O’ZBEKISTON ALOQA VA AXBOROTLASHTIRISH AGENTLIGI

TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI FARG’ONA FILIALI

“Telekommunikatsiya” kafedrasi

“Kompyuter tizimlari va tarmoqlari” fanidan 5521900 «AT», 5140900 «KT », 5522200 «TK», 5811200 «S» bakalavriat ta`lim yo’nalishlari talabalariga amaliy mashg’ulotlar uchun

Uslubiy qo’llanma

Farg’ona 2009

“Kompyuter tizimlari va tarmoqlari” fanidan
5521900 «AT», 5140900 «KT », 5522200 «TK», 5811200 «S» bakalavriat ta`lim yo’nalishlari talabalariga amaliy mashg’ulotlar ucun

Uslubiy qo’llanma

Kafedra uslubiy seminarida tasdiqlangan

Bayon « 26 » avgust 2009 y.

Tuzuvchilar : katta o’qituvchi Jo’raev N.
asistent Rayimjonova O.
Mulaydinov F.

Mas`ul muxarrir: dots. Polvonov F.Yu.

So’z boshi

Ushbu o’quv qo’llanmasi 5521900 «AT», 5140900 «KT », 5522200 «TK», 5811200 «S» bakalavriat ta`lim yo’nalishlari talabalariga **“Kompyuter tizimlari va tarmoqlari ”** fanidan amaliy mashg’ulotlarni bajarish uchun mo’ljallangan bo’lib, “Kompyuter tizimlari va tarmoqlari” sohasida kerak bo’ladigan zarur bilimlarni o’z ichiga oladi. Bu qo’llanmani o’rgangandan so’ng talabalar quyidagi bilimlarga ega bo’ladilar :

Kompyuterlarni elektr tarmoq manbalariga ulash, viruslar haqida tushuncha va ularni bartaraf etish usullari, mahalliy tarmoq qurilmalari, kriptografik tizimlar, lokal va periferiya shinalari, WWW da ishlash tamoyillari va OSI modeli haqida ma`lumotlarga ega bo’ladilar.

“Kompyuter tizimlari va tarmoqlari” fanidan amaliy mashg’ulotlar mavzulari

1. Kompyuterni elektr tarmoq manbaiga ulash. Uzluksiz ta`minot manbalarining tiplari va ishlash printsiplari.

2. Viruslarning kompyuter ishiga salbiy ta`siri, viruslarni aniqlash va yo’q qilish uchun dasturlar, dastur detektorlar.

3. Tashqi qurilmalarni bevosita mahalliy tarmoqqa ulash va nosozlarini almashtirish jarayoni.

4. Kompyuter tarmoqlari havfsizligini ta`minlash: kriptografik tizimlar, mahfiy kalitlar, parol.

5. Lokal va periferiya shinalari. Periferiya shinalarining zamonaviy texnologiyada tutgan o’rni, Plug&Play texnologiyasining ahamiyati.

6. World Wide Web da ishlash va uning asosiy kontseptsiyalari. Gipermatn va gipermedia.

7. OSI modeli va uning sathlari. IEEE 802.x standartining tuzilishi va tarkibi.

Amaliy ish №1

Mavzu: Kompyuterni elektr tarmoq manbaiga ulash. Uzluksiz ta`minot manbalarining tiplari va ishlash printsiplari.

Ishdan maqsad: *Kompyuterni elektr tarmoq manbaiga ulash. Tarmoq filtrlari va uzluksiz ta`minot manbalari orqali ulashni o'rganish. Uzluksiz ta`minot manbalarining tiplari va ishlash printsiplarini amalda qo'llash.*

I. Nazariy qism.

Kompyuterni elektr tarmog'iga ulash

Kompyuterni ishonchli va beto'xtov ishlashi uchun uni turli xil kutilmagan tasodiflardan himoya qiluvchi, uning elektr tarmog'idan ta`minlanishini maxsus tizimini ko'zda tutish kerak. Bu kutilmagan tasodiflar, birinchi navbatda elektr ta`minoti parametrlarini standartdan turlicha chetga og'ishlaridir.

Texnik nuqtai nazardan, bu:

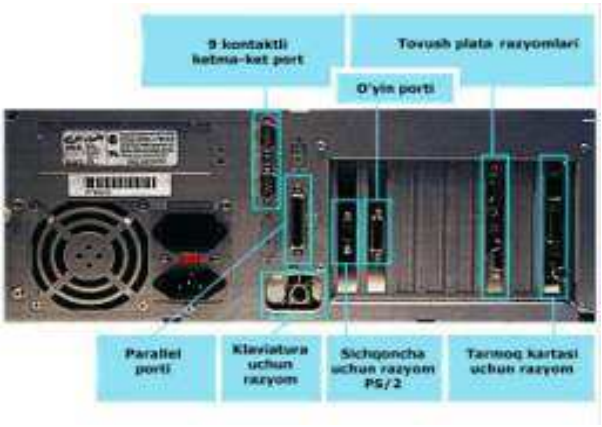
• kuchlanishning yo'qolib qolishi **(blackout)** — shubxasiz, barcha kompyuterlardan foydalanuvchilar xatto kuchlanishning qisqa vaqtli yo'qolib qolishidan, shakllanishiga bir necha soatlab ish vaqti sarflangan asosiy xotiradagi ma`lumotlarni yo'qolishidan ma`naviy iztirob chekkanlar;

• kuchlanishning o'tirib qolishi **(brounout)** — bir vaqtning o'zida bir nechta quvvatli elektr energiyasi iste`molchilarining ulanishi bilan kelib chiqqan kuchlanish amplitudasining juda qisqa vaqtga nominaldan pastga tushib ketishi;

• kuchlanishning sakrashlari **(strike)** — elektr energiyasining quvvatli iste`molchilari ulanganda va o'zilganda, statik razryadlar va yashin urishlar bilan ham va elektr tarmog'idagi o'tkinchi jarayonlar bilan ham chiqariluvchi, amplitudasi bir necha ming voltlargacha yetadigan kuchlanishning qisqa vaqt oshib ketishi;

• elektromagnit halaqitlar **(electromagnetic interference)** — turli xil jixozlarning ishlashidan kelib chiqadigan induktiv yoki galvanik oshib ketishlar natijasida kuchlanish shaklining sinusoidal shakldan og'ishi;

• chastotaning og'ishi **(frequency deviation)** — kuchlanish manbai chastotasining doimiy emasligidan kelib chiqadi.



Bu barcha og'ishlar, odam uchun deyarli kuchlanishni to'liq yo'qolib qolishidan tashqari sezilmaydi, lekin kompyuter ishini buzishi mumkin. Baholashlarga qaraganda, ShK ishlashidagi 75 % tushuntirib bo'lmaydigan buzulishlar (osilib qolishlar, dasturlar ishlashidagi uzulishlar, xotiraga murojaat qilishdagi xatoliklar) past sifatli elektr ta`minoti sababli kelib chiqadi.
SHuning uchun kompyuterni hech bo'lmaganda kerakmas ruxiy zarbalardan saqlash uchun ham elektr tarmog'ining ko'ngilsiz ta`sirlaridan himoya qilish maqsadga muvofiqdir.

Kompyuterni elektr ta`minoti qurilmasining ushbu ikki tipini ishlatishni tavsiya etish mumkin:

• tarmoqli filtrlar;

• uzluksiz ta`minot manbalari;

Tarmoq filtrlari (masalan, Pilot tipidagi) kompyuterlar elektr ta`minoti zanjirlarini va boshqa elektron apparaturani kuchlanish sakrashlaridan va elektromagnit xalaqitlardan himoya qilish uchun mo'ljallangan.

Uzluksiz ta`minot manbalari (UTM)

elektr ta`minot ko'ngilsizliklaridan kompyuterni kompleks himoya qilishni amalga oshiradi.

Ular ikki asosiy vazifani bajaradi:

• kirish kuchlanishi to'liq, yo'q bo'lib qolganda yoki o'zoq, vaqt keskin pasayganda (o'rnatilgan diapazondan tashqarida) zaxiraviy elektr ta`minoti;

• kirish kuchlanishining ko'ngilsiz holatlarini bartaraf qilish yo'li bilan kuchlanishning ma`qul sifatini ta`minlash.

Aytilgan vazifalarni amalga oshirish uchun UTM mos ravishda quyidagilarga ega:

• zaryadlash qurilmasiga ega bo'lgan akkumulyator batareyasi;

• elektromagnit va impuls xalaqitlarni bartaraf etish uchun kirish filtri.

UTM uch tipda ishlab chiqariladi:

• zaxiraviy (off line) — faqat minimal himoyani ta`ninlovchi oddiy UTM;

• interaktiv (line interactive), u zaxiradagidan kirish kuchlanishini doimiylashtirish sxemasining borligi bilan farq, qilib, bu sxema, xususan, pasaygan ta`minot kuchlanishida akkumulyatorning tez razryadlanishining oldini oladi;

• almashtiriluvchi (on line) yoki kuchlanishni ikkilangan o'zgartiruvchi, u himoyaning eng yuqori darajasini ta`minlaydi, lekin ular nisbatan qimmatdir (taxminan 2 marta qimmatroqdir).

UTM ni tanlashda birinchi navbatda quyidagilarga e`tiborni qaratish kerak:

• qurilmaning chiqish quvvati — u kompyuterning barcha bloklari iste`mol qiladigan quvvatdan taxminan 40 % ga kattaroq bo'lishi kerak;

• o'zib quyilgan ta`minotda avtonom ishlash vaqti;

• UTM tarmoqdan ishlaydigan kirish kuchlanishining ruxsat etilgan oralig'i.

Pirovardida bir necha maslahatlarni beramiz:

• odatda UTM yerga ulash sifatiga juda talabchandir; manba birinchi marta ulanganda agar chiyillay boshlasa xayron bo'lmang — elektr tarmog'ining «erga ulash» va neytral (betaraf)ini aloxida yotqizilishi to'g'risida oldindan g'amini yeyish tavsiya etiladi;

• UTM ga lazerli printerlarni ulash tavsiya etilmaydi — lazerli printer qizish vaqtida iste`mol qiladigan tok nominal qiymatdan 10 marta oshib ketishi mumkin;

• bazi bir ishlab chiqaruvchilar qurilmani yevropacha variantda sotishadi — harid qilishda UTM da kirish kuchlanishi 220 volt bo'lishiga ishonch hosil qiling.

II. Amaliy qism.

Tarmoq filtr(pilot)lari

Bugungi kunda tarmoq filtrlarini ishlab chiqaruvchi ko'plab firmalar mavjud. Quyida tarmoq filtrlariing bir necha xil shakldagi ko'rinishlari keltirilgan:

Ushbu rasmlardan ko’rinib turibdiki tarmoq filtr(pilot)lari tashqi ko’rinishdan bir-biridan dizayni va unga suqilishi mumkin bo’lgan uyalar soni bilan farqlanar ekan. Lekin pilotning eng muxim xususiyati kuchlanish sakrashlaridan va elektromagnit xalaqitlardan elektron apparaturani himoya qilishdir. Pilot xarid qilishda anashu xususiyatga e`tibor berish maqsadga muvofiq.
Quyidagi rasmda pilotning umumiy tashqi jixozlari ko’rsatilgan:

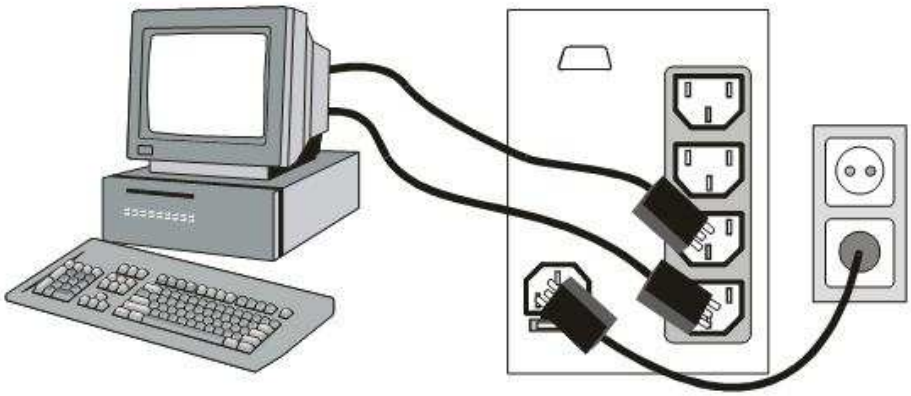
Kompyuterni elektr tarmog’iga tarmoq filtrlari orqali ulash uning ishlash muddatini uzoq saqlashga sabab bo’ladi. Chunki kutilmagan kuchlanish sakrashlari va elektromagnit xalaqitlari kompyuterni normal ishlashiga qarshilik qiluvchi omillardandir. Tarmoq filtrlari orqali elektr tarmog’iga ulangan kompyuterlarda bu muammo xal etilganligi foydalanuvchi uchun qulaylik yaratadi.

Quyidagi rasma tarmoq filtrlarini umumiy xolatda elektr manbaiga ulanayot-gandagi ko’rinishi tasvirlangan:

Uzluksiz ta`minot manbalari (UTM)

**Uzluksiz ta`minot manbalari (UTM) -** Elektr ta`minot ko'ngilsizliklaridan kompyuterni kompleks himoya qilishni amalga oshiradi. UTM ni ishlab chiqaruvchi firmalar soni juda ko'p xuddi tarmoq filtrlari kabi ulardan sifatlisini tanlash maqsadga muvofiq. Quyida bir necha xil UTM ni ko'rinishlari keltirilgan:

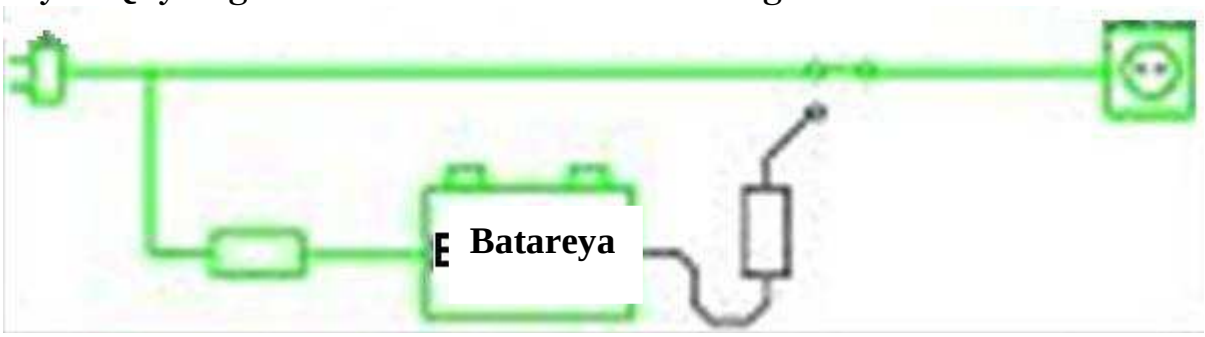
UTM kompyuterni elektr manbaida yuz berishi mumkin bo'lgan turli zararli xolatlardan saqlanishiga katta yordam beradi. Quyidagi rasmda kompyuter qurilmasini UTM ga ulangan xolati tasvirlangan:



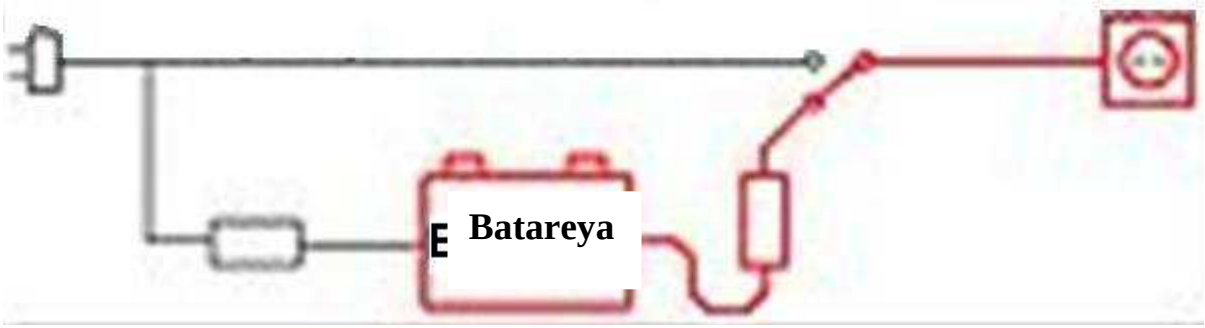
Umumiy xolatda kopyuterning monitor va Case qurilmalaridan chiqqan kabellari UTM qurilmasiga ulanadi. Rasmlarga e`tibor bersangiz UTM qurilmasida bir nechta kabel suqiladigan uyalar mavjud. Ular asosan ikki xil bo'lad: biri elektr manbaidan keladigan kabel(rasmda chap quyidagisi) ikkinchisi kompyuter qurilmalari kabellari.

Quyidagi rasmda kompyuter, UTM, pilot va boshqa qurilmalarni elektr manbaiga ulanish tartibi tasvirlangan:

Tarmoqda elektr toki bor vaqtida UTM qurilmasining batareyasi to'yinib boradi, ushbu xolatda UTM qurilmasi elektr toki iste`molchisi vazifasini o'taydi. Quyidagi rasmda anashu xolat tasvirlangan:



Agar tarmoqda elektr toki o'chadigan bo'lsa zanjirning elektr manbaiga ulangan qismi o'chib UTM qurilmasi batareyasi o'zida saqlab olgan tokni kompyuterni vaqtinchalik bo'lsada o'chmasdan ishlab turishini ta`minlashga sarflaydi. Ushbu xolat sxemasi quyidagicha:



Topshiriqlar:

1. Nazariy qismda berilagan ma`lumotlar bilan tanishib chiqing.
2. Elektr ta`minoti parametrlarini standartdan turlicha chetga og'ishlari deganda nima tushuniladi.

3. Tarmoq filtrlariga misol keltiring va amaliyotda kompyuterni tarmoq filtriga ulab ishlating.

4. Uzluksiz ta`minot manbalari haqida ma`lumot bering . Amaliyotda kompyuterni UTM qurilmasi orqali ishlatish malakasini egallang.

Amaliy ish №2

Mavzu: Viruslarning kompyuter ishiga salbiy ta`siri. Viruslarni aniqlash va yo'q qilish uchun dasturlar, dastur detektorlar.

Ishdan maqsad: *Viruslarninig kompyuter ishiga salbiy ta`siri. Avtonom va lokal xolatlarda ishlarda ishlayotgan kompyuterlarda virusdan profilaktik nazorat. Viruslarni aniqlash va yo'q qilish uchun dasturlar. Dastur detektorlar.*

I. Nazariy qism.

Kompyuter viruslari. Bu nima va unga qarshi qanday kurashish kerak? Bu mavzuga o'nlab kitoblar va yuzlab maqolalar yozilgan. Kompyuter viruslariga qarshi minglab professional mutaxassislar ko'plab kompaniyalarda ish olib borishmoqda. Bu mavzu o'ta qiyin va muhimki ko'p e`tiborni talab kilmoqda. Kompyuter virusi ma`lumotni yo'qotish sabablaridan biri va asosiysi bo'lib qolmoqda. Viruslar ko'plab tashkilot va kompaniyalarni ishlarini buzishga olib kelganligi ma`lum. Shunday ma`lumotlar mavjudki, Niderlandiya gospitallaridan birida bemorga kompyuter qo'ygan tashxis bo'yicha iste`mol qilingan dori oqibatida bemor olamdan o'tgan. Bu kompyuter virusining ishi bo'lgan.

E`tiborsizlik bilan qilingan ishdan kompyuter tezda virus bilan zararlanadi. Inson kasallik virusi bilan zararlansa issiqligi o'zgarishi, vazni o'zgarishi, xolsizlanish va og'riqning paydo bo'lishi ko'zda tutiladi. Kompyuter virusi bilan zararlangan kompyuterlarda quyidagilar kuzatiladi: dasturlarning ishlashining sekinlashishi, fayllarni hajmi o'zgaradi, g'ayritabiiy va ba`zi bir noma`lum xatoliklar, ma`lumotlar va sistema fayllari yo'qotilishi. Ba`zi viruslar zararsiz ko'payadi, lekin qo'rqinchli emas. Bu viruslar ekranga xato ma`lumot chiqaradi. Ammo, bir turdagi viruslar hujum qiluvchi, ya`ni, yomon asoratlar qoldiruvchi hisoblanadi. Masalan, viruslar qattiq diskdagi ma`lumotlarni o'chirib tashlaydi.

Virus nima?

Virus(Вирус) inglizcha “yuqumli boshlanish”, “yomon boshlanish – buzuvchi boshlanish”, “yuqumli kasal” degan ma`nolarni anglatadi.
Mashxur «doktor» lardan biri D.N.Lozinskiy virusni kotibaga o’xshatadi. Tartibli kotibani faraz kilsak, u ishga keladi va stolidagi bir kunda qilishi kerak bo’lgan ishlarni - qog’ozlar qatlamini ko’radi. U bir varog’ni ko’paytirib bir nusxasini o’ziga ikkinchisini keyingi qo’shni stolga qo’yadi. Keyingi stoldagi kotiba ham kamida ikki nusxada ko’paytirib, yana bir kotibaga o’tkazadi. Natijada kontoradagi birinchi nusxa bir necha nusxalarga aylanadi. Ba`zi nusxalar yana ko’payib boshqa stollarga ham o’tishi mumkin.
Kompyuter viruslari taxminan shunday ishlaydi, Faqat qogozlar o’rnida endi dasturlar, kotiba bu - kompyuter. Birinchi buyruk «ko’chirish-nusxa olish» bo’lsa, kompyuter buni bajaradi va virus boshqa dasturlarga
o’tib oladi. Agar kompyuter biror zararlangan dasturni ishga tushirsa virus boshqa dasturlarga tarqalib borib butun kompyuterni egallashi mumkin.
Agar bir dona virusning ko’payishiga 30 sekund vaqt ketsa, bir soatdan keyin bu 1000000000 dan ortib ketishi mumkin. Aniqrog’i kompyuter xotirasidagi bo’sh joylarni band qilishi mumkin.
Xuddi shunday voqea 1988 yili Amerikada sodir bo’lgan. Global tarmoq orqali uzatilayotgan ma`lumot orqali virus bir kompyuterdan boshqasiga o’tib yurgan. Bu virus Morris virusi deb atalgan.
Ma`lumotlarni virus qanday yo’q qilishi mumkin degan savolga shunday javob berish mumkin:
Virus nusxalari boshqa dasturlarga tez ko’payib o’tib oladi;
Kalendar bo’yicha 13-sana juma kunga to’g’ri kelsa hamma xujjatlarni yo’q qiladi.
Buni hammaga ma`lum «Jerusalem» («Time» virusi ham deb ataladi) virusi juda «yaxshi» amalga oshiradi.
Ko’p xollarda bilib bo’lmaydi, virus qaerdan paydo bo’ldi.
Virusni aniqlanishi shundagi, u kompyuter sistemasida joylashib va ko’payib borishiga bog’lik. Misol uchun, nazariy jihatdan operativ sistemada virus davolab bo’lmaydi. Bajaruvchi kodning sohasini tuzish va o’zgartirish ta`kiklangan sistema misol bo’lishi mumkin.
Virus hosil bo’lishi uchun bajariluvchi kodlar ketma-ketligi ma`lum bir sharoitda shakllanishi kerak. Kompyuter virusining xossalaridan biri o’z nusxalarini kompyuter tarmoqlari orqali bajariluvchi ob`ektlarga ko’chiradi. Bu nusxalar ham o’z-o’zidan ko’payish imkoniyatiga ega.

Kompyuter viruslari qanday hosil bo’ladi?

Biologik viruslardan farqli o’laroq, kompyuter viruslarini inson tomonidan tuziladi. Viruslar kompyuter foydalanuvchilariga katta zarar yetkazadi. Ular kompyuter ishini to’xtatadi yoki qattiq diskdagi ma`lumotlarni o’chiradi. Virus sistemaga bir necha yo’llar bilan tushishi mumkin: disketalar, dastur ta`minot yuklangan CD-ROM, tarmoq

interfeysi yoki modemli bog'lanish, global Internet; tarmog'idagi elektron pochta.
Disketa virusdan zararlanishi oson. Zararlangan kompyuterga disketni solib o'qitilganda diskning bosh sektoriga virus tushadi.
Internet ma`lumotlar almashinishiga katta imkoniyat yaratadi. Lekin, kompyuter viruslari va zararli dasturlar tarqalishi uchun yaxshi muhit yaratadi. Albatta Internet dan olingan barcha ma`lumotlarda virus bor deb bo'lmaydi. Kompyuterda ishlovchi ko'pchilik mutaxassislar va operatorlar qabul qilinadigan ma`lumotlarni viruslardan tekshirishni doimo bajaradi. Internet da ishlayotgan har bir kishi uchun yaxshi antivirus himoya zarur. «Kasperskiy laboratoriyasi» texnik ta`minot xizmati statistikasiga ko'ra, viruslardan zararlangan xolatlarning 85% i elektron
pochta orqali sodir bo'lgan. 1999 yilga nisbatan xozirgi kunda bu ko'rsatkich 70 % tashkil etadi. «Kasperskiy laboratoriyasi» elektron pochtalarga yaxshi antivirus himoyasi kerakligini ta`kidlaydi.
Virus tuzuvchilarga elektron pochta juda qulay. Amaliyot shuni ko'rsatadiki, ommabop dasturlar, operatsion sistemalar, ma`lumotlarni uzatish texnologiyalari uchun viruslar ko'plab tuzilmoqda. Xozirda elektron pochta biznes va boshqa sohalarda muloqot uchun asosiy vosita bo'lib qolmoqda. Shuning uchun virus tuzuvchilari elektron pochtaga dikkatini qaratmoqda.

Virus paydo bo'lish belgilari.

Zararlangan kompyuterda eng muhimi virusni aniqlash. Buning uchun virusni asosiy belgilarini bilish kerak:
1.Funktsiopal dasturlarni ishini to'xtatish yoki noto'g'ri ishlashi;
2.Kompyuterni sekin ishlashi;
3.OS ni yuklanmasligi;
4.Fayl va kataloglarni yo'qolishi yoki ulardagi ma`lumotlarni buzilishi;
5.Fayllar modifikatsiyasining sana va vaqtining o'zgarishi;
6.Fayl hajmining o'zgarishi;
7.Diskdagi fayllar miqdorining keskin ko'payishi;
8.Bo'sh operativ xotira hajmining keskin kamayishi;
9.Kutilmagan ma`lumotlar va tasvirlarning ekranga chiqishi;
10.Kutilmagan tovushlarning paydo bo'lishi;
11 .Kompyuterning tez-tez osilib kolishi.

Yuqoridagi belgilar boshqa sabablarga ko'ra ham bo'lishi mumkinligini eslatib o'tamiz.

Qisqacha tarix.

80-yillarda IVM-RS bilan ishlagan kishilar bo'lsa 1987-89 yillardagi viruslarni tarqalishini unutishganicha yo'q. Ekrandagi harflar har xil ko'rinishda buzilgan va foydalanuvchilar ommasi mutaxassislarga

displeylarini olib kela boshlashgan. Keyinchalik kompyuter «Yankee Doodle» deb nomlangan o'zga yerlik virusini chalishni boshlagan. Lekin, buni tuzatishni hech kim tashlamadi juda tez xal bo'ldi. Bu o'nlab viruslar to'plami edi.
Shunday qilib, viruslar fayllarni zararlay boshladi. «Vgat» va ekranda shariklar paydo qiluvchi «Pingpong§» viruslari Boot sektor ustidan ham g'olib chiqishdi. Bu hammasi IVM-RS dan foydalanuvchilarga unchalik yoqmadi va antiviruslar paydo bo'ldi. Birinchi antiviruslardan biri ANTI-KOT: afsonaviy Oleg Kotik o'zining antivirusining birinchi versiyasi dunyo yuzini ko'rdi. U 4 ta virusni yo'q qildi. Afsuski, ANTI-KOT MS DOS kombinatsiyasidan foydalanib fayl oxirida «Time» virusini aniqlandi. Boshqa antiviruslar esa .com va .exe kengaytmali fayllarning har bir harfigacha zanjirlaydi.
Vaqt o'tishi bilan viruslar ko'payib bormoqda. Bularning hammasi bir-biriga o'xshash, xotiraga o'rnashadi, sektor va fayllarga bog'lanadi, fayllarni, disket va vinchesterlarni yo'q qiladi. Birinchilardan bo'lib, «Frodo.4096» virusi ommabop bo'lib chiqdi. Bu virus INT2Ih ni egallab, DOS ga murojaat etilganda zararlangan fayl xuddi hech narsa bo'lmaganday xolda ko'rinish bergan. Ammo, bu MS DOS ustidan o'rnashib xukmini o'tkazgan. Bir yil ham o'tmasdanok «elektr suvaraklar» DOS yadrosiga o'rnashib olishgan. Ko'rinmas virus «Deast.512» deb atalgan. Ko'rinmaslik fikri ko'payib rivojlanib bordi: 1991 yil yozida kompyuter o'lati - virus «Dir_n» paydo bo'ldi. Biroq ko'rinmaslarga qarshi kurash sodda: RAM ni davolab xotirjam bo'lish mumkin. Shunday viruslar ham kelib chiqdiki, ular o'zlarini shifrlab olish imkoniyatiga ega bo'lishdi. Bu viruslarni davolash va yo'q qilish uchun maxsus qism dasturlar yaratish kerak bo'lgan. Lekin bunga hech kim e`tibor bermadi, toki bu viruslarning yangi avlodlari kelib chiqmaguncha.

Kompyuter viruslaridan axborotlarga ruxsatsiz kirish va ulardan foydalanishni tashkil etish.

Shuni aytib o'tish lozimki, xozirgi paytda xar-xil turdagi axborot va dasturlarni o'g'irlab olish niyatida kompyuter viruslaridan foydalanish eng samarali usullardan biri hisoblanadi.
Dasturli viruslar kompyuter tizimlarining havfsizligiga tahdid solishning eng samarali vositalaridan biridir. Shuning uchun ham dasturli viruslar-ning imkoniyatlarini tahlil qilish masalasi hamda bu viruslarga qarshi kurashish xozirgi paytning dolzarb masalalaridan biri bo'lib qoldi.
Viruslardan tashqari fayllar tarkibini buzuvchi troyan dasturlari mavjud. Virus ko'pincha kompyuterga sezdirmasdan kiradi. Foydalanuvchinint o'zi troyan dasturini foydali dastur sifatida diskka yozadi. Ma`lum bir vaqt o'tgandan keyin buzg'unchi dastur o'z ta`sirini ko'rsatadi.
O'z-o'zidan paydo bo'ladigan viruslar mavjud emas. Virus dasturlari inson tomonidan kompyuterning dasturiy ta`minotini, uning qurilmalarini

zararlash va boshqa maqsadlar uchun yoziladi. Viruslarning hajmi bir necha baytdan to o'nlab kilobaytgacha bo'lishi mumkin.

Troyan dasturlari foydalanuvchiga zarar keltiruvchi bo'lib, ular buyruklar (modullar) ketma – ketligidan tashkil topgan, omma orasida juda keng tarqalgan dasturlar (tahrirlovchilar, o'yinlar, translyatorlar) ichiga o'rnatilgan bo'lib, bir qancha hodisalar bajarilishi bilan ishga tushadigan «mantiqiy bomba» deb ataladigan dasturdir. O'z navbatida, «mantiqiy bomba»ning turli ko'rinishlaridan biri «soat mexanizmli bomba» hisoblanadi.

SHuni ta`kidlab o'tish kerakki, troyan dasturlari o'z-o'zidan ko'paymasdan, kompyuter tizimi bo'yicha dasturlovchilar tomonidan tarqatiladi.

Troyan dasturlardan viruslarning farqi shundaki, viruslar kompyuter tizimlari buylab tarqatilganda, ular mustaqil ravishda hosil bo'lib, o'z ish faoliyatida dasturlarga o'z matnlarini yozgan holda ularga zarar ko'rsatadi.

Zararlangan dasturda dastur bajarilmasdan oldin virus o'zining buyruqlari bajarilishiga imkoniyat yaratib beradi. Buning uchun ham virus dasturning bosh qismida joylashadi yoki dasturning birinchi buyrug'i unga yozilgan virus dasturiga shartsiz o'tish bo'lib xizmat qiladi. Boshqarilgan virus boshqa dasturlarni zararlaydi va shundan so'ng virus tashuvchi dasturga ishni topshiradi.

Virus hayoti odatda quyidagi davrlarni o'z ichiga oladi: qo'llanilish, inkubatsiya, replikatsiya (o'z-o'zidan ko'payish) va hosil bo'lish. Inkubatsiya davrida virus passiv bo'lib, uni izlab topish va yo'qotish qiyin. Hosil bo'lish davrida u o'z funktsiyasini bajaradi va qo'yilgan maqsadiga erishadi.

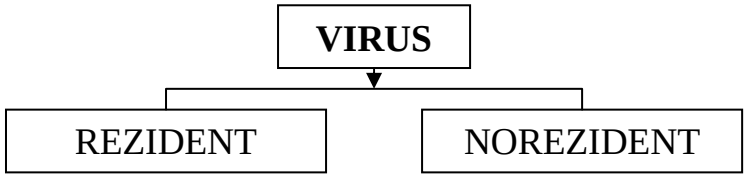
Tarkibi jihatidan virus juda oddiy bo'lib, bosh qism va bazi hollarda dumdan iborat. Virusning bosh qismi deb boshqarilishini birinchi bo'lib ta`minlovchi imkoniyatga ega bo'lgan dasturga aytiladi. Virusning dum qismi zararlangan dasturda bo'lib, u bosh qismidan alohida joyda joylashadi.

Kompyuter viruslari xarakterlariga nisbatan norezident, rezident, butli, gibridli va paketli viruslarga ajratiladi.

Faylli norezident viruslar to'liqligicha bajarilayotgan faylda joylashadi, shuning uchun ham u faqat virus tashuvchi dastur faollashgandan so'ng ishga tushadi va bajarilgandan so'ng tezkor xotirada saqlanmaydi.

Rezident virus norezident virusdan farqliroq tezkor xotirada saqlanadi.

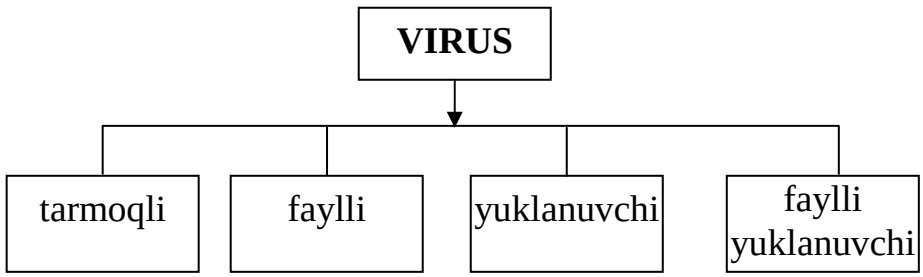
Rezident viruslarning yana bir ko'rinishi but viruslar bo'lib, bu virusning vazifasi vinchester va egiluvchan magnitli disklarning yuklovchi sektorini ishdan chiqarishdan iborat. But viruslarning boshi diskning yuklovchi but sektorida va dumi disklarning ixtiyoriy boshqa sektorlarida joylashgan bo'ladi.



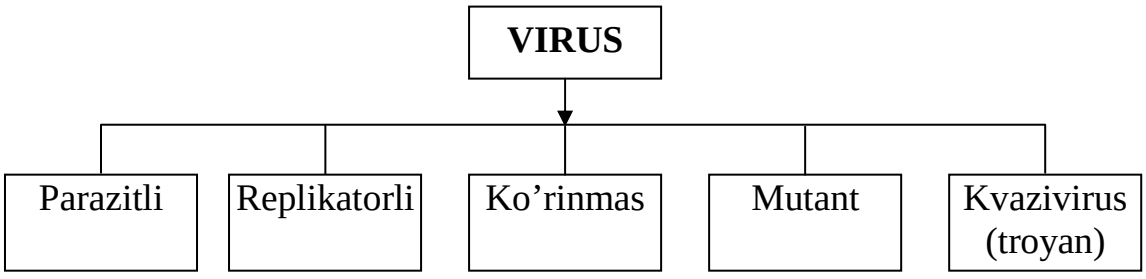
Paketli virusning bosh qismi paketli faylda joylashgan bo'lib, u operatsion tizim topshiriqlaridan iborat.
Gibridli viruslarning boshi paketli faylda joylashadi. Bu virus ham faylli, ham but sektorli bo'ladi.
Tarmoqli viruslar kompyuter tarmoqlarida tarqalishga moslashtirilgan, ya`ni tarmoqli viruslar deb axborot almashishda tarqaladigan viruslarga aytiladi.

Viruslarning turlari:

1) fayl viruslari. Bu viruslar som, exe kabi turli fayllarni zararlaydi;
2) yuklovchi viruslar. Kompyuterni yuklovchi dasturlarni zararlaydi;
3) drayverlarni zararlovchi viruslar. Operatsion tizimdagi sonfig.sys faylni zararlaydi. Bu kompyuterning ishlamasligiga sabab bo'ladi;
4) DIR viruslari. FAT tarkibini zararlaydi;
5) stels-viruslari. Bu viruslar o'zining tarkibini o'zgartirib, tasodifiy kod o'zgarishi bo'yicha tarqaladi. Uni aniqlash juda qiyin, chunki fayllarning o'zlari o'zgarmaydi;



6) Windows viruslari. Windows operatsion tizimidagi dasturlarni zararlaydi.
Misol sifatida quyidagilarni keltirish mumkin:
1) Eng havfli viruslardan biri Internet orqali tarqatilgan **«Chernobil»** virusi bo'lib, u 26 aprelda tarqatilgan va har oyning 26-kunida komp`yuterlarni zararlashi mumkin.
2) **I LOVE YOU** virusi Filippindan 2000 yil 4 mayda E-mail orqali tarqatilgan. U bugun jahon bo'yicha 45 mln. kompyuterni zararlagan va ishdan chiqargan. Moddiy zarar 10 mlrd. AQSH dollarini tashkil qilgan.
3) 2003 yil mart oyida Shvetsiyadan elektron pochta orqali **GANDA** virusi tarqatilgan va u butun dunyoda minglab kompyuterlarni zararlagan. Bu virusni tarqatgan shaxs hozir qo'lga olingan va u 4 yil qamoq jazosiga hukm etilishi mumkin.
Asoslangan algoritmlar bo'yicha dasturli viruslarni quyidagicha tasniflash mumkin.



Hamjixat-yo'ldoshlar - fayllarni o'zgartirmaydigan viruslar. Bu viruslar EXE kengaytmali fayllarga qo'shimcha nusxa olib, bu nusxani .com yoki .bat kengaytmali fayl qilib yozib qo'yadi. Bunday faylga murojaat etilganda birinchi .com yoki .bat kengaytmali fayl ishga tushadi So'ngra esa virus .exe kengaytmalisini ishga tushirib yuboradi.

Chuvalchang-luqmalar -bu viruslar kompyuter tarmoqlariga tarqaydi, fayl va disk sektorlarini o'zgartirmaydi. Ular kompyuter tarmog'i orqali xotiraga kiradi. Boshqa viruslar adreslarini topib ularga o'z nusxalarini yozib qo'yadi. Bunday viruslar ba`zida fayllar tuzadi, lekin umuman kompyuter resurslariga murojaat qilmaydi.

Talaba viruslari - juda ko'p xatoliklar keltirib chiqaruvchi hisoblanadi. Ular har -xil harflarni paydo qilishi kutiladi.

Polimorfik-ajina-mutantlar virusi -etarlicha tutish qiyin bo'lgan viruslar hisoblanadi. Ular aniq bir joyda turmaydi (ko'chib yuradi). Ko'p xollarda polimorfik viruslar o'zining bir xil nusxasiga ega bo'lmaydi.

Makro viruslari - asosan ma`lumotlarni qayta ishlashga to'sqinlik qiladi va matn muharrirlariga zarar yetkazadi. Xozirgi vaqtda Microsoft Word, Exse1 va Assess muharrirlarida tayyorlangan xujjatlarda ko'plab uchrab turadi.

Parazitli virus — fayllarning tarkibini va diskning sektorini o'zgartiruvchi virus. Bu virus oddiy viruslar turkumidan bo'lib, osonlik bilan aniqlanadi va o'chirib tashlanadi.

Replikatorli virus — «chuvalchang» deb nomlanadi, kompyuter tarmoqlari bo'yicha tarqalib, kompyuterlarning tarmoqdagi manzilini aniqlaydi va u yerda o'zining nusxasini qoldiradi.

Ko'rinmas virus — stels-virus deb nom olib, zararlangan fayllarga va sektorlarga operatsion tizim tomonidan murojaat qilinsa, avtomatik ravishda zararlangan qismlar o'rniga diskning toza qismini taqdim etadi. Natijada ushbu viruslarni aniqlash va tozalash juda katta qiyinchiliklarga olib keladi.

Mutant virus — shifrlash va deshifrlash algoritmlaridan iborat bo'lib, natijada virus nusxalari umuman bir-biriga o'xshamaydi. Ushbu viruslarni aniqlash juda qiyin muammo.

Kvazivirus virus — «Troyan» dasturlari, deb nom olgan bo'lib, ushbu viruslar ko'payish xususiyatiga ega bo'lmasa-da, «foydali» qism-dastur hisobida bo'lib, antivirus dasturlar tomonidan aniqlanmaydi.
SHu bois ham ular o'zlarida mukammallashtirilgan algoritmlarni to'siqsiz bajarib, qo'yilgan maqsadlariga erishishlari mumkin. Ular kerakli dasturlar ichiga kirib olib har bir buyruk berilganda qaqshatgich zarba bera oladi.U kompyuter va uning tarmoqlari orqali ko'payib sezilarli zararlarni paydo qiladi

O'z davrida keng tarqalgan viruslar

Windows 98 qaroqchilik nusxalari bilan tarqaladigai virus.
Karnegi-Mellon universiteta kompyuter xodisalariga javob beruvchi gurux muvofiqlashtirish markazi xabariga ko'ra 2000 yil boshida yangi virus paydo bo'ldi. Bu Trojan.kill troyan virusi bo'lib, yana – lnst98 degan nomga ham ega. U S: diskdagi hamma ma`lumotlarni o'chiradi. Dastlab Microsoft Windows98 operatsion tizimining qaroqchilik nusxalarida uchradi, biroq virus elektron pochta va birgalikda foydalanilayotgan tarmoq disklari orqali ham tarqalishi mumkin. Xabar berilishicha, virus 5682 bayt o'lchamdagi INSTAL.EXE faylida bo'ladi. Ushbu fayl KEY V.com klaviatura joylashish faylga ko'chiriladi.

REMOTE EXPLORER dasturi.
1998 yil 17- dekabrda Microsoft World Com ichki tarmoqqa Remote Explorer nomli virus hujum qildi. Buning oqibatida bir qancha saytlar va bir necha ming serverlar va ishchi stantsiyalar zararlandi. Virus funktsiyasiga ko'ra o'zini System 32\<dirvers ga nusxasini hosil qiladi va «Remote Exrlorer»xizmati kabi o'zini o'rnatadi shundan so'ng o'zini boshqa mashinalarga nusxa ko'rinishini boshlaydi. (Faqatgina NT tarmog'ida). Virus ish bajarish jarayonida bajaruvchi fayllarni zararlashi bilan birgalikda, tanlangan matnli fayllarni ham ixtiyoriy tarzda shifrlaydi. Bu faoliyat shanba 15:00 dan yakshanba 6:00 gacha bo'lgan davrda kuchayadi. Remote Exrlorer virusi troyanlar turidagi viruslarga qo'shish mumkin, chunki kompyuter qayta yuklanganda u yo'qoladi va virus zararlanishi uchun uni odatda tezda ishga tushirish kerak.

«Chernobil» virusi
1999 yil 26-aprel kuni «Chernobil» virusi tufayli dunyo bo'yicha kompyuter fojiasi sodir bo'ldi. Zararlangan kompyuterlar xaqida Angliya, Shvetsiya, Turkiya, Yaponiya, Rossiya, Janubiy Koreya, Xindiston, Malta, Finlendiya, Yangi Zelandiya va boshqa mamlakatlardan xabar keldi. yevro Osiyo qit`asining mamlakatlari katta zarar ko'rdi. Umumman olganda taxminan 600000 mashina ishdan chiqdi. Janubiy koreyada 300000 ta Xitoyda 100000 ta, Rossiyada 100000 ta Amerikada asosan xususiy sektor, maktablar va universitetlar (1000) zararlandi. CIN nomli virus vinchestirdagi barcha ma`lumotlarni o'chirib tashlaydi. U Windows 95/98

da ishlaydi. Asosiy tarqalish yo'li - elektron pochta va zararlangan disketalar. Virus EXE fayllarga yopishib oladi va iz qoldirmaydi, chunki an`anaviy aniqlash
usullaridan qochish uchun «Space Filler» xususiyatlaridan yaxshi foydalanadi. Virus quyidagicha ishlaydi: Hard drive (Kattik disk)ning fayl tartibi yoziladigan sohaning ma`lumotning o'chirib yuboradi. Bu ma`lumotsiz sistema fayllarni ko'rmaydi So'ngra BIOS (Basic Input output Sistem)ga ta`sir qilib, OS ni zararlaydi. Bu esa vinchestirdagi ma`lumotlarninng umuman o'chirishga olib keladi. Kompyuter qachon zararlanishi noma`lum. Virusni keng tarqalishi oylab davom ettan bo'lishi mumkin. Virus 26-aprel kuni ishga tushdi. 1986yil 26-aprel Chernobil fojeasi sodir bo'lgan kun bilan ustma-ust tushganligi uchun «Chernobil» virusi deb ataldi.

Antivirus dasturlari

Hozirgi vaqtda viruslarni yo'qotish uchun ko'pgina usullar ishlab chiqilgan va bu usullar bilan ishlaydigan dasturlarni antiviruslar deb atashadi. Antiviruslarni, qo'llanish usuliga ko'ra, quyidagilarga ajratishimiz mumkin: detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar.

Detektorlar — virusning signaturasi (virusga taalluqli baytlar ketma-ketligi) bo'yicha tezkor xotira va fayllarni ko'rish natijasida ma`lum viruslarni topadi va xabar beradi. YAngi viruslarni aniqlab olmasligi detektorlarning kamchiligi hisoblanadi.

Faglar — yoki doktorlar, detektorlarga xos bo'lgan ishni bajargan holda zararlangan fayldan viruslarni chiqarib tashlaydi va faylni oldingi xolatiga qaytaradi.

Vaktsinalar — yuqoridagilardan farqli ravishda himoyalanayotgan dasturga o'rnatiladi. Natijada dastur zararlangan deb hisoblanib, virus tomonidan o'zgartirilmaydi. Faqatgina ma`lum viruslarga nisbatan vaktsina qilinishi uning kamchiligi hisoblanadi. Shu bois ham, ushbu antivirus dasturlari keng tarqalmagan.

Privivka — fayllarda xuddi virus zararlagandek iz qoldiradi. Buning natijasida viruslar «privivka qilingan» faylga yopishmaydi.

Filtrlar — qo'riqlovchi dasturlar ko'rinishida bo'lib, rezident holatda ishlab turadi va viruslarga xos jarayonlar bajarilganda, bu haqda foydalanuvchiga xabar beradi.

Revizorlar — eng ishonchli himoyalovchi vosita bo'lib, diskning birinchi holatini xotirasida saqlab, undagi keyingi o'zgarishlarni doimiy ravishda nazorat qilib boradi.

Detektor dasturlar kompyuter xotirasidan, fayllardan viruslarni qidiradi va aniqlangan viruslar xaqida xabar beradi.

Doktor dasturlari nafaqat virus bilan kasallangan fayllarni topadi, balki ularni davolab, dastlabki holatiga qaytaradi. Bunday dasturlarga Aidstest, Doctor Web dasturlarini misol kilib keltirish mumkin. Yangi viruslarning to'xtovsiz paydo bo'lib turishini hisobga olib, doktor dasturlarini ham yangi versiyalari bilan almashtirib turish lozim.

Filtr dasturlar kompyuter ishlash jarayonida viruslarga xos bo'lgan shubhali harakatlarni topish uchun ishlatiladi.

Bu harakatlar quyidagicha bo'lishi mumkin:

- fayllar atributlarining o'zgarishi;
- disklarga doimiy manzillarda ma`lumotlarni yozish;
- diskning ishga yuklovchi sektorlariga ma`lumotlarni yozib yuborish.

Tekshiruvchi (revizor) dasturlari virusdan himoyalanishning eng ishonchli vositasi bo'lib, kompyuter zararlanmagan holatidagi dasturlar, kataloglar va diskning tizim maydoni holatini xotirada saqlab, doimiy ravishda yoki foydalanuvchi ixtiyori bilan kompyuterning joriy va boshlangach holatlarini bir-biri bilan solishtiradi. Bunga ADINF dasturini misol qilib keltirish mumkin.

Viruslarga qarshi chora-tadbirlar

Kompyuterni viruslar bilan zararlanishidan saqlash va axborotlarni ishonchli saqlash uchun quyidagi qoidalarga amal qilish lozim:

- kompyuterni zamonaviy antivirus dasturlar bilan ta`minlash;
- disketalarni ishlatishdan oldin har doim virusga qarshi tekshirish;
- qimmatli axborotlarning nusxasini har doim arxiv fayl ko'rinishida saqlash.

Kompyuter viruslariga qarshi kurashning quyidagi turlari mavjud:

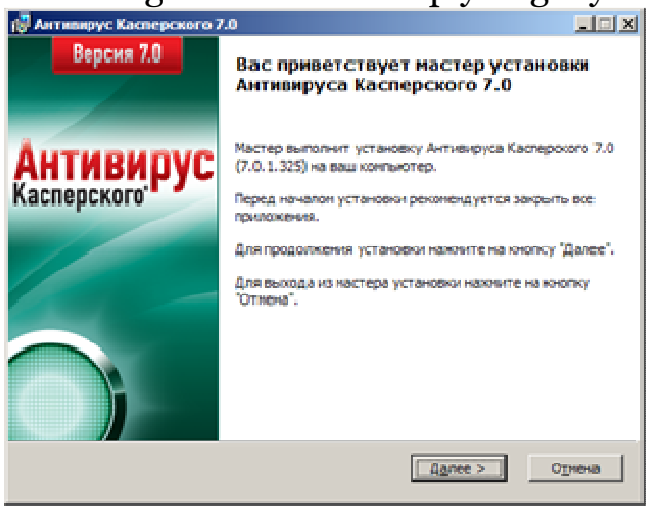
- viruslar kompyuterga kirib buzgan fayllarni o'z holiga qaytaruvchi dasturlarning mavjudligi;
- kompyuterga parol bilan kirish, disk yurituvchilarning yopiq turishi;
- disklarni yozishdan himoyalash;
- litsenzion dasturiy ta`minotlardan foydalanish va o'g'irlangan dasturlarni qo'llamaslik;
- kompyuterga kiritalayotgan dasturlarning viruslarning mavjudligini tekshirish;
- antivirus dasturlaridan keng foydalanish;
- davriy ravishda kompyuterlarni antivirus dasturlari yordamida viruslarga qarshi tekshirish.

Antivirus dasturlaridan DrWeb, Adinf, AVP, VootCHK va Norton Antivirus, Kaspersky Security , Symantek Antivirus kabilar keng foylalaniladi.

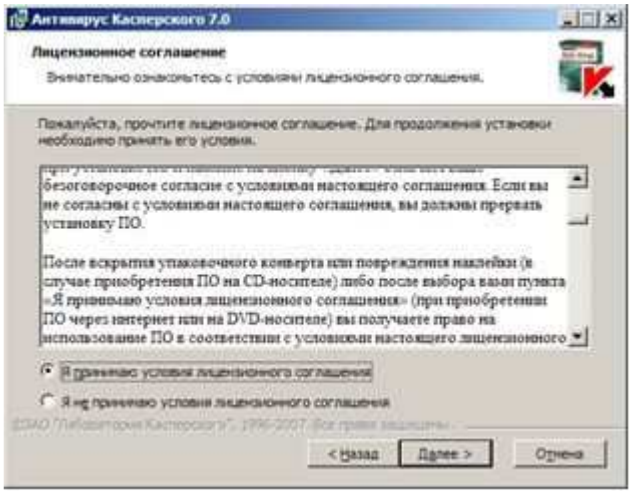
II. Amaliy qism.

Antivirus dasturini o’rnatish

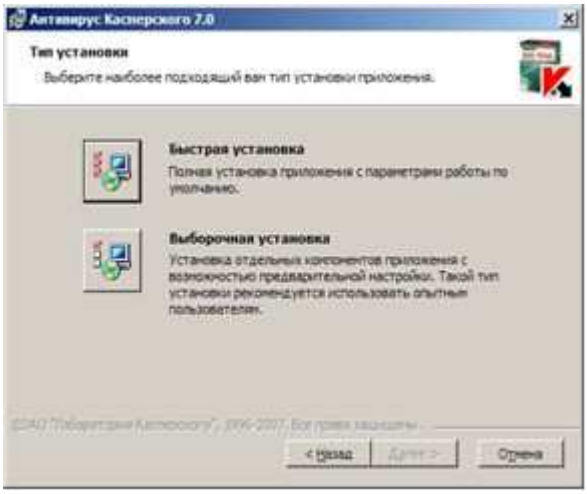
Hozirda kompyuterlarni viruslardan himoya qilish uchun turli antivirus dasturlari va yordamchi vositalari mavjuddir. Bunday dasturlar ichida Kasperskiy antivirusi mashhur. Ushbu dasturni bugungi kunda bir nechta versiyalari mavjud. Kasperskiy 5.0, Kasperskiy 6.0, Kasperskiy 7.0, Kasperskiy 2009 lar bunga misoldir. Kasperskiy antivirusini 7.0 versiyasini o’rnatish, bazasini yangilash va ishlatishni ko’rib chiqamiz.
Dasturni o’rnatish maxsus .exe dasturini ustida sichqoncha chap tugmasi ikki marta bosish bilan ishga tushiriladi va quyidagi oyna xosil bo’ladi:

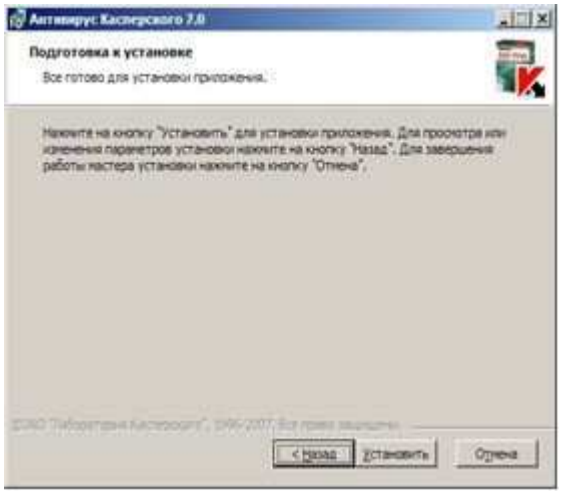


Далее tugmasini bosamiz va keyingi oynada “**Я принимаю ... соглашения**” ni tanlab **Далее** tugmasini bosamiz.

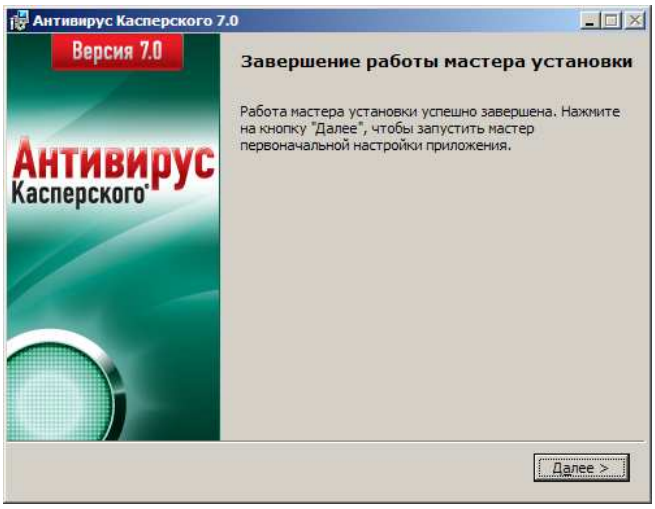


Keyingi ochilgan oynada bizga qaysi tipda:
Tezkor yoki tanlov usulida dasturni o’rnatishimiz so’raladi. Biz **Быстрая установка** tugmasini bosamiz. Keyingi oynada Ustonovit tugmasini bosamiz.





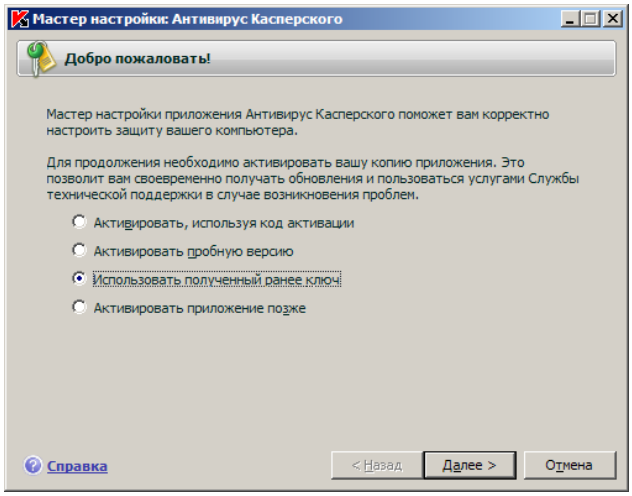
Xosil bo'lgan oynada **Далее** tugmasini bosamiz.



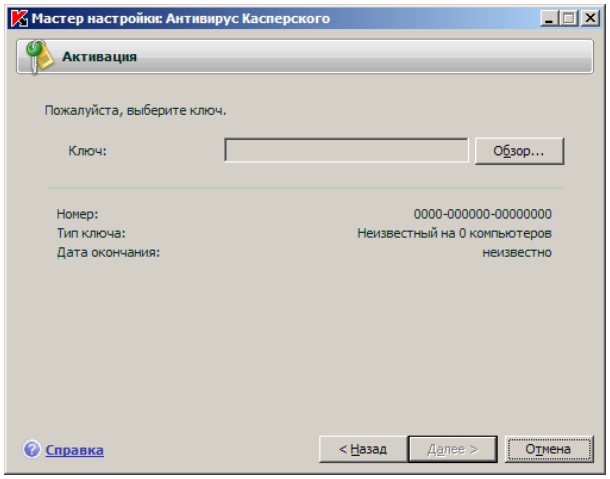
Ochilgan oynada bizga antivirus dasturini aktivatsiyasi uchun dastur kalitini so'raydi. Bunda to'rtta bo'lim mavjud bular :

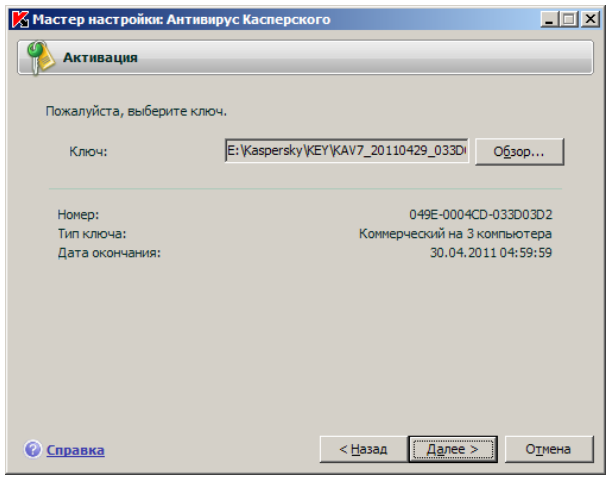
- **Активировать, используя код активации** – aktivattsiya kodidan foydalangan holda dasturni aktivlashtirish;
- **Активировать пробную версию** – 30-kunlik sinov kalitidan foydalanish;
- **Использовать ранее полученный ключ** – oldindan olingan kalit yordamida dasturni aktivlashtirish;
- **Активировать приложения позже** – dasturni keyinroq aktivlashtirish.

Biz ulardan **Использовать ранее полученный ключ** bo'limi tanlaymiz.

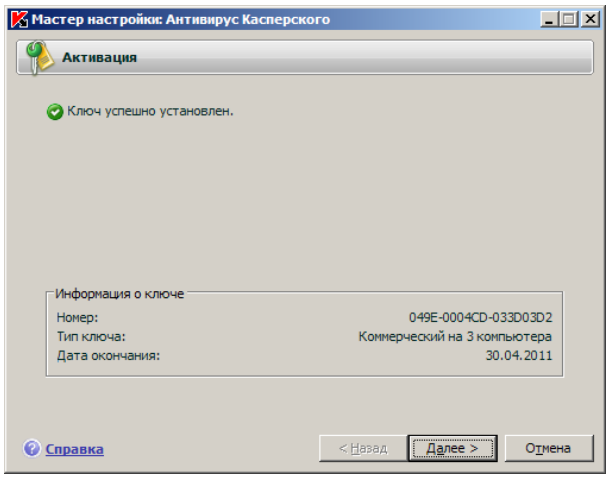


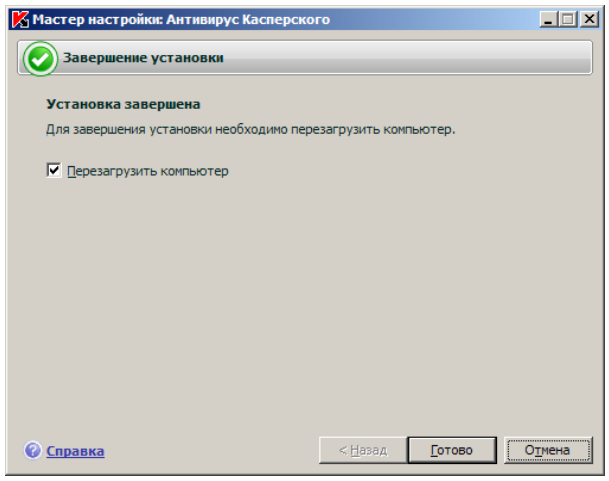
Keyingi oynada **Обзор** tugmasini bosish bilan kalit ko'rsatilib Далее tugmasi bosiladi.





Kalit o'rnatildi **Далее** tugamasini bosamiz xosil bo'lgan oynada **Готово** tumasini bosish bilan Kasperskiy antivirusini o'rnatishni yakunlaymiz.



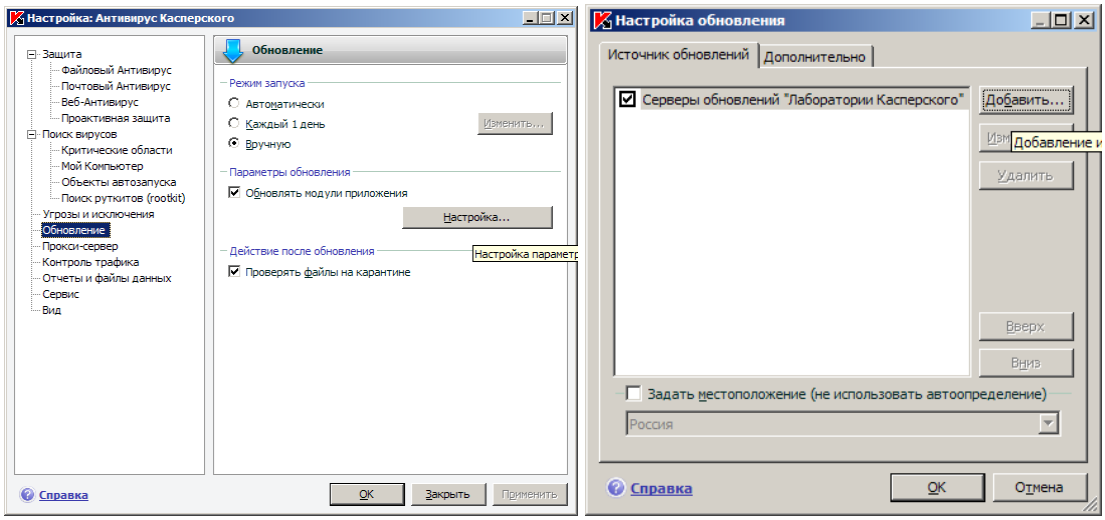


Antivirus bazasini yangilash

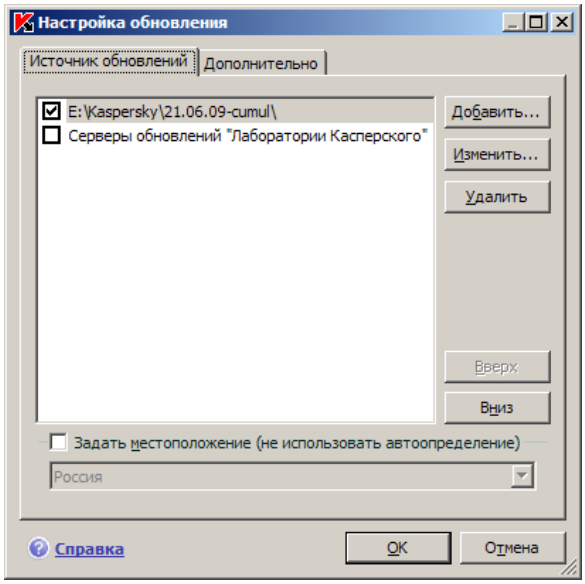
Kasperskiy antivirusini bazasi eskirib turadi va bu haqda avtomatik tarzda foydalanuvchiga xabar berib turadi. Ayniqsa komyuterga viruslar xavfi kuchayganda bu xol tez-tez takrorlanadi.
Antivirus bazasini yangilash uchun Kasperskiy oynasi ochiladi. Buning uchun →**Пуск Все программы► Антивирус Касперского 7.0 Антивирус Касперского 7.0** amallari ketma-ket bajariladi.

Ochilgan oynadan **Настройка** bo'limi tanlanadi.

Keyingi oynadan **Обновление** bo'limidan **Настройка** tugmasini bosamiz. Ochilgan oynadan **Добавить** tugmasini bosib antivirus bazasini ko'rsatib **OK** tugmasini bosamiz.



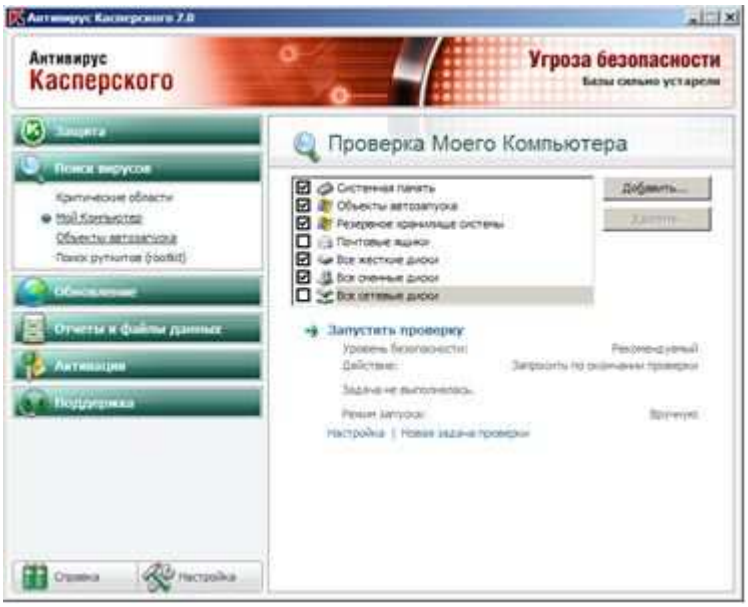
Belgini yangilayotgan bazadan boshqasiga qo'yilmaydi va **OK** tugmasi bosiladi.



Antivirusning asosiy oynasiga o'tib **Обновление** bo'limi tanlanadi. Bu bo'limda **Обновить базы** ni bosish bilan ko'rsatilgan baza yuklana boshlaydi va shuning bilan antivirus dasturi bazasini yangilash tugatiladi.

Dastur yordamida virusni tekshirish

Buning uchun Kasperskiy antivirusi asosiy oynasidan **Поиск вирусов** bo'limi tanlanadi va tekshirilishi kerak bo'lgan ob`ektlar tanlanib **Запустить проверку** bosilib viruslardan tekshiriladi.



Boshqacha usulda ham viruslarni tekshirish mumkin. Buning uchun biror faylni, papkani, disk bo'limini yoki ma`lumot tashish vositalarini ustida sichqoncha o'ng tugmasi bosilib **Проверить на вирусы** tanlanadi.

Topshiriqlar:

1. Virus nima va uning kompyuterga qanday salbiy ta`sirlarini bilasiz ?
2. Xozirgi kunda qanday antivirus dasturlari mavjud va ularni farqi nimada?
3. Kompyuteringiz ximoyasi uchun qaysi antivirus dasturidan foydalanasiz, nima uchun (uning afzallik tomonlarini tushuntirib bering).
4. Amaliyotda Kasperskiy antivirusini o'rnatib bazasini yangilang va komyuterni viruslardan tekshirish malakasini o'rganing xosil qiling.
5. Qanday xavfli kompyuter viruslarini bilasiz va xavfli omillarini gurux doirasida muxokama qiling.

Amaliy ish №3

Mavzu: Tashqi qurilmalarni bevosita mahalliy tarmoqqa ulash va nosozlarini almashtirish jarayoni.

Ishdan maqsad: *Tashqi qurilmalarni bevosita mahalliy tarmoqqa ulash, nosozlarini almashtirish jarayoni haqida nazariy ma`lumotlarga ega bo'lish. Tajribada nosozlarini almashtirish.*

I. Nazariy qism.

Mahalliy hisoblash tarmog'ining apparat ta`minoti

Mahallliy hisoblash tarmoq qurilmalari abonentlar o'rtasidagi real aloqani ta`minlab beradilar. Tarmoqni loyihalashtirish bosqichida qurilmalarni tanlash juda katta ahamiyatga ega, chunki qurilmalarni narxi umumiy tarmoq narxining katta qismini tashkil qiladi. Aloqa qurilmalarini o'zgartirish esa, nafaqat qo'shimcha mablag'ni talab qiladi, yana qiyin ish hajmini oshishga ham sabab bo'ladi.

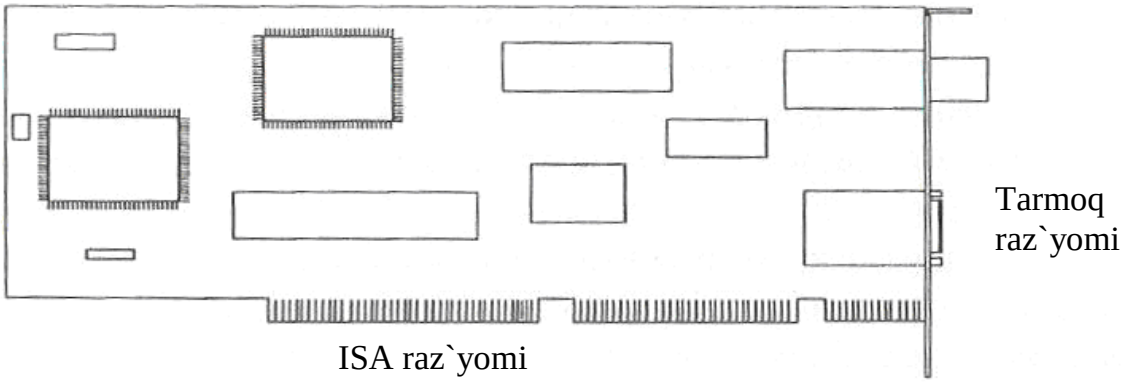
Mahalliy tarmoq qurilmalariga quyidagilar kiradi:

- axborot uzatish uchun kabellar;
- kabellarni ulash uchun razemlar;
- moslovchi terminatorlar;
- tarmoq adapterlari;
- repiterlar;
- transiverlar;
- konsentratorlar;
- ko'priklar ;
- yo'naltirgichlar (marshrutizatorlar);
- shlyuzlar.

Ularni ba`zilarini ko'rib chiqamiz.

Tarmoq adapterlarini turli adabiyotlarda yana kontroller, karta, plata, interfeyslar, NIC (Network Interface Card) nomlari bilan ham ataydilar. Bu qurilmalar mahalliy tarmoqning asosiy qismi, ularsiz tarmoq hosil qilish mumkin emas. Tarmoq adapterlarining vazifasi – kompyuterni (yoki boshqa abonentni) tarmoq bilan ulash, yana qabul qilingan qoidalarga rioya qilgan holda kompyuter bilan aloqa kanali o'rtasida

axborot almashinuvini ta`minlashdir. Aynan shu qurilmalar OSI modelining quyi bosqichlari bajarishi kerak bo'lgan vazifalarni amalga oshiradi. Odatda tarmoq adapterlari plata ko'rinishida ishlab chiqariladi va kompyuterni sistema magistrallarini kengaytirish uchun qoldirilgan razemga o'rnatiladi (odatda ISA yoki PSI). Tarmoq adapter platasida ham odatda bitta yoki bir nechta tashqi razemlar bo'lib, ularga tarmoq kabellari ulanadi (1-rasm).



1-rasm. Tarmoq adapteri platasi

Tarmoq adapterlarining hamma vazifalari ikkiga bo'linadi :
1) magistral
2) tarmoq.
Magistral vazifalari adapter bilan kompyuterning sistema shinasi o'rtasidagi almashinuvni amalga oshirish (ya`ni o'zining magistral manzilini tanish, kompyuterga axborot uzatish va kompyuterdan axborot qabul qilish, kompyuter uchun uzilish signalini hosil qilish va hokazolar) kiradi.
Tarmoq vazifalari esa adapterlarni tarmoq bilan muloqotini bilan ta`minlashdir.

Kompyuter tarkibida adapter platasini ravon ishlashi uchun uning asosiy ko'rsatkichlarini to'g'ri o'rnatish kerak :
a) kiritish-chiqarish portining asos manzilini (ya`ni manzil maydonining boshlanish manzilini, u orqali kompyuter adapter bilan muloqot qiladi) ;
b) foydalaniladigan uzilish nomeri (ya`ni taqiqlash yo'lining nomeri, u orqali kompyuterga adapter o'zi bilan axborot almashinuvi zarurligi haqida xabar beradi) ;
c) bufer hamda yuklanuvchi xotiralarning asos manzili (ya`ni adapter tarkibiga kiruvchi kompyuter aynan shu xotira bilan muloqot qilishi uchun).

Bu ko'rsatkichlarni foydalanuvchi tomonidan adapterdagi ulash moslamasi (jamper) yordamida tanlab o'rnatish mumkin, lekin plata beriladigan maxsus adapterni initsializatsiyalovchi dastur yordamida ham o'rnatish mumkin. Hamma ko'rsatkichlarni (manzil va uzilish

nomeri) tanlashda e`tibor berish kerakki, ular kompyuterning boshqa qurilmalarida o'rnatilib band bo'lgan ko'rsatkichlaridan farq qilishi kerak. Hozirgi zamon tarmoq adapterlarida ko'pincha Plug-and-Play tartibi qo'llaniladi, ya`ni ko'rsatkichlarni foydalanuvchi tomonidan o'rnatilishining (sozlashning) hojati yo'q, ularda sozlash kompyuter elektr manbaiga ulanganda avtomatik ravishda amalga oshiriladi.

Adapterning asosiy tarmoq vazifalariga quyidagilar kiradi :

- ✓ kompyuter va mahalliy tarmoq kabelini galvanik ajratish (buning uchun odatda signalni impuls transformatori orqali uzatiladi) ;
- ✓ mantiqy signallarni tarmoq signallariga va aksiga o'zgartirish ;
- ✓ tarmoq signallarini kodlash va dekodirlash ;
- ✓ qabul qilinayotgan paketlardan aynan shu abonentga manzillashtirilgan paketlarni tanlab qabul qilish ;
- ✓ parallel kodni ketma-ket kodga axborot o'ztilishda o'zgartirish va axborot qabul qilishda aksiga o'zgartirsh ;
- ✓ adapterning bufer xotirasiga uzatilayotgan va qabul qilinayotgan axborotlarni yozish ;
- ✓ qabul qilingan axborot almashinuvini boshqarish usulida tarmoqqa ega bo'lishni tashkil qilish ;
- ✓ axborotlarni qabul qilish va uzatishda paketlarning nazorat bitlari yig'indisini hisoblash.

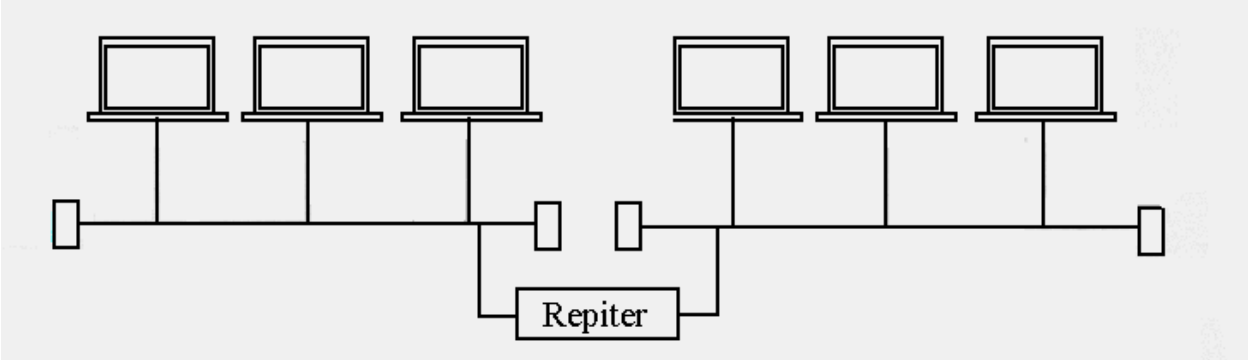
Odatda hamma tarmoq vazifalari maxsus katta integral sxemalar yordamida amalga oshirilganligi uchun adapter platasining o'lchami kichik va narxi arzondir.

Agarda tarmoq adapteri bir necha turdagi kabellar bilan ishlay olsa, u holda yana bir sozlanishi lozim bo'lgan ko'rsatkich qo'shiladi (kabel turini tanlash). Masalan, adapter platasida u yoki bu turdagi kabelga ulash uchun moslama (peremьichka) bo'lishi mukin.

Adapterdan boshqa hamma mahalliy tarmoq qurilmalari yordamchi qurilmalar bo'lib, ko'pincha ularsiz ham ishni tashkil qilish mumkin. Transiverlar yoki uzatish va qabul qilish qurilmalari (Transmitter-Receiver, priemoperedatchiki), ular adapter bilan tarmoq kabeli o'rtasidagi axborotni uzatish uchun xizmat qiladilar yoki tarmoqning ikki qismlari (segment) o'rtasidagi axborot uzatishni amalga oshiradilar. Transiver signalni kuchaytirish, signal qiymatlarini o'zgartirish yoki signal ko'rinishini o'zgartirish (masalan elektr signalni yorug'lik signaliga va teskarisiga) ishlarini bajaradi. Ko'pincha adapter platasiga o'rnatigan qabul qilish va uzatish qurilmasini transiver deb ham yuritiladi.

Repiterlar yoki qaytaruvchi (repeater, povtoritel) qurilmasi transiverga nisbatan ancha oddiy vazifani bajaradi. U faqat susaygan signalni qayta tiklab avvalgi, ya`ni uzatilgan vaqtdagi ko'rinishga (amplitudasi va ko'rinishini) keltiradi. Signalni qayta tiklashning asosiy maqsadi, tarmoq uzunligini oshirishdan iborat (2-rasm). Lekin repiterlar ko'pincha boshqa vazifalarni ham bajaradilar, masalan, tarmoqqa ulanadigan

qismlarni galvanik ajratish. Repiterlar va transiverlar hech mahal o'zidan o'tayotgan axborotga hech qanday ishlov bermaydilar.



2-rasm. Tarmoqning ikki bo'lagini repiter yordamida ulash

Yo'naltirgichlar – har bir paket uchun qulay uzatish yo'lini tanlab, uzatuvchi qurilma. Buning uchun tarmoqning eng ko'p yuklangan qismlarini va buzilgan qismlarini aylanib o'tishi kerak. Ular odatda murakkab shoxlamali tarmoqda ishlatiladi, bu holda alohida olingan abonentlar o'rtasida bir necha aloqa yo'li mavjud bo'lishi mumkin.

Informatsion texnologiyalarda port va uning vazifalari

Informatsion texnologiyalarda port – bu yuborilayotgan va qabul qilinayotgan axborotlar o'rtasidagi bog'lanishni tashkil etadi (mantiqiy yoki fizik) odatda quyidagilar:

Qurilmali (apparatli) portlar – bu asosan kompyuterning fizik qurilmasi bo'lib u asosan vilka yoki kabel yordamida kompyuterga bog'lanadi.Ularga quyidagilar kiradi:

Parallel port, Davomli port, USB, ATA/SATA, IEEE 1384 (FireWire), PS/2

Kiritish- chiqarish porti – mikroprotsessorlarda (masalan Intel) qurilmalar yordamida ma`lumotlar almashish imkonini beradi. Kiritish-chiqarish porti dasturga ma`lumotlar berish va uni almashishni tashkil etadi.

Tarmoqli port – TCP va UDP protokol parametrlari bo'lib u IP formatidagi mahlumotlar paketi qo'llanilishini aniqlaydi.

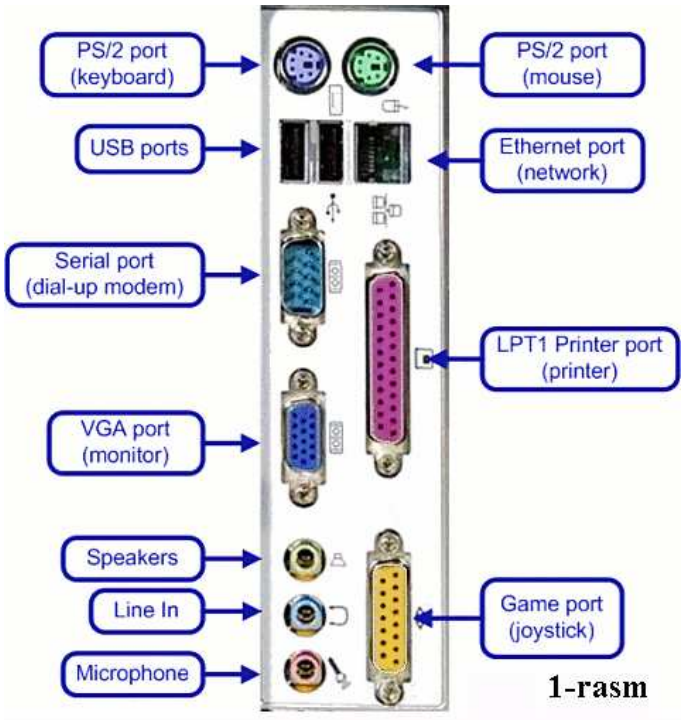
1 

2 

Kompyuterning tashqi qurilmalari bilan axborot almashishi jarayonini, kompyuterning tashqi interfeysi tashkil qiladi. Tashqi interfeys tashqi portlar, shinalar, kompyuterlar birlashmasi va tashqi qurilmalar jamlamasidan iboratdir. Asosan kompyuter va tashqi qurilmalarni bir-biriga bog'lashda shinalardan foydalaniladi.

Kompyuterga printer, skaner, sichqoncha, klaviatura va shunga o'xshash qurilmalarning kompyuterga ulanishi tashqi interfeysga misol bo'ladi. Tashqi interfeysni amalga oshirish uchun unga apparat va dasturiy ta`minot: tashqi qurilmani boshqaruvchisi (controller) va kontrollerni boshqaruvchi maxsus dastur, drayver (driver) kerak bo'ladi.

Har qanda kompyuterda tashqi interfeys bir qancha portlar, jumladan, LPT, PS/2, COM, USB, ...kabilar orqali amalga oshiriladi. (1-rasmga qarang). Har bir portning o'ziga yarasha vazifasi bor.



1-rasm

IEEE 1284 (Printer port, parallel port, LPT) – shaxsiy kompyuterga ulashga mo'ljallangan xalqaro parallel interfeys standartiga mos tushuvchi qurilma. "LPT " nomi MS DOS oilasidagi operatsion tizimdagi " LPT 1" (Line Printer Terminal yoki Line PrinTer) standart nomidan kelib chiqqan. Hozirgi vaqtda bu interfeys asosan USB interfeysi bilan mos tushadi va u yig'ma apparatlarni (skaner – printer - kserokopiya) ulash uchun ishlatiladi. Lekin asosan yuqori tezlikda chop etish va printer uchun ishlatiladi. Bu bilan asosan Cetronics, Betronics, HP, Hewlett-Packard firmalari tomonidan ishlab chiqariladi. Ular 1284.3-2000 va 1284.4-2000 standartiga asoslangan. Ishchi rejimlari

SPP (Standart Paralell Port) — bir yo'nalishli port, to'laligicha Cetronics interfeysi bilan mos tushadi.
Nibble Mode — SPP rejimida ikki yo'nalishli ma`lumotlar almashinishga asoslangan (4 baytli) qo'shimcha qurilmalar bilan jihozlangan
Byte Mode — Ba`zida qo'llaniluvchi IEEE 1284 standartiga asoslangan eski kontrollerlardan ikki tomonlama ma`lumot almashish uchun foydalaniladi.
EPP (Enhanced Parallel Port) —ishchi qurilma Intel, Xircom va Zenith Data **Systems** — firmalariga tegishli ikki tomonlama ma`lumot almashish, 2 Mbayt/sekund tezlikda
ESR (Extended Capabilities Port)— ishchi qurilma Hewlett-Packard va Microsoft kompaniyalari, qo'shimcha ravishda ma`lumotlarni siqish appatiga ega va DMA rejimida ishlovchi qurilma
Tarmoq kommutatori (TCP/IP port) yoki svitch (switch - qo'shmoq, qayta ulagich)- kompyuter tizimlarida bir necha uzellarni bir segmentda birlashtirish uchun mo'ljallangan qurilma. Konsentratorlardan asosiy farqi bitta qurilmaga berilgan ma`lumotlar kommutator orqali boshqa kommutatorlarga uzatiladi. Kommutatorlar OSI modelining kanal rejimida ishlaydi va bir- bir biriga MAC adresslari orqali uzellar bir tarmoqqa bog'lanadi. Bir necha tarmoqlarni birlashtirish uchun tarmoq darajali marshrutizatorlardan foydalaniladi.

Yuqorida keltirilgan port va kommutatorlar orqali mahalliy tarmoqqa qo'shimcha qurilmalar ulanadi. Bunday qurilmalardan ommalashganlari modem, printer va veb kameradir.

Modem qurilmasi va uning vazifalari.

Hozirda kompyuterlar o'rtasida telefon liniyasi yordamida aloqa o'rnatilgan. Bu aloqani o'rnatish uchun maxsus qurilma talab qilinadi. Bu qurilmani vazifasi telefon liniyasi orqali olingan signalni raqamli signalga aylantirish, kirishda esa teskari operatsiyani amalga oshirishdan iborat. Demak u modulyatsiya va demodulyatsiya operatsiyalarini bajarishi kerak. Shuning uchun qurilma Modem nomini olgan.

Modemni vazifasi kompyuterdan kelgan "0" va "1" lardan iborat raqamli signalni akustik diapazondagi elekr tebranishiga aylantirib uzatish va teskari operatsiyani bajarishdir.

Modem akustik kanalni past va yuqori chastotali polosalarga bo'ladi. Past chastotali polosa informatsiya uzatish, yuqori chastotali palosa informatsiyani qabul qilish uchun qo'llaniladi.
Informatsiyalarni kodlashtirishni ko'p yo'llari mavjud. Ulardan keng tarqalgani FKS (Frequency Shift Keying) usuli. U 300 bod (1 bod=1 bit/c) tezlikda informatsiya uzatilishiga mo'ljallangan.

RSK (Rhase Shift Keying) yetarli katta tezlikda ishlovchi modemlari uchun, informatsiya uzatish tezligi 2400 bodgacha.

FSK to’rtta ajratilgan chastotalarni qo’llaydi. Informatsiya uzatishda 1070 Gts chastotali signalni “nol” deb, 1270 Gts li signalni logik “bir” deb tushuniladi.Qabul qilishda esa nolga 2025 Gts, birga 2225 Gts chastotali signallar mos keladi.

RSK esa ikkita chastotani ishlatadi: Informatsiya uzatish 2400 Gts, qabul qilish uchun 1200 Gts. Informatsiya ikki bitdan uzatiladi, bu yerda kodlash faza surilishi bilan amalga oshiriladi. 0 gradus “00” uchun, 90 gradus “01”, 180 gradus “10”, 270 gradus “11” larni belgilaydi.

Bulardan tashqari boshqa modullashlar ham bor. Model tashqi yoki ichki bo’lishi mumkin. Tashqi modelni bitta kabeli telefon liniyasiga, ikkinchi kabeli esa kompyuterning standart COM portiga ulanadi.

Ichki modem esa oddiy platadan iborat bo’lib umumiy shinaga ulanadi.

Modemni tashkil etgan qurilmalar.

Modem kontrolleri kichik maxsus kompyuter bo’lib tipi SC 1107 yoki SC 1108. U 8 razryadli arifmetik – logik qurilma, 8 Kbayt doimiy xotira, 128 baytli operativ xotira, taymer, buyruq registri, to’xtalish kontrolleri, kiritish va chiqarish portlariga ega.

Eng ko’p tarqalgan modemlardan biri HAYES bo’lib, ishlab chiqargan firma nomi bilan yuritiladi. Bu modemlar AT (Attention) buyruqlarni qo’llaydi. AT komandalari boshqa modemlarga ham mos keluvchi hisoblanib, ko’p sondagi buyruqlarni o’z ichiga oladi.

Modemda qo’llanilayotgan buyruqlar boshqa modemlarga ham mos kelishidan tashqari, telefon liniyasida uzatilayotgan informatsiya kodi (signali) biror xalqaro standartga mos kelishi kerak. Bunday standart MK KTT (xalqaro telegraf va telefon konsultativ komiteti) CCITT(Comit Consultariv International Telegrarhique et Telerhonique) rekomendatsiyasidir. AQSH va Kanadada yuqoridagi singari standart bo’lib uning nomi Bell. Uni SSITT dan farqi faqat logikdir.

Informatsiya almashinuvi 2400 bod gacha, modemlar standartga mos keluvchilari erkin informatsiya almashadi. Tezligi 2400 boddan ortiq bo’lgan modemlarda standartdan chetlanishlari mavjud bo’ladi. Bu chetlanishlar maxsus ilova protokolida keltiriladi.

Keng tarqalgan va arzon modemlarga misol qilib Srort, Worldrort, Courier larni keltirish mumkin. Ularni ishlash tezligi 9600 dan 21600 bod gacha. Bundan tashqari Zy XEL firmasi modemlarni ham keng tarqalgan. U o’zini protokoliga ega bo’lib informatsiya almashinuv tezligi 19200 bod ga teng.

Keng tarqalmagan, qimmat lekin kuchli, turg’un signalli, himoya filtrlarni ham e`tiborga olmaydigan Telebit firmasi modemlari TraiBlazer ham mavjud.

Ba`zi kuzatiladigan xatoliklar va ularni bartaraf etish.

Kuzatilgan xatoliklarni aniqlanish usullaridan biri yangi o’rnatilgan qurilmalarni qattiqroq rejimda ishlatishdir. Chunki kompyuterning hamma qurilmalari zavod tomonidan sinab ko’rilgan bo’lib, undan tashqari amaliyotni ko’rsatishiga kompyuterlarni elektron qurilmalarida buzuqliklar bo’lsa, u birinchi 90 soat kompyuterni ishlashida bilinadi.

Agar kompyuter birinchi uch kun ichida normal ishlasa uning qurilmalarida buzuqliklar 1-2 yil ekspluatatsiya davomida kuzatilmaydi.

Ma`lumki har safar kompyuter ishga tushirilishi bilan ROST dasturi ishga tushib kompyuter asosiy qurilmalarini ish faoliyatini test orqali tekshiradi. Agar biror xatolik kuzatilsa, u to’g’risida xabar berib xatolik kodini ko’rsatadi. Foydalanuvchi xatoliklar jadvalidan kodga mos kelgan xatolik sababini olib tuzatishi mumkin. Bundan tashqari kompyuter elektr tarmog’iga ulanishi yoki qayta yuklatish bilan biror xatolik (biror qurilma ulanmasa yoki ishlamasa) boshqa turdagi ovoz signali chiqishi bilan bildiriladi.

Eng ko’p xatoliklar kompyuter qurilmalarini takomillashtirishda kuzatiladi. Demak bu xollarda kuzatiladigan xatolikni tuzatish oson bo’ladi.

Agar kompyuter tarmoqga ulanishi bilan monitor ekraniga hech qanday ma`lumot chiqmasa, kompyuter qurilmalarini aniq ketma-ketlikda almashtirib ko’rish maqsadga muvofiq. Chunki kompyuter qurilmalari modul sifatida qurilgan bo’lib ularni olib qo’yish oson.

Ko’p xollarda yangi qurilma qo’yilganda undagi yoki asosiy platadagi DIR-pereklyuchatellari yangi qurilmaga mos kelmasligi mumkin.

ROST dasturi ko’rsatgan xatoliklarni ba`zi sabablari:
101-sistema platasi ishlamasligi;
102-BIOS ROM da nazorat summasida xatolik;
104-to’xtatish nazoritidagi xatolik;
105-taymerdagi xatolik;
106-sistema platasidagi xatolik;
107-sistema platasi, yoki matematik soprotsessor xatoligi.

II. Amaliy qism.

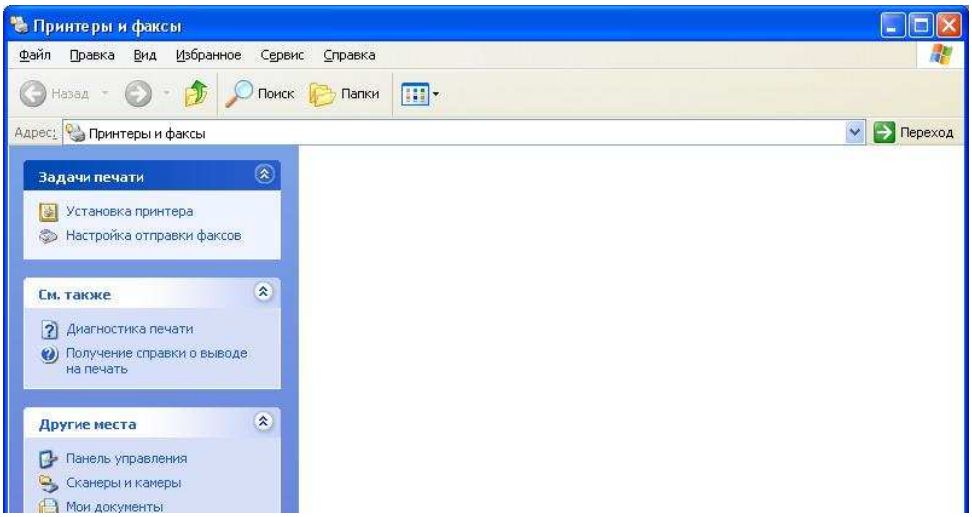
Mahalliy tarmoq printeridan foydalanish

Mahalliy tarmoq printeri bu mahalliy tarmoqqa ulangan kompyuterlardan chop etish uchun ma`lumotlar qabul qiluvchi, chop etuvchi qurilma hisoblanadi. Ushbu amaliyotda biz qanday qilib mahalliy tarmoq printeriga ma`lumot jo’natish va chop etish jarayonlarini o’rganamiz.

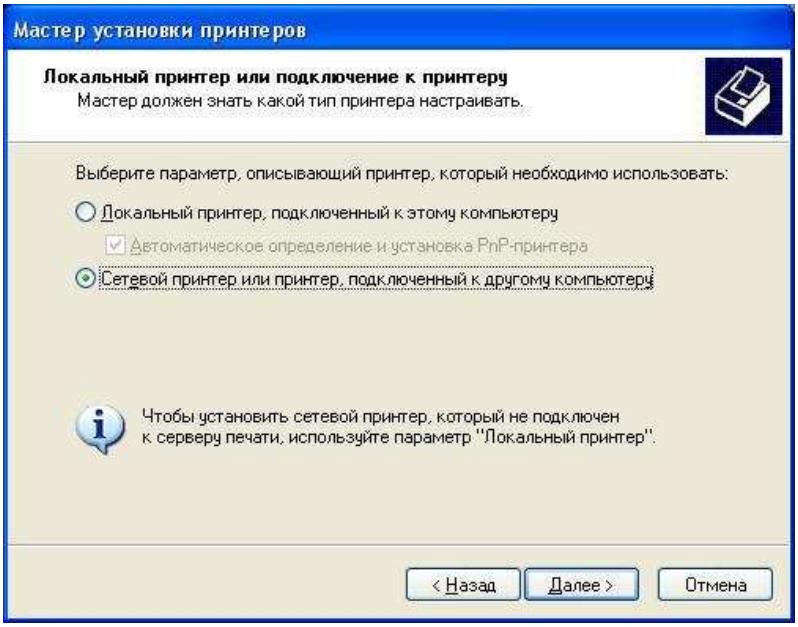
Buning uchun bizning kompyuterimiz mahalliy tarmoqqa ulangan bo’lishligi va printer ulangan komyuterdan bizga foydalanishga ruxsat (dostup) bo’lishligi lozim.

Mahalliy tarmoq printeriga bog’lanishni 2 xil turini ko’rib chiqamiz.

Dastlab bizni kompyuterimizda biror printerga bog'lanish borligini bilish uchun **Пуск→ Принтьеры и факсы** ёки→**Пуск Панел управления Принтьеры и факсы** bo'limiga kiramiz.

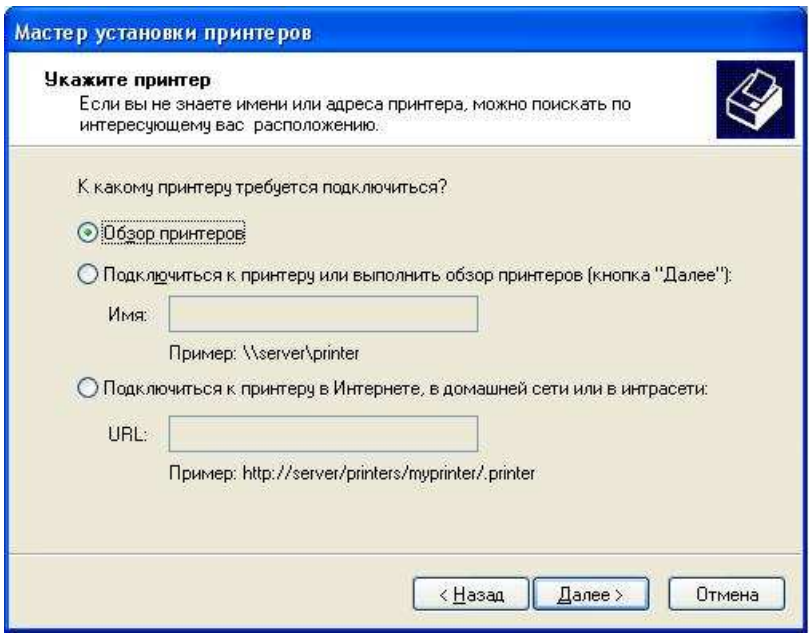


Ochilgan oynadan **Устьановка принтьера** ustida sichqoncha chap tugmasini ikki marta bosamiz. Natijada bizga printerlar o'rnatish ustasi oynasi ochiladi. **Далее** tugmasi bosib printer o'rnatish jarayonini boshlaymiz. Xosil bo'lgan oynada printer o'rnatishni ikki turini:
Kompyuterga ulangan printerni va tarmoq yoki boshqa kompyuterga ulanan printerni o'rantishni so'raydi. Biz **Сетьевой принтьер или принтьер, подключенный к другому компютьеру** tanlaymiz va Далее tugmasini bosamiz.

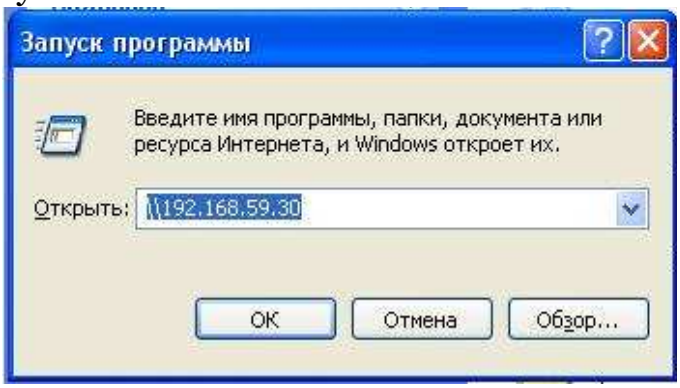


Ochilgan oynada bizga qaysi turdagi printerga ulanish so'raladi. Bunda

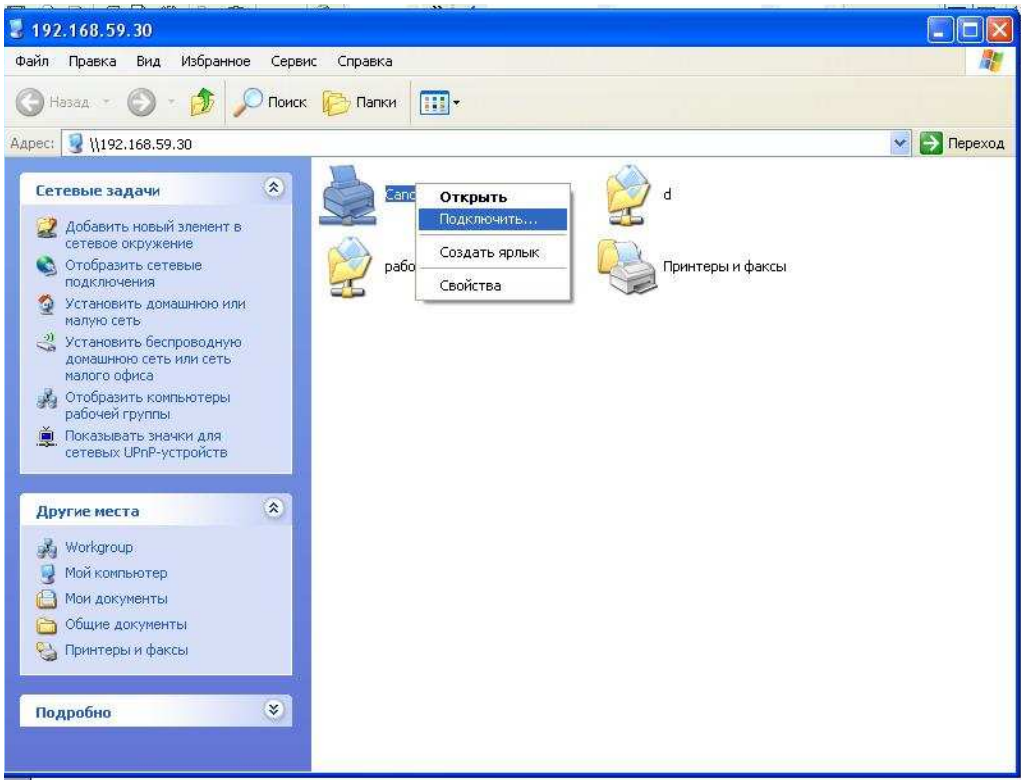
1) Printerlarni avtomatik qidirish
2) Printer ulangan kompyuter nomi yoki IP raqami orqali ulanib topish
3) Internet ulanish orqali topish shartlari qo'yiladi.



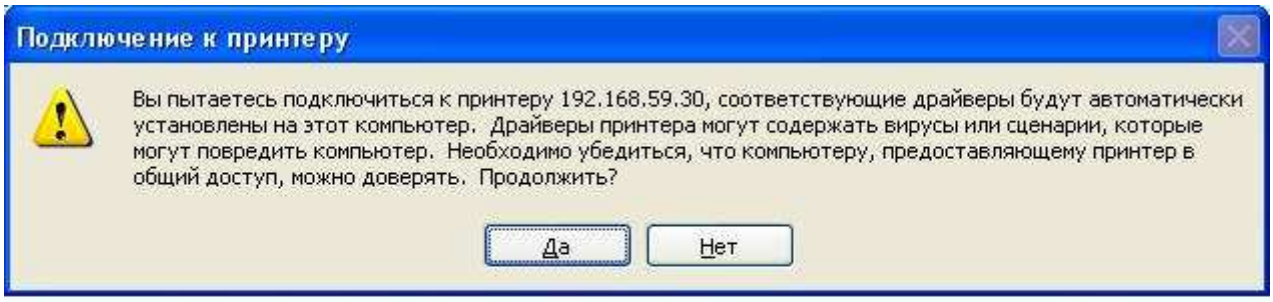
Biz ikkinchisini tanlaymiz av printer mavjud bo'lgan kompyuterni IP raqamini va printerniturini yozamiz. Misol uchun o'sha IP 192.168.59.30 va printer nomi CanonLBP2900 bo'lsin u holda Imya bandiga quyidagicha yozidladi:
\\192.168.59.30\ CanonLBP2900 ni yozib Далее tugmasini bosamiz va keyingi ochilgan oynalar so'rovlarini tasdiqlaymiz.
Ikinchi usulda oldin printerga foydalanishga ruxsat etilgan IP manziliga kiramiz. Buning uchun **Пуск →Выполнить** amallar ketma-ketligini bajaramiz. Ochilgan oyna maydoniga yuqoridagi IP manzilni, ya`ni \\192.168.59.30 ni yozamiz.



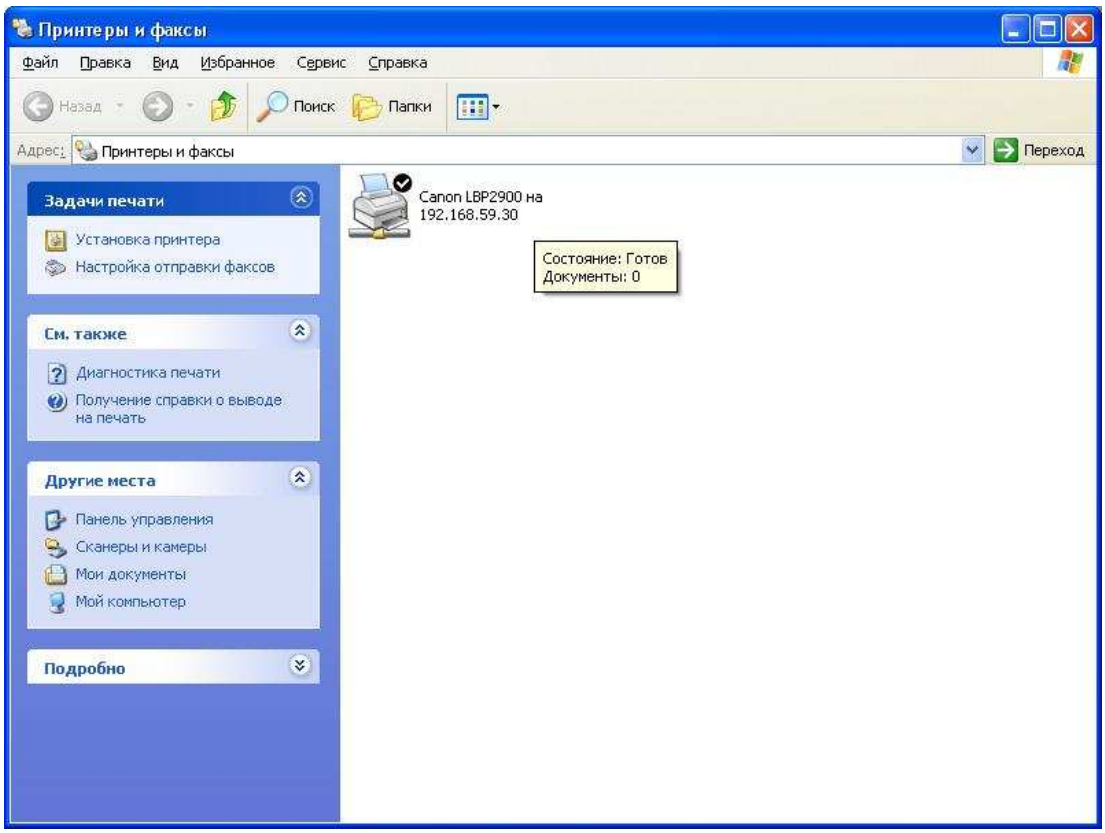
Ochilgan oynada o'rnatilgan printer nomi mavjud bo'ladi (bizda printer nomi CanonLBP2900). Uning ustida sichqoncha o'ng tugmasini bosamiz va undan **Подключить** tanlaymiz.



Ochilgan so’rov oynasida **Да** ni bosamiz. Bunda biz ulangan printer drayverlari avtomatik tarzda kompyuterimizga o’rnatiladi. Shuning bilan kompyuterimiz mahalliy tarmoq printeridan ulandi endi tayyorlagan ma`lumotlarimizni kompyuterimizdan turib ushbu printerda chop qila olamiz.



Kompyuterga haqiqatda ham printer o’rnatilganligini tekshirish uchun yana →**Пуск Принтьеры и факсы** ga kiramiz. 192.168.59.30 IP dagi CanonLBP2900 printeriga ulanganlik yorlig’i xosil bo’ldi.



Kompyuterimizda ushbu printerda ma`lumotlarni chop etish uchun ma`lumotni chop etishga berayotganda ushbu printerni tanlash kifoya.

Topshiriqlar:

1. Mahalliy tarmoq qurilmalari haqidagi nazariy ma`lumotlarni o'qib chiqing va bu qurilmalarni vazifalarini tushuntiring.
2. Tarmoq adapteri haqida ma`lumot bering.
3. Modem nima va uning vazifalari haqida so'zlang.
4. Mahalliy tarmoq printeri haqida ma`lumot bering.
5. O'rgangan bilimlaringiz asosida mustaqil, mahalliy tarmoqda mavjud bo'lgan birorta printerga ulaning va maelumot eting.