КОМПЬЮТЕРЛІК ВИРУСТАР. АРХИВАТОРЛАР

КОМПЬЮТЕРЛІК ВИРУСТАРДЫҢ АНЫҚТАМАСЫ.

- Компьютерлік вирус – арнайы жазылған шағын көлемді (200-5000 байт) программа.Ол өздігінен басқа программалар соңына немесе алдына қосымша жазылады да, оларды “бүлдіруге” кіріседі, сондай-ақ компьютерде тағы басқа келеңсіз әрекеттерді істеуі мүмкін.Ішінен осындай вирус табылған программа “ауру жұққан” немесе “бүлінген” деп аталады.Қазіргі кезде 50 мыңнан астам вирус белгілі.

Компьютерлік вирус ұғымы

Компьютерге вирус жұққанының белгілері мынадай:

- Кейбір бағдарламалар істемей қалады немесе қате істейді;
- Кейбір орындалатын файлдардың көлемі өзгереді. Бірінші кезекте командалық файлдар;
- Процессордың көлемі вирус көлеміне ұлғаяды;
- Экранға бөтен таңба, жазулар, дыбыс, видео шығып кетеді;
- Компьютердің жұмысы баяулайды және бос жедел жады азаяды;
- Кейбір файлдар мен дискілер істен шығады;
- Компьютер қатты дискіден жүктелмей қалады.

Компьютерлік вирустардың түрлері

Санаттары

- Компьютерлік вирустар
- Желілік құрттар
- Трояндық программалар («троян аттары»)
- Зомби
- Тыңшы программалар
- Мобилді вирустар
- Пайдалы вирустар
- Зиянкес программалар
- Хакерлік шабуылдар

Тіршілік ортасына қарай

- Файлдық вирустар
- Жүктелу вирустары
- Макро-вирустар
- Желілік вирустар

Мекендеу ортасына қарай

Файлдық

Жүктейтін

Макровирустар

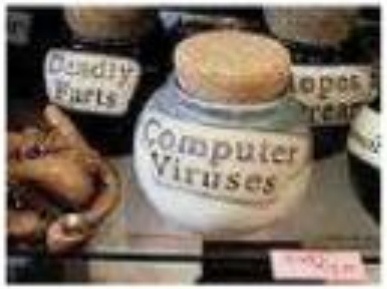
Бұл қолданбалы программалардың ішіне енгізілген программалық кодалық блоктар. Вирустық кода программа жүктелгенде жіберіледі.

Негізгі жүктейтін жазбаға немесе жүктейтін секторға вирус жұқтырады. Операциялық жүйе жүктелгенде жұқпалы тасушыдан вирус жұғады.

Word құжаттары және Excel электрондық кестесі құжаттарына вирус жұқтырады. Жұғу құжат файлын ашқанда орындалады.

Компьютерлік вирус ұғымы

***Компьютерлік вирус** – бұл арнайы жазылған кішкене бағдарлама, ол басқа бағдарламалар мен файлдарға өзін қоса алады, яғни жұғады, сондай-ақ компьютерге түрлі зиян келтіреді.*



«Вирус» аты биологиядағы сияқты өзінен-өзі көбею қабілетіне сай алынған.

***Компьютерлік вирустар** тірі вирустарға өте ұқсас қасиеттерге ие:*

- ***жасырындығы;***
- ***көбею қабілеті;***
- ***ортаға бейімделгіштігі;***
- ***қозғала алуы;***
- ***басқа нысандарға өздігінен кіріге алуы, т.с.с.***

ЖҰМЫС ЛОГИКАСЫНА ЖӘНЕ МАҚСАТЫНА ҚАРАЙ

ҰСТАУЫШ - ВИРУСТАР

ЛОГИКАЛЫҚ БОМБАЛАР

ҚҰРТТАР

ТРОЯН АТТАРЫ

- **Полифагтар.**Олардың қызметі-вирустарды табу ғана емес, оның кодасын жұқпалы (ауру жұққан) программадан жою.Өте қуатты полиграф-сканер И.Данилов құрған **Dr. Web** (Doctor Web) болып табылады.Ол вирустарды жақсы айырып таниды, бірақ оның базасында вирусқа қарсы күресетін құралдар басқа вирусқа қарсы программаларға қарағанда анағұрлым аз. Жалпыға әйгілі полифаг Е.Касперский зертханасы құрған **Kaspersky Anti-Virus** программасы вирусқа қарсы бірден-бір сенімді программа ретінде бүкіл әлемге әйгілі.
- Компьютер әлемін вирустардың жаулап алмауы үшін мынандай тапсырмаларды орындау керек.

Полифагтар

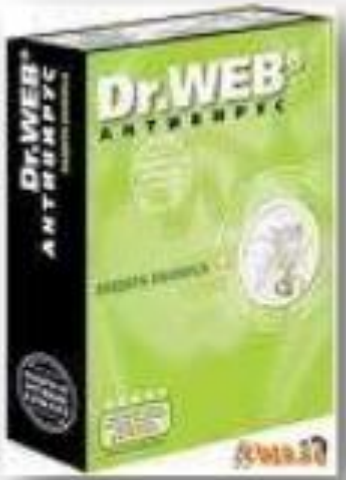
Жедел жадын, диск секторларын, файлдарды тексеріп, олардан белгілі де, жаңа да вирустарды табатын антивирустық программалар. Полифагтар файлдарды жедел жадына жүктелу барысында тексеруді қамтамасыз ете алады. Мұндай программаларды антивирустық мониторлар деп атайды.

Полифагтардың артықшылығы: әмбебаптығы.

Кемшілігі: вирустарды іздеу жылдамдығының төмендігі.

Мысалдар:

Kaspersky Antivirus, Dr.WEB.



- **Детектор-**
- **Программалар-** тек бұрыннан белгілі вирус түрлерінен ғана қорғай алады, жаңа вирусқа олар дәрменсіз болып келеді,
- **Доктор-**
- **Программалар-**
- немесе “**фагтар**” вирус жұққан программалармен дискілерді “вирус” әсерін алып тастау,яғни “жұлып алу” арқылы емдеп – оларды бастапқы қалпына келтіреді

- **Ревизор-**
- **Программалар-** да алдымен программалар мен дискінің жүйелік аймағы туралы мәліметтерді есіне сақтап, содан соң оны кейінгісімен салыстыра отырып сәйкессіздікті анықтаса, оны дереу программа иесіне хабарлайды.
- **Доктор-**
- **Ревизорлар-** доктор-программа мен ревизорлар арасынан шыққан гибрид. Бұлар тек файлдағы өзгерістерді, анықтап қана қоймай, оларды автоматты түрде “емдеп” бастапқы қалыпты жағдайға түзеп келтіреді
- **Сүзгі-**
- **Программалар-** компьютердің оперативтік(жедел) жадында тұрақты (резиденттік) орналасады да, вирустардың зиянда әрекетіне әкелетін операцияны ұстап алып, бұл туралы жұмыс істеп отырған адамға дер кезінде хабарлап отырады.Одан әрі шешім қабылдау әркімнің өзіне байланысты болады.

Желілік вирустар

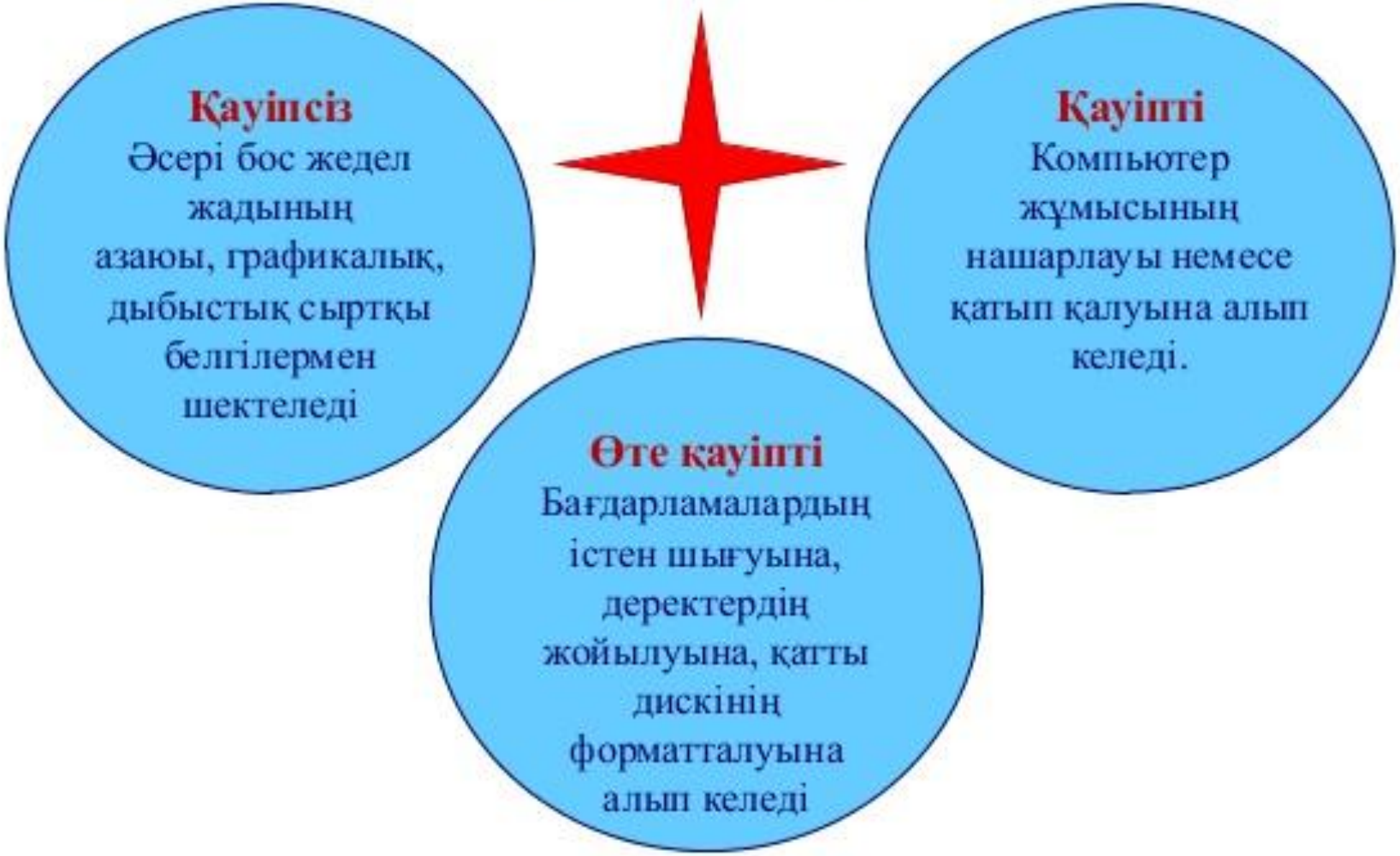
Компьютерлік желі арқылы таралады және файлдық сервер-мұрағаттардан файлдарды алған кезде жұғады. Желілік вирустардың электрондық пошта және интернет арқылы таралатын түрлері бар.

Желілік вирустардың түрлері өте көп.

«Пошталық» вирустар	*Интернет - құрттар*	*Скрипт - вирустар*
Пошта хабарламаларына салынған файлдарда болады. Сол файлдарды ашқан кезде компьютерге жұғады.	Пошта хабарламаларына салынған файлдар арқылы компьютерлік желіде таралады.	Жеке компьютерге интернеттен сайт беттерін браузер арқылы жүктеген кезде жұғатын зиянкес программалар

Компьютерлік вирус ұғымы

Келтіретін зиянына қарай вирустар 3 топқа бөлінеді.



Бейсауат

Шантаж жасаушы

Мақсатына қарай

Насихатшы

Мағынасыз

КОМПЬЮТЕРЛІК ВИРУСТРАДЫҢ ЖІКТЕЛУІ

- Компьютерлік вирустардың бірнеше онмыңдаған түрлері белгілі.Компьютерлік вирустарды жіктеуге болатын бірнеше қағидалар бар:
- операциялық жүйелердің таралуы бойынша;
- зақымдалған нысандар бойынша;
- қолданылатын технологиялар бойынша;
- жасау құралы бойынша;
- зақымдалу амалдары бойынша.

- **Макровирустар**
- Макровирустар құжаттарды зақымдайды.Құжаттар мәтіннен өзге кірістірілген нысандардан, форматтау сипаттамасынан, макростаттардан құралады.
- **Полиморфты вирустар**
- Олар өз беттерінше кодтарын өзгертуге алады.Олар өз денелерінде шифрланған бөлік пен шифрден тұрады, әрі шифрді ашушы автоматтты түрде генерацияланатын әр данасында әртүлі.
- **Құрт секілді вирустар**
- Құрт вирустар олар қолданушының қатысунсыз программалық қамтамасыз етудегі қателер мен кемшіліктердіпайдалана отырып таралатын вирустар.
- **Трояндық вирустар**
- Басқа программалардың ішінде тығылып тұрады және көбінесе компьютерге жүктелетін программалар. Олар мәліметті жою, өзгерту мен көшіруге, бұғаттауға әкеліп соқтырады.

АРХИВАТОРЛАР

- Архиваторлар, бұл файлдың олшемін кішірейту арқылы, дисктегі орынды үнемдеуге мумкіндік беретін программалар болып табылады. Архивтеу программасы өте көп. Мысалға: PKZIP, ARJ,RAR, Windows ортасы үшін- WinZIP,WinRAR. Бұлардың барлығы жеткілікті тез және жақсы жұмыс жасайды. Олардың әрқайсысын да қолдануға болады. Бізге информатика оқулыгын жазу барысында жасалған файлдарды архивтеу (буып-таңу) керек болсын. Бұл файлдар информатика бумасында жинақталған. Егер Сізде WinRAR архиваторы бар болса, онда Сіз тышқан курсорын сол бумаға көрсетесіз де оң жақ пернесін басасыз. Жауап ретінде нұсқаулары бар терезе шығады. «Добавить в архив “Информатика”» нұсқауын таңдайсыз. Егер тышқанды сырт еткізсеңіз, архивтеу үрдісі жүктеледі, ақпарат терезесі дәлелдеме болады

- Архивті ашу үшін де архиватор программасы қолданылады. Біз бұл жағдай да архивтеуде тышқанмен орындалған амалдарды орындаймыз. Сонда нұсқауларымен пайда болған терезеде бізге тиімді пунктті тандаймыз. Әрі қарай программа архиватор файлдарды біртіндеп алып, көрсетілген бумаға жаза береді. Буылған файлды жаңартуда, ягни файддың кене үлгілерін жойып жаңа файлды қосу «Ашу» нұсқауының көмегімен орындалады. Барлық терезелер сияқты бұл терезе де тақырыбынан, менюлер жолынан, құрал-саймандар жолынан және т.б. тұрады, жасалатын қимылыңызға байланысты меню пунктін немесе құралды таңдайсыз.
- IBM-сыңайлас компьютерлермен жұмыс жасағанда қолдану ыңғайлылығы түсінігі көңілді аудартады.
- Ең бастысы жеке белек қосымшамен біртіндеп гәжірибе жинақтай отырып, әрқайсысының ыңғайы мен араласу принциптері бірдей
- екенін ұмытпау.

КОМПЬЮТЕРЛІК ВИРУСТАР ЖӘНЕ ОЛАРДАН ҚОРҒАНУ

- Көпшілікті ақпараттандыру урдісінің оң салдарларымен бірге теріс жақтары да бар. Мысалға, компьютерлердің глобальдық желіге бірігуі, бір жағынан көп мөлшердегі адамдардың ақпараттар әлемінде жинақталған үлкен массивке араласуына әкелсе, екінші жағьшан желіге орналастырылып сақталған интеллектуалдық меншікті қорғауға қиындық тудырды.
- Компьютерлік вирустер әсерінің нәтижесінде ДК тұтынушылары өте жиі ақпараттарын жоғаттады. Компьютерлік вирустер, тұтынушыға және қызмет атқарушы ДК мерсоналына көптеген қиындықтар туғызатын, ерекше типті зиян тасушы программалар болып табылады.

- *Компьютерлік вирус* деп өздігінен пайда болу, көбею және басқа программаларға белсенді ену қасиетіне ие программаны айтады. Компьютерлік және биологиялық вирустер ұқсастығы анық. Вирустар әруақытта кесел келтіреді – ДК-ің қалыпты жұмысына кедергі болады, файлдық құрылымды бұзады және т.б., сондықтан олар зиян тасушы программалар қатарына жатады. *Компъютерлік вирустердің өмірлік циклі* міндетті түрде келесі фазалардан тұрады:
- 1) латенттік период, вирустың ешқандай қимыл жасамайтын уақыты;
- 2) өсу периоды, вирустың тек қана көбею уақыты;
- 3) белсенді период, көбеюмен бірге вирус алгоритміне салынган рұхсатсыз қимылдар жасалатын уақыт.
- Алғашқы екі фаза вирус көзін, оның өту каналын жасырып және барынша көп файлды бүлдіруші, вирус білінгенше жаралау қызметін агқарады.

ВИРУСТАРДАН ҚОРҒАЙТЫН ПРОГРАММАЛАР МЫНАЛАРҒА БӨЛІНЕДІ: ДЕТ ПРОГРАММАСЫ ВИРУСТАРДЫ ТАБАДЫ; ИММУНАЗАТОР.

- Программасы вирустар оны бүлдірдік деп санайтындай етіп программаны өзгертеді. Көптеген вирустар екінші мәрте файлды бүлдіре алмайды, өйткені иммуниттеу вирустардың мұндай «бір жолғы» әрекетінен қорғауға мүмкіндік береді; фаги-программасы вирустарды тауып қана қоймай, олардың көзін құртады, яғни оларды жояды. Егер программа әр түрлі вирустарды құрта алатын болса, онда оны әдетте полифаг деп атайды. Кейде вирустарды жойғаннан кейін бүлінген файлды бұрынғы (бастапқы) қалпына келтіруге болады. Ал, бастапқы қалпына келмеген файлды емделмейтін, яғни жөнделмейтін файл деп атайды. Мұндай жағдайда емделмейтін файлды жойып, жоқ қылу керек. Сонымен қатар, мұндай жағдайда дискетке жазып алудан қорғалатындай етіп орналастырылған программаның тазарезервтік көшірмесі қажет болады; сүзгі-программасы (программа фильтры), (күзетші – қарауыл, монитор) компьютер қосылғаннан кейін ұдайы жұмыс жағдайында болады және қалыпты жұмыс істеп тұрған компьютерде сәл ауытқу пайда болса қатер төнгенін білдіріп, бірден дабыл қағады (белгі береді). Бұл компьютерге, яғни программаға еніп кеткен вирусты ерте тауып, сол кірген сәттегі алғашқы кезеңінде-ақ оның бүлдірушілік әрекеттерін асқындырмай, алдын алып, негұрлым залалсыздандыруға ұмтылады.

КОМПЬЮТЕРЛІК ВИРУСТАРДЫ ТАУЫП, ЖОЮ ҮШІН DOCTORWEB ПРОГРАММА ДЕСТЕСІН ҚОЛДАНУ ТӘРТІБІ.

- 1. Негізгі мәзірдің немесе жұмыс орнының тиісті таңбашасының басу немесе Программа – DoctorWeb – DoctorWeb командасымен DoctorWeb программасын іске қосу.
- 2. Баптау – Орнатуды өзгерту командасының, Орнату таңбашасын немесе F9 функциялық пернесінің оперативті түрде жадында сақтауын тестілегеннен кейін параметрлер терезесін шақырып, қарау керек әрі қажет болған жағдайда вирустарды іздестіруді орындайтын режимді қалпына келтіру;
- 3. Программаның негізгі терезесінде тексерілуі тиіс дискіні көрсету.
- 4. Тексеруді бастау/аяқтау командасын орындау үшін Файл -Тексеруді бастау немесе Ctrl+F5 перңесін бірге басумен тексеру процесін іске қосу.
- 5. Файл – Шығу командасымен, Шығу таңбашасымен немесе Alt+ X пернесін үштастырумен дестенің жұмысын аяқтау.