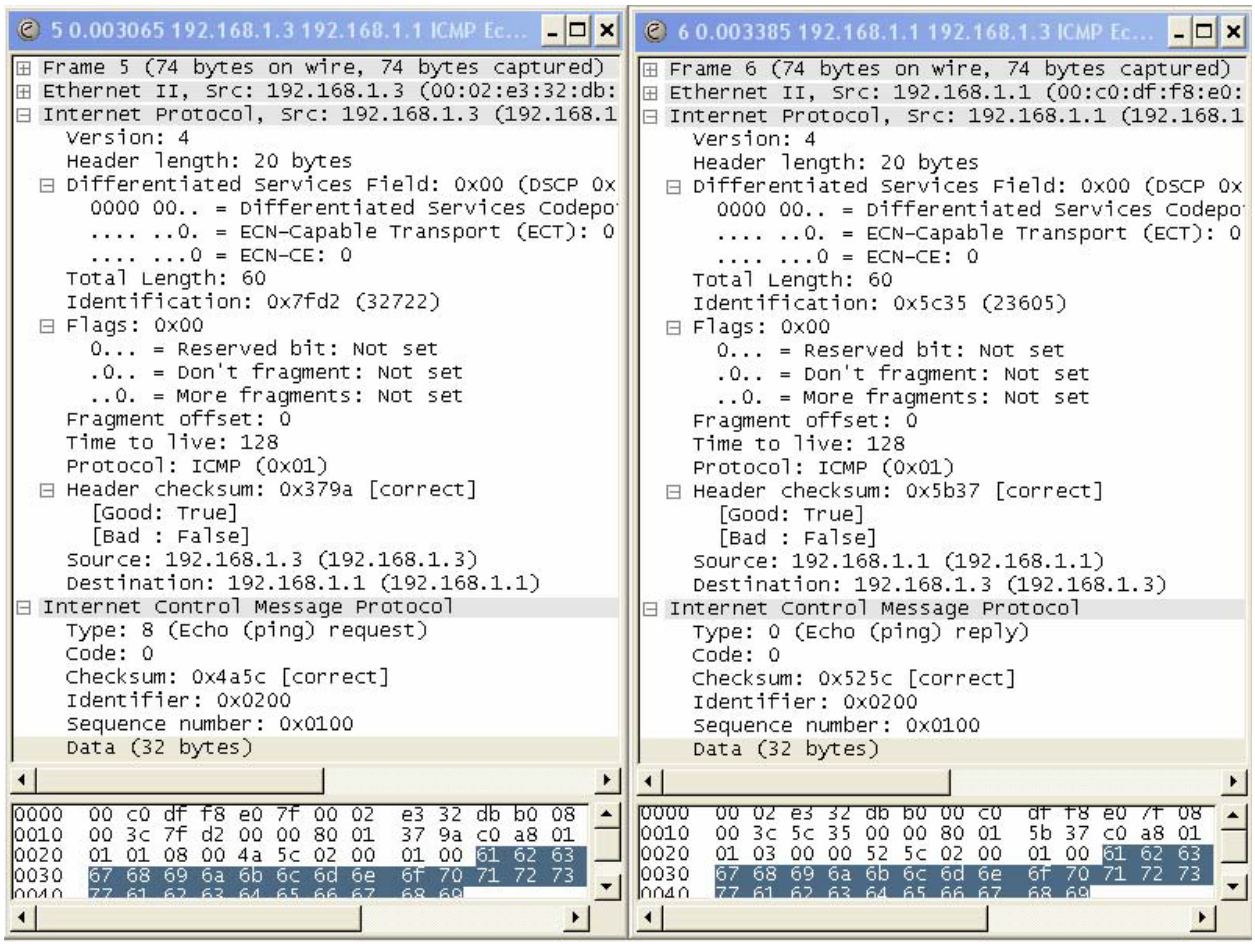
1.9. Kadrlarni alohida oynada ko’rish.

Skrinshotlar yordamida hisobotlar tuzish vaqtida, ma’lumotlarni analiz qilishda ikkita paketni birgalikda kuzatish uchun kadrlarni alohida oynada ko’rish imkoniyati qo’shimcha qulayliklarni tug’diradi.

Bunday imkoniyat ***View => Show Packet in New Window*** buyrug’I orqali amalga oshirilishi mumkin.Turli xil paketlarni namoyish etuvchi oynalar 1.7. – rasmda ko’rsatilgan.



(1.6. – rasm)


5 0.003065 192.168.1.3 192.168.1.1 ICMP Ec...
Frame 5 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 192.168.1.3 (00:02:e3:32:db:
Internet Protocol, Src: 192.168.1.3 (192.168.1
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x
0000 00.. = Differentiated Services Codepo
.... ..0. = ECN-Capable Transport (ECT): 0
....0 = ECN-CE: 0
Total Length: 60
Identification: 0x7fd2 (32722)
Flags: 0x00
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 128
Protocol: ICMP (0x01)
Header checksum: 0x379a [correct]
[Good: True]
[Bad : False]
Source: 192.168.1.3 (192.168.1.3)
Destination: 192.168.1.1 (192.168.1.1)
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x4a5c [correct]
Identifier: 0x0200
Sequence number: 0x0100
Data (32 bytes)
0000 00 c0 df f8 e0 7f 00 02 e3 32 db b0 08
0010 00 3c 7f d2 00 00 80 01 37 9a c0 a8 01
0020 01 01 08 00 4a 5c 02 00 01 00 61 62 63
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73
6 0.003385 192.168.1.1 192.168.1.3 ICMP Ec...
Frame 6 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 192.168.1.1 (00:c0:df:f8:e0:
Internet Protocol, Src: 192.168.1.1 (192.168.1
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x
0000 00.. = Differentiated Services Codepo
.... ..0. = ECN-Capable Transport (ECT): 0
....0 = ECN-CE: 0
Total Length: 60
Identification: 0x5c35 (23605)
Flags: 0x00
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 128
Protocol: ICMP (0x01)
Header checksum: 0x5b37 [correct]
[Good: True]
[Bad : False]
Source: 192.168.1.1 (192.168.1.1)
Destination: 192.168.1.3 (192.168.1.3)
Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0x525c [correct]
Identifier: 0x0200
Sequence number: 0x0100
Data (32 bytes)
0000 00 02 e3 32 db b0 00 c0 df f8 e0 7f 08
0010 00 3c 5c 35 00 00 80 01 5b 37 c0 a8 01
0020 01 03 00 00 52 5c 02 00 01 00 61 62 63
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73

(1.7. – rasm)

“AXBOROT XAVFSIZLIGINING USUL VA VOSITALARI” FANIDAN “KOMPYUTER TARMOG’IDA INFORMATSIYA HIMOYASI” MAVZUSI BO’YICHATAJRIBA MASHG’ULOTI TA`LIM TEXNOLOGIYASI

Kadrlar tayyorlash Milliy dasturining ikkinchi bosqichi ta`lim jarayonidagi sifat ko’rsatkichlarini yaxshilash, ya`ni jahon andozalariga mos, raqobatbardosh, yuqori saviyaga ega bo’lgan mutaxassislar tayyorlashdir. Ushbu murakkab muammolarni yechimini topib ularni amalda keng qo’llash oliy ta`lim tizimi personali oldiga juda katta vazifalar belgilaydi. Bunda aniq vazifalar sifatida bevosita o’quv jarayonini yaxshilash, o’quv dasturlarini yanada takomillashtirish, o’qitishning zamonaviy pedagogik texnologiyalarini amalga joriy qilish, texnik vositalaridan keng foydalanish va shu asosda masofadan o’qitishni keng joriy qilishdan iboratdir.

Shaxsga yo’naltirilgan ta`lim. Bu ta`lim o’z mohiyatiga ko’ra ta`lim jarayonining barcha ishtirokchilarini to’laqonli rivojlanishlarini ko’zda tutadi. Bu esa ta`limni loyihalashtirilayotganda, albatta, ma`lum bir ta`lim oluvchining shaxsini emas, avvalo, kelgusidagi mutaxassislik faoliyati bilan bog’liq o’qish maqsadlaridan kelib chiqgan holda yondoshishni nazarda tutadi.

Shundan kelib chiqqan holda quyida “Axborot xavfsizligining usul va vositalari” o’quv fani bo’yicha “Kompyuter tarmog’ida informatsiya himoyasi” mavzusida tajriba mashg’ulotining o’tish tartibi keltiriladi.

Tajriba vizual tajriba shaklida olib boriladi. Tajribaning mazkur shakli vizual materiallarni namoyish etish hamda ularga aniq va qisqa sharhlar berishga qaratilgan. Pedagogik vazifasi: yangi o’quv malumotlarini o’qitishning texnik vositalari va audio, videotexnika yordamida berish.

Talabani baholashda FSMU texnologiyasidan foydalaniladi. Ushbu texnologiya talaba (yoki o’quvchi)larni tarqatilgan oddiy qog’ozga o‘z fikrlarini aniq va qisqa holatda ifoda etib, tasdiqlovchi dalillar yoki inkor etuvchi fikrlarni bayon etishga yordam beradi.

Tajribani o’qitish texnologiyasi

O’quv mashg’uloti shakli:	**Tajriba**
Tajriba mashg’uloti tuzilishining rejasi:	**1. Kompyuter tarmoqlarida uchraydigan hujumlar.** **2. AirSlax OT dasturlar to’plami yordamida Wi-Fi tarmog’i xavfsizligini tekshirish.**
O’quv mashg’ulotining maqsadi:	**Kompyuter tarmoqlarida hujumlarnini mavjudligi va ularni amalda bajarish.**
Pedagogik vazifalar: **1. Kompyuter tarmoqlarida uchraydigan hujumlar to`g`risida ma`lumot berish** **2. AirSlax OT da dasturlar to’plamini ishlatishni o’rganish**	**O’quv faoliyatining natijalari:** **1. Kompyuter tarmoqlarida uchraydigan hujumlar to`g`risida ma`lumot olish** **2. AirSlax OT da dasturlar to’plamini ishlatishni o’rganish**
O’qitish vositasi:	**Kompyuter, videoproektor, taqdimot slaydlari, virtual ko’rgazma, kartochkalar, AirSlax OT.**
O’qitish shakli:	**Vizual tajriba;**
O’qitish shartlari:	**Guruhiy ishlash uchun texnik jihozlangan auditoriya.**
Monitoring va baholash:	**FSMU so’rov va reyting bali asosida baholash.**

“KOMPYUTER TARMOG’IDA INFORMATSIYA HIMOYASI”

mavzusidagi tajribaning texnologik xaritasi

Darsbosqichlari	Vaqt daq	Dars mazmuni	Metod	Vosita
1.Tashkiliy qism	5	1.1.Salomlashish, yo’qlama qilish. 1.2.Talabalarning darsga tayyorgarligini ko’zdan kechirish.		
2.Motivatsiya	10	2.1.Mashg’ulot mavzusi, maqsadi, kutilayotgan natijalarni bayon qilish (1-Slayd).	Tajriba Aqliy hujum	Slayd Qog’oz,

		2.2.Talabalarni faollashtirishga oid savol qo’yiladi, javob yozish uchun qog’oz kartochkalar tarqatiladi, vaqt belgilanadi va javoblar yig’ib olinadi. Javoblar muhokama qilinmaydi (2-Slayd).		kartochkalar
3.Yangi mavzu bayoni	50	Talabalarga mavzu bo’yicha umumiy ma`lumot, tushunchalar beriladi va tayyor dasturiy vositalar orqali.	Tajriba nazariy qismi	Kompyuter, proektor slayd, animatsion tasvirli Virtual ko’rgazma
4.Talabalar bilimini baholash	10	4.1.Har bir talabaga FSMU varaqaralarini tarqatadi. Yakka tartibdagi ish tugagach talabalar kichik guruhlarga bo’linadi va har bir guruhga vazifalar topshiriladi (FSMU texnologiyasi, 3-Slayd). Tayyorlangan javoblar tinglanadi va muhokama qilinadi.	Kichik guruhlarda ishlash	Kartoteka
5.Yakuniy qism	5	5.1.O’qituvchi kichik guruhlarda bajarilgan ishlar bo’yicha fikrlarni umumlashtiradi.Barcha guruhlarni baholaydi, mashg’ulot bo’yicha talabalarning fikrlarini tinglaydi. 5.2. Uyga topshiriq beriladi (4-Slayd).	Muhokama Nazorat savollari	Doska, bo’r. Slayd

1 – Slayd

MAVZU: KOMPYUTER TARMOG'IDA INFORMATSIYA HIMOYASI

Kompyuter tarmoqlarida uchraydigan hujumlar

AirSlax OT dasturlar to'plami yordamida Wi-Fi tarmog'i xavfsizligini tekshirish

2 – Slayd

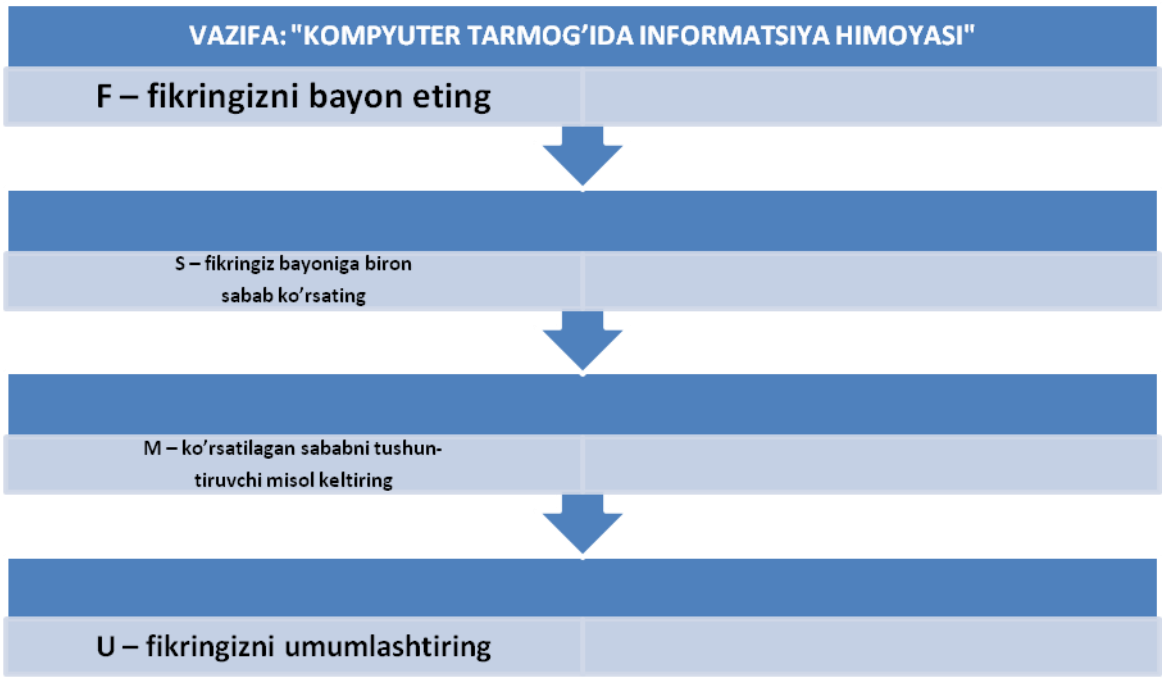
Aqliy hujum

1. Qanaqa tarmoq hujumlarini bilasiz?

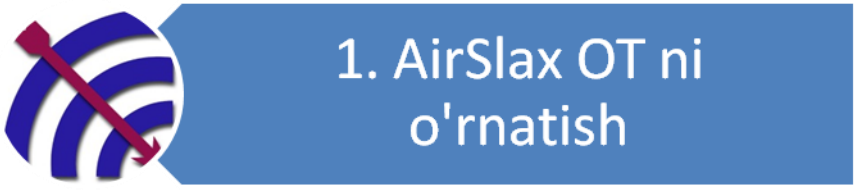
2. Qanday vositalardan foydalanib bu hujumlarni amalga oshirib bo`ladi?

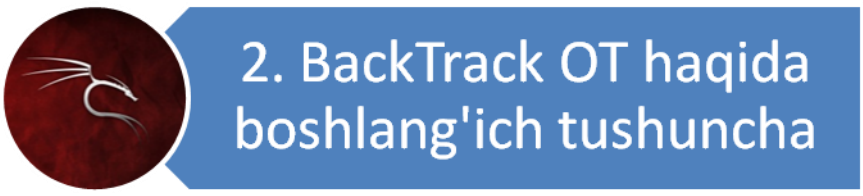
3 – Slayd

F S M U texnologiyasi



4 – Slayd





Hayot Faoliyati Xavfsizligi

1. Kompyuter xonasiga qo'yiladigan talablar

Xonani shifti oq ko'k fon bilan oqlanishi va devorlari esa yashil rangga oqlanishi kerak. Bu ranglar bizga yaxshi rang iqlimini yaratib beradi. Xonalarga qo'yilgan talablar ishchi muhit, ishchining (operator) ish joyi, tashqi muhit faktorlari yig'indisi bo'lib ular quyidagi ishlardan iborat: fizik, ximik, biologik, axborot, sotsial - psixologik va estetik faktorlar tashqi muhit xossalari bo'lib operatorga ta`sir etadi. Ishchi muhit turlicha bo'lishi mumkin: ish joyida hayot faoliyatini ta`minlovchi vositalar operatorning talab etilgan mehnat qobiliyati sharoitini hosil qiladi va uni noxush faktorlar ta`siridan himoya qiladi.

Xodimlar samarali faoliyat ko'rsatishi uchun sharoit yaratish va texnik vositalarni ishlash uchun xonalar yorug', toza, tovush va tebranishdan izolyatsiyalangan holatda loyihalanadi. Shkaf va devorlar tovush yutuvchi plitkalar bilan qoplanishi maqsadga muvofiqdir. Xona harorati optimal haroratda 21-23°S da, optimal namlik 40-60 %, chang kontsentratsiyasi 0,2 mg/m3 dan va chang maksimal zarracha o'lchash 3 mk dan oshmasligi lozim. Xonalarda bunday sharoitni ushlab turish maqsadida, xonalarni havo almashtirib turish ko'zda tutiladi.

2. Operatorning ishchi joyini tashkil etish

Operatorning komfort ishlashiga operatorning ish joyini tashkil etilganligi, axborotning ko'rsatish manbai va mashinaning boshqarish organlari ta`sir ko'rsatadi. Ular shovqin chiqarmasligi va ish jarayonida diskomfort hisini uyg'otmasligi, inson uchun maksimal qulay bo'lishi kerak. EHM operatori komfort sharoit bilan ta`minlashning asosiy yo'li uni ishchi joyini tashkilash kiradi. Bunda har narsaga e`tibor berishi kerak ko'zga ko'rinmagan kichkina narsa ham uzoq vaqt davomidagi jarayondan keyin diskomfort keltirib chiqarishi mumkin va kasalliklarga olib kelishi mumkin .

Operatorning uzoq vaqt davomida monitor ortida o'tirishi natijasida ko'rish apparatining zo'riqishi, ishdan qoniqmaslik, bosh og'rig'i, buzilishi charchoq va ko'z, bo'yin, bel, qo'larda og'riqlar sezila boshlanadi. EHM operatorining ish joyi deyilganda texnik manbalar va yordamchi qurilmalar bilan jihozlangan konkret ishlab chiqarish masalarni yechishga mo'ljalangan "operator - odam" ish faoliyati bilan shug'ulanadigan hudud tushiniladi. Ish joyni mehnat xavfsizligi qoidalari va standartlar talablariga mos ravishda jihozlash kerak. Uskunaning tashqi va konstruktiv ko'rinishini jihozlash minimal charchash uchun sharoit yaratadi.

Ish mebelining konstruktsiyasi GOST 12.2.032-78(9), GOST 2226976(10) talablariga mos tushuvchi ishchining bo'yiga qarab sozlanadigan va qulay ozoda turadigan bo'lishi kerak. Operatorning ish joyini to'g'ri tashkil etilganida uning mehnat unumdorligi 8-20% oshadi.

Kompyuter o'rnatiladigan xonaga kompyuter soniga qarab turib quyidagi talablar qo'yiladi: axborotlashtirish, bu tinglovchilarni yoki ishlovchilarning kompyuterda nazariy va amaliy mashg'ulotlar o'tkazish bilan bajariladi. Shuning uchun kompyuter xonasida 2 tadan 5 tagacha kompyuter o'rnatilishi mumkin va shu bilan birga kompyuter xonasini o'lchamlari quyidagicha bo'lishi kerak (3x6x2,8 m).

3. Ish joyining yoritilganligi

Ish joyini loyihalash vaqtida su`niy va tabiiy yoritish masalasi hal qilinishi kerak. Yoritish nafaqat ishlab chiqarish masalarini hal qilish balki u ishlayotgan odamning psixologik hamda fizik holatiga ta'sir ko'rsatadi. Ishlab chiqarish joylaridagi ratsional yoritganlikka qo'yilgan talablar:

- yorug'lik manbai va yoritish tizimini to'g'ri tanlash;
- ishlab chiqarish tepaliklarini kerakli darajadagi yorug'lik darajasi bilan ta`minlash;
- ko'zni oladigan yorug'likni cheklash;
- o'liklarni yo'qotish, tekis yorug'likni tashkilash;
- yorug'lik oqimining vaqtga nisbatan tebranishini yo'qotish yoki cheklash.

Kerakli darajadagi yoritilmaganlik oqibatida va ko'rish holatining zo'riqishida bajarilyotgan ish davomida ko'zning charchashi kuchayadi, umumiy ishlashi va ishlab chiqarish unumdorligi tushib ketadi va xatolar soni ko'payadi. Ish joyidagi yoritganlik gigienik talablarga binioan mehnatning ko'rish sharoitlariga to'g'ri kelishi kerak. GOST 12.01.006-84 (11) ga binoan displey bilan ishlash vaqtida yoritilganlik 200lk hujjatlar bilan ishlash paytida 400lk bo'lishi kerak.

Tarqatilgan yoritishdan, shiftlarning, devorlarning, uskunalarning och ranglarga bo'yash qo'laniladi. Operatorning ko'rish maydonida yorug'lik maydoni bo'lsa to'g'ri yaltirash, ko'rish maydoni ichida qaytaradigan yorug'lik tekisliklari mavjud bo'lsa qaytaruvchi yaltirash deyiladi. To'g'ri yaltirashni ko'rish maydonidan yarqilagan yorug'likni 60 sm kamaytirish yo'li bilan kamaytirish mumkin. Qaytaruvchi yaltirashdan esa yorug'likni tarqatuvchi manbalar hamda polirovka qilingan tekisliklar o'rniga matoviy ishlatish yo'li bilan kamaytirish mumkin. Ekran monitoridagi bliklarni kamaytirish uchun tasvirni konrastligini kuchaytiruvchi va bliklarni kamaytirtiruvchi ekran filtrlaridan foydalanish kerak yoki antiblik

qoplamasi mavjud monitorlardan foydalanish zarur . Yorug'likni turini tanlash muhim masala hisoblanadi (tabiiy yoki su`niy). Tabiiy yorug'likdan foydalanish ko'p kamchiliklarga ega:

- yorug'lik tushishi faqat bir tomondan;
- yorug'likni vaqtda va hajmda bir xil bo'lmaganligi;
- ravshan quyosh nurlarining ko'zni olishi va boshqalar.

Su`niy yorug'likdan foydalanish yuqoridagi kamchiliklarni bartaraf etadi va optimal yorug'lik rejimini yaratishga yordam beradi. Lekin oynalarsiz inshotlardan foydalanish insonlarda o'ziga ishonchsizlikva uyaluvchanlikni keltirib chiqaradi. To'g'ri yorug'lik uzatishni tashkil etish uchun quyosh nurlariga yaqin su`niy yorug'likni tanlash kerak.

4. Stol va stullarning joylashuviga bo'lgan talablar

Kompyuter xonasida stol va stulllarga talablar mavjud bo'lib, stol balandligi yerdan 68-77 sm, stullar esa aylanuvchan bo'lishi kerak va orqasida suyanchig'i bo'lishi kerak. Chunki stol stullar o'z gabariti bilan to'g'ri kelmasa foydalanuvchi tezda charchab qoladi. Stol va stullar shunday joylashtirilishi kerakki, ular insonlarga turib yurishga xalaqit bermasligi kerak. Bundan tashqari, operatorlar bemalol har bir operatorlar oldiga borib birga ishlay olishi kerak. Ish joyining konstruktivigi va elemenlarining joylashinuvi (o'tirg'ichlar, axborotning ko'rsatish, boshqarish organlari) antropometrik, fiziologik va psixologik talablarga hamda ishning xarakteriga to'g'ri kelishi kerak.

Shunday konstruktsiyalangan ish joyi monitor maydonidan tashqaridagi bajarilishi qiyin bo'lgan operatsiyalarni bajarish imkonini beradi. Axborotning ko'rsatish manbalari bu holda EHM ning displeyi SNIP 2.01.02-85 (5) ga to'g'ri keladi.

Ko'zga tushayotgan nagruzkani kamaytirish uchun displey ergonomika nuqtai nazaridan optimal o'rnatilishi kerak, displeyning tepa burchagi ko'z bilan bir tekislikda bo'lishi kerak, ekrangacha masofa 28-60 sm bo'lishi kerak. Ekraning miltilashi mil>70 Gts bo'lishi kerak. Antropometrik mos tushishi operatorning ish borayotgan vaqtda fazoda, kenglikda tananing joylanishi imkoniyati va turli pozani egallashi nazarda tutiladi. Bu masalani hal qilish uchun birinchi navbatda boshqarish pul'ti asboblaridan operatorning oyog'i borib etadigan zona aniqlanadi.Bu mos kelishini ta`minlash qiyinchilik bilan erishiladi, chunki har bir kishining antropometrik ko'rsatkichlari turlicha.O'rta bo'yli kishini qoniqtirgan o'rindiq, baland yoki past bo'yli bo'lgan kishiga noqulay bo'lishi mumkin.

Xavfsiz faoliyat ko'rsatish maqsadida inson tanasi o'lchamlari quyidagi holatlarда hisobga olinadi:

- poldan yoki ish maydonidan, mashinalar ishlashini nazorat qilish, to'g'rilash zonasi, signalizatsiya va nazorat asboblariga bo'lgan sathni optimal balandligini o'lchashda;
- balandlikda qo'lda boshqariladigan mashinalar frontini joylashtirishda, ayniqsa avariya organlarining puxta joylashtirishda;
- boshqarish organlarini shakli va o'lchamlarini tanlashda.

Mashinalarni loyihalashda inson antropometrik ko'rsatgichlarni to'g'ri tanlash uchun o'zini topografiya qilish usuli yoki modellash usuli qo'llaniladi. O'zini topografiya qilishda inson ishchi tanasini turli holatlarini sxematik konstruktsiyalash va ishchi bajaradigan ishlar va operatsiyalar bilan bog'lash kiradi.

Modellash usuliga inson figurasini hajmiy va tekislikda modellash kiradi. Insonning antrapometrik quyidagicha: o'rtacha balandligi 1 metr 72 sm, yelka kengligi 39 sm, qo'llar yoyilmasi 160 sm agar bu antropometrik o'lchovlar hisobga olinmasa operatorlar ish paytida bir - biriga xalaqit berishi mumkin. Shuning uchun antropometrik o'lchovlarni hisobga olish katta ahamiyatga ega.

5. Monitordan insonning ko'zigacha bo'lgan optimal masofa

Monitor ko'zdan ozgina pastroqda va 50 sm dan kam bo'lmagan masofada joylashishi kerak. Monitor va ko'z orasidagi masofa 80 sm gacha bo'lishi tavsiya qilinadi, bu masofa kichik bo'lsa insonning ko'zi tez charchaydi. Monitorni dizayni va ranggi o'ziga e`tiborni jalb qilmasligi kerak. Shuning uchun monitorning sirt tomonida har xil reklama yopishtirgichlar bo'lmasligi kerak. Monitorning ekrani zangori va ko'k ranglarga bo'yalishi maqsadga muvofiq hisoblanadi. Chunki bu ranglar inson ko'ziga eng yaxshi ranglardan hisoblanadi.

Qisman monitor oldidagi o'tirishda xavfsizlikni va kamfort ish joyini ratsional tashkil etish lozim. Foydalanuvchi usul asosiy xavfsizlik vidiomanitor ekran displeydan chiqadi deb bo'lmaydi. Eng kuchli nurlanish odatda manitorni yon va orqa tomonidan ham tarqaladi. Shuning uchun foydalanuchi joyini bir necha kompyuter qarama - qarshi turgan joyda undan ham yomoni orqama - ketin joylashtirishdir.

Videomonitor xillari orasidagi tavsiya etiladigan oradagi masofa 2 m dan kam bo'lmasligi va yon tomondagi masofa 1,2 m dan kam bo'lmasligi lozim. Kompyuterlar joylashgan xona yetarli darajada keng va doimiy ravishda havosi almashib turishi kerak. Bitta displey uchun minimal standart norma 6m ni, minimal hajm esa 20 m tashkil etishi kerak.

Displey oldida ishlaganda xonani yoritilishi yaxshi bo'lishi va imkoni boricha tabiiy kunduzgi yoritilishga yaqin bo'lishi kerak. YOritish uchun displeyga yaqin

joylashgan lyuminitsent lampochkalardan foydalanib bo'lmaydi. Bu strobaktik effekt deb aytiladi, displey ekranda ma`lumotni buzilishiga olib keladi.

Yoritishni eng maqbul usuli galten nurlanishli manbadir. Amerikalik olimlarning ham foydalanuvchilarga tavsiyasi diqqatga loyiqdir:

- Displey ekraniga yaxshi himoya filtri o'rnatish, to'rli filtrlardan foydalanmang;
- Ekran o'z sathidan 20 sm pastda va ko'zdan 65 sm masofada bo'lishi kerak(agar shu yaqindan yoki ko'rsangiz ham displey bilan burningizni uning yaqiniga olib borib ishlamang, hatto burun ham zarar ko'rishi mumkin);
- Ekranni oynaga nisbatan to'g'ri burchak holida o'rnating;
- Ekranning yoritish xonasining yoritishiga teng bo'lishi kerak (taxminan 500-700 lk) yorqin lyumensent nurdan saqlanish;
- Yorqin fonda qora harflar oson o'qiladi;
- Har 10 minutda nigohni ekrandan boshqa tomonga oling;
- Chernovikdan ma`lumotni SHKga kiritishda uni ekran yaqinroq joyga qo'ying;
- Ko'zga displey yonida ishlaganda alohida ko'zoynak lozimligini ko'z doktori bilan gaplashib ko'ring. (masalan perforirovamniy oynak)

Barcha nurlantirishlarni yaxshi yutuvchi ayrim o'simliklar bor. Ular ko'pgina nurlanishlarda ular juda zo'r rivojlanadi. Shuning uchun ko'pgina ofislarda xonani bezash uchun emas, balki nuralanish kamaytirish uchun xona o'simliklardan foydalanishadi. Shuning uchun ushbu tavsiya kompyuterdan foydalanuvchilar uchun berish mumkin. Umuman xulosa shuki:

- Ekranni lippillashi va yarqirashi, yaqinda yomon ko'rish, asab stresslari va asabiylikka olib keladi.
- Past chastotali maydon nur kasalliklari, stresslar, homiladorlarni buzilishlar bilan o'tishga, reprodukov funktsional buzilishga va yomon sharoitli ishlar paydo bo'lishiga olib keladi.
- Elektron maydon hujjatlarini o'zgartirish va rivojlanishni to'xtatishga olib keladi. Bu ko'zning xuristalini xiralashish - katarakta keltirib chiqarish mumkin.

6. Kompyuter bilan ishlaganda charchash sabablari

Kompyuter bilan ishlash vaqtida inson quyidagi faktorlardan charchaydi:

- ekraning me`yoridan ortiq yorug'ligi;
- kontrast va fon o'rtasidagi aniqligi;
- kompyuterda ishlash paytidagi issiqlikdan nurlanishi;
- kompyuterda nurlanishning insonga ta`siri;
- kompyuter buzuqligi.

Kompyuterdan nurlanishning oldini olishi uchun himoya filtrlaridan foydalaniladi.Shunday qilib, monitor butunlay xalqaro standart MPR-2 (LOW radiation displeylari) talablarini qoniqtirganda ham, uni nurlanishda qo'shimcha himoya kerak bo'ladi.Bu to'g'risida takliflar juda ko'pdir. Amerikalik mutaxasislar, masalan, ekranda qo'l cho'zilgandagina bo'lgan masofada joylashishni maslahat beriladi, qo'shni monitorlar 222,8 masofada joylashishi lozim. Eng effektli (foydali) vosita rivojlangan dunyoda tan olingan ekran qismi filtrlaridir. Monitorlar uchun himoya filtrlari quyidagi turlarda bo'ladi.

1. Turli filtrlar - amalda elektromagnit nurlardan va statik elektrdan himoya qilmaydi, bundan tashqari sur`atning kontrastligini kamaytiradi. Lekin ular tashqi yorqinlikda va ekranni bikirlashidan himoya qiladi, bu ko'z uchun katta ahamiyatga egadir.

2. Plyonkali filtrlar statik elektrni to'smaydi past chastotali elektromagnit maydonidan deyarli himoya qilmaydi, lekin sur`atni talbaning konrastligini ortiradi, ul'trafiolet nurlanishlarni butunlay yutadi va rengen nurlarini kamytiradi. Yashindan faqat polerizatsiya plyonkali filtrlar himoya qiladi. Eng taniqlilisi Polorid firmasining plyonkali filtrlardir (SR 50): ularni ko'plari sur`atni kontrastligi va aniqliyligini oshiradi. Lekin haqiqatdan shuni ta`kidlash kerakki, polerizatsiya filtrlari poleefir simolalari ostida tayyorlanadi. Bu material yuqori darajada mustahkam emas va uzoqqa chidamaydi va tez fizik qorishish va tuzilishiga olib keladi.(Plyonka Polorid SR 50 filtrlarni universal ishlashini polerizatsiya filtrlari bilan chalkashtirib bo'lmaydi. Keyingi filtrlar ham statik va elektromagnit maydonlardan yomon himoya qilmaydi).

3. Shisha filtrlar eng keng tarqalgandir. Ularning bir necha modifikatsiyasi mavjuddir.

a) Oddiy shisha filtrlar, odatda osiyoda ishlab chiqilgan (Defender GL14V, Optical Class) o'zini effektivligi bilan taxminlangan turli fil`trlarga tengdir. Ularni ko'plari sifat sertifikati va boshqa hujjatlar bilan ta`minlanmaydi.

b) Erga ulagan shisha fil`trlar sezilarli darajada effektivdir: ular qisman statik zaryadni kamaytiradi, elektromagnit maydon, ul`trabinafsha nurlari kuchini kamaytiradi, sur`at kontrasitligini oshiradi. Bu filtrlar juda avtomatlashgandir.

v) To'liq himoyali shishali filtrlar (Ergoster Xenium Vnus) - odatda, yuqori sifatli mahsulotdir, optik oyna asosida ko'p qatlamli maxsus o'qlamalar bilan tayyorlangan, o'zida polirizatsiya fil`trni ham mujassam etgan. Bu fil`trlar ul'trafiolet nurlarini, statik maydonlarni bartaraf etadi ko'p darajada elektromagnit maydon va rentgen nurlanishlarini kamaytiradi. Suratda sakrashlar bo'lmaydi, suratni kontrastliligi oshadi, lekin bu filtrlar juda qimmatdir.

g) Rossiya federatsiyasida ishlab chiqilgan filtrlar shishali filtrlar (Global Shield va Defended Argon filtrlari) ular ham to'la himoya sinfiga mansub. O'zini xarakteristikasi bilan xorijiy filtr namunalardan qolishmaydi, 2-3 marotaba arzon, nisbatan yangi filtrlar ularni sifati ko'pgina texnik xulosalar va sertifikatlar bilan tasdiqlangan, ular mehnat printsipi past ITI testdan o'tkazilgan, shvetsil nurlanishdan himoya va ko'rsatkich vositalari ergonomikasi ITU dan ham sinovda o'tkazilgan rejim Davlat Standarti sertifikati va gigiena sertifikatiga ega.

Kompyuter xonasida hamma jihozlar elektr tokida ishlaydi.Shuning uchun elektrdan shikastlanishiga uchrash mumkin.Buning oldini olish uchun kompyuterlarni erga ulash talablariga amal qilish shart.

Hamma kompyuterlarda elektr tarmog'iga ulash uchun maxsus sistema ishlatiladi va unda "0" ulash himoyasi qo'llanilgan. "0" ga ulash himoyasi bu "0" simini korpuslarga bog'lash va har xil issiqlikda ishlaydigan avtomatlarni ishga tushiruvchi sistemadir. Himoyalovchi erga ulash qurilmalari 2 xil:

1. Konturli yerga ulash;

2. Tashqariga chiqarilgan yerga ulash - bu usul ko'pincha ulovchi asbob - uskunalar turgan joydan tashqariga chiqarib ma`lum bir maydonchaga to'planib o'rnatiladi. Yerga ulashning bu turi asosan kuchlanishi 1000 V gacha bo'lgan qurilmalarda ishlatiladi.Buning afzalligi shundaki, elektrod vazifasini bajaruvchi qoziqlarni erga qoqish uchun qarshiligi kam bo'lgan erlarni tanlash imkoni bor.

Elektr tokining inson organizmiga ta`siri

Elektr tokidan inson organizimidan termik (ya`ni issiqlik), elektrolitik va biologik ta`sir ko'rsatiladi. Elektr tokining termik ta`siri inson tanasining ba`zi joylarida kuyish, qon tomirlari, nerv va xujayralarning qizishi sifatida kuzatiladi. Elektrolitik ta`sir esa, qon tarkibidagi yoki xujayralar tarkibidagi tuzalrning parchalanishi natijasida qonning fizik va kimyoviy xususiyatlarining o'zgari shiga olib keladigan holat tushuniladi. Bunda elektir toki markaziy asab tizimi va yurak-qon tizimni kesib o'tmasdan tananing ba`zi bir qisimlarigagina ta`sir ko'rsatishi mumkin.

Elektr tokining biologik ta`siri - bu tirik organizm uchun xos bo'lgan xususiyat xisoblanadi. Bu ta`sir natijasida muskullarning keskin qisqarishi tufayli

inson organizmidagi tirik xujayralar to'lqinlanadi, bunda asosan organizimdagi bioelektrik jarayon buziladi. Ya`ni inson organizmi asosan bioelektrik toklar yordamida boshqariladi. Bunga tashqi muhitdan yuqori kuchlanishdagi elektr tokining ta`siri natijasida biotoklar rejimi buziladi va oqibatda inson organizmida tok urish holati vujudga keladi. Ya`ni boshqarilmay qolgan organizmda hayot faoliyatining ba`zi bir funktsiyalari boshqarilmay qoladi: nafas olishning yomonlashuvi, qon aylanish tizimining ishlamay qolishi va x.k.

Elektr tokining inson organizmiga ta`sirining xilma xilligidan kelib chiqib, uni ikki gurupaga bo'lib qarash mumkin: mahalliy elektr ta`siri va tok urish.

Mahalliy elektr ta`siri - kuyib qolish, elektr belgilari hosil bo'lishi, terining metallashib qolishi hollaridir. Elektr ta`qsirida kuyish asosan organizim bilan elektr o'tkazgichi o'rtasida volta yoyi hosil bo'lganda sodir bo'ladi. Elektr o'tkazgichdagi kuchlanishning ta`siriga qarab bunday kuyish turlicha bo'lishi mumkin. Yengil kuyish faqat yallig'lanish bilan chegaralanadi, o'rtacha og'irlikdagi kuyishda pufakchalar hosil bo'ladi va og'ir kuyishda xujayra va terilar ko'mirga aylanib, og'ir asoratlarga olib kelishi mumkin. Elektr belgilari - bu terining ustki qismida aniq kulrang yoki och sarg'ish rangli 1-5 mm diametrdagi belgi paydo bo'lishi bilan ifodalanadi.Bunday belgilar odatda xavfli emas. Terining metallashib qolishida, odatda erib mayda zarrachalarga parchalanib ketgan metal teri ichiga kirib qoladi. Bu holat ham elektr yoyi hosil bo'lganda ro'y beradi. Ma`lum vaqt o'tgandan keyin bu teri ko'chib tushib ketadi va hech qanday asorat qoldirmaydi.

Elektr urishi (yoki tok urushi ham deb yuritiladi) to'rt darajaga bo'lib qaraladi.

1. muskullar keskin qisqarishi natijasida odam tok ta`sirida chiqib ketadi va xushini yo'qotmaydi.
2. muskullar keskin qisqarishi natijasida odam xushini yo'qotadi, ammo yurak va nafas olish faoliyati ishalb turadi.
3. xushini yo'qotib nafas olish tizim yoki yurak urishi to'xtab qoladi.
4. klinik o'lim holati, bunda insonda hech qanday hayot alomatlari ko'rinmay qoladi.

Klinik o'lim holati bu hayot bilan o'lim oralig'i bo'lib, ma`lum vaqtgacha inson ichki imkoniyatlar xisobiga yashab turadi. Bu vaqtda unda hayot belgilari: ya`ni nafas olish, qon aylanish bo'lmaydi, tashqi ta`sirlarga farqsiz bo'ladi, og'riq sezmaydi, ko'z qorachig'i kengayadi va yorug'likni sezmaydi. Ammo bu davrda qali undagi hayot butunlay so'nmagan, xujayralarda ma`lum modda almashinuv jarayonlari davom etadi va bu organizmning minimal hayot faoliyatini davom ettirishiga etarli bo'ladi. SHuning uchun tashqi ta`sir natijasida hayot faoliyatini yo'qotgan organizmning ba`zi bir qisimlarini tiklash natijasida uni hayotga

qaytarish imkoniyati bor. Klinik o'lim holati 5-8 minut davom etadi. Hech qanday yordam bo'lmagan takdirda eng oldin bosh miya qobigadagi xujayralar parchalanadi va klinik o'lim holati biologik o'lim holatiga o'tadi.Biologik o'lim-qaytarib bo'lmaydigan jarayon bo'lib, organizmdagi biologik jarayonlar butunlay to'xtashi bilan xarakterlanadi, shuningdek, organizmdaga oqsil parchalanadi. Bu klinik o'lim vaqti tugagandan keyin ro'y beradi.Tokning inson organizmiga ta`siri bir necha omillarga bog'liq. Asosiy omillardan biri insonga tok ta`sirining davomliligi, ya`ni odam tok ta`sirida qancha ko'p qolib ketsa, u shuncha ko'p zararlanadi. Ikkinchi omil sifatida odam organizmining shaxsiy xususiyatlari va shuningdek, tokning turi va chastotasi katta rol' o'ynaydi.

Inson organizmining tok ta`siriga ma`lum qarshiligi, shuningdek tokning kuchlanishi ma`lum ta`sir darajasini belgalaydi, chunki inson organizmining qarshiligi o'zgarmagan holda, kuchlanish ko'payishi natijasida organizmdan oqib o'tgan tok mikdori oshib ketadi. Inson organizmining qarshiligi teri qarshiligi va ichki organlar qarshiliklari yig'indisi sifatida olinadi.

Teri, asosan quruq va o'lik xujayralarning qattiq qatlamlaridan tashkil topganliga sababli katta qarshilikka ega va u umuman inson organizmining qarshiligani ifodalaydi. Organizm ichki organlarining qarshiligi uncha katta emas. Odamning quruq,zararlanmagan terisi 2.000 dan 20.000 Om gacha va undan yuqori qarshilikka ega bo'lgani holda, namlangan, zararlangan teri qarshiliga 40-5000 Om qarshilikka ega bo'ladi va bu qarshilik inson ichki a`zolari qarshiligiga teng hisoblanadi. Aytilganlarni hisobga olgan holda umuman texnik hisoblar uchun inson organizmi qarshiligi 1000 Om deb qabul qilingan.

Inson organizmi orqali oqib o'tgan tokning mikdori uning asoratini belgalaydi, ya`ni oqib o'tgan tok qancha katta bo'lsa, uning asorati ham shuncha katta bo'ladi. Inson organizmi orqali 50 Gts li sanoat elektr tokining 0,6-1,5 mA oqib o'tsa, buni u sezadi va bu mikdordagi tok sezish chegarasidagi elektr toki deb ataladi. Agar inson organizmidan oqib o'tgan tokning mikdori 10-15 mA ga etsa, unda organizmdagi muskullar tartibsiz qisqarib, inson o'z organizmi qismlarini boshqarish qobiliyatidan mahrum bo'ladi, ya`ni, elektr toki bo'lgan simni ushlab turgan bo'lsa, panjalarini ocha olmaydi, shuningdek unga ta`sir ko'rsatayotgan elektr simini olib tashlay olmaydi. Bunday tok chegara mikdordagi ushlab qoluvchi tok deyiladi.Tok miqdori 25-50 mA ga etsa, unda tok ta`siri ko'krak qafasiga ta`sir ko'rsatadi, buning natijasida nafas olish qiyinlashadi. Tok ta`siri uzoq vaqt davom etsa, ya`ni bir necha minutga cho'zilsa, unda nafas olishning to'xtab qolishi natijasida odam o'lishi mumkin. Tok miqdori 100 mA va undan ortiq bo'lsa, bunday tok yurak muskullariga ta`sir ko'rsatadi va yurakning ishlash ritmi buziladi, natijada qon aylanish tizimi butunlay ishdan chiqadi va bu holat ham o'limga olib keladi.

Inson organizmi orqali oqib o'tgan tokning davomliligi ham alohida

ahamiyatga ega, chunki tok ta`siri uzoq davom etsa, unda inson organizmining tok o'tkazuvchanligi orta boradi va tokning zararli ta`siri organizmda yig'ila borishi natijasida asorat og'irlasha boradi. Tokning turi va chastotasi ham zararli ta`sir ko'rsatishda muhim rol' o'ynaydi. Eng zararli tok 20-100 Gts atrofidagi elektr toki hisoblanadi. CHastotasi 20 Gts dan kichik va 100 Gts dan katta toklarning ta`sir darajasi kamayadi. Katta chastotadagi elektr toklarida tok urish bo'lmaydi, lekin kuydirishi mumkin. Agar tok o'zgarmas bo'lsa, unda tokning sezish chegarasidagi mikdori 6-7 mA, ushlab qoluvchi chegara miqdori 50-70 mA, 0,5 s davomida yurak faoliyatini ishdan chiqarishi mumkin bo'lgan mikdori 300 mA gacha ortadi.

Elektr toki ta`siriga tushgan kishiga birinchi tibbiy yordam ko'rsatish

Elektr toki ta`siriga tushgan kishiga tibbiyot xodimi kelgunga qadar ko'rsatiladigan yordamni ikki qismga bo'lib qaraladi: tok ta`siridan qutqazish va birinchi yordam ko'rsatish.

Tok ta`siridan qutqazish o'z navbatida bir necha xil bo'lishi mumkin.eng oson va qulay usuli bu elektr qurilmasining o'sha qismiga kelayotgan tokni o'chirishdir.

Agar buning iloji bo'lmasa (masalan, o'chirish qurilmasi uzoqda bo'lsa), unda tok kuchlanishi 1000 B dan ko'p bo'lmagan elektr qurilmalarida elektr simlarini sopi yog'ochli bo'lgan boltalar bilan kesish yoki zararlangan kishining kiyimi quruq bo'lsa, uning kiyimidan tortib tok ta`siridai qutqazib qolish mumkin.

Agar elektr tokining kuchlanishi 1000 V dan ortiq bo'lsa, unda dielektrik qo'lqop va elektr izolyatsiyasi mustahkam bo'lgan elektr asboblaridan foydalanish kerak.

Elektr ta`siriga tushgan kishiga birinchi yordam ko'rsatish, uning holatiga qarab belgilanadi.Agar ta`sirlangan kishi hushini yo'qotmagan bo'lsa, uning tinchlantirib, vrach kelishini kutish yoki uni tezda davolash muassasasiga olib borish zarur. Agar tok ta`sirida xushini yo'qotgan ammo nafas olishi va yurak tizimi ishlayotgan bo'lsa, unda uni quruq va qulay joyga yotqizish, kamari va yoqasini bo'shatish va sof havo kelishni ta`minlash zarur.

Nashatir spirti hidlatish, yuziga suv purkash, tanasini va qo'llarini ishqalash yaxshi natija beradi. Agar jarohatlangan kishining nafas olishi qiyinlashsa, qaltirash holati bo'lsa, ammo yurak urish ritmi nisbatan yaxshi bo'lsa, unda bu kishiga sun`iy nafas oldirish ishlarini bajarish zarur.

Klinik o'lim holati yuz bergan taqdirda sun`iy nafas berish bilan bir qatorda yurakni ustki tomondan massaj qilish kerak.

Sun`iy nafas berish jarohatlangan kishini tok ta`siridan qutqazib olish, uning holatini anikdash bilanoq boshlanishi kerak. Sun`iy nafas berish "og'izdan og'izga" deb ataluvchi usul bilan, ya`ni yordam ko'rsatuvchi kishi o'z o'pkasini havoga to'ldirib, jarohatlangan kishi og'zi orqali uning o'pkasiga bu havoni haydaydi. Odam o'pkasidan chiqqan havo, ikkinchi odam o'pkasi ishlashi uchun etarli midorda kislorodga ega bo'lishi aniklangan.Bu usulda jarohatlangan kishi chalqancha yotqiziladi, og'zini ochib begona narsalardan tozalanadi.havo o'tish yo'lini ochish uchun boshini bir yo'li bilan peshona aralash ko'tariladi, ikkinchi yo'l bilan dahanidan tortib, dahanini bo'yni bilan taxminan bir chiziqqa keltiriladi. Shundan keyin ko'krak qafasini to'ldirib nafas olib, kuch bilan bu havoni jarohatlangan kishi og'zi orqali puflanadi. Bunda yordam ko'rsatayotgan kishi og'zi bilan, jarohatlangan kishining og'zini butunlay berkitishi va yuzi yoki panjalari yordamida uning burnini berkitish kerak.

Shundan keyin yordam ko'rsatuvchi boshini ko'tarib yana o'pkasini havoga to'ldiradi. Bu vaqtda jarohatlangan kishi passiv ravishda nafas chiqazadi. Bir minutda taxminan 10-12 marta puflashni doka, dastro'mol va trubka orqali ham bajarish mumkin. Agar jarohatlangan kishi mustaqil nafas olishini tiklagan taqdirda ham, sun`iy nafas oldirishni uning nafas olishiga bemor o'ziga kelguncha davom ettiriladi.

XULOSA

Mening bitiruv malakaviy ishim mavzusi ““Axborot xavfsizligining usul va vositalari” fanidan “Kompyuter tarmog’ida informatsiya himoyasi” moduli bo’yicha laboratoriya ishlarini bajarish uchun elektron qo’llanma” yaratish deb nomlanadi.

Kompyuter tarmoqlarida axborot xavfsizligini ta’minlash har doim ham eng asosiy va muhim vazifalardan bo’lib qolaveradi. Har qanday yangi shifrlash algoritmari yoki himoya vositalari ishlab chiqilmasin, ular hech qachon 100% himoyani ta’minlay olishmaydi.Information tarmoqlarsiz esa hozirgi hayotni tasavvur qilib bo’lmaydi.

Xulosa qiladigan bo’lsak, biz tarmoq yaratilishining asosiy tushunchalari, masalan OSI modeli, va ushbu modelning turli darajalaridagi tarmoq himoyasining boshlang’ich tushunchalari bilan tanishib o’tdik. Har bir protokol, algoritm va metodlarning kamchilik va yutuqlari, afzallik jihatlari, tasviya etiladigan qo’llanish sohalari, ularni kombinatsiyalashda to’gri tanlovni amalga oshirish, qo’shimcha xususiyat va parametrlari ko’rib chiqildi.

Amaliy misol tariqasida simsiz tarmoqlarda parolni topish orqali tarmoq xavfsizlik darajasini tekshirish ishlari olib borildi.

Elektron qo`llanmadakompyuter tarmoqlari ish tamoyili va ularda uchraydigan hujumlarni bartaraf etish usullarini tushunarli va sodda ifodalangan. Elektron qo`llanmani yaratishda AirSlax OT va Ethereal paketlar to’plamidan ko’proq foydalandim. Elektron qo`llanmani nafaqat nazariy ma`lumot, balki undan interaktiv ravishda darsda foydalaniladigan qilib yaratdim. Ushbu elektron qo`llanmani ma`lumotlarni faqat talaba emas, balki ixtiyoriy o’qituvchi hamda dasturchi foydalanish imkoniyatiga ega bo’lishini ta`minlashni o’z oldimga maqsad qilib qo’ydim va bu maqsadimga erishdim.

Yaratilgan elektron qo`llanmadan ta`lim jarayonida ma`lumotnoma dasturi sifatida ham foydalansa bo’ladi. Hozircha bu elektron qo`llanma ushbu sohada yaratgan ilk ishim bo’lib, keyinchalik bunaqa elektron qo`llanmalarni yanada rivojlantirib Respublikamizning turli kasb-hunar kollejlari, akademik litsey va oliy o’quv yurtlarida foydalanishlari uchun ham yaratish niyatidaman.

KIRISH

					Bitiruvmalakaviyish			
					“Axborotxavfsizligiiningusulvavositalari” fanidan “Kompyutertarmog’idainformatsiyahimoyasi” modulibo’yichalaboratoriyaishlarinibajarishuchunelektronqo’llanmayaratish			
		FIO	Imzo	Sana				
Bitiruvchi		Ibragimov N.						
Rahbar		Ibragimov U.						
Maslah.						Varaq №	Varaqlar	
						BMTI		
Kaf.m.		Razzoqov Sh.						

IBOB

«Nazariy qism»

					Bitiruvmalakaviyish			
					“Axborotxavfsizligiiningusulvavositalari” fanidan “Kompyutertarmog’idainformatsiyahimoyasi” modulibo’yichalaboratoriyaishlarinibajarishuchunelektronqo’llanmayaratish			
		FIO	Imzo	Sana				
Bitiruvchi		Ibragimov N.						
Rahbar		Ibragimov U.						
Maslah.						Varaq №	Varaqlar	
						BMTI		
Kaf.m.		Razzoqov Sh.						

IIBOB

«Asosiy qism»

					Bitiruvmalakaviyish			
					“Axborotxavfsizligiiningusulvavositalari” fanidan “Kompyutertarmog’idainformatsiyahimoyasi” modulibo’yichalaboratoriyaishlarinibajarishuchunelektronqo’llanmayaratish			
		FIO	Imzo	Sana				
Bitiruvchi		Ibragimov N.						
Rahbar		Ibragimov U.						
Maslah.						Varaq №	Varaqlar	
						BMTI		
Kaf.m.		Razzoqov Sh.						

IIIBOB

«Hayot faoliyati xavfsizligi»

					Bitiruvmalakaviyish			
					“Axborotxavfsizligiiningusulvavositalari” fanidan “Kompyutertarmog’idainformatsiyahimoyasi” modulibo’yichalaboratoriyaishlarinibajarishuchunelektronqo’llanmayaratish			
		FIO	Imzo	Sana				
Bitiruvchi		Ibragimov N.						
Rahbar		Ibragimov U.						
Maslah.						Varaq №	Varaqlar	
Kaf.m.		Razzoqov Sh.						

BMTI

XULOSA

					Bitiruvmalakaviyish			
					“Axborotxavfsizligiiningusulvavositalari” fanidan “Kompyutertarmog’idainformatsiyahimoyasi” modulibo’yichalaboratoriyaishlarinibajarishuchunelektronqo’llanmayaratish			
		FIO	Imzo	Sana				
Bitiruvchi		Ibragimov N.						
Rahbar		Ibragimov U.						
Maslah.						Varaq №	Varaqlar	
						BMTI		
Kaf.m.		Razzoqov Sh.						

ILOVA

					Bitiruvmalakaviyish			
					“Axborotxavfsizligiiningusulvavositalari” fanidan “Kompyutertarmog’idainformatsiyahimoyasi” modulibo’yichalaboratoriyaishlarinibajarishuchunelektronqo’llanmayaratish			
		FIO	Imzo	Sana				
Bitiruvchi		Ibragimov N.						
Rahbar		Ibragimov U.						
Maslah.						Varaq №	Varaqlar	
						BMTI		
Kaf.m.		Razzoqov Sh.						

FOYDALANILGAN ADABIYOTLAR

					Bitiruvmalakaviyish			
					“Axborotxavfsizligiiningusulvavositalari” fanidan “Kompyutertarmog’idainformatsiyahimoyasi” modulibo’yichalaboratoriyaishlarinibajarishuchunelektronqo’llanmayaratish			
		FIO	Imzo	Sana				
Bitiruvchi		Ibragimov N.						
Rahbar		Ibragimov U.						
Maslah.						Varaq №	Varaqlar	
						BMTI		
Kaf.m.		Razzoqov Sh.						