Алматы Сән және Дизайн Колледжі

Реферат

Тақырыбы: Антивирус

Орындаған: СП 16-1 студенті Нұсқақбай Аружан

Тексерген: Керимбекова Айнұр Мухаметовна

**Антивирус** (латын тілінен анти – қарсы немесе кері, ал вирус - [у](https://kk.wikipedia.org/wiki/%D0%A3) деп аударылады) -- Антивирус аты айтып тұрғандай компьютерге енген қауіпті нұсқауларды яғни вирустардан, қауіпті тудырғыш программалардан қорғап, операциялық жүйе мен файлдардың ластануынан және кедергісі көп кодтардан қорғайды. Ол вирустардың таралуы мен көбеюін болдырмауға арналған программа. Оның жұмыс істеу (сканирование) принципы: Компьютерді(C;D) толық сканированиедан өткізіп, вирустарды табу. Компьютердегі(C;D) өзіне сәйкес қимыл орындамайтын немесе вирустанған файл-программаларды табу, олардың қауіптілік дәрежесін анықтау.

Табылған вирустарды антивирус программа базасына жеткізіледі. Ол вирустық қасиетке ие болып зияны болса , база сигнатурасында тіркелсе келесі бұйрықтарды орындауға мүмкіншілік болады: 1.Вирустанған (инфицированный) файлды жою. 2.Вирустанған файлдың басқа барлық файлға байланысын жою. 3.Карантинға енгізу(Антивирустың критериясы бойынша вирустың таралуы қауіпінен оны қолдануға мүмкіншілк бермейді). 4.Файлды тазарту, яғни енген вирусты жою. 5.Ешқай бұйрық орындалмайтын жағдайда оны операциялық жүйенің келесі перезагрузкасында ғана вирусты толығымен жоюға болады.

Антивирустардың көп түрі әсіресе жүйесінде сигнатуры бар бағдарламалар вирустарды операциялық жүйенің файлдарға бұйыруы кезінде іздейді. Бұл әдіс өте тиімді. Компьютердің жүйелік администрациясы оның тексерілетін күнделікті, тұрақты расписаниясын енгізеді. Антивирустық бағдарламалардың көбісі сигнатурлық жүйе арқылы орындалады. Олар әдетте компьютердің файл-құжаттарының зақымдануына кедергі келтіреді. Вирустардың авторлары мұндай программалармен кездеспеулерін қалайды. Олар сондықтан олигоморфикалық , полиморфикалық және метаморфты вирустарды құрайды. Олардың қолдану себебі вирустардың сигнатурдағы жазылған мәліметпен (запись) сәйкес келуі.

Антивирустық бағдарлама өз антивирустық көзқарасы бойынша вирусты тапқан бетте оны жоюды қарастырмай енген файлдың іс-әрекетін бақылап потенцияалды зиянды қолданушыға хабарлап немесе оның қимылын тоқтатады(блокировка) Антивирус - сүзгiлер - бұл бағдарлама қандай болмасын барлық талпыныстар туралы қолданушы дисктерге жазылуға дабылдайтын резидент программасы ол әсiресе формат жасау, сонымен бiрге басқа күдiктi әсерлер туралы. Сонымен бiрге шешу немесе осы әсердi тыйым туралы сұрау салу iске аспай қалады. Бұл бағдарламалардың жұмыс принципі үзулердiң тиiстi векторларының ұстап қалуында негiзделген. Тексерушiлер(Ревизор) - бұл файлдар және дисктiң жүйелiк облыстарының ағымдағы күйлерiн талдайтын және оның осы тексерушiлердiң файлдардың бiрлерiнде бұрын сақталған мәлiметпен салыстыратын бағдарлама. Доктор ВЕб Басқа вирусқа қарсы бағдарлама - диалог фирманы ұсынатын Doctor Webның мәлiмдiлiгi соңғы кезде шапшаң өседi. Ұсынған [компания](https://kk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F) “Диалог-Наука” деп аталады. Бұл бағдарлама И.А.Данилов, 1994 жылында жасалды. Dr.Web тура Aidstestтер сияқтылар детекторлардың классына жатады - дәрiгерлер, бiрақ айырмашылыққа соңғы "Эвристикалық анализатор" деп аталатын алады - белгiсiз вирустер ашуға мүмкiндiк беретiн алгоритм. "Емдiк өрмекшiнiң торы", бағдарламаның ағылшын атауынан жiберiлетiн басып кiруiне байттың бiр де бiр тән тiркесiн болып қалмағандайдың өз денесi көбейтуде түрлендiретiн вирус өзiнен модификацияланатын отандық бағдарламашылары жауап болды.

Дәл осылай сонымен қатар Aidstestпен жағдайда оған вирусты бiлдiрген файлдар өйткенi үлгiге вирусқа қарсы программада сау бағдарламада кездесе алуға қабылданған байт тiзбек шығаруға болмайды бағдарламаға бастапқы тестеуiнде емдеуге рұқсат беруге болмайды. Aidstestтерге қарағанда, Dr.Web: бағдарлама полиморфизм вирустарын шырамытады;

эвристикалық анализатормен жабдықтаған;

және архивтардағы файлдарды емдеуге тексеруге икемi болады;

CPAV вакциналанған файлдарды тестеуге мүмкiндiк бередi LZEXE, PKLITE, DIET қапталған. Диалог фирма DOS үшiн DrWebның әртүрлi бағдарламаның нұсқаларын ұсынады. Белгiлi жай, дәстүр бойынша 16-дәрежелiк және 32 деп аталған DOS үшiн екi болжам дәрежелiк болады 16-дәрежелiк болжам, басқару жүйе үстiне қойылатын түсiнiктi жадтардың көлемi бойынша шектеулерге байланысты "Бiлу" кейбiр аса маңызды бүгiнгi күнге ие болмайды, онда жеке алғанда (және жад бойынша арқасында көрcетiлген шектеулер, қосыла алмайды) қосылмаған.