1.Общие сведения. Компьютерный вирус – это 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. Сегодня компьютерам доверяют решение многих критических задач. Поэтому выход из строя компьютерных систем может иметь весьма тяжелые последствия, вплоть до человеческих жертв (представьте себе, например, вирус в компьютерных системах аэродромных служб…). 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. Есть и комбинированные вирусы, которые можно отнести одновременно к нескольким типам. Вирусы представлены в хронологическом порядке появления.
1.Файловые вирусы. Внедряясь в тело файлов программ .COM и .EXE, файловые вирусы изменяют их таким образом, что при запуске управление передается не зараженной программе, а вирусу. Вирус может записать свой код в конец, начало или середину файла. Получив управление, вирус может заразить другие программы, внедриться в оперативную память компьютера и т. д. Далее вирус передает управление зараженной программе, и та исполняется обычным образом. Помимо .COM и .EXE файловые вирусы могут заражать программные файлы других типов – оверлеи MS-DOS (.OVL, .OVI, .OVR и другие), драйверы .SYS, библиотеки .DLL, а также любые файлы с программным кодом. Известны файловые вирусы для различных ОС – MS-DOS, Microsoft Windows, Linux, IBM OS/2 и т. д.

2.Загрузочные вирусы. Загрузочные вирусы 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. Исходные записи BR или MBR при этом обычно не пропадают (хотя бывает и иначе): вирус копирует их в один из свободных секторов диска. 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.

Комбинированные вирусы. Очень часто встречаются 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. Он представляет собой стелс-вирус и при распространении применяет полиморфные алгоритмы.

Вирусы-спутники. Как известно, в MS-DOS и в Microsoft Windows различных версий существует три типа файлов, которые пользователь может запустить на выполнение. Это командные или пакетные файлы .BAT, а также исполняемые файлы .COM и .EXE. Когда вирус-спутник заражает файл .EXE или .BAT, он создает в этом же каталоге еще один файл с таким же именем, но с расширением .COM. Вирус записывает себя в этот COM-файл, который запускается до EXE-файла. При запуске программы первым получит управление вирус-спутник, который затем может запустить ту же программу, но уже под своим контролем.

3.Вирусы в пакетных файлах. Существует несколько вирусов, способных заражать пакетные файлы .BAT. Они записывают свой двоичный код в тело пакетного файла после оператора комментария REM. При запуске такой пакетный файл копирует вирусный код в обычный исполняемый файл. Затем файл с вирусной программой запускается и удаляется. Получив управление, исполняемый файл вируса выполняет вредоносные действия и заражает другие пакетные файлы.

Шифрующиеся и полиморфные вирусы. Некоторые вирусы шифруют собственный код, чтобы затруднить их обнаружение. Каждый раз, заражая новую программу, вирус использует для шифрования новый ключ. В результате два экземпляра такого вируса могут значительно отличаться друг от друга, даже иметь разную длину. Для шифрования применяются не только разные ключи, но и разные процедуры шифрования. Два экземпляра такого вируса не имеют ни одной совпадающей последовательности кода. Вирусы, способные полностью изменять

свой код, получили название полиморфных.

Стелс-вирусы. 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. Макрокомандные вирусы очень распространены, чему в немалой степени способствует популярность Microsoft Office. Они могут изменять зараженные документы, оставаясь незамеченными долгое время.

4.Вредоносные программы других типов. 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 т. д.

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.

Логические бомбы. Логической бомбой называется 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. Программы-черви.

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.

5.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.

6.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.