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 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 также, 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 резидентно, т.е. до перезагрузки DOS, в памяти компьютера и время от времени заражает программы и выполняет вредные действия на компьютере.

Компьютерный вирус может испортить, т.е. изменить ненадлежащим образом, любой файл на имеющих 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 без данных, таблицы табличных процессоров и другие аналогичные файлы не могут быть заражены вирусом, он может их только испортить.

------- ПРОЯВЛЕНИЕ НАЛИЧИЯ ВИРУСА В РАБОТЕ НА ПЭВМ -------

Все действия вируса могут выполняться достаточно быстро и без выдачи каких-либо сообщений, поэтому пользователю очень трудно заметить, что в компьютере происходит что-то необычное.

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

\* некоторые программы перестают работать или начинают работать неправиль но;

\* 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) программ являются зараженными вирусом, а некоторые файлы и диски - испорченными. Более того, зараженные программы с одного компьютера могли быть перенесены с помощью дискет или по локальной сети на другие компьютеры.

Некоторые виды вирусов ведут себя еще более коварно. Они вначале незаметно заражают большое число программ или дисков, а потом причняют очень серьезные повреждения, например формируют весь жесткий диск на компьютере. А бывают вирусы, которые стараются вести себя как можно более незаметно, но понемногу и постепенно портят данные на жестком диске компьютера.

Таким образом, если не предпринимать мер по защите от вируса, то последствия заражения компьютера могут быть очень серьезными.

-------- РАЗНОВИДНОСТИ КОМПЬЮТЕРНЫХ ВИРУСОВ --------

Каждая конкретная разновидность вируса может заражать только один или два типа файлов. Чаще всего встречаются вирусы, заражающие исполнимые файлы. Некоторые вирусы заражают и файлы, и загрузочные области дисков. Вирусы, заражающие драйверы устройств, встречаются крайне редко, обычно такие вирусы умеют заражать и исполнимые файлы.

В последнее время получили распространение вирусы нового типа - вирусы, имеющие 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.

Чтобы предотвратить свое обнаружение, некоторые вирусы применяют довольно хит-

рые приемы маскировки. Я расскажу о двух из них: "невидимых" и самомодифицирую-

щихся вирусах.

"НЕВИДИМЫЕ" вирусы. Многие резидентные вирусы (и файловые, и загрузочные)

предотвращают свое обнаружение тем, что перехватывают обращения DOS (и тем самым

прикладных программ) к зараженным файлам и областям диска и выдают 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.

САМОМОДИФИЦИРУЮЩИЕСЯ вирусы. Другой способ, применяемый вирусами для того,

чтобы укрыться от обнаружения, - модификация своего тела. Многие вирусы хранят

большую часть своего тела в закодированном виде, чтобы с помощью дизассемблеров

нельзя было разобраться в механизме их работы. Самомодифицирующиеся вирусы испо-

льзуют этот прием и часто меняют параметры этой кодировки, а кроме того, изменя-

ют и свою стартовую часть, которая служит для раскодировки остальных команд ви-

руса. Таким образом, в теле подобного вируса не имеется ни одной постоянной це-

почки байтов, по которой можно было бы идентифицировать вирус. Это, естествен-

но, затрудняет нахождение таких вирусов программами-детекторами.

-------- 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 ошибоч-

ных действий пользователя;

\* профилактические меры, позволяющие уменьшить вероятность заражения ви-

русом;

\* специализированные программы для защиты от вирусов.

Общие средства защиты информации полезны не только для защиты от вирусов. Име-

ются 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 вируса-

ми, неправильно работающими программами и ошибочными действиями пользо-

вателей.

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 ви-

дов: детекторы, доктора (фаги), ревизоры, доктора-ревизоры, фильтры и вакцины

(иммунизаторы).

ПРОГРАММЫ-ДЕТЕКТОРЫ позволяют обнаруживать файлы, зараженные одним из неско-

льких известных вирусов. Эти программы проверяют, имеется ли в файлах на указан-

ном 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 ви-

русы, которые ей "известны". Программа Scan фирмы McAfee Associates и Aidstest

Д.Н.Лозинского позволяют обнаруживать около 1000 вирусов, но всего их более пяти

тысяч! Некоторые программы-детекторы, например Norton AntiVirus или AVSP фирмы

"Диалог-МГУ", могут настраивать на новые типы вирусов, им необходимо лишь ука-

зать комбинации байтов, присущие этим вирусам. Тем не мение невозможно разрабо-

тать такую программу, которая могла бы обнаруживать любой заранее неизвестный

вирус.

Таким образом, из того, что программа не опознается детекторами как заражен-

ная, не следует, что она здорова - в ней могут сидеть какой-нибудь новый вирус

или слегка модифицированная версия старого вируса, неизвестные программам-детек-

торам.

Многие программы-детекторы (в том числе и Aidstest) не умеют обнаруживать за-

ражение "невидимыми" вирусами, если такой вирус активен в памяти компьютера. Де-

ло 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.

Некоторые детекторы, скажем, ADinf фирмы "Диалог-Наука", умеют ловить "неви-

димые" вирусы, даже когда они активны. Для этого они читают диск, не используя

вызовы DOS. Правда, этот метод работает не на всех дисководах.

Большинство программ-детекторов имеют функцию "доктора", т.е. они пытаются

вернуть зараженные файлы или области диска в их исходное состояние. Те файлы, ко-

торые не удалось восстановить, как правило, делаются неработоспособными или уда-

ляются.

Большинство программ-докторов умеют "лечить" только от некоторого фиксирован-

ного 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 опе-

рационной системы, необходимо включить команду запуска программы-ревизора в ко-

мандный файл AUTOEXEC.BAT. Это позволяет обнаружить заражение компьютерным виру-

сом, 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 про-

граммы, 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. Понятно, что в нормальной ситу-

ации такие изменения практически никогда не встречаются, поэтому программа-реви-

зор, зафиксировав факт таких изменений, может с уверенностью сообщить, что они

вызваны именно вирусом.

Следует заметить, что многие программы-ревизоры не умеют обнаруживать зараже-

ние "невидимыми" вирусами, если такой вирус активен в памяти компьютера. Но неко-

торые программы-ревизоры, например ADinf фирмы "Диалог-Наука", все же умеют де-

лать это, не используя вызовы DOS для чтения диска (правда, они работают не на

всех дисководах).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 некото-

рых "хитрых" вирусов все это бесполезно.

Для проверки того, не изменился ли файл, некоторые программы-ревизоры про-

веряют длину файла. Но эта проверка недостаточна - некоторые вирусы не изменяют

длину зараженных файлов. Более надежная проверка - прочесть весь файл и вычис-

лить его контрольную сумму. Изменить файл так, чтобы его контрольная сумма оста-

лась 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 фай-

лов.

Существуют также ПРОГРАММЫ-ФИЛЬТРЫ, которые располагаются резидентно в опера-

тивной 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 соответ-

ствующей 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.

Ни один тип антивирусных программ по отдельности не дает полной защиты от

вирусов. Лучшей стратегией защиты от вирусов является многоуровневая, "эшелони-

рованная" оборона. Опишу 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. Эти программы могут пер-

выми сообщить о работе вируса и предотвратить заражение программ и дисков.

Второй эшелон обороны составляют программы-ревизоры, программы-доктора и док-

тора-ревизоры.

Самый глубокй эшелон обороны - это средства разграничения доступа. Они не

позволяют вирусам и неверно работающим программам, даже если они проникли в ком-

пьютер, испортить важные данные.

В "стратегическом резерве" находятся архивные копии информации. Это позволяет

восстановить информацию при её повреждении.

Это неформальное описание позволяет лучше понять методику применения антиви -

русных средств.

---------- ДЕЙСТВИЯ ПРИ ЗАРАЖЕНИИ ВИРУСОМ ----------

При заражении компьютера вирусом (или при подозрении на это) важно соблюдать

4-е правила:

1) Прежде всего не надо торопиться и принимать опрометчивых решений.

Непродуманные действия могут привести не только к потери части файлов, но к пов-

торному заражению компьютера.

2) Надо немедленно выключить компьютер, чтобы вирус не продолжал

своих разрушительных действий.

3) Все действия по обнаружению вида заражения и лечению компьютера

следует выполнять при загрузке компьютера с защищенной от записи дискеты с ОС

(обязательное правило).

4) Если Вы не обладаете достаточными знаниями и опытом для лечения

компьютера, попросите помочь более опытных коллег.