**Содержание**

# Введение. ……………………………………………………………. 2

# Компьютерные вирусы и защита от них……….. 3

# Что такое компьютерный вирус?…………………………… 3

# Испорченные и зараженные файлы………………………… 5

# Классификация вирусов……………………………………… 7

# Борьба с компьютерными вирусами…………….. 12

# Основные методы защиты от компьютерных вирусов…… 12

# Программы - детекторы и доктора…………………………. 14

# Действия при заражении вирусом…………………………… 16

# Профилактика против заражения вирусом………………… 18

# Заключение. …………………………………………………………. 19

1. **Введе****ние.**

В настоящее время очень многие области деятельности человека связаны с применением компьютеров. Почему же эти электронные машины так плотно внедряются в нашу жизнь. Все довольно тривиально. Они выполняют рутинную расчетную и оформительскую работу, освобождая наш мозг для более необходимых и ответственных задач. В результате утомляемость резко снижается, и мы начинаем работать гораздо производительнее, нежели без применения компьютера.

Возможности современных компьютеров поражают самое богатое воображение. Они способны параллельно выполнять несколько задач, сложность которых довольно велика. По этому некоторые производители задумываются над созданием искусственного интеллекта. Да и сейчас работа компьютера напоминает работу интеллектуального электронного помощника человека.

Но кто бы мог подумать, что этому электронному чуду техники свойственны болезни похожие на человеческие. Он так же как и человек может подвергнуться атаке "**вируса**" но компьютерного. И если не принять мер, компьютер скоро "заболеет" т.е. начнет выполнять неправильные действия или вообще "умрет" т.е. повреждения нанесенные "вирусом" окажутся очень серьезными. О том что такое компьютерные вирусы и как с ними бороться пойдет речь далее.

**Глава 1. Компьютерные виру****сы и защита от них.**

**§ 1. Что т****а****ко****е компьюте****рный вирус?**

Компьютерный вирус - это специально написанная небольшая по размерам программа, которая может "приписывать" себя к другим программам (т.е. "заражать" их), а также выполнять различные нежелательные действия на компьютере. Программа, внутри которой находится вирус, называется зараженной. Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и "заражает" другие программы, а также выполняет какие-нибудь вредные действия (например, портит файлы или таблицу размещения файлов (FAT) на диске, "засоряет" оперативную память и т.д.). Для маскировки вируса действия по заражению других программ и нанесению вреда могут выполняться не всегда, а скажем, при выполнении определенных условий. После того как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится, и она работает как обычно. Тем самым внешне работа зараженной программы выглядит так же, как и незараженной.

Многие разновидности вирусов устроены так, что при запуске зараженной программы вирус остается в памяти компьютера и время от времени заражает программы и выполняет нежелательные действия на компьютере.

Все действия вируса могут выполняться очень быстро и без выдачи каких либо сообщений, по этому пользователю очень трудно, практически невозможно, определить, что в компьютере происходит что-то необычное.

Пока на компьютере заражено относительно мало программ, наличие вируса может быть практически незаметным. Однако по прошествии некоторого времени на компьютере начинает твориться что-то странное, например:

* некоторые программы перестают работать или начинают работать неправильно;
* на экран выводятся посторонние сообщения, символы и т.д.;
* работа на компьютере существенно замедляется;
* некоторые файлы оказываются испорченными и т.д.

К этому моменту, как правило, уже достаточно много (или даже большинство) тех программ, с которыми вы работаете, являются зараженными вирусом, а некоторые файлы и диски — испорченными. Более того, зараженные программы с Вашего компьютера могли быть уже перенесены с помощью дискет или локальной сети на компьютеры ваших коллег и друзей.

Некоторые вирусы ведут себя очень коварно. Они вначале незаметно заражают большое число программ и дисков, а затем наносят очень серьезные повреждения, например, форматируют весь жесткий диск на компьютере, естественно после этого восстановить данные бывает просто невозможно. А бывают вирусы, которые ведут себя очень скрытно, и портят понемногу данные на жестком диске или сдвигают таблицу размещения файлов (FAT). К последним относится вирус **OneHalf**, имеющий множество модификаций.

Таким образом, если не принимать мер по защите от вируса, то последствия заражения могут быть очень серьезными. Например, в начале 1989г. вирусом, написанным американским студентом Моррисом, были заражены и выведены из строя тысячи компьютеров, в том числе принадлежащих министерству обороны США. Автор вируса был приговорен судом к трем месяцам тюрьмы и штрафу в 270 тыс. дол. Наказание могло быть и более строгим, но суд учел, что вирус не портил данные, а только размножался.

Для того, чтобы программа-вирус была незаметной, она должна иметь небольшие размеры. По этому вирусы пишут обычно на низкоуровневых языках Ассемблер или низкоуровневыми командами языка СИ.

Вирусы пишутся опытными программистами или студентами просто из любопытства или для отместки кому-либо или предприятию, которое обошлось с ними недостойным образом или в коммерческих целях или в целях направленного вредительства. Какие бы цели не преследовал автор, вирус может оказаться на вашем компьютере и постарается произвести те же вредные действия, что и у того, для кого он был создан.

Следует заметить, что написание вируса — не такая уж сложная задача, вполне доступная изучающему программирование студенту. Поэтому еженедельно в мире появляются все новые и новые вирусы. И многие из них сделаны в нашей стране.

**§ 2. Ис****по****рченные и зараженные ф****айлы**

Компьютерный вирус может испортить, т.е. изменить ненадлежащим образом, любой файл на имеющихся в компьютере дисках. Но некоторые виды файлов вирус может "заразить". Это означает, что вирус может "внедриться" в эти файлы, т.е. изменить их так, что они будут содержать вирус, который при некоторых обстоятельствах может начать свою работу.

Следует заметить, что тексты программ и документов, информационные файлы баз данных, таблицы табличных процессоров и другие аналогичные файлы не могут быть заражены обычным вирусом, он может их только испортить. Заражение подобных файлов делается только Макро-вирусами. Эти вирусы могут заразить даже ваши документы.

Обычным вирусом могут быть заражены следующие виды файлов:

1. ***Исполняемые файлы***, т.е. файлы с расширениями имен **.com** и **.exe**, а также оверлейные файлы, загружаемые при выполнении других программ. Вирусы, заражающие файлы, называются **файловыми**. Вирус в зараженных исполняемых файлах начинает свою работу при запуске той программы, в которой он находится. Наиболее опасны те вирусы, которые после своего запуска остаются в памяти резидентно — они могут заражать файлы и вредить до следующей перезагрузки компьютера. А если они заразят любую программу, запускаемую из файла AUTOEXEC.BAT или CONFIG.SYS, то и при перезагрузке с жесткого диска вирус снова начнет свою работу.
2. ***Загрузчик операционной системы и главная загрузочная запись жесткого диска.*** Вирусы, поражающие эти области, называются **загрузочными** или **BOOT**-вирусами. Такой вирус начинает свою работу при начальной загрузке компьютера и становится резидентным, т.е. постоянно находится в памяти компьютера. Механизм распространения — заражение загрузочных записей вставляемых в компьютер дискет. Часто такие вирусы состоят из двух частей, поскольку загрузочная запись имеет небольшие размеры и в них трудно разместить целиком программу вируса. Часть вируса располагается в другом участке диска. например в конце корневого каталога диска или в кластере в области данных диска (обычно такой кластер объявляется дефектным, чтобы исключить затирание вируса при записи данных на диск).
3. ***Драйверы устройств***, т.е. файлы, указываемые в предложении DEVICE файла CONFIG.SYS. Вирус, находящийся в них начинает свою работу при каждом обращении к соответствующему устройству. Вирусы, заражающие драйверы устройств, очень мало распространены, поскольку драйверы редко переписывают с одного компьютера на другой. То же относится и к системным файлам DOS (MSDOS.SYS и IO.SYS) — их заражение также теоретически возможно, но для распространения вируса малоэффективно.

Как правило, каждая конкретная разновидность вируса может заражать только один или два типа файлов. Чаще всего встречаются вирусы, заражающие исполняемые файлы. На втором месте по распространенности загрузочные вирусы. Некоторые вирусы заражают и файлы и загрузочные области дисков. Вирусы, заражающие драйверы устройств, встречаются крайне редко, обычно такие вирусы умеют заражать и исполняемые файлы.

**§ 3. Классифи****кация в****ир****усов**

Теперь попробуем объять необъятное и представить себе весь всевозможный спектр существующих вирусов. Вирусы можно делить на классы по разным признакам. Вот например по признаку **вероломности**:

* вирусы, моментально поражающие компьютер, форматируют жесткий диск, портят таблицу размещения файлов, портят загрузочные сектора, стирают так называемое Flash-ПЗУ (где находится BIOS) компьютера (вирус "**Чернобыль**"), другими словами, как можно быстрее наносят непоправимый урон компьютеру. Сюда же можно отнести и результаты обид программистов, пишущих вирусы, на антивирусные программы. Имеются в виду так называемые **аллергии** на определенные антивирусные программы. Эти вирусы достаточно вероломны. Вот например, аллергия на Dr.Weber при вызове этой программы, не долго думая блокирует антивирус, портит все, что находится в директории с антивирусом и C:\WINDOWS. В результате приходится переустанавливать операционную систему и затем бороться с вирусом другими средствами.
* вирусы, рассчитанные на продолжительную жизнь в компьютере. Они постепенно и осторожно заражают программу за программой, не афишируя, свое присутствие и производят подмену стартовых областей программ на ссылки к месту где расположено тело вируса. Кроме этого они производят незаметное для пользователя изменение структуры диска, что даст о себе знать только когда некоторые данные уже будут безнадежно утеряны (вирус "**OneHalf-3544**","**Yankey-2C**").

По признаку **способов передачи и размножения** тоже можно провести разделение.

* Раньше вирусы в основном поражали только **исполняемые файлы** (с расширениями .com и .exe). Действительно, ведь вирус это программа и она должна выполняться.
* Теперь вирусы отправляют электронной почтой как демонстрационные программки или как картинки, например, если по электронной почте пришел файл "PicturesForYou.jpg", не спешите его смотреть, тем более, что он пришел неизвестно откуда. Если посмотреть на название повнимательнее, то окажется, что оно имеет еще 42 пробела и действительное расширение .exe. То есть реально полное имя файла будет таким:

"PicturesForYou.jpg .exe". Теперь любому понятно, что на самом деле несет в себе эта картинка. Это не файл рисунка, который при активизации вызывает просмотрщик рисунков, а наглый чуточку завуалированный вирус, который только и ждет когда его активизируют щелчком мыши или нажатием клавиши . Такой вирус вы сами загружаете себе на компьютер, под оболочкой какой-нибудь картинки, как "Троянского коня". Отсюда и жаргонное название таких вирусов как "**Трояны**".

* На данный момент существуют такие оболочки информационных каналов как Internet Explorer, Outlook Express, Microsoft Office. Сейчас появляется немногочисленный класс так называемых "**Макро**-вирусов". Они содержат скрытые команды для данных оболочек, которые нежелательны для рядового пользователя. И этот код уже не является кодом для компьютера, то есть это уже не программа, а текст программы, выполняемый оболочкой. Таким образом, он может быть записан в любом необходимом формате: .html, .htm - для Internet Explorer, .doc, .xls, .xlw, .txt, .prt, или любой другой - для Microsoft Office и т. д.. Такие вирусы наносят вред только определенного характера, ведь оболочка не имеет команд, к примеру, для форматирования жесткого диска. Но все же этот вид вирусов заслуживает внимания, ведь с помощью скрытых гиперссылок он способен самостоятельно загрузить из Интернета на ваш компьютер тело вируса, а некоторые вирусы способны обновляться и загружаться по частям через Интернет с определенных серверов. Вот, например, одним из японских студентов разработан именно такой вирус, который подключает небольшой "загрузчик" к любому формату входных данных из Интернета. Далее этот загрузчик самостоятельно скачивает из Интернета с сервера с IP-адресом Babilon5 тела вируса. Этих тел четыре. Каждая из них способна самостоятельно разрушать ваш компьютер, но имеет определенное назначение. Этот вирус по типу является гибридом между макро-вирусами и обычными вирусами. Но надо отметить, что именно гибриды являются наиболее живучими, хитрыми, опасными и многочисленными среди вирусов. Совсем недавно нашумел скандал о программисте, который, как утверждают эксперты, создал и начал распространение макро-вируса, заражавшего текстовые файлы для Microsoft Word. Его вычислили по дате и времени создания исходного документа, которое хранится в невидимых частях .doc файлов. Возможно, что файл был создан другим человеком до того, как к нему был приделан вирус, тогда вопрос о злоумышленнике остается открытым. Но эксперты утверждают, что это именно он.

Теперь попробуем рассмотреть способы маскировок и защит, применяемых вирусами против нас рядовых пользователей и антивирусных программ.

* **вероломность** — это основной и самый быстрый способ сделать пакость до обнаружения. Действительно, если вирус моментально производит непоправимые действия, нам спешить уже некуда. :-))) Вирус "Чернобыль", например, полностью стирает BIOS (стартовую программу, расположенную в микросхеме ПЗУ, обеспечивающую работу компьютера). После такого компьютер вообще ничего не сможет выдать на экран. Но его работа легко блокируется, если внутри компьютера установлен переключатель, запрещающий писать в область ПЗУ. По этому это был первый, но и, как я думаю, последний представитель аппаратных вирусов. Моментальное форматирование жесткого диска, тоже не из приятных, но в большинстве случаев пользователь, с достаточным опытом, способен предотвратить катастрофу.
* **Регенеративные** вирусы делят свое тело на несколько частей и сохраняют их в разных местах жесткого диска. Соответственно эти части способна самостоятельно находить друг друга и собираться для регенерации тела вируса. Программа - антивирус обнаруживает и убивает лишь тело вируса, а части этого тела не заложены в антивирусной базе, так как являются измененными. От таких вирусов помогает целенаправленное низкоуровневое форматирование жесткого диска. Предварительно необходимо принять осторожные меры по сохранению информации.
* Хитрые вирусы прячутся не только от нас, но и от антивирусных программ. Эти "хамелеоны" **изменяют сами себя** с помощью самых хитрых и запутанных операций, применяя и текущие данные (время создания файла) и используя чуть ли не половину всего набора команд процессора. В определенный момент они, конечно же, по хитрому алгоритму превращаются в подлый вирус и начинают заниматься нашим компьютером. Это самый трудно обнаруживаемый тип вирусов, но некоторые антивирусные программы, такие как "Dr.Weber", способны с помощью так называемого эвристического анализа обнаруживать и обезвреживать и подобные вирусы.
* "**Невидимые**" вирусы чтобы предотвратить свое обнаружение применяют так называемый метод "Stelth". Он заключается в том, что вирус, находящийся в памяти резидентно, перехватывает обращения DOS (и тем самым прикладных программ) к зараженным файлам и областям диска и выдает их в исходном (незараженном) виде. Разумеется этот эффект наблюдается только на зараженном компьютере — на "чистом" компьютере изменения в файлах и загрузочных областях диска можно легко обнаружить. Но некоторые антивирусные программы могут обнаруживать вирусы - "невидимки" даже на зараженных компьютерах. Так, программа Adinf фирмы "Диалог-Наука" для этого выполняет чтение диска, не пользуясь услугами DOS, а программа AVSP фирмы "Диалог-МГУ" — "отключает" на время проверки вирус (последний метод работает не всегда).

Некоторые антивирусные программы (например, AVSP фирмы "Диалог-МГУ") используют для борьбы с вирусом свойство "невидимых" файловых вирусов "вылечивать" зараженные файлы. Они считывают (при работающем вирусе) информацию из зараженных файлов и записывают их на диск в файл или файлы, где эта информация хранится в неискаженном виде. Затем уже после загрузки с "чистой" дискеты, исполняемые файлы восстанавливаются в исходном виде.

* В последнее время получили распространение вирусы, изменяющую файловую систему на диске. Эти вирусы обычно называются **DIR**. Такие вирусы прячут свое тело в некоторый участок диска (обычно в последний кластер диска) и помечают его в таблице размещения файлов (FAT) как конец файла. Для всех .com- и .exe- файлов, содержащихся в соответствующих элементах каталога, указатели на первый участок файла заменяются ссылкой на участок диска, содержащий вирус, а правильный указатель в закодированном виде прячется в неиспользуемой части элемента каталога. По этому при запуске любой программы в память загружается вирус, после чего он остается в памяти резидентно, подключается к программам DOS для обработки файлов на диске и при всех обращениях к элементам каталога выдает правильные ссылки. Таким образом, при работающем вирусе файловая система кажется совершенно нормальной. При поверхностном осмотре на "чистом" компьютере зараженного диска также ничего странного не наблюдается. Разве что при попытке прочесть или скопировать с зараженной дискеты программные файлы из них будут прочтены или скопированы только 512 или 1024 байта, даже если файл гораздо длиннее. А при запуске любой исполняемой программы с зараженного таким вирусом диска этот диск, как по волшебству, начинает казаться исправным (неудивительно, ведь компьютер при этом становится зараженным).

При анализе на "чистом" компьютере с помощью программы ChkDsk или NDD файловая система зараженного DIR-вирусом диска кажется безнадежно испорченной. Так программа ChkDsk выдает кучу сообщений о пересечении файлов ("…cross linked on cluster…") и о цепочках потерянных кластеров ("…lost clusters found in … chains…"). Не следует исправлять эти ошибки программами ChkDsk или NDD — при этом диск окажется безнадежно испорченным. Именно так ведет себя вирус **OneHalf-3544**. Для исправления зараженных этими вирусами дисков надо пользоваться только специальными антивирусными программами, о которых будет рассказано далее.

Можно много рассуждать о классификации вирусов. Однако стоит знать, что никогда заранее неизвестно каким вирусом будет атакован ваш компьютер. Соответственно нужно учитывать все возможные типы и принимать все возможные меры для профилактики заражения. Так, например, для того, чтобы противостоять вирусу "Чернобыль" достаточно аппаратно отключить возможность перезаписывать Flash ПЗУ компьютера, а для предотвращения заражения загрузочными вирусами необходимо запретить загрузку компьютера с дискет. Но большинство вирусов не поддается правилам. Обычно вирусы пишутся как можно хитрее, и естественно, что они могут больше, чем представители одного класса. Т.е. они сочетают в себе достоинства каждого вида, превращаясь в гибриды. Сложность обнаружения и борьбы с гибридными вирусами возрастает.

**Глава 2. Профилактика и борьба с компьютерными вирусами**

**§ 1. Основ****ные метод****ы з****а****щ****иты** **от компьютерных вирусов**

Для защиты от вирусов можно использовать:

* Общие средства защиты информации, которые полезны также ка страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователей;
* 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 одних недостаточно. Необходимо применять специализированные программы для защиты от вирусов. Эти программы можно разделить на несколько видов:

1. **Программы - детекторы** позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов.
2. **Программы - доктора**, или фаги, "лечат" зараженные программы или диски, "выкусывая" из зараженных программ тело вируса, т.е. восстанавливая программу в том состоянии, в котором она находилась до заражения вирусом.
3. **Программы - ревизоры** сначала запоминают сведения о состоянии программ и системных областей дисков, а затем сравнивают их состояние с исходным. При выявлении несоответствий, об этом сообщается пользователю.
4. **Доктора - ревизоры** — это гибриды ревизоров и докторов, т.е. программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут автоматически вернуть их в исходное состояние.
5. **Программы - фильтры** 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 пользователю. Пользователь может разрешить или запретить выполнение соответствующей операции.
6. **Программы - вакцины**, или иммунизаторы, модифицируют программы и диски таким образом, что это не отражается на работе программ, но вирус, от которого производится вакцинация, считает эти программы и диски уже зараженными. Эти программы крайне неэффективны и далее не рассматриваются.

***Стратегия защиты от вирусов.*** Ни один тип антивирусных программ по отдельности не дает, к сожалению, полной защиты от вирусов. По этому наилучшей стратегией защиты от вирусов является многоуровневая, "эшелонная" оборона. Опишем структуру этой обороны.

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 (резидентные программы для защиты от вируса). Эти программы могут первыми сообщить о вирусной атаке и предотвратить заражение программ и диска.

Второй эшелон обороны составляют программы-ревизоры, программы-доктора и доктора-ревизоры. Ревизоры обнаруживают нападение даже тогда, когда вирус сумел "просочиться" через передний край обороны. Программы-доктора применяются для восстановления зараженных программ, если ее копий нет в архиве. Но они не всегда лечат правильно. Доктора-ревизоры обнаруживают нападение вируса и лечат зараженные файлы, причем контролируют правильность лечения.

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.

И наконец, в "стратегическом резерве" находятся архивные копии информации и "эталонные" дискеты с программными продуктами. Они позволяют восстановить информацию при ее повреждении на жестком диске.

**§ 2. Программ****ы - дете****кто****ры и д****октора**

В большинстве случаев для обнаружения вируса, заразившего Ваш компьютер, можно найти уже разработанные программы-детекторы. 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 режим лечения или уничтожения зараженных файлов.

Следует отметить, программа - детектор может обнаруживать только те вирусы, которые ей известны (т.е. занесены в антивирусную базу данных этой программы). Например программа **AVP** Касперского способна обнаружить на 10 Февраля 2000 года **33556** вирусов. Ниже приведено диалоговое окно этой антивирусной программы. Все в ней отличается удобным и понятным интерфейсом. Программа выполнена для операционной системы Windows'95/'98/NT/3.11, что позволяет ей работать параллельно с другими приложениями.

Рис.1

 Некоторые программы, такие как **Dr.Weber,** могут с помощью эвристического анализа находить модифицированные вирусы. Ниже приведено диалоговое окно антивирусной программы Dr.Weber. Программа написана под операционную систему MS DOS.

Рис. 2

 Тем не менее, невозможно разработать такую программу, которая могла бы обнаруживать любой заранее неизвестный вирус. Многие антивирусные программы способны находить зараженные файлы даже внутри архивов

***Лечение от вирусов***. Большинство программ - детекторов имеют также и функцию "доктора", т.е. они пытаются вернуть зараженные файлы и 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 количества вирусов, по этому они быстро устаревают. Но некоторые программы могут обучаться не только способам обнаружения, но и способам лечения от новых вирусов. К таким программам относится **AVSP** фирмы "Диалог-МГУ". Другой перспективный подход — восстановление файлов на основе заранее сохраненной информации об их состоянии. Этим занимаются программы - ревизоры и доктора - ревизоры.

**§ 3. Действия пр****и зар****ажен****и****и вирусом**

При заражении компьютера вирусом (или подозрении на это) важно соблюдать четыре правила.

1. Прежде всего не надо торопиться и принимать опрометчивых решений. Как говорится, "семь раз отмерь, один раз отрежь" — непродуманные действия могут привести не только к потере части файлов, которые можно было бы восстановить, но и к повторному заражению компьютера.
2. Тем не менее одно действие должно быть выполнено немедленно, — надо выключить компьютер, чтобы вирус не продолжал свою работу.
3. Все действия по обнаружению вида заражения и л лечению компьютера следует выполнять только после перезагрузки компьютера с защищенной от записи "эталонной" дискеты с операционной системой. При этом следует пользоваться исполняемыми файлами находящимися только на защищенных от записи "эталонных" дискетах. Несоблюдение этого правила может привести к очень тяжелым последствиям, поскольку при загрузке ОС или запуске программы с зараженного диска в компьютере может быть активирован вирус, а при работающем вирусе лечение компьютера будет бессмысленным, так как оно будет сопровождаться дальнейшим заражением дисков и программ.
4. Если Вы не обладаете достаточными опытом и знаниями для лечения компьютера, попросите о помощи более опытных коллег или специалистов.

***Лечение компьютера***. Рассмотрим случай когда вирус уже успел заразить или испортить какие-то файлы на дисках компьютера. При этом надо выполнить следующие действия.

1. Перезагрузить ОС (Операционную Систему) с заранее подготовленной эталонной дискеты. Эта дискета, как и другие дискеты, используемые при ликвидации последствий заражения компьютерным вирусом, должна быть защищена от записи. Заметим, что перезагрузку нельзя выполнять , используя комбинацию клавиш <Ctrl><Alt><Del>, так как некоторые вирусы способны анализировать это прерывание клавиатуры и продолжать работать. Они могут сымитировать перезагрузку компьютера, а могут ответить вам каким-то жестоким образом. Для перезагрузки нужно использовать кнопку "RESET" на системном блоке или вообще перезапустить питание.
2. Необходимо проверить правильность конфигурации компьютера при начальной загрузке компьютера.
3. Сначала необходимо запустить программу - детектор для определения типа вируса и зараженных файлов.
4. Далее нужно поочередно обезвредить все диски, которые могли подвергнуться заражению. Если жесткий диск разделен на несколько логических дисков, то при перезагрузке с дискеты будет виден только логический диск, с которого стартует ОС. Необходимо прежде всего очистить от заражения его, а затем, перегрузившись с жесткого диска, заняться его остальными разделами.
5. Теперь, когда известно, что вирусов типа DIR на диске нет или они успешно вылечены можно проверить целостность файловой системы и поверхности диска программой NDD или ChkDsk. Если повреждения FAT (файловой системы) значительные, то целесообразно попробовать сделать копии необходимой информации, после чего отформатировать диск. При незначительных повреждениях можно попробовать восстановить диск также применяя программу DiskEdit из комплекса Norton Utilities.
6. Если до заражения использовалась программа - ревизор, можно запустить ее для диагностики изменений в файлах.
7. Если вы не уверены в своих архивных копиях, проверьте их на наличие вируса.
8. Удалить с диска все файлы, которые были изменены и имеют копии на других дисках. Нельзя оставлять на диске .exe и .com файлы которые по мнению ревизора были изменены. Оставлять их можно только в исключительных случаях.
9. Если обрабатываемый диск системный, то его систему стоит обновить с "эталонной" дискеты командой SYS.
10. Файлы, которые доктор не смог восстановить следует уничтожить.
11. С помощью архивных копий следует восстановить файлы, размещавшиеся на диске.
12. Если имеется хорошая программа - фильтр, целесообразно некоторое время поработать с ней.

**§ 4. Профилактика пр****оти****в зара****жени****я вирусом**

В настоящем разделе описываются меры, которые позволяют уменьшить вероятность заражения компьютера вирусом, а также свести к минимуму ущерб от заражения вирусом, если оно все таки произойдет. Нет необходимости использовать все описываемые средства для профилактики портив заражения вирусом.

Копирование информации и разграничение доступа:

1. Неплохо бы иметь и при необходимости обновлять архивные и эталонные копии используемых Вами пакетов программ и данных. Перед архивацией данных целесообразно проверить их на наличие вируса.
2. Целесообразно так же скопировать на дискеты служебную информацию вашего диска (FAT, загрузочные сектора) и CMOS (энергонезависимая память компьютера). Копирование и восстановление подобной информации можно выполнить с помощью программы Rescue программного комплекса Norton Utilities.
3. Следует устанавливать защиту от записи на архивных дискетах.
4. Не следует заниматься нелицензионным и нелегальным копированием программного обеспечения с других компьютеров. На них может быть вирус.
5. Все данные, поступающие извне, стоит проверять на вирусы, особенно файлы, "скачанные" из Интернета.
6. Надо заблаговременно подготовить восстанавливающий пакет на дискетах с защитой от записи.
7. На время обычной работы, не связанной с восстановлением компьютера, стоит отключить загрузку с дискеты. Это предотвратит заражение загрузочным вирусом.
8. Используйте программы - фильтры для раннего обнаружения вирусов.
9. Периодически проверяйте диск программами -детекторами или докторами - детекторами или ревизорами для обнаружения возможных провалов в обороне.
10. Обновляйте базу антивирусных программ.
11. Не допускайте к компьютеру сомнительных пользователей.

**Закл****ю****че****ние****.**

В заключении хотелось бы предостеречь от слишком рьяной борьбы с компьютерными вирусами. Не стоит переоценивать возможностей этих подлых программ. Например, очень неразумным будет распоряжение начальника отформатировать все жесткие диски на компьютерах в отделе только из-за того, что на одном из них было обнаружено **подозрение** на вирус такой-то. Это приведет к неоправданной потере информации и сильной потери времени и сил, что, по нанесенному ущербу, будет больше, чем смог бы сделать вирус. Ежедневный запуск полного сканирования жесткого диска на наличие вирусов так же не блестящий шаг в профилактике заражений. Не превращайте компьютер в неприступную крепость, вооруженную до зубов, а то может не хватить ресурсов для выполнения необходимых задач. Если все же вам захочется затруднить задачу для вирусов, установите на вашем компьютере операционную систему **WindowsNT**, эта оболочка по своей архитектуре не допускает прямых обращений к устройствам даже для драйверов. Единственный цивилизованный способ защиты от вирусов я вижу в соблюдении профилактических мер предосторожности при работе на компьютере. А кроме того, даже если вирус все-таки проник на компьютер, это не повод для паники. Методы борьбы с ним описаны в предыдущей главе. Не стесняйтесь прибегать к помощи специалистов для борьбы с компьютерным вирусом, если вы не чувствуете уверенности в себе.