КОМПЮТЪРНИ ВИРУСИ И АНТИВИРУСНИ ПРОГРАМИ

1. Същност на компютърните вируси?

В софтуерната индустрия са известни над 50000 вируса. Терминът "вирус" идва от латински и означава "отровен сок". В биологията така се означават микроорганизми, прилепващи се към клетки-стопани и използващи ги за своето размножаване. След определено време вирусът се активира и болестта избухва. По подобен начин действат и компютърните вируси.

Компютърният вирус е кратка паразитна програма, която следва предварително зададени логически инструкции за действие и самосъхранение, причинява сериозни разстройства в работата на компютъра и води до повреди и загуба на важна информация в него. Тези инструкции представляват поредица от команди, написани на асемблер, на език от високо ниво, на команден език или от смесена форма на тези езици.

Характерна черта на вирусите е способността им за самовъзпроизвеждане. Копието, което те могат да направят сами, е точно възпроизвеждане на първоначалната поредица от инструкции, заложена във вируса при създаването му. Съществуват и вируси, които притежават способността да мутират в процеса на възпроизвеждане и по този начин да се различават от оригинала.

2. Кратки исторически сведения.

Официално се счита, че създателят на първия компютърен вирус е проф. Фредерик Коен – специалист по защита на компютърната информация – през 1983г. Той демонстрирал "произведението" си на семинар по компютърна сигурност през 1984г. Целта е била да се покаже уязвимостта на компютърната информация и да се провокира разработването на средства за защита. Неофициално се предполага, че професорът е проявил интерес към темата, след като се е сблъскал с "произведението" на неизвестен злосторник.

През 1986г. се появява Brain – първият вирус за PC, който заразява сектора за начално зареждане на 360K дискети, а през 1987г. е регистрирана първата вълна от вируси, един от които е познатия и днес Jerusalem. Нашествието на нови вируси в края на 80-те и началото на 90-те години водят до създаването на EICAR – Европейски институт за компютърни антивирусни проучвания. През 1992г. е създаден вирусът Michelangelo, който заразява boot-сектора на твърдия диск и се активира на 6 май – рождения ден на Michelangelo.

След като биват създадени голямо количество вируси, през 90-те години възниква необходимостта от регистриране и класифициране на известните до този момент вируси. През 1993г. е публикуван първият списък "WildList" с всички потвърдени вируси. През 1995г. започва нашествието на макровирусите, а през 1999г. – на Интернет вирусите, някои от тях създадени с новите технологии на Java и JavaScript. През същата година е разпространен и един от най-разрушителните злонамерени кодове, който може да форматира твърди дискове – вируса CIH, т. е. Чернобил (активира са на 26 май), както и първият мрежови вирус – Funlove, активен и до днес. През 2001г. най-големи щети нанасят вирусите Code Red (първият, който се разпространява посредством HTTP), Nimba (един от първите червеи със собствена SMTP машина, който се разпространява при наличие на активна връзка с Интернет) и Klez (най-упоритият вирус в историята на компютрите). През 2002г. се появява Bugbear – комплексен вирус, който се разпространява посредством споделени мрежови устройства и спира активните антивирусни програми. Най-оригиналният вирус за 2003г. като програмна техника е SQLSlammer, който причини големи щети в много компании и порази множество сървъри в целия свят като се възползва от уязвимостта в Microsoft SQL Server. Blaster е масов вирус, причинил големи щети за кратко време. През 2003г. масово разпространен беше и червеят с много модификации – RORO (по недоказани твърдения някои негови варианти са с български произход, а може би и оригиналният). През 2005 г. бяха регистрирани четири мащабни вирусни епидемии. Това бяха модификацията на пощенския червей Bagle, мрежовият вирус-червей Mytob.c и двете модификации на пощенския червей Sober – Sober.p и Sober.y. Storm Worm е червей, който се разпространява доста през 2006-2007 г. Хората започват да наричат вируса Storm Worm, защото едно от имейл съобщенията, носещи вируса има заглавието „230 жертви след буря в Европа.

Вече съществуват и вируси за WAP (Wireless Application Protocol). За сега е само един – Timofonica, но това е само началото. Очаква се да се появят и нови вируси. Те могат да правят всякакви номера като раздуване на сметката, разпращане на телефони и какво ли не още, което е свързано с мобилните телефони и лаптопи, ползващи този протокол.

Вече има и защитно приложение от F-Secure Corporation, действащо едновременно като защитна стена и антивирусна програма за WAP с цел да се предпазят потребителите. За сега проблемът е само в Испания, но това е достатъчно, за да се вземат защитни мерки от рано.

3. Начини за разпространение на вирусите:

- При копиране на заразени файлове от дисков носител – диск, дискета (в някои случаи от игри, драйвери, операционни среди, среди за програмиране, транслиращи програми, архивирани пакети...). Затова не трябва да се копира от съмнителни дискети и нелицензирани CD. Преди употреба софтуерът трябва да се проверявя за вируси.

- Чрез електронна поща. Много често, освен текст, към писмата има прикрепени файлове (attachment) от различен тип, които могат да съдържат както вируси, така и други опасни програми – аплети, скриптове и др. Ситуацията се утежнява от факта, че съвременните E-mail програми, които функционират в персоналните компютри, могат да получават писма в HTML формат и тези програми изпълняват автоматично скритите в такива писма скриптове. Затова е по-добре да не се отварят електронни писма от непознати податели и да не се свалят прикачени към електронни писма файлове, за които не сме сигурни какво съдържат.

- При свързване с Интернет сайтове. За съжаление, едва ли има Интернет сървъри, които могат да се похвалят с абсолютна обезопасеност и непробиваемост от страна на хакери. Това се дължи на разнообразните интернет приложения, които функционират в тях и в които често могат да бъдат открити пропуски, допускащи неоторизиран достъп до базисния софтуер. По този начин злонамерени лица могат да проникнат в сървъра и да инсталират свои програми в някои Web страници, без съответния администратор да знае за това. При това почти всички Интернет сървъри използват най-новите технологии, като Java и ActivX програми, за да създават динамични и впечатляващи Интернет страници, а тези програми се зареждат и изпълняват автоматично при обръщение към съответната страница.

- При сваляне на файлове от Интернет (download). Това е съвременен аналог на заразяването от дискети. Трябва да се избягва тегленето от съмнителни сайтове, както и от сайтове, в които се предлагат модифицирани файлове – много вероятно е те да съдържат вирус или троянски кон. Затова е най-добре снабдяването с програма от Интернет да стане директно от сайта на производителя й.

Има и други начини на разпространение (по IRC, по локална или глобална мрежа и др.), но това са най-често срещаните.

4. Механизъм на действие на вирусите.

Механизмът на действие на вируса включва четири основни стъпки:

- **разпознаване** – като се използва специална парола, вирусът може да определи дали файлът е поразен от него или не. По този начин се избягва двойното заразяване.

- **копиране** – вирусът търси части от програмата, където може да се копира и по този начин да стане част от нея.

- **действие** – това е същинската част от вредното влияние на вируса. При настъпването на определени условия се задейства неговия разрушаващ механизъм. Тези условия могат да бъдат някое обичайно действие при работа с програмата, като копиране на файл и отваряне на меню, както и настъпване на определено събитие в цялата компютърна система (напр. определена дата и час).

- **придвижване** – след обработката на съответната част от командата вирусът се връща в програмата, от която е дошъл. Това става, за да може извиканата потребителска програма, която е поразил да започне работа.

5. Видове компютърни вируси.

Вирусите биват разделяни на множество видове, но често те представляват няколко от тези видове, събрани в един вирус.

а) Според начина на заразяване:

- **Преписващи** – записват своя код върху части от заразената програма и я разрушават;

- **Дописващи** – "прикачат" се към оригиналната програма, като увеличават обема на заеманата от нея памет.

б) Според областта на поразяване на вируса:

- **Файлови**. Поражения търпят програмните файлове, т. е. вирусът се присъединява към файлове с разширения COM или EXE, въпреки че в отделни случаи могат да се заразят и файлове с разширения SYS, DRV,BIN,DLL, SRC, SCR, OVL или OVY. (Потребителите на Macintosh обаче могат да получат вирус от всеки файл, защото файловата им система включва разклонения на ресурсите, където вирусите могат да се скрият.) След като се стартира заразената програма, вирусът се зарежда в паметта и заразява други изпълними файлове. Така на практика, за кратко време и без знанието на потребителя може да се зарази целия наличен софтуер. Някои от тях са **полиморфни** – произвеждат променящо се (но работоспособно!)

копие на себе си. На теория това ги прави по-трудно откриваеми за антивирусния софтуер, но на практика се оказва, че не са чак толкова добре написани, за да успеят да се променят достатъчно.

- **Boot-секторни**. Boot-секторът (зареждащият сектор) е място на твърдия диск на компютъра, към което компютърът се обръща при стартирането си. Там е записана най-важната информация, която системата трябва да знае при стартирането си – за формата на устройството, за записаните на него данни, както и малка програмка, зареждаща системните файлове. Именно тази програмка е целта на вирусите. Те преместват системните файлове, така че да не могат да се използват. При поразяване от такъв вирус компютърът изобщо не може да се стартира и по тази причина вирусът не може своевременно да бъде открит и блокиран. Съществуват и т. нар. вируси FAT Scrabmlers - тези вируси така разбъркват двете копия на FAT, че всичко записано на диска става негодно за каквито и да е манипулации. Двете копия на FAT се разбъркват всяко по различен начин с цел максимални щети. Няма друг изход освен Форматиране от BIOS и след това предформатна подготовка с FDISK и повторно форматиране с Format /u /c /s.

- **BIOS-вируси**. Те поразяват входно-изходната система на компютъра, като променят неговата конфигурация, което прави някои устройства или цялата система неизползваема. Най-честите промени са свързани с флопитата, често се обявява че флопитата не са инсталирани и компютъра не може да ги използва. Разбира се и често пъти вирусите така разбъркват данните от BIOS-а, че компютърът не може да се стартира. Вирусите причинили всякакви промени по BIOS-а не позволяват нормалното преконфигуриране. Трети вируси се самозаписват в BIOS-а и се самостартират от там още преди ОС да е заредена. Борбата с тези вируси е много сложна, защото те контролират целият хардуер и софтуер.

- **Макровируси**. Те заразяват файлове с данни на текстообработващи програми и електронни таблици (най-вече файлове създадени с приложенията от пакета Microsoft Office - Word и Excel). Те нападат най-напред файла Normal.dot (за Word) и Normal.xls (за Excel). Разпространението им се дължи главно на приложенията, в които са вградени програмни езици за писане на макроси, т. е. минипрограми, написани от потребителя, автоматизиращи изпълнението на рутинни задачи. Макровирусът също е макрос. Причиняват правописни и стилистични грешки (напр. разместване на думи в документите), променят данните или ги унищожават (напр. суматорните вируси са предвидени да събират и закръглят стойности предизвиквайки много големи бъркотии – започвайки от най-ниските нива на Excel и стигат до най-високите нива на счетоводни и ведомствени и подбанкови и банкови нива и функции)., изпращат документи по e-mail без уведомяване на потребителя, и много, много други, включително до форматиране на твърдия диск. Тези вируси са най-масово разпространени – около 75% от всички вируси, бродещи из мрежата и дисковите носители. Разпространяват се бързо поради големия обмен на такива документи, поради лекотата, с която се пишат (в сравнение с трудното кодиране при останалите вируси) и поради факта, че се прикрепят към файлове, използвани от широк кръг потребители, често не толкова бдителни и трудно разпознаващи вирусите когато ги получат.

- **Многостранно действащи вируси** – инфектират и boot-секторите, и файловете. Това е сложна ситуация, която най-често означава дълъг цикъл от самозаразяване на компютъра. Понякога от този вид цикли е много трудно да се излезе, без да се пожертва цялата информация, записана на твърдия диск.

в) Според присъствието на вируса в паметта:

- **Резидентни**. Вирусът се разполага в паметта на компютъра и пречи на нормалното функциониране на операционната система, което се проявява в нетипични действия при работа с програмите. Резидентните вируси остават активни до изключване на компютъра от захранването (както например някои драйвери).

- **Нерезидентни**. Те се разполагат в програмния код на програмата.

г) Според характера на действието си:

- "**Безвредни**" (всъщност такива вируси няма) – за безвредни се считат вирусите, които нанасят пренебрежимо малки щети – заемат част от дисковото пространство, нарушават видеоизображението, предизвикват неочаквани звукови ефекти и др.

- Разрушителни – спектърът на действие обхваща всевъзможни щети (от промяна в съдържанието на определен сектор до форматиране на диска);

Съществуват и вируси-убийци – по непотвърдени данни тази категория вируси не поврежда данни или каквото и да било друго, но убива оператора (работещия с компютъра). Такъв вирус са използвали в КГБ

като крайна мярка на защита на компютрите им през студената война. Вируса се е казвал 666 (но няма нищо общо с разпространения файлов 666 вирус, носещ същото име за заблуда) и е объркал до такава степен мозъчните вълни, че е причинявял невероятно главоболие и смърт. Много любопитни хакери, кракери, експерти и програмисти са се опитвали да откраднат вируса но никой още не е успял...

д) Според начина на заразяване:

- **Файлови** – те се прикрепват към програма и пренаписват част от програмния й код, което нарушава нейния нормален начин на работа.

- **Системни** – разполагат се директно в оперативната памет на компютъра и модифицират действието на всички програми, които се зареждат за изпълнение. Те поразяват boot-сектора и командния интерпретатор, който анализира въведените команди, стартира съответните функции и съдържа всички вътрешни команди (при MS DOS това е файлът command.com).

- **Стелт вируси (Stealth)**. Тези вируси се настаняват както във файлове, така и оставят свои модули в оперативната памет. Те прикриват симптомите на вирусната инфекция и взаимодействат с различни антивирусни програми, като принуждават програмата да каже, че няма вируси. Тези вируси не показават промени по размерите на файла, който са инфектирали, което ги прави трудни за засичане и обезвреждане! Самият вирус лесно се укрива и трудно се премахва. Единият от начините на самозащита на тези вируси е секторите от харддиска и (или) дискетата, където е записан оригинала на вируса да се маркират като лоши (механично повредени), въпреки че не са повредени по никакъв начин. Всички антивирусни програми които проверяват твърдия диск или дискетите "виждат" маркираното - "лош сектор" и го прескачат и не засичат вируса. А другият начин за самосъхранение на този вид вируси е да притежават самопроменящ се код, което прави тяхното откриване трудно. Ако модулът, оставен в паметта, забележи, че някое приложение се опитва да чете заразен файл, той сменя в движение данните, все едно, че файлът е чист. Ето защо тези вируси не могат да бъдат уловени от антивирусните програми.

е) Вирусоподобни програми:

- **"Терористи" (Droppers)** – програми, създадени да прокарат вируса, без той да бъде засечен от антивирусна програма. За целта се използва кодиране, което блокира възможността антивирусната програма да разпознае вируса. След като го транспортират успешно, "терористите" изчакват указано събитие или време и го активират;

- **"Троянски коне" (Trojan Horse)** – това са програми, представящи се за легално съществуващ полезен софтуер (приложни програми, игри, драйвери и др.). Често това са обемисти програми и дори за по-голяма достоверност понякога наистина изпълняват част от официално обявените си функции. Те не инфектират други файлове, но могат да причинят сериозни неприятности, например като изпращат на определен адрес в Интернет файла с паролите на заразения компютър – така компютърът е превзет отвътре и може да бъде управляван отвън (по приликата с дървения кон на гърците, подарък за Троя). Пример за това е FreeWare програмата ProMail 2000 v. 1.02, която служи като оптимизатор на мрежовия трафик и разпределение на пощата. Програмата създава файла ACCOUNT.INI в който се съдържат всички имена пароли и привилегии за достъп на всички потребители и информация за степента на защита на мрежата който файл се копира и копието му се изпраща като прикачен файл по електронна поща до създателя на програмата.

- **"Червеи" (Worms)** – Разпространяват се най-вече в компютърни мрежи и Интернет. Те копират сами себе си без да заразяват други файлове. Причиняват вреда с това, че се намират в системата, отнемайки дисково пространство. Най-често се заразяват непредпазливите потребители на електронна поща. Обикновено вирусите използват възможностите на електронната поща на "приемника", за да продължат разпространението си, като се "самоизпращат" от негово име. Така се настаняват в друг компютър. Същевременно нанасят и много сериозни щети, като изпращат на определен адрес информация за заразения компютър – пароли, файлове с данни, подбрани по определен критерий и др.

6. Поведение на компютърната система при заразяване.

Наличието на вирус в компютъра не винаги се установява навреме от неговия потребител. Това може да доведе до безпрепятственото му разпространяване, което увеличава риска от поразяване. Типичните симптоми, които са знак за наличието на вирус в компютърната система са:

- забавена работа на компютъра;

- приложните програми изискват несанкциониран достъп до твърдия диск или дискета;

- продължително време за зареждане на програмите;

- неочакван недостиг на памет;

- неестествено голям размер на файловете;
- неадекватно поведение на системата;
- безпричинно изчезване, повреждане или промяна в размера на файла;
- нарастване броя на дефектните сектори по носителите;
- съобщения или повреди на дисковите устройства;
- получаване на файлове със странни имена или с двойни разширения;
- извеждане на съобщения, които нямат нищо общо с възложената на компютъра работа;
- блокиране на клавиатурата или мишката;
- неочаквано появяващи се надписи или анимации;
- изненадващо и неочаквано рестартиране на компютъра;
- изчезване на файлове и разместване на папки;
- невъзможност за зареждане на операционната система.

При съмнение за наличието на вирус трябва: Да се рестартира компютъра чрез бутона Reset, а не чрез комбинацията от клавиши Ctrl + Alt + Del, защото повечето вируси са способни да издържат удара и остават в паметта. След това е необходимо да се стартира поне една програма за антивирусна защита. Най-добре е да се използват няколко програми от различни производители, което би осигурило по-пълно засичане на заразените файлове и вируса (вирусите) които са ги заразили.

Изтриват се всички заразени файлове и се възстановяват от архив. Проверява се дали настройките във BIOS-а не са разбъркани от вируса. Някои вируси променят настройките на BIOS-а така, че да се прескачат флопитата. Ако настройките са разбъркани трябва да се възстановят. Други вируси просто разбъркват настройките на BIOS-а, за да не може въобще да се стартира компютъра. Трети вируси се записват в BIOS-а на компютъра и се зареждат с данните за компютъра. Препоръчително е да се изтриват всичките заразени файлове защото няма гаранция, че изчистването на файла (ако е възможно) е отстранило тялото и кода на вируса изцяло и коректно и има възможност "изчистеният" файл да се зарази отново. Винаги възстановяването на файловете от архив трябва да става след като заразените файлове са изтрити. Когато е засечена инфекция веднага трябва да се преформатират всички дискети, които са масово използвани от BIOS-а на компютъра, ако тази опция е включена (някои стари BIOS-и нямат директно записана настройваща програма на самия чип и ползват специални дискети на които е записана настройващата програма.) Това предпазва от повторно заразяване. Вирусът създава множество свои копия върху дискетата - заразява я. Ако тези дискети се използват повторно преди да се преформатират ще се разпространи заразата отново. Преди стартиране на коя да е антивирусна програма трябва да се рестартира от гарантирано чиста системна дискета, която трябва да бъде защитена срещу запис. Програмите, които ще се стартират срещу вирусите трябва да са на същата системна дискета от която е заредено. Премахването на BIOS-вирус става по следния начин: Стартира се BIOS-а и внимателно се преписват всички настройки. Сваля се от дънната платка батерийката, захранваща BIOS и се сваля и BIOS чипа за около 1 минута - достатъчна да се изтрият променливите на опциите на BIOS и самия вирус. После по обратен ред се връщат на местата обратно първо BIOS чипа и после батерийката. Включва се компютъра и се възстановяват обратно преписаните настройки от началото.

Добра идея е при Windows 95/98 да се използва сканиране от Safe mode, защото тогава се зарежда само Windows в минимален режим и ако има вируси, те няма да се заредят, освен ако не са заразили win.com файла.

Ако вируса се разпространява по e-mail, то тогава се преписват всички адреси в тефтерче и се изтриват от адресната книга, после се спира интернет връзката, откача се телефонния кабел от модема и се следват горните описания. Най-добре е с всичко това да се занимава специалист.

7. Антивирусни програми.

За борба срещу вирусите се създават специални програми за антивирусна защита, наречени антивирусни програми. Те проверяват компютъра за наличието на вируси. Антивирусния софтуер бива два типа: антивирусни програми и програми, изпълняващи ролята на "защитна стена" (firewall) за компютъра или локалната мрежа. Целта на програмите от тип "защитна стена" е да не допускат заразяването, като предотвратят нерегламентирания достъп до компютърната система.

Известни антивирусни програми са Norton Antivirus, McAfee Antivirus, F-Prot, Kaspersky Antivirus, Panda Antivirus и много други.

Антивирусната програма е програма, следяща всички процеси в компютъра за някакъв вид активност, която би могла да повреди

файлове в компютъра или да форматира диска, или да нанесе всякакви поражения. Тя се състои от няколко основни части

- База данни с дефиниции на вируси - това са ключови уникални низове от тялото на вируса - части от вируса по които вируса бива идентифициран.

- Файлов скенер - тази част от антивирусната програма преглежда файловете за тези ключови низове - и ако ги има предприема мерки за отстраняването на вируса - това става чрез "имунизация на файла". Често пъти антивирусните програми записват като скрити файлове из свойте или из всички папки файлове които съдържат информация за файла - атрибутите: checksum - контролна сума, CRC - Cyclical Redundancy Check на файла и размер на файла. При зараза тези атрибути се променят за да напаснат на новите процедури във файла. Един файл може да има само един верен CRC и една вярна контролна сума за даден размер на файла. При премахване на вируса антивирусната програма премахва частите на вируса докато новите контролна сума, размера и CRC не съвпаднат с тези в контролния файл записани преди заразата. Ако програмата е безвъзвратно повредена то антивирусната програма няма друг избор, освен да изтрие заразения файл. Най-добрите програми като F-Secure, McAfee virus scan, AVX, Panda Antivirus, Norton Antivirus използват комбинирани методи за сканиране като включват имунизация. Това сканиране се състои от сканиране за низове, сканиране за промяна на CRC и на контролната сума и размера на файла едновременно. Така се улавят непознати вируси. Тази техника дори позволява да се изчислат с приближение шансовете за възстановяване на файла. Не рядко е имало успехи при премахването на непознати вируси.

- Резидентен модул - този модул тази част е подобно на скенера, но вместо да следи файловете по твърдия диск в непроменено състояние, тя следи за всичко това когато един файл се копира, мести, стартира, отваря, записва, редактира, затвара и прочие действия с файлове. При откриване на зараза, резидентната част извиква файловия скенер като преустановява работата на текущия процес, предизвикал тревогата. Резидентния модул затваря всички файлове и ги записва по твърдия диск след което потребителя бива подканен да стартира файловия скенер. Резидентния модул сканира за вичко това в реално време като използва част от системните ресурси, като краен ефект се забелязва леко забавяне на компютъра.

- Интерфейс - това е тази част от антивирусната програма, която потребителя вижда и чрез която той общува с антивирусната програма. Колкото по лек, приятен за окото и по интуитивен е той, толкова по-лесно и ефективно се работи с програмата.

- Евристичен скенер това са допълнителни алгоритми изследващи поведението на файла, анализират резултата от поведението и решават да вдигнат ли тревога. Тези скенери са много чувствителни и мнителни. Възможно е те да вдигнат празна тревога. Ако файла е заразен то вие сте получили предупреждение и можете да го сложите в карантина където да решите какво да го правите. Но карантинната папка не е 100% сигурна. Тя не позволява на софтуера да преглежда файловете, но вие винаги можете да се поровите с файловия си мениджър по диска и да ровите в папката. (Карантинна папка – това е една папка която се създава от антивирусната програма с цел там да се държат съмнителни или заразени файлове, докато решите какво да ги правите или да ги изтриете.)

- Допълнителни модули и функции - срещат се при първокласните програми, които трябва да бъдат прецизни до краен предел.

* Мрежови модули - позволяват антивирусната програма да се инсталира само на сървъра в мрежа а програмата да покрива цялата мрежа - сканиране, следене на заявките, следене на трафика, интернет връзката, и всичко което използва мрежата.
* WEB филтри - тези модули позволяват да се ограничи достъпа до потенциално опасни сайтове, а и родителите могат да ги използват за ограничаване на достъпа до порнографски сайтове или сайтове с насилие или оскърбително съдържание. С тях може да се блокират и банерите и рекламите като се каже на филтъра да филтрира рекламния сървър.
* Пощенски модул - едно допълнение което би трябвало да е в секцията задължителни. Този модул сканира пощата ви, като се активира само ако работите с нея.
* Даунлоад контрол - следи всичко което се тегли от мрежата, като отново се активира само при заявка за даунлоад.
* Архивен Модул - създава архивно копие на твърдия диск върху външен носител. Това е най-висшата степен на защита - ако има

проблем, програмата изтрива заразените файлове и възстановява техни копия от архива.

Много антивирусни програми предлагат възможност да се отстрани вирусът веднага след откриването му. Тази задача може да се управлява от потребителя. Това означава, че той може да избира между следните възможности:

- никакво отстраняване;
- отстраняване след потвърждение;
- отстраняване без потвърждение с допълнителна възможност да се изчисти заразения файл или той да се изтрие от твърдия диск.

Част от антивирусните програми при стартиране на компютърната система се зареждат в паметта. При опит за четене или запис от дискета те проверяват за наличието на вируси преди изпълнението на операцията. Друга част от антивирусните програми се използват за проверка и отстраняване на вируси в процеса на работа с компютъра. Най-добрите програми позовляват проверка на постъпващите данни в персоналния компютър от локалната мрежа и Интернет, в това число и електронната поща.

Няколко са основните характеристики, съществени при оценяване работата на един антивирусна програма:

- Области на приложение – до каква степен програмата осигурява защита от повторна инфекция и отстраняване на вируса;
- Брой на вирусите за откриване – програмата трябва да предоставя списък на вирусите, които открива и да отчита процентната грешка при сканирането;
- Необходимо време за търсене – добрите програми притежават възможност за извършване на сканиране в предварително програмируемо време, когато не се работи активно със системата;
- Редовна актуализация – тъй като непрекъснато се появяват нови вируси, трябва антивирусните програми да се обновяват със средства за борба срещу тези нови вируси (т. нар. антивирусни дефиниции). Това става посредством актуализация чрез Интернет.

Освен отстраняването на вируси тези програми осигуряват защита срещу несанкционирани опити за запис върху носител или неговото форматиране и срещу промяна на boot-сектора на твърдия диск или дискета. Те се грижат за проверка на появили се лоши сектори. Добрите програми за антивирусна защита дават съобщение при опит за инсталиране на резидентни програми.

Единственото научно звено у нас, специализирано в борбата с вируси, е Националната лаборатория по компютърна вирусология при Българска Академия на Науките. Тя предлага комплект от антивирусни програми, в които влизат Dir2Clr, VirC, F-Prot, F-Macrow, F-stop, Agent и др. По нейни данни 80% от случаите на заразяване в страната стават чрез комуникационни връзки, а останалите 20% - чрез дискети.

8. Правила за предпазване от компютърни вируси.

- Да се използват програми, в чийто произход сме сигурни. (Предимството е на страната на оригиналния софтуер.);
- Ограничаване на достъпа до компютъра на външни лица (в най-голяма степен това се отнася до компютърните игри). Колкото кръгът на работещите е по-ограничен, толкова сигурността е по-голяма;
- Редовно да се правят копия на файловете с данни и на по-важните програми, като трябва да сме сигурни, че когато правим копията, компютърът е "чист";
- Изтриване незабавно на всички програми, за които имаме съмнения, че може да са заразени;
- Да се инсталира антивирусна програма и винаги да се свалят най-новите антивирусни дефиниции за нея от Интернет (най-добре от сайта на производителя). Те не трябва да са по-стари от месец.
- Поне веднъж седмично да се прави пълно антивирусно сканиране на компютъра с антивирусна програма;
- Да се сканира с антивирусна програма всеки свален от Интернет, получен на дискета или нелицензиран CD файл.
- Редовно да се правят архивни копия на данните. Това е една от най-добрите мерки не само срещу вируси, но и срещу 99% от всички неприятности, които биха ни сполетели. Ако вирус или грешка унищожи данните просто се форматира твърдия диск, инсталират се програмите отново и се възстановяват данните от архива.