**Министерство образования и науки Украины**

**Криворожский естественно-научный лицей**

**Кафедра информационных технологий**

# Компьютерные вирусы и антивирусы

Научно-исследовательская работа

II курса физико-математического

факультета

Научный руководитель

Будник Наталья Григорьевна

учитель информатики

г. Кривой Рог

2007 г.**Содержание**

Введение

Раздел 1. Кто и почему пишет вирусы?

Раздел 2. Компьютерные вирусы, их свойства и классификация

2.1 Свойства компьютерных вирусов

2.2 Классификация вирусов

2.3 Загрузочные вирусы

2.4 Файловые вирусы

2.5 Загрузочно-файловые вирусы

2.6 Полиморфные вирусы

2.7 Стелс-вирусы

2.8 Троянские кони, программные закладки и сетевые черви

Раздел 3. Пути проникновения вирусов в компьютер и механизм распределения вирусных программ

3.1 Признаки появления вирусов

Раздел 4. Методы защиты от компьютерных вирусов

Раздел 5. Антивирусные программы

5.1 Doctor Web

5.2 Microsoft Antivirus

Заключение

Список литературы

##### Введение

Вряд ли стоит напоминать, что компьютеры стали настоящими помощниками человека и без них уже не может обойтись ни коммерческая фирма, ни государственная организация. Однако в связи с этим особенно обострилась проблема защиты информации.

Вирусы, получившие широкое распространение в компьютерной технике, взбудоражили весь мир. Многие пользователи компьютеров обеспокоены слухами о том, что с помощью компьютерных вирусов злоумышленники взламывают сети, грабят банки, крадут интеллектуальную собственность...

Сегодня массовое применение персональных компьютеров, к сожалению, оказалось связанным с появлением самовоспроизводящихся программ-вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации, поэтому темой моей научной работы есть «Компьютерные вирусы и антивирусы». Цель работы: Выяснить пути проникновения и влияние вирусов на работу компьютера и найти методы защиты от них. Предмет: методы защиты от компьютерных вирусов. Объект научной работы: Компьютерные вирусы и антивирусы. Исходя из темы, можно сформулировать следующие задачи:

1. Определить пути проникновения вирусов в компьютер;
2. Определить влияние компьютерных вирусов;
3. Ознакомиться с существующими методами защиты.

Все чаще в средствах массовой информации появляются сообщения о различного рода пиратских проделках компьютерных хулиганов, о появлении все более совершенных саморазмножающихся программ. Совсем недавно заражение вирусом текстовых файлов считалось абсурдом - сейчас этим уже никого не удивишь. Достаточно вспомнить появление "первой ласточки", наделавшей много шума - вируса WinWord. Concept, поражающего документы в формате текстового процессора Microsoft Word for Windows 6.0 и 7.0. Несмотря на принятые во многих странах законы о борьбе с компьютерными преступлениями и разработку специальных программных средств защиты от вирусов, количество новых программных вирусов постоянно растет. Это требует от пользователя персонального компьютера знаний о природе вирусов, способах заражения вирусами и защиты от них.

Хочется сразу заметить, что слишком уж бояться вирусов не стоит, особенно если компьютер приобретен совсем недавно, и много информации на жестком диске еще не накопилось. Вирус компьютер не взорвет. Ныне известен только один вирус (Win95.CIH), который способен испортить "железо" компьютера. Другие же могут лишь уничтожить информацию, не более того.

В литературе весьма настойчиво пропагандируется, что избавиться от вирусов можно лишь при помощи сложных (и дорогостоящих) антивирусных программ, и якобы только под их защитой вы можете чувствовать себя в полной безопасности. Это не совсем так - знакомство с особенностями строения и способами внедрения компьютерных вирусов поможет вовремя их обнаружить и локализовать, даже если под рукой не окажется подходящей антивирусной программы.

Раздел 1

Кто и почему пишет вирусы?

Кто же пишет вирусы? На мой взгляд, основную их массу создают студенты и школьники, которые только что изучили язык ассемблера, хотят попробовать свои силы, но не могут найти для них более достойного применения. Отраден тот факт, что значительная часть таких вирусов их авторами часто не распространяется, и вирусы через некоторое время «умирают» вместе с дискетами, на которых хранятся. Такие вирусы пишутся скорее всего только для самоутверждения.

Вторую группу составляют также молодые люди (чаще - студенты), которые еще не полностью овладели искусством программирования, но уже решили посвятить себя написанию и распространению вирусов. Единственная причина, толкающая подобных людей на написание вирусов, это комплекс неполноценности, который проявляет себя в компьютерном хулиганстве.

Из-под пера подобных «умельцев» часто выходят либо многочисленные модификации «классических» вирусов, либо вирусы крайне примитивные и с большим числом ошибок (такие вирусы я называю «студенческими»). Значительно облегчилась жизнь подобных вирусописателей после выхода конструкторов вирусов, при помощи которых можно создавать новые вирусы даже при минимальных знаниях об операционной системе и ассемблере, или даже вообще не имея об этом никакого представления. Их жизнь стала еще легче после появления макро-вирусов, поскольку вместо сложного языка Ассемблер для написания макро-вирусов достаточно изучить довольно простой Бейсик.

Став старше и опытнее, но так и не повзрослев, многие из подобных вирусописателей попадают в третью, наиболее опасную группу, которая создает и запускает в мир «профессиональные» вирусы. Эти очень тщательно продуманные и отлаженные программы создаются профессиональными, часто очень талантливыми программистами. Такие вирусы нередко используют достаточно оригинальные алгоритмы, недокументированные и мало кому известные способы проникновения в системные области данных. «Профессиональные» вирусы часто выполнены по технологии «стелс» и(или) являются полиморфик-вирусами, заражают не только файлы, но и загрузочные сектора дисков, а иногда и выполняемые файлы Windows и OS/2.

Довольно значительную часть в моей коллекции занимают «семейства» - группы из нескольких (иногда более десятка) вирусов. Представителей каждой их таких групп можно выделить по одной отличительной черте, которая называется «почерком»: в нескольких различных вирусах встречаются одни и те же алгоритмы и приемы программирования. Часто все или почти все представители семейства принадлежат одному автору, и иногда довольно забавно следить за «становлением пера» подобного художника - от почти «студенческих» попыток создать хоть что-нибудь, похожее на вирус, до вполне работоспособной реализации «профессионального» вируса.

По моему мнению, причина, заставляющая таких людей направлять свои способности на такую бессмысленную работу все та же - комплекс неполноценности, иногда сочетающийся с неуравновешенной психикой. Показателен тот факт, что подобное вирусописательство часто сочетается с другими пагубными пристрастиями. Так, весной 1997 года один из наиболее известных в мире авторов вирусов по кличке Talon (Австралия) скончался в возрасте 21 года от летальной дозы героина.

Несколько отдельно стоит четвертая группа авторов вирусов - «исследователи». Эта группа состоит из довольно сообразительных программистов, которые занимаются изобретением принципиально новых методов заражения, скрытия, противодействия антивирусам и т.д. Они же придумывают способы внедрения в новые операционные системы, конструкторы вирусов и полиморфик-генераторы. Эти программисты пишут вирусы не ради собственно вирусов, а скорее ради «исследования» потенциалов «компьютерной фауны».

Отношение к авторам вирусов у меня тройственное. Во-первых, все, кто пишет вирусы или способствует их распространению, являются «кормильцами» антивирусной индустрии, годовой оборот которой я оцениваю как минимум две сотни миллионов долларов или даже более того (при этом не стоит забывать, что убытки от вирусов составляют несколько сотен миллионов долларов ежегодно и в разы превышают расходы на антивирусные программы). Если общее количество вирусов к концу 1997 года скорее всего достигнет 20.000, то нетрудно подсчитать, что доход антивирусных фирм от каждого вируса ежегодно составляет минимум 10 тысяч долларов. Конечно же, авторам вирусов не следует надеяться на материальное вознаграждение: как показывает практика, их труд был и остается бесплатным. К тому же на сегодняшний день предложение (новые вирусы) вполне удовлетворяет спрос (возможности антивирусных фирм по обработке новых вирусов).

Во-вторых, мне несколько жаль авторов вирусов, особенно «профессионалов». Ведь для того, чтобы написать подобный вирус, необходимо: a) затратить довольно много сил и времени, причем гораздо больше, чем требуется для того, чтобы разобраться в вирусе занести его в базу данных или даже написать специальный антивирус; и б) не иметь другого, более привлекательного, занятия. Следовательно, вирусописатели -»профессионалы» довольно работоспособны и одновременно с этим маются от безделья - ситуация, как мне кажется, весьма печальная.

И в третьих, к моему отношению к авторам вирусов довольно сильно подмешаны чувства нелюбви и презрения как к людям, заведомо и бесцельно тратящим себя во вред всем остальным.

##### Раздел 2

##### Компьютерные вирусы, их свойства и классификация

###### **2.1 Свойства компьютерных вирусов**

Сейчас применяются персональные компьютеры, в которых пользователь имеет свободный доступ ко всем ресурсам машины. Именно это открыло возможность для опасности, которая получила название компьютерного вируса.

Что такое компьютерный вирус? Формальное определение этого понятия до сих пор не придумано, и есть серьезные сомнения, что оно вообще может быть дано. Многочисленные попытки дать «современное» определение вируса не привели к успеху. Чтобы почувствовать всю сложность проблемы, попробуйте, к примеру, дать определение понятия «редактор». Вы либо придумаете нечто очень общее, либо начнете перечислять все известные типы редакторов. И то и другое вряд ли можно считать приемлемым. Поэтому мы ограничимся рассмотрением некоторых свойств компьютерных вирусов, которые позволяют говорить о них как о некотором определенном классе программ.

Прежде всего, вирус - это программа. Такое простое утверждение само по себе способно развеять множество легенд о необыкновенных возможностях компьютерных вирусов. Вирус может перевернуть изображение на вашем мониторе, но не может перевернуть сам монитор. К легендам о вирусах-убийцах, «уничтожающих операторов посредством вывода на экран смертельной цветовой гаммы 25-м кадром» также не стоит относиться серьезно. К сожалению, некоторые авторитетные издания время от времени публикуют «самые свежие новости с компьютерных фронтов», которые при ближайшем рассмотрении оказываются следствием не вполне ясного понимания предмета.

Вирус - программа, обладающая способностью к самовоспроизведению. Такая способность является единственным средством, присущим всем типам вирусов. Но не только вирусы способны к самовоспроизведению. Любая операционная система и еще множество программ способны создавать собственные копии. Копии же вируса не только не обязаны полностью совпадать с оригиналом, но, и могут вообще с ним не совпадать!

Вирус не может существовать в «полной изоляции»: сегодня нельзя представить себе вирус, который не использует код других программ, информацию о файловой структуре или даже просто имена других программ. Причина понятна: вирус должен каким-нибудь способом обеспечить передачу себе управления.

###### **2.2 Классификация вирусов**

В настоящее время известно более 5000 программных вирусов, их можно классифицировать по следующим признакам:

* среде обитания
* способу заражения среды обитания
* воздействию
* особенностям алгоритма

В зависимости от среды обитания вирусы можно разделить на сетевые, файловые, загрузочные и файлово-загрузочные. Сетевые вирусы распространяются по различным компьютерным сетям. Файловые вирусы внедряются главным образом в исполняемые модули, т. е. В файлы, имеющие расширения COM и EXE. Файловые вирусы могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах, они никогда не получают управление и, следовательно, теряют способность к размножению. Загрузочные вирусы внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Re-cord). Файлово-загрузочные вирусы заражают как файлы, так и загрузочные сектора дисков.

По способу заражения вирусы делятся на резидентные и нерезидентные. Резидентный вирус при заражении (инфицировании) компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера. Нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время.

По степени воздействия вирусы можно разделить на следующие виды:

* неопасные, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах
* опасные вирусы, которые могут привести к различным нарушениям в работе компьютера
* очень опасные, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

По особенностям алгоритма вирусы трудно классифицировать из-за большого разнообразия. Простейшие вирусы - паразитические, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены. Можно отметить вирусы-репликаторы, называемые червями, которые распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии.

Известны вирусы-невидимки, называемые стелс-вирусами, которые очень трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска. Наиболее трудно обнаружить вирусы-мутанты, содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов. Имеются и так называемые квазивирусные или «троянские» программы, которые хотя и не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.

Теперь поподробнее о некоторых из этих групп.

**2.3 Загрузочные вирусы**

Рассмотрим схему функционирования очень простого загрузочного вируса, заражающего дискеты.

Что происходит, когда вы включаете компьютер? Первым делом управление передается программе начальной загрузки, которая хранится в постоянно запоминающем устройстве (ПЗУ) т.е. ПНЗ ПЗУ.

Эта программа тестирует оборудование и при успешном завершении проверок пытается найти дискету в дисководе А:

Всякая дискета размечена на т.н. секторы и дорожки. Секторы объединяются в кластеры, но это для нас несущественно.

Среди секторов есть несколько служебных, используемых операционной системой для собственных нужд (в этих секторах не могут размещаться ваши данные). Среди служебных секторов нас интересует сектор начальной загрузки (boot-sector).

В секторе начальной загрузки хранится информация о дискете - количество поверхностей, количество дорожек, количество секторов и пр. Но нас сейчас интересует не эта информация, а небольшая программа начальной загрузки (ПНЗ), которая должна загрузить саму операционную систему и передать ей управление.

Таким образом, нормальная схема начальной загрузки следующая:

ПНЗ (ПЗУ) - ПНЗ (диск) - СИСТЕМА

Теперь рассмотрим вирус. В загрузочных вирусах выделяют две части: голову и т.н. хвост. Хвост может быть пустым.

Пусть у вас имеются чистая дискета и зараженный компьютер, под которым мы понимаем компьютер с активным резидентным вирусом. Как только этот вирус обнаружит, что в дисководе появилась подходящая жертва - в нашем случае не защищенная от записи и еще не зараженная дискета, он приступает к заражению. Заражая дискету, вирус производит следующие действия:

* выделяет некоторую область диска и помечает ее как недоступную операционной системе, это можно сделать по-разному, в простейшем и традиционном случае занятые вирусом секторы помечаются как сбойные (bad)
* копирует в выделенную область диска свой хвост и оригинальный (здоровый) загрузочный сектор
* замещает программу начальной загрузки в загрузочном секторе (настоящем) своей головой
* организует цепочку передачи управления согласно схеме.

Таким образом, голова вируса теперь первой получает управление, вирус устанавливается в память и передает управление оригинальному загрузочному сектору. В цепочке

ПНЗ (ПЗУ) - ПНЗ (диск) - СИСТЕМА

появляется новое звено:

ПНЗ (ПЗУ) - ВИРУС - ПНЗ (диск) - СИСТЕМА

Мы рассмотрели схему функционирования простого бутового вируса, живущего в загрузочных секторах дискет. Как правило, вирусы способны заражать не только загрузочные секторы дискет, но и загрузочные секторы винчестеров. При этом в отличие от дискет на винчестере имеются два типа загрузочных секторов, содержащих программы начальной загрузки, которые получают управление. При загрузке компьютера с винчестера первой берет на себя управление программа начальной загрузки в MBR (Master Boot Record - главная загрузочная запись). Если ваш жесткий диск разбит на несколько разделов, то лишь один из них помечен как загрузочный (boot). Программа начальной загрузки в MBR находит загрузочный раздел винчестера и передает управление на программу начальной загрузки этого раздела. Код последней совпадает с кодом программы начальной загрузки, содержащейся на обычных дискетах, а соответствующие загрузочные секторы отличаются только таблицами параметров. Таким образом, на винчестере имеются два объекта атаки загрузочных вирусов - программа начальной загрузки в MBR и программа начальной загрузки в бут-секторе загрузочного диска.

###### **2.4 Файловые вирусы**

Рассмотрим теперь схему работы простого файлового вируса. В отличие от загрузочных вирусов, которые практически всегда резидентны, файловые вирусы совсем не обязательно резидентны. Рассмотрим схему функционирования нерезидентного файлового вируса. Пусть у нас имеется инфицированный исполняемый файл. При запуске такого файла вирус получает управление, производит некоторые действия и передает управление «хозяину»

Какие же действия выполняет вирус? Он ищет новый объект для заражения - подходящий по типу файл, который еще не заражен. Заражая файл, вирус внедряется в его код, чтобы получить управление при запуске этого файла. Кроме своей основной функции - размножения, вирус вполне может сделать что-нибудь замысловатое (сказать, спросить, сыграть) - это уже зависит от фантазии автора вируса. Если файловый вирус резидентный, то он установится в память и получит возможность заражать файлы и проявлять прочие способности не только во время работы зараженного файла. Заражая исполняемый файл, вирус всегда изменяет его код - следовательно, заражение исполняемого файла всегда можно обнаружить. Но, изменяя код файла, вирус не обязательно вносит другие изменения:

* он не обязан менять длину файла
* неиспользуемые участки кода
* не обязан менять начало файла

Наконец, к файловым вирусам часто относят вирусы, которые «имеют некоторое отношение к файлам», но не обязаны внедряться в их код.

Таким образом, при запуске любого файла вирус получает управление (операционная система запускает его сама), резидентно устанавливается в память и передает управление вызванному файлу.

###### **2.5 Загрузочно-файловые вирусы**

Мы не станем рассматривать модель загрузочно-файлового вируса, ибо никакой новой информации вы при этом не узнаете. Но здесь представляется удобный случай кратко обсудить крайне «популярный» в последнее время загрузочно-файловый вирус OneHalf, заражающий главный загрузочный сектор (MBR) и исполняемые файлы. Основное разрушительное действие - шифрование секторов винчестера. При каждом запуске вирус шифрует очередную порцию секторов, а, зашифровав половину жесткого диска, радостно сообщает об этом. Основная проблема при лечении данного вируса состоит в том, что недостаточно просто удалить вирус из MBR и файлов, надо расшифровать зашифрованную им информацию.

###### **2.6 Полиморфные вирусы**

Большинство вопросов связано с термином «полиморфный вирус». Этот вид компьютерных вирусов представляется на сегодняшний день наиболее опасным. Объясним же, что это такое.

Полиморфные вирусы - вирусы, модифицирующие свой код в зараженных программах таким образом, что два экземпляра одного и того же вируса могут не совпадать ни в одном бите.

Такие вирусы не только шифруют свой код, используя различные пути шифрования, но и содержат код генерации шифровщика и расшифровщика, что отличает их от обычных шифровальных вирусов, которые также могут шифровать участки своего кода, но имеют при этом постоянный код шифровальщика и расшифровщика.

Полиморфные вирусы - это вирусы с самомодифицирующимися расшифровщиками. Цель такого шифрования: имея зараженный и оригинальный файлы, вы все равно не сможете проанализировать его код с помощью обычного дизассемблирования. Этот код зашифрован и представляет собой бессмысленный набор команд. Расшифровка производится самим вирусом уже непосредственно во время выполнения. При этом возможны варианты: он может расшифровать себя всего сразу, а может выполнить такую расшифровку «по ходу дела», может вновь шифровать уже отработавшие участки. Все это делается ради затруднения анализа кода вируса.

2.7 Стелс-вирусы

В ходе проверки компьютера антивирусные программы считывают данные - файлы и системные области с жестких дисков и дискет, пользуясь средствами операционной системы и базовой системы ввода/вывода BIOS. Ряд вирусов, после запуска оставляют в оперативной памяти компьютера специальные модули, перехватывающие обращение программ к дисковой подсистеме компьютера. Если такой модуль обнаруживает, что программа пытается прочитать зараженный файл или системную область диска, он на ходу подменяет читаемые данные, как будто вируса на диске нет.

Стелс-вирусы обманывают антивирусные программы и в результате остаются незамеченными. Тем не менее, существует простой способ отключить механизм маскировки стелс-вирусов. Достаточно загрузить компьютер с не зараженной системной дискеты и сразу, не запуская других программ с диска компьютера (которые также могут оказаться зараженными), проверить компьютер антивирусной программой.

При загрузке с системной дискеты вирус не может получить управление и установить в оперативной памяти резидентный модуль, реализующий стелс-механизм. Антивирусная программа сможет прочитать информацию, действительно записанную на диске, и легко обнаружит вирус.

### **2.8 Троянские кони, программные закладки и сетевые черви**

Троянский конь – это программа, содержащая в себе некоторую разрушающую функцию, которая активизируется при наступлении некоторого условия срабатывания. Обычно такие программы маскируются под какие-нибудь полезные утилиты. Вирусы могут нести в себе троянских коней или "троянизировать" другие программы – вносить в них разрушающие функции.

«Троянские кони» представляют собой программы, реализующие помимо функций, описанных в документации, и некоторые другие функции, связанные с нарушением безопасности и деструктивными действиями. Отмечены случаи создания таких программ с целью облегчения распространения вирусов. Списки таких программ широко публикуются в зарубежной печати. Обычно они маскируются под игровые или развлекательные программы и наносят вред под красивые картинки или музыку.

Программные закладки также содержат некоторую функцию, наносящую ущерб ВС, но эта функция, наоборот, старается быть как можно незаметнее, т.к. чем дольше программа не будет вызывать подозрений, тем дольше закладка сможет работать.

В более 80% компьютерных преступлений, расследуемых ФБР, "взломщики" проникают в атакуемую систему через глобальную сеть Internet. Когда такая попытка удается, будущее компании, на создание которой ушли годы, может быть поставлено под угрозу за какие-то секунды.

Этот процесс может быть автоматизирован с помощью вируса, называемого сетевой червь.

Червями называют вирусы, которые распространяются по глобальным сетям, поражая целые системы, а не отдельные программы. Это самый опасный вид вирусов, так как объектами нападения в этом случае становятся информационные системы государственного масштаба. С появлением глобальной сети Internet этот вид нарушения безопасности представляет наибольшую угрозу, т. к. ему в любой момент может подвергнуться любой из 40 миллионов компьютеров, подключенных к этой сети.

Раздел 3

Пути проникновения вирусов в компьютер и механизм распределения вирусных программ

Основными путями проникновения вирусов в компьютер являются съемные диски (гибкие и лазерные), а также компьютерные сети. Заражение жесткого диска вирусами может произойти при загрузке программы с дискеты, содержащей вирус. Такое заражение может быть и случайным, например, если дискету не вынули из дисковода А и перезагрузили компьютер, при этом дискета может быть и не системной. Заразить дискету гораздо проще. На нее вирус может попасть, даже если дискету просто вставили в дисковод зараженного компьютера и, например, прочитали ее оглавление.

Вирус, как правило, внедряется в рабочую программу таким образом, чтобы при ее запуске управление сначала передалось ему и только после выполнения всех его команд снова вернулось к рабочей программе. Получив доступ к управлению, вирус, прежде всего, переписывает сам себя в другую рабочую программу и заражает ее. После запуска программы, содержащей вирус, становится возможным заражение других файлов.

Наиболее часто вирусом заражаются загрузочный сектор диска и исполняемые файлы, имеющие расширения EXE, COM, SYS, BAT. Крайне редко заражаются текстовые файлы.

3.1 Признаки появления вирусов

При заражении компьютера вирусом важно его обнаружить. Для этого следует знать об основных признаках проявления вирусов. К ним можно отнести следующие:

* прекращение работы или неправильная работа ранее успешно функционировавших программ
* медленная работа компьютера
* невозможность загрузки операционной системы
* исчезновение файлов и каталогов или искажение их содержимого
* изменение даты и времени модификации файлов
* изменение размеров файлов
* неожиданное значительное увеличение количества файлов на диске
* существенное уменьшение размера свободной оперативной памяти
* вывод на экран непредусмотренных сообщений или изображений
* подача непредусмотренных звуковых сигналов
* частые зависания и сбои в работе компьютера

Следует отметить, что вышеперечисленные явления необязательно вызываются присутствием вируса, а могут быть следствием других причин. Поэтому всегда затруднена правильная диагностика состояния компьютера.

**Раздел 4**

## Методы защиты от компьютерных вирусов

Каким бы не был вирус, пользователю необходимо знать основные методы защиты от компьютерных вирусов.

Для защиты от вирусов можно использовать:

* общие средства защиты информации, которые полезны также и как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя;
* профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
* специализированные программы для защиты от вирусов.

Общие средства защиты информации полезны не только для защиты от вирусов. Имеются две основные разновидности этих средств:

* копирование информации - создание копий файлов и системных областей дисков;
* разграничение доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

Несмотря на то, что общие средства защиты информации очень важны для защиты от вирусов, все же их недостаточно. Необходимо и применение специализированных программ для защиты от вирусов. Эти программы можно разделить на несколько видов: детекторы, доктора (фаги), ревизоры, доктора-ревизоры, фильтры и вакцины (иммунизаторы).

ПРОГРАММЫ-ДЕТЕКТОРЫ позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов. Эти программы проверяют, имеется ли в файлах на указанном пользователем диске специфическая для данного вируса комбинация байтов. При ее обнаружении в каком-либо файле на экран выводится соответствующее сообщение. Многие детекторы имеют режимы лечения или уничтожения зараженных файлов. Следует подчеркнуть, что программы-детекторы могут обнаруживать только те вирусы, которые ей "известны". Программа Scan фирмы McAfee Associates и Aidstest Д.Н.Лозинского позволяют обнаруживать около 9000 вирусов, но всего их более двадцати тысяч! Некоторые программы-детекторы, например Norton AntiVirus или AVSP фирмы "Диалог-МГУ", могут настраивать на новые типы вирусов, им необходимо лишь указать комбинации байтов, присущие этим вирусам. Тем не мнение невозможно разработать такую программу, которая могла бы обнаруживать любой заранее неизвестный вирус.

Таким образом, из того, что программа не опознается детекторами как зараженная, не следует, что она здорова - в ней могут сидеть какой-нибудь новый вирус или слегка модифицированная версия старого вируса, неизвестные программам-детекторам.

Многие программы-детекторы (в том числе и Aidstest) не умеют обнаруживать заражение "невидимыми" вирусами, если такой вирус активен в памяти компьютера. Дело в том, что для чтения диска они используют функции DOS, а они перехватываются вирусом, который говорит, что все хорошо. Правда, Aidstest и другие детекторы пытаются выявить вирус путем просмотра оперативной памяти, но против некоторых "хитрых" вирусов это не помогает. Так что надежный диагноз программы-детекторы дают только при загрузке DOS с "чистой", защищенной от записи дискеты, при этом копия программы-детектора также должна быть запущена с этой дискеты.

Большинство программ-детекторов имеют функцию "доктора", т.е. они пытаются вернуть зараженные файлы или области диска в их исходное состояние. Те файлы, которые не удалось восстановить, как правило, делаются неработоспособными или удаляются.

Большинство программ-докторов умеют "лечить" только от некоторого фиксированного набора вирусов, поэтому они быстро устаревают. Но некоторые программы могут обучаться не только способам обнаружения, но и способам лечения новых вирусов. К таким программам относится AVSP фирмы "Диалог-МГУ".

ПРОГРАММЫ-РЕВИЗОРЫ имеют две стадии работы. Сначала они запоминают сведения о состоянии программ и системных областей дисков (загрузочного сектора и сектора с таблицей разбиения жесткого диска). Предполагается, что в этот момент программы и системные области дисков не заражены. После этого с помощью программы-ревизора можно в любой момент сравнить состояние программ и системных областей дисков с исходным. О выявленных несоответствиях сообщается пользователю.

Чтобы проверка состояния программ и дисков проходила при каждой загрузке операционной системы, необходимо включить команду запуска программы-ревизора в командный файл AUTOEXEC.BAT. Это позволяет обнаружить заражение компьютерным вирусом, когда он еще не успел нанести большого вреда. Более того, та же программа-ревизор сможет найти поврежденные вирусом файлы.

Многие программы-ревизоры являются довольно "интеллектуальными" - они могут отличать изменения в файлах, вызванные, например, переходом к новой версии программы, от изменений, вносимых вирусом, и не поднимают ложной тревоги. Дело в том, что вирусы обычно изменяют файлы весьма специфическим образом и производят одинаковые изменения в разных программных файлах. Другие программы часто используют различные полумеры – пытаются обнаружить вирус в оперативной памяти, требуют вызовы из первой строки файла AUTOEXEC.BAT, надеясь работать на "чистом" компьютере, и т.д. Увы, против некоторых "хитрых" вирусов все это бесполезно.

Для проверки того, не изменился ли файл, некоторые программы-ревизоры проверяют длину файла. Но эта проверка недостаточна - некоторые вирусы не изменяют длину зараженных файлов. Более надежная проверка - прочесть весь файл и вычислить его контрольную сумму. Изменить файл так, чтобы его контрольная сумма осталась прежней, практически невозможно.

В последнее время появились очень полезные гибриды ревизоров и докторов, т.е. ДОКТОРА-РЕВИЗОРЫ,- программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут в случае изменений автоматически вернуть их в исходное состояние. Такие программы могут быть гораздо более универсальными, чем программы-доктора, поскольку при лечении они используют заранее сохраненную информацию о состоянии файлов и областей дисков. Это позволяет им вылечивать файлы даже от тех вирусов, которые не были созданы на момент написания программы.

Но они могут лечить не от всех вирусов, а только от тех, которые используют "стандартные", известные на момент написания программы, механизмы заражения файлов.

Существуют также ПРОГРАММЫ-ФИЛЬТРЫ, которые располагаются резидентно в оперативной памяти компьютера и перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователя. Пользователь может разрешить или запретить выполнение соответствующей операции.

Некоторые программы-фильтры не "ловят" подозрительные действия, а проверяют вызываемые на выполнение программы, на наличие вирусов. Это вызывает замедление работы компьютера.

Однако преимущества использования программ-фильтров весьма значительны – они позволяют обнаружить многие вирусы на самой ранней стадии, когда вирус еще не успел размножиться и что-либо испортить. Тем самым можно свести убытки от вируса к минимуму.

ПРОГРАММЫ-ВАКЦИНЫ, или ИММУНИЗАТОРЫ, модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными. Эти программы крайне неэффективны.

Раздел 5

Антивирусные программы

Итак, что же такое антивирус? Сразу же развеем одну часто возникающую иллюзию. Почему-то многие считают, что антивирус может обнаружить любой вирус, то есть, запустив антивирусную программу или монитор, можно быть абсолютно уверенным в их надежности. Такая точка зрения не совсем верна. Дело в том, что антивирус - это тоже программа, конечно, написанная профессионалом. Но эти программы способны распознавать и уничтожать только известные вирусы. То есть антивирус против конкретного вируса может быть написан только в том случае, когда у программиста есть в наличии хотя бы один экземпляр этого вируса. Вот и идет эта бесконечная война между авторами вирусов и антивирусов, правда, первых в нашей стране почему-то всегда больше, чем вторых. Но и у создателей антивирусов есть преимущество! Дело в том, что существует большое количество вирусов, алгоритм которых практически скопирован с алгоритма других вирусов. Как правило, такие вариации создают непрофессиональные программисты, которые по каким-то причинам решили написать вирус. Для борьбы с такими "копиями" придумано новое оружие - эвристические анализаторы. С их помощью антивирус способен находить подобные аналоги известных вирусов, сообщая пользователю, что у него, похоже, завелся вирус. Естественно, надежность эвристического анализатора не 100%, но все же его коэффициент полезного действия больше 0,5. Таким образом, в этой информационной войне, как, впрочем, и в любой другой, остаются сильнейшие. Вирусы, которые не распознаются антивирусными детекторами, способны написать только наиболее опытные и квалифицированные программисты.

Таким образом, на 100% защититься от вирусов практически невозможно (подразумевается, что пользователь меняется дискетами с друзьями и играет в игры, а также получает информацию из других источников, например из сетей). Если же не вносить информацию в компьютер извне, заразиться вирусом невозможно - сам он не родится.

### **5.1 DOCTOR WEB**

В последнее время стремительно растет популярность другой антивирусной программы - Doctor Web. Dr.Web так же, как и Aidstest относится к классу детекторов - докторов, но в отличие от последнего, имеет так называемый "эвристический анализатор" - алгоритм, позволяющий обнаруживать неизвестные вирусы. "Лечебная паутина", как переводится с английского название программы, стала ответом отечественных программистов на нашествие самомодифицирующихся вирусов-мутантов. Последние при размножении модифицируют свое тело так, что не остается ни одной характерной цепочки байт, присутствовавшей в исходной версии вируса. Dr.Web можно назвать антивирусом нового поколения по сравнению с Aidstest и его аналогами.

Управление режимами также как и в Aidstest осуществляется с помощью ключей. Пользователь может указать программе, тестировать как весь диск, так и отдельные подкаталоги или группы файлов, либо же отказаться от проверки дисков и тестировать только оперативную память. В свою очередь можно тестировать либо только базовую память, либо, вдобавок, ещё и расширенную (указывается с помощью ключа /H). Как и Aidstest Doctor Web может создавать отчет о работе (ключ /P), загружать знакогенератор Кириллицы (ключ /R), поддерживает работу с программно-аппаратным комплексом Sheriff (ключ /Z).

Но, конечно, главной особенностью "Лечебной паутины" является наличие эвристического анализатора, который подключается ключом /S. Баланса между скоростью и качеством можно добиться, указав ключу уровень эвристического анализа: 0 - минимальный, 1 - оптимальный, 2 - максимальный; при этом, естественно, скорость уменьшается пропорционально увеличению качества. К тому же Dr.Web позволяет тестировать файлы, вакцинированные CPAV, а также упакованные LZEXE, PKLITE, DIET. Для этого следует указать ключ /U (при этом распаковка файлов будет произведена на текущем устройстве) или /U диск: (где диск: - устройство, на котором будет производиться распаковка), если дискета, с которой запущен Doctor Web защищена от записи. Многие программы упакованы таким способом, хотя пользователь может и не подозревать об этом. Если ключ /U не установлен, то Doctor Web может пропустить вирус, забравшийся в запакованную программу.

Важной функцией является контроль заражения тестируемых файлов резидентным вирусом (ключ /V). При сканировании памяти нет стопроцентной гарантии, что "Лечебная паутина" обнаружит все вирусы, находящиеся там. Так вот, при задании функции /V Dr.Web пытается воспрепятствовать оставшимся резидентным вирусам, заразить тестируемые файлы.

Тестирование винчестера Dr.Web-ом занимает на много больше времени, чем Aidstest-ом, поэтому не каждый пользователь может себе позволить тратить столько времени на ежедневную проверку всего жесткого диска. Таким пользователям можно посоветовать более тщательно (с опцией /S2) проверять принесенные извне дискеты. Если информация на дискете находится в архиве (а в последнее время программы и данные переносятся с машины на машину только в таком виде; даже фирмы-производители программного обеспечения, например Borland, пакуют свою продукцию), следует распаковать его в отдельный каталог на жестком диске и сразу же, не откладывая, запустить Dr.Web, задав ему в качестве параметра вместо имени диска полный путь к этому подкаталогу. И все же нужно хотя бы раз в две недели производить полную проверку "винчестера" на вирусы с заданием максимального уровня эвристического анализа.

Так же как и в случае с Aidstest при начальном тестировании не стоит разрешать программе лечить файлы, в которых она обнаружит вирус, так как нельзя исключить, что последовательность байт, принятая в антивирусе за шаблон может встретиться в здоровой программе. Если по завершении тестирования Dr.Web выдаст сообщения о том, что нашел вирусы, нужно запустить его с опцией /P (если эта опция не была указана) для того, чтобы посмотреть, какой файл заражен. После этого нужно скопировать файл на дискету или на электронный диск и попытаться удалить, указав "Лечебной паутине" ключ /F. При неудачном лечении следует поступить так же, как в аналогичной ситуации, описанной выше для программы Aidstest.

5.2 MICROSOFT ANTIVIRUS

В состав современных версий MS-DOS (например, 7.10) входит антивирусная программа Microsoft Antivirus (MSAV). Этот антивирус может работать в режимах детектора-доктора и ревизора.

MSAV имеет дружественный интерфейс в стиле MS-Windows, естественно, поддерживается мышь. Хорошо реализована контекстная помощь: подсказка есть практически к любому пункту меню, к любой ситуации. Универсально реализован доступ к пунктам меню: для этого можно использовать клавиши управления курсором, ключевые клавиши (F1-F9), клавиши, соответствующие одной из букв названия пункта, а также мышь. Флажки установок в пункте меню Options можно устанавливать как клавишей ПРОБЕЛ, так и клавишей ENTER. Серьёзным неудобством при использовании программы является то, что она сохраняет таблицы с данными о файлах не в одном файле, а разбрасывает их по всем директориям.

При запуске программа загружает собственный знакогенератор и читает дерево каталогов текущего диска, после чего выходит в главное меню. Не понятно, зачем читать дерево каталогов сразу при запуске: ведь пользователь может и не захотеть проверять текущий диск. В главном меню можно сменить диск (Select new drive), выбрать между проверкой без удаления вирусов (Detect) и с их удалением (Detect&Clean). При запуске проверки диска (как в режиме удаления, так и без него) программа сначала сканирует память на наличие известных ей вирусов. При этом выводится индикация проделанной работы в виде цветной полоски и процента выполненной работы. После сканирования памяти MSAV принимается за проверку непосредственно диска.

При первой проверке MSAV создает в каждой директории, содержащей исполнимые файлы, файлы CHKLIST.MS, в которые записывает информацию о размере, дате, времени, атрибутах, а также контрольную сумму контролируемых файлов. При последующих проверках программа будет сравнивать файлы с информацией в CHKLIST.MS-файлах. Если изменились размер и дата, то программа сообщит об этом пользователю и запросит о дальнейших действиях: обновить информацию (Update), установить дату и время в соответствие с данными в CHKLIST.MS (Repair), продолжить, не обращая внимания на изменения в данном файле (Continue), прервать проверку (Stop). Если изменилась контрольная сумма, то MSAV выведет такое же окно, только вместо пункта Repair будет пункт Delete (удалить), так как программа не может восстановить содержимое файла. При обнаружении вируса в режиме Detect&Clean программа удалит этот вирус. Проверку диска в обоих режимах можно приостановить, либо полностью прервать, нажав ESC (или F3) и ответив на соответствующий вопрос программы. Во время сканирования диска выводится информация о проделанной работе: процент обработанных каталогов и процент обработанных файлов в текущем каталоге. Эта информация выдается также наглядно, в виде цветной полоски, как и при проверке памяти. В конце проверки MSAV выдает отчет в виде таблицы, в которой сообщается о количестве проверенных жестких дисков и гибких дисков, о количестве проверенных, инфицированных и вылеченных файлов. Кроме того, выводится время сканирования.

В меню Options можно сконфигурировать программу по собственному желанию. Здесь можно установить режим поиска вирусов-невидимок (Anti-Stealth), проверки всех (а не только исполнимых) файлов (Check All Files), а также разрешить или запретить создавать таблицы CHKLIST.MS (Create New Checksums). К тому же можно задать режим сохранения отчета о проделанной работе в файле. Если установить опцию Create Backup, то перед удалением вируса из зараженного файла его копия будет сохранена с расширением \*.VIR

Находясь в основном меню, можно просмотреть список вирусов, известных программе MSAV, нажав клавишу F9. При этом выведется окно с названиями вирусов. Чтобы посмотреть более подробную информацию о вирусе, нужно подвести курсор к его имени и нажать ENTER. Можно быстро перейти к интересующему вирусу, набрав первые буквы его имени. Информацию о вирусе можно вывести на принтер, выбрав соответствующий пункт меню.

Заключение

Ни один тип антивирусных программ по отдельности не дает полной защиты от вирусов. Лучшей стратегией защиты от вирусов является многоуровневая, "эшелонированная" оборона. Средствам разведки в "обороне" от вирусов соответствуют программы-детекторы, позволяющие проверять вновь полученное программное обеспечение на наличие вирусов. На переднем крае обороны находятся программы-фильтры. Эти программы могут первыми сообщить о работе вируса и предотвратить заражение программ и дисков. Второй эшелон обороны составляют программы-ревизоры, программы-доктора и доктора-ревизоры. Самый глубокий эшелон обороны - это средства разграничения доступа. Они не позволяют вирусам и неверно работающим программам, даже если они проникли в компьютер, испортить важные данные.

**Список литературы**

1. Безруков Н.Н. "Классификация компьютерных вирусов MS-DOS и методы защиты от них", Москва, СП "ICE", 1990 г.
2. Безруков Н.Н. "Компьютерные вирусы", Москва, Наука, 1991.
3. Денисов Т.В. "Антивирусная защита"//Мой Компьютер-№4-1999г.
4. Мостовой Д.Ю. "Современные технологии борьбы с вирусами" // Мир ПК. - №8. - 1993.
5. Ф.Файтс, П.Джонстон, М.Кратц "Компьютерный вирус: проблемы и прогноз", Москва, "Мир", 1993 г.

Интернет:

1. <http://www.symantec.ru/region/ru/product/navbrochure/index.htm>
2. <http://www.symantec.ru>
3. <http://www.dials.ru/>
4. [http://www.avp.ru/](http://www.apl.ru/isvwsolaris.htm)
5. [http://www.dialognauka.ru/](http://www2.dialognauka.ru/)
6. <http://www.apl.ru/isvwsolaris.htm>
7. <http://www.act.ru/av/Solomon/DrSolom_report.asp>