Amaliy mashg`ulotlar

Mavzu: № 1 Personal kompyuterning tavsiflarini aniqlash.

Reja

1. **Personal kompyuterningkelib chiqish tarixi.**
2. Shaxsiy kompyuterni funksional tavsiflari
3.

1969 yilda mikroprotsessorning (MP) kashf qilinishi 70-yillarda EHM ning yana bir sinfi-mikro EHM ning paydo bo'lishiga olib keldi. Aynan shu MP ning borligi avvaliga mikro EHM ni aniqlovchi belgisi bo'lib xizmat kildi. Hozirda mikroprotsessorlar hamma sinfcagi EHM larda ishlatilmoqda.

Mikro EHM quyidagilarga bo'linadi: Ko'p foydalanuvchili mikro EHM-bu kuchli mikro EHM bo'lib, u bir nechta videoterminal bilan jixozlangan va vaqtning bo'linish rejimida ishlaydi, bu esa ularda birdaniga bir nechta foydalanuvchi samarali ishlashini ta'minlaydi.

SHaxsiy EHM bir odam foydalanadigan mikro EHM bo'lib, qo'llanishda umumiy murojaat qilish va universallik talablarini qondiradi.

Ishchi stanciyalar hisoblash tarmoqlarida aniq ishlar turini bajarish uchun mo'ljallangan bir odam foydalanadigan mikro EHM ko'rinishiga egadir.

Serverlar-hisoblash tarmoqdagi ko'p foydalanuvchili kuchli mikro EHMlar bo'lib, ular maxsus ish turlarini va tarmoqning barcha stanciyalaridan so'rovlarni qayta ishlashni bajarish uchun ajratilgan.

Albatta, yuqorida keltirilgan tasnif nisbatan shartlidir, negaki muammoga mo'ljallangan dasturlar va apparat ta'minoti bilan jixozlangan kuchli zamonaviy EHM to'laqonli ishchi stanciya sifatida ham, ko'p foydalanuvchili mikro EHM sifatida ham, yaxshi server sifatida ham ishlatilishi mumkin, u o'zining tavsiflari bo'yicha deyarli kichik EHM lardan qolishmaydi.

Shaxsiy EHM yoki boshqacha aytganda, shaxsiy kompyuter (SHK) aslida o'zi nima ?

Qo'llashning universalligini va umumiy murojaat qilish talablarini qondirish uchun shaxsiy EHM quyidagi sifatlarga ega bo'lishi kerak:

• SHK ning shaxsiy sotib oluvchi uchun olsa bo'ladigan oraliqlarda joylashgan kam baxosi;
• atrof - muxit sharoitlariga maxsus talablar quyilmasdan, avtonom ishlatish;
• boshqarish, fan, ta'lim, maishiy xizmat sohasidagi turli xil qo'llanishlarga SHK moslashishini ta'ninlovchi arxitekturaning moslashuvchanligi;
• SHK bilan foydalanuvchining maxsus kasbiy tayyorgarligisiz ishlash imkoniyatini beradigan operatsion tizimning va boshqa dasturli ta'minotning "do'stona" munosabatdaligi;
• yuqori ish ishonchliligi (5000 soatdan ko'proq buzilmasdan beto'xtov ishlay olishi).

Xorijiy SHK orasida birinchi navbatda Amerikaning IBM (International Busieness Mashine Corporation) firmasi kompyuterlarini ta'kidlash kerak:
• IBM PC XT (Personal Computer extended Technology);
• 80286 (16 razryadlik) mikroprotsessorlaridagi (MP) IBM PC AT (Personal Computer Advanced Technology);
• IBM PS/28030-PS/28080 (PS - Personal System, PS/28080 dan boshqa hammasi-16 razryadlik, PS/28080 esa 32 razryadlik);
• IBM PC - 80386 va 80486 (32-razryadlik) MP dagi;
• IBM PC-Pentium va Pentium Pro (64 razryadlik) MP dagi.

Amerikaning Compaq Computer, Apple (Macintosh), Hewlet Packard (HP), Dell, DEC hamda Buyuk Britaniyaning Spectrum, Amstrad, Franciyaning Micral, Italiyaning Olrvetty, YAponiyaning Toshiba, Panasonic va Partner firmalari ishlab chiqarayotgan shaxsiy kompyuterlar keng ma'pumdir.

IBM firmasining birinchi modellari 1981 yilda paydo bo'lgan shaxsiy kompyuterlari va boshqa firmalarning bunga analoglari hozirgi vaqtda eng ommaviydir; ommaviylik bo'yicha Apple va DEC (Digital Equipment Corporation) firmalarining SHK lari ulardan ancha orqada koddi, ular tarqalganligi bo'yicha 2-o'rinni egallaydilar.

90-yillarning boshlarida kompyuterlarning jahon parki taxminan 150 mln donani tashkil etdi, ulardan 90% dan ortiqrog'i bu shaxsiy kompyuterlar, xususan, IBM PC tipidagi kasbiy SHK lari 10 mln

donadan ortiqroq (hamma SHEHM larning 75% ga yaqini); Apple va DEC tipidagi kasbiy SHK lar 5 mln donadan ortiqroq. Hozirgi vaqtda kompyuterlarning soni taxminan uch marta ko'paydi.

Xorijda hozirgi vaqtda kompyuterlarni eng ko'p tarqalgan modeli bo'lib Pentium va Pentium Pro mikroprotsessorli IBM PC kompyuterlari hisoblanadi.
Hozirgi vaqtda Rossiyadagi ko'p sonli kompyuter firmalari chet el elementlaridan asosan IBM SHKlari bilan ishlaydigan kompyuterlarni yiqish bilan shug'ullanmoqdalar.

Avlodi bo'yicha shaxsiy kompyuterlar quyidagicha:
1-avlod SHK: 8-bitlik mikroprotsessordan foydalanadi;
2-avlod SHK: 16-bitlik mikroprotsessordan foydalanadi;
3-avlod SHK: 32-bitlik mikroprotsessordan foydalanadi;
4-avlod SHK: 64-bitlik mikroprotsessordan foydalanadi.

Shaxsiy kompyuterni funksional tavsiflari
1. Tezkorligi, unumdorligi, taktli chastotasi.
Zamonaviy EHM larning unumdorligi odatda sekundiga millionta amal bilan o'lchanadi. O'lchov birligi bo'lib quyidagilar xizmat qiladi:

NIPS (MIPS-Mega Inctruction Per Second)-qayd qilingan vergul (nuqta) shaklida tasvirlangan sonlar ustida amallar uchun;
 MfloPS (MfloPC-Mega Flops Per Second)-ko'chib yuradigan vergul (nuqta) shaklida tasvirlangan sonlar ustida amallar uchun quyidagi o'lchov birliklari kamroq ishlatiladi:
 KOPS (KOPS-Kilo Operation Per Second)-past unumlilar uchun-sonlar ustida mingta qandaydir o'rtacha amallar;
GfloRS (GfloPC-Giga Flops Per Second)-ko'chib yuradigan vergulli sonlar ustida sekundiga milliard amal.

EHM unumdorligini baholash har doim taxminiydir, negaki qandaydir o'rtacha yoki, aksincha, aniq bir amallar turiga mo'ljallanadi. Haqiqatda turli masalalar echishda turli xil amallar to'plami ishlatiladi. SHuning uchun SHK tavsifi uchun unumdorlik o'rniga, odatda, mashina tezkorligini yanada ob'ektivroq aniqlaydigan taktli chastota ko'rsatiladi, chunki har bir amal o'zining bajarilishi uchun to'liq aniqlangan sondagi taktlarni talab qiladi. Taktli chastotani bilgan holla istalgan mashina amalining bajarilish vaqtini etarlicha to'liq aniqlash mumkin.

Misol. Buyruqlarni konveyerli bajarish bo'lmaganda va mikroprotsessorning ichki chastotasi oshirilganda 33 MGc chasgotali taktli generator sekundiga 7 mln ta qisqa mashina amallarini (oddiy qo'shish va ayirish, ma'lumotni jo'natish va b.), 100 MGc chasgotali generator sekundiga 20 mln ta qisqa amallarni bajarishni ta'minlaydi.

2. Mashina va interfeys kodli shinalarning razryadliligi.

Razryadlilik-bu ikkilik sonning bir vaqtning o'zila mashina amali, shu jumladan ma'lumotni uzatish amali, bajarilishi mumkin bo'lgan razryadlari maksimal miqdori, razryadlilik qanchalik katta bo'lsa, turli xil tent sharoitlarda SHK unumdorligi shunchalik yuqori bo'ladi.

3. Tizimli va lokal interfeys tiplari.

Turli interfeys tiplari mashina uzellari orasidagi turli ma'lumotlarni uzatish tezligini ta'minlaydi, tashqi qurilmalarning turli miqdorlarini va ularning turli ko'rinishlarida ulanishiga imkon beradi.

4. Tezkor xotira sig'imi.

Tezkor xotira sig’imi ko’pincha Mbaytlarda, kamroq hollarda Kbaytlarda o’lchanadi. Eslatib o’tamiz, 1 Mbaytq1024 Kbaytq10242 bayt. Tezkor xotira sig’imi 8 Mbaytdan kam bo’lganda ko’plab zamonaviy amaliy dasturlar ishlamaydi yoki ishlasa ham juda sekin ishlaydi. Shuni hisobga olish kerakki, tezkor xotira sig’imini 2 marta oshirish, bularning hammasidan tashqari, qiyin masalalarni echishda EHM ning samarali unumdorligini taxminan 1,7 marta oshiradi.

5. qattiq, magnit disklardagi yig’uvchishshg (vinchesterning) sig’imi. Vinchester sig’imi odatda megabaytlarda yoki gigabaytlarda o’lchanadi. 1 Gigabayt q 1024 Megabayt.

6. Egiluvchan magnit disklaridagi yig’uvchilarning tili va sig’imi.

Hozir 3,5 dyuym va 5,25 dyuym diametrli disketalarni ishlatuvchi egiluvchan magnit disklaridagi yig’uvchilar qo’llanilmoqda. Birinchisi 1,44 Mbayt standart sig’imga, ikkinchisi esa 1,2 Mbayt sig’imga ega.

7. Kesh-xotira mavjudlign, turlari va sig’imi.

Kesh-xotira-bu buferli, tez harakatlanadigan, foydalanuvchi uchun tegishli bo’lmagan xotira bo’lib, sekinroq harakatlanadigan eslab qoluvchi qurilmalarda saqlanayotgan ma’lumotlar ustidagi amallarni tezlashgirish uchun kompyuter tomonidan avtomatik ishlatiladi. Masalan, asosiy xotira bilan amallarni tezlashtirish uchun mikroprotsessor ichida registrli kesh-xotira (birinchi darajali kesh-xotira) yoki mikroprotsessor tashqarisida bosh platada (ikkinchi darajali kesh-xotira) tash-kil etiladi; diskli xotira bilan amallarni tezlashtirish uchun elektron xotira yacheykalarida kesh-xotira tashkil etiladi.

SHuni inobatga olish kerakki, 256 Kbayt kesh-xotira borligi SHK unumdorligini taxminan 20% ga oshiradi.

8. Videomonitor (displey) va videoadapter tipi.
9. Printerning borligi va tipi.
10. Ixcham-disklardagi CD-ROM yig’uvchilarning borligi va tipi.
11 Modemning borligi va tipi.
12. Multimediali audio-, videovositalarning borligi va turlari.
13. Matematik soprotsessorning borligi.
Matematik soprotsessor qayd qilingan va ko’chib yuradigan vergulli ikkilik sonlar usgida va ikkilik-kodlangan o’nlik sonlar usgida amallarning bajarilishini un marta tezlashtirish imkonini beradi.

14. Bor bo’lgan dasturli ta’mnnot va operaciey tizim turi.
15. Boshqatipdagi EHM bilan apparatli va dasturli mos kelishlik.

Boshqa tipdagi EHM bilan apparatli va dasturli mos kelishlik-bu kompyuterda, mos ravishda, boshqa tipdagi mashinalarning texnik elementlarini va dasturli ta’minotini ishlatish imkoniyatini bildiradi.

16. Hisoblash tarmog’ada ishlash imkoniyati.
17. Ko’p masalalik rejimida ishlash imkoniyati.

Ko’sh masalalik rejimi, bir vaqtning o’zida bir nechta dasturlar bo’yicha (ko’p dasturli rejim) yoki bir nechta foydalanuvchilar uchun (ko’p foydalanuvchilar rejimi) hisoblashlarni bajarishga imkon beradi. Bu rejimda mashinani bir nechta qurilmalarini vaqt bo’yicha mumkin bo’lgan ishlashi EHM ni samarali tezkorligini sezilarli oshirish imkonini beradi.

18. Ishonchliligi.

Ishonchlilik-bu tizimni unga berilgan barcha vazifalarni to’liq va to’g’ri bajarish qobiliyatidir. SHK ishonchliligi, odatda, inkor qilguncha ishlashning o’rtacha vaqti bilan o’lchanadi.

19. Narxi.

20. O’lchamlari va og’irligi.

Aqliy hujum uchun savollar:

1.Jamiyatni axborotlashtirish deganda nimani tushunasiz?
2. Jamiyatning rivojlanishida axborot zahiralari qanday rol o’ynaydi?
3. "Axborot portlashi" ga nimalar sabab bo’ldi?
4. "Axborotiy zo’riqish" nima va u qanday oqibatlarga olib keladi?
5. Jamiyatni kompyuterlashtirish deganda nimalarni tushunasiz?
6. Kelajakdagi boshqarishni yoki "kelajak ofisi" ni qanday faraz qilasiz?
7. Axborotlashtirilgan va kompyuterlashtirilgan jamiyatda inson qanday rol o’ynashi mumkin?
8. Respublikamizda axborotlashtirish va kompyuterlashtirish sohasida qanday ishlar amalga oshirilmoqda? Qanday qaror va qonunlar qabul qilingan?
9. Reapublikamizda qabul qilingan “Axborotlashtirish kontseptsiyasi” qanday muammolarni hal qilishni o’z oldiga qo’ygan?
10. Respublikamizni axborotlashtirish va kompyuterlashtirishning asosiy tamoyillari qanday?
11.Informatika fani nimani o`rganadi?
12.Informatika fanining vazifalari nimadan iborat?
13.Informatika fani amaliy fan sohasi sifatida nimani o`rganadi?
14.Informatsiya deganda nimani tushunasiz?
15. Informatsiya qanday sifatlarga ega bo`lishi lozim?
16.Axborotni o’lchov birliklarini aytib bering.
17.EHM avlodlari haqida ayting.

2 AMALIY MASHG`ULOT

Kompyuter viruslari haqida ma'lumot

Kompyuter viruslari haqida ma'lumot

Hamma kompyuter viruslari ham bir xil tarzda harakat qilmaydi. Ularning ko’payishi va kompyuteringizni zararlash usullari ham turlicha. Hozirgi kunga kelib kompyuterga zarar yetkazuvchi programmalar va virus turlari juda ko’p bularga qarshi qanday chora ko'rish mumkin va qanday antiviruslardan foydalangan ma'qul deb o'ylaymiz lekin mana shu viruslarni ham qanday guruhlarga bulishini bilib olsak foydadan holi bo'lmasdi. Zero bularning barchasi o'zimiz uchun foydalidir, keling endi mana shu viruslar haqida to'htalib o'tamiz.

Kompyuteringizda antivirus tomonidan ushlangan viruslarning qaysi turga kirishini bilish sizga nima beradi?
Birinchidan, sizga bu virusga qarshi qanday samarali kurashishda yordam berish mumkin. Ikkinchidan, bu viruslarning qanday zarar yetkazishi mumkinligini bilib olasiz, keyinchalik bunday viruslardan ogoh bo’lasiz. Uchinchidan, bu ma’lumotlar sizning kompyuter savodxonligingizni oshishiga yordam beradi degan umiddaman.
Quyidagi umumiy tavsifda ularning eng asosiy turlari keltirilgan:

Troyanlar (Trojan Horses) – Qadimgi yunonlarning Troyaga yurishlari davrida qo’llagan hiylasi, ya’ni troyaliklarni otga ishqiboz ekanligidan foydalanib, ularga katta yog’och ot sovg’a qilishlari va bu otning troyaliklar mag’lubiyatiga olib kelishi voqeasidan olingan nom. Hozirda troya oti iborasi "**hosiyatsiz sovg’a**" degan ma’noni bildiradi. Kompyuter va internet dunyosida troyanlar "**hosiyatsiz programma**" deb nomlanishi maqsadga muvofiq. Troyanlar odatda internet orqali tarqaladi. Troyanlar kompyuteringizga o’rnashib olib, dastlab foydali programma sifatida o’zlarini tanishtiradilar, lekin ularning asl vazifasi foydalanuvchiga noma’lumligicha qoladi. Yashirin ravishda ular o’zlarining yaratuvchisi (**cracker – yovuz haker**) tomonidan belgilangan harakatlarni amalga oshiradilar. Troyanlar o’z-o’zidan ko’paymaydi, lekin kompyuteringiz xavfsizligini ishdan chiqaradi: troyanlar kerakli ma’lumotlaringizni o’chirib yuborishi, kompyuterdagi ma’lumotlarni kerakli manzilga jo’natishi, kompyuteringizga internetdan ruxsatsiz ulanishlarni amalga oshirishi mumkin.

Chuvalchang viruslar (Worms) – Chuvalchang viruslar o’z nomiga mos ravishda juda tez o’z-o’zidan ko’payadigan viruslardir. Odatda bu viruslar internet yoli intranet tarmoqlari orasida tarqaladi. Tarqalish usuli sifatida elektron xatlar yoki boshqa tez tarqaluvchi mexanizmlardan foydalanadi. Ular haqiqatan ham kompyuteringizdagi ma’lumotlar va kompyuter xavfsizligiga katta ziyon yetkazadi. Chuvalchang viruslar operatsion tizimning nozik joylaridan foydalanish yoki zararlangan elektron xatlarni ochish yo’li bilan kompyuteringizga o’rnashib olishi mumkin.

Boot sektor viruslari (Bootsector viruses) – Bu viruslar kompyuterning ishlay boshlashi (загрузка) uchun foydalaniladigan qattiq diskning maxsus qismini ishdan chiqaradi. Bu virus kompyuteringizni zararlaganidan keyin kompyuter ishlamay qolishi mumkin. Odatda floppy disklar orqali tarqaladi.

Makro viruslar (Macro viruses) – Macro viruslar bu – o’zlarining tarqalishi uchun boshqa bir programmaning makro dasturlash tilidan foydalanadigan viruslardir. Ular odatda Microsoft Word yoki Excel xujjatlarini zararlaydi.

Operativ xotirada yashovchi viruslar (Memory Resident Viruses) - Bu viruslar kompyuteringizning operativ xotirasida (RAM) yashaydi va zararli harakatini amalga oshiradi. Odatda ularni ishga tushirish uchun boshqa virusdan foydalaniladi. Ular o’zlarining ishga tushishga yordam bergan virus yopilgan bo’lsa ham kompyuter xotirasida qoladi, shuning uchun ham ularga yuqoridagi nom berilgan.

Rootkit viruslari (Rootkit viruses) – Rootkitlar viruslar orasida o’zlarining eng xavfliligi va yashirinishga ustaligi bilan alohida ajralib turadi. Rootkitlar kompyuteringizni yovuz hakerlar tomonidan qo’lga olinishi uchun foydalaniladi. Ba’zi rootkitlarni antivirus programmalari ham aniqlay olmaydi, chunki ular o’zlarini operativ tizim fayllari sifatida ko’rsatishadi. Rootkitlar odatda troyanlar tomonidan kompyuteringizga o’rnatiladi.

O’zgaruvchan viruslar (Polymorphic viruses) – Bu viruslar nafaqat o’z-o’zidan ko’payadi, balki ko’paygan paytda o’zlarining kodlarini ham o’zgartirib turishadi. O’zgaruvchan viruslarni aniqlash ham ba’zi antiviruslar uchun qiyin kechishi mumkin.

Vaqt bombasi viruslari (Time or Logic Bombs) – Bu viruslar muayyan sana yohud payt kelganida yoki foydalanuvchi tomonidan muayyan harakat amalga oshirilganida ishga tushadigan viruslardir. Misol uchun Kulgi kunida(1 aprel) yoki Yangi yilda kompyuteringizdagi ma’lumotlarni o’chirib tashlab sizga "sovg’a” taqdim etishi mumkin.

Manba: ww.ref.uz dan olindi.

III-BOB. VIRUSLARGA QARSHI CHORA-TADBIRLAR

3.1 Antivirus dasturlari va ularning turkumlanishi

Kompyuter viruslarini aniqlash va ulardan himoyalanish uchun maxsus dasturlarning bir necha xillari ishlab chiqilgan bo’lib, bu dasturlar kompyuter viruslarini aniqlash va yo’qotishga imkon beradi. Bunday dasturlar virusga qarshi dasturlar deb yuritiladi. Umuman, barcha virusga qarshi dasturlar zaharlangan dasturlarning va yuklama sektorlarning avtomatik tarzda tiklanishini ta’minlaydi.

Viruslarga qarshi dasturlar foydalanadigan viruslarni aniqlashning asosiy usullari quyidagilar:

- Etalon bilan taqqoslash usuli;
- Evristik taxlil;
- Virusga qarshi monitoring;
- O’zgarishlarni aniqlovchi usul;
- Kompyuterning kiritish/chiqarish bazaviy tizimiga (BIOSra) virusga qarshi vositalarni o’rnatish va h.
- *Etalon bilan tazoslash usuli* eng oddiy usul bo’lib, ma’lum virus-larni qidirishda niqoblardan foydalanadi. Virusning niqobi mana shu muayyan virusga xos kodning qandaydir o’zgarmas ketma-ketligidir. Virusga qarshi dastur ma’lum virus niqoblarini qidirishda tekshiriluvchi fayl-larni ketma-ket ko’rib chiqadi (skanerlaydi). Virusga qarshi skanerlar faqat niqob uchun belgilangan, oldindan ma’lum viruslarni topa oladi. Oddiy skanerlar kompyuterni yangi viruslarning suqilib kirishidan himoyalamaydi. Yangi dasturni yoki yuklama sektorini zaharlashda kodini to’la o’zgartira oluvchi shifrlanuvchi va polimorf viruslar uchun niqob ajratish mumkin emas. Shu sababli skaner ularni aniqlamaydi.

Evristik tahlil. Kompyuter virusi ko’payishi uchun xotirada nusxalanish, sektorga yozilish kabi qandaydir muayyan xarakatlarni amalga oshirishi lozim. Evristik taxdillagichda bunday harakatlarning ro’yxati mavjud. Evristik taxdillagich dasturlarni va disk va disket yuklama sek-torlarini, ularda virusga xos kodlarni aniqlashga uringan holda, tekshiradi. Taxlillagich zaharlangan faylni topib, monitor ekraniga axborot chiqaradi va shaxsiy yoki tizimli jurnalga yozadi. Evristik taxlil oldin ma’lum bo’lmagan viruslarni aniqlaydi.

Virusga qarshi monitoring. Ushbu usulning mohiyati shundan iboratki, kompyuter xotirasida boshqa dasturlar tomonidan bajariluvchi shubhali harakatlarni monitoringlovchi virusga qarshi dastur doimo bo’ladi. Virusga qarshi monitoring barcha ishga tushiriluvchi dasturlarni, yaratiluvchi, ochiluvchi va saklanuvchi xujjatlarni, Internet orqali olingan yoki disketdan yoki har qanday kompakt-diskdan nusxalangan dastur va xujjatlarning fayllarini tekshirishga imkon beradi. Agar qandaydir dastur xavfli harakatni qilishga urinmoqchi bo’lsa, virusga qarshi monitor foy-dalanuvchiga xabar beradi.

O'zgarishlarni aniqlovchi usul. Diskni taftish qiluvchi deb ataluvchi ushbu usulni amalga oshirishda virusga qarshi dastur diskning xujumga duchor bo'lishi mumkin bo'lgan barcha sohalarini oldindan xotirlaydi, so'ngra ularni vaqti-vaqti bilan tekshiradi. Virus kompyuterlarni zaharlaganida qattiq disk tarkibini o'zgartiradi: masalan, dastur yoki fayllar.

Xujjat fayliga o'zining kodini qo'shib qo'yadi, **Autoexec.bat** fayliga dasturvirusni chaqirishni qo'shadi, yuklama sektorni o'zgartiradi, fayl-yo'ldosh yaratadi. Disk sohalari xarakteristikalarining qiymatlari solishtirilganida virusga qarshi dastur ma'lum va no'malum viruslar tomonidan qilingan o'zgarishlarni aniqlashi mumkin.

Kompyuterlarning kiritish-chiqarish bazaviy tizimiga (BIOS) virusga qarshi vositalarni o'rnatish. Kompyuterlarning tizimli platasiga viruslardan himoyalashning oddiy vositalari o'rnatiladi. Bu vositalar qattiq disklarning bosh yuklama yozuviga hamda disklar va disketlarning yuklama sektorlariga barcha murojaatlarni nazoratlashga imkon beradi. Agar qandaydir dastur yuklama sektorlar tarkibini o'zgartirishga urinsa, himoya ishga tushadi va foydalanuvchi ogohlantiriladi. Ammo bu himoya juda ham ishonchli emas.

Virusga qarshi dasturlarning xillari. Virusga qarshi dasturlar-ning quyidagi xillari farqlanadi:

- Dastur-faglar (virusga qarshi skanerlar);
- Dastur-taftishchilar (CRC-skanerlar);
- Dastur-blokirovka qiluvchilar;
- Dastur-immunizatorlar.

Dastur-faglar eng ommaviy va samarali virusga qarshi dastur hisoblanadi. Samaradorligi va ommaviyligi bo'yicha ikkinchi o'rinda dastur-taftishchilar turadi. Odatda, bu ikkala dastur xillari bitta virusga qarshi dasturga birlashtiriladi, natijada uning quvvati anchagina oshadi. Turli xil blokirovka qiluvchilar va immunizatorlar ham ishlatiladi.

Dastur-faglar (skanerlar) viruslarni aniqlashda etalon bilan taqqoslash usulidan, evristik taxlillashdan va boshqalardan foydalanadi. Dastur-faglar operativ xotira va fayllarni skanerlash yo'li bilan muayyan virusga xarakterli bo'lgan niqobni qidiradi. Dastur-faglar nafaqat viruslar bilan zaharlangan fayllarni topadi, balki ularni davolaydi ham, ya'ni fayldan dastur-virus badanini olib tashlab, faylni dastlabki xolatiga qaytaradi. Dastur-faglar avval operativ xotirani skanerlaydi, viruslarni aniqlaydi va ularni yo'qotadi, so'ngra fayllarni davolashga kirishadi. Fayllar ichida viruslarni katta sonini qidirishga va yo'q qilishga atalgan dastur-faglar, ya'ni polifaglar ham mavjud.

Dastur-faglar ikkita kategoriyaga bo'linadi: universal va ixtisos-lashtirilgan skanerlar. Universal skanerlar skaner ishlashi mo'ljallangan operatsion tizim xiliga bog'liq bo'lmagan holda, viruslarning barcha xillarini qidirishga va zararsizlantirishga mo'ljallangan. Ixtisoslashtirilgan skanerlar viruslarning chegaralangan sonini yoki ularning bir sinfini, masalan makroviruslarni zararsizlantirishga atalgan. Faqat makroviruslarga mo'ljallangan ixtisoslashtirilgan skanerlar MS WORD va Excel muhitlarida xujjat almashinish tizimini himoyalashda eng qulay va ishonchli yechim hisoblanadi.

Dastur-faglar skanerlashni "bir zumda" bajaruvchi monitoringlashning rezident vositalariga va faqat so'rov bo'yicha tizimni tekshirishni ta'mnlovchi rezident bo'lmagan skanerlarga ham bo'linadi. Monitoringlashning rezident vositalari tizimni ishonchliroq himoyalashni ta'minlaydi, chunki ular viruslar paydo bo'lishiga darrov reaksiya ko'rsatadi, rezident bo'lmagan skaner esa virusni aniqlash qobiliyatiga faqat navbatdagi ishga tushirilishida ega bo'ladi.

Dastur-faglarning afzalligi sifatida ularning universalligini ko'rsatish mumkin. Dastur-faglarning kamchiligi sifatida viruslarni qidirish tezligining nisbatan katta emasligini va virusga qarshi bazalarning nisbatan katta o'lchamlarini ko'rsatish mumkin. Undan tashqari, yangi viruslarning doim paydo bo'lishi sababli dastur-faglar tezdan eskiradi va ular versiyalarining muntazam yangilanishi talab etiladi.

Dastur-taftishchilar (CRC-skanerlar) viruslarni qidirishda o'zgarishlarni aniqlovchi usuldan foydalanadi. CRC-skanerlar diskdagi fayllar/tizimli sektordagilar uchun CRC-yig'indini (tsiklik nazorat kodini) hisoblashga asoslangan. Bu CRC-yig'indilar virusga qarshi ma'lumotlar ba'zasida fayllar uzunligi, sanalar va oxirgi modifikatsiyasi va boshqa parametrlar xususidagi qo'shimcha axborotlar bilan bir qatorda saqlanadi. CRC-skanerlar ishga tushirilishida ma'lumotlar bazasidagi ma'lumot bilan real hisoblangan qiymatlarni taqqoslaydi. Agar ma'lumotlar bazasidagi yozilgan fayl xususidagi axborot real qiymatlarga mos kelmasa, CRC-skanerlar fayl o'zgartirilganligi yoki virus bilan zaharlanganligi xususida xabar beradi. Odatda xolatlarni taqqoslash operatsion tizim yuklanishdan so'ng darhol o'tkaziladi.

CRC-skanerlarning kamchiligi sifatida ularning yangi fayllardagi viruslarni aniqlay olmasligini ko'rsatish mumkin, chunki ularning ma'lumotlar bazasida bu fayllar xususidagi axborot mavjud emas.

Dastur-blokirovka qiluvchilar virusga qarshi monitoringlash usulini amalga oshiradi. Virusga qarshi blokirovka qiluvchilar rezident dasturlar bo'lib, virus xavfi vaziyatlarini to'xtatib qolib, u xususida foy-dalanuvchiga xabar beradi. Virus xavfi vaziyatlariga viruslarning ko'payishi onlaridagi xarakterli chaqiriqlar qiladi. Blokirovka qiluvchilarning afzalliklari sifatida viruslar ko'payishining ilk bosqichida ularni to'xtatib qolishini ko'rsatish mumkin. Bu ayniqsa, ko'pdan beri ma'lum virusning muntazam paydo bo'lishida muhim hisoblanadi. AMMO, ular fayl va disklarni davolamaydi. Blokirovka qiluvchilarning kamchiligi sifatida ular himoyasining aylanib o'tish yo'llarining

mavjudligini va ularning "xiralikligini" (masalan, ular bajariluvchi fayllarning harqanday nusxalanishiga urinish xususida muntazam ogoxdantiradi) ko'rsatish mumkin. Ta'kidlash lozimki, kompyuter apparat komponenti sifatida yaratilgan virusga qarshi blokirovka qiluvchilar mavjud.

Dastur-immunizatorlar - fayllar zaharlanishini oldini oluvchi dasturlar ikki xilga bo'linadi: zaharlanish xususida xabar beruvchi va virusning qandaydir xili bo'yicha zaharlanishni blokirovka qiluvchi. Birinchi xil immunizatorlar, odatda, fayl oxiriga yoziladi va fayl ishga tushirilganda har marta uning o'zgarishini tekshiradi. Bunday immunizatorlar bitta jiddiy kamchilikka ega. Ular stels-virus bilan zaxarlanishni aniqday olmaydilar. Shu sababli bu xil immunizatorlar hozirda ish-latilmaydi.

Ikkinchi xil immunizatorlar tizimni virusning ma'lum turi bilan zaharlanishdan himoyalaydi. Bu immunizator dastur yoki diskni shunday modifikatsiyalaydiki, bu modifikatsiyalash ularning ishiga ta'sir etmaydi, virus esa ularni zaharlangan deb qabul qiladi va suqilib kirmaydi. Immunizatsiyalashning bu xili universal bo'laolmaydi, chunki fayllarni barcha ma'lum viruslardan immunizatsiyalash mumkin emas. Ammo bunday immuni-zatorlar chala chora sifatida kompyuterni yangi no'malum virusdan, u virusga qarshi skanerlar tomonidan aniqlanishiga qadar, ishonchli himoyalashi mumkin.

Virusga qarshi dasturning sifat mezonlari. Virusga qarshi dasturni bir necha mezonlar bo'yicha baholash mumkin. Quyida bu mezonlar muhimligi darajasi pasayishi tartibda keltirilgan:

- Ishonchlilik va ishlash qulayligi foydalanuvchilardan maxsus harakatlarni talab etuvchi texnik muammolarning yo'qligi; virusga qarshi dasturning ishonchliligi eng muhim mezon hisoblanadi, chunki hatto eng yaxshi virusga qarshi dastur skanerlash jarayonini oxirigacha olib bora olmasa, u befoyda hisoblanadi;
- Viruslarni barcha tarqalgan xillarini aniqlash fazilati, ichki fayl-xujjatlar / jadvallarni (MS Office), joylashtirilgan va arxivlangan fayllarni skanerlash, virusga qarshi dasturning asosiy vazifasi-100% viruslarni aniqlash va ularni davolash;
- Barcha ommaviy platformalar (DOS, Windows 95/NT, Novell Net Ware, OS/2, Alpha, Linux va h.) uchun virusga qarshi dastur versiyalarining mavjudligi; so'rov bo'yicha skanerlash va "bir zumda" skanerlash rejimlarining borligi, tarmoqni ma'murlash imkoniyatli server versiyalarining mavjudligi. Virusga qarshi dasturning ko'p platformaliligi muhim mezon hisoblanadi, chunki muayyan operatsion tizimga mo'ljallangan dasturgina bu tizim funktsiyalaridan to'la foydalanish mumkin. Fayllarni "bir zumda" tekshirish imkoniyati ham virusga qarshi dasturlarning etarlicha muhim mezoni hisoblanadi. Kompyuterga keluvchi fayllarni va qo'yiluvchi disketlarni bir lahzada va majburiy tekshirish virusdan zaharlanmaslikka 100%-li kafolat beradi. Agar virusga qarshi dasturning server variantida tarmoqni ma'murlash imkoniyati bo'lsa, uning kiymati yanada oshadi.
- Ishlash tezligi. Virusga qarshi dasturning ishlash tezligi ham uning muhim mezoni hisoblanadi. Turli virusga qarshi dasturlarda virusni qidirishning har xil algoritmlaridan foydalaniladi. Vir algoritm tezkor va sifatli bo'lsa, ikkinchisi sust va sifati past bo'lishi mumkin.

Himoyaning profilaktika choralari. Har bir kompyuterda viruslar bilan zaharlangan fayllar va disklarni o'z vaqtida aniqlash, aniqlangan viruslarni tamomila yo'qotish virus epidemiyasining boshqa kompyuterlarga tarqalishining oldini oladi. Har qanday virusni aniqlashni va yo'q qilishni kafolatlovchi mutloq ishonchli dasturlar mavjud emas. Kompyuter viruslari bilan kurashishning muhim usuli o'z vaqtidagi profilaktika hisoblanadi.

Virusdan zaharlanish ehtimolligini jiddiy kamaytirish va disklardagi axborotni ishonchli saqlanishini ta'minlash uchun quyidagi profilaktika choralarini bajarish lozim:

- Faqat qonuniy, rasmiy yo'l bilan olingan dasturiy ta'minotdan foydalanish;
- Kompyuterni zamonaviy virusga qarshi dasturlar bilan ta'minlash va ular versiyalarini doimo yangilash;
- Boshqa kompyuterlarda disketda yozilgan axborotni o'qishdan odin bu disketda virus borligini o'zining kompyuteridagi virusga qarshi dastur yordamida doimo tekshirish;
- Axborotni ikkilash. Avvalo dasturiy ta'minotning distributiv eltuvchilarini saqlashga va ishchi axborotni sakdanishiga e'tibor berish;
- Kompyuter tarmoqlaridan olinuvchi barcha bajariluvchi fayllarni nazoratlashda virusga qarshi dasturdan foydalanish;
- Kompyuterni yuklama viruslardan zaharlanishiga yo'l qo'ymaslik uchun, operatsion tizim ishga tushirilganida yoki qayta yuklanishida diskovod cho'ntagida disketani qoldirmaslik.

Virusga qarshi dasturlarning har biri o'zining afzalliklariga va kamchiliklariga ega. Faqat virusga qarshi dasturlarning bir necha xilini kompleks ishlatilishi maqbul natijaga olib kelishi mumkin.

Quyida virusdan zaharlanish profilaktikasiga, viruslarni aniqlash va yo'qotishga mo'ljallangan ba'zi dasturiy komplekslar tavsiflangan.

AVP (Antivirus Kasperskogo Personal) - Rossiyaning virusga qarshi paketi. Paket tarkibiga quyidagilar kiradi:

Office Guard - blokirovka qiluvchi, makrovirusdan 100% himoyalanishni ta'minlaydi;

- Inspector - taftishchi, kompyuterdagi barcha o'zgarishlarni kuzatadi, virus faolligi aniqlanganida diskning asl nusxasini tiklashga va zarar keltiruvchi kodlarni chiqarib tashlashga imkon beradi;
- Monitor - viruslarni ushlab qoluvchi, kompyuter xotirasida doimo hozir bo'lib, fayllar ishga tushirilganida, yaratilishida yoki nusxalani shida ularni virusga qarshi tekshiradi;
- Scanner - virusga qarshi modul, lokal va tarmoq disklar tarkibini keng ko'lamli tekshirish imkonini beradi. Skanerni qo'l yordamida yoki be rilgan vaqtda avtomatik tarzda ishga tushirish mumkin.

Paket yordamida elektron pochtani virusga qarshi filtrlash va pochta korrespondentsiyasini kompleks tekshirish amalga oshiriladi. Virusga qarshi bazani yangilash Internet orqali bajariladi.

Dr.Web - Rossiyaning virusga qarshi ommaviy dasturi, Windows 9x/NT/2000/XP uchun mo'ljallangan bo'lib, faylli, yuklama, va fayl-yuklama viruslarni qidiradi va zararsizlantiradi. Dastur tarkibida rezident qorovul SpIDer Guard, Internet orqali virus bazalarini yangilashning avtomatik tizimi va avtomatik tekshirish jadvalini rejalashtiruvchi mavjud. Pochta fayllarini tekshirish amalga oshirilgan.

Dr.Web da ishlatiluvchi algoritmlar haqida ma'lum bo'lgan barcha virus xillarini aniqlashga imkon beradi. Dr.Web dasturining muhim xususiyati - oddiy signaturli qidirish natija bermaydigan murakkab shifrlangan va polimorf viruslarni aniqlash imkoniyatidir.

Symantec Antivirus - Symantec kompaniyasining korporativ foydalanuvchilarga taklif etgan virusga qarshi mahsuloti to'plami.

Symantec mahsulotidan ishchi joylarining umumiy soni 100 va undan ortiq bo'lganida va bo'lmaganda bitta Windows NT/2000/NetWare serveri mavjudligida foydalanish maqsadga muvofiq hisoblanadi. Ushbu paketning bashqalardan ajralib turadigan xususiyati quyidagilar:

- Boshqarishning ierarxik modeli;
- Yangi virus paydo bo'lishiga reaktsiya qilish mexanizmining mavjudligi.

AntiVir Personal Edition - virusga qarshi dastur AVP, Dr.Web va h.lar imkoniyatlaridek imkoniyatlarga ega. Dastur komplektiga quyidagilar kiradi:

- Disklarni skanerlovchi;
- Rezident qorovul;
- Boshqarish dasturi;
- Rejalashtiruvchi.

Dastur Internetdan yuklanuvchi fayllarni skanerlaydi. Internet orqali yangilanishlarni avtomatik tarzda tekshirish va yuklash funktsiyasi ham mavjud. Dastur xotirani, yuklanish sektorini tekshirishda va unda viruslar bo'yicha keng ko'lamdagi ma'lumotnoma mavjud.

Antivirus dasturlarini bir necha turga ajratish mumkin: detektorlar, vaktsinalar (immunizatorlar), doktorlar, revizorlar (fayl va disklarning tizimli soxalaridagi o'zgarishlarni nazorat qiluvi dasturlar), doktor revizorlar va filtrlar (virusdan ximoyalanish uchun mo'ljallangan rezident dasturlar). Ularning xususiyatlarini kurib chikamiz.

Revizor dasturlar — dastlab dastur va diskning tizimli soxasi xaqidagi ma'lumotlarni xotiraga oladi, so'ngra ularni dastlabkisi bilak solishtiradi. Mos kelmagan hollar xaqida foydalanuvchiga ma'lum qiladi. Masalan, CRCLIST va CRCTEST dasturlar.

Doktor revizorlar — revizor va doktorning aralashmasi, boshqacha aytganda, fayl va diskning tizimli soxasidagi o'zgarishlarni nafakat aniqlaydigan, balki o'zgargan xolda ularni dastlabki xolatga qaytarishi mumkin bo'lgan dasturlardir.

Filtr dasturlar yoki rezident dasturlar kompyuterning tezkor xotirasida rezidentday joylanadi va viruslar tomonidan zararni ko'paytirish va ziyon etkazish maqsadida operatsion tizimga qilinayotgan murojaatlarni ushlab qolib, ular xaqida foydalanuvchiga ma'lum qiladi. Foydalanuvchi ushbu amalii bajarish yoki bajarmaslikka ko'rsatma beradi. Masalan, Flushot Plus va Antirus dasturlari.

Virusga qarshi dasturlar quvvatiga qarab bir necha turga bulinadi. Quyida eng ko'p tarqalgan virusga qarshi **DSAV 2.0** («Dialog-nauka A.B.») kompleksi bilan tanishamiz. Uning tarkibiga quyidagilar kiradi:

1. AIDSTEST — viruslarni aniqlash va yo'qotish uchun mo'ljallangan virusga qarshi ko'p kirrali dastur (xap xaftada yangilanib turadi).

2. Ros(og WEB (Dr Web) — yangidan yaratilgan, ma'lum va noma'lum viruslarni aniqlash va yo'qotish uchun ishlatiladigan virusga qarshi dastur. U arxivlangan va vaktsiyalangan fayllarda xam viruslarni aniqlay oladi (xar oyda o'rtacha 2 marta yangilanadi).

3. ADINF — diskdagi barcha o'zgarishlarni nazorat qiluvchi, disklarning virusga qarshi revizor dasturi (bir yilda bir necha marta yangilanadi). Diskdagi barcha dasturlarning fizik kamchiliklarini nazorat kiladi. Diskning tizimli soxasini va fayllar xolatini eslab qoladi va qayta yuklashda diskdagi o'zgarishlarni aniqlaydi, agar biror xavfli o'zgarishlar aniqlansa, foydalanuvchiga bu xaqida xabar beradi.

4. ADINF CURE MODVLE — ADINF disklar revizoridagi davolash moduli bo'lib, revizor tomonidan zararlanganligi aniqlangan fayllarni avtomatik xolatda tiklaydi (yiliga bir necha marta yangilanadi).

5. SHERIF — qattiq diskdagi operatsion tizim, dasturlar va ma'lumotlar faylini 100% kafolat bilan ximoyalovchi rezident dastur.

Bu dasturlar asosan **MS DOS** muxitida ishlatiladi (ularni Windows muxitiga moslash xam mumkin). Amalda yuqoridagilarning bittasidan foydalanish maqsadga muvofiq. Biror dasturni o'rnatib, uni doimiy ravishda yangilab borilsa, foydaliroq, bo'ladi.

Kompyuterlarga virus yuqqanda (yoki yuqganlik xaqida gumon bo'lsa) quyidagi qoidalarni esda tutish va qo'llash lozim:

1. Dastlab, qarshi kurash qarorlarini qabul qilishga shoshmaslik kerak. uylamasdan kilingan xarakatlarni tiklash mumkin bulgak fayllarning bir qismini yo'qotishgina emas, balki kompyuterni yana qayta kasallantirishga olib kelishi mumkin.

2. Virus uzining buzgunchiligini davom ettirmasligi uchun kompyuterni uchirish lozim.

3. Kompyuter kasallanishi va davolash ko'rinishini aniqlashga mo'ljallangan barcha amallarni yozishdan ximoyalangan operatsion tizimli disk bilan kompyuterni ishga tushirish orqaligina bajarish mumkin. Drweb dasturidan foydalanish bilan tanishib chikamiz. Bu dasturni ishga tushirish uchun drweb.exe faylidan foydalaniladi. Natijada 3-rasmdagi tasvir — dasturning asosiy menyusi xosil bo'ladi. Menyudan foydalanib qanday fayllarni tekshirish va tekshirish bilan bog'lik, barcha parametrlar O'rnatiladi. So'ngra «Test» dagi «Lechenie» ko'rsatmasini tanlash yoki **Ctrl** va **F5**tugmachalarini birgalikda bosish orqali viruslardan davolash jarayoni boshlab yuboriladi. Dastur xotiraning ko'rsatilgan qismini tekshirib, mavjud viruslarni davolashga xarakat qiladi va ish oxirida mos xisobotni chiqaradi.

Shu erdan viruslarni uchirishingiz mumkin

Kompyuter viruslari va ularni davolash

Kompyuter virusi o'lchami bo'yicha katta bo'lmagan, maxsus yozilgan dasturdan iborat bo'lib, u o'zini boshqa dasturlarga «yozib ko'yishi», shuningdek, kompyuterda turli noxush amallarni bajara olishi mumkin. Bunday dastur ishlashni boshlaganda dastlab virus boshqaruvni o'z qo'liga oladi. Virus boshqa dasturlarni topadi va unga «yuqadi», shuningdek, qandaydir zararli amallarni (masalan, diskdagi fayl yoki fayllarning joylashish jadvalini buzadi, tezkor xotirani «ifloslaydi» va x.k.) bajaradi. Virus uziga tegishli amallarni bajarib bo'lgandan so'ng boshqaruvni o'zi joylashgan dasturga uzatadi. Virus joylashgan dastur odatdagidek ishini davom ettiradi. Tashqaridan dasturning «kasallanganligi» bilinmaydi.

Ko'p turdagi viruslar shunday tuzilganki, kasallangan dasturni ishga tushirganda virus kompyuter xotirasida doimiy qoladi va vaqt-vaqti bilan dasturlarni kasallaydi va kompyuterda zararli amallarni bajaradi.

Virusning barcha amallari etarlicha tez va hech qanday ma'lumot e'lon qilmasdan bajariladi. Shuning uchun foydalanuvchi kompyuterda qanday jarayonlar amalga oshayotganligini bilishi qiyin.

Kompyuterdagi dasturlarning kamchilik qismi kasallangan bo'lsa, virus borligi umuman bilinmaydi. Lekin aniq vaqt o'tgandan so'ng kompyuterda fizik xolatlar paydo bo'la boshlaydi. Masalan, ba'zi dasturlar ishlamay qoladi yoki noto'g'ri ishlaydi, ekranga begona ma'lumotlar yoki belgilar chiqariladi, kompyuterning ishlash tezligi sezilarli darajada pasayadi, ba'zi fayllar buzilib qoladi va xokazo.

Bu paytgacha kompyuterdagi anchagina dasturlar, ba'zi boshqa turdagi fayllar ishdan chikadi. Bundan tashqari, virus disk yoki lokal tarmoq, orqali boshqa kompyuterlarga utishi xam mumkin.

Shuning uchun virusdan ximoyalanmasa yoki yukishining oldi olinmasa juda katta noxushliklarga olib kelishi mumkin.

Virus dasturi ko'rinmaydigan bo'lishi uchun u juda kichik bo'lishi kerak. Shuning uchun xam ularning ko'pchiligi assembler tilida yoziladi.

Viruslarning paydo bo'lishiga dastlabki mualliflarning «shumligi» va o'zlari tushunmagan xolda kimnidir «tuzlashni» maqsad qilib quyishlari sabab bo'lgan.. Oqibatning bu

darajada yomonlashuvi ularning xayoliga kelmagan bo'lsa kerak.

Xozirgi kunda 36000 dan ortiq kompyuter viruslari kompyuter tizimlari va ma'lumotlari ishi uchun asosiy xavfni tashkil etadi. Bunda, asosan, zarar ko'radiganlar litsey, institut, universitetlar va boshqa tashkilotlardir. Bunday muassasa kompyuterlarida ma'lumotlardan foydalanish ochiq va chegarasiz bo'lganligi uchun viruslarning qurboni bo'linadi va katta moddiy talafot ko'riladi. Shu bois, kompyuter ishini nazoratga olish muximdir.

Kompyuter ishini nazoratga olish deganda nima tushuniladi? Unga quyidagilar kiradi:

1) Litsenziyasiz dasturiy ta'minotdan foydalanmaslik;

2) Tashqaridan kiritiladigan viruslarning oldini olish;

3)Tizimga sanktsiyasiz kiruvchi xakerlarga imkon bermaslik. Axborot va dasturlar xavfsizligini ta'minlash uchun quyidagilar zarur bo'ladi: birinchidan, litsenziyalangan dasturiy ta'minotni ishlatish; ikkinchidan, tashqi tarmoqlarga ulanishda filtr cheklovchilar o'rnatish (viruslardan ximoyalanish va sanktsiyasiz foydalanishni cheklash).

Albatta, bunday ximoya vositalari uzluksiz rivojlanib takomillashib bormoqda.

Kompyuter viruslarini quyidagi guruxlarga ajratish mumkin:

1.Diskning yuklanish sektorlarini buzadigan yuklanish viruslari;

2.Bajariladigan fayllar — **.com, .exe, .sys, .bat, .cmd** fayllarini buzuvchi fayl viruslari;

3.Diskning yuklanish sektora va bajariladigan fayllarni buzadigan yuklanish fayla viruslari;

4.Stels (**invisible**) — ko'rinmas viruslar;

5.Microsoft Word muxarriri yordamida xosil kilingan ma'lumotli fayllarni yozuvchi — makrobuyruk viruslari.

Bundan tashqari boshqa turdagi viruslar xam mavjud. Virus lardan ximoyalanishda axborotni ximoya qilishning umumiy vositalaridan foydalanish kifoya qilmaydi. Juda ko'pchilik viruslar bir xil algoritmda ko'payadi.

Masalan virus tuzuvchi **Auto.exe** nomli virus yaratdi.

Bu virus ishga tushgandan so'ng o'zini bir nusxasini sistema katalogiga tashlaydi.(C:/Windows/system32/..)Bu nusxani "ONA" virus desa xam bo'ladi chunki virus nusxasini kompyuter kataloglariga yoyadi, yo'q qilingan viruslarni o'rniga yana nusxasini yozadi. Tizim Reestriga,"kompyuter bilan birga ishga tushish xaqidagi axborotni yozadi.

So'ng mavjud disklarning yuklanuvchi qismiga(C:/ …D:/…) bir nusxasini va **Autorun.inf**degan faylni tashlaydi. **Autorun.inf**-fayli disk ishga tushganda " **Auto.exe ni ishga tushur"** degan buyruqni o'z ichiga oladi. Shu tariqa ko'payadi. Ba'zi viruslar **Autorun.inf** faylini generatsiya qilmaydi. Chunki bunday viruslarni biz bilmasdan ishga tush irib yuboramiz. Lekin bu viruslar xam nusxasini ko'paytiradi.

"ONA"-virus

"ONA" virusning "bolalari"

Kompyuter viruslaridan saqlanishnnng ehtiyotkorlik tadbirlari

Virusdan kuriladigan zararlarga quyidagilarni misol qilib kursatish mumkin:

• Kompyuter qattik diski yoki tezkor xotirasining ifloslanishi — virusli dastur ko'payishi jarayonida butun qattiq diskni o'zining nuqtalari yoki boshqa belgilari bilan to'ldirishi mumkin. Bularni u tezkor xotiraga xam yozishi va shu bilan uning xajmini kamaytirishi mumkin;

• Fayllar joylashish jadvalining buzilishi. U buzilsa, diskdan kerakli fayl va katalogni o'qish mumkin bo'lmaydi;

• Yuklanish sektoridagi ma’lumotlarning buzilishi. Yuklanish sektora diskdagi maxsus dastur bo’lib, uning buzilishi disk ishini to’xtatib qo’yadi;

• Diskni qayta formatlash — diskdagi barcha axborot butunlay yo’qotish;

• Diskka biror xabar chiqarishi yoki biror kuyni ijro etishi mumkin. Ko’p xollarda bu xabar tushunarsiz bo’ladi;

• Kompyuterning o’z-o’zidan qayta yuklanishi;

• Tugmachalar majmui ishini to’xtatib qo’yishi;

• Dasturli va ma’lumotli fayllar mazmunining o’zgarishi. Virus ma’lumotlarni ixtiyoriy ravishda aralashtirib qo’yadi va xokazo.

Oddiy virusdan zararlanishni virusga qarshi dasturlar yordamida oson aniqlash mumkin. Polimorf (murakkab tuzilishga ega) viruslarni bu usul bilan aniqlash qiyin, chunki ular o’z-o’zini nusxalashda ko’rinishini o’zgartiradi.

Makroslar bilan ishlaydigan ilovalar makroviruslar bilan zararlanishi mumkin.

Makroviruslar — fayllarga ma’lumotlar bilan birga o’rnatiladigan buyruqlardir. Bunday ilovalarga misol qilib **Word, Excel** va **Postscripter** interpretatorlarini ko’rsatish mumkin. Ular ma’lumotlar faylini ochayotganda makrovirus bilan zararlanadi.

Ilgari faqat disklar virus bilan zararlanar edi. Chunki viruslar disklar orqali kompyuterdan kompyuterga ugar edi. Yangi BBS viruslari esa modem orqali tarqaladigan bo’ldi. Internetning paydo bo’lishi viruslarga qarshi kurashning an’anaviy usullari foyda bermaydigan yana bitta kanalning xosil bo’lishiga olib keldi.

Viruslar bilan zararlanish extimoli kompyuterda yangi fayllar va ilovalarning paydo bo’lish chastotasiga mos ravishda ortadi, Kompyuterdagi ma’lumotlarning axamiyati qanchalik zarur bo’lsa, virusga qarshi xavfsizlik choralari shunchalik yuqori bo’lishi kerak. Bu narsalarga befarq bo’lish nafakat katta moddiy zarar kurish, balki tashkilot yoki firmaning bundan keyingi faoliyati masalasini xam o’rtaga quyishi mumkin.

Shuni esdan chiqarmaslik kerakki, viruslar, odatda, foydalanuvchining biror amali (masalan, ilovalarni o’rnatish, tarmoqdan fayllarni uqish, elektron aloqani uqish va x.k.) natijasida paydo bo’ladi. Shuning uchun ma’lumotlar kirish joyiga maxsus filtrlar, zararlangan fayl va dasturlarni yuklashni cheklovchi maxsus dasturlar o’rnatilishi zarur. Bunday ko’rilmalardan biri Symantic korporatsiyasi maxsulidir (Toshkentda Nuron DC kompaniyasi uning partnyori xisoblanadi). Symantic bitta mashina o’rniga butun korporativ tarmoqni kompleks ximoyalash g’oyasini ilgari suradi. Virusning korparativ tarmoqqa kirish nuqtasi istalgan nuqtada — brauzerdan to ishchi stantsiyagacha bo’lishi mumkin. Shuning uchun nazorat barcha bosqichlarda amalga oshiriladi. Virusga qarshi Symantic dasturiy ta’minoti Dynamic Document Revie n korporatsiyasi texnologiyasida bajarilgan va E-mail viruslariga xam qarshi kurash olib boradi.

Virusga qarshi dasturli ta’minot ishining aloxida xususiyati shundaki, virusga qarshi dasturlar omborini o’z vaqtida yangilab turish kerak.

3.2 Viruslarga qarshi evristik tahlil

EVRISTIK TAHLIL

Tahlil metodlari ximoyaning bir qancha komponentalarida qo'llaniladi, masalan, fayl antivirusi , , Pochta va Web Antivirusi.

Bizga ma'limki tekshirishning, barcha xavfli dasturlar va davolashning yangi metodlarini o'z ichiga olgan bazadan foydalaniladigan signaturali metodi, aniq to'xtamga kelishimizga yordam beradi, "*Ushbu tekshirilayotgan obyekt zararli emasmikan? Agar zararli bo'lsa qaysi turkumga kirar ekan*?" kabi savollarga xam javob olish mumkin. Evristik metod Signaturali metoddan farqli o'laroq, xavfli kodlar signaturasini tahlil qilmaydi, balki sodir bo'layotgan jarayonlarning ketma ketligni tahlil qiladi. Bu esa , fayl xaqida kerakli mantiqiy xulosa qilishimizga zamin yaratadi.

Evristik tahlilning faydali jixati shundan iboratki, uning ishlashi uchun yangi ba'za talab etilmaydi. Tekshirishlarning turli xil metodlarini bir paytda qo'llash xavfsizlikni keskin kuchaytiradi.

Evristik analizatorga boror fayl shubxali ko'rinsa bu obyekt avval xavfsiz virtual rejimda ishga tushirib ko'riladi. Agar bu fayl ishlash davomida shubxali ishlarni amalga oshirsa , ushbu ob'yekt darxol "xavfli dasturlar" ro'yhatiga qo'shib qo'yiladi va uning kompyuterda ishlashi to'xtatiladi. Foydalanuvchiga ushbu yo'sindagi xabar beriladi :

- Bazaning keyingi yangilanganida tekshirish uchun karantinga joylashtirish;
- Ob'yektni o'chirib tashlash;
- O'tkazib yuborish, agar ushbu ob'yekt xavfli emasligiga to'liq ishonchingiz komil bo'lsa.

Evristik metoddan foydalanish uchun Evristik analizatordan foydalanish punktiga bayroqcha qo'yish kerak. Evristik analizning kamchiligi shundan iboratki, uning intensivligini qancha oshirsak shuncha sistema resursini talab qiladi va tekshirish uzoqqa cho'ziladi.

3.3 Kaspersky 10.0 Antivirusini kompyuterga o'rnatish

ZAO «KASPERSKY LABARATORIYASI» XAQIDA QISQACHA MA'LUMOT

ZAO «Kaspersky labaratoriyasi» 1997 yilda asos solingan. Xozirgi kunda Rossiyada bu kompaniya maxsuloti "axborot xavfsizligi" dasturiy ta'minoti bo'yicha eng ommaviy xisoblanadi: Viruslardan ximoyalanish tizimni, kutilmagan xatlar (SPAM) va xakerlik xujumlari shular jumlasiga kiradi.

ZAO «Kaspersky labaratoriyasi» – xalqaro kompaniya xisoblanadi. Markaziy offis Rossiyada joylashgan bo'lib, uning ochiq lokal offislari Buyuk Britaniya, Frantsiya, Germaniya , Yaponiya, , benilyuks mamlakatlarida , Xitoy , Polsha , Ruminiya ,va AQSH (Kalifornya) kabi davlatlarda joylashgan. Fransiyada "Antivirus tadqiqotlari Evropa markazi" yangi bo'limi o'z ishini boshladi. Kasperskiyning xamkorlik tarmog'i dunyoning 500 dan ortiq yirik kompaniyalarni birlashtiradi va xamkorliklar olib boradi.

«Kaspersky labaratoriyasi» da bugungi kunda 450 dan ortiq yuqori malakali analitik mutaxassislar ish olib borishadi, ularning 10 tasi MVA diplomiga ega 16 tasi fan nomzodlari. «Kaspersky labaratoriyasi» ning qolgan virusolog analitiklari Computer Anti-virus Researcher's Organization (CARO) tashkilotining a'zolari xisoblanadi.

Kompaniyaning asosiy axamiyati – mukammal bilim va tajriba xisoblanadi. Analitiklarning viruslarga qarshi tinimsiz izlanishlar olib borishi orqali yangi xujumlar va viruslarni aniqlash imnkoniyati yuzaga keladi. Bu esa kompaniya maxsulotining asosi va avfzalligi xisoblanadi.

«Kaspersky labaratoriyasi» birinchi bo'lib ko'pgina antivirus dasturlarining standartlarini ishlab chiqqan kompaniya xisoblanadi. Kompaniyaning asosiy maxsuloti «Антивирус Касперского®» xisoblanib, virusli xujumlarning barcha tularidan mukammal ximoya qiladi: ishchi stansiya (Workgroup), Fayl serverlari, pochta tizimlari, tarmoqlar aro ekranlar va internet shlyuzlar, cho'ntak kompyuterlari shular jumlasidandir. Ko'plab g'arb korxonalari o'zlarining maxsulotlariga «Антивируса Касперского®» yadrosini qo'llaydilar, masalan: Nokia ICG (AQSH), F-Secure (Finlandiya), Aladdin (Isroil), Sybari (AQSH), G Data (Germaniya), Deerfield (AQSH), Alt-N (AQSH), Microworld (Hindiston), BorderWare (Kanada).

«Лаборатории Касперского» mijozlari, biznesga qo'yiladigan talab va tizimning uzluksiz ishini ta'minlaydigan xizmatlarni kafolatlaydi.

Manzil:	Rossiya, 123060, Moskva, 1-chi Volokolamskiy proezdi, 1 chi uy
Telefon, fax:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00
Favqulotda tuni kunlik yordam:	+7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08
Mijozlarning biznes maxsulotlari xizmati:	+7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08 (с 10 до 18:30 moskva vaqti bo'yicha) http://support.kaspersky.ru/helpdesk.html
Korporativ mijozlarga xizmat ko'rsatish:	Kontakt axborotlar, texnik xizmat ko'rsatish paketiga qarab korporativ maxsulotlar xarid qilinganda taqdim etiladi.
«Лаборатории Касперского» ning veb forumi:	http://forum.kaspersky.com
Antivirus pochtasi	newvirus@kaspersky.com
Foydalanuvchi dokumentatsiyasi bilan ishlash guruxi:	docfeedback@kaspersky.com (Faqat elektron xabarnoma xizmatidan foydalanish uchun)
Savdo deportamenti:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00 sales@kaspersky.com
Umumiy ma'lumot:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00 info@kaspersky.com
WWW:	http://www.kaspersky.ru http://www.viruslist.ru

TIZIMGA QO'YILADIGAN TALABLAR (APPARAT VA DASTURIY TA'MINOT)

Kaspersky Antivirusining normal ishini ta'minlash uchun eng kamida quyidagilar talab qilinadi:

Umumiy talab qilinadiganlar:

• Qattiq diskda 75 MB bo'sh joy.

• CD-ROM (Maxsulotni CD-ROM dan o'rnatish uchun).

• Kiritish qurilmasi, «sichqoncha» tipidagi manipulyator.

• Microsoft Internet Explorer 5.5 yoki undan yuqorisi (dasturning bazasi va modullarini internet orqali yangilash uchun).

• Microsoft Windows Installer 2.0.

Microsoft Windows XP Home Edition (2 yangilanish paketi yoki undan yuqori), Microsoft Windows XP Professional (2 yangilanish paketi yoki undan yuqori), Microsoft Windows XP Professional x64 Edition (2 yangilanish paketi yoki undan yuqori):

• Intel Pentium 300 Mgs protsessori yoki undan yuqoti .

• Tezkor xotiraning 256BM li maydoni

Microsoft Windows Vista Starter x32, Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate:

- Intel Pentium 800Mgs protsessori 32-bit (x86) / 64-bit (x64) yoki undan yuqori
- Tezkor xotiraning 512 BM li maydoni

KASPERSKY ANTIVIRUSINI KOMPYUTERGA O'RNAISH

Kaspersky Antivirusi interaktiv usulda o'rnatish ustasi yordamida komoyuterga o'rnatiladi.

O'rnatish ishlarini boshlashdan oldin kompyuterdagi barcha dasturlar ishini to'xtatib turish maslaxat beriladi.

Kaspersky Antivirusini o'rnatish uchun CD diskdagi distributiv fayli (.exe kengaytmali) ishga tushiriladi.

Xarid qilingan CD diskdagi Kaspersky Antivirus dasturi va Internetdan ko'chirib olingan Kaspersky antivirusi dasturi to'la muvofiq va bir xildir.

So'ng dasturning o'rnatish paketini (.msi kengaytmali) izlash ishga tushadi va agar u mavjud bo'lsa internet orqali Kaspersky laboratoriyasi serveridan undanda yangi versiyasini izlash boshlanadi. Agar o'rnatish paketi topilmasa, uni yuklab olish taklif etiladi. Yuklanish tugagandan so'ng Kaspersky antivirusi ishga tushadi. Faylni yuklab olish bekor qilinsa, o'rnatish ishlari oddiy rejimda davom etadi.

Antivirusni o’rnatish paketining xar bir oynasi o’ziga xos buyruqlardan tashkil topgan. Ular Dastur xaqida qisqacha ma’lumot:

- **Далее** – Oynadagi amallarni tasdiqlash va keyingi bosqichga o’tish.
- **Назад** – Bitta oldingi oynaga o’tish.
- **Отмена** – Antivirusni o’rnatishni bekor qilish.
- **Готово** – Kompyuterdagi o’rnatish ishlarini yakunlash.

O’rnatishning xar bir qadamini qisqacha ko’rib chiqamiz.

USHBU BO’LIMDA

1 QADAM. Tizimdan ushbu dasturga mufofiq yanada yangiroq dasturni izlash
2. QADAM. Tizimning o’rnatilayotgan dastur bilan mufoviqligi tekshiriladi
3. QADAM. O’rnatish ustasi
4. QADAM Litsenziyon kelishuv bilan tanishish
5. QADAM O’rnatish turini tanlash
6. QADAM O’rnatish papkasini tanlash
7. QADAM O’rnatiladigan dastur komponentalarini tanlash
8. QADAM Boshqa antivirus dasturlarini tizimdan qidirish
9. QADAM Dasturning o’rnatilishini tekshirish ishlarini so’ngi bosqichi
10. QADAM O’rnatish ishlarini yakunlash
11.QADAM Dasturni aktivatsiya qilish

1 QADAM. TIZIMDAN USHBU DASTURGA MUFOFIQ YANADA YANGIROQ DASTURNI IZLASH

Kaspersky antivirusini o’rnatish ishlari boshlanganda dastur avval Internetdan Kaspersky antivirusi serveriga murojatni amalga oshiradi.

Agar murojat bo’yicha kasperskyning yangi versiyasi aniqlanmasa, ishga tushirgan dasturimizdagi ilova bo’yicha ornatish ishi davom etadi.

Agar yangilanish serverida Kaspersky Antivirusining yanada yangi versiyasi aniqlansa , ushbu versiyani internetdan ko’chirib olish va o’rnatish taklif etiladi. Agar rad etsangiz o’rnatish ishlari diskdan davom etaveradi.

2. QADAM. TIZIMNING O’RNATILAYOTGAN DASTUR BILAN MUFOVIQLIGI TEKSHIRILADI

Kaspersky Antivirusi o’rnatilishidan oldin ishga tushirilgan ilova tizimni ko’zdan kechiradi , ya’ni operatsiyon tizim versiyasi va yangilanish paketini. Yana kompyuterda talab qilinadigan dasturiy vositalar mavjudligi va kompyuterdagi rolingiz xam tekshiriladi.

Agar yuqoridagi tekshiruvlar qoniqarli bo’lmasa bu xaqda o’rnatilayotgan dastur xabar beradi.

3. QADAM. O’RNATISH USTASI

Agar tizim to’liq qanoatlantirsa “Kaspersky Labaratoriyasi” dan yangi versiyasi aniqlanmasa yoki yuklab olishni rad etsangiz ushbu o’rnatilayotgan versiya xavola etiladi.

Kompyuetr oynasida o’rnatish ustasining birinchi saxifasi namoyon bo’ladi.

O’rnatish ishlarini davom ettirish uchun **Далее** tugmasi bosiladi. Dasturni o’rnatishni bekor qilish uchun **Отмена**tugmasi bosiladi.

4. QADAM LITSENZIYON KELISHUV BILAN TANISHISH

Ushbu saxifa “Kaspersky laboratoriyasi” va siz ortangizdagi litsenziyon kelishuv xaqidagi axborotlarni o’zida saqlaydi. Barcha so’zlarni diqqat bilan o’qib chiqish talab qilinadi, va barcha talablarga rozi ekanligingizni tasdiqlash uchun **Я принимаю условия лицензионного соглашения** tugmasi bosiladi so’ng **Далее** tugmasi bilan keyingi saxifaga o’tiladi .

Dasturni o’rnatishni bekor qilish uchun **Отмена** tugmasi bosiladi.

5. QADAM O’RNATISH TURINI TANLASH

Ushbu bo’limda Kaspersky Antivirusi o’rnatilishining eng qulay turini tanlab olish xaqida gap ketadi:

Быстрая установка. (Tezkor o’rnatilish) Ushbu punkt tanlanganda dastur, Kaspersky **Выборочная установка.** (Tanlab o’rnatish) Ushbu punkt belgilanganda sizdan quyidagi narsalarni tanlash taklif etiladi: Dasturning qanday komponentalarini o’rnatmoqchi ekanligingizni, papkani ko’rsatish, dastur qayerga o’rnatilishi kerak, jumladan dasturni aktivatsiya qilish va maxsus master yordamida uni sozlash.Laboratoriyasi mutaxassislari bergan yo’riqnomalar, Birinchi variant tanlanganda dastur, 8 chi qadamga o’tib ketadi. (Boshqa antivirus daturlarini qidirish). Ikkinchi xolatda esa xar bir etapda biron narsa kiritish yoki tasdiq talab etiladi.

- xavfsizlik parametrlari bilan to’liq o’rnatilad

6. QADAM O’RNATISH PAPKASINI TANLASH

Ushbu etapda dastur o’rnatilishi kerak bo’lgan catalog ko’rsatiladi

“Kaspersky Antivirusi”. Sukunat bo’yicha berilga manzil:

–32-razryadli tizimlar uchun:

- **<Disk> \ Program Files \ Kaspersky Lab \ Kaspersky Anti-Virus 2009**

–64-razryadli tizimlar uchun:

- **<Disk > \ Program Files (x86) \ Kaspersky Lab \ Kaspersky Anti-Virus**

Siz **Обзор** tugmasini bosib biror boshqa manzil ko’rsatishingiz mumkin yoki manzil nomnini klaviatura orqali kiritishimiz mumkin.

Esda saqlang! Agar **Обзор** tugmasi orqali manzilni o’zgartirishga zarurat tug’ilsa manzil simvollari uzunligi 200 dan oshmasligi lozim.

O’rnatish ishlarini davom ettirish uchun **Далее** tugmasi bosiladi.

7. QADAM O’RNATILADIGAN DASTUR KOMPONENTALARINI TANLASH

Ushbu saxifa faqat “выборочная установка” tanlab o’rnatish punkti belgilanganda xavola qilinadi.

“выборочная установка” tanlab o’rnatish punkti tanlanganda Kaspersky Antivirusining maxsus komponentalari tanlash talab etiladi.Sukunat bo’yicha ushbu komponentalar barchasi tanlangan bo’ladi.

Qaysi komponentani o’rnatilishingiz zarur bo’lmasligi xaqida bilmoqchi bo’lsangiz komponentalar xaqida qisqacha axborot beradigan punktini tanlab tanishishingiz mumkin.

Komponentalardan biron birini o’rnatmaslikga qaror qilsangiz o’sha komponenta menyusidagi **Компонент будет недоступен (**komponent mavjud bo’lmaydi**)** punkti tanlanadi. Yana shuni esda tutish kerakki, kopmonentalarni o’rnatilishini bekor qilib , ba’zi xavfli dasturlarning tahdidini kuchaytirgan bo’lasiz..

Komponentlar tanlash ishlari tugagandan so’ng **Далее** tugmasi bosiladi. Komponentalarning sukunat bo’yicha berilgan ro’yhatini qayta tiklash uchun **Сброс** tugmasi bosiladi.

8. QADAM BOSHQA ANTIVIRUS DASTURLARINI TIZIMDAN QIDIRISH

Ushbu etapda kompyuterga o’rnatilgan boshqa Antivirus tasturiy vositalarini jumladan “Kaspersky Laboratoriyasi” ilovalarin qidirish protsessi ko’rib chiqiladi.

Agar kompyuteringizda biron o’rnatilgan Antivirus dasturi aniqlansa, o’sha dastur xaqida ro’yhat xavola qilinadi .Dasturni o’rnatishni davom ettirish uchun ularni tizimdan o’chirib tashlash taklif etiladi.

Agar tizimda biz o’rnatayotgan antivirusning bitta oldingi eski versiyasi aniqlansa ushbu versiyani o’chirib tashlashdan oldin uning kalit fayli va boshqa parametrlarini saqlab qolish tavsiya etiladi.

Bu bilan yangi versiyaga kalit olish talab qilinmaydi va eskisini kalit sifatida ishlatish imkoniyati tug’iladi.

O’rnatish ishlarini davom ettirish uchun **Далее** tugmasi bosiladi.

9. QADAM DASTURNING O’RNATILISHINI TEKSHIRISH ISHLARINI SO’NGI BOSQICHI

Ushbu etapda Kaspersky Antivirusining kompyuteringizga o’rnatishning eng so’ngi pallasi xavola etiladi.

Boshlang'ich va tanlov bo'yicha o'rnatish paytida При первоначальной и выборочной установке (5ch qadam) dasturda **Включить зашиту модулей до начала установки** yozuvidagi bayroqchani olib tashlash tavfsiya etilmaydi. Bu Kaspersky Antivirusining modulini ruxsat etilmagan foydalanuvchilarning o'zgartirish kiritishidan saqlaydi. Dastur qayta o'rnatilganda yoki qayta tiklanadigan xollardagina bayroqchani olib turish tavfsiya etiladi.

O'rnatish ishlarini davom ettirish uchun **Далее** tugmasi bosiladi. Natijada dastur distributivlarining kompyuterga ko'chirilish priotsesi boshlanadi.

Antivirus o'rnatilish paytida amaldagi barcha tarmoq bog'lanishlari vaqtinchalik dastur tomonidan to'xtatiladi. Ushbu bog'lanishlar bir qancha vaqtdan so'ng yana ishga tushadi.

10. QADAM O'RNATISH ISHLARINI YAKUNLASH

Завершение установки oynasi Kaspersky Antivirusining kompyuterga o'rnatilib bo'lganligini xaqidagi axborotni o'z ichiga oladi.

Keyingi qadam – Kompyuteringizdagi axborotlarning xavfsizligini maksimal darajada ta'minlash uchun dasturni sozlashdan iborat .

11.QADAM DASTURNI AKTIVATSIYA QILISH

Kaspersky Antivirusini aktivatsiyasi, yuqorida aytilgandek agar Kasperskyning eski versiyasi mavjud bo'lsa va litsenziya muddati xali tugamagan bo'lsa ushbu kalitni o'chirmasdan ushbu versiyaga qo'llasa bo'ladi. Agar dastur endi o'rnatilayotgan bo'lsa u xolda "**Активация с помоshью ключа**" saxifasidagi "**Обзор**" tugmasi bosiladi. Shundan so'ng sizdan (.key) kengaytmali kalit faylining joylashgan manzilini ko'rsatish talab etiladi. Kalit fayl manzili ko'rsatilgan dan so'ng "**Далее"** tugmasi bosiladi.

Xarid qilingan kalit xaqidagi qisqacha axborot beruvchi saxifa ochiladi. O'rnatishni davom ettirish uchun ushbu saxifadagi "**Далее"** tugmasi bosiladi.:

Keyingi etapda dastur tizimdagi barcha sistemali fayllar va kataloglarni analiz qilib chiqadi. Bu esa keyinchalik ushbu analiz qilingan fayllarning xavfsizligini kuchli ta’minlash imkonini beradi.

Keyingi etapda Kaspersky Antivirusini kompyuterga o’rnatishning so’ngi pallasini namoyish qiluvchi oyna xavola qilinadi. Ushbu oynada sukunat bo’yicha “Запустить Kaspersky internet Security” punktida bayroqcha belgilangan bo’ladi va “Завершить” tugmasini bosganimizda o’rnatish ishlari oynasi yopiladi va Kaspersky dasturini ishga tushadi.

Dasturning tashqi interfeys