## Методы и средства защиты программ от компьютерных вирусов.

###### **3.1.1. Общая характеристика и классификация компьютерных вирусов**

Под компьютерным вирусом (или просто вирусом) понимается автономно функционирующая программа, обладающая способностью к самостоятельному внедрению в тела других программ и последующему самовоспроизведению и самораспространению в информационно-вычислительных сетях и отдельных ЭВМ [[3](http://citforum.ru/security/articles/kazarin/4.shtml#3),[5](http://citforum.ru/security/articles/kazarin/4.shtml#5),[16](http://citforum.ru/security/articles/kazarin/4.shtml#16),[59](http://citforum.ru/security/articles/kazarin/4.shtml#59),[65](http://citforum.ru/security/articles/kazarin/4.shtml#65)]. Предшественниками вирусов принято считать так называемые троянские программы, тела которых содержат скрытые последовательности команд (модули), выполняющие действия, наносящие вред пользователям. Наиболее распространенной разновидностью троянских программ являются широко известные программы массового применения (редакторы, игры, трансляторы и т.д.), в которые встроены так называемые "логические бомбы", срабатывающие по наступлении некоторого события. Следует отметить, что троянские программы не являются саморазмножающимися.

Принципиальное отличие вируса от троянской программы состоит в том, что вирус после его активизации существует самостоятельно (автономно) и в процессе своего функционирования заражает (инфицирует) программы путем включения (имплантации) в них своего текста. Таким образом, компьютерный вирус можно рассматривать как своеобразный "генератор троянских программ". Программы, зараженные вирусом, называются вирусоносителями.

Заражение программы, как правило, выполняется таким образом, что-бы вирус получил управление раньше самой программы. Для этого он либо встраивается в начало программы, либо имплантируется в ее тело так, что первой командой зараженной программы является безусловный переход на компьютерный вирус, текст которой заканчивается аналогичной командой безусловного перехода на команду вирусоносителя, бывшую первой до заражения. Получив управление, вирус выбирает следующий файл, заражает его, возможно, выполняет какие-либо другие действия, после чего отдает управление вирусоносителю.

"Первичное" заражение происходит в процессе поступления инфицированных программ из памяти одной машины в память другой, причем в качестве средства перемещения этих программ могут использоваться как магнитные носители (дискеты), так и каналы вычислительных сетей. Вирусы, использующие для размножения сетевые средства, принято называть сетевыми. Цикл жизни вируса обычно включает следующие периоды: внедрение, инкубационный, репликации (саморазмножения) и проявления. В течение инкубационного периода вирус пассивен, что усложняет задачу его поиска и нейтрализации. На этапе проявления вирус выполняет свойственные ему целевые функции, например необратимую коррекцию информации в компьютере или на магнитных носителях.

Физическая структура компьютерного вируса достаточно проста. Он состоит из головы и, возможно, хвоста. Под головой вируса понимается его компонента, получающая управление первой. Хвост - это часть вируса, расположенная в тексте зараженной программы отдельно от головы. Вирусы, состоящие из одной головы, называют несегментированными, тогда как вирусы, содержащие голову и хвост - сегментированными.

Наиболее существенные признаки компьютерных вирусов позволяют провести следующую их классификацию. По режиму функционирования:

* резидентные вирусы - вирусы, которые после активизации посто-янно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам;
* транзитные вирусы - вирусы, которые выполняются только в момент запуска зараженной программы.

По объекту внедрения:

* файловые вирусы - вирусы, заражающие файлы с программами;
* загрузочные (бутовые) вирусы - вирусы, заражающие программы, хранящиеся в системных областях дисков.

В свою очередь файловые вирусы подразделяются на вирусы, заражающие:

* исполняемые файлы;
* командные файлы и файлы конфигурации;
* составляемые на макроязыках программирования, или файлы, содержащие макросы (макровирусы);
* файлы с драйверами устройств;
* файлы с библиотеками исходных, объектных, загрузочных и оверлейных модулей, библиотеками динамической компоновки и т.п.

Загрузочные вирусы подразделяются на вирусы, заражающие:

* системный загрузчик, расположенный в загрузочном секторе дискет и логических дисков;
* внесистемный загрузчик, расположенный в загрузочном секторе жестких дисков.

По степени и способу маскировки:

* вирусы, не использующие средств маскировки;
* stealth-вирусы - вирусы, пытающиеся быть невидимыми на основе контроля доступа к зараженным элементам данных;
* вирусы-мутанты (MtE-вирусы) - вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса.

MtE-вирусы делятся на

* обычные вирусы-мутанты, в разных копиях которых различаются только зашифрованные тела, а расшифровщики совпадают;
* полиморфные вирусы, в разных копиях которых различаются не только зашифрованные тела, но их дешифровщики.

Наиболее распространенные типы вирусов характеризуются следующими основными особенностями.

Файловый транзитный вирус целиком размещается в исполняемом файле, в связи с чем он активизируется только в случае активизации вирусоносителя, а по выполнении необходимых действий возвращает управление самой программе. При этом выбор очередного файла для заражения осуществляется вирусом посредством поиска по каталогу. Файловый резидентный вирус отличается от нерезидентной логической структуры и общим алгоритмом функционирования. Резидентный вирус состоит из так называемого инсталлятора и программ обработки прерываний. Инсталлятор получает управление при активизации вирусоносителя и инфицирует оперативную память путем размещения в ней управляющей части вируса и замены адресов в элементах вектора прерываний на адреса своих программ, обрабатывающих эти прерывания. На так называемой фазе слежения, следующей за описанной фазой инсталляции, при возникновении какого-либо прерывания управление получает соответствующая подпрограмма вируса. В связи с существенно более универсальной по сравнению с нерезидентными вирусами общей схемой функционирования, резидентные вирусы могут реализовывать самые разные способы инфицирования.

Наиболее распространенными способами являются инфицирование запускаемых программ, а также файлов при их открытии или чтении. Отличительной особенностью последних является инфицирование загрузочного сектора (бут-сектора) магнитного носителя. Голова бутового вируса всегда находится в бут-секторе (единственном для гибких дисков и одном из двух - для жестких), а хвост - в любой другой области носителя. Наиболее безопасным для вируса способом считается размещение хвоста в так называемых псевдосбойных кластерах, логически исключенных из числа доступных для использования.

Существенно, что хвост бутового вируса всегда содержит копию оригинального (исходного) бут-сектора. Механизм инфицирования, реализуемый бутовыми вирусами, например, при загрузке MS DOS, таков. При загрузке операционной системы с инфицированного диска вирус, в силу своего положения на нем (независимо от того, с дискеты или с винчестера производится загрузка), получает управление и копирует себя в оперативную память. Затем он модифицирует вектор прерываний таким образом, чтобы прерывание по обращению к диску обрабатывались собственным обработчиком прерываний вируса, и запускает загрузчик операционной системы. Благодаря перехвату прерываний бутовые вирусы могут реализовывать столь же широкий набор способов инфицирования и целевых функций, сколь и файловые резидентные вирусы.

Stealth-вирусы пользуются слабой защищенностью некоторых операционных систем и заменяют некоторые их компоненты (драйверы дисков, прерывания) таким образом, что вирус становится невидимым (прозрачным) для других программ. Для этого заменяются функции DOS таким образом, что для зараженного файла подставляются его оригинальная копия и содержание, каким они были до заражения.

Полиморфные вирусы содержат алгоритм порождения дешифровщиков (с размером порождаемых дешифровщиков от 0 до 512 байтов) непохожих друг на друга. При этом в дешифровщиках могут встречаться практически все команды процессора Intel и даже использоваться некоторые специфические особенности его реального режимы функционирования.

Макровирусы распространяются под управлением прикладных программ, что делает их независимыми от операционной системы. Подавляющее число макровирусов функционируют под управлением системы Microsoft Word for Windows. В то же время, известны макровирусы, рабо-тающие под управлением таких приложений как Microsoft Exel for Win-dows, Lotus Ami Pro, Lotus 1-2-3, Lotus Notes, в операционных системах фирм Microsoft и Apple .

Сетевые вирусы, называемые также автономными репликативными программами, или, для краткости, репликаторами, используют для размножения средства сетевых операционных систем. Наиболее просто реализуется размножение в тех случаях, когда сетевыми протоколами предусмотрен обмен программами. Однако, размножение возможно и в тех случаях, когда указанные протоколы ориентированы только на обмен сообщениями. Классическим примером реализации процесса размножения с использованием только стандартных средств электронной почты является уже упоминаемый репликатор Морриса. Текст репликатора передается от одной ЭВМ к другой как обычное сообщение, постепенно заполняющее буфер, выделенный в оперативной памяти ЭВМ-адресата. В результате переполнения буфера, инициированного передачей, адрес возврата в программу, вызвавшую программу приема сообщения, замещается на адрес самого буфера, где к моменту возврата уже находится текст вируса.

Тем самым вирус получает управление и начинает функционировать на ЭВМ-адресате.

"Лазейки", подобные описанной выше и обусловленные особенностями реализации тех или иных функций в программном обеспечении, являются объективной предпосылкой для создания и внедрения репликаторов злоумышленниками. Эффекты, вызываемые вирусами в процессе реализации ими целевых функций, принято делить на следующие группы:

* искажение информации в файлах либо таблице размещения файлов (FAT-таблице), которое может привести к разрушению файловой системы в целом;
* имитация сбоев аппаратных средств;
* создание звуковых и визуальных эффектов, включая, например, отображение сообщений, вводящих оператора в заблуждение или затрудняющих его работу;
* инициирование ошибок в программах пользователей или операционной системы.

Теоретически возможно создание "вирусных червей" - разрушающих программ, которые незаметно перемещаются между узлами вычислительной сети, не нанося никакого вреда до тех пор, пока не доберутся до целевого узла. В нем программа размещается и перестает размножаться.

Поскольку в будущем следует ожидать появления все более и более скрытых форм компьютерных, уничтожение очагов инфекции в локальных и глобальных сетях не станет проще. Время компьютерных вирусов "общего назначения" уходит в прошлое.

###### **3.1.2. Общая характеристика средств нейтрализации компьютерных вирусов**

Наиболее распространенным средством нейтрализации ПВ являются антивирусные программы (антивирусы). Антивирусы, исходя из реализованного в них подхода к выявлению и нейтрализации вирусов, принято делить на следующие группы:

* детекторы;
* фаги;
* вакцины;
* прививки;
* ревизоры;
* мониторы.

Детекторы обеспечивают выявление вирусов посредством просмотра исполняемых файлов и поиска так называемых сигнатур - устойчивых последовательностей байтов, имеющихся в телах известных вирусов. Наличие сигнатуры в каком-либо файле свидетельствует о его заражении соответствующим вирусом. Антивирус, обеспечивающий возможность поиска различных сигнатур, называют полидетектором.

Фаги выполняют функции, свойственные детекторам, но, кроме того, "излечивают" инфицированные программы посредством "выкусывания" вирусов из их тел. По аналогии с полидетекторами, фаги, ориентированные на нейтрализацию различных вирусов, именуют полифагами.

В отличие от детекторов и фагов, вакцины по своему принципу действия подобны вирусам. Вакцина имплантируется в защищаемую программу и запоминает ряд количественных и структурных характеристик последней. Если вакцинированная программа не была к моменту вакцинации инфицированной, то при первом же после заражения запуске произойдет следующее. Активизация вирусоносителя приведет к получению управления вирусом, который, выполнив свои целевые функции, передаст управление вакцинированной программе. В последней, в свою очередь, сначала управление получит вакцина, которая выполнит проверку соответствия запомненных ею характеристик аналогичным характеристикам, полученным в текущий момент. Если указанные наборы характеристик не совпадают, то делается вывод об изменении текста вакцинированной программы вирусом. Характеристиками, используемыми вакцинами, могут быть длина программы, ее контрольная сумма и т.д.

Принцип действия прививок основан на учете того обстоятельства, что любой вирус, как правило, помечает инфицируемые программы каким-либо признаком с тем, чтобы не выполнять их повторное заражение. В ином случае имело бы место многократное инфицирование, сопровождаемое существенным и поэтому легко обнаруживаемым увеличением объема зараженных программ. Прививка, не внося никаких других изменений в текст защищаемой программы, помечает ее тем же признаком, что и вирус, который, таким образом, после активизации и проверки наличия указанного признака, считает ее инфицированной и "оставляет в покое".

Ревизоры обеспечивают слежение за состоянием файловой системы, используя для этого подход, аналогичный реализованному в вакцинах. Программа-ревизор в процессе своего функционирования выполняет применительно к каждому исполняемому файлу сравнение его текущих характеристик с аналогичными характеристиками, полученными в ходе предшествующего просмотра файлов. Если при этом обнаруживается, что, согласно имеющейся системной информации, файл с момента предшествующего просмотра не обновлялся пользователем, а сравниваемые наборы характеристик не совпадают, то файл считается инфицированным. Характеристики исполняемых файлов, получаемые в ходе очередного просмотра, запоминаются в отдельном файле (файлах), в связи с чем увеличения длин исполняемых файлов, имеющего место при вакцинации, в данном случае не происходит. Другое отличие ревизоров от вакцин состоит в том, что каждый просмотр исполняемых файлов ревизором требует его повторного запуска.

Монитор представляет собой резидентную программу, обеспечивающую перехват потенциально опасных прерываний, характерных для вирусов, и запрашивающую у пользователей подтверждение на выполнение операций, следующих за прерыванием. В случае запрета или отсутствия подтверждения монитор блокирует выполнение пользовательской программы. Антивирусы рассмотренных типов существенно повышают вирусозащищенность отдельных ПЭВМ и вычислительных сетей в целом, однако, в связи со свойственными им ограничениями, естественно, не являются панацеей. В работе приведены основные недостатки при использовании антивирусов.

В связи с этим необходима реализация альтернативных подходов к нейтрализации вирусов: создание операционных систем, обладающих высокой вирусозащищенностью по сравнению с наиболее "вирусодружественной" MS DOS, разработка аппаратных средств защиты от вирусов и соблюдение технологии защиты от вирусов.

###### 3.1.3. Классификация методов защиты от компьютерных вирусов

Проблему защиты от вирусов необходимо рассматривать в общем контексте проблемы защиты информации от несанкционированного доступа и технологической и эксплуатационной безопасности ПО в целом. Основной принцип, который должен быть положен в основу разработки технологии защиты от вирусов, состоит в создании многоуровневой распределенной системы защиты, включающей:

* регламентацию проведения работ на ПЭВМ,
* применение программных средств защиты,
* использование специальных аппаратных средств.

При этом количество уровней защиты зависит от ценности информации, которая обрабатывается на ПЭВМ. Для защиты от компьютерных вирусов в настоящее время используются следующие методы: Архивирование. Заключается в копировании системных областей магнитных дисков и ежедневном ведении архивов измененных файлов.

Архивирование является одним из основных методов защиты от вирусов. Остальные методы защиты дополняют его, но не могут заменить полностью.

Входной контроль. Проверка всех поступающих программ детекторами, а также проверка длин и контрольных сумм вновь поступающих программ на соответствие значениям, указанным в документации. Большинство известных файловых и бутовых вирусов можно выявить на этапе входного контроля. Для этой цели используется батарея (несколько последовательно запускаемых программ) детекторов. Набор детекторов достаточно широк, и постоянно пополняется по мере появления новых вирусов. Однако при этом могут быть обнаружены не все вирусы, а только распознаваемые детектором. Следующим элементом входного контроля является контекстный поиск в файлах слов и сообщений, которые могут принадлежать вирусу (например, Virus, COMMAND.COM, Kill и т.д.). Подозрительным является отсутствие в последних 2-3 килобайтах файла текстовых строк - это может быть признаком вируса, который шифрует свое тело.

Рассмотренный контроль может быть выполнен с помощью специальной программы, которая работает с базой данных "подозрительных" слов и сообщений, и формирует список файлов для дальнейшего анализа. После проведенного анализа новые программы рекомендуется несколько дней эксплуатировать в карантинном режиме. При этом целесообразно использовать ускорение календаря, т.е. изменять текущую дату при повторных запусках программы. Это позволяет обнаружить вирусы, срабатывающие в определенные дни недели (пятница, 13 число месяца, воскресенье и т.д.).

Профилактика. Для профилактики заражения необходимо организовать раздельное хранение (на разных магнитных носителях) вновь поступающих и ранее эксплуатировавшихся программ, минимизация периодов доступности дискет для записи, разделение общих магнитных носителей между конкретными пользователями.

Ревизия. Анализ вновь полученных программ специальными средствами (детекторами), контроль целостности перед считыванием информации, а также периодический контроль состояния системных файлов.

Карантин. Каждая новая программа проверяется на известные типы вирусов в течение определенного промежутка времени. Для этих целей целесообразно выделить специальную ПЭВМ, на которой не проводятся другие работы. В случае невозможности выделения ПЭВМ для карантина программного обеспечения, для этой цели используется машина, отключенная от локальной сети и не содержащая особо ценной информации.

Сегментация. Предполагает разбиение магнитного диска на ряд логических томов (разделов), часть из которых имеет статус READ\_ONLY (только чтение). В данных разделах хранятся выполняемые программы и системные файлы. Базы данных должны хранится в других секторах, отдельно от выполняемых программ. Важным профилактическим средством в борьбе с файловыми вирусами является исключение значительной части загрузочных модулей из сферы их досягаемости. Этот метод называется сегментацией и основан на разделении магнитного диска (винчестера) с помощью специального драйвера, обеспечивающего присвоение отдельным логическим томам атрибута READ\_ONLY (только чтение), а также поддерживающего схемы парольного доступа. При этом в защищенные от записи разделы диска помещаются исполняемые программы и системные утилиты, а также системы управления базами данных и трансляторы, т.е. компоненты ПО, наиболее подверженные опасности заражения. В качестве такого драйвера целесообразно использовать программы типа ADVANCED DISK MANAGER (программа для форматирования и подготовки жесткого диска), которая не только позволяет разбить диск на разделы, но и организовать доступ к ним с помощью паролей. Количество используемых логических томов и их размеры зависят от решаемых задач и объема винчестера. Рекомендуется использовать 3 - 4 логических тома, причем на системном диске, с которого выполняется загрузка, следует оставить минимальное количество файлов (системные файлы, командный процессор, а также программы - ловушки).

Фильтрация. Заключается в использовании программ - сторожей, для обнаружения попыток выполнить несанкционированные действия.

Вакцинация. Специальная обработка файлов и дисков, имитирующая сочетание условий, которые используются некоторым типом вируса для определения, заражена уже программа или нет.

Автоконтроль целостности. Заключается в использовании специальных алгоритмов, позволяющих после запуска программы определить, были ли внесены изменения в ее файл.

Терапия. Предполагает дезактивацию конкретного вируса в зараженных программах специальными программами (фагами). Программыфаги "выкусывают" вирус из зараженной программы и пытаются восстановить ее код в исходное состояние (состояние до момента заражения). В общем случае технологическая схема защиты может состоять из следующих этапов:

* входной контроль новых программ;
* сегментация информации на магнитном диске;
* защита операционной системы от заражения;
* систематический контроль целостности информации.

Необходимо отметить, что не следует стремиться обеспечить глобальную защиту всех файлов, имеющихся на диске. Это существенно затрудняет работу, снижает производительность системы и, в конечном счете, ухудшает защиту из-за частой работы в открытом режиме. Анализ показывает, что только 20-30% файлов должно быть защищено от записи.

При защите операционной системы от вирусов необходимо правильное размещение ее и ряда утилит, которое можно гарантировать, что после начальной загрузки операционная система еще не заражена резидентным файловым вирусом. Это обеспечивается при размещении командного процессора на защищенном от записи диске, с которого после начальной загрузки выполняется копирование на виртуальный (электронный) диск. В этом случае при вирусной атаке будет заражен дубль командного процессора на виртуальном диске. При повторной загрузке информация на виртуальном диске уничтожается, поэтому распространение вируса через командный процессор становится невозможным.

Кроме того, для защиты операционной системы может применяться нестандартный командный процессор (например, командный процессор 4DOS, разработанный фирмой J.P.Software), который более устойчив к заражению. Размещение рабочей копии командного процессора на виртуальном диске позволяет использовать его в качестве программы-ловушки. Для этого может использоваться специальная программа, которая периодиче-ски контролирует целостность командного процессора, и информирует о ее нарушении. Это позволяет организовать раннее обнаружение факта вирусной атаки.

В качестве альтернативы MS DOS было разработано несколько операционных систем, которые являются более устойчивыми к заражению. Из них следует отметить DR DOS и Hi DOS. Любая из этих систем более "вирусоустойчива", чем MS DOS. При этом, чем сложнее и опаснее вирус, тем меньше вероятность, что он будет работать на альтернативной операционной системе.

Анализ рассмотренных методов и средств защиты показывает, что эффективная защита может быть обеспечена при комплексном использовании различных средств в рамках единой операционной среды. Для этого необходимо разработать интегрированный программный комплекс, поддерживающий рассмотренную технологию защиты. В состав программного комплекса должны входить следующие компоненты.

* Каталог детекторов. Детекторы, включенные в каталог, должны запускаться из операционной среды комплекса. При этом должна быть обеспечена возможность подключения к каталогу новых детекторов, а также указание параметров их запуска из диалоговой среды. С помощью данной компоненты может быть организована проверка ПО на этапе входного контроля.
* Программа-ловушка вирусов. Данная программа порождается в процессе функционирования комплекса, т.е. не хранится на диске, поэтому оригинал не может быть заражен. В процессе тестирования ПЭВМ программа - ловушка неоднократно выполняется, изменяя при этом текущую дату и время (организует ускоренный календарь). Наряду с этим программа-ловушка при каждом запуске контролирует свою целостность (размер, контрольную сумму, дату и время создания). В случае обнаружения заражения программный комплекс переходит в режим анализа зараженной программы - ловушки и пытается определить тип вируса.
* Программа для вакцинации.Предназначена для изменения среды функционирования вирусов таким образом, чтобы они теряли способность к размножению. Известно, что ряд вирусов помечает зараженные файлы для предотвращения повторного заражения. Используя это свойство возможно создание программы, которая обрабатывала бы файлы таким образом, чтобы вирус считал, что они уже заражены.
* База данных о вирусах и их характеристиках. Предполагается, что в базе данных будет храниться информация о существующих вирусах, их особенностях и сигнатурах, а также рекомендуемая стратегия лечения. Информация из БД может использоваться при анализе зараженной программы-ловушки, а также на этапе входного контроля ПО. Кроме того, на основе информации, хранящейся в БД, можно выработать рекомендации по использованию наиболее эффективных детекторов и фагов для лечения от конкретного типа вируса.
* Резидентные средства защиты. Отдельная компонента может резидентно разместиться в памяти и постоянно контролировать целостность системных файлов и командного процессора. Проверка может выполняться по прерываниям от таймера или при выполнении операций чтения и записи в файл.