Тема 6.1. Обзор и способы классификации компьютерных вирусов.

Способы распространения вирусов

Для того чтобы персональные компьютеры дома или локальная сеть в образовательном учреждении не оказались под угрозой заражения вирусами, необходимо представлять не только что это такое, и к каким последствиям это может привести, но и быть осведомленными в вопросах борьбы с вирусами. Ознакомимся с тем, что представляют из себя вирусы.

Вирусы - это фрагменты программного кода, которые видоизменяют другие программы на компьютере при приведении их в действие. Они могут распространяться как вложения в электронные письма, храниться на сайтах ваших коллег и друзей по интересам и ждать, когда вы их скачаете, или же храниться на сайтах, принимая вид полезных файлов.

Прежде чем вирус нанесет вред, он должен начать работать. Например, кто-то присылает вам вирус, а вы, не зная того, сохраняете его как вложение в электронное письмо, и он «поселяется» на вашем жестком диске; но пока он не начал работать, вы не заражены.

Наиболее распространенный способ заставить вирус работать - сделать двойной щелчок и открыть файл, содержащий спрятанный в нем вирус. Зараженный файл может быть чем угодно - от картинки до музыки и даже setup-файлом для новых программ, скачанных вами из Интернета.

Было время, когда открытие зараженного вложения было единственным способом заставить скрытую программу-вирус работать, но писатели вирусов отладили этот процесс так, что некоторые вирусы начинают работать автоматически. В 2005-6 году в Microsoft была внедрена методика написания безопасного для атак кода, до сих пор не применяемая большинством других разработчиков.

История вредоносных программ

Мнений по поводу рождения первого компьютерного вируса очень много. Нам доподлинно известно только одно: на машине Чарльза Бэббиджа, считающегося изобретателем первого компьютера, вирусов не было, а на Univax 1108 и IBM 360/370 в середине 1970-х годов они уже были.

Обратимся к истории массовых вирусных атак. Когда и с чего это все началось? В 1988 году произошла первая массовая компьютерная эпидемия — эпидемия червя Морриса, и Американская ассоциация компьютерного оборудования объявила 30 ноября международным Днем защиты информации (Computer Security Day).

Несмотря на это, сама идея компьютерных вирусов появилась значительно раньше. Отправной точкой можно считать труды Джона фон Неймана по изучению самовоспроизводящихся математических автоматов. Эти труды стали известны в 1940-х годах. А в 1951 г. знаменитый ученый предложил метод, который демонстрировал возможность создания таких автоматов. Позднее, в 1959 г., журнал "Scientific American" опубликовал статью Л.С. Пенроуза, которая также была посвящена самовоспроизводящимся механическим структурам. В отличие от ранее известных работ, здесь была описана простейшая двумерная модель подобных структур, способных к активации, размножению, мутациям, захвату. Позднее, по следам этой статьи другой ученый - Ф.Ж. Шталь - реализовал модель на практике с помощью машинного кода на IBM 650.

Необходимо отметить, что с самого начала эти исследования были направлены отнюдь не на создание теоретической основы для будущего развития компьютерных вирусов. Наоборот, ученые стремились усовершенствовать мир, сделать его более приспособленным для жизни человека. Ведь именно эти труды легли в основу многих более поздних работ по робототехнике и искусственному интеллекту. И в том, что последующие поколения злоупотребили плодами технического прогресса, нет вины этих замечательных ученых.

В 1962 г. инженеры из американской компании Bell Telephone Laboratories - В.А. Высотский, Г.Д. Макилрой и Роберт Моррис - создали игру "Дарвин". Игра предполагала присутствие в памяти вычислительной машины так называемого супервизора, определявшего правила и порядок борьбы между собой программ-соперников, создававшихся игроками. Программы имели функции исследования пространства, размножения и уничтожения. Смысл игры заключался в удалении всех копий программы противника и захвате поля битвы.

На этом теоретические исследования ученых и безобидные упражнения инженеров ушли в тень, и совсем скоро мир узнал, что теория саморазмножающихся структур с неменьшим успехом может быть применена и в несколько иных целях(по материалам сайта **http://www.viruslist.com/ru/viruslist.html**).

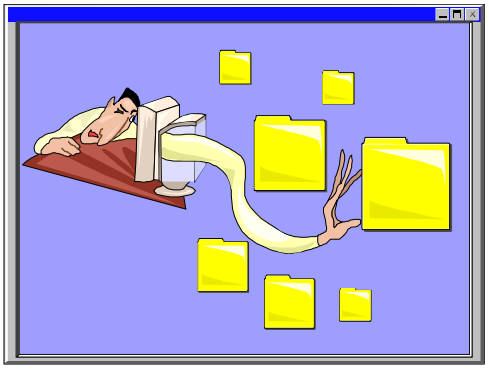
От истории перейдем к вирусной терминологии, владение которой поможет ориентироваться в компьютерном мире и находить правильные

методы защиты от проникновения вирусов в домашние и школьные компьютеры.

Вирусная терминология

Познакомьтесь с некоторыми из терминов, обычно используемых в разговоре о вирусах, такими как: вредоносный код, вирус, червь, антивирусная программа и база, уязвимость, программы удаленного администрирования, клавиатурные шпионы. А также рассмотрим некоторую классификацию вирусов.

Вредоносный код. Любая часть компьютерного кода, обычно программа, которая может нанести вред или отрицательно воздействовать на компьютер.



Вирус. Программа, которая заражает компьютер и изменяет другие программы (включая операционную систему).

Червь. Тип вируса, который может распространяться, не заражая отдельные программы или файлы. Большинство червей распространяется по электронной почте или через компьютеры, объединенные в сеть.

Антивирусная программа. Антивирусный сканер или программа, которая оценивает данные на жестком диске или входящие данные и определяет, не содержат ли они компьютерные вирусы.

Антивирусная база. База данных известных вирусов, которую имеет любая компания, производящая антивирусные программы. База данных вирусов обновляется по мере того, как появляются и распространяются новые вирусы. Технические характеристики каждого вируса использованы как критерии, по которым антивирусный сканер оценивает файлы, выполняя поиск зараженных файлов.

Уязвимость. Любая ошибка или ряд особенностей, которые дают хакеру или вирусу возможность недозволенного входа в машину. Когда разработчикам программ становится известно об уязвимостях, они выпускают патчи, которые пользователи должны скачать и установить, чтобы ликвидировать уязвимость.

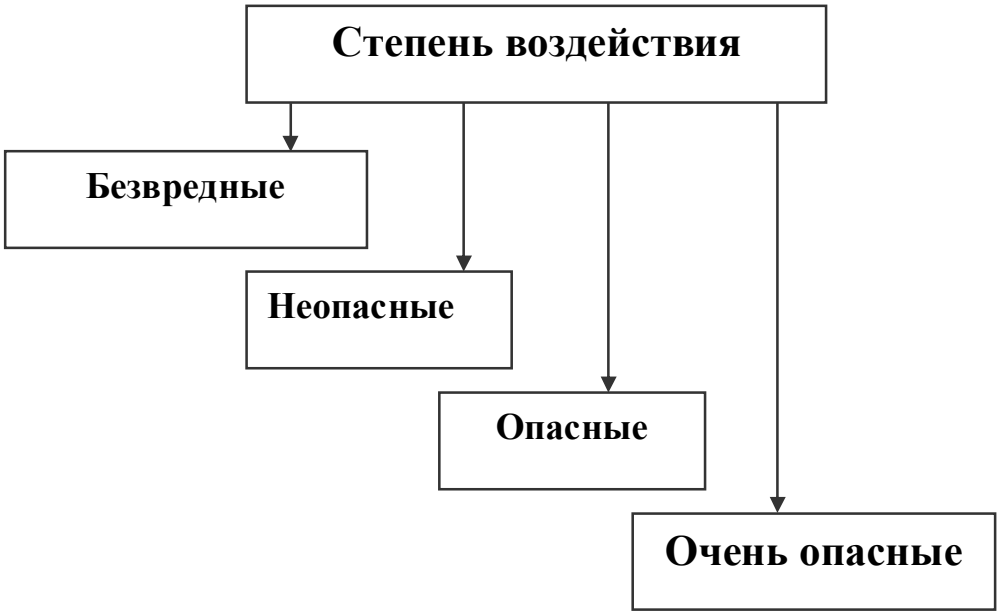
Программы удаленного администрирования (Backdoor' Trojans). Программы, которые прячутся на вашем компьютере, пытаясь избежать обнаружения во время совершения несанкционированных действий.

Клавиатурные шпионы. Это программы, записывающие щелчки мыши, нажатия клавиш и иногда скриншоты во время работы на компьютере. Они создают запись событий, которая может быть послана по электронной почте или прочитана злоумышленниками, если они имеют непосредственный доступ к вашему компьютеру.

Классификация вирусов

Операционная система или приложение может подвергнуться вирусному нападению в том случае, если она имеет возможность запустить программу, не являющуюся частью самой системы. Данному условию удовлетворяют все популярные «настольные» операционные системы, многие офисные приложения, графические редакторы, системы проектирования и прочие программные комплексы, имеющие встроенные скриптовые языки.
Если операционная система существует в единичных экземплярах, то вероятность ее злонамеренного использования близка к нулю. Если же производитель системы добился ее массового распространения, то очевидно, что рано или поздно хакеры и вирусописатели попытаются использовать ее в своих интересах. Чем популярнее операционная система или приложение, тем чаще она будет являться жертвой вирусной атаки. Практика это подтверждает — распределение количества вредного программного обеспечения для Windows и Linux практически совпадает с долями рынка, которые занимают эти операционные системы.

По масштабу вредных воздействий, которые могут нанести вирусы их можно разделить на 4 группы.



Безвредные уменьшают свободную область на диске за счет своего размножения.

Неопасные, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках.

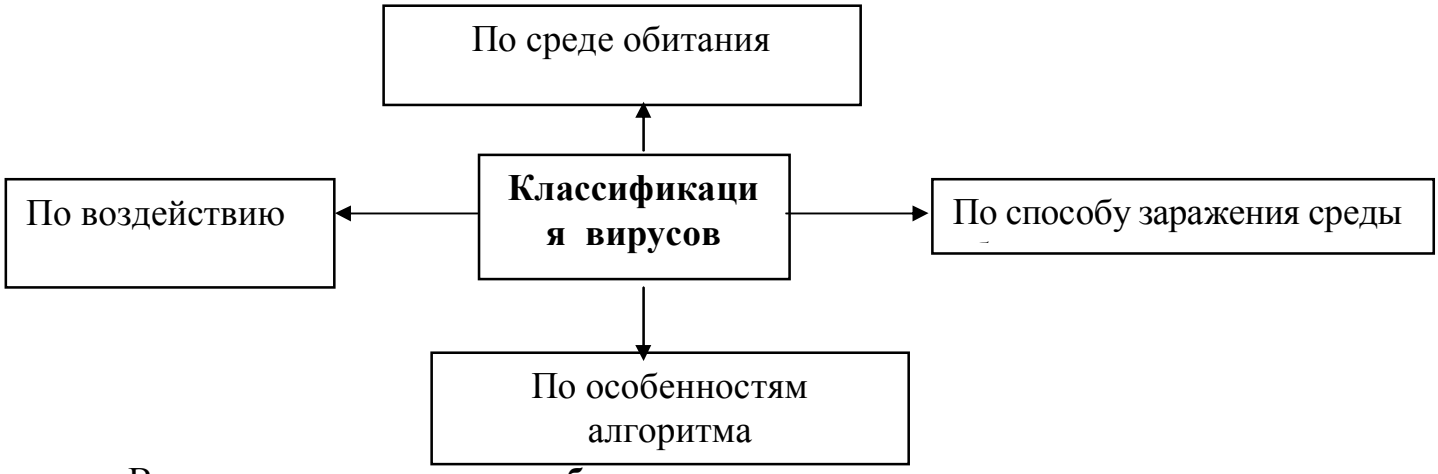
Действия таких вирусов проявляются в каких-либо графических или звуковых эффектах. Но даже если в алгоритме вируса не найдено ветвей, наносящих ущерб

системе, этот вирус нельзя с полной уверенностью назвать безвредным, так как проникновение его в компьютер может вызвать непредсказуемые и порой катастрофические последствия.

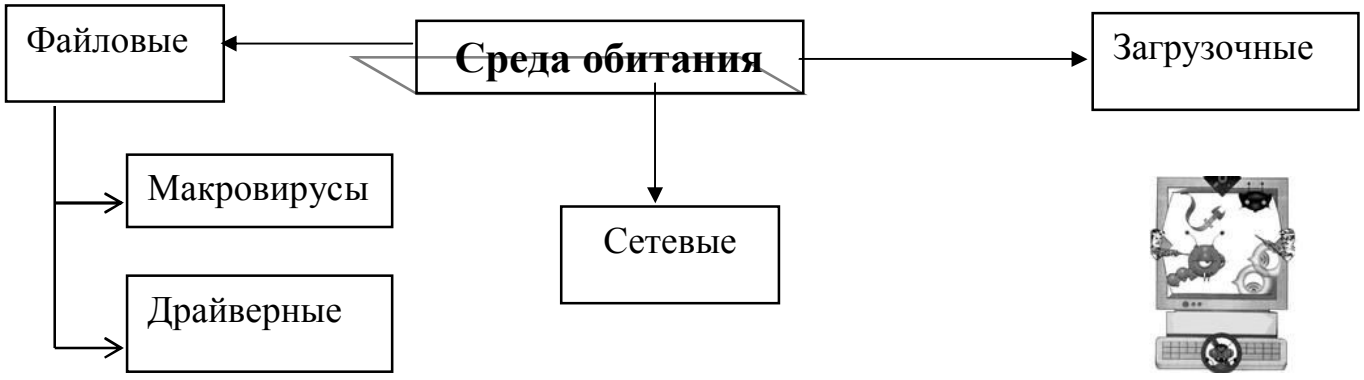
Опасные вирусы, которые могут привести к различным нарушениям в работе компьютера;

Очень опасные, воздействие которых может привести к безовзвратной потере программ, уничтожению данных, стиранию информации в системных областях диска.

В настоящее время известны тысячи компьютерных вирусов, которые можно классифицировать по следующим признакам:



В зависимости от **среды обитания** вирусы можно разделить на сетевые, файловые, загрузочные.



Сетевые вирусы распространяются по различным компьютерным сетям. Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

Файловые вирусы внедряются главным образом в исполняемые модули, т. е. в файлы, имеющие расширения COM и EXE и активируются

при их запуске. Находятся в оперативной памяти до выключения компьютера.

Загрузочные вирусы внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Record). При загрузке операционной системы с зараженного диска внедряется в оперативную память и ведет себя как файловый вирус.

Макровирусы - являются макрокомандами, которые заражают файлы документов Word, Excel, находятся в оперативной памяти до закрытия приложения.

Драйверные вирусы – заражают драйверы устройств компьютера или запускают себя путем включения в файл конфигурации дополнительной строки.

Вирус не может содержаться в ASCII-текстах, графических или звуковых файлах, т.к. он является программой и требует исполнения своего кода.

Самые распространенные вирусы

На сегодняшний день очень популярными являются вирусы, которые называют червями.

Большинство известных червей распространяется в виде файлов: вложение в электронное письмо, ссылка на зараженный файл на каком-либо веб- или FTP-ресурсе в ICQ- и IRC-сообщениях, файл в каталоге обмена P2P и т. д. Некоторые черви (так называемые «бесфайловые» или «пакетные» черви) распространяются в виде сетевых пакетов, проникают непосредственно в память компьютера и активизируют свой код. Некоторые черви обладают также свойствами других разновидностей вредоносного программного обеспечения, например, содержат троянские функции или способны заражать выполняемые файлы на локальном диске, т. е. имеют свойство троянской программы. Троянские программы осуществляют различные несанкционированные пользователем действия, например, сбор информации и передачу ее злоумышленнику, разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в

неблаговидных целях. Отдельные категории троянских программ наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособность зараженного компьютера.

Сведения о самых распространенных угрозах и потенциально нежелательных программах можно всегда найти на портале Центра Microsoft по защите от нежелательных программ (***http://www.microsoft.com/rus/protect/products/computer/malwareprotectioncenter.mspx)***. А также специалисты «Лаборатории Касперского» постоянно информируют о новых угрозах, новых появившихся вирусах (***http://www.securelist.com/ru/descriptions)***.

Макровирусы

Переходя к рассмотрению макровирусов особое внимание обратим на вирусы, распространяющиеся по глобальной сети через электронную почту и телеконференции.

Итак, основным источником вирусов на сегодняшний день является глобальная сеть Интернет. Наибольшее число заражений вирусом происходит при обмене письмами в форматах Word/Office. Особо широкое распространение в последнее время получили макровирусы.

Макровирусы - программы, написанные на языке макропоследовательностей программ Microsoft Word и Excel. Макровирусы записываются в документы и шаблоны документов Word и Excel. Открыв документ, зараженный макровирусом, вы заразите стандартный шаблон документов, находящийся на вашем компьютере, а через него все документы, которые будете открывать в дальнейшем. Уже существует множество разновидностей макровирусов - от достаточно безобидных до удаляющих системные и программные файлы и форматирующих жесткий диск. Пользователь зараженного макровирусом редактора, сам того на подозревая, рассылает зараженные письма адресатам, который, в свою очередь, отправляют новые зараженные письма, и т. д.

Нередки случаи, когда зараженный файл-документ или таблица Excel по причине недосмотра попадает в списки рассылки коммерческой информации какой-либо крупной компании. В этом случае страдают сотни или даже тысячи абонентов таких рассылок, которые затем разошлют зараженные файлы десяткам тысяч своих абонентов.

Файл-серверы «общего пользования» и электронные конференции также служат одним из основных источников распространения вирусов. Практически каждую неделю приходит сообщение о том, что какой-либо пользователь заразил свой компьютер вирусом, который был снят с BBS, ftp-сервера или получен из какой-либо электронной конференции.

Теперь обратимся к такому понятию как **«цикл функционирования вируса»**.

В цикле функционирования или существования любого вируса можно выделить три этапа.

Первый этап: вирус находится в **неактивном состоянии**. В этом состоянии он внедрен в тело исполняемого файла или находится в загрузочном секторе диска и «ждет» своего часа. Именно в неактивном состоянии вирусы переносятся вместе с программами или дискетами от одного ПК к другому. Для того чтобы он начал свою работу, необходимо запустить исполняемый файл или загрузиться с зараженной дискеты. В этот момент **активизируется вирус**, который либо **создает резидентную** в памяти **программу**, способную порождать копии или производить какие-то разрушительные действия, либо **немедленно приступает к работе.**

Если вирус создал резидентную программу, то ее активизация осуществляется различными способами - все зависит от фантазии автора вируса.

Второй этап: жизнедеятельности вируса - это этап активного размножения, поэтому вирусная программа стремится максимально скрыть от пользователя ПК результаты своей деятельности.

Третий этап: После того как заражено достаточно много файлов, наступает этап, связанный с внешними проявлениями работы вируса. Ваш компьютер вдруг начнет вести себя странно: зазвучит ли музыкальная фраза, или начнут “сыпаться” символы на экране дисплея. Некоторые вирусы к этому моменту могут уже безвозвратно нарушить файловую структуру.

Методы борьбы с вирусами

Защита информации от преднамеренного искажения или уничтожения — это защита от вирусов. Здесь эффективен комплекс мер, включающий в себя профилактические (использование антивирусных программ) и общие методы защиты.

При заражении компьютера вирусом важно его обнаружить. Для этого следует знать об основных признаках проявления вирусов.

Вот несколько основных признаков того, что компьютер может быть заражен вирусом:

- Компьютер работает медленнее, чем обычно
- Компьютер перестает отвечать на запросы и часто блокируется
- Каждые несколько минут происходит сбой и компьютер перезагружается
- Компьютер самопроизвольно перезагружается и после этого работает со сбоями

- Установленные на компьютере приложения работают неправильно
- Диски или дисководы недоступны
- Не удается выполнить печать
- Появляются необычные сообщения об ошибках
- Открываются искаженные меню и диалоговые окна

Это типичные признаки заражения. Однако они характерны и для неполадок программного обеспечения или оборудования, не имеющих ничего общего с вирусами. Пока на компьютере не запущено **средство удаления вредоносных программ Microsoft**) и не установлена последняя версия **антивирусного программного обеспечения**, соответствующего отраслевым стандартам, нельзя с уверенностью сказать, заражен ли компьютер вирусом.

Одним из основных методов борьбы с вирусами является, как и в медицине, своевременная профилактика. Компьютерная профилактика предполагает соблюдение небольшого числа правил, которые позволяют значительно снизить вероятность заражения вирусом и потери каких-либо данных. Если компьютер не защищен при подключении к Интернету, хакеры могут получить доступ к личным сведениям пользователя. Они могут установить программный код, который уничтожит файлы или вызовет сбои в работе, либо использовать компьютер для атак на другие домашние или офисные компьютеры, подключенные к Интернету.

Для того чтобы не подвергнуть компьютер заражению вирусами и обеспечить надежное хранение информации, необходимо соблюдать следующие правила:

2. При переносе на свой компьютер файлов в архивированном виде проверяйте их сразу же после разархивации на жестком диске, ограничивая область проверки только вновь записанными файлами.

3. Всегда защищайте свои носители информации от записи при работе на других компьютерах, если на них не будет производиться запись информации.

4. Обязательно делайте архивные копии ценной для вас информации.

5. Используйте **брандмауэр Интернета**. Брандмауэр - это программное или аппаратное обеспечение, которое блокирует атаки хакеров и не позволяет вирусам и вирусам-червям попадать на компьютер через Интернет. Если вы пользуетесь компьютером дома или на малом предприятии, применение брандмауэра - самое эффективное и важное действие по защите компьютера. Очень важно включить брандмауэр и антивирусную программу *до* подключения к Интернету.

6. Посетите **Центр обновления Microsoft** и включите функцию

автоматического обновления. (Если на компьютере установлен пакет Office 2003 или Office XP, он будет обновляться автоматически. Если используется более ранняя версия пакета Microsoft Office, посетите **Центр загрузки Office**).

7. Подпишитесь на получение **стандартного антивирусного программного обеспечения** и регулярно обновляйте его.

8. Никогда не открывайте вложения в сообщениях электронной почты, полученных от незнакомых людей.

9. Не открывайте также вложенные файлы в сообщениях, полученных от знакомых, если характер содержимого точно не известен. Отправитель может и не подозревать о наличии вируса в сообщении.

10. Чтобы наверняка не заразиться макровирусом, на вкладке Общие параметры настройки диалогового окна Параметры, вызываемого командами **меню Сервис/Параметры** Word и Excel, воспользуйтесь **пунктом Защита** от вирусов в макросах.

11. При попытке открыть документ, содержащий автоматически выполняющуюся макропоследовательность, программа предупредит **об** этом и предложит отменить выполнение подозрительного макроса, который может оказаться макровирусом.

Портал Центра Microsoft по защите от нежелательных программ (Microsoft Malware Protection Center, MMPC)

Это интерактивный веб-портал, который содержит сведения о новых угрозах безопасности компьютера и мерах борьбы с ними. Этот портал служит для сообщения пользователям результатов исследований Центра по защите от нежелательных программ в области вредоносных программ и мер борьбы с ними.

Портал Центра Microsoft по защите от нежелательных программ включает приведенные ниже разделы и сведения:

- Энциклопедия вредоносных программ. Здесь можно узнать о конкретном вирусе или другой угрозе, с помощью функции поиска в энциклопедии.
- Описание способа отправки образцов для испытаний. В этом разделе можно отправить файлы, которые, по вашему мнению, могут быть заражены вредоносными или нежелательными программами. Специалисты Центра проведут анализ этих файлов и на вашу электронную почту будут высланы результаты анализа файлов.
- Новейшие сигнатуры вирусов для **Защитника Windows.** Вредоносные программы постоянно меняются. Здесь можно получить мгновенный доступ к новейшим описаниям угроз.
- Сведения о самых распространенных угрозах и потенциально нежелательных программах, предоставленные пользователями,

которые сообщают о них в Центр MMPC, а также по сведениям, полученным от продуктов по обеспечению безопасности компании Microsoft, таких как **средство удаления вредоносных программ**, **Защитник Windows**. В этом разделе можно получить новейшие сведения о десяти самых распространенных категориях угроз про которых сообщают пользователи. Каждая угроза сопровождается ссылкой для отображения дополнительных сведений.