15-amaliy mashg‘ulot. Axborot kommunikatsiya tizimlarda xavfsizlikni ta’minlash.

Reja.

15.1.Axborotni himoyalash usullari

15.2. Antivirus dasturlari bilan ishlash

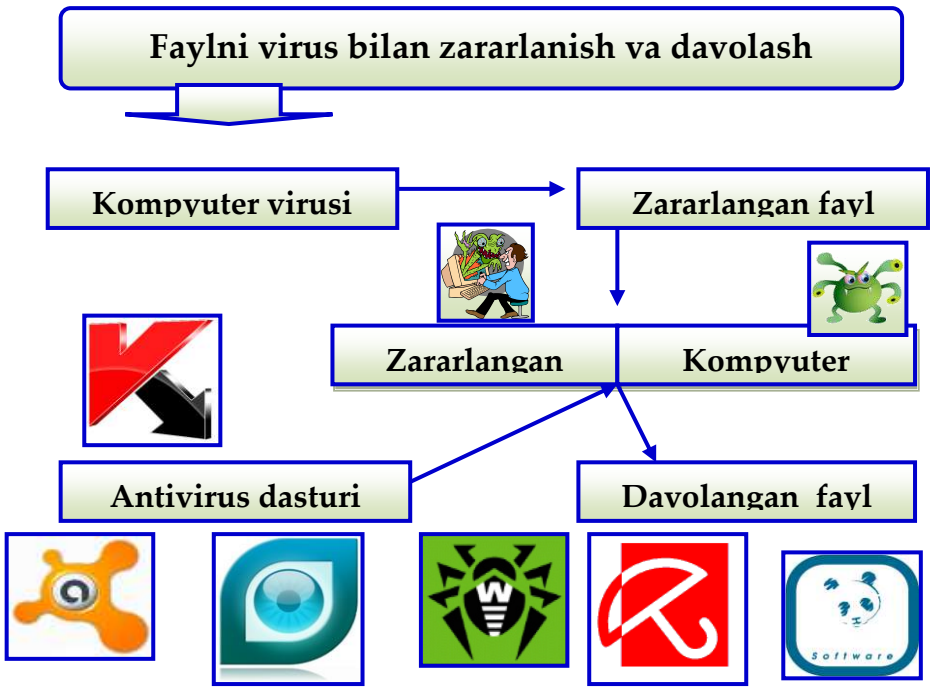
15.3. Kompyuterlarda axborot xavfsizligi

15.4. Axborot xavfsizlinini ta‘minlash vositalari

Maqsad: Mazkur amaliy ishni bajarish jarayonida talabalar kompyuter viruslari, kompyuter viruslari turlari va ulardan himoyalanish bo‘yicha amaliy ko‘nikmaga ega bo‘ladilar.

***Mavzuga oid asosiy tushunchalar*: (https://nrm.uz/)**

kompyuter virusi - destruktiv xususiyatga, o‘z nusxasini ko‘paytira olish (asl nusxa bilan to‘liq mos bo‘lmasligi ham mumkin) va foydalanuvchi bilmagan holda ularni kompyuter tizimlari, tarmoqlari turli resurslari va shu borada joriy etish qobiliyatiga ega bo‘lgan dasturdir (bajariladigan kodlar to‘plami);



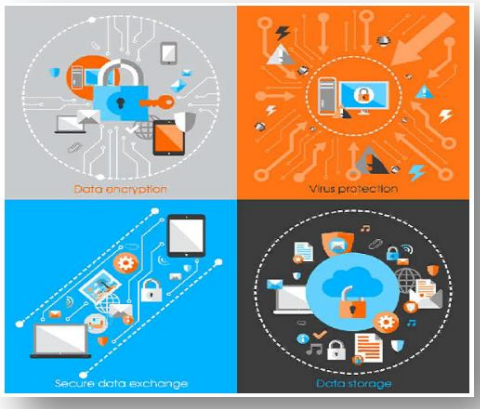
antivirus dasturi - kompyuter virusiga qarshi dastur, viruslarni aniqlash uchun mo‘ljallangan va ularni yo‘q qilish taklifini berishi mumkin bo‘lgan yoki yo‘q qiluvchi dastur;

antivirus himoyasi - antivirus dasturlari yordamida kompyuter viruslari ta’sirining oldini olish, viruslarni topish va zararsizlantirishga qaratilgan chora-tadbirlar majmui;

autentifikatsiya qilish - foydalanuvchi, dastur, qurilma yoki ma’lumotlarning haqiqiyligini tasdiqlash tartib-taomili;

axborot resursi - axborot tizimi tarkibidagi elektron shakldagi axborot, ma’lumotlar banki, ma’lumotlar bazasi;

axborot tizimi - axborotni to‘plash, saqlash, izlash, unga ishlov berish hamda undan foydalanish imkonini beradigan, tashkiliy jihatdan tartibga solingan jami axborot resurslari, axborot texnologiyalari va aloqa vositalari;



axborot xavfsizligi - axborot munosabatlarining sub'ektlariga nomaqbul ziyonlarni keltirishi mumkin bo'lgan tabiiy yoki sun'iy xususiyatli tasodifiy yoki qasddan qilingan ta'sirlardan axborot va ta'minlab turadigan infratuzilmaning muhofaza qilinganligi;

axborot xavfsizligi noxush hodisasi - axborot xavfsizligining yagona voqeasi yoki bir qator noxush yoki kutilmagan voqealari bo'lib, ushbu voqealar tufayli axborotning oshkor bo'lishi va axborot xavfsizligiga tahdidlar ehtimoli;

hujum - axborot aktivlarini yo'q qilish, ochish, o'zgartirish, blokirovkalash, tutib olish, ruxsat etilmagan foydalanish huquqini olish yoki axborot aktivlaridan ruxsatsiz foydalanishga urinish;

monitoring - avtomatlashtirilgan axborot tizimlari holatini kuzatish;

server xonasi - korxona serverlari, telekommuni-katsiya qurilmalari, uzluksiz quvvat manbalari va boshqa hisoblash texnikalari joylashgan xona;

tarmoqlararo ekran - avtomatlashtirilgan tizimiga kelib tushadigan va (yoki) tizimdan chiqib ketadigan axborotning nazorat qilinishini amalga oshiradigan dastur va (yoki) dasturiy vosita;

xesh summasi - kriptografik algoritm yordamida hisoblangan, fayl butligini tekshirish summasi;

shaxsga doir ma'lumotlar - muayyan jismoniy shaxsga taalluqli bo'lgan yoki uni identifikatsiya qilish imkonini beradigan, elektron tarzda, qog'ozda va (yoki) boshqa moddiy jismda qayd etilgan axborot;

avtomatlashtirilgan tizim - faoliyat sohasida axborotni to'plash, saqlash, izlash, unga ishlov berish va undan foydalanishni amalga oshirish uchun mo'ljallangan axborot tizimi;

elektron arxiv - arxiv maqomiga ega bo'lgan, bank elektron hujjatlarini jamlovchi, hisobga oluvchi, saqlovchi va foydalanishni amalga oshiruvchi bankning tarkibiy bo'limi.

Manba: **https://studfile.net/preview/7882776/**

Kompyuter virusi nima?

Viruslardan himoyalanish har bir kompyuter foydalanuvchisi oldida turgan asosiy muammolardan biri hisoblanadi. Kompyuter viruslaridan keladigan zararlar milliardlab dollarlar bilan belgilanadi.

Kompyuter virusi – maxsus yozilgan dastur bo'lib, kompyuterda ishlashda barcha mumkin bo'lgan xalaqitlarni yaratish, fayl va kataloglarni buzish, dasturlarni ishdan chiqarish maqsadida hisoblash tizimlariga, kompyuterning tizimli sohalariga, fayllarga tadbiq qilinadigan, o'zlarining nusxalarini yaratish, boshqa dasturlarga o'z-o'zidan birikib oladigan xossalarga egadirlar.

Ichida virus joylashgan dastur ***zararlangan*** deb ataladi.

Bunday dastur o‘z ishini boshlaganda, oldin boshqarishni virus o‘z qo‘liga oladi.

Virus boshqa dasturlarni topadi va «zararlantiradi» hamda biror-bir zararli ishlarni (masalan, fayllarni yoki diskda fayllarni joylashish jadvalini buzadi, tezkor xotirani ishlash jarayonini pasaytiradi va h.k.) bajaradi.

Virusni niqoblash uchun boshqa dasturlarni zararlantirish va zarar yetkazish bo‘yicha ishlar har doim ham emas, aytaylik ma’lum bir shartlar bajarilganda bajarilishi mumkin.

Virus unga kerakli ishlarni bajargandan keyin u boshqarishni o‘zi joylashgan dasturga uzatadi va u dastur odatdagiday ishlay boshlaydi. Shu bilan birga tashqi ko‘rinishdan zararlangan dasturning ishlashi zararlanmagandek kabi ko‘rinadi.

Viruslarning ko‘pgina ko‘rinishlari shunday tuzilganki, zararlangan dastur ishga tushirilganda virus kompyuter xotirasida har doim qoladi va vaqti-vaqti bilan dasturlarni zararlantiradi va kompyuterda zararli ishlarni bajaradi.

Virusning barcha harakatlari yetarlicha tez bajarilishi mumkin va biror-bir xabarni bermaydi, shuning uchun foydalanuvchi kompyuterda birorta odatdan tashqari ishlar bo‘layotganini payqashi juda mushkuldir.

Kompyuterda nisbatan kam dasturlar zararlangan bo‘lsa, virusning borligi deyarli sezilarsiz bo‘ladi. Lekin vaqt o‘tishi bilan kompyuterda qandaydir g‘alati hodisalar ro‘y bera boshlaydi, masalan:

- ba’zi dasturlar ishlashdan to‘xtaydilar yoki noto‘g‘ri ishlaydi;
- ekranga begona xabar yoki belgilar chiqadi;
- kompyuterning ishlash tezligi sekinlashadi;
- ba’zi bir fayllar buzilib qoladi va h.k.

Bu vaqtga kelib, qoidaga ko‘ra, foydalanuvchi ishlayotganda yetarlicha ko‘p (yoki hatto ko‘pchilik) dasturlar viruslar bilan zararlangan, ba’zi bir fayl yoki disklar esa ishdan chiqqan hisoblanadi.

Bundan tashqari, foydalanuvchi kompyuteridagi zararlangan dasturlar disketalar yordamida yoki lokal tarmoq bo‘yicha foydalanuvchi hamkasblari va o‘rtoqlarining kompyuteriga o‘tib ketgan bo‘lishi mumkin.

Viruslarning ba’zi bir ko‘rinishlari o‘zlarini yanada xavfliroq kirib tushadilar. Ular boshlanishda katta miqdordagi dasturlarni yoki disklarni bildirmasdan zararlantiradilar, keyin esa jiddiy shikastlanishlarini keltirib chiqaradi, masalan, kompyuterdagi butun qattiq diskni formatlaydi.

Dastur – virus sezilarsiz bo‘lishi uchun u katta bo‘lmasligi kerak. Shuning uchun, qoidaga ko‘ra, viruslar yetarlicha yuqori malakali dasturlovchilar tomonidan ***Assembler*** tilida yoziladi.

Kompyuter viruslarini paydo bo‘lishi va tarqatilishi sabablari, bir tomondan, inson shahsiyatining ruhiyatida va uning yomon xislatlarida yashirinadi (havaslar, qasos olishlar, tan olinmagan ijodkorlarning mansabparastligi, o‘z qobiliyatlarini konstruktiv qo‘llash imkoniyati yo‘qligi), ikkinchi tomondan esa, himoya qilishning apparat vositalarini va shaxsiy kompyuterning operatsion tizimi tomonidan qarshi harakatlarning yo‘qligi bilan bog‘liqdir.

Viruslarni kompyuterga kirib olishining asosiy yo‘llari olinadigan disklar (egiluvchan va lazerli) ham kompyuter tarmoqlari hisoblanadi. Qattiq diskni viruslar

bilan zararlanishi kompyuterni virusni o‘zida saqlagan disketadan yuklaganda amalga oshishi mumkin.

Bunday zararlanish tasodifiy bo‘lishi mumkin, masalan, disketani A diskovoddan chiqarib olmasdan va kompyuterni qayta yuklanganda, bunda disketa tizimli bo‘lmasligi ham mumkindir. Disketani zararlantirish juda oddiyroqdir. Unga virus hattoki, agar disketani zararlangan kompyuter diskovodiga qo‘yilganda va uning mundarijasini o‘qilganda, tushish mumkin.

Zararlangan disk bu yuklanish sektorida dastur – ***virus joylashgan diskdir.***

Virusni o‘z ichiga olgan dastur ishga tushirilgandan keyin boshqa fayllarni zararlantirish mumkin bo‘lib qoladi.

Eng ko‘proq viruslar bilan diskning yuklanadigan sektori va ***.EXE, *.COM, *.SYS** yoki **BAT** kengaytmasiga ega bo‘lgan fayllar zararlanadi.

Kam matnli va grafikli fayllar kam zararlanadi.

Zararlangan dastur, bu unga tadbiq qilingan dastur – virusni o‘z ichiga olgan dasturdir. Kompyuter virusi bilan zararlanishda o‘z vaqtida uni payqash juda muhimdir. Buning uchun viruslarni paydo bo‘lishining asosiy belgilari to‘g‘risida bilimlarga ega bo‘lish kerak.

Ularga quyidagilar tegishli bo‘lishi mumkin:

- ***oldin muvaffaqiyatli ishlagan dasturlarning ishlashdan to‘xtashi yoki noto‘g‘ri ishlashi;***
- ***kompyuterning sekin ishlashi;***
- ***operatsion tizimni yuklash imkoni yo‘qligi;***
- ***fayl va kataloglarni yo‘qolib qolishi yoki ularning mazmunini buzilishi;***
- ***fayllarni o‘zgartirilganlik sanasi va vaqtining o‘zgarishi;***
- ***diskda fayllar soni bexosdan juda oshib ketishi;***
- ***bo‘sh tezkor xotira o‘lchamining jiddiy kamayishi;***
- ***ekranga ko‘zda tutilmagan xabarlarni yoki tasvirlarni chiqarish;***
- ***ko‘zda tutilmagan tovushli xabarlarni berish;***
- ***kompyuter ishlashda tez-tez bo‘ladigan osilib qolishlar va buzilishlar.***

Ta’kidlash kerakki, yuqorida sanab o‘tilgan hodisalar viruslarni kelib chiqishi bilan bo‘lishi majburiy emas, boshqa sabablarning oqibatlari ham bo‘lishi mumkin. Shuning uchun kompyuter holatini to‘g‘ri diagnostikalash har doim mushkuldir.

Kompyuter virusi kompyuterda mavjud bo‘lgan disklardagi istalgan faylni yetarlicha o‘zgartirish va buzishi mumkin.

Lekin fayllarning ba’zi bir turlarini virus «zararlantirishi» mumkin. Bu shuni bildiradiki, virus bu fayllarga «tadbiq» qilinishi mumkin, ya’ni ularni shunday o‘zgartiradiki, ular virusni o‘z ichida saqlaydi va bu virus ba’zi bir holatlarda o‘zining ishini boshlashi mumkin.

Ta’kidlash lozimki, dastur va hujjatlarning matnlari, ma’lumotlar bazasining axborotli fayllari, jadvalli protsessor jadvallari va boshqa shunga o‘xshash fayllar virus bilan zararlanishi mumkin emas, bu fayllarni viruslar buzishi mumkin.

Virus bilan «zararlanishi» mumkin bo‘lgan fayllarning turlari quyidagilardir:

1. ***Bajariladigan fayllar***, ya’ni **.SOM** va **.YeXE** kengaytmali fayllar, hamda boshqa dasturlar bajarilganda yuklanadigan overlokli (takrorlanadigan) fayllardir. Zararlangan bajariladigan fayllardagi virus shu virus joylashgan dastur ishga tushirilganda o‘zining ishini boshlaydi. Virus bilan zararlanishning eng xavflisi **DOS** buyruqli protsessorini **COMMAND.COM** dasturini zararlanishidir, chunki bu virus **DOS**ning istalgan buyrug‘i bajarilganda ishlaydi va istalgan bajariladigan dastur zararlanadi (agar virus uni zararlantira olsa).

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, vaksinalar, privivkalar, revizorlar, monitorlar***.

Detektorlar – virusning signaturasi (virusga taalluqli baytlar ketma-ketligi) bo‘yicha operativ xotira va fayllarni ko‘rish natijasida ma’lum viruslarni topadi va xabar beradi. Yangi viruslarni aniqlay olmasligi detektorlarning kamchiligi hisoblanadi.

Faglar – yoki doktorlar, detektorlarga xos bo‘lgan ishni bajargan holda zararlangan fayldan viruslarni chiqarib tashlaydi va faylni oldingi holatiga qaytaradi.

Vaksinalar **-** yuqoridagilardan farqli bo‘lib, u himoyalanayotgan dasturga o‘rnatiladi. Natijada dastur zararlangan deb hisoblanib, virus tomonidan o‘zgartirilmaydi. Faqatgina ma’lum viruslarga nisbatan vaksina qilinishi uning kamchiligi hisoblanadi. Shu bois, ushbu antivirus dasturlar 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 haqida 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 hakida xabar beradi.

Doktor dasturlari nafaqat virus bilan kasallangan fayllarni topadi, balki ularni davolab, dastlabki holatiga qaytaradi.

Bunday dasturlarga ***Aidstest, Doctor Web*** dasturlarini misol qilib keltirish mumkin. Yangi viruslarning to‘xtovsiz paydo bo‘lib turishini hisobga olib, doktor dasturlarni ham yangi versiyalari bilan almashtirib turish lozim.

https://www.softmagazin.ru/blog/dr_web/ - **Dr.Web - funksii, vozmojnosti i preimuщestva**

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 boshlang‘ich holatlarini bir-biri bilan solishtiradi. Bu dasturga ADINF dasturini misol qilib keltirish mumkin.

Viruslarga qarshi chora-tadbirlar

Kompyuterni viruslar bilan zararlanishidan va axborotlarni ishonchli saqlashini ta’minlash uchun quyidagi qoidalarga amal qilish lozim:

- kompyuterni zamonaviy antivirus dasturlar bilan ta’minlash;
- disketalarni ishlatishdan oldin har doim tekshirish;
- qimmatli axborotlarning nusxasini har doim arxiv fayl ko‘rinishida tarmoqlarda saqlash.

Kompyuter viruslarig qarshi kurashning quyidagi turlari mavjud:

- kompyuter viruslari kompyuterga kirganda 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;
- kiritilayotgan dasturlarni viruslarning mavjudligiga tekshirish;
- antivirus dasturlaridan keng foydalanish;
- davriy ravishda kompyuterlarni antivirus dasturlari yordamida viruslarga qarshi tekshirish.

Viruslarni aniqlash va davolash usullari

Hozirgi kunda kompyuter viruslariga qarshi kurashga ixtisoslashgan kompaniyalar vujudga kelgan. Ular har kun, har soat mijozlarning kompyuteridagi mavjud viruslarni topib, ularni yo‘q qiladigan antivirus dasturlarini yaratadilar.

Hozirgi kunda kompyuter viruslariga qarshi kurashuvchi antivirus dasturlaridan eng asosiylari **KasperskyAnti-Virus (AVP) ScriptChecker, NortonAntivirus, DrWeb, Adinf, AVP**lar hisoblanadi.

KasperskyAnti-Virus dasturi bugungi kunda kompyuter viruslarining 100000 dan ortiq turini aniqlaydi va davolaydi.

Kompyuter viruslaridan himoya qilish usullari

Kompyuter viruslaridan himoya qilishning uchta chegarasi mavjuddir:

- viruslarning kirib kelishini bartaraf etish;
- agar virus baribir kompyuterga kirgan bo‘lsa, virus hujumini bartaraf etish;
- agar hujum baribir amalga oshgan bo‘lsa, buzuvchi oqibatlarni bartaraf etish.

Himoya qilishni amalga oshirishning uchta usuli mavjuddir:

- himoya qilishning dasturli usullari;
- himoya qilishning apparatli usullari;
- himoya qilishning tashkiliy usullari.

Muhim ma’lumotlarni himoya qilish masalasida ko‘pincha maishiy yondashish ishlatiladi: «kasallikni davolagandan ko‘ra uning oldini olgan yaxshiroq».

Afsuski, aynan u eng buzuvchi oqibatlarni keltirib chiqaradi. Kompyuterga viruslarni kirib olish yo‘lida barrikadalarni yaratib olib, ularning mustahkamligiga ishonib va buzuvchi hujumdan keyingi harakatlarga tayyor bo‘lmasdan qolmaslik kerak. Shu bilan birga, virusli hujum, bu muhim ma’lumotlarni yo‘qotishni yagona bo‘lmagan hattoki keng tarqalmagan sababidir. Shunday dasturli uzilishlar mavjudki, ular operatsion tizimni ishdan chiqarishi mumkin hamda shunday apparatli uzilishlar borki, ular qattiq diskni ishlashga layoqatsiz qilib qo‘yish qobiliyatiga egadirlar. O‘g‘irlash, yong‘in yoki boshqa favqulodda holatlar natijasida muhim ma’lumotlar bilan birgalikda kompyuterni yo‘qotish ehtimoli har doim ham mavjuddir.

Shuning uchun xavfsizlik tizimini yaratishni birinchi navbatda «oxiridan» boshlash kerak – istalgan ta’sirni, u virus hujumi, xonada o‘g‘irlik yoki qattiq diskni fizik ishdan chiqishidan qat’iy nazar, buzuvchi oqibatlarini bartaraf etishdan boshlash kerak.

Ma’lumotlar bilan ishonchli va xavfsiz ishlashga faqat shundagina erishiladiki, agar istalgan kutilmagan hodisa, shu jumladan kompyuterni to‘liq fizik ishdan chiqarish ham, salbiy oqibatlarga olib kelmasligi kerak.

Ishni bajarish uchun topshiriqlar

1. Kompyuterni zararlovchi virus turlari haqida ma’lumot bering.
2. Hozirda qўllanilayotgan antiviruslar haqida ma’lumot bering.
3. Viruslarni kompyuterga tushish yўllarini tushuntirib bering.
4. Antivirus dasturlari turlarini bir-biridan farqini tushuntiring.

Nazorat savollari

1. Kompyuter virusi nima?
2. Fayl va disklarda kompyuter viruslari mavjudligini tekshirish.
3. Elementlarni, uzel(tugun) va qurilmalarda kompyuter viruslari mavjudligini tekshirish.
4. Virus nima va uning bajaradigan vazifasi?
5. Viruslar kompyuterda qanday paydo bo‘ladi?
6. Viruslarning qanday turlarini bilasiz?
7. Kompyuterda viruslar mavjudligi qanday aniqlanadi?
8. Antivirus dasturlarining qanday turlarini bilasiz?
9. Kompyuter viruslaridan himoyalanishda ehtiyotkorlik choralari nimalardan iborat?

Qo‘shimcha (Internet) materiallari:

Axborotlarni tashuvchi vositalar: fleshka, CD va DVD disklar:

- Flesh disklar juda katta hajmdagi axborotni o‘z ichiga sig‘dira oladigan yarim o‘tkazgichli elementlardan qurilgan xotira.
- Hozirgi kunda flesh xotiralarning hajmi **64 Gb** gacha bo‘lgan axborotni o‘ziga sig‘dira oladi.
- Flesh xotiralar o‘lcham jihatidan juda kichik bo‘lib foydalanish uchun juda qulay. Ma’lumot yozish tezligi **6700** kbayt/sek gacha etadi.
- Ma’lumot o‘qish tezligi esa 18000 kbayt/sek gacha boradi.
- Flesh xotiralar hozirgi kunda eng asosiy axborot tashuvchilardan hisoblanadi.
- **CD** disklar – bu kompakt disk so‘zlarining bosh harflaridan olingan nomli disklar bo‘lib, axborotlarni saqlash uchun optik yuzadan iborat, yumaloq disk ko‘rinishidagi axborot tashuvchi hisoblanadi. Kompakt disklar 700 Mbayt hajmga ega bo‘lib, unga ma’lumot disk o‘quvchi qurilmaning lazer nuri yordamida yoziladi va o‘qiladi.
- **DVD** disklar – bu dijital video disk so‘zlarining bosh harfidan iborat nomli disklar hisoblanadi. Bu disklar 4.5 Gbayt hajmga ega bo‘lib, CD disklarga nisbatan 7 barobar ko‘p axborot sig‘dirishi mumkin.

Kompyuter viruslari haqida va ularning turlari

- Hozirgi kunda hamma kompyuter foydalanuvchilari virus degan tushunchani yaxshi bilishadi. Bu kichik dastur bilan bir necha bor uchrashishgan. Ko‘p hollarda mag‘lub ham bo‘lishgan. Bilib olgan bo‘lsangiz bu maqolamiz viruslarga bag‘ishlanadi.
- ***Virus*** – bu dasturchi tomonidan tuzilgan, kompyuter ish faoliyatini tekis ishlashiga halaqit beradigan, oqibatda kompyuterni yoqilishini ham taqiqlab qo‘yadigan dasturdir. Bu dasturlar asosan internet tarmog‘i orqali foydalanuvchi kompyuteriga tushadi.
- Albatta, bu dastur, internet foydalanuvchisi bilmagan holda o‘z kompyuterida paydo bo‘ladi. Ularga qarshi kurashadigan dastur antivirus deyiladi (bu to‘g‘risida keyingi maqolalarda).
- ***Viruslar kompyuterlarda o‘zini har hil tutadi***. Ba’zi birlari kompyuteringizni kerakmas fayllar bilan to‘ldirsa, yana ba’zilari operativ xotirani ko‘p qismini ishlatib, kompyuteringizni qotirib qo‘yadi, viruslarning bir qismi esa, kerakli fayllaringizni yoki tizim fayllarini o‘chirib sizga zarar yetkazadi. Shulardan saqlanish uchun viruslarning

turini bilib olish lozim, ya’ni qaysi virus nima ish qiladi va bundan saqlanish o‘z o‘zidan kelib chiqadi. Quyida ularning turlari keltirilgan(turlari ref.uz dan olindi):

- ***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 yo‘li intranet tarmoqlari orasida tarqaladi. Tarqalish usuli sifatida elektron xatlar yoki boshqa tez tarqaluvchi mexanizmlardan foydalanadi. Ular haqiqatdan 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 (zagruzka) 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** hujjatlarini 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) – Rootkit’lar viruslar*** orasida o‘zlarining eng xavfliligi va yashirinishga ustaligi bilan alohida ajralib turadi. **Rootkit’**lar kompyuteringizni yovuz hakerlar tomonidan qo‘lga olinishi uchun foydalaniladi. Ba’zi **Rootkit’**larni antivirus programmalari ham aniqlay olmaydi, chunki ular o‘zlarini operativ tizim fayllari sifatida ko‘rsatishadi. **Rootkit’**lar 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.

https://www.texnoman.uz/post/kompyuter-viruslari-haqida-va-ularning-turlari.html - Kompyuter viruslari haqida va ularning turlari

Operasion tizimning axborot xavfsizligini ta’minlash vositalari

Detektor dasturlar

- bir nechta taniqli viruslar bilan zararlangan fayllarni aniqlash imkoniyatini beradi.
- foydalanuvchi tomonidan ko’rsatilgan diskda virusga oid maxsus baytlar kombinasiyasi borligini tekshiradi.
- U yoki bu faylda shunday holatlar borligi aniqlansa, u hakida foydalanuvchi tegishli xabarlar chiqariladi.
- Masalan: **Norton AntiVirus ili AVSP**
- **Polifag, skaner – antivirus dasturi**. Ishlash prinsipi fayllarni, disklarni yuklovchi sektorlarini va operativ xotirani tekshirish, ularda ma’lum va yangi viruslarni aniqlashga asoslangan
- **Antivirus blokirovka qiluvchi – posbon (monitorlar)-dasturlar**. Ular kompyuterning operativ xotirada rezendent sifatida joylashadi va operativ xotradi viruslarni ko’payishi va zarar keltiruvchi murojaatlarini ushlab oladi, va ular hakida foydalanuvchiga xabar beradi. «Virusli-xavfli» hollarga viruslarning o’z-o’zidan ko’payishi momentigaga xarakterli bo’lgan quyidagi holatlar kiradi: bajariladigan fayllarni yozish uchun ochishga chaqiruvlar, disklarning boot-sektoriga yoki vinchestriga yozuvlar. Foydalanuvchi joriy operasiyani bajarilishiga ruhsat berishi yoki mann qilishi mumkin.
- **Doktorlar – «davolovchi antiviruslar».**
- **Vaksinalar** - virus bilan zararlanmagan fayllarni zararlangan fayllar kabi ko’rinishga keltiradi. Virus dasturlar fayllarni zararalab borish jarayonida bu fayllarni «zararlangan» fayl sifatida hisoblab o’tkazib yuboradi.

Revezor dasturlar

- Ishlashnini ikkita stadiyasiga ega. Ular dastlab dasturlar va disklarni tizimli sohasini (yuklanuvchi sektorlar va qattiq diskni jadvalli bo’linishi sektorlarini) dastlabki holatini eslab qoladilar. Bu momentda dasturlar va disk sohalari viruslar bilan zaralanmagan deb qaraladi.
- Bunday paytlarda istalgan momentda dastur – revizor yordamida dasturlar va diskni tizimli sohalarini dastlabki va amaldagi holatini taqqoslash imkoniyati yuzaga keladi. Keyin aniqlangan nomuvofiqliklar haqida foydalanuvchiga xabar beriladi.
- Masalan, Kasperskiy dasturiga joylashtirilgan AdInf (Advanced Diskinfoscope) , IDSMonitor

Doktor - revizorlar

- Bu dasturlar fayllardagi va operasion tizimning diskli sohalaridagi o’zgarishlarni nafaqat aniqlaydi, balki o’zgarishlar ro’y berganda ularni avtomatik holda dastlabki holatiga keltiradi. Bunday dasturlar bir muncha universal hisoblanadi, ular fayllar va diskli sohalarni holatini oldindan saqlangan ma’lumotlari asosida davolash ishlarini amalga oshiradi.
- Lekin bu dasturlar, davolash momentlarida fayllarni zararlanish mexanizmi ma’lum bo’lgan kompyuter viruslarini davolaydi.
- **Masalan: AVP, Aidstest, Scan, Norton AntiVirus, Doctor Web.**

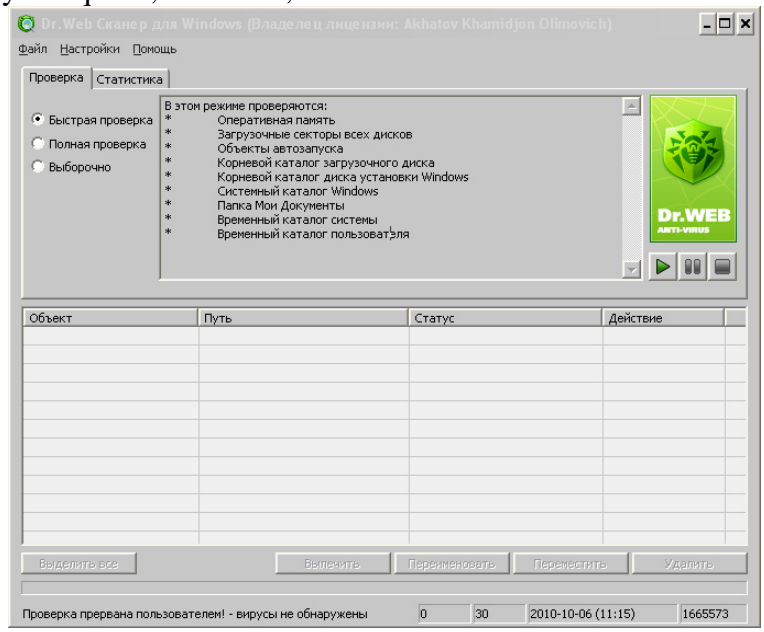
Antivirus Kasperskogo antivirus dasturining imkoniyatlari

•Viruslardan , troyan dasturlari va chuvalchang viruslardan himoyalash ;
•shipion, reklamali va potensial xavfli bo'lgan viruslardan himoyalash;
•Fayllarni, pochtalarni va intenet trafiklarni real vaqt rejimida tekshirish;
•yangi va noma'lum xurujlardan faol himoyalanish;
•istalgan tipdagi tashqi axborot tashuvchilarni antivirusnaya tekshiruvidan o'tkazish;
•arxivlangan fayllarni tekshirish va davolash;
•Microsoft Office hujjatlarida xavfli makroburuqlarni bajarilishini nazorat qilish;
•diskning buzilgan sohalarini qayta tiklash tizimi.

Antivir, DrWeb, Nod 32, Antivirus Kaspersky, Avast, Antivirus Panda

DOCTOR WEB

Doctor Web dasturini ishga tushurgandan so'ng antivirus dasturi avtomatik ravishda tizimga tegishli bo'lgan fayllarni tekshirib chiqadi. Doctor Web dasturining ishchi oynasi sarlavha satri, menyular qatori, tekshiruv, statistika va ishchi sohalardan iborat (9-rasm).

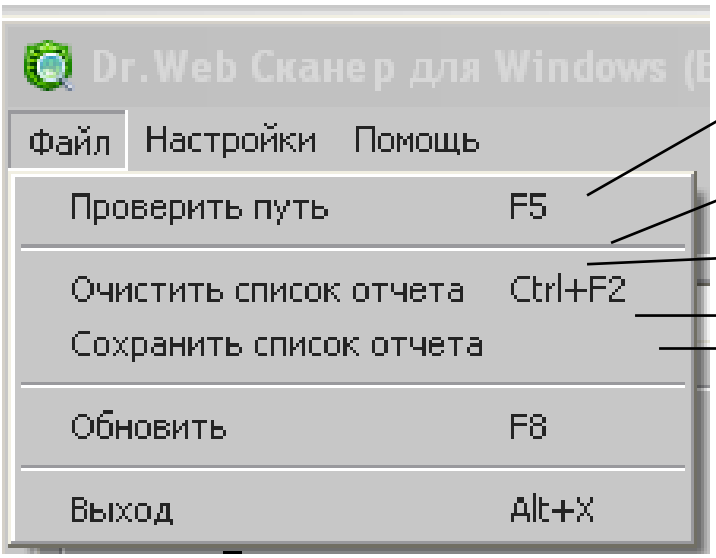


9-rasm

10-rasm

Menyular qatori

Файл (Fayl) menyusi quyidagi bo'limlardan iborat



Yo'lni tekshirish

Xisobotdagi ro'yxatni tozalash

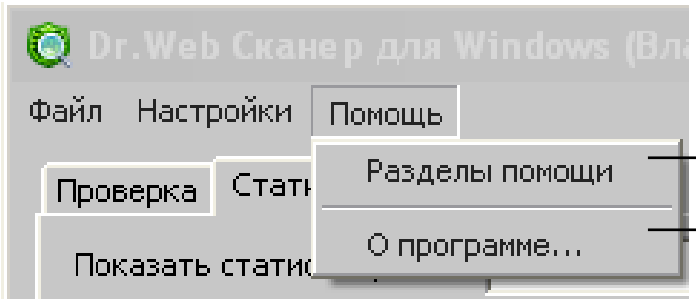
Xisobotdagi ro'yxatni saqlash

Obnovit

Dasturdan chiqish

Настройка (Sozlash) menyusi quyidagi bo’limlardan iborat

Dastur parametrlarini sozlash
Sozlangan parametrni saqlash
Tilni tanlash (Rus tili va Ingliz tili)
Помощь (Yordam) menyusi quyidagi bo’limlardan iborat



Yordamchi ma’lumot

Dastur haqida

Sozlash menyusidagi Bajarish (Действия) bo’limi orqali avtomatik ravishda kasallangan fayl va hujjatlarni davolash, davolab bo’lmagan fayllarni o’chirish va viruslarni o’chirish, arxivlangan va pochtali fayllarni o’zgartirish va qolgan buzuvchi va xavfli deb topilgan fayllarni o’chirishni dasturga ta’minlab qo’yish imkoniyati mavjud (11-rasm). Bajarish bo’limini o’zgartirgandan so’ng sozlash menyusidan Сохранить настройка bo’limi tanlanib saqlab qo’yilishi lozim.

11-rasm

Virus dasturlarni izlash 3-qismdan iborat:

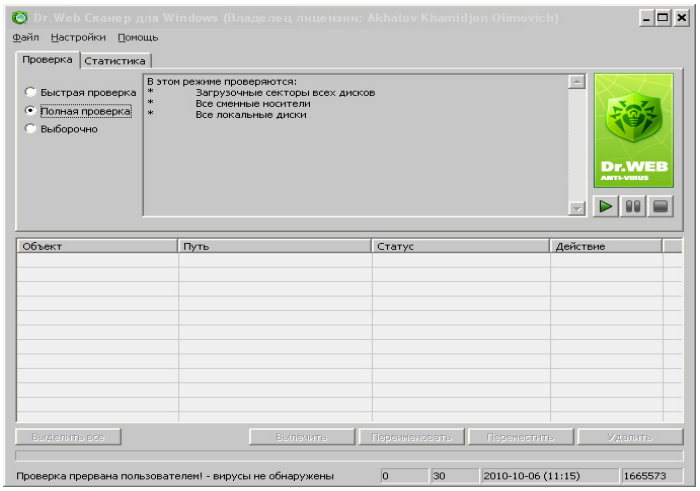
- Быстрая проверка (Tezkor izlash) (9-rasm)
- Полная проверка (To’liq tekshirish) (12-rasm)
- Выборочно (tanlov orqali tekshirish) (13-rasm)

Быстрая проверка (Tezkor izlash) orqali Operativ xotira va barcha disk sektorlaridagi fayllarni, avtomatik ishga tushuvchi ob’ektlarni, Windows operatsion tizimini ishga tushiruvchi tizimli fayllarni, Мои Документы (Mening hujjatlarim) papkasidagi fayllarni, vaqtinchalik saqlanayotgan katalog va fayllarni tezkor ravishda izlash imkoniyati mavjud.

Полная проверка (To’liq tekshirish) orqali barcha disk sektorlaridagi fayllarni, barcha asosiy va qo’shimcha o’rnatilgan disklarni to’liq ravishda tekshirish imkoniyati mavjud.

Выборочно (tanlov orqali tekshirish) orqali foydalanuvchining tanloviga ko’ra ixtiyoriy bitta yoki bir nechta disklarni tekshirish imkoniyati mavjud.

Foydalanuvchi tomonidan ixtiyoriy tekshirishlardan birortasi tanlangandan so’ng, начать проверку (tekshirishni boshlash) tugmasi bosiladi. Tekshirishni vaqtinchalik tuxtatib turish uchun Приостановить проверку (Tekshirishni to’xtatish) tugmasi bosiladi. Tekshirishni to’xtatish uchun Остановить проверку (Tekshirishni to’xtatish) tugmasi bosiladi.



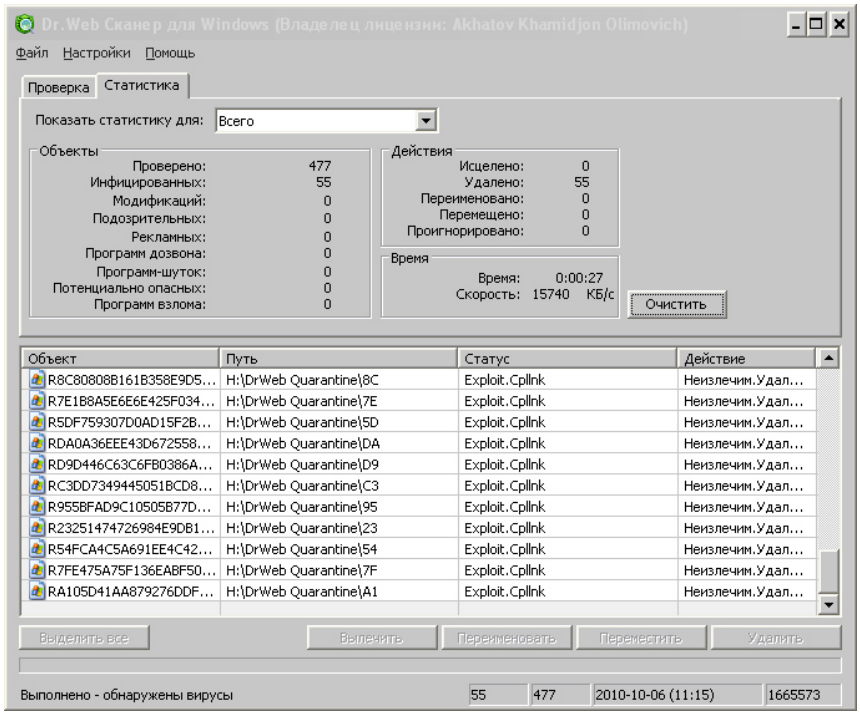
12-rasm

13-rasm

Virus dasturlari izlab topilgandan so’ng, dastur avtomatik ravishda zararlangan fayllarni davolaydi, davolab bo’lmagan fayllarni esa o’chirib chiqadi. Tekshirilgan fayllar, zararlangan fayllar, davolangan fayllar, o’chirilgan, arxivlangan va o’zgartirilgan fayllar sonini Статистика (Hisobot) oynasida ko’rsatib boriladi (14-rasm).

Agar sozlash menyusidan avtomatik davolash va o’chirish buyruqlari berilmagan bo’lsa, u holda topilgan virus dasturlarini sichqoncha yordamida yoki Выделеть все (Hammasini belgilash) tugmasi orgali belgilab, Вылечить (Davolash) tugmasi orqali zararlangan fayllarni davolash, Преименовать (O’zgartirish) tugmasi orqali o’zgartirish, Переместить (Ko’chirish) tugmasi orqali ishonchli joyga ko’chirish va Удалить (O’chirish) tugmasi orqali davolab bo’lmagan fayllarni o’chirish imkoniyati mavjud.

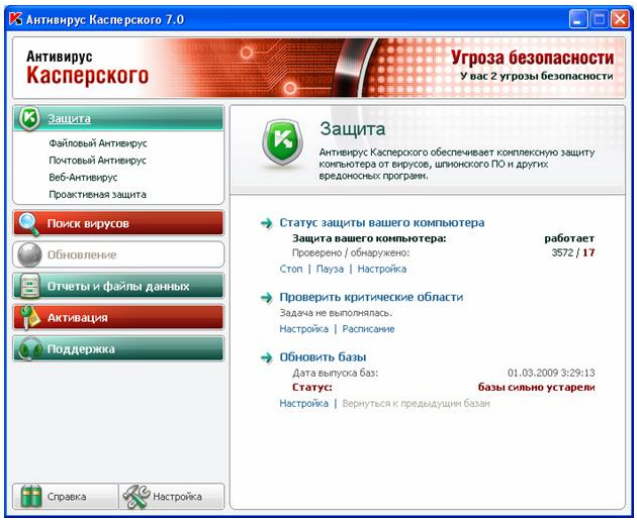
Oynaning eng qo’yi qismida esa topilgan viruslar sonini, tekshirib chiqilgan hujjatlar sonini, tekshirilgan vaqtni va sanani ko’rsatib turadi.



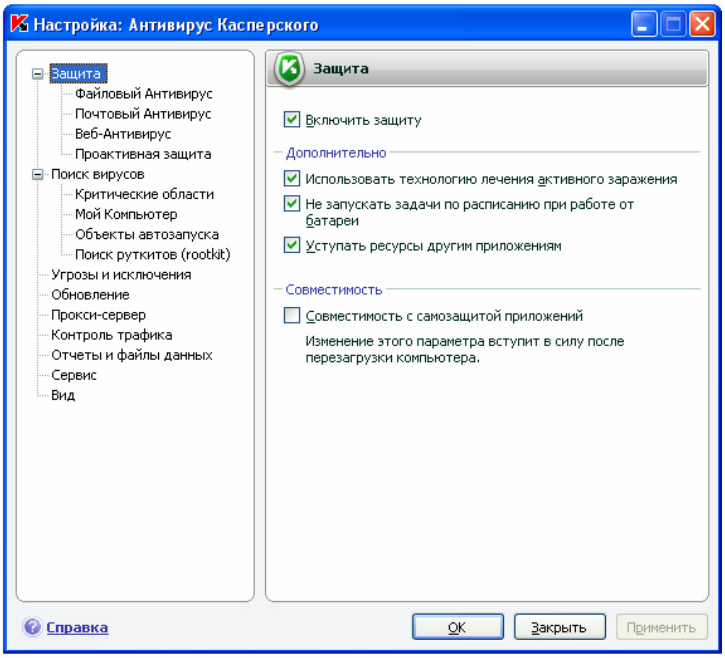
14-rasm

ANTIVIRUS KASPERSKIY

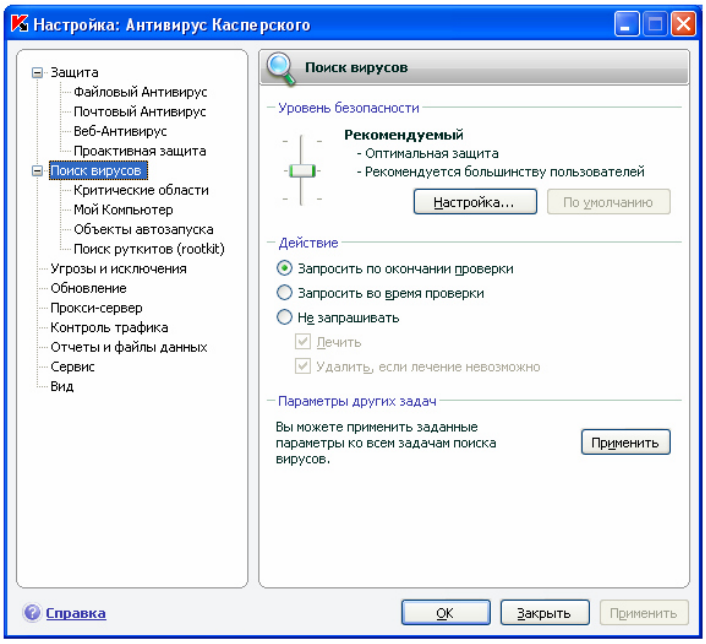
Kasperskiy antivirus dasturini ishga tushirgandan so’ng, sozlash (Настройка) qismiga kirib, virus dasturlarni izlab topgandan so’ng uni davolash, davolab bo’lmagan fayllarni esa o’chirishni avtomatik rejimga qo’yish lozim bo’ladi (16, 17 - rasmlar).



15-rasm



16-rasm



17-rasm

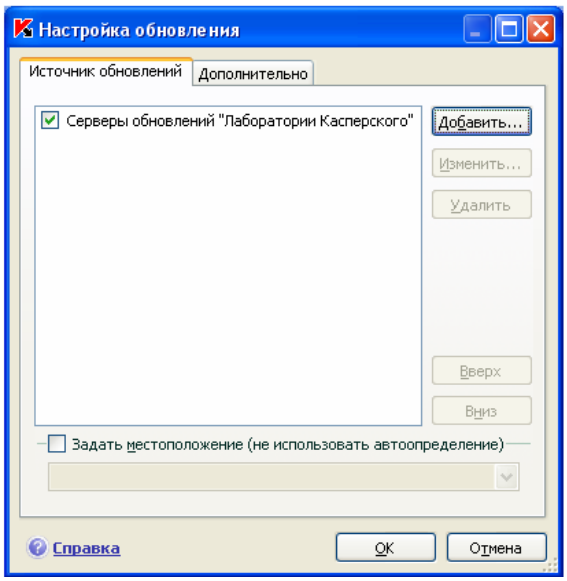
Dastur bazasini yangilab turish uchun sozlash (Настройка) bo'limiga kirib, Обновление qismidan kerakli buyruqlar tanlanadi. Обновление qismi quyidagi buyruqlardan iborat:

- Автоматически
- Каждый 1 день
- Вручную

Автоматически buyrug’i dastur har ishga tushirilganda baza avtomatik ravishda yangilanib turadi. Каждый 1 день buyrug’i bazani har kuni yangilab turadi. Вручную buyrug’i orqali esa foydalanuvchi o’zi hoxlagan vaqtda bazani yangilab turishi mimkin (18-rasm).

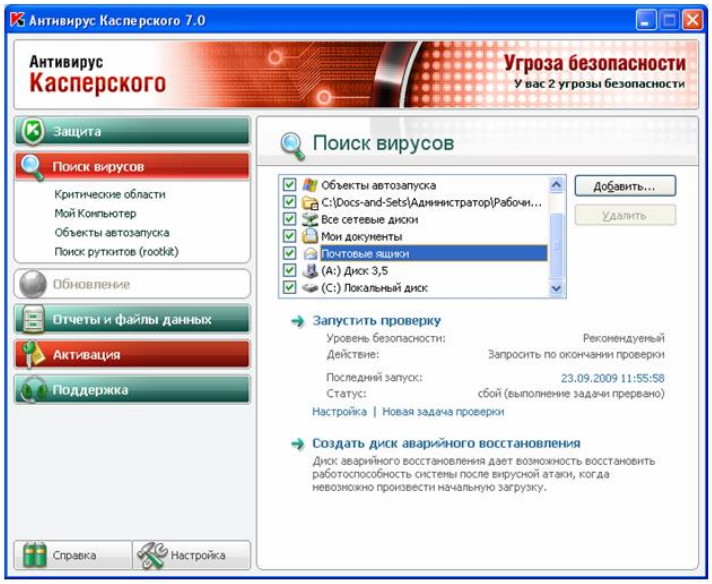
Buyruqlardan biri tanlangandan so’ng, sozlash (Настройка…) tugmasi bosiladi va bazani yo’li ko’rsatiladi. Agar kompyuter internet tarmog’iga ulangan bo’lsa, baza avtomatik ravishda yangilanadi. Agar baza kompyuterning o’zida bo’lsa, Добавить… tugmasi orqali baza turgan joy ko’rsatiladi va OK tugmasi bosiladi (19-rasm). Baza ko’rsatilgandan so’ng, dastur oynasidan Обновление tugmasi bosiladi va baza yangilanadi.

18-rasm



19-rasm

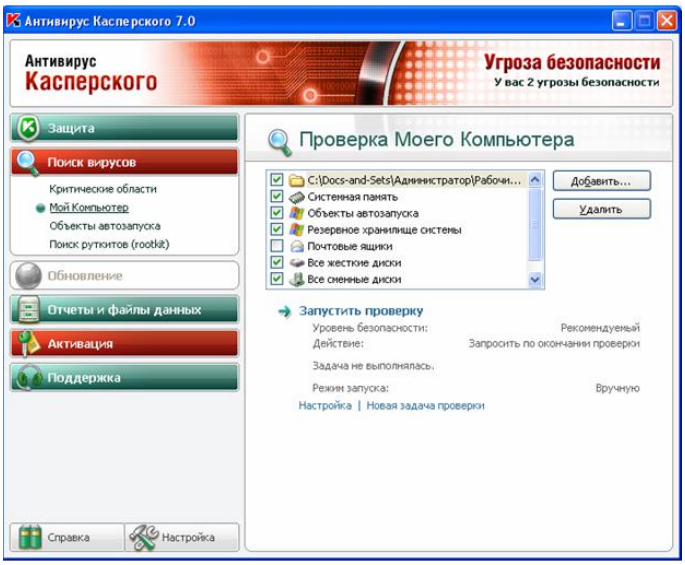
Virus bilan zararlangan dasturlarni izlash uchun Virusni qidirish (Поиск вирусов) qismiga kiriladi, kerakli buyruq tanlanib izlashni ishga tushirish (Запустить проверку) tugmasi bosiladi (20, 21, 22, 23 - rasmlar).



20-Rasm

21-Rasm

22-Rasm



23-Rasm

ESET NOD32 ANTIVIRUSI DA ISHLASH

ESET NOD32 antivurs dasturining ishchi oynasida quyidagi bo'limlar mavjud.

- Himoya holati (Состояние защиты)
- Kompyuterni tekshirish (Сканирование ПК)
- Bazani yangilash (Обновление)
- Sozlash (Настройка)
- Yordamchi ma'lumotlar (Справка и поддержка) (24-rasm)

24-Rasm

HIMOYA HOLATI (Состояние защиты) – bu bo'limda kompyuterdan aniqlangan virus dasturlar holati va turlari, ularning soni haqida to'liq ma'lumot berib turadi. (25,26-Rasmlar)

25-Rasm

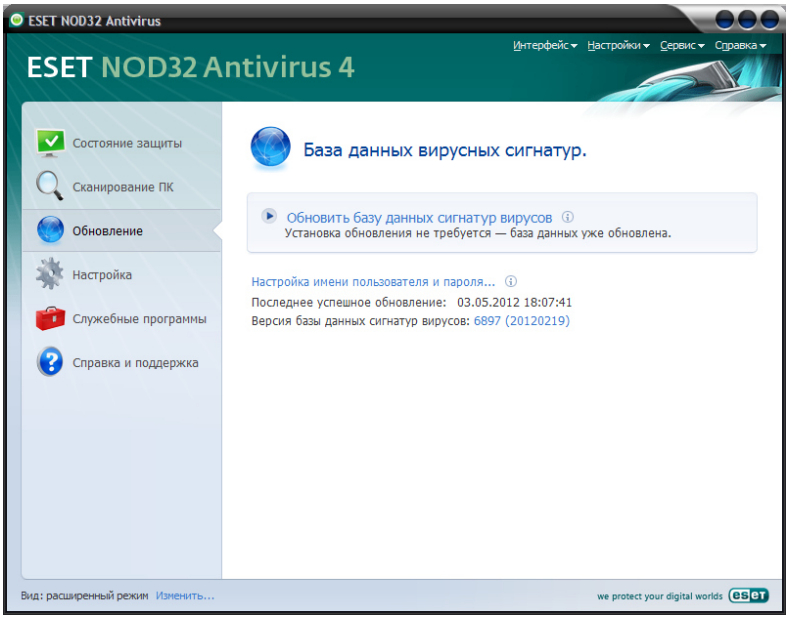
26-Rasm

KOMPYUTERNI TEKSHIRISH (Сканирование ПК) – bu bo'limda kompyuter disklarini virusga teshirish imkonini beradi. (27-rasm)

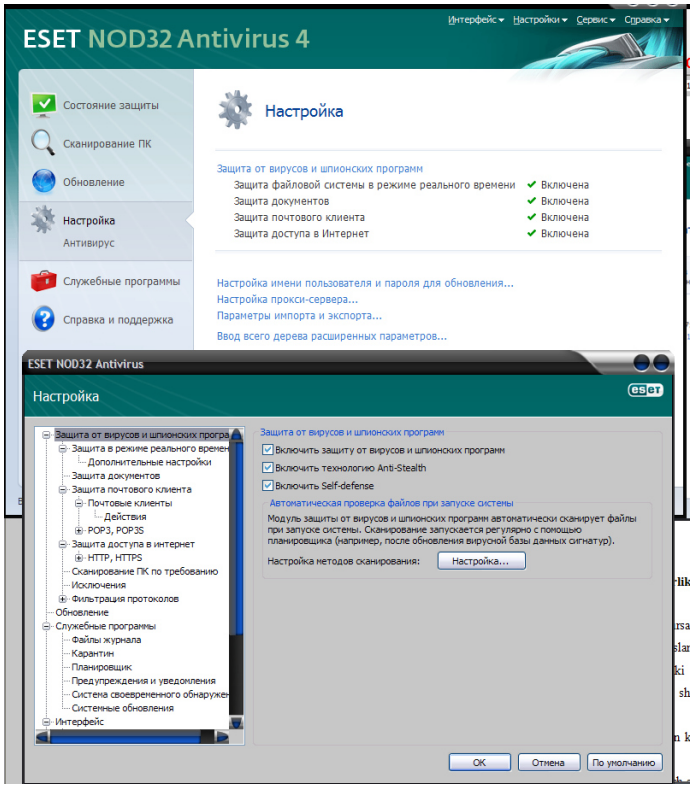
27-Rasm

BAZANI YANGILASH (Обновление) – bo'limoda antivirus dastur bazasini yangilab turish imkonini beradi**. (28-rasm)**

SOZLASH (Настройка) – bo'limoda dasturning parametrlarini sozlash, o'zgartirish, himoyani ishlash holatini sozlash imkoniyatini beradi. (29-rasm)



28-Rasm



29-Rasm

KOMPYUTER VIRUSLARIDAN SAQLANISHNINING EHTIYOTKORLIK TADBIRLARI

Virusdan kuriladigan zararlarga kuyidagilarni misol qilib kursatish mumkin:

• kompyuter qattik diski yoki tezkor xotirasining ifloslanishi — virusli dastur kupayishi jarayonida butun kattik diskni uzining nuktalari yoki boshka belgilari bilan tuldirishi 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 ukish mumkin bulmaydi;

• yuklanish sektoridagi ma’lumotlarning buzilishi. Yuklanish sektora diskdagi maxsus dastur bulib, uning buzilishi disk ishini tuxtatib kuyadi;

• diskni kayta formatlash — diskdagi barcha axborot butunlay yukoladi;

• diskka biror xabar chikarishi yoki biror kuyni ijro etishi mumkin. Kup xollarda bu xabar tushunarsiz bo’ladi;

• kompyuterning o’z-o’zidan karta yuklanishi;

• tugmachalar majmui ishini tuxtatib kuyishi;

• dasturli va ma’lumotli fayllar mazmunining uzgarishi. Virus ma’lumotlarni ixtiyoriy ravishda aralashtirib kuyadi va xokazo.

Oddiy virusdan zararlanishni virusga karshi dasturlar yordamida oson aniklash mumkin. Polimorf (murakkab tuzilishga ega) viruslarni bu usul bilan aniklash kiyin, chunki ular uz-uzini nusxalashda kurinishini uzgartiradi.

Makroslar bilan ishlaydigan ilovalar makroviruslar bilan zararlanishi mumkin. Makroviruslar — fayllarga ma’lumotlar bilan birga urnatiladigan buyruklardir. Bunday ilovalarga misol kilib Word, Excel va Postscri pter interpretatorlarini kursa tish mumkin. Ular ma’lumotlar faylini ochayotganda makrovirus bilan zararlanadi.

Ilgari faqat disklar virus bilan zararlanar edi. Chunki viruslar disklar orkali kompyuterdan kompyuterga ugar edi. Yangi BBS viruslari esa modem orkali tarkaladigan buldi. Internetning paydo bulishi viruslarga karshi kurashning an’anaviy usullari foyda bermaydigan yana bitta kanalning xosil bulishiga olib kelli.

Viruslar bilan zararlanish extimoli kompyuterda yangi fayllar va ilovalarning paydo bulish chastotasiga mos ravishda ortadi, Kompyuterdagi ma’lumotlarning axamiyati kanchalik zarur bulsa, virusga karshi xavfsizlik choralari shunchalik yukori bulishi kerak. Bu narsalarga befark bulish nafakat katta moddiy zarar kurish, balki tashkilot yoki firmaning bundan keyingi faoliyati masalasini xam o’rtaga kuyishi mumkin.

Shuni esdan chikarmaslik kerakki, viruslar, odatda, foydalanuvchining biror amali (masalan, ilovalarni urnatish, tarmokdan fayllarni ukish, elektron alokani ukish va x.k.) natijasida paydo buladi. Shuning uchun ma’lumotlar kirish joyiga maxsus filtrlar, zararlangan fayl va dasturlarni yuklashni cheklovchi maxsus dasturlar urnatilishi zarur. Bunday kurilmalardan biri Symantic korporasiyasi maxsulidir (Toshkentda Nuron DC kompaniyasi uning partnyori xisoblanadi). Symantic bitta mashina o’rniga butun korporativ tarmokni kompleks ximoyalash goyasini ilgari suradi. Virusning korparativ tarmokka kirish nuktasi istalgan nuqtada — brauzerdan to ishchi stansiyagacha bulishi mumkin. Shuning uchun nazorat barcha boskichlarda amalga oshiriladi. Virusga karshi Symantic dasturiy ta’minoti Dynamic Document Revie n korporasiyasi texnologiyasida bajarilgan va Ye-mail viruslariga xam karshi kurash olib boradi.

Virusga karshi dasturli ta’minot ishining aloxida xususiyati shundaki, virusga karshi dasturlar omborini uz vaktida yangilab turish kerak.