Компьютерные Вирусы

- Общие сведение о вирусах
- Основные свойства вирусов
- Классификация вирусов
- Виды вирусов
- Лавинообразное заражение компьютеров вирусом
- Пути заражения вирусами
- Профилактика компьютерных вирусов
- Уничтожение компьютерных вирусов

Пути заражения вирусами

Распространяются вирусы в основном по глобальным и локальным сетям, а также переносятся от одной машины к другой на гибких или оптических дисках с инфицированными программами и документами.

Заражение компьютера происходит :

- При выполнении программы, зараженной вирусом;
- При работе с зараженными макровирусами документами, созданными в приложениях Пакета MS Office;
- При просмотре гипертекстовых документах в Интернете, содержавшие макровирусы;
- При просмотре вложений, прошедших с сообщениями электронной почты, которые содержат инфицированные программы или документы;
- При загрузке операционной системы с зараженного системного диска;
- При установке на компьютере уже зараженной операционной системы.

ДАЛЕЕ ➔

Заражение любого диска происходит при записи на этот диск зараженной программы Или документа, причем такая запись может быть выполнена без указания пользователя, как результат действия вируса. Заражение может произойти, даже если вставить гибкий диск в дисковод зараженного компьютера и прочитать его оглавление.

Итак, вирусы могут быть прятаться, в основном, в исполняемых файлах с расширениями

- .com, .exe – обычные программы;
- .bat – командные файлы, содержащие последовательности команд операционной системе;
- .vbs – файлы программы на языке Visual Basic for Application;
- .scr – файлы программ хранителей экрана;
- .dll, .lib, .obj –файлы библиотек;

ДАЛЕЕ ➔

А также в файлах документов с расширением :

- .doc – документ MS Word;
- .xls – документы MS Excel;
- .mdb – документы MS Access;
- .ppt – документы MS Power Point;
- .dot – шаблоны приложений пакета MS Office.

Следует отметить, что иногда файлы программ с целью с маскировки содержащихся в них вирусы снабжаются как бы двойным расширением типа .jpeg .vbs.
На самом деле любой файл может иметь только одно расширение. Отделенное от Фактического расширения .vbs большим количеством пробелов и не внушающее опасение <<как бы>> расширение .jpeg на самом деле (вместе с пробелами) является Частью имени. Так прятался знаменитый в свое время (в 200 году) вирус I Love You.

В НАЧАЛО !

Общие сведение о вирусах.

Компьютерными вирусами принято называть программу, основной целью Выполнения которых является нанесение различного вреда пользователям и компьютерам – начиная от выдачи простых и достаточно безобидных звуковых и визуальных эффектов до полного уничтожения информации, Хранящейся в компьютере, и вывода из строя аппаратных средств.

Первая “эпидемия” компьютерного вируса произошла в 1986 году, когда вирус Brain (англ. “мозг”) “заражал” дискеты персональных компьютеров. В настоящее время известно десятки тысяч вирусов, заражающих компьютеры и распространяющихся по компьютерным сетям.

Компьютерные вирусы являются программой, которые могут “размножаться” (самокопироваться) и незаметно для пользователя внедрять свой программный Код в файлы, документы, WEB-страницы всемирной паутины (Интернет)

В НАЧАЛО !

Основные свойства вирусов

Основными отличительными свойствами программ-вирусов является :

- Их относительно маленькие размеры ;
- Способность к самораспространению, или более точно к самовоспроизведению (размножению) ;
- Выполнение разрушительных или вредных для пользователя и компьютеров действий.

Небольшие размеры помогают вирусам прятаться среди массы полезных программ и документов и облегчают их передачу по сети и на дисках, то есть обеспечивают подходящие условия для их саморазмножения. Собственно саморазмножение вирусов Выполняется различными путями. В частности, это происходит следующим образом. Программа-вирус, попав каким-либо путем в оперативную память компьютера, перехватывает процессор и инициирует собственное выполнение. Во время этого выполнения, вирус ищет на дисковых устройствах программы или документы, в которых он может спрятаться, и при первой возможности переписывает их, копируя сам себя в эти программы или документы, в которые попал вирус, называются инфицированными или зараженными.

ДАЛЕЕ ➔

Во время выполнения зараженных программ или открытия зараженных документов вирус вновь перехватывает процессор, активизируется и заражает другие программы и документы.

Один единственный вирус способен заразить большое количество “здоровых” программ или документов, которые в свою очередь становятся источником “заразы”..

если обнаружится, что вирус поразил хотя бы одну программу или документ, наверняка зараженными окажутся и другие программы или документы, находящиеся на дисках той же машины, а также в машинах, связанных с нею одной сетью.

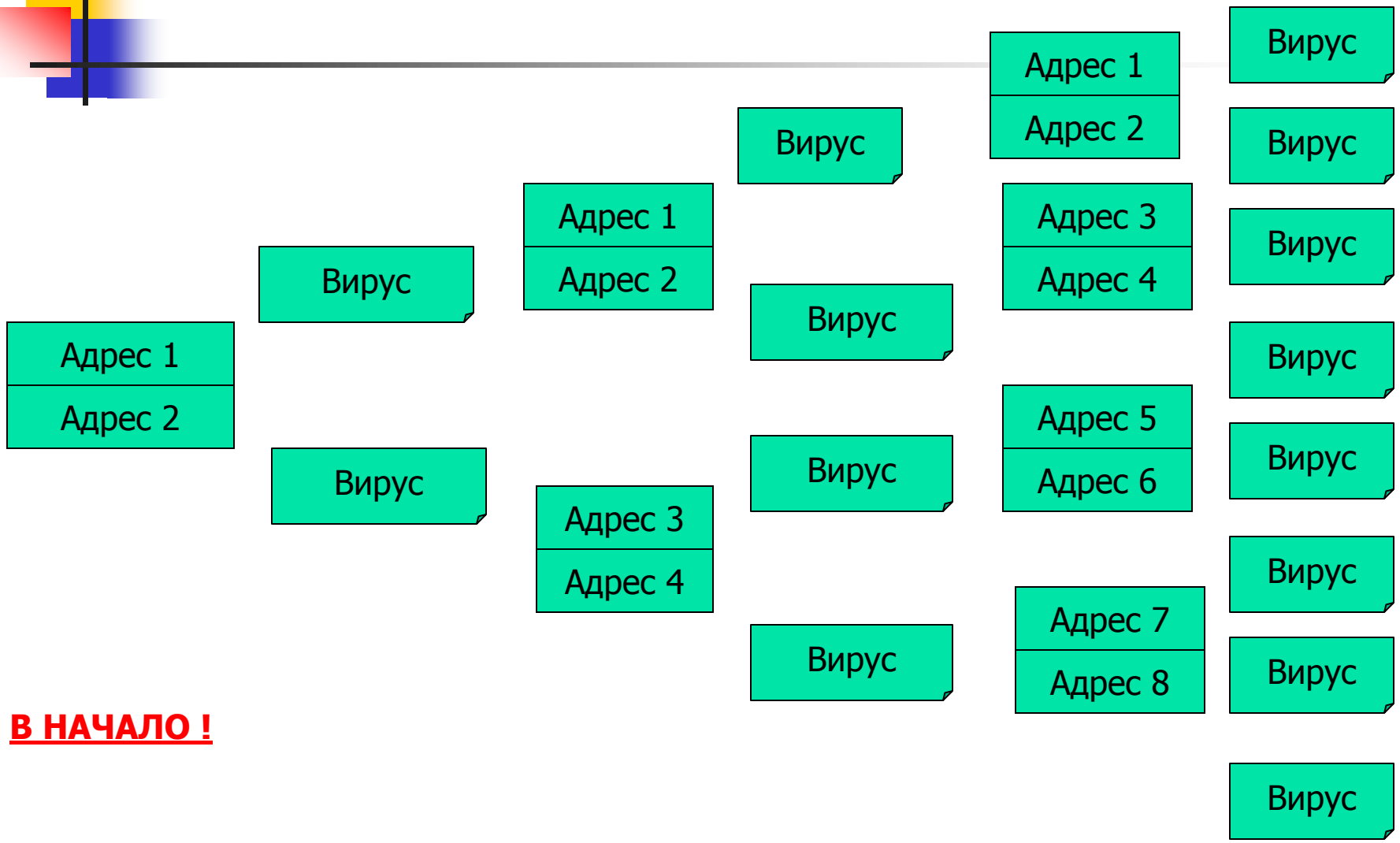
В НАЧАЛО !

Лавинообразное заражение компьютеров вирусом

Лавинообразная цепная реакция распространения почтовых вирусов базируется на том, что вирус после заражения компьютера начинает рассылать себя по всем адресам электронной почты, которые имеются в электронной адресной книге пользователя. Например, даже если в адресных книгах пользователей имеются только по два адреса, почтовый вирус, заразивший компьютер одного пользователя, через три рассылки поразит уже компьютеры восьми пользователей.

ДАЛЕЕ ➔

Лавинообразное заражение компьютеров вирусом



В НАЧАЛО !

Классификация вирусов.

Компьютерным вирусам, как и биологическим, характерны определенные стадии существования:

- Латентная стадия, в которой вирусом никаких действий не предпринимается;
- Инкубационная стадия, в которой основная задача вируса - создать как можно больше своих копий и внедрить их в среду обитания;
- Активная стадия, в которой вирус, продолжая размножаться, проявляется и выполняет свои деструктивные действия.

Классификация вирусов.

Различные вирусы значительно отличаются друг от друга и по наносимому вреду и по способам маскировки и размножению.

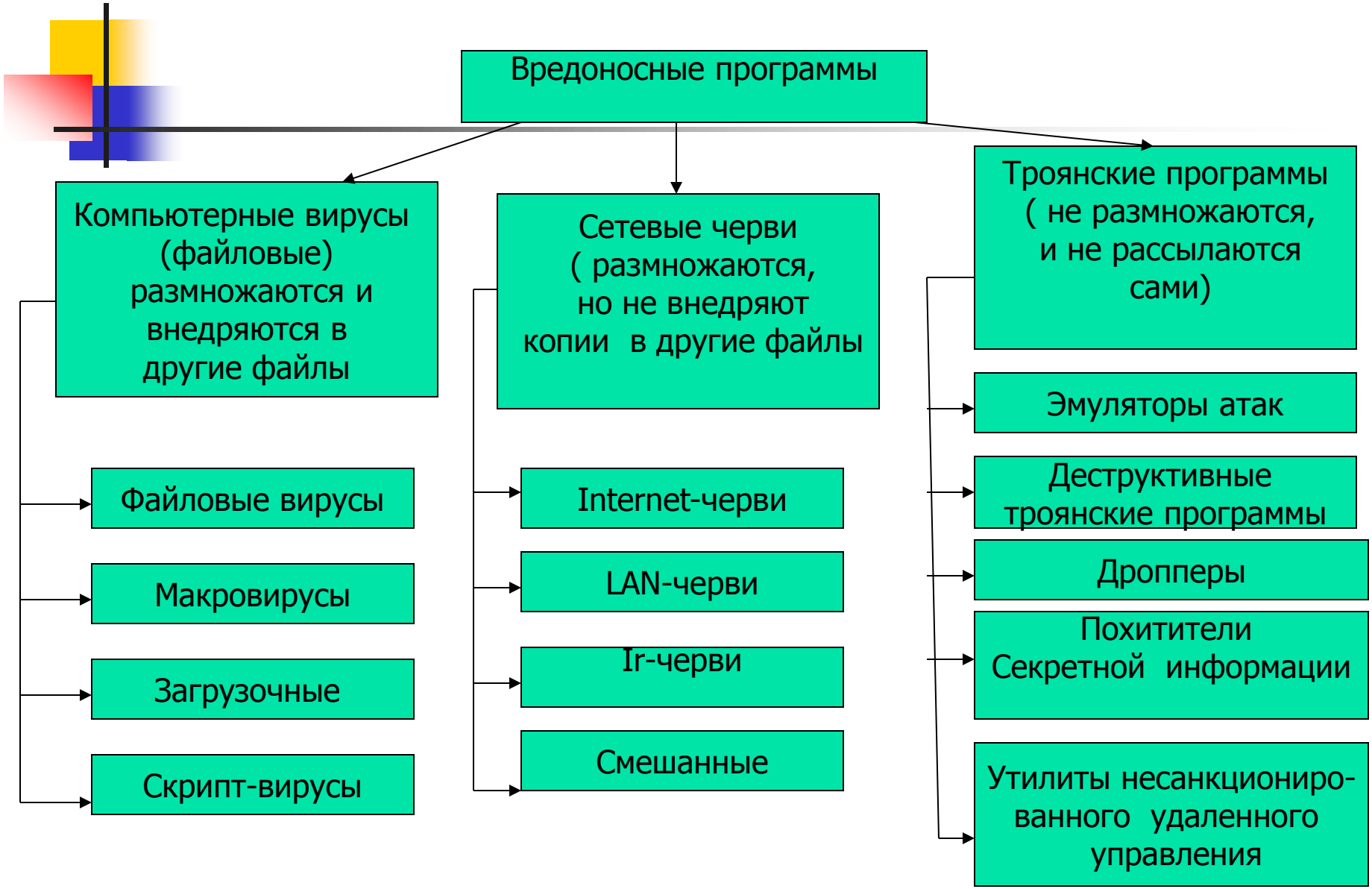
- Файловые вирусы, поражающие исполняемые файлы
- Загрузочные вирусы, поражающие загрузочные секторы дисков. Загрузочные сектора диска содержат специальную программу, которая осуществляет загрузку операционной системы. Поражение этой программы вирусом дает невозможной нормальной загрузки системы и блокирирует работу компьютера.
- Комбинированные вирусы, сочетающие в себе свойства файловых и загрузочных Вирусов.
- Макровирусы, Поражающие документы созданные в приложение пакета MS Office, В основном, в документах текстового редактора
- “Троянские” программы. Которые осуществляют негласный сбор различной , в основном, секретной информации о пользователях, Пароли т т.д.

ДАЛЕЕ ➔

- Полифорные вирусы (вирусы-мутанты), содержащие в себе алгоритмы шифровки-расшифровки, благодаря которым два экземпляра одного и того же вируса, Заразившие два разных файла, не имеют ни одной повторяющейся цепочки байт, что существенно затрудняет опознать таких вирусов специализированными антивирусными Программами.
- Стелс-вирусы (вирусы-невидимки), в которых реализованы алгоритмы, скрывающие присутствия вируса на зараженной машине. Их нельзя обнаружить, например, просто Просматривая файлы на диске с помощью файлового менеджера.

В НАЧАЛО !

Классификация вредоносных программ



Виды вирусов

Файлы вирусов чаше всего внедряются в исполняемые файлы, имеющие расширение .exe и .com, но могут внедрятся и объектные файлы , библиотеки, в командные Пакетные файлы, программные файлы на языках процедурного программирования. Файловые вирусы могут создавать файлы-двойники.

Загрузочные вирусы внедряются в загрузочный сектор дискеты (Boot-sector) или в Сектор , содержащий программу загрузки системного диска (master boot record). При Загрузки ОС с зараженного диска такой вирус изменяет программу начальной загрузки Либо модифицирует таблицу размещений файлов на диске, создавая трудности в работе компьютера или даже невозможный запуск операционной системы.

Файлово-загрузочные вирусы интегрируют возможности двух предыдущих групп. Макровирусы заражают и искажают текстовый файл (.Doc) и файлы электронных таблиц некоторых популярных редакторов. Комбинированные сетевые макровирусы не только заражают создаваемые документы, но и рассылают копии этих документов По электронной почте. (печально известный вирус “I love You”)

ДАЛЕЕ ➔

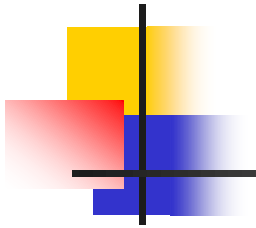
Сетевые черви используют для своего распространения команды и протоколы телеком-муникационных систем. Они подразделяются на Internet-черви(распространяющихся по Интернету), LAN-черви (распространяющихся по локальным системам), IRC-черви (распространяются через чаты)

В отдельную группу выделяются троянские программы, которые не размножаются И не рассылаются сами.

Троянские программы подразделяются на несколько видов которые маскируются под Полезные программы и выполняют деструктивные функции. Они могут обеспечить злоумышленнику скрытый несанкционированный доступ к информации на компьютере Пользователя и ее похищение. Такие программы иногда называют утилитами Несанкционированного удаленного управления.

Эмуляторы DDoS –атак (Distributed Denial of Service) приводят к атакам на веб-сервера При которых на веб-сервер из разных мест поступают большое количество пакетов, что приводит к отказам работы системы.

ДАЛЕЕ ➔



Дроппер (от английского drop – бросать) – программы, которая “сбрасывает” в систему вирус или другие вредоносные программы, при этом сама больше ничего не делает.

Скрип-вирус - это вирус, написанные на скрип-языках, таких как Visual Basic Script. Java Script и др.

В НАЧАЛО !

Профилактика компьютерных вирусов

1. Регулярно проводить профилактические работы по выявлению вирусов могут полностью исключить появление и распространение вирусов в ПК. Поэтому целесообразно включить эти работы в планы работы подразделений.

К основным профилактическим работам относятся :

- Ежедневная автоматическая проверка наличия вируса при включении ПК
- Регулярная комплексная проверка наличия вирусов во всех ПК
- Изучение информации по сообщениям в компьютерных журналах и газетах о новых вирусах
- Создание резервных копий программного продукта сразу же после приобретения
- Создание дискеты с наиболее важными программами.
- Тщательная проверка всех поступающих и купленных программ и баз данных

В НАЧАЛО !

Уничтожение компьютерных вирусов

Уничтожение вирусов выполняются администратором с привлечением других специалистов подразделения информатизации.

Если вирус поразил какие-либо программы, то уничтожение вируса выполняются путем уничтожения программы на винчестере либо на дискете. После уничтожения зараженной программы необходимо восстановить программу, используя резервную Копии программы.

Если вирус поразил файлы, то вирус уничтожается либо путем стирания этих файлов, Либо путем использования специальных лечащих программ. Использования лечащих Программ не дает полной гарантии восстановления файла. Поэтому после лечения Необходима проверка восстановления данного файла.

Лечащие программы используются лишь в тех случаях, когда отсутствует резервная копия зараженной программы либо файла с данными.

ДАЛЕЕ ➔

Антивирусные программы можно разделить на:

- Программы – детекторы;
- Программы-ревизоры;
- Программы-фильтры;
- Программы –доктора, или дезинфекторы, фаги;
- Программы-вакцины, или иммунизаторы.

Программы-детекторы

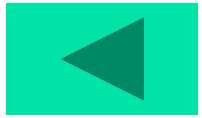
- Программы – детекторы осуществляют поиск компьютерных вирусов в памяти машины и при их обнаружении сообщают об этом. Детекторы могут искать как уже известные вирусы (ищут характерную для конкретного уже известного вируса последовательность байтов-сигнатуру вируса), так и произвольные вирусы (путем подсчета контрольных сумм для массива файла).

Программы-ревизоры

- Программы-ревизоры являются развитием детекторов, но выполняют более сложную работу. Они запоминают исходное состояние программ, каталогов, системных областей и периодически или по указанию пользователя сравнивают его с текущим. При сравнении проверяется длина файлов, дата их создания и модификации, контрольные суммы и байты циклического контроля и другие параметры. Ревизоры эффективнее детекторов.

Программы-фильтры

- Программы-фильтры обеспечивают выявление подозрительных, характерных для вирусов действий (коррекция исполняемых .exe и .com файлов, запись в загрузочные сектора дисков, изменение атрибутов файлов, прямая запись на диск по прямому адресу и т.д.) При обнаружении таких действий фильтры посылают пользователю запрос о подтверждении правомерности таких процедур.



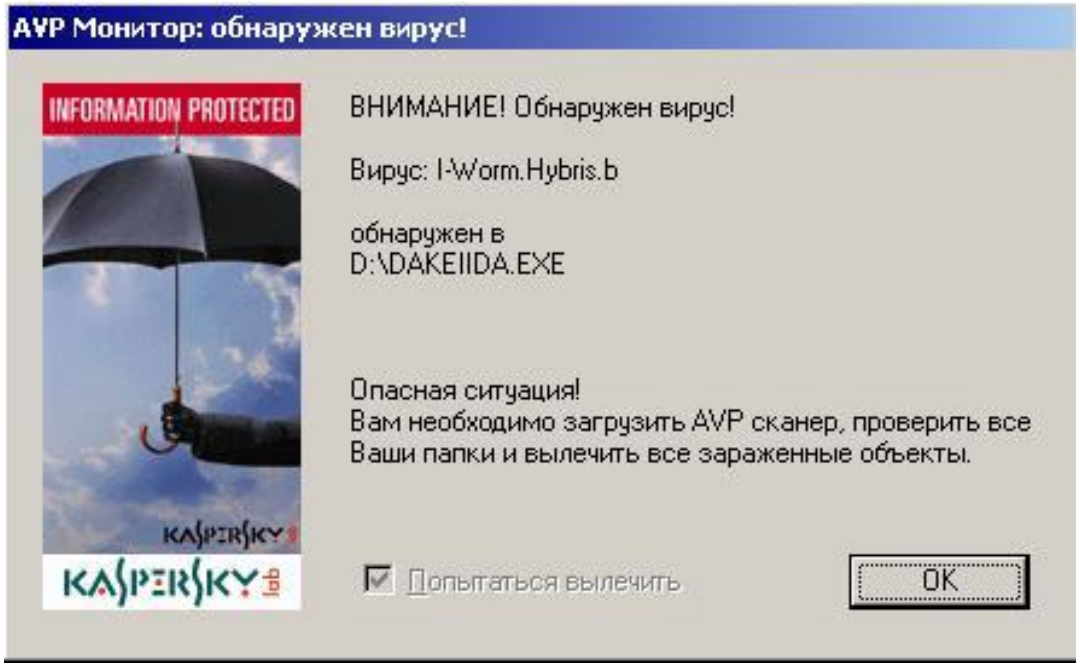
Программы - доктора

- Самые распространенные и популярные (например, Kaspersky Antyvirus, Doctor Web, Norton Antyvirus и т.д.), которые не только обслуживают, но и лечат зараженные вирусами файлы и загрузочные секторы дисков. Они сначала ищут вирусы в оперативной памяти и уничтожают их там (удаляют тело резидентного файла), а затем лечат файлы и диски. Многие программы-доктора являются полифагами и обновляются достаточно часто.

Программы-вакцины

- Применяются для предотвращения заражения файлов и дисков известными вирусами. Вакцины модифицируют файл или диск таким образом что он воспринимается программой-вирусом уже зараженным, и поэтому вирус не внедряется.

- Если вирус поразил таблицу FAT , то можно восстановить эту таблицу, используя пакет программы Norton Utilites, которая для восстановления использует вторую таблицу FAT, имеющуюся в ПК.
- Для восстановления зараженной загрузочной записи винчестера необходимо использовать специальную системную дискету, на которую записана загрузочная запись



В НАЧАЛО !