ФГОУ ВПО "Саратовский государственный аграрный университет имени Н.И. Вавилова"

РЕФЕРАТ

Тема: Компьютерные вирусы и антивирусные программы

Студент I курса

Заочное отделение

Специальность: земельный кадастр

Ермачков Денис Александрович

Преподаватель: Гаманюк Николай Григорьевич

Саратов 2010 г.

**1. Понятие "компьютерного вируса" и его свойства**

Компьютерный вирус - это вредоносный самораспространяющийся в информационной среде программный код. Он может внедряться в исполняемые и командные файлы программ, распространяться через загрузочные секторы дискет и жестких дисков, документы офисных приложений, через электронную почту, Web-сайты, по другим электронным каналам. Проникнув в компьютерную систему, вирус может ограничиться безобидными визуальными или звуковыми эффектами, но может и вызвать потерю или искажение данных, утечку личной и конфиденциальной информации. В худшем случае компьютерная система, пораженная вирусом, окажется под полным контролем злоумышленника.

(Virus - с лат.) - вид программ, характеризующихся способностью скрытого от пользователя саморазмножения для поражения других программ, компьютеров или сетей.

Основную массу вирусов создают студенты и школьники, которые только что изучили язык ассемблера, хотят попробовать свои силы. Значительная часть таких вирусов их авторами часто не распространяется.

Вторую группу составляют также молодые люди (чаще - студенты), которые еще не полностью овладели искусством программирования, но уже решили посвятить себя написанию и распространению вирусов. Как правило, они создают многочисленные модификации "классических" вирусов, либо вирусы крайне примитивные и с большим числом ошибок. Выход конструкторов вирусов, при помощи которых можно создавать новые вирусы даже при минимальных знаниях об операционной системе и ассемблере значительно облегчил им работу.

Став старше и опытнее, многие из подобных вирусописателей попадают в третью, наиболее опасную группу, которая создает и запускает в мир "профессиональные" вирусы. Это тщательно продуманные и отлаженные программы. Такие вирусы нередко используют достаточно оригинальные алгоритмы, недокументированные и мало кому известные способы проникновения в системные области данных.

Четвертая группа авторов вирусов - "исследователи". Эта группа состоит из талантливых 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 вирусологии".

При заражении компьютера вирусом важно его обнаружить, для этого следует знать основные признаки его проявления:

- 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 размера 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. Заразиться компьютерным вирусом можно только в очень ограниченном количестве случаев. Это:

- запуск на компьютере исполняемой программы, заражённой вирусом;

- загрузка компьютера с дискеты, содержащей загрузочный вирус;

- подключение к системе заражённого драйвера;

- открытие документа, заражённого макровирусом;

- установка на компьютере заражённой операционной системы.

Компьютер не может быть заражён, если:

- на него переписывались текстовые и графические файлы (за исключением файлов, предусматривающих выполнение макрокоманд);

- на нём производилось копирование с одной дискеты на другую при условии, что ни один файл с дискет не запускался;

- на компьютере производится обработка принесённых извне текстовых и графических файлов, файлов данных и информационных файлов (за исключением файлов, предусматривающих выполнение макрокоманд);

- переписывание на компьютер заражённого вирусом файла ещё не означает заражения его вирусом. Чтобы заражение произошло нужно либо запустить заражённую программу, либо подключить заражённый драйвер, либо открыть заражённый документ (либо, естественно, загрузиться с заражённой дискеты). Иначе говоря, заразить свой компьютер можно только в том случае, если запустить на нём непроверенные программы и (или) программные продукты, установить непроверенные драйвера и (или) операционные системы, загрузиться с непроверенной системной дискеты или открыть непроверенные документы, подверженные заражению макровирусами.

**2. Классификация компьютерных вирусов**

На сегодняшний день известны десятки тысяч различных вирусов. Несмотря на такое изобилие, число типов вирусов, отличающихся друг от друга механизмом распространения и принципом действия, весьма ограниченно. Существуют и комбинированные вирусы, которые можно отнести одновременно к нескольким типам. Таким образом, вирусы можно классифицировать по следующим признакам:

- среде обитания;

- способу заражения среды обитания;

- степени воздействия;

- особенностям алгоритма.

1. В зависимости от **среды обитания** вирусы делят на:

1) сетевые – распространяются по различным компьютерным сетям;

2) файловые - поражают файлы с расширением .com, .ехе, реже .sys или оверлейные модули .ехе файлов. Эти вирусы дописывают своё тело в начало, середину или конец файла и изменяют его таким образом, чтобы первыми получить управление. Получив управление, вирус может заразить другие программы, внедриться в оперативную память компьютера и т.д. Некоторые из этих вирусов не заботятся о сохранение заражаемого файла, в результате чего он оказывается неработоспособным и не подлежащим восстановлению;

3) загрузочные - получают управление на этапе инициализации компьютера, еще до начала загрузки ОС. При заражении дискеты или жесткого диска загрузочный вирус заменяет загрузочную запись BR или главную загрузочную запись MBR. При начальной загрузке компьютера BIOS считывает загрузочную запись с диска или дискеты, в результате чего вирус получает управление еще до загрузки ОС. Затем он копирует себя в конец оперативной памяти и перехватывает несколько функций BIOS. В конце процедуры заражения вирус загружает в память компьютера настоящий загрузочный сектор и передает ему управление. Далее все происходит, как обычно, но вирус уже находится в памяти и может контролировать работу всех программ и драйверов;

4) файлово–загрузочные – комбинированные вирусы, объединяющие свойства файловых и загрузочных. В качестве примера можно привести широко распространенный когда-то файлово-загрузочный вирус OneHalf. Проникая в компьютер с ОС MS-DOS, этот вирус заражает главную загрузочную запись. Во время загрузки вирус постепенно шифрует секторы жесткого диска, начиная с самых последних секторов. Вирус OneHalf использует различные механизмы маскировки.

2. По **способу заражения среды обитания** вирусы делятся на:

1) резидентные - 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;

2) нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время.

3. По **степени воздействия** вирусы можно разделить на:

1) 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;

2) опасные вирусы, которые могут привести к различным нарушениям в работе компьютера;

3) особо опасные, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

4. По **особенностям алгоритма**:

Большое разнообразие вирусов вызывает трудности в их классификации по данному признаку.

1) Простейшие вирусы - паразитические, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены;

2) вирусы-невидимки (стелс-вирусы) – пытаются скрыть свое присутствие в компьютере. Они имеют резидентный модуль, постоянно находящийся в оперативной памяти компьютера. Этот модуль перехватывает обращения к дисковой подсистеме компьютера. Если ОС или другая программа считывают файл зараженной программы, то вирус подставляет настоящий, незараженный, файл программы. Для этого резидентный модуль может временно удалять вирус из зараженного файла. После окончания работы с файлом он заражается снова. Загрузочные стелс-вирусы действуют по такой же схеме. Когда какая-либо программа считывает данные из загрузочного сектора, вместо зараженного подставляется настоящий загрузочный сектор.

3) макрокомандные вирусы. Файлы документов Microsoft Office могут содержать в себе небольшие программы для обработки этих документов, составленные на языке Visual Basic for Applications. Это относится и к базам данных Access, а также к файлам презентаций Power Point. Такие программы создаются с использованием макрокоманд, поэтому вирусы, живущие в офисных документах, называются макрокомандными. Макрокомандные вирусы распространяются вместе с файлами документов. Чтобы заразить компьютер таким вирусом, достаточно просто открыть файл документа в соответствующем приложении. Распространнености данного вида вирусов в немалой степени способствует популярность Microsoft Office. Они могут изменять зараженные документы, оставаясь незамеченными долгое время.

Кроме вирусов принято выделять еще, по крайней мере, три вида вредоносных программ. Это троянские программы, логические бомбы и программы-черви. Четкого разделения между ними не существует: троянские программы могут содержать вирусы, в вирусы могут быть встроены логические бомбы и др.

4) Троянские программы - по основному назначению троянские программы совершенно безобидны или даже полезны. Но когда пользователь запишет программу в свой компьютер и запустит ее, она может незаметно выполнять вредоносные функции. Чаще всего троянские программы используются для первоначального распространения вирусов, для получения удаленного доступа к компьютеру через Интернет, кражи данных или их уничтожения;

5) логические бомбы - программа или ее отдельные модули, которые при определенных условиях выполняют вредоносные действия. Логическая бомба может, например, сработать по достижении определенной даты или тогда, когда в базе данных появится или исчезнет запись, и т. д. Такая бомба может быть встроена в вирусы, троянские программы и даже в обычные программы;

6) программы-черви нацелены на выполнение определенной функции, например, на проникновение в систему и модификацию данных. Можно, скажем, создать программу-червь, подсматривающую пароль для доступа к банковской системе и изменяющую базу данных. Широко известная программа-червь была написана студентом Корнельского университета Робертом Моррисом. Червь Морриса был запущен в Интернет 2 ноября 1988 г. и за 5 часов смог проникнуть более чем на 6000 компьютеров. Некоторые вирусы-черви (например, Code Red) существуют не внутри файлов, а в виде процессов в памяти зараженного компьютера. Это исключает их обнаружение антивирусами, сканирующими файлы и оставляющими без внимания оперативную память компьютера;

7) вирусы в системах документооборота - документы, хранящиеся в базах данных таких систем документооборота, как Lotus Notes и Microsoft Exchange, тоже могут содержать вирусы, точнее, вредоносные макрокоманды. Они могут активизироваться при выполнении каких-либо действий над документом (например, когда пользователь щелкает кнопку мышью). Поскольку такие вирусы расположены не в файлах, а в записях баз данных, для защиты от них требуются специализированные антивирусные программы;

8) новые и экзотические вирусы. По мере развития компьютерных технологий совершенствуются и компьютерные вирусы, приспосабливаясь к новым для себя сферам обитания. Так, новый вирус W32/Perrun, сообщение о котором есть на сайте компании Network Associates, способен распространяться… через файлы графических изображений формата JPEG. Сразу после запуска W32/Perrun ищет файлы с расширением .JPG и дописывает к ним свой код. Надо сказать, что данный вирус не опасен и требует для своего распространения отдельной программы. Среди других "достижений" создателей вредоносных программ заслуживает внимания вирус Palm.Phage. Он заражает приложения "наладонных" компьютеров PalmPilot, перезаписывая файлы этих приложений своим кодом. Появление таких вирусов, как W32/Perrun и Palm.Phage, свидетельствует о том, что в любой момент может родиться компьютерный вирус, троянская программа или червь нового, неизвестного ранее типа, либо известного типа, но нацеленного на новое компьютерное оборудование. Новые вирусы могут использовать неизвестные или не существовавшие ранее каналы распространения, а также новые технологии внедрения в компьютерные системы.

**3. Антивирусные программы**

## Антивирус - это программа, предназначенная для сканирования и распознавания на компьютере пользователя программ или скриптов (скрипт *-* текстовый файл, содержащий секции, параметры секций и значения параметров секций, описывающие действия, которые необходимо выполнить интерпретатору скрипта), макросов (макрос - это набор команд, которые можно применить, нажав всего лишь одну клавишу). С помощью макроса можно автоматизировать любое действие, которое выполняется в используемом приложении, которое может причинить вред пользователю или существенно замедлить работу компьютера.

## Антивирусные программы можно разделить на несколько типов:

## - Детекторы. Их назначение - лишь обнаружить вирус. Детекторы вирусов могут сравнивать загрузочные сектора дискет с известными загрузочными секторами, формируемыми операционными системами различных версий, и таким образом обнаружить загрузочные вирусы или выполнять сканирование файлов на магнитных дисках с целью обнаружения сигнатур известных вирусов. Такие программы в чистом виде в настоящее время редки.

## - Доктора (Фаги. Фаг) - это программа, которая способна не только обнаружить, но и уничтожить вирус, т.е. удалить его код из зараженных программ и восстановить их работоспособность (если возможно). Известнейшим в России фагом является Aidstest, созданный Д.Н.Лозинским. Одна из последних версий обнаруживает более 8000 вирусов. Aidstest для своего нормального функционирования требует, чтобы в памяти не было резидентных антивирусов, блокирующих запись в программные файлы, поэтому их следует выгрузить, либо, указав опцию выгрузки самой резидентной программе, либо воспользоваться соответствующей утилитой.

## - Ревизоры. Программа-ревизор контролирует возможные пути распространения программ-вирусов и заражения компьютеров. Программы-ревизоры относятся к самым надежным средствам защиты от вирусов и должны входить в арсенал каждого пользователя. Ревизоры являются единственным средством, позволяющим следить за целостностью и изменениями файлов и системных областей магнитных дисков. Наиболее известна в России программа-ревизор ADinf, разработанная Д.Мостовым.

## - Вакцины. Так называются антивирусные программы, ведущие себя подобно вирусам, но не наносящие вреда. Вакцины предохраняют файлы от изменений и способны не только обнаружить факт заражения, но и в некоторых случаях "вылечить" пораженные вирусами файлы. В настоящее время антивирусные программы-вакцины широко не применяются, так как в прошлые годы некоторыми некорректно работающими вакцинами был нанесен ущерб многим пользователям.

## Для нахождения вирусов Dr Web использует программу эмуляцию процессора, т.е. он моделирует выполнение остальных файлов с помощью программной модели микропроцессора I-8086 и тем самым создает среду для проявления вирусов и их размножения. Таким образом, программа Dr Web может бороться не только с полиморфными вирусами, но и вирусам, которые только еще могут появиться в перспективе.

## Основными функциональными особенностями Dr Web являются:

## · защита от червей, вирусов, троянов, полиморфных вирусов, макровирусов, spyware, программ-дозвонщиков, adware, хакерских утилит и вредоносных скриптов;

## · обновление антивирусных баз до нескольких раз в час, размер каждого обновления до 15 KB;

## · проверка системной памяти компьютера, позволяющая обнаружить вирусы, не существующие в виде файлов (например, CodeRed или Slammer);

## · эвристический анализатор, позволяющий обезвредить неизвестные угрозы до выхода соответствующих обновлений вирусных баз.

## Любой современный антивирусный продукт - это не только набор отдельных технологий детектирования, но и сложная система защиты, построенная на собственном понимании антивирусной компанией того, как нужно обеспечивать безопасность от вредоносных программ.

## Антивирус Касперского Personal предназначен для антивирусной защиты персональных компьютеров, работающих под управлением операционных систем Windows 98/ME, 2000/NT/XP, от всех известных видов вирусов, включая потенциально опасное программное обеспечение. Программа осуществляет постоянный контроль всех источников проникновения вирусов - электронной почты, интернета, дискет, компакт-дисков и т.д. Уникальная система эвристического анализа данных эффективно нейтрализует неизвестные вирусы. Можно выделить следующие варианты работы программы (они могут использоваться как отдельно, так и в совокупности):

## · Постоянная защита компьютера - проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов.

## · Проверка компьютера по требованию - проверка и лечение как всего компьютера в целом, так и отдельных дисков, файлов или каталогов. Такую проверку вы можете запускать самостоятельно или настроить ее регулярный автоматический запуск.

## Программа создает надежный барьер на пути проникновения вирусов через электронную почту. Антивирус Касперского Personal автоматически осуществляет проверку и лечение всей входящей и исходящей почтовые корреспонденции по протоколам POP3 и SMTP и эффективно обнаруживает вирусы в почтовых базах. Программа поддерживает более семисот форматов архивированных и сжатых файлов и обеспечивает автоматическую антивирусную проверку их содержимого, а также удаление вредоносного кода из архивных файлов формата ZIP, CAB, RAR, ARJ, LHA и ICE. В состав Антивируса Касперского включен специальный компонент, обеспечивающий защиту файловой системы компьютера от заражения - Файловый Антивирус. Он запускается при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые вами или программами файлы.