

Компьютерлік вирустар



Мазмұны

- Компьютерлік вирус ұғымы
- Вирустардың пайда болу тарихы
- Компьютерлік вирустардың түрлері
- Компьютерлік вирустардан қорғану әдістері
- Антивирустік бағдарламалар

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.*

❖ басқа нысандарға өздігінен кіріге алуы, т.с.с.

❖ қозғала алуы

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 вирус ұғымы

Келтіретін зиянына қарай вирустар 3 топқа бөлінеді.

Қауіпсіз

Әсері бос жедел жадының азаюы, графикалық, дыбыстық сыртқы белгілермен шектеледі



Қауіпті

Компьютер жұмысының нашарлауы немесе қатып қалуына алып келеді.

Өте қауіпті

Бағдарламалардың істен шығуына, деректердің жойылуына, қатты дискінің форматталуына алып келеді

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

Компьютерлік вирус түрлері

Желілік құрттар

Құрт (Worm) – қатты дискте, компьютер жсадында көбейетін және желі арқылы таралатын вирус. Құрттардың басқа вирустардан ерекшелігі сол, олар арнайы зақымдаумен шұғылданбайды, тек өзін-өзі көбейтеді, сөйтіп жадты толтырып тастайды да, компьютер жұмысын құрт тежейді. Алдымен желі арқылы вирустың «басы» келеді де, кейін «денесін» сол желіден «тартып» алады. Сондықтан бұл вирусты «желілік құрт» деп атаған.



ТРОЯНДЫҚ ПРОГРАММАЛАР



Троян немесе троян аты (Trojans) – кез-келген қолданбалы программаның ішіне жасырын салып жіберетін зиянкес программа, қолданбалыны орнатқанда ол да компьютерге жасырын орнығып алып, өзінің мынадай зымиян мақсаттарын іске асыра бастайды – компьютерге нақты зиян келтіру: құпия мәліметтерді ұрлау, бұзу немесе жою, компьютерді істен шығару немесе оны басқа зиянкестік мақсаттарда пайдалану.

Міне, сондықтан да, трояндық программалар ең қауіпті зиянкес программаларға жатады, өйткені оларға небір құйтырқы да зымиян әрекеттер жасау мүмкіндіктері беріледі.

Тыңшы (шпиондық) программалар

Тыңшы-программа (Spyware) – компьютерге рұқсатсыз, жасырын келіп орналасып алатын программа, оның бірден-бір мақсаты компьютерді толық өз басшылығына қаратып, үздіксіз аңдып, жеке құпия ақпараттарды ұрлау немесе жою.

Бұл программалар компьютерге көбіне желілік құрттар, трояндар немесе жарнамалық программалар (adware) арқылы кіріп алады.



Мобилді вирустар

Мобилді вирустар – Бұл ұялы телефондарға жұғатын вирустар. Олар **SMS** және **MMS** хабарламалар мен **Bluetooth** каналдары арқылы таралады.

Бұл вирустардың да мақсаты ұялы телефон иесінің жеке құпия мәліметтерін ұрлау және пайдалану, бөтен телефондарға халықаралық және ақылы қоңыраулар соққызу немесе **SMS**, **MMS**-тер жөнелтіру арқылы пайда түсіру.

Бұл вирустардың ең көп таралғандары: **Cabir**, **Comwar**, **Brador**, **Viver** және т.б.

Файлдық вирустар

Файлдық вирустар әр түрлі жолдармен командалық файлдарға кіріп алады, олар орындалатын *.exe, *.com кеңейтілімдегі файлдар және осы файлдар іске қосылған кезде бірге белсенді күйге көшеді. Өзі зақымдаған файл орындала бастағаннан вирус та онымен бірге компьютердің жедел жадына орналасып, сол жерден өзінің зиянкестік әрекеттерін іске асырады. Мысалы, басқа да файлдарға жұға береді. Ол тек компьютер өшкенде немесе операциялық жүйе қайта жүктелгенде ғана өзінен-өзі жойылып кетеді. Бірақ файлдық вирустар берілгендер файлын зақымдай алмайды.



Жүктемелі вирустар

Жүктемелі вирустар өзін өзі қатты дисктің жүктеу секторына (нөлдік секторға) жазып қоя алады. Операциялық жүйені компьютердің қатты дискінен жедел жадына жүктегенде бұл вирустар да сол жерге орналасып алады. Одан әрі жүктемелі вирустар да файлдық вирустар сияқты әрекет ете бастайды. Командалық файлдарға жұғып, олармен бірге қосылып, зиянкестік әрекеттерін жүзеге асырады, одан әрі қарай жұғады.

Вирус қатты дискінің жүктеу секторын зақымдайды және сол жерден дискет, флеш-карта арқылы бір компьютерден басқа компьютерге жұғуы мүмкін.



Макро вирустар

Макро-вирустар Word құжаттары мен Excel электрондық кестелерін зақымдайды. Макро-вирустар деген сол офистік программаларда қолданылатын макрокомандалар арқылы жазылатын программалар (макростар). Зақымданған құжат өзі жасалған қолданбалы программада ашылған кезде макро- вирус компьютер жадына орналасып алады да, басқа да құжаттарға жұға береді. Жұғу қаупі тек қолданбалы программа жабылғанда тоқтайды.



Желілік вирустар

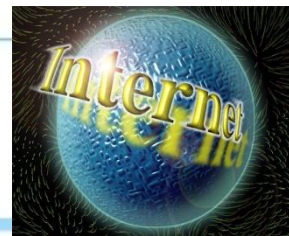
Компьютерлік желі арқылы таралады және файлдық сервер-мұрағаттардан файлдарды алған кезде жұғады. Желілік вирустардың электрондық пошта және интернет арқылы таралатын түрлері бар.

Желілік вирустардың түрлері өте көп.

<i>«Пошталық» вирустар</i>	<i>Интернет - құрттар</i>	<i>Скрипт - вирустар</i>
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



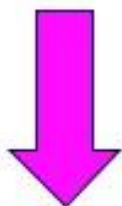
© 2004 Microsoft



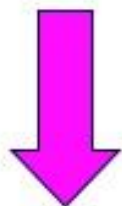
Компьютерлік вирустардан қорғану әдістері

1. Резервтік көшірме жасау – компьютердегі барлық программалардың, файлдардың көшірмелерін қосымша CD, DVD жүйелік және апаттық дискілерге жазып, сақтап қою. Вирустар жүйені істен шығарса, осы дискілерден оны қайта тіктеп алу мүмкіндігі болады.
2. Компьютерге қолжетімділікті шектеу – әкімшілік құқық, құпия сөздер, жабық дискілер әдістерін пайдалану арқылы.
3. Антивирустық қорғанысты қосу – компьютердің BIOS-ындағы Setup программасы арқылы жүктелу вирустарынан қорғануға болады.
4. Тек лицензиялы программаларды пайдалану – олар вирустардан таза болады, ал пираттық көшірмелерде вирустар еркін жүреді.
5. Компьютерге сырттан келетін ақпараттың бәрін тексеріп отыру – желіден, CD, DVD, флеш дискілерден алынатын файлдарды вирустарға тексеру әдетке айналу керек.
6. Антивирустық программаларды үздіксіз пайдаланып, оларды тұрақты жаңалап отыру керек.
7. Дискіні жөндеу программалық құрал-саймандар топтамасын дайын ұстау (антивирустар және дискіні жөндеп, баптау дискілері).

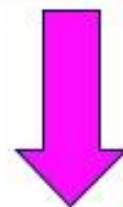
Антивирустық программалар



Полифагтар



Ревизорлар



Тосқауылшылар

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.

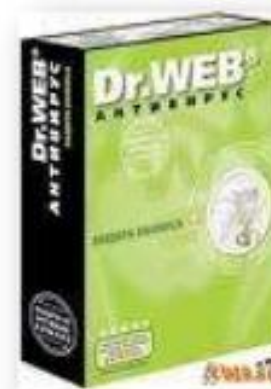


Полифагтардың артықшылығы:
әмбебаптығы.

Кемшілігі: вирустарды іздеу
жылдамдығының төмендігі.

Мысалдар:

Kaspersky Antivirus, Dr.WEB.



Ревизорлар

Бұл антивирустардың деректер қорында барлық файлдардың бастапқы ақпараттық есебі сақтаулы тұрады. Файлдарды үздіксіз тексеру барысында бар ақпарат деректер қорымен салыстырылып отырады. Егер олар бір-біріне сәйкес келмесе ревизор кейбір файлдардың өзгертілгені немесе вирус жұққаны туралы хабарлама жасайды.

Кемшілігі: ревизор жаңа файлдардағы вирустарды ұстай алмайды (флешкадағы, файлдарды мұрағаттан ашқанда, электрондық поштада), өйткені жаңа файлдар туралы мәліметтер антивирустың деректер қорында әлі жоқ болады.

Мысал: **ADinf**



Тосқауылшылар (блокировщики)

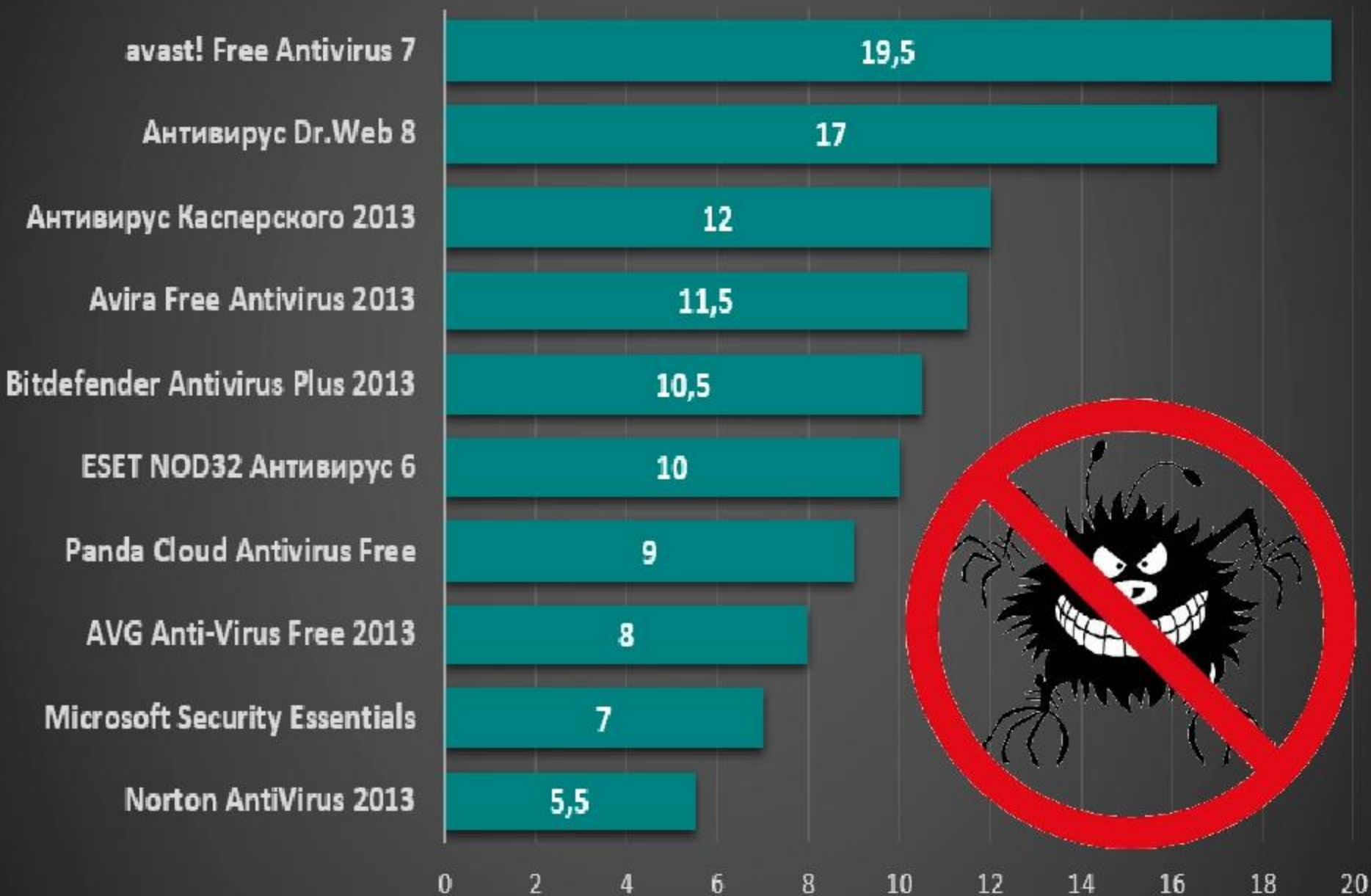
Бұл «**вирустік қауіпті**» (мысалы, дискінің жүктеу секторына жазылуды) алдын-ала ұстап алып, хабарлайтын антивирустік программа.

Ең көп тарағаны компьютердің BIOS-ғы антивирустық тосқауылшылары. BIOS Setup программасы арқылы қатты дискінің жүктеу секторына жазуды тоқтатып қоюға болады, сонда компьютер жүктелу вирустарынан толық қорғаныста істейді.

Артықшылығы: вирусты көбеюдің ең алғашқы сағатында, яғни барынша ертерек ұстап алып, оған тосқауыл қоя біледі.



Общий рейтинг антивирусов





**Назарларыңызға
рахмет!!!**

