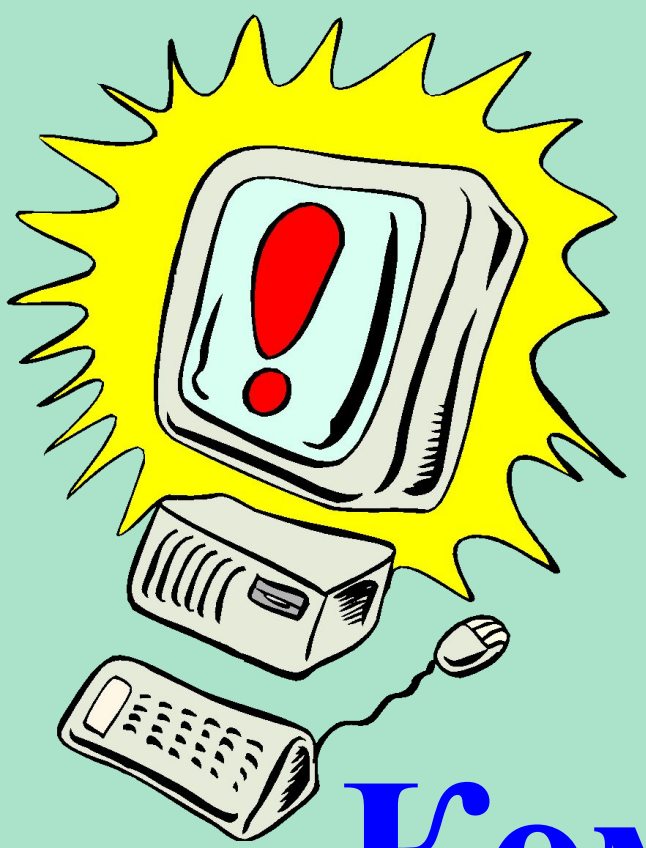


Компьютерные вирусы

Содержание:

1. Что такое компьютерный вирус?
2. История компьютерных вирусов
3. Классификация компьютерных вирусов
4. Методы обнаружения и удаления компьютерных вирусов

Что такое компьютерный вирус?

Объяснений, что такое компьютерный вирус, можно привести несколько. Самое простое дадим на примере клерка, работающего исключительно с бумагами. Представим себе аккуратного клерка, который приходит на работу в контору и каждый день обнаруживает у себя на столе стопку листов бумаги со списком заданий на день. Клерк берёт верхний лист, читает указания начальства, пунктуально их выполняет, выбрасывает в корзину для бумаг "отработанный" лист и переходит к следующему листу.

Предположим, что некий злоумышленник тайком прокрадывается в контору и подкладывает в стопку с заданиями лист, на котором написано следующее: "***Переписать этот лист два раза и положить копии в стопку заданий соседей***". Что сделает клерк? Дважды перепишет лист, положит его соседям на стол, уничтожит оригинал и перейдёт к выполнению следующего листа из стопки, т.е. продолжит выполнять свою настоящую работу. Что сделают соседи, являясь такими же аккуратными клерками, обнаружив новое задание? То же, что и первый: перепишут его по два раза и раздадут другим клеркам. Итого в конторе бродят уже четыре копии первоначального документа, которые и дальше будут копироваться и передаваться на другие столы.

Примерно также работает и компьютерный вирус, только стопками бумаг-указаний являются **программы**, а клерком - **компьютер**. Как и клерк, компьютер аккуратно выполняет все команды программы (листы заданий), начиная с первой. Если же первая команда звучит как - "***скопируй меня в две другие программы***", то компьютер так и сделает, и команда-вирус попадёт в две другие программы. Когда компьютер перейдёт к выполнению этих заражённых программ, вирус тем же способом будет расходиться всё дальше и дальше по всему компьютеру.

В приведённом выше примере про клерка и его контору лист-вирус не проверяет, заражена очередная папка заданий или нет. В этом случае к концу рабочего дня контора будет завалена такими копиями, а клерки только и будут что переписывать один и тот же текст и раздавать его соседям. Ведь первый клерк сделает две копии, очередные жертвы вируса - уже четыре, затем 8, 16, 32, 64 и т.д., т.е. количество копий каждый раз будет увеличиваться в два раза.

Если клерк на переписывание одного листа тратит 30 секунд и ещё 30 секунд на раздачу копий, то через час по конторе будет "бродить" более 1 000 000 000 000 000 000 копий вируса! Скорее всего конечно же не хватит бумаги, и распространение вируса будет остановлено по столь банальной причине.

Как это не смешно (хотя участникам этого инцидента было совсем не смешно), именно такой случай произошёл в 1988 г. в Америке: несколько глобальных сетей передачи информации оказались переполненными копиями сетевого вируса (вирус Морриса), который рассылал себя от компьютера к компьютеру. Поэтому "правильные" вирусы делают так: "***Переписать этот лист два раза и положить копии в стопку заданий соседей, если у них ещё нет этого листа***".
Проблема решена - "перенаселения" нет, но каждая стопка содержит по копии вируса, при этом клерки ещё успевают справляться и с обычной работой.

"***А как же уничтожение данных***?" - спросите вы. Всё очень просто - достаточно написать на листе примерно следующее:

1) ***Переписать этот лист два раза и положить копии в стопку заданий соседей, если у них ещё нет этого листа***.

2) ***Посмотреть календарь и, если сегодня пятница, попавшая на 13-е число, выкинуть все документы в мусорную корзину***.

Подобную инструкцию хорошо выполняет известный вирус ***Jerusalem*** (другое название - ***Time***).

Кстати, на примере клерка очень хорошо видно, почему в большинстве случаев нельзя точно определить, откуда в компьютере появился вирус. Все клерки имеют одинаковые (с точностью до почерка) КОПИИ, но оригинал-то с почерком злоумышленника уже давно в корзине!

Вот такое простое объяснение работы вируса. Плюс к нему хотелось бы привести две **аксиомы**, которые, как это ни странно, не для всех являются очевидными.

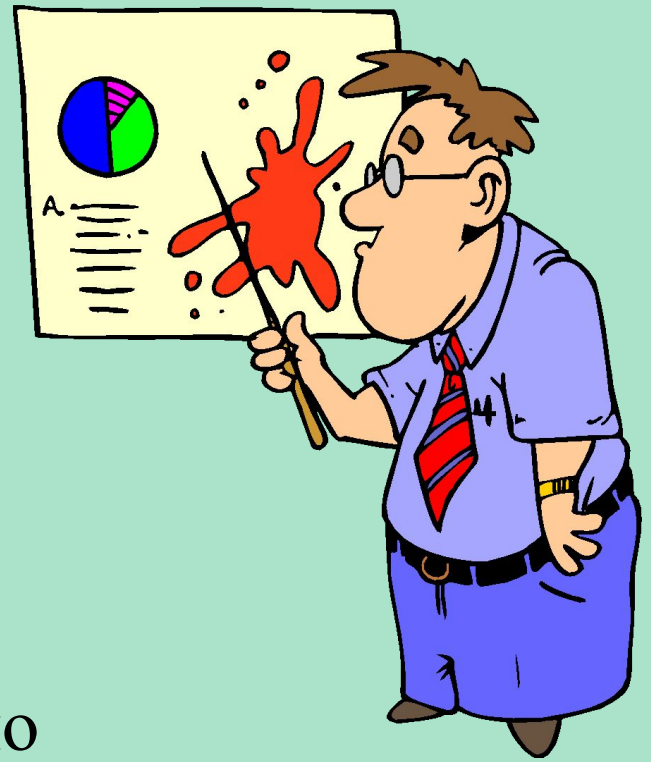
Во-первых: вирусы не возникают сами собой - их создают очень злые и нехорошие программисты-хакеры и рассылают затем по сети передачи данных или подкидывают на компьютеры знакомых. Вирус не может сам собой появиться на вашем компьютере: либо его подсунули на дискетах или на компакт-диске, либо вы его случайно "скачали" из компьютерной сети передачи данных.

Во-вторых: компьютерные вирусы заражают только компьютер и ничего больше, поэтому не надо бояться - через клавиатуру и мышь они не передаются.

Компьютерный вирус -

- это специально написанная программа, обычно небольшая по размерам, способная самостоятельно дописывать себя к другим программам (заражать их), и производить различные нежелательные действия.

компьютерный вирус



Термин "**компьютерный вирус**" появился позднее, официально считается, что его впервые употребил сотрудник Лехайского университета (США) Ф.Коэн в **1984 г**. на 7***-й конференции по безопасности информации***, проходившей в США. С тех пор прошло немало времени, острота проблемы вирусов многократно возросла, однако строгого определения, что же такое компьютерный вирус, так и не дано, несмотря на то что многие пытались это сделать неоднократно.

Программа, внутри которой находится вирус, называется *«зараженной»*

Когда такая программа начинает работу, то сначала управление получает вирус.

После того, как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится, и она работает так же, как обычно.

Поэтому представляется возможным сформулировать только обязательное условие для того, чтобы некоторая последовательность выполняемого кода являлась вирусом.

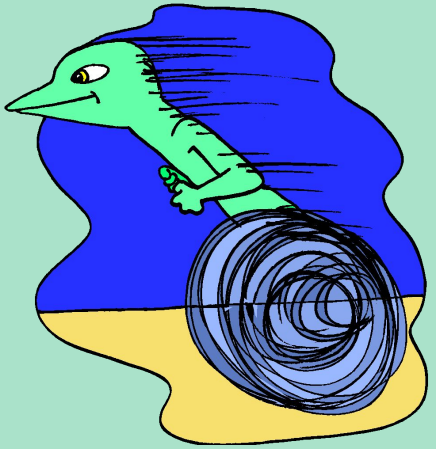
Обязательное (необходимое) свойство компьютерного вируса - возможность создавать свои дубликаты (не всегда совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.

История компьютерных вирусов

Конец 1960-х - начало 70-х годов: "***кролик***" (**the rabbit**) - программа клонировала себя, занимала системные ресурсы и таким образом снижала производительность системы.

Первая половина 70-х годов: под ОС Tenex создан вирус **The Creeper**, использовавший для своего распространения глобальные компьютерные сети. Вирус был в состоянии самостоятельно войти в сеть через модем и передать свою копию удалённой системе. Для борьбы с этим вирусом была создана программа **Reeper** – первая известная антивирусная программа.

История компьютерных вирусов



Начало 80-х годов: компьютеры становятся всё более и более популярными, результат этого – большое число разнообразных «***троянских коней***» - программ, которые при запуске наносят системе какой-либо вред.

1981 год: эпидемия загрузочного вируса ***Elk Cloner*** на компьютерах Apple II. Вирус записывался в загрузочные сектора дискет, к которым шло обращение. Проявлял он себя весьма многосторонне – переворачивал экран, заставлял мигать текст на экране и выводил разнообразные сообщения.

История компьютерных вирусов

1986 год: эпидемия первого IBM PC-вируса ***Brain***. Вирус, заражающий 360 Кб дискеты, практически мгновенно разошёлся по всему миру. Причина такого «успеха» - скорее всего, в неготовности компьютерного общества к встрече с таким явлением, как компьютерный вирус. Вирус был написан в Пакистане братьями Basit и Amjad Farooq Alvi, оставившими в вирусе текстовое сообщение, содержащее их имена, адрес и телефонный номер. Как утверждали авторы вируса, являвшиеся владельцами компании по продаже программных продуктов, они решили выяснить уровень пиратского копирования в их стране. К сожалению, их эксперимент вышел за границы Пакистана. Интересно, что этот вирус являлся также и первым «стелс»-вирусом – при попытке чтения заражённого сектора он «подставляет» его незаражённый оригинал.

История компьютерных вирусов

1987 год: появление вируса ***Vienna*** и ещё несколько вирусов для IBM PC. Это знаменитые в прошлом ***Lehigh***, заражающий только COMMAND.COM, ***Suriv-1*** (другое название – April1st), заражающий COM-файлы, ***Suriv-2***, заражающий (впервые) EXE-файлы, и ***Suriv-3*** заражающий как COM-, так и EXE-файлы. В декабре 1987 года случилась первая известная повальная эпидемия сетевого вируса ***Cristmas Tree***, написанного на языке REXX и распространявшего себя в операционной среде VM/CMS. 9 декабря вирус был запущен в сеть в Западной Германии и через четыре дня 13 декабря парализовал сеть IBM Vnet. При запуске вирус выводил на экран изображение рождественской ёлочки и рассылал свои копии всем пользователям сети.

История компьютерных вирусов

1988 год: в пятницу 13 мая сразу несколько фирм и университетов разных стран мира познакомились с вирусом ***Jerusalem*** – в этот день вирус уничтожал файлы при их запуске. Это, пожалуй, один из первых MS-DOS-вирусов, ставший причиной настоящей эпидемии: сообщения о заражённых компьютерах поступали из Европы, Америки и Ближнего Востока. Название, кстати, вирус получил по месту одного из инцидентов – университета в Иерусалиме.

В этом году была создана новая антивирусная программа – Dr.Solomon's Anti-Virus Toolkit, являющаяся на сегодняшний день одним из самых мощных антивирусов.

История компьютерных вирусов

1989 год: обнаружен новый вирус ***Datacrime***, который имел крайне опасное проявление – с 13 октября по 31 декабря он форматировал винчестер. Следует отметить тот факт, что 1989 год являлся началом повальной эпидемии компьютерных вирусов в России – всё те же вирусы Cascade, Jerusalem, Vienna заполонили компьютеры наших соотечественников.

В конце 1989 года в России Е.В. Касперским была разработана первая версия антивируса AVP (AntiViral Toolkit Pro). .

История компьютерных вирусов

1990 год: этот год принёс несколько довольно заметных событий. Первое из них – появление полиморфик-вирусов **Chameleon** (другое название – V2P1, V2P2, V2P6). До этого момента антивирусные программы для поиска вирусов пользовались так называемыми «масками» - кусками вирусного кода. После обнаружения вирусов Chameleon разработчики антивирусов были вынуждены искать другие методы детектирования вирусов.

Второе событие – появление болгарского «завода по производству вирусов»: огромное число новых вирусов имело болгарское происхождение. В июле произошёл инцидент с компьютерным журналом **PC Today** (Великобритания). Он содержал гибкий диск, заражённый вирусом ***DiskKiller***. Было продано более 50 000 экземпляров журнала.

История компьютерных вирусов

1991 год: популяция компьютерных вирусов непрерывно растёт, достигая уже нескольких сотен. В апреле разразилась настоящая эпидемия файлово-загрузочного полиморфик-вируса ***Tequila***. Россию это событие практически не затронули.

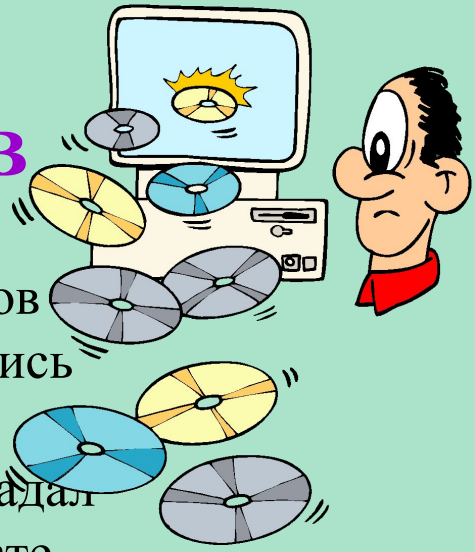
Лето 1991: эпидемия вируса ***Dir_II***, использовавшего принципиально новые способы заражения файлов (link-вирус). В целом 1991 год был достаточно спокойным – этакое затишье перед бурей, разразившейся в 1992.

История компьютерных вирусов

1992 год: первый ***полиморфик-генератор MtE***, на его базе через некоторое время появляется сразу несколько полиморфик-вирусов. Первый вирус для Windows, заражающий выполняемые файлы этой ОС, открыл новую страницу в вирусописательстве.

1993 год: появляется всё больше вирусов, использующих весьма необычные способы заражения файлов, проникновения в систему и т.д.

История компьютерных вирусов



1994 год: всё большее значение приобретает проблема вирусов на CD-дисках. Быстро став популярными, эти диски и оказались одним из основных путей распространения вирусов.
Зафиксировано сразу несколько инцидентов, когда вирус попадал на мастер-диск при подготовке партии CD-дисков. В результате на компьютерный рынок были выпущены довольно большие тиражи (десятки тысяч) заражённых CD-дисков. Естественно, что об их лечении говорить не приходится – их надо просто уничтожать.
В июне началась повальная эпидемия вируса OneHalf, до сих пор являющегося самым распространённым в России.
Сентябрь: «***ЗАРАЗА***» - эпидемия файлово-загрузочного вируса, использующего крайне необычный способ внедрения в MS-DOS. Ни один антивирус не оказался готовым к встрече с подобного типа монстром.

История компьютерных вирусов

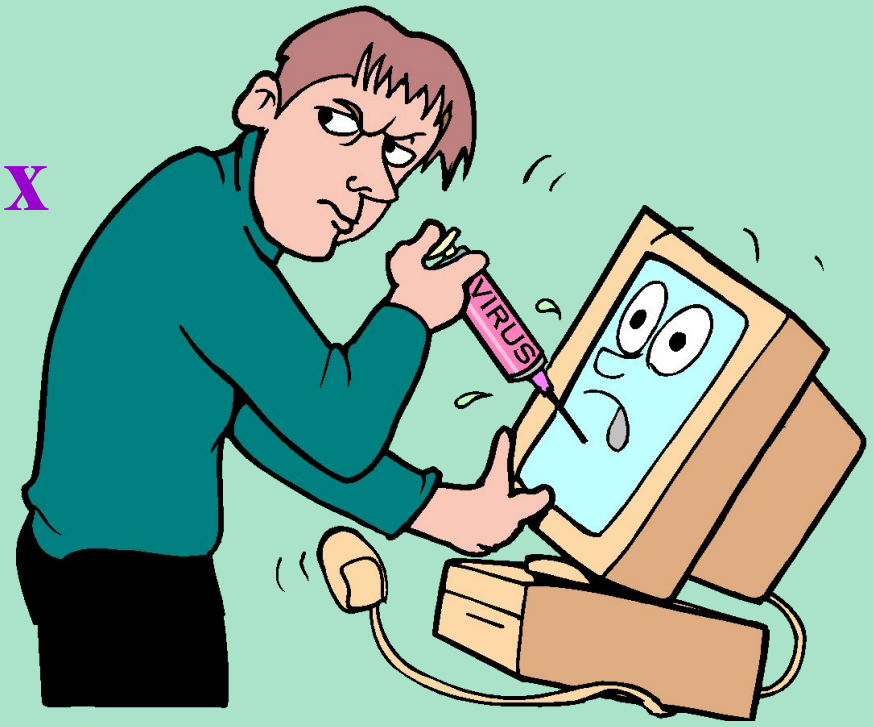
1995 год: произошёл инцидент с Microsoft: на диске, содержащем демонстрационную версию Windows 95. Копии этого диска были разосланы бета-тестерами, один из которых не поленился проверить диск на вирусы.

Август: один из поворотных моментов в истории вирусов и антивирусов – в «живом виде» обнаружен первый вирус для Microsoft Word (***Concept***). Буквально за месяц вирус «облетел» весь земной шар, заполнил компьютеры пользователей MS-DOS и прочно занял первое место в статических исследованиях.

История компьютерных вирусов

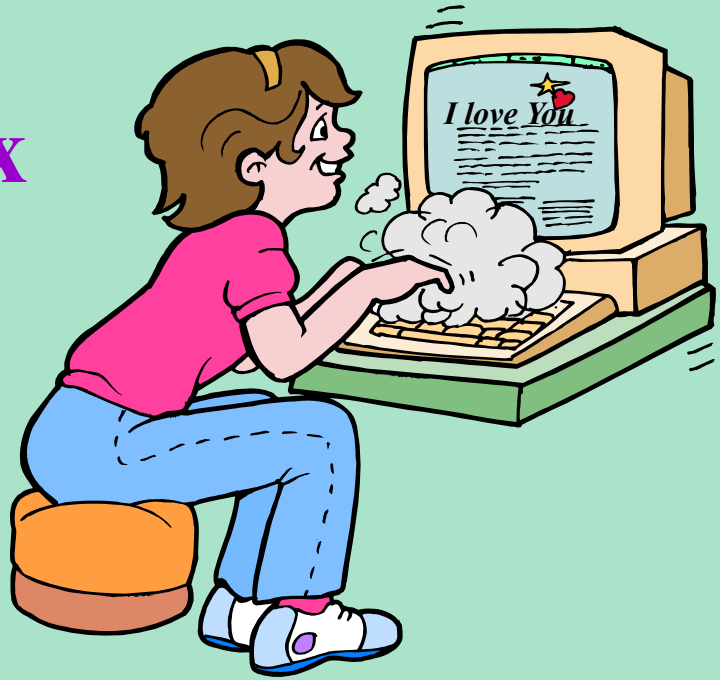
1996 год: два достаточно заметных события – появился первый вирус для Windows 95 (***Win95.Boza***) и началась эпидемия крайне сложного полиморфик –вируса ***Zhengix*** в Санкт-Питербурге.
Март: первая эпидемия вируса для Windows 3.x (***Win.Tentacle***).
Июль: ***Laroux*** - первый вирус для Microsoft Excel, к тому же пойманный в «живом виде».

История компьютерных вирусов



1997 год: макровирусы перебрались в Office 97, поэтому появились вирусы, ориентированные только на документы Office 97.
Апрель: ***Homer*** – первый сетевой вирус-червь, использующий для своего размножения File Transfer Protocol (ftp).
Июнь: появление первого самошифрующегося вируса для Windows 95.

История компьютерных вирусов



2000 год: появление и эпидемия в России вируса «***I love You***».

Контрольные вопросы:

1. Когда впервые появился термин «компьютерный вирус»?

2. Какое обязательное свойство компьютерного вируса?

3. Когда появилась первая версия антивируса Е.В. Касперского?

Классификация компьютерных вирусов:

Вирусы можно разделить на классы по следующим основным признакам:

1. ***среда обитания;***
2. ***способ заражения среды обитания);***
3. ***особенности алгоритма работы;***
4. ***деструктивные возможности.***

В зависимости от **среды обитания** вирусы можно разделить на:

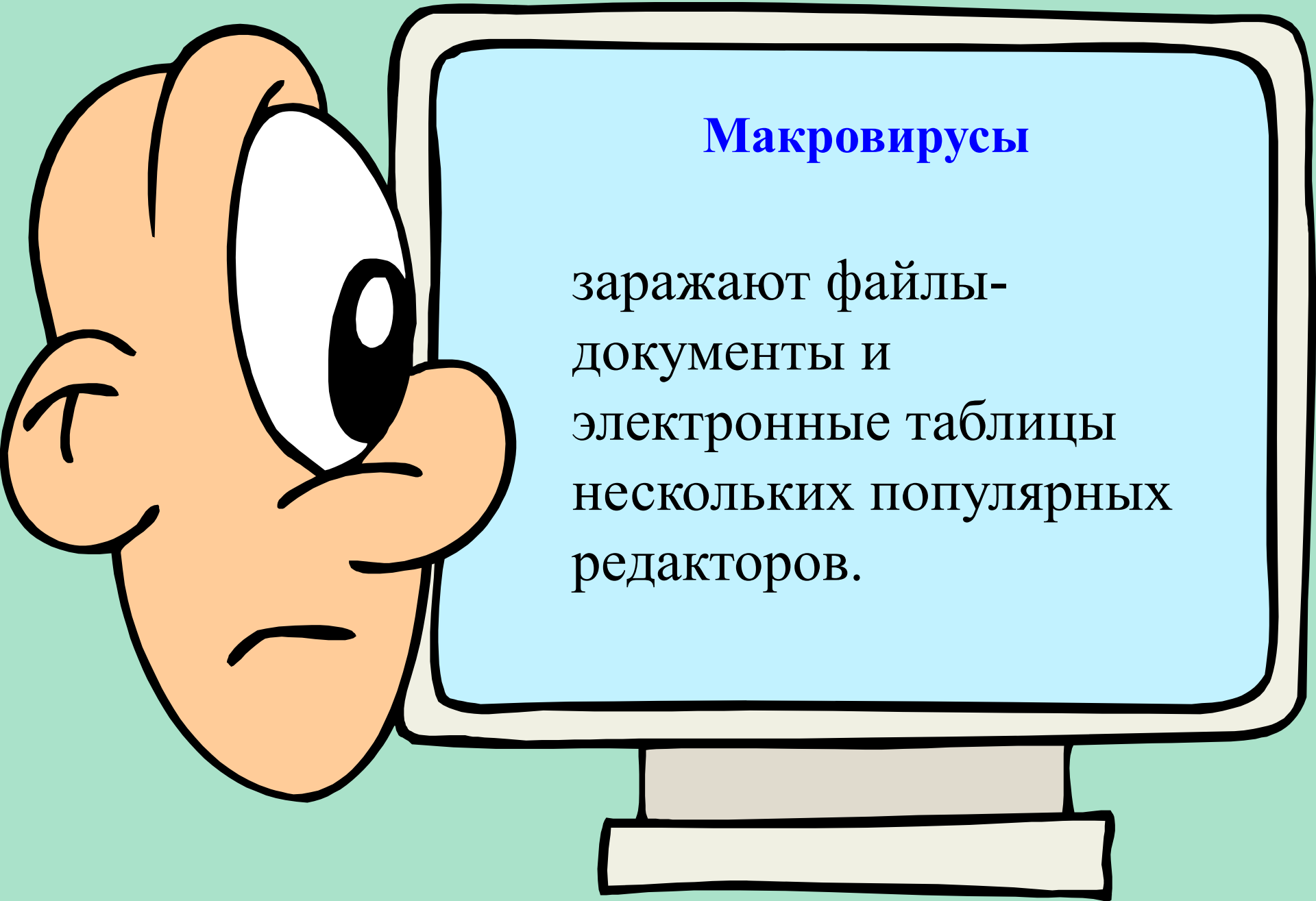
- ***файловые***;
- ***загрузочные***;
- ***макровирусы***;
- ***сетевые***.

Файловые вирусы

либо различными способами внедряются в выполняемые файлы (наиболее распространённый тип вирус), либо создают файлы-двойники (вирусы-компаньоны), либо используют особенности организации файловой системы (link-вирусы).

Загрузочные вирусы

записывают себя либо в загрузочный сектор диска (boot-секторы), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record), либо меняют указатель на активный boot-сектор.



Макровирусы

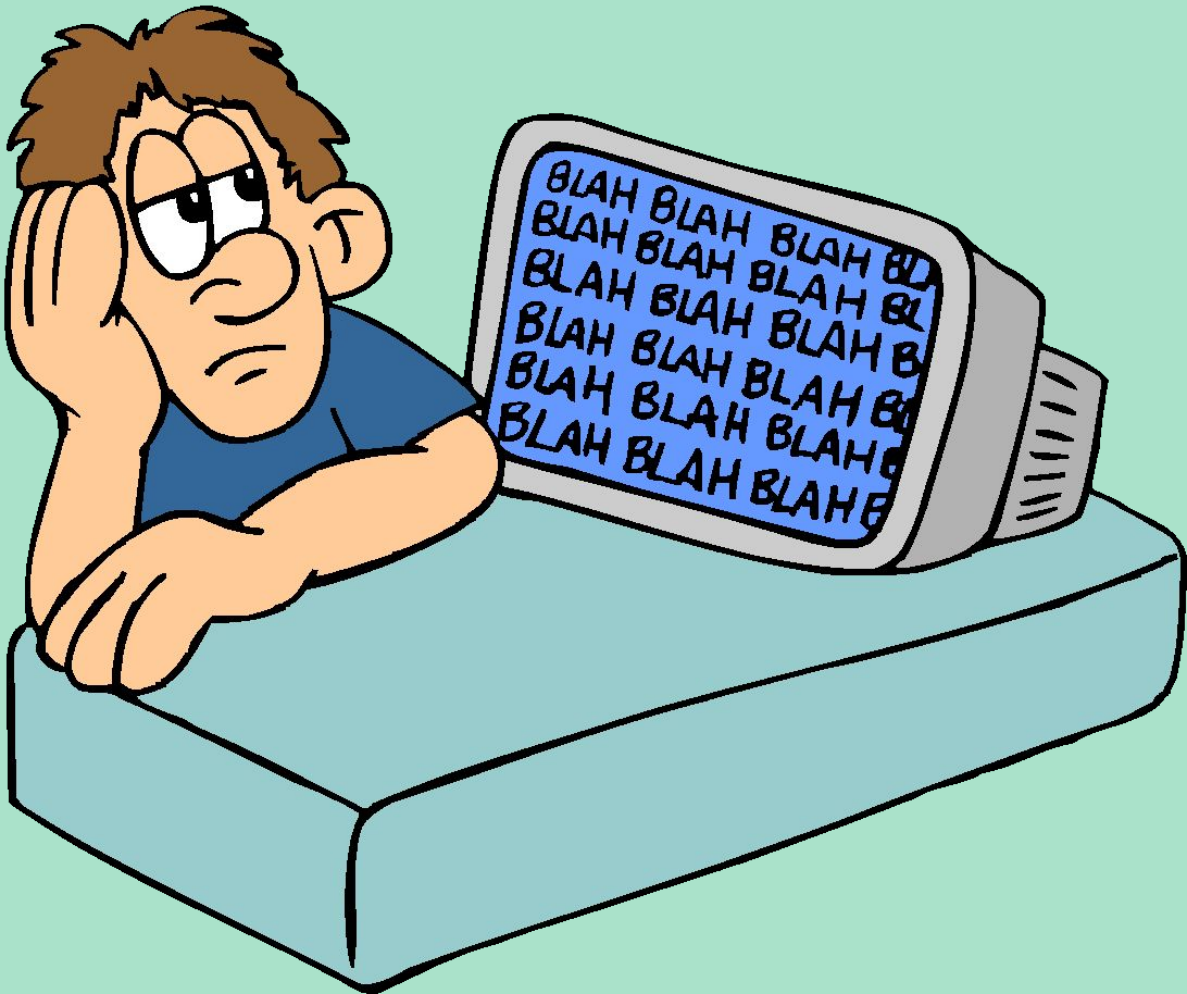
заражают файлы-документы и электронные таблицы нескольких популярных редакторов.

Сетевые вирусы

используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

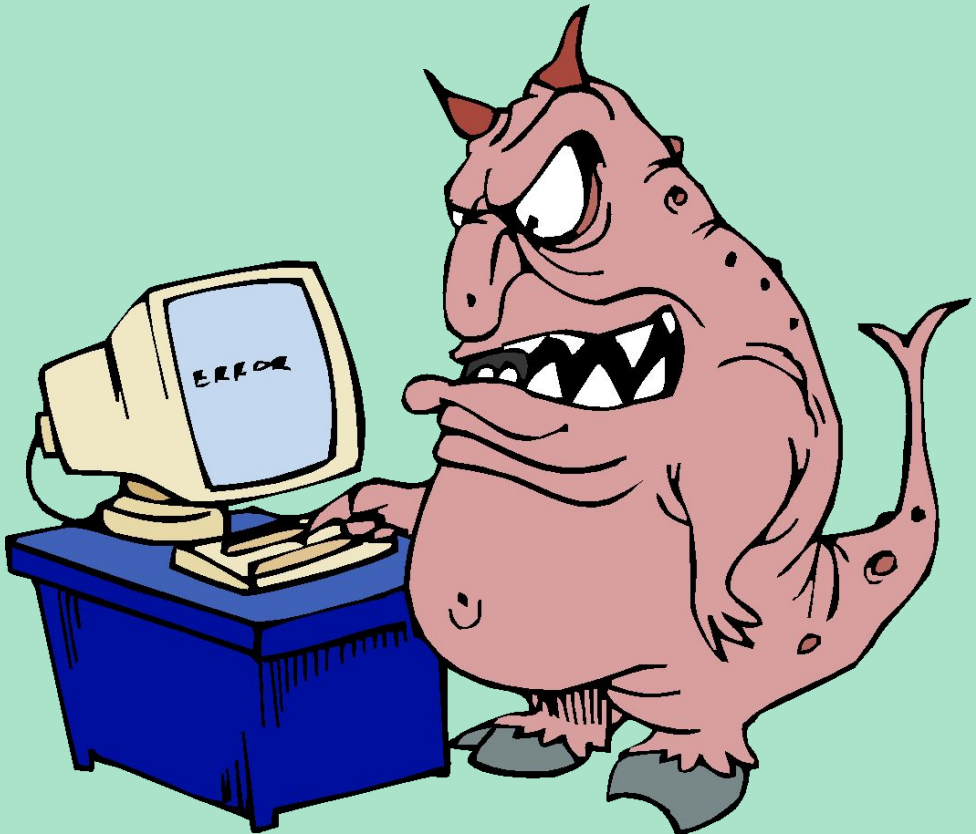
Существует большое количество сочетаний, например ***файлово-загрузочные вирусы***, заражающие как файлы, так и загрузочные секторы дисков. Такие вирусы, как правило, имеют довольно сложный алгоритм работы, часто применяют оригинальные методы проникновения в систему, используют «стелс» и полиморфик-технологии. Другой пример такого сочетания – ***сетевой макровирус***, который не только заражает редактируемые документы, но и рассылают свои копии по электронной почте.

Заражаемая **операционная система** является вторым уровнем деления вирусов на классы. Каждый файловый или сетевой вирус заражает файлы какой-либо одной или нескольких ОС.



Среди **особенностей алгоритма работы** вирусов выделяются следующие:

- ***резидентность***;
- ***использование «стелс»-алгоритмов***;
- ***самошифрование и полиморфичность***;
- ***использование нестандартных приёмов***.



Резидентный вирус

при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращения ОС к объектам заражения и внедряется в них. Эти вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки ОС.

Использование **«стелс»-алгоритмов** позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространённым «стелс»-алгоритмом является перехват запросов ОС на чтение-запись заражённых объектов и затем «стелс»-вирусы либо временно лечат их, либо подставляют вместо себя незаражённые участки информации.

Самошифрование и полиморфичность используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру обнаружения вируса.

Полиморфик-вирусы достаточно трудно поддаются обнаружению; они не имеют сигнатур, т.е. не содержат ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфик-вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

По **диструктивным** возможностям вирусы можно разделить на:
- ***безвредные***, т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);
- ***неопасные***, влияние которых ограничивается уменьшением свободной памяти на диске и графическим, звуковым и прочими эффектами;
- ***опасные вирусы***, которые могут привести к серьёзным сбоям в работе компьютера;
- ***очень опасные*** – в алгоритм их работы заведомо заложены процедуры, которые могут вызвать потерю программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти, и даже, как гласит одна из непроверенных компьютерных легенд, способствовать быстрому износу движущихся частей механизма – вводить в резонанс и разрушать головки некоторых типов винчестеров.

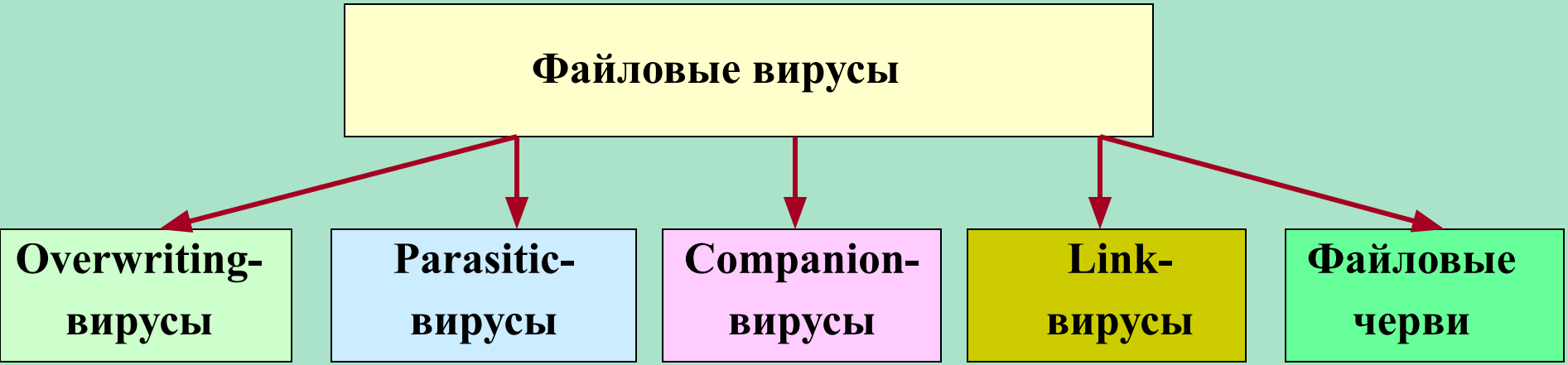
Файловые вирусы

К данной группе относятся вирусы, которые при своем размножении тем или иным способом используют файловую систему какой-либо (или каких-либо) ОС.

Файловые вирусы могут внедряться практически во все исполняемые файлы всех популярных ОС. На сегодняшний день известны вирусы, поражающие все типы выполняемых объектов стандартной DOS: командные файлы (BAT), загружаемые драйверы (SYS, в том числе специальные файлы IO.SYS и MSDOS.SYS) и выполняемые двоичные файлы (EXE, COM). Существуют вирусы, поражающие исполняемые файлы других ОС - Windows 3.x, Windows 95/NT, OS/2, Macintosh, Unix, включая VxD-драйверы Windows 3.x и Windows 95.

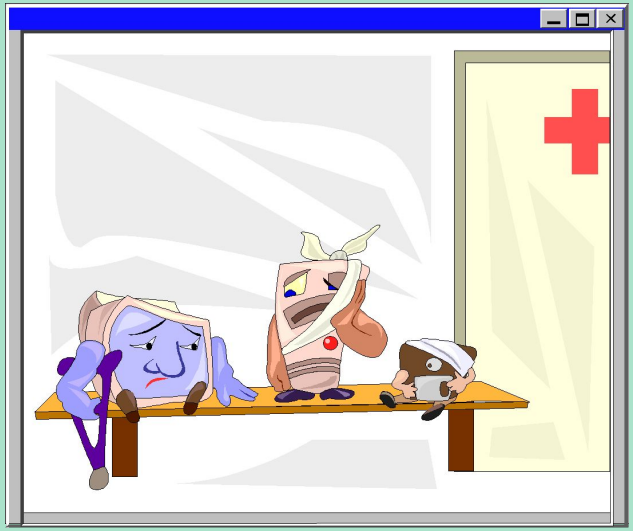
Файловые вирусы

По способу заражения файлов вирусы делятся на:



Overwriting-вирусы

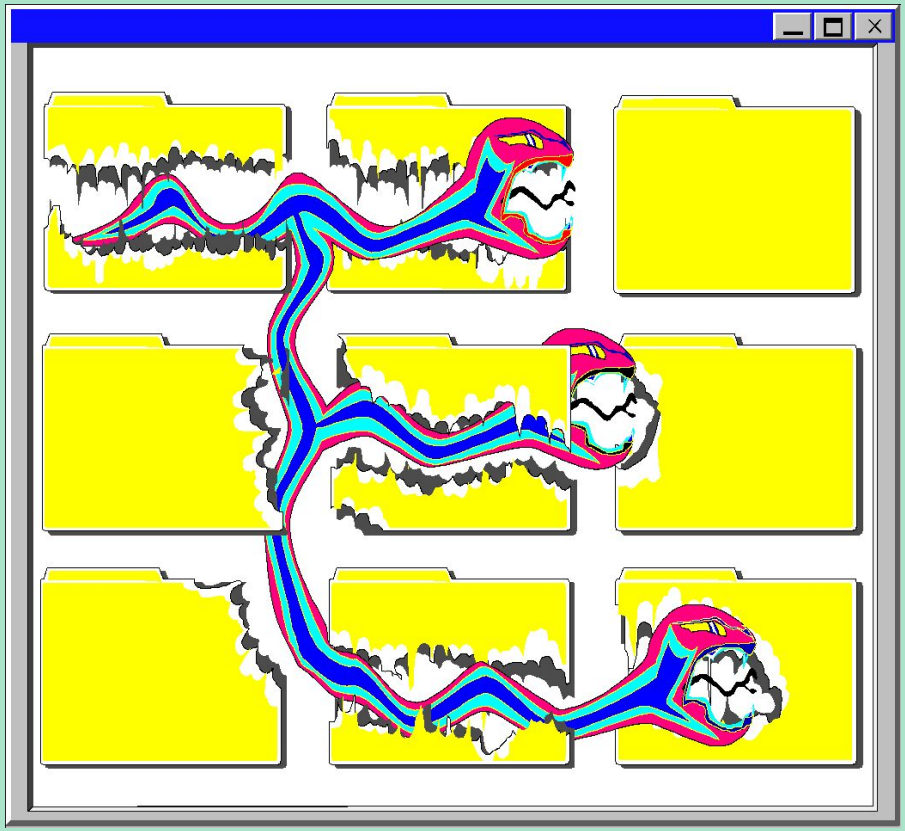
Данный метод заражения является наиболее простым : вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое. Естественно, что при этом файл перестает работать и не восстанавливается. Такие вирусы очень быстро обнаруживают себя, так как ОС и приложения довольно быстро перестают работать. Не известно ни одного случая, когда подобного типа вирусы были бы обнаружены "в живом виде" и стали причиной эпидемии.



К разновидности overwriting-вирусов относятся вирусы, записывающиеся вместо DOS-заголовка NewEXE-файлов. Основная часть файла при этом остается без изменений и продолжает нормально работать в соответствующе ОС, однако DOS-заголовок оказывается испорченным.

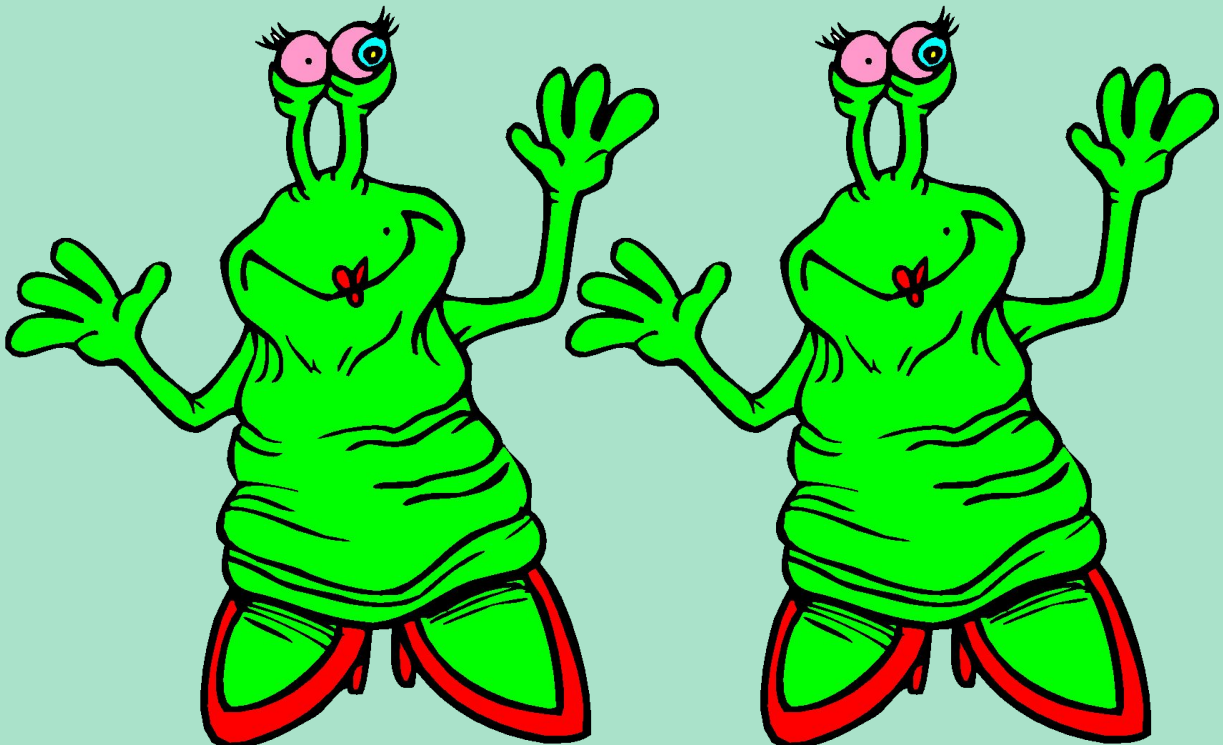
Parasitic-вирусы

К паразитическим относятся все файловые вирусы, которые при распространении своих копий обязательно изменяют содержимое файлов, оставляя сам файлы при этом полностью или частично работоспособными. Основными типами таких вирусов являются вирусы, записывающиеся в начало файлов (*prepending*), в конец файлов (*appending*) и в середину файлов (*inserting*). В свою очередь, внедрение вирусов в середину файлов происходит различнь ми методами - путем переноса части файла в его конец или внедрения в заведомо неиспользуемые данные файла (*cavity-вирусы*).



Companion-вирусы

К категории компаньон-вирусов относятся вирусы, не изменяющие заражаемых файлов. Алгоритм работы этих вирусов состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т. е. вирус.



Link-вирусы

Link-вирусы, как и компаньон-вирусы, не изменяют физического содержимого файлов, однако при запуске зараженного файла заставляют ОС выполни свой код. Этой цели они достигают модификацией необходимых полей файловой системы.

На сегодняшний день известен единственный тип link-вирусов - вирус семейства ***Dir_II***. При заражении системы они записывают свое тело в последний кластер логического диска. При заражении файла вирусы корректируют лишь номер первого кластера файла, расположенный в соответствующем секторе каталога. Новый начальный кластер файла будет указывать на кластер, содержащий тело вируса. Таким образом, при заражении файлов и длина и содержимое кластеров с этими файлами не изменяются, а на все зараженные файлы на одном логическом диске будет приходиться только одна копия вируса.

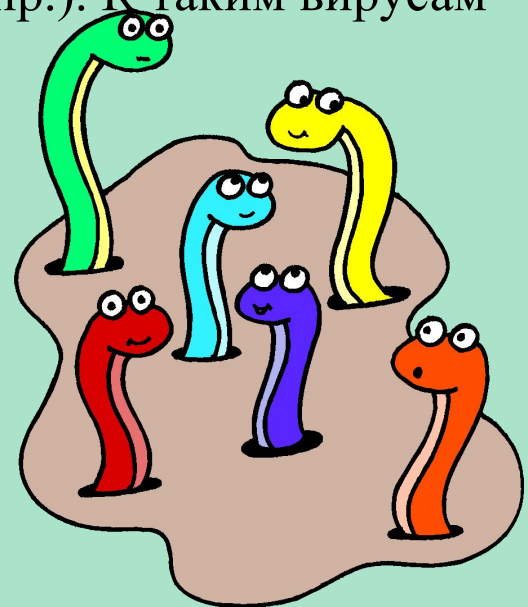
До заражения данные каталога хранят адрес первого кластера файла.
После заражения данные каталога указывают на вирус, т. е. при запуске файла управление получают не файлы, а вирус.

Файловые черви

Файловые черви (worms) являются в некотором смысле разновидностью компаньон-вирусов, но при этом никоим образом не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они всего лишь копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем. Иногда эти вирусы дают своим копиям "специальные" имена, чтобы подтолкнуть пользователя на запуск своей копии, например **INSTALL.EXE** или **WINSTART.BAT**.

Существуют вирусы-черви, использующие довольно необычные приемы, например, записывающие свои копии в архивы (ARJ, ZIP и пр.). К таким вирусам относятся "***ArjVirus***" и "***Winstart***".

Не следует путать файловые вирусы-черви с сетевыми червями. Первые используют только файловые функции какой-либо операционной системы, вторые же при своем размножении пользуются сетевыми протоколами.



Алгоритм работы файлового вируса

Получив управление, вирус совершает следующие действия: (приводим список наиболее общих действий вируса при его выполнении; для конкретного вируса список может быть дополнен, пункты могут поменяться местами и значительно расшириться):

- резидентный вирус проверяет оперативную память на наличие своей копии и инфицирует память компьютера, если копия вируса не найдена; резидентный вирус ищет незараженные файлы в текущем и (или) корневом каталогах, в каталогах, отмеченных командой PATH, сканирует дерево каталогов логических дисков, а затем заражает обнаруженные файлы;

Алгоритм работы файлового вируса

Получив управление, вирус совершает следующие действия:

- выполняет, если они есть, дополнительные функции: деструктивные действия, графические или звуковые эффекты и т. д. (дополнительные функции резидентного вируса могут вызываться спустя некоторое время после активизации в зависимости от текущего времени, конфигурации системы, внутренних счетчиков вируса или других условий; в этом случае вирус при активизации обрабатывает состояние системных часов, устанавливает свои счетчики и т. д.);

Алгоритм работы файлового вируса

Получив управление, вирус совершает следующие действия:

- возвращает управление основной программе (если она есть). Паразитические вирусы при этом либо восстанавливают программу (но не файл) в исходном виде (например, у COM-программы восстанавливается несколько первых байтов, у EXE-программы вычисляется истинный стартовый адрес, драйвера восстанавливаются значения адресов программ стратегии и прерывания), либо лечат файл, выполняют его, а затем снова заражают. Компаньон-вирусы запускают на выполнение своего "хозяина", вирусы-черви и overwriting-вирусы возвращают управление DOS.

Загрузочные вирусы

Загрузочные вирусы заражают загрузочный (**boot**) сектор гибкого диска в **boot-сектор** или **Master Boot Record** (MBR) винчестера. Принцип действия загрузочных вирусов основан на алгоритмах запуска ОС при включении или перезагрузке компьютера: после необходимых тестов установленного оборудования (памяти, дисков и т. д.) программа системной загрузки считывает первый физический сектор загрузочного диска и передает управление на A:, C: или CD-ROM, в зависимости от параметров, установленных BIOS Setup.

Загрузочные вирусы

При заражении дисков загрузочные вирусы подставляют свой код вместо какой-либо программы, получающей управление при загрузке системы. Принцип заражения, таким образом, одинаков во всех описанных выше способах: вирус "заставляет" систему при ее перезапуске считать в память и отдать управление не оригинальному коду загрузчика, а коду вируса.

Загрузочные вирусы

Заражение дискет производится единственным известным способом: вирус записывает свой код вместо оригинального кода boot-сектора дискеты. Винчестер заражается тремя возможными способами: вирус записывается либо вместо кода MBR, либо вместо кода boot-сектора загрузочного диска (обычно диска C:), либо модифицирует адрес активного boot-сектора в Disk Partition Table, расположенный в MBR винчестера.

Алгоритм работы загрузочного вируса

Практически все загрузочные вирусы резидентны. Они внедряются в память компьютера при загрузке с инфицированного диска. При этом системный загрузчик считывает содержимое первого сектора диска, с которого производится загрузка, помещает считанную информацию в память и передает на нее (т. е. на вирус) управление. После этого начинают выполняться инструкции вируса, который:

- как правило, уменьшает объем свободной памяти (слово по адресу 0040:0013), копирует в освободившееся место свой код и считывает с диска свое продолжение (если оно есть). В дальнейшем некоторые вирусы ждут загрузки DOS и восстанавливают это слово в его первоначальном значении. В результате они оказываются расположенными не за пределами DOS, а как отдельные блоки DOS-памяти;

Алгоритм работы загрузочного вируса

- перехватывает необходимые векторы прерываний (обычно - INT 13H), считывает в память оригинальный boot-сектор и передает на него управление.

В дальнейшем загрузочный вирус ведет себя так же, как резидентный файловый: перехватывает обращения ОС к дискам и инфицирует их, в зависимости от некоторых условий совершает деструктивные действия или вызывает звуковые или видеоэффекты.

Макровирусы

Макровирусы (*macro viruses*) являются программами на языках (макроязыках), встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т. д.). Для своего размножения такие вирусы используют возможности макроязыков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие.

Наибольшее распространение получили макровирусы для ***Microsoft Word, Excel и Office 97.***

Макровирусы

Для существования вирусов в конкретной системе необходимо наличие встроенного в систему макроязыка с возможностями:
1) привязки программы на макроязыке к конкретному файлу;
2) копирования макропрограмм из одного файла в другой;
3) получения управления макропрограммой без вмешательства пользователя (автоматические или стандартные макросы).

Данным условиям удовлетворяют редакторы ***Microsoft Word***, ***Office 97*** и ***AmiPro***, а также электронная таблица ***Excel***. Эти системы содержат себе макроязыки (**Word - Word Basic, Excel и Office 97 - Visual Basic**), а также:
1) макропрограммы привязаны к конкретному файлу (AmiPro) или находятся внутри файла (Word, Excel, Office 97);
2) макроязык позволяет копировать файлы (AmiPro) или перемещать как подпрограммы в служебные файлы системы и редактируемые файлы (Word, Excel, Office 97);
3) при работе с файлом при определенных условиях (открытие, закрытие и т. д.) вызываются макропрограммы (если таковые есть), которые определены специальным образом (AmiPro) или имеют стандартные имена (Word, Excel, Office 97).

Макровирусы

Эта особенность макроязыков предназначена для автоматической обработки данных в больших организациях или в глобальных сетях и позволяет организовать так называемый "автоматизированный документооборот". С другой стороны, возможности макроязыков таких систем позволяют вирусу переносить свой код в другие файлы и заражать их.

На сегодняшний день известны четыре системы, для которых существуют вирусы, - Microsoft Word, Excel, Office 97 и AmiPro. В этих системах вирус получают управление при открытии или закрытии зараженного файла, перехватывают стандартные файловые функции и затем заражают файлы, к которым каким-либо образом идет обращение. По аналогии с MS-DOS можно сказать, что большинство макровирусов являются резидентными: они активны не только в момент открытия/закрытия файла, но до тех пор, пока активен сам редактор.

Макровирусы

Макровирусы, поражающие файлы Word, Excel или Office 97, как правило, пользуются одним из трех приемов: в вирусе либо присутствует автомакрос (автофункция), либо переопределен один из стандартных системных макросов (ассоциированный с каким-либо пунктом меню), либо макрос вируса вызывается автоматически при нажатии на какую-либо клавишу или комбинацию клавиш. Существуют также полувирусы, которые не используют всех этих приемов и размножаются, только когда пользователь самостоятельно запускает их на выполнение.

Таким образом, если документ заражен, при его открытии Word вызывает зараженный автоматический макрос AutoOpen (или AutoClose при закрытии документа) и запускает код вируса, если это не запрещено системной переменной DisableAutoMacros. Если вирус содержит макросы со стандартными именами, они получают управление при вызове соответствующего пункта меню (File/Open, File/Close, File/SaveAs). Если же переопределен какой-либо символ клавиатуры, то вирус активизируется только после нажатия на соответствующую клавишу.

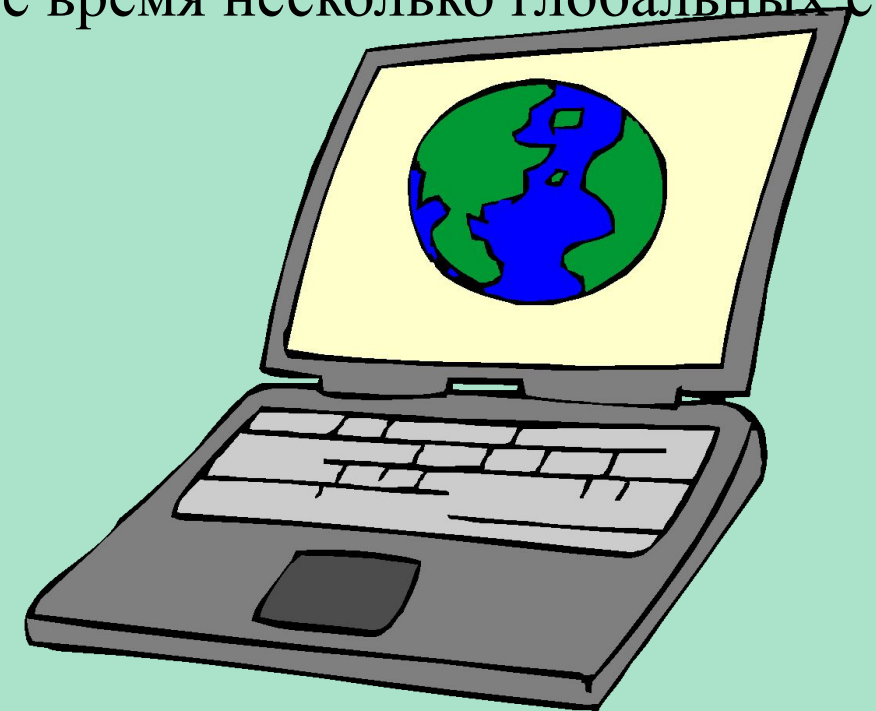
Сетевые вирусы

К сетевым относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. "Полноценные" сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свои код на удаленном компьютере или, по крайней мере, "подтолкнуть" пользователя к запуску зараженного файла.

Бытует ошибочное мнение, что сетевым является любой вирус, распространяющийся в компьютерной сети. Но в таком случае практически все вирусы были бы сетевыми, даже наиболее примитивные из них: ведь самый обычный нерезидентный вирус при заражении файлов не разбирается, сетевой (удаленный) это диск или локальный. В результате такой вирус способен заражать файлы в пределах сети, но отнести его к сетевым никак нельзя.

Сетевые вирусы

Наибольшую известность приобрели сетевые вирусы конца 80-х, их так же называют ***сетевыми червями*** (worms). К ним относятся вирус ***Моррuса***, вирусы ***Cristmas Tree*** и ***Wank Worm***. Для своего распространения они использовали ошибки и недокументированные функции глобальных сетей того времени. Вирусы передавали свои копии с сервера на сервер и запускали их на выполнение. Эпидемия вируса Морриса захватила в свое время несколько глобальных сетей в США.

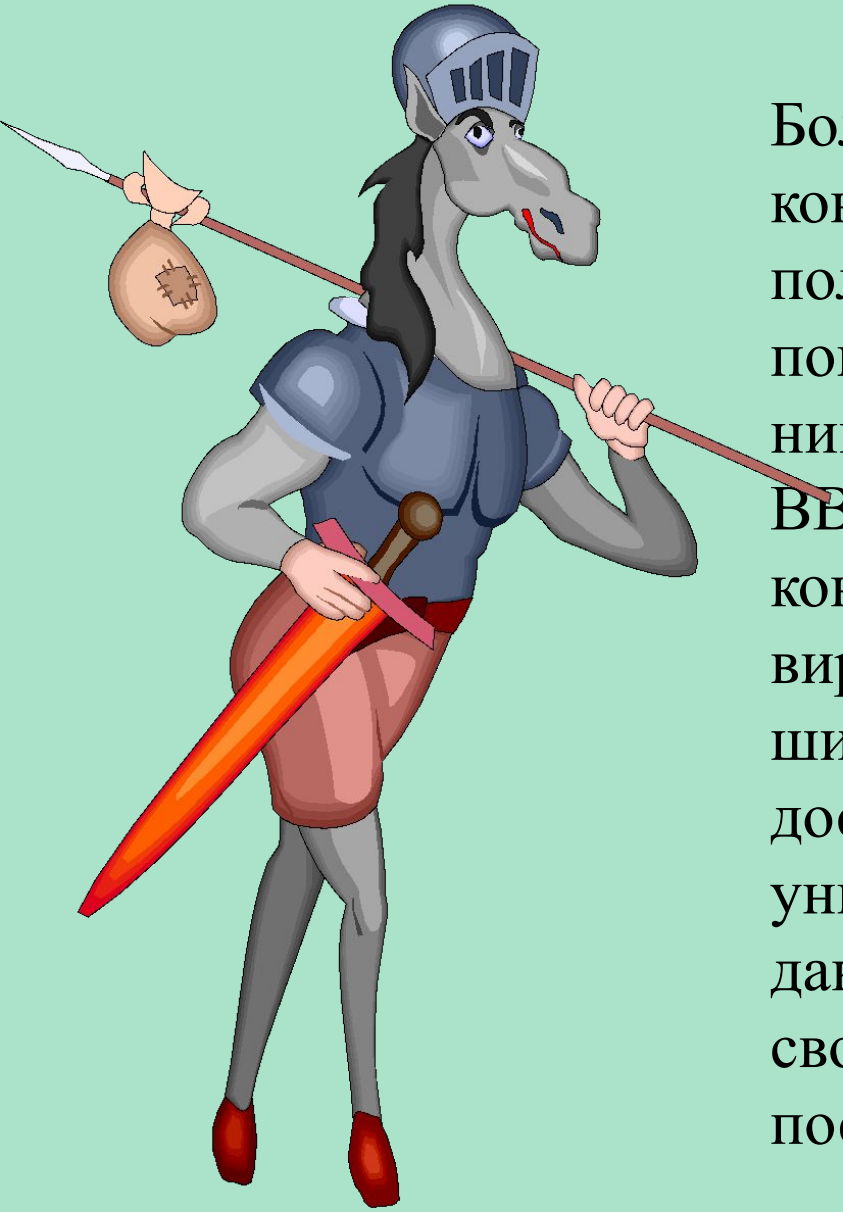


Прочие вредные программы

К вредным программам помимо вирусов относятся также "***троянские кони***" (логические бомбы), ***intended-вирусы***, ***конструкторы вирусов*** и ***полиморфик-генераторы***.

"**Троянский конь**" - это программа, наносящая какие-либо разрушительные действия, т. е. в зависимости от определенных условий или при каждом запуске уничтожающая информацию на дисках, "приводящая" систему (к зависанию) и т. п.

Прочие вредные программы



Большинство известных "троянских коней" подделываются под какие-либо полезные программы, новые версии популярных утилит или дополнения к ним. Очень часто они рассылаются по BBS-станциям или электронным конференциям. По сравнению с вирусами "троянские кони" не получают широкого распространения по достаточно простым причинам: они либо уничтожают себя вместе с остальными данными на диске, либо демаскируют свое присутствие и уничтожаются пострадавшим пользователем.

Прочие вредные программы

Следует отметить также "***злые шутки***" (hoax). К ним относятся программы, которые не причиняют компьютеру какого-либо прямого вреда, однако выводят сообщения о том, что такой вред уже причинен, либо будет причинен при каких-либо условиях, либо предупреждают пользователя о несуществующей опасности. К "злым шуткам" относятся, например, программы, которые "пугают" пользователя сообщениями о форматировании диска (хотя никакого форматирования на самом деле не происходит), определяют вирусы в незараженных файлах (как это делает широко известная программа ***ANTITIME***), выводят странные вирусоподобные сообщения (драйвер диска CMD640X от какого-то коммерческого пакета) и т. д. - варианты зависят от чувства юмора автора такой программы. Видимо, к "злым шуткам" относится также строка ***CHOLEEPA*** во втором секторе винчестеров фирмы Seagate. К этой же категории шуток можно отнести заведомо ложные сообщения о новых супервирусах. Такие сообщения периодически появляются в электронных конференциях и обычно вызывают среди пользователей панику.

"Стелс"-вирусы

"Стелс"-вирусы теми или иными способами скрывают факт своего присутствия в системе. Известны "стелс"-вирусы всех типов за исключением Windows-вирусов, файловые DOS-вирусы и даже макровирусы. Появление "стелс"-вирусов, заражающих файлы Windows, скорее всего дело времени.

Загрузочные "стелс"-вирусы для скрытия своего кода используют два основных способа. Первый из них заключается в том, что вирус перехватывает команды чтения зараженного сектора (INT 13h) и подставляет вместо него незараженный оригинал. Этот способ делает вирус невидимым для любой DOS-программы, включая антивирусы, неспособные "лечить" оперативную память компьютера. Возможен перехват команд чтения секторов на уровне более низком, чем INT 13h.

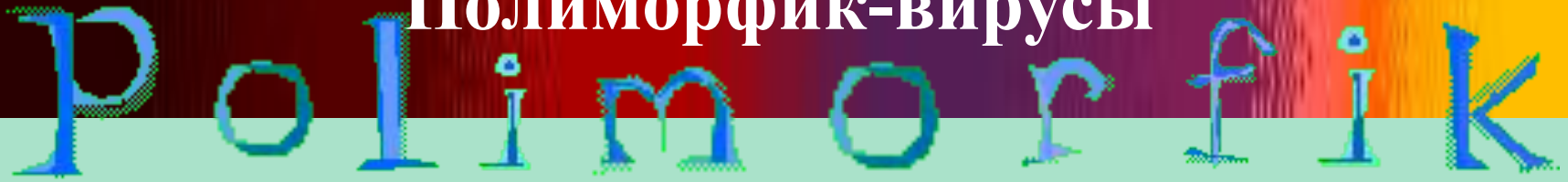
"Стелс"-вирусы

Второй способ направлен против антивирусов, поддерживающих команды прямого чтения секторов через порты контроллера диска. Такие вирусы при запуске любой программы (включая антивирус) восстанавливают зараженные сектора, а после окончания ее работы снова заражают диск. Поскольку для этого вирусу приходится перехватывать запуск и окончание работы программ, то он должен перехватывать также DOS-прерывание INT 21h.

"Стелс"-вирусы

Большинство файловых "стелс"-вирусов использует те же приемы, что приведены выше: они либо перехватывают DOS-вызовы обращения к файлам (INT21h), либо временно лечат файл при его открытии и заражают при закрытии. Так же как и для загрузочных вирусов, существуют файловые вирусы, использующие для своих "стелс"-функций перехват прерываний более низкого уровня - вызовы драйверов DOS, INT 25h и даже INT 13h. Полноценные файловые "стелс"-вирусы, использующие первый способ скрытия своего кода, в большинстве своем достаточно громоздки, поскольку им приходится перехватывать большое количество DOS-функций работы с файлами: открытие-закрытие, чтение-запись, поиск, запуск, переименование и т.д., причем необходимо поддерживать оба варианта некоторых вызовов (FCB/ASCII), а с появлением Windows 95/NT необходимо также обрабатывать третий вариант - функции работы с длинными именами файлов.

Полиморфик-вирусы



Полиморфик-вирусами являются те, обнаружение которых невозможно , или крайне затруднительно осуществить при помощи так называемых вирусных масок - участков постоянного кода, специфичных для конкретного вируса.

Достигается это двумя основными способами - шифрованием основного кода вируса с непостоянным ключом и случайным набором команд расшифровщика или изменением самого выполняемого кода вируса. Существуют также другие, достаточно экзотические примеры полиморфизма - DOS-вирус Bomber, например, не зашифрован, однако последовательность команд, которая передает управление коду вируса, является полностью полиморфной.

Полиморфизм различной степени сложности встречается в вирусах всех типов - от загрузочных и файловых DOS-вирусов до Windows-вирусов и даже макровирусов.

Контрольные вопросы:

1. На сколько классов подразделяются вирусы?

2. По каким основным признакам подразделяются вирусы?

3. Что из себя представляют макровирусы?

Методы обнаружения и удаления компьютерных вирусов

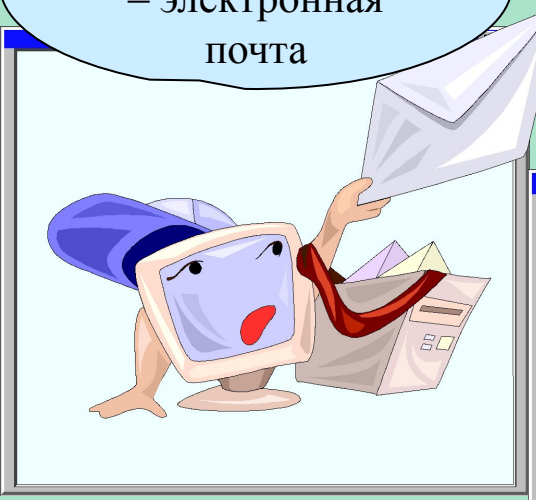
Профилактика заражения компьютера

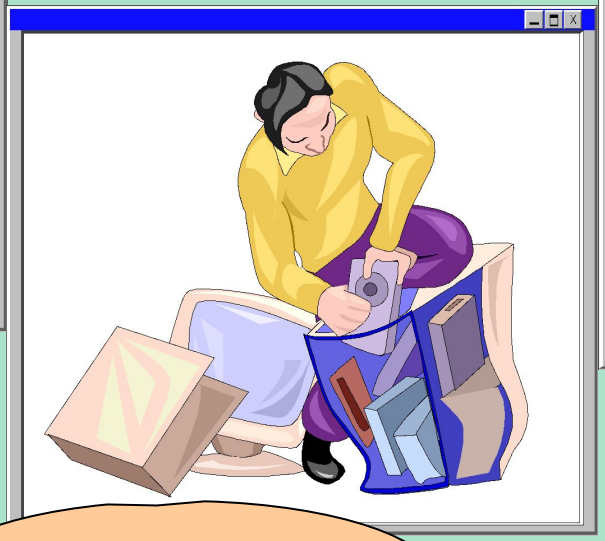
Одним из основных методов борьбы с вирусами является, как и в медицине, своевременная профилактика.

Компьютерная профилактика предполагает соблюдение некоторых правил, позволяющих значительно снизить вероятность заражения вирусом и потери данных. Поэтому, чтобы определить эти основные правила компьютерной гигиены, необходимо выяснить пути проникновения вируса в компьютер и компьютерные сети.

Откуда берутся вирусы

Глобальные сети – электронная почта





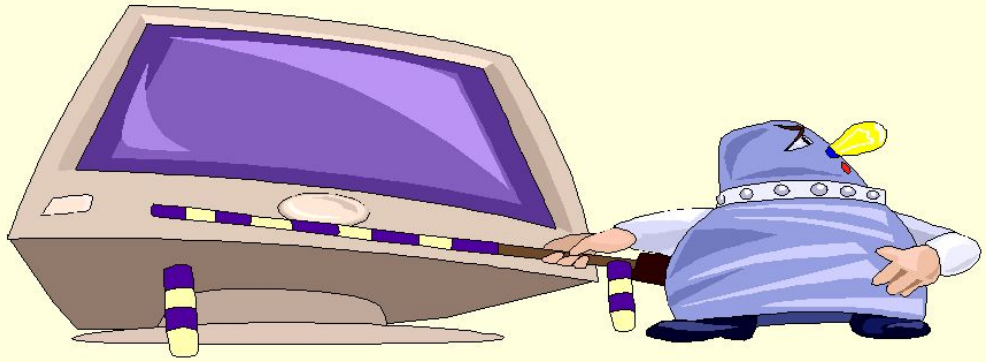
Локальные сети

Ремонтные службы

Персональный компьютер общего пользования

Пиратское программное обеспечение

Основные правила защиты

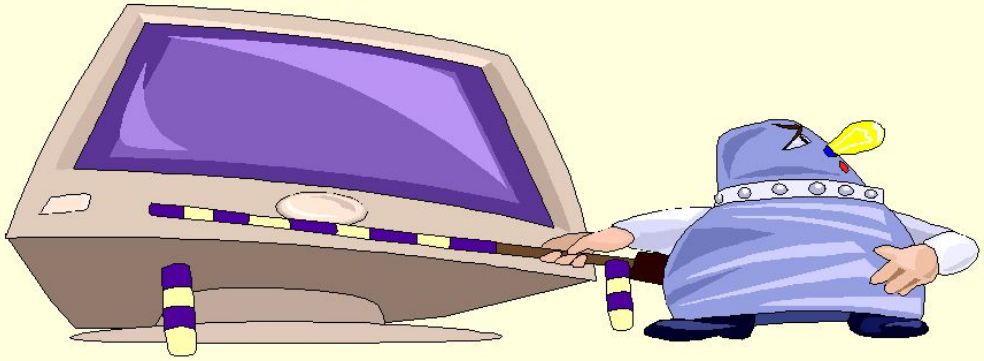


Правило первое: крайне осторожно относитесь к программам и документам Word/Excel 97, которые получаете из глобальных сетей. Перед тем как открыть документ обязательно проверьте его на наличие вирусов.

Правило второе: защита локальных сетей (ограничение прав пользователей, использование антивирусных программ, использование бездисковых рабочих станций.

Правило третье: используйте только хорошо зарекомендовавшие себя источники программ.

Основные правила защиты



Правило четвёртое: старайтесь не запускать не проверенные файлы. Перед запуском новых программ обязательно проверьте их одним или несколькими антивирусами.

Правило пятое: необходимо ограничивать круг лиц, допущенных к работе на конкретном компьютере. Как правило, наиболее часто подвержены заражению многопользовательские ПК.

Антивирусные программы

Наиболее эффективны в борьбе с компьютерными вирусами антивирусные программы. Однако сразу хотелось бы отметить, что не существует антивирусов, гарантирующих 100% защиту от вирусов.

Какой антивирус самый лучший? Любой, если на вашем компьютере вирусы не водятся и вы не пользуетесь вирусоопасными источниками информации.

Антивирусные программы

Если же вы любитель игрушек, ведёте активную переписку по электронной почте, то вам всё-таки следует использовать какой-либо антивирус. Какой именно – решайте сами, однако есть несколько позиций, по которым различные антивирусы можно сравнить между собой.

Качество антивирусной программы определяется по следующим позициям, приведённым в порядке убывания их важности:

Антивирусные программы

1. Надёжность и удобство работы

2. Качество обнаружения вирусов всех распространённых типов. Отсутствие «ложных срабатываний». Возможность лечения заражённых объектов.

2. Существование версий антивируса под все популярные платформы (операционные системы)

Антивирусные программы наиболее известные в России

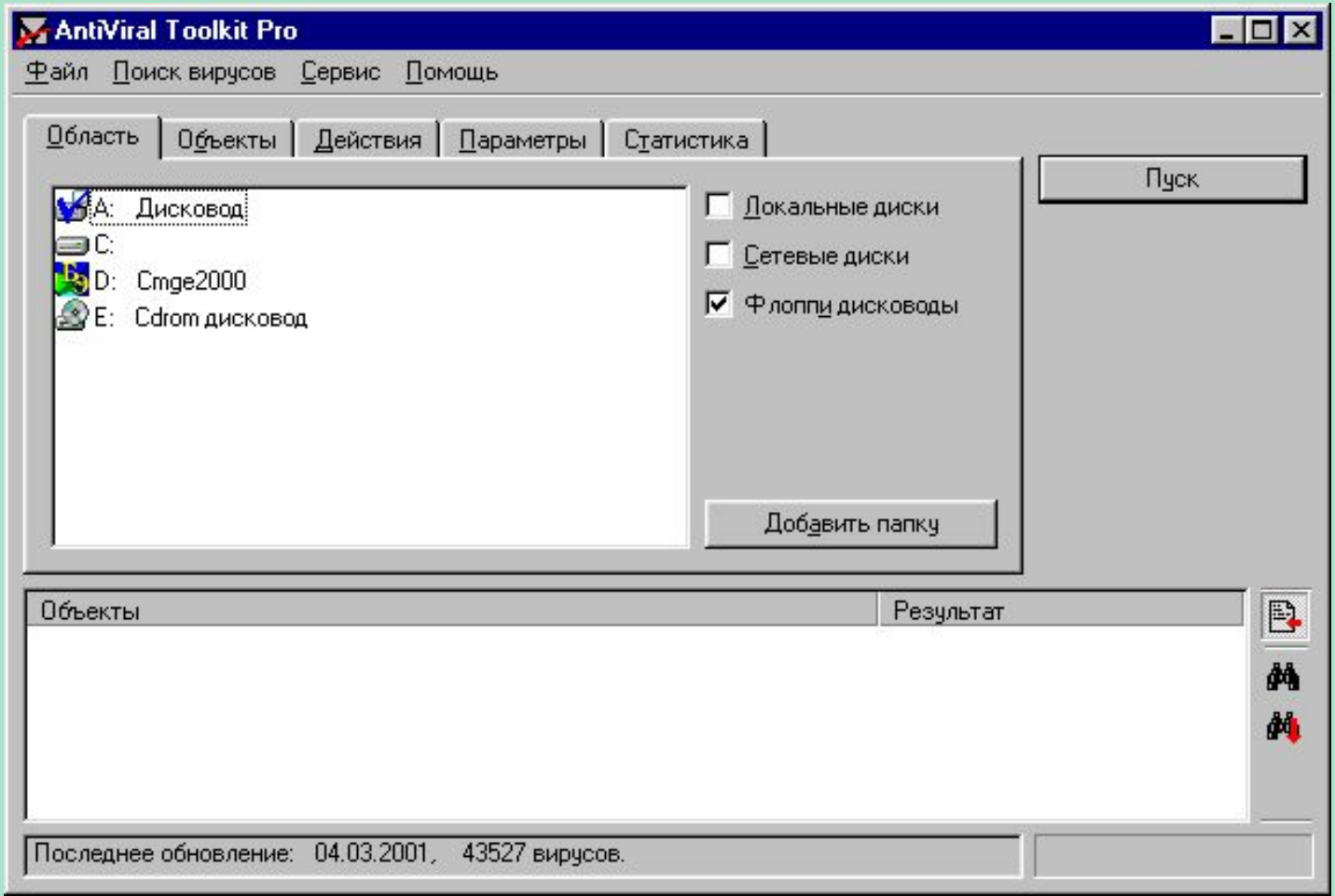
AIDSTEST – популярность можно объяснить лишь крайним консерватизмом отечественных пользователей. Из необходимых антивирусным программам качеств этой присущи лишь надёжность и неплохая скорость работы. AIDSTEST абсолютно бессилен против большинства современных вирусов.

AVP – один из самых надёжных и мощных антивирусов в мире .

DrWeb – неплохая программа, имеющая все необходимые функции поиска и лечения вирусов. К недостаткам можно отнести очень небольшую базу данных (всего около 3000 вирусов).

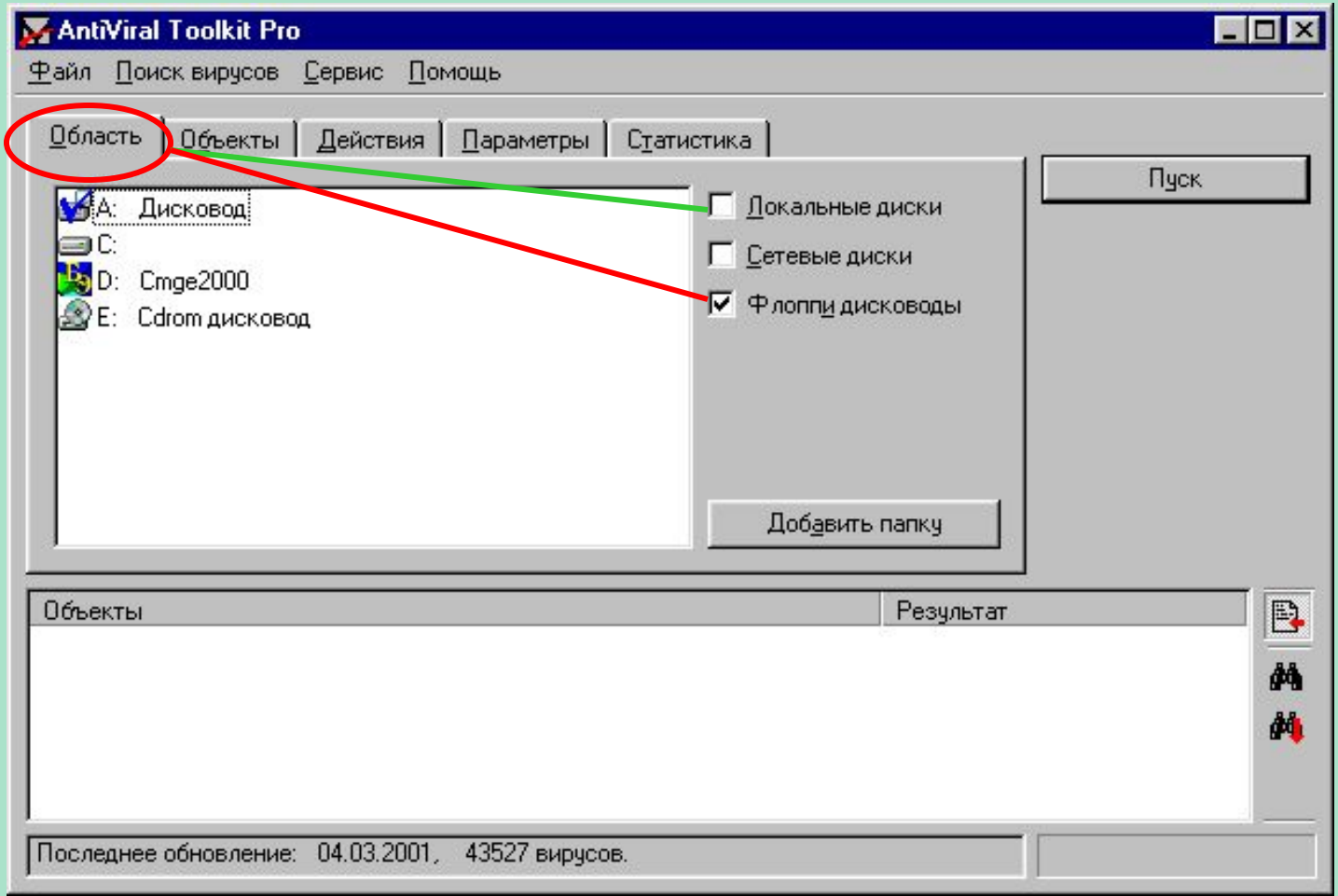
Проверка дисков на наличие вирусов антивирусной программой AVP

AntiViral Toolkit Pro (AVP) запускается Пуск – Программы - AntiViral Toolkit Pro – AVP сканер.
Появится окно программы.



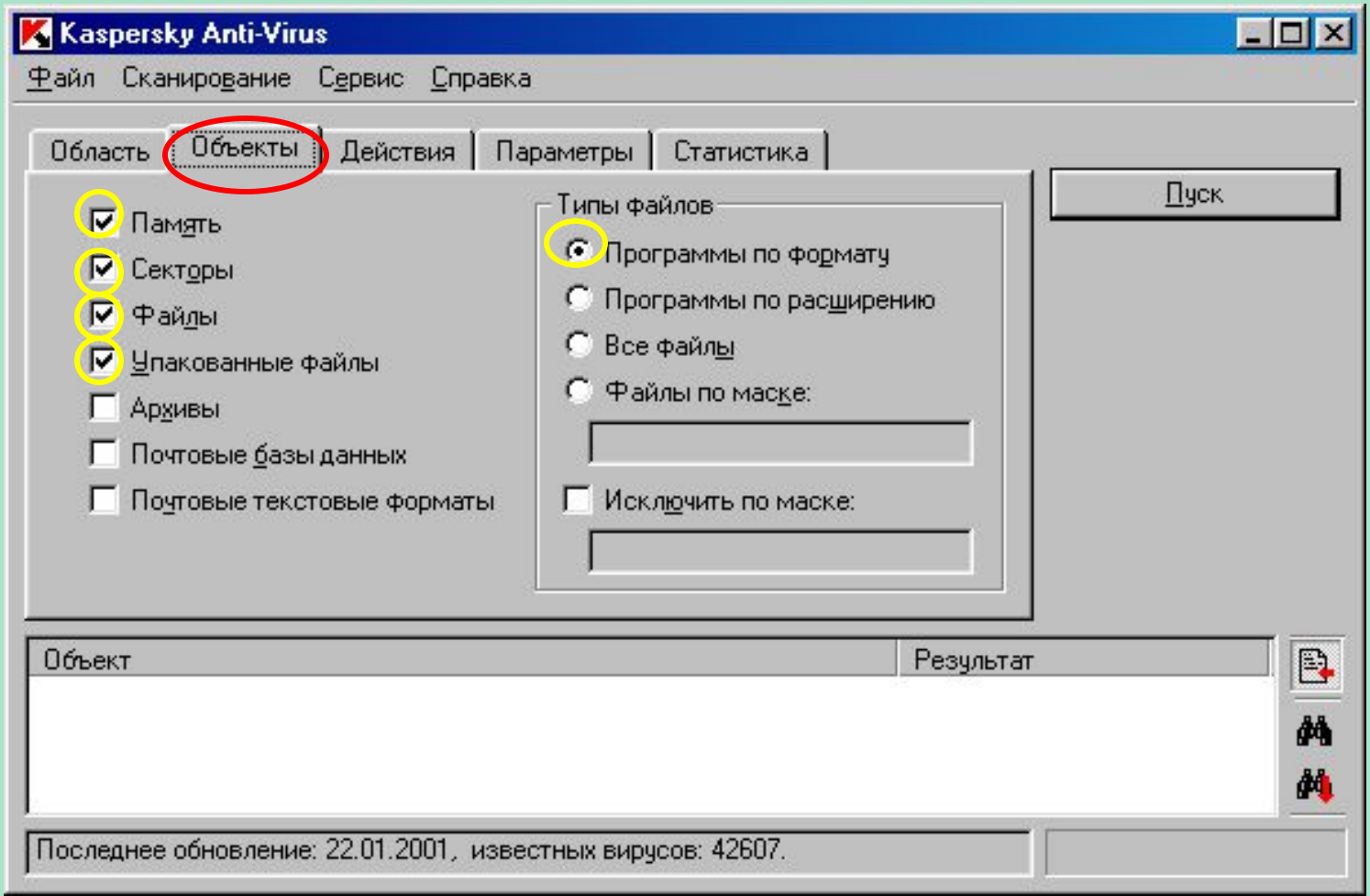
Проверка дисков на наличие вирусов антивирусной программой AVP

В закладке «**Область**» щёлкните по нужному для проверки диску



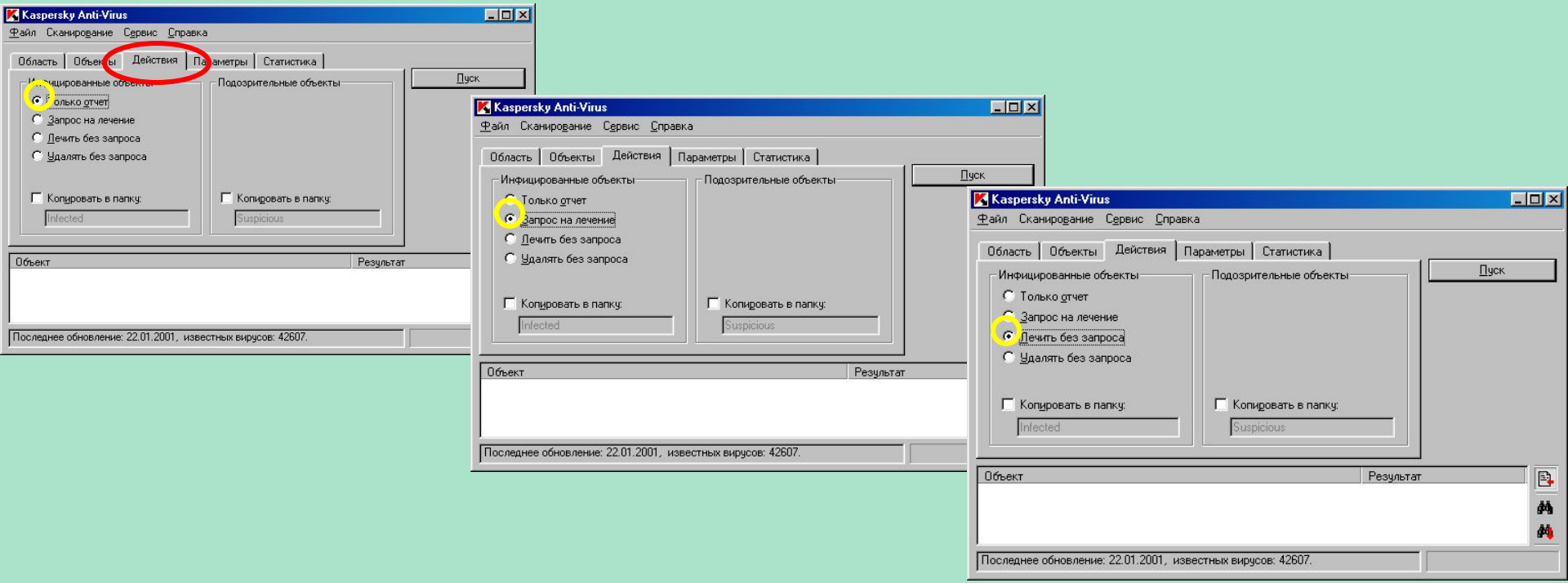
Проверка дисков на наличие вирусов антивирусной программой AVP

В закладке «**Объекты**» установите галочки в опциях «**Память**», «**Сектора**», «**Файлы**», «**Упакованные объекты**», «**Архивы**», в поле «**Тип файлов**» выберите «**Программы по формату**».



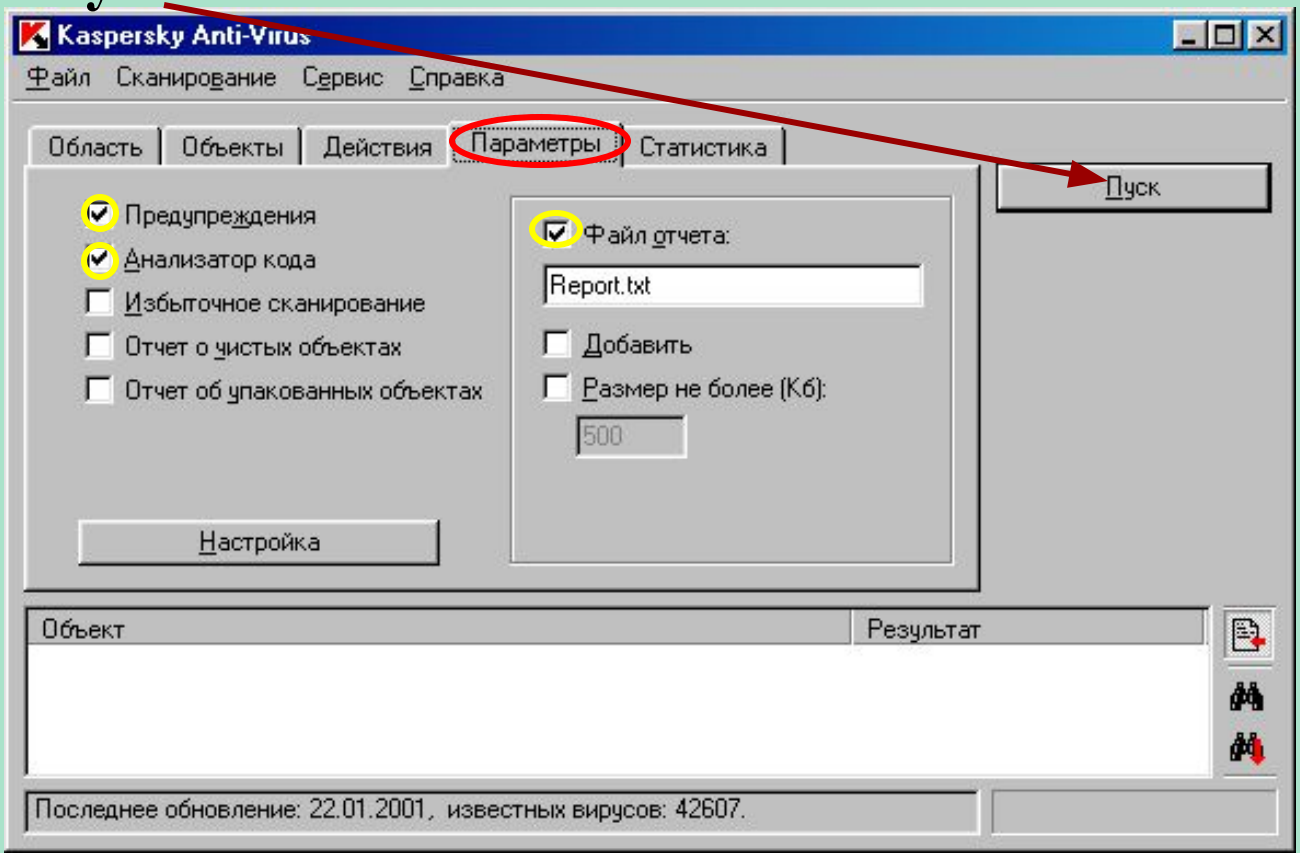
Проверка дисков на наличие вирусов антивирусной программой AVP

В закладке «**Действия**» выбрать ту опцию, которая необходима в данном конкретном случае.



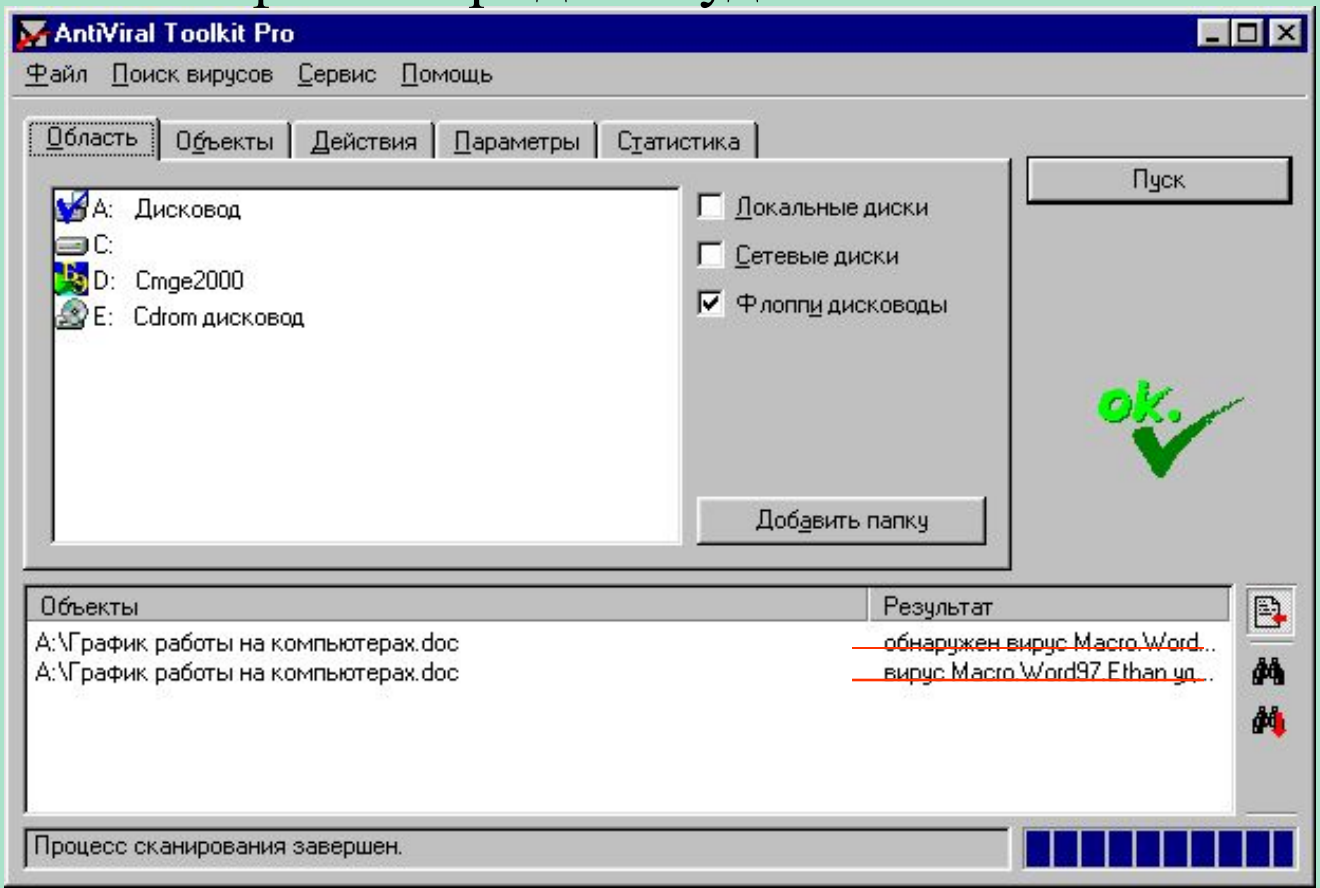
Проверка дисков на наличие вирусов антивирусной программой AVP

В закладке «**Параметры**» установите режимы «**Предупреждения**» и «**Анализатор кода**». Также отметьте опцию «**Файл отчёта**». Этот файл с результатами тестирования потом можно показать системному программисту. После всех установок щёлкните по кнопке «**Пуск**» в окне AVP.



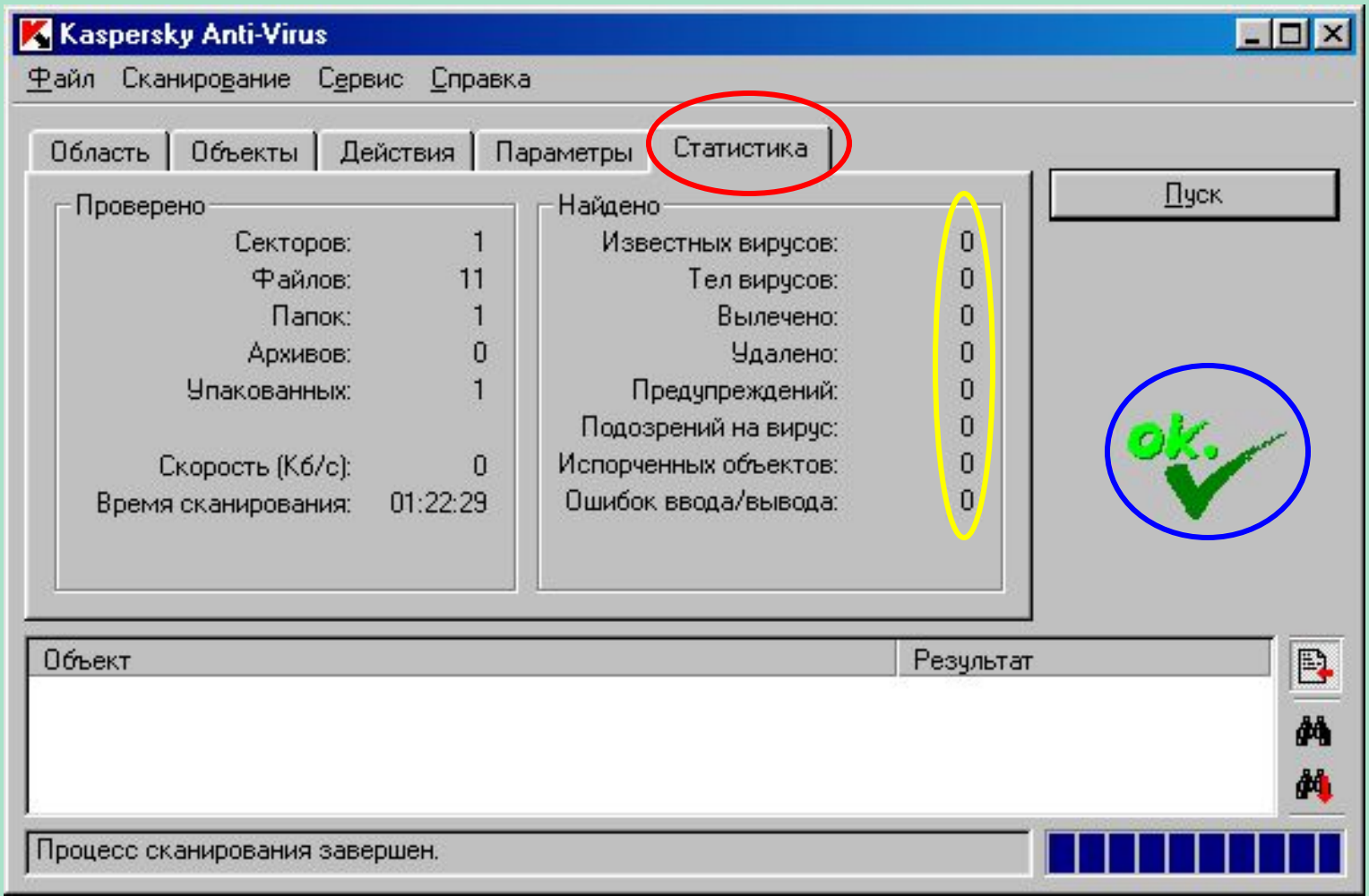
Проверка дисков на наличие вирусов антивирусной программой AVP

Если будут обнаружены заражённые файлы, попробуйте их лечить. К сожалению, лечение не всегда возможно, так как некоторые вирусы необратимо портят информацию. В этом случае инфицированные файлы придётся удалить.



Проверка дисков на наличие вирусов антивирусной программой AVP

Если вирусы не обнаружены на проверенных дисках, то появится **ОК** под кнопкой «Пуск». В закладке «**Статистика**» можно ознакомиться с результатами проверки.



Контрольные вопросы:

1. Каким требованиям должна отвечать антивирусная программа?

2. Перечислите основные правила защиты от вирусов

3. Какие антивирусные программы используются в России?

4. Откуда берутся вирусы?

Удачи

в борьбе с компьютерными вирусами!