**Федеральное агентство по культуре и кинематографии.**

**Кировский филиал**

**Государственного образовательного учреждения высшего**

**профессионального образования**

**«Пермский государственный институт искусства и культуры».**

**КОНТРОЛЬНАЯ РАБОТА**

**По Информатике**

**на тему:**

**Компьютерные вирусы. Методы и средства защиты.**

**Выполнила студентка группы Рт-3**

**Решетникова Светлана Михайловна**

**Киров – 2007**

**Оглавление**

1. Введение

## 2. Компьютерные вирусы и их разновидности

3. Методы защиты от компьютерных вирусов

4. Средства антивирусной защиты

Вывод

Список использованной литературы

**1. Введение**

Еще не так давно, всего три десятка лет назад, ЭВМ представляла собой целый комплекс огромных шкафов, занимавших несколько больших помещений. А всего и делала-то, что довольно быстро считала. Нужна была буйная фантазия журналистов, чтобы увидеть в этих гигантских арифмометрах «думающие агрегаты, и даже пугать людей тем, что ЭВМ вот-вот станут разумнее человека. ЭВМ стремительно совершенствовалась: резко сокращались её размеры, она работала все быстрее и быстрее, обрастала все новыми приспособлениями, с помощью которых стала печатать текст, чертить чертежи и даже рисовать картинки.

Что же говорить о современных компьютерах, компактных, быстродействующих, оснащённых руками - манипуляторами, экранами дисплеев, печатающими, рисующими и чертящими устройствами, анализаторами образов, звуков, синтезаторами речи и другими «органами»! На всемирной выставке в Осаке компьютеризированные роботы уже ходили по лестнице, перенося вещи с этажа на этаж, играли с листа на фортепьяно, беседовали с посетителями. Так и кажется, что они вот-вот сравняются по своим способностям с человеком, а то и превзойдут его. Да компьютеры многое могут. Но, конечно, далеко не всё.

Самый главный минус в компьютере – это вирус, который может появиться не только через Интернет, но и через обычные диски. КОМПЬЮТЕРНЫЙ ВИРУС, программа ЭВМ, способная без ведома пользователя и вопреки его желанию самопроизвольно размножаться и распространяться; нарушая работоспособность программного обеспечения ЭВМ (отсюда его название по аналогии с болезнетворным вирусом). Впервые появился в начале 1980-х гг. в США. К 1995 насчитывалось несколько десятков разновидностей компьютерных вирусов. Для борьбы с ними разрабатываются антивирусные программы.

**2. Компьютерные вирусы и их разновидности**

Компьютерным вирусом называется рукотворная программа, способная самостоятельно создавать свои копии и внедряться в другие программы, в системные области дисковой памяти компьютера, распространяться по каналам связи с целью прерывания и нарушения работы программ, порчи файлов, файловых систем и компонентов компьютера, нарушения нормальной работы пользователей.

Компьютерным вирусам, как и биологическим, характерны определенные стадии существования:

1. латентная стадия, в которой вирусом никаких действий не предпринимается;2. инкубационная стадия, в которой основная задача вируса - создать как можно больше своих копий и внедрить их в среду обитания;3. активная стадия, в которой вирус, продолжая размножаться, проявляется и выполняет свои деструктивные действия.

Сейчас существуют сотни тысяч различных вирусов, и их можно классифицировать по нескольким признакам.

По среде обитания вирусы можно разделить на:

1.файловые;2.загрузочные;3.файлово-загрузочные;4.сетевые;5.документные. Файловые вирусы чаще всего внедряются в исполняемые файлы, имеющие расширения .ехе и .com (самые распространенные вирусы), но могут внедряться и в файлы с компонентами операционных систем, драйверы внешних устройств, объектные файлы и библиотеки, в командные пакетные файлы (вирус подключает к такому файлу исполняемые программы, предварительно заразив их), программные файлы на языках процедурного программирования (заражают при трансляции исполняемые файлы). Файловые вирусы могут создавать файлы-двойники (компаньоны-вирусы). В любом случае файловые вирусы при запуске программ, ими зараженных, берут на время управление на себя и дезорганизуют работу своих "квартирных хозяев".

Загрузочные вирусы внедряются в загрузочный сектор дискеты (boot-sector) или в сектор, содержащий программу загрузки системного диска (master boot record). При загрузке DOS с зараженного диска такой вирус изменяет программу начальной загрузки либо модифицируют таблицу размещения файлов на диске, создавая трудности в работе компьютера или даже делая невозможным запуск операционной системы.

Файлово-загрузочные вирусы интегрируют возможности двух предыдущих групп и обладают наибольшей "эффективностью" заражения.Сетевые вирусы используют для своего распространения команды и протоколы телекоммуникационных систем (электронной почты, компьютерных сетей).

Документные вирусы (их часто называют макровирусами) заражают и искажают текстовые файлы (.doc) и файлы электронных таблиц некоторых популярных редакторов. Комбинированные сетевые макровирусы не только заражают создаваемые документы, но и рассылают копии этих документов по электронной почте.

По способу заражения среды обитания вирусы делятся на: -резидентные; -нерезидентные. Резидентные вирусы после завершения инфицированной программы остаются в оперативной памяти и продолжают свои деструктивные действия, заражая следующие исполняемые программы и процедуры вплоть до момента выключения компьютера. Нерезидентные вирусы запускаются вместе с зараженной программой, и после ее завершения из оперативной памяти удаляются.

Вирусы бывают неопасные и опасные. Неопасные вирусы тяжелых последствий после завершения своей работы не вызывают; они прерывают на время работу исполняемых программ, создавая побочные звуковые и видеоэффекты (иногда даже приятные), или затрудняют работу компьютера, уменьшая объем свободной оперативной и дисковой памяти. Опасные вирусы могут производить действия, имеющие далеко идущие последствия: искажение и уничтожение данных и программ, стирание информации в системных областях диска и даже вывод из строя отдельных компонентов компьютера (жесткие диски, Flash-чипсет BIOS, перепрограммируя его). По алгоритмам функционирования вирусы весьма разнообразны, но можно говорить о таких, например, их группах, как:

1. паразитические вирусы, изменяющие содержимое файлов или секторов диска; они достаточно просто могут быть обнаружены и уничтожены;

2. вирусы-репликаторы ("черви" WORM), саморазмножающиеся и распространяющиеся по телекоммуникациям и записывающие по вычисленным адресам сетевых компьютеров транспортируемые ими опасные вирусы (сами "черви" деструктивных действий не выполняют, поэтому их часто называют псевдовирусами);

3. "троянские\*- вирусы маскируются под полезные программы (существуют в виде самостоятельных программ, имеющих то же имя, что и действительно полезный файл, но иное расширение имени; часто, например, присваивают себе расширение .com вместо .ехе) и выполняют деструктивные функции (например, очищают файловые структуры); самостоятельно размножаться, как правило, не могут;

4. вирусы-невидимки (стелс-вирусы), по имени самолета-невидимки "stealth", способны прятаться при попытках их обнаружения; они перехватывают запрос антивирусной программы и мгновенно либо удаляют временно свое тело из зараженного файла, либо подставляют вместо своего тела незараженные участки файлов;

5. самошифрующиеся вирусы (в режиме простоя зашифрованы, и расшифровываются только в момент начала работы вируса);

6. мутирующиеся вирусы (периодически автоматически видоизменяются, копии вируса не имеют ни одной повторяющейся цепочки байт), необходимо каждый раз создавать новые антивирусные программы для обезвреживания этих вирусов;

7. "отдыхающие" вирусы (основное время проводят в латентном состоянии и активизируются только при определенных условиях, например, вирус "Чернобыль" в сети Интернет функционирует только в день годовщины чернобыльской трагедии).

Прежде всего следует знать возможные источники заражения вирусами и аккуратно с ними работать, т.е. осуществлять антивирусную профилактику (особенно если ты на LANе, там много любителей засылать трояны и мониторить). Источниками вирусного заражения могут явиться только съемные носители и системы телекоммуникаций.

Вирус можно написать на любом языке программирования, конечно же, самыми распространенными являются C++ и Delphi, но можно и на "бэйсике", все зависит от назначения вируса.

При подробном изучении вирусов их научились объединять в семейства и распознавать по специальным сигналам и текстам. Каждое семейство имеет своё название.

[1] Time, семейство

Резидентные неопасные вирусы. Перехватывают INT 1Ch, 21h и записываются в конец запускаемых .EXE-файлов. Приблизительно раз в час пищат несколько раз спикером компьютера.

[2] Havoc (Stealth\_Boot), семейство

Загрузочные стелс- вирусы. При загрузке с пораженного флоппи записываются в MBR винчестера. Затем перехватывают INT 13h и поражают флоппи-диски при чтении с них. Заражение дискет происходит по алгоритму "Brain".

В зависимости от системного таймера "Havoc.a,b,Innocent" стирают сектора дисков. "Havoc.Amse" безобиден, никак не проявляется.

"Havoc.Alfredo" расшифровывает текст и выводит его на принтер:

LIMA – PERU (c) Laboratorio Luz de Luna ANGEL X TE SALUDA

[3] Brain, семейство

Состоит из двух практически совпадающих безобидных вирусов: "Brain-Ashar" и "Brain-Singapore". Они заражают загрузочные сектора дискет при обращении к ним (INT 13h, AH=02h). Продолжение вируса и первоначальный загрузочный сектор размещаются в секторах, которые принадлежат свободным кластерам диска. При поиске этих кластеров вирусам приходится анализировать таблицу размещения файлов (FAT). В FAT эти кластеры помечаются как сбойные (так называемые "псевдосбойные" кластеры). У зараженного диска устанавливается новая метка "(C) Brain". Вирусы используют "стелс"-механизм: при попытке просмотра загрузочного сектора зараженного диска они "подставляют" истинный сектор.

[4] Vienna, семейство

Нерезидентные вирусы. При запуске ищут .COM-файлы и записывается в их конец. Ищут файлы в текущем каталоге и в зависимости от версии вируса в корневом каталоге, либо в каталогах, отмеченных системной переменной PATH.

Заражение происходит при запуске инфицированной программы, при этом заражается не более одного файла. Многие вирусы семейства при попытке заражения проверяют у файла значение секунд (или месяца в зависимости от версии вируса) последней модификации файла. Если оно равно 1Fh (62 секунды, соответственно 0Dh - 13-й месяц), то файл не заражается. Некоторые представители семейства в зависимости от таймера могут "убивать" файлы, записывая в их начало 5 байтов либо команды перехода на перезагрузку JMP F000:FFF0, либо JMP C800:0005, JMP C800:0000 или JMP C800:0006 в зависимости от версии вируса.

[5] Cascade

Очень опасен. Иногда выводит сообщение:

IL SISTEMA К FOTTUTO!!

S.E.K. VIRUS Made in ITALY RM

5iD G.Ferraris 90/91 (c)

и стирает сектора дисков. Также уничтожает файл CHKLIST.CPS.

[6] Ping-Pong

Не опасен. Перехватывает INT 8, 13h. Имеет байт, содержащий номер версии вируса. Если обнаруживает диск, зараженный своей предыдущей версией, то "обновляет" ее. Вызывает видеоэффект скачущего шарика (знак 07h ASCII), который перемещается по экрану, отражаясь от знаков и границ экрана.

[7] VirDem, семейство

Опасные нерезидентные вирусы, записываются в начало .COM-файлов текущего диска.

"Virdem.833" двигает по экрану изображение жука.

"VirDem.1542" заполняет экран цветной абстрактной картинкой.

"VirDem.1336.a" снимает и не восстанавливает атрибуты файла.

 [8] GoodTimes - миф о компьютерном вирусе

В начале декабря 1994 по сетям Internet и FIDO прошло сообщение о якобы существующем вирусе, который заражает компьютер посредством электронной почты - при получении и чтении писем. Сообщение выглядело следующим образом:

Here is some important information. Beware of a file called GoodTimes. Happy Chanukah everyone, and be careful out there. There is a virus on America Online being sent by E-Mail. If you get anything called "Good Times", DON'T read it or download it. It is a virus that will erase your hard drive. Forward this to all your friend. It may help them a lot.

Это сообщение вызвало настоящую панику среди пользователей Internet. Было зафиксировано даже несколько сообщений о действительно зараженных компьютерах - однако все такие сообщения были "секонд-хенд", но никто в действительности так никогда и не встретился с этим монстром (по той причине, что такого вируса никогда и не было).

Весной 1995 история с "GoodTimes" продолжилась еще одним сообщением на ту же тему - о вирусе, распространяющем себя по всем E-mail адресам, которые присутствуют в ящиках Inbox и SentMail. Как и в первом случае, никакого такого вируса обнаружено так и не было.

Тогда же в очередном номере журнала вирусописателей "VLAD" появились исходные тексты вируса, названного его автором "Good Times" (разработчики антивирусов назвали сей вирус "GT-Spoof"). Это был обычный DOS-вирус, не имевший никакого отношения к сетям и Internet.

[9] Vacsina, Yankee, семейство

Семейство вирусов "VACSINA" (не "VACCINA"!) и "Yankee" насчитывает более 40 файловых резидентных неопасных вирусов. Характерной особенностью вирусов данного семейства является то, что они восстанавливают файлы, зараженные предыдущими версиями вирусов семейства, и затем инфицируют их снова. Заражают COM- и EXE-файлы при их выполнении (вирусы версий до 26h) или загрузке в память (вирусы версий 26h и выше). Стандартно заражают COM- файлы. Кроме того, вирусы "Vacsina" увеличивают длину заражаемого файла до параграфа. Начиная с версии 2Ah к файлу после заражения дописываются дополнительные 4 байта.

Вирусы младших версий (до 23h) инфицируют EXE-файлы специальным образом: файлы переводятся в формат COM-файлов. Для этого к файлу дописывается небольшой фрагмент вируса (132 байта), настраивающий адреса по таблице адресов при загрузке файла в память для выполнения, и изменяются первые три байта файла (JMP на фрагмент). Дописанные к файлу 132 байта не распространяют вируса. Их действие заключается только в настройке адресов программы при ее запуске. Обработанный таким образом файл будет выполняться операционной системой и заражаться многими вирусами как COM-файл. При запуске EXE-программы, содержащейся в подобном файле, управление передается на фрагмент настройки адресов, который анализирует таблицу адресов в заголовке файла и соответствующим образом корректирует загруженную программу. Затем управление передается на стартовый адрес, указанный в заголовке файла. Вирусы перехватывают вектор прерывания 21h, а некоторые представители семейства "Yankee" - INT 1, 3, 9, 1Ch.

Вирусы вызывают звуковые эффекты: при заражении файла вирусом "VACSINA" раздается звуковой сигнал (BELL), вирусы "Yankee" в зависимости от некоторых условий (при одновременном нажатии клавиш Alt-Ctrl-Del либо в 17.00) исполняют мелодию "Yankee Doodle Dandy". При некоторых условиях вирус "Vacsina.06" расшифровывает и выдает на экран строку "Az sum vasta lelja."

Yankee.2189

Семейство "Yankee". Зашифрован, периодически 'крутит' символы '/', '\', '- ', '|'.

Yankee.Estonia.1716

Семейство "Yankee". Резидентный опасный вирус. По понедельникам в 14 часов расшифровывает и выводит в центр экрана текст: "Independent Estonia presents", затем играет "Собачий вальс" и перезагружает компьютер.

[10] Aids

Резидентный очень опасный вирус. Перехватывает INT 3, 21h и записывается в конец EXE-файлов при их закрытии. В каждый 16-й закрываемый COM-файл записывает часть своего кода (файл не восстанавливается, так как вирус не сохраняет старое содержимое файла). При запуске такого файла не экран крупными буквами выдается слово "AIDS".

[11] Peterburg

Бехобидный резидентный вирус. Перехватывает INT 21h и записывается в начало .COM-файлов при их запуске. Никак не проявляется.

[12] Voronezh, семейство

Voronezh.370,600 - резидентные вирусы, безобидны. Часть вируса "Voronezh.600" (50 байт) зашифрована (XOR DDh). Перехватывают INT 21h и записываются в начало .COM- файлов при загрузке их в память для выполнения, "Voronezh.370" не заражает COMMAND.COM. При внедрении в файл переписывают его начало в конец файла, а свою копию помещают на освободившееся место в начале. При этом переписываемая часть файла шифруется (XOR BBh). Никак не проявляются и не имеют деструктивных функций. "Voronezh.600" содержит зашифрованный (XOR 1Ah) текст "Oleynikoz S., 1990". Видимо, проба пера начинающего программиста, так как невооруженным глазом заметно достаточно слабое знание возможностей языка ассемблера.

Voronezh.650

Резидентный неопасный вирус. Перехватывает INT 21h и поражает выполняемые COM-файлы по алгоритму вируса "Voronezh.600". При запуске файлов (приблизительно 1 раз на 60 запусков) сообщает:

Video mode 80x25 not supported

Voronezh.1600

Резидентный опасный вирус. Перехватывает INT 21h и поражает файлы при их выполнении или открытии. COM-файлы заражаются по схеме вируса "Voronezh.600". EXE-файлы инфицируются по сложному алгоритму: у них изменяется пять байт точки входа в программу на код команды CALL FAR Loc\_Virus, при этом изменение адреса точки входа в заголовке файла не требуется. Вирус корректирует таблицу настройки адресов (ТНА): добавляет в нее один элемент, соответствующий команде CALL FAR Loc\_Virus; необходимым образом изменяет один элемент ТНА, указывающий на измененные 5 байт (если такой элемент существует). Затем вирус дописывает к файлу свою копию.

Вирус содержит ошибки: анализируются не более 640 элементов ТНА; не анализируется случай, когда модифицируемый элемент ТНА указывает на пятый байт от точки входа (т.е. слово, которое настраивается при загрузке файла, лежит на границе изменяемых 5 байт). При запуске такого файла возможно зависание компьютера.

[13] LoveChild, семейство

Очень опасные резидентные вирусы. Перехватывают INT 21h и записывается в конец COM-файлов.

LoveChild.488

При создании своей резидентной копии копирует себя в таблицу векторов прерываний по адресу 0000:01E0. Затем заражает .COM-файлы при их загрузке в память, при открытии и создании. Изменяет первые 4 байта файла на команду перехода на тело вируса (STI; JMP Loc\_Virus).

Имеет деструктивные функции: в зависимости от счетчика времени может уничтожать файлы или создавать вместо файла подкаталог с таким же именем.

Вирус периодически модифицирует EXE-файлы таким образом, что их запуск вызовет стирание секторов винчестера (стирается часть информации, расположенной на секторах, соответствующих 0-3 головкам записи/чтения).

LoveChild.2710

Резидентный очень опасный стелс -вирус. Перехватывает INT 13h, 21h и записывается в конец COM-файлов. Работает только в DOS 3.30, т.к. делает "врезку" в теле операционной системы. Если на машине стоит другая версия DOS, выводит фразу: «Тебе мама не говорила в детстве, что лучше DOS 3.30 версии нет?» после чего портит MBR. С полуночи до 4 часов утра при запуске зараженных программ распечатывает экран. 22 февраля, 32 апреля (?!), 23 июня, 24 августа, 6 октября и 5 ноября занимается гнусностью: пишет "Привет от ГКЧП", затем очищает экран и выводит длинное послание, после чего стирает информацию на винчестере. Вот часть этого сообщения: «Вирусисты всех стран, соединяйтесь. Объединение MMM предлагает за рубли, по ценам ниже рыночных отечественные вирусы, совместимые с IBM PC/AT PC/XT с любой периферией. Поставка со склада в Москве. Гарантийное и послегарантийное обслуживание. У МММ не было проблем. LoveChild v4 in reward for software stealing. LoveChild virus family. (c) Flu Systems intnl. Россия-Украина. Вирусы LoveChild будут появляться до тех пор, пока в СССР (или как его там) не будет принят закон об авторских правах. А пока - червонец в зубы и к Лозинскому».

[14] Win95.HPS, aka Hanta

Заражает PE-файлы (Portable Executable). При запуске инсталлирует себя в ядро Windows95/98, перехватывает системные события и записывается в конец PE EXE-файлов, к которым идет обращение. Длина вируса - 5124 байт. При заражении файлов шифрует себя полиморфик-кодом и записывает результат в последнюю секцию файла, предварительно увеличив ее размер, и затем меняет адрес точки входа в заголовке файла. Размер полиморфик-цикла варьируется от заражения к заражению, поэтому длина файлов может быть увеличена на различные значения.

Вирус проявляется видео-эффектом: если инсталляция вируса в память Windows произошла в субботу, то вирус затем переворачивает справа-налево изображения в неупакованных BMP-файлах. Повторного переворачивания не происходит - вирус помечает такие BMP-файлы записав в них метку DEADBABEh.

[15] Win95.CIH

Резидентный вирус, работает только под Windows95 и заражает PE-файлы (Portable Executable). Имеет довольно небольшую длину - около 1Кб. Обнаружен "в живом виде" в Тайване в июне 1998 - был разослан автором вируса в местные Интернет-конференции. За последующую неделю вирусные эпидемии были зарегистрированы в Австрии, Австралии, Израиле и Великобретании, затем вирус был обнаружен и в нескольких других странах, включая Россию.

При запуске зараженного файла вирус инсталлирует свой код в память Windows, перехватывает обращения к файлам и при открытии PE EXE-файлов записывает в них свою копию. Содержит ошибки и в некоторых случаях завешивает систему при запуске зараженных файлов. В зависимости от текущей даты стирает Flash BIOS и содержимое дисков.

Запись в Flash BIOS возможна только на соответствующих типах материнских плат и при разрешающей установке соответственного переключателя. Этот переключатель обычно установлен в положение "только чтение", однако это справедливо не для всех производителей компьютеров. К сожалению Flash BIOS на некоторых современных материнских платах не может быть защищена переключателем: одни из них разрешают запись в Flash при любом положении переключателя, на других защита записи в Flash может быть отменена программно.

При тестировании вируса в лаборатории память Flash BIOS осталась неповрежденной - по непонятным причинам вирус завесил систему без каких-либо побочных эффектов. Однако из других источников известно, что вирус при определенных условиях действительно портит содержимое Flash BIOS.

После успешного стирания Flash-памяти вирус переходит к другой деструктивной процедуре: стирает информацию на всех установленных винчестерах. При этом вирус использует прямой доступ к данным на диске и тем самым обходит встроенную в BIOS стандартную антивирусную защиту от записи в загрузочные сектора.

Известно три версии вируса. Они достаточно похожи друг на друга и отличаются лишь незначительными деталями кода в различных подпрограммах. Версии вируса имеют различные длины, строки текста и дату срабатывания процедуры стирания дисков и Flash BIOS:

Длина Текст Дата срабатывания Обнаружен "в живом виде"

1003 CCIH 1.2 TTIT 26 апреля

Да

1010 CCIH 1.3 TTIT 26 апреля

Нет

1019 CCIH 1.4 TATUNG 26 каждого месяца Да - во многих странах[1]

[16] Macro.Word97.Melissa

Заражает файлы документов и шаблонов MS Word и рассылает свои копии в сообщениях электронной почты при помощи MS Outlook. Вирус распространяется чрезвычайно быстро: процедура рассылки зараженных писем отсылает большое количество вирусных копий по адресам из всех списков адресной книги MS Outlook. Вирус также изменяет системный реестр, выключает антивирусную защиту MS Word.

Для рассылки своих копий через электронную почту вирус использует возможность Visual Basic активизировать другие приложения MS Windows и использовать их процедуры. Вирус вызывает MS Outlook, считывает из базы адресов Outlook адреса электронной почты и посылает по этим адресам сообщение. Это сообщение содержит:

Тема: "Important Message From [UserName]" (UserName берется из базы адресов).

В письме написано: "Here is that document you asked for ... don't show anyone else ;-)". К сообщению также присоединен документ (естественно зараженный), причем вирус присоединяет тот документ, который в данный момент редактируется (активный документ). Как побочный эффект подобного распространения передаются файлы пользователя, которые могут содержать конфиденциальные данные.

Количество рассылаемых писем зависит от конфигурации адресной книги Outlook (базы адресов e-mail) на конкретном компьютере. Вирус открывает каждый список в адресной книге и отсылает зараженное сообщение по 50 первым адресам из каждого списка. Если в списке меньше 50 адресов, вирус отсылает сообщение на все из них. Для каждого списка создается одно зараженное письмо, поле адресата которого содержит первые 50 адресов из списка.

Вирус использует электронную почту для своего распространения только один раз - для этого проверяется специальная "метка" в системном реестре:

HKEY\_CURRENT\_USER\Software\Microsoft\Office\ "Melissa?" = "... by Kwyjibo"

Если этот ключ не найден, то вирус посылает сообщения электронной почты с приложенными зараженными документами и создает этот ключ в реестре. Вирус способен распространяться не только в версии Word97, но и в Word2000. Эта особенность вируса связана с возможностью Word2000 преобразовывать файлы старого формата в новый при их открытии. При этом в новый формат конвертируются все необходимые секции файла, включая макро-программы (включая код вируса). Как результат, вирус получает возможность распространяться в среде Word 2000.

При запуске вируса в Word 2000 он производит дополнительные действия: выключает (устанавливает в минимум) установки безопасности (антивирусную защиту).

Код вируса хранится в одном макро модуле "Melissa" и состоит из одной авто-процедуры: в зараженных документах это "Document\_Open", в NORMAL.DOT (область глобальных макросов) - "Document\_Close". Вирус заражает NORMAL.DOT при открытии зараженного документа и записывается в другие документы при их закрытии. При заражении вирус копирует свой код построчно из зараженного объекта в файл-жертву. В случае заражения области глобальных макросов вирус переименовывает свою процедуру в "Document\_Close", когда же происходит заражение документов, то вирусная процедура переименовывается в "Document\_Open". В результате вирус заражает Word при открытии зараженного документа, а при закрытии других документов они, в свою очередь, оказываются зараженными.

Вирус также содержит процедуру-эффект, которая срабатывает в случае если день равен минутам в момент активации вирусного кода. Эта процедура вставляет следующий текст в редактируемый документ: Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here.

Этот текст, так же, как и прозвище автора вируса ("Kwyjibo"), взят из телевизионного мульт-сериала "Симпсоны" ("Simpsons"). Вирус также содержит комментарии в своем коде:

WORD/Melissa written by Kwyjibo

Works in both Word 2000 and Word 97

Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!

Word -> Email | Word 97 <--> Word 2000 ... it's a new age!

[17] Explorer, семейство

Неопасные резидентные зашифрованные вирусы. Перехватывают INT 21h и записываются в конец запускаемых EXE-файлов. Также ищут и поражают \*.SYS- файлы. Уничтожают файлы CHKLIST.MS и CHKLIST.CPS. В зависимости от своих внутренних счетчиков перехватывают INT 15h, 1Ch и проявляются каким-то видео-эффектом.

[18] I-Worm.LoveLetter

Этот Интернет-червь вызвал массовые поражения компьютеров и сетей в начале мая 2000. Червь распространяется в электронных письмах и при активизации рассылает себя с зараженных компьютеров. При своем распространении червь использует почтовую систему Microsoft Outlook и рассылает себя по всем адресам, которые хранятся в адресной книге Outlook. В результате пораженный компьютер рассылает столько зараженных писем, сколько адресов хранится в адресной книге.

Червь написан на скрипт-языке Visual Basic Script (VBS). Запускается только в операционных системах с установленным Windows Scripting Host (WSH) (в Windows 98, Windows 2000 он установлен по умолчанию). При размножении червь использует функции Outlook, которые доступны только в Outlook98/2000.

При активизации червь рассылает свои копии по электронной почте, инсталлирует себя в систему, выполняет деструктивные действия, скачивает из Интернета и устанавливает в систему троянский файл. Червь также способен распространяться через IRC-каналы.

Червь ищет все файлы на всех доступных дисках. Для файлов с разными расширениями червь выполняет различные действия: VBS, VBE: записывает вместо них свою копию. JS, JSE, CSS, WSH, SCT, HTA: переименовывает их с расширением .VBS и записывает в них свою копию.

JPG, JPEG: добавляет к именам файлов расширение .VBS и записывает в них свою копию (например, PIC1.JPG.VBS). Оригинальный файл червь удаляет. MP2, MP3: создает новый файл с именем MP-файла и расширением .VBS и записывает в него свою копию. У первоначальных MP-файлов устанавливает атрибут "скрытый".

[19] I-Worm.Sircam

Опасный сетевой червь, распространяющийся по сети Интернет и ресурсам локальных вычислительных сетей. Файл-носитель червя представляет собой Windows-приложение, размером около 130 Кб, написанное на языке программирования Delphi. В процессе распространения червь может прикреплять к своим файлам дополнительные файлы DOC, XLS, ZIP и других форматов (см. ниже), так что размер вложенного файла может превышать 130 Кб.

После запуска (например, двойным щелчком на вложенном зараженном файле), червь внедряется в систему, рассылает зараженные сообщения (содержащие вложенные файлы с копией червя), заражает компьютеры, подключенные к доступной ЛВС (если в сети существуют диски, доступные для записи), а также, в зависимости от системной даты, выполняет встроенную деструктивную процедуру.

В зависимости от текущей системной даты и времени, червь с вероятностью 5% удаляет все файлы и поддиректории на диске, где установлена Windows. При каждой загрузке операционной системы с вероятностью 2% червь создает файл SirCam.Sys в корневой директории текущего диска и записывает в него следующий текст:

[SirCam\_2rP\_Ein\_NoC\_Rma\_CuiTzeO\_MicH\_MeX]

[SirCam Version 1.0 Copyright L 2001 2rP Made in / Hecho en - Cuitzeo,

Michoacan Mexico]

С каждым разом червь добавляет этот файл, тем самым постепенно поглощая свободное место на диске. Эти и многие другие текстовые строки в теле червя содержатся в зашифрованном виде.

[20] IIS-Worm.CodeRed (AKA "Code Red", "Bady")

Первый представитель данного семейства сетевых червей, "Code Red" (также известный под именем "Bady"), по данным ZDNet, он заразил около 12 000 серверов по всему миру и провел крупномасштабную DDoS атаку на Web сервер Белого дома (www.whitehouse.gov), вызвав нарушение его нормальной работы.

"Bady" заражает только компьютеры под управлением Windows 2000 (без установленных сервисных пакетов), с установленным Microsoft Internet Information Server (IIS) и включенной службой индексирования (Indexing Service). Вместе с тем, именно это программное обеспечение чаще всего используется на коммерческих Web, FTP и почтовых серверах, что и определило широкое распространение червя. Масштабы эпидемии могли бы быть еще более внушительными, если бы червь поражал и другие версии Windows, например Windows NT и Windows XP. Однако автор червя умышленно "нацелил" его только на системы Windows 2000.

Для проникновения на удаленные компьютеры червь использует обнаруженную в июне 2001 г. брешь в системе безопасности IIS, которая позволяет злоумышленникам запускать на удаленных серверах посторонний программный код. Для этого "Bady" посылает на случайно выбранный удаленный сервер специальный запрос, дающий компьютеру команду запустить основную программу червя, которая в свою очередь попытается таким же образом проникнуть на другие серверы. Одновременно в памяти компьютера может существовать сразу сотни активных процессов червя, что существенно замедляет работу сервера.

Важной особенностью "Bady" является то, что в процессе работы он не использует никаких временных или постоянных файлов. Данный червь уникален: он существует либо в системной памяти зараженных компьютеров, либо в виде TCP/IP-пакета при пересылке на удаленные машины. Подобная "бестелесность" представляет серьезную проблему для защиты серверов, поскольку требует установки специальных антивирусных модулей на межсетевые экраны.

Помимо значительного замедления работы зараженных компьютеров, "Bady" имеет другие побочные действия. Во-первых, червь перехватывает обращения посетителей к Web сайту, который управляется зараженным IIS-сервером, и вместо оригинального содержимого передает им следующую страницу: После показа фальсифицированной стартовой страницы взломанного Web сайта в течение 10 часов, червь автоматически возвращает все на свои места и посетители видят оригинальную версию сайта. Важно отметить, что данный эффект проявляется только на системах, где по умолчанию используется язык "US English". Во-вторых: между 20 и 27 числами каждого месяца включительно червь осуществляет DDoS (Distributed Denial of Service) атаку на сайт Белого дома США (www.whitehouse.gov). Для этого копии червя на всех зараженных компьютерах посылают многочисленные запросы на соединение, что вызывает зависание сервера, обслуживающего данный Web-сайт.

Для нейтрализации, а также в качестве профилактической меры для предотвращения проникновения червя на сервер, мы рекомендуем пользователям немедленно установить "заплатку" для исправления "бреши" в системе безопасности IIS.

[21] I-Worm.MyLife

Вирус-червь. Распространяется через Интернет в виде файлов, прикрепленных к зараженным письмам.

Червь является приложением Windows (PE EXE-файл), имеет размер около 30 K (упакован UPX, размер распакованного файла - около 55 K), написан на Visual Basic.

Деструктивная процедура:

Червь проверяет текущее время, и если текущее значение минуты больше 45, червь запускает деструктивную процедуру: он удаляет файлы с расширениями .SYS и .COM в корневой директории диска C:, файлы с расширениями .COM, .SYS, .INI, .EXE в каталоге Windows, а также файлы с расширениями .SYS, .VXD, .EXE, .DLL в системном каталоге Windows.

[22] I-Worm.Cervivec!

Интернет-червь Cervivec распространяется через Интернет в виде файлов, прикрепленных к зараженным письмам. Червь является приложением Windows (PE EXE-файл), имеет размер около 230K (упакован UPX, размер распакованного файла - около 670K), написан на Delphi.

Червь активизируется только если пользователь сам запускает зараженные файл (при двойном щелчке на вложении). Затем червь инсталлирует себя в систему и запускает процедуры своего распространения. Для скрытия своей активности червь запускает видео-эффект: разноцветные "червяки", поедающие экран.[2]

**3. Методы защиты от компьютерных вирусов**

Существуют три рубежа защиты от компьютерных вирусов:

* предотвращение поступления вирусов;
* предотвращение вирусной атаки, если вирус всё-таки поступил на компьютер;
* предотвращение разрушительных последствий, если атака всё-таки произошла.

Существует три метода реализации рубежей обороны:

* программные методы защиты;
* аппаратные методы защиты;
* организационные методы защиты.

В вопросе защиты ценных данных часто используют бытовой подход: «болезнь лучше предотвратить, чем лечить». К сожалению, именно он и вызывает наиболее разрушительные последствия. Создавая бастионы на пути проникновения вирусов в компьютер, нельзя полагаться на их прочность и остаться не готовым к тому, что надо делать, когда вирусная атака всё-таки произойдёт. К тому же вирусная атака – далеко не единственная возможность полной утраты информации.

Существуют программные сбои, которые могут вывести из строя операционную систему, аппаратные сбои, способные сделать жёсткий диск нечитаемым. Всегда существует вероятность того, что компьютер вместе с ценными данными может быть утрачен в результате кражи, пожара или иного стихийного бедствия.

Поэтому создавать систему защиты следует в первую очередь «с конца» - с предотвращения разрушительных последствий любого воздействия, будь то вирусная атака, кража в помещении или физический выход жёсткого диска из строя. Надёжная и безопасная работа с компьютером достигается только тогда, когда любое неожиданное событие, в том числе и полное уничтожение данных на жёстком диске, не приведёт к ощутимым потерям (потеря нескольких часов на восстановление работоспособности компьютерной системы в данном случае не считается значительной).

**4. Средства антивирусной защиты**

Основным средством защиты информации является резервное копирование наиболее ценных данных. В случае утраты информации по любой из вышеперечисленных причин жёсткие диски переформатируют и подготавливают к новой эксплуатации. На «чистый» отформатированный диск устанавливают операционную систему с дистрибутивного компакт-диска, затем под её управлением устанавливают всё необходимое программное обеспечение, которое тоже берут с дистрибутивных носителей. Восстановление компьютера завершается восстановлением данных, которые берут с резервных носителей.

При резервировании данных следует также иметь в виду и то, что надо отдельно сохранять всю регистрационную и парольную информацию для доступа к сетевым службам Интернета. Её можно хранить, например, в записной книжке.

Создавая план мероприятий по резервному копированию информации, необходимо учитывать, что резервные копии должны храниться отдельно от компьютера. То, есть например, резервирование информации на отдельном жёстком диске того же компьютера только создаёт иллюзию безопасности. Относительно новым и достаточно надёжным методом хранения данных является хранение их на удалённых серверах в Интернете. Есть службы, бесплатно предоставляющие пространство (до нескольких Мбайт) для хранения данных пользователя.

Вспомогательными средствами защиты информации являются антивирусные программы и средства аппаратной защиты. Так, например, простое отключение перемычки на материнской плате не позволит осуществить стирание перепрограммируемой микросхемы ПЗУ (флэш-BIOS), независимо от того, кто будет пытаться это сделать: компьютерный вирус или неаккуратный пользователь.

Существует достаточно много программных средств антивирусной защиты. Они предоставляют следующие возможности.

1. Создание образа жёсткого диска на внешних носителях (например, на гибких дисках). В случае выхода из строя информации в системных областях жёсткого диска сохранённый «образ диска» может позволить восстановить если и не всю информацию, то по крайней мере её большую часть. Это же средство может защитить от утраты информации при аппаратных сбоях и при неаккуратном форматировании жёсткого диска.
2. Регулярное сканирование жёстких дисков в поисках компьютерных вирусов. Сканирование обычно выполняется автоматически при каждом включении компьютера и при размещении внешнего диска в считывающем устройстве. При сканировании следует иметь в виду, что антивирусная программа ищет вирус путём сравнения кода программ с кодами известных ей вирусов, хранящимися в базе данных. Если база данных устарела, а вирус является новым, сканирующая программа его не обнаружит. Для надёжной работы следует регулярно обновлять антивирусную программу. Желательная периодичность обновления – 1 раз в две недели; допустимая – один раз в три месяца. Для примера скажем, что разрушительные последствия атаки вируса W95.CIH.1075 («Чернобыль»), вызвавшего уничтожение информации на сотнях тысяч компьютеров 26 апреля 1999 года, было связано не с отсутствием средств защиты от него, а с длительной задержкой (более года) в обновлении этих средств.
3. Контроль за изменением размеров и других атрибутов файлов. Поскольку некоторые компьютерные вирусы на этапе размножения изменяют параметры заражённых файлов, контролирующая программа может обнаружить их деятельность и предупредить пользователя.
4. Контроль за обращениями к жёсткому диску. Поскольку наиболее опасные операции, связанные с работой компьютерных вирусов, так или иначе обращены на модификацию данных, записанных на жёстком диске, антивирусные программы могут контролировать обращения к нему и предупреждать пользователя о подозрительной активности.

**Вывод**

## Интернет стремительно входит в нашу жизнь. Сегодня это уже не только Всемирная справочная система, но и средство связи, которое с каждым днём всё шире и шире используется не только для личного, но и для делового общения и даже для коммерции.

## Пока вопросами безопасности в Интернете занимаются в основном специалисты, но всего лишь через несколько лет коммерциализация Интернета достигнет такого уровня, что эти вопросы станут обычным делом для рядовых граждан. К этому надо готовиться уже сегодня, и полезно знать основные понятия компьютерной безопасности, понимать, о чём идёт речь, и знать простейшие приёмы самозащиты.

## В вычислительной технике понятие безопасности является весьма широким. Оно подразумевает и надёжность работы компьютера, и сохранность ценных данных, и защиту информации от внесения в неё изменений неуполномоченными лицами, и сохранение тайны переписки в электронной связи. Разумеется, во всех цивилизованных странах на страже безопасности граждан стоят законы, но в сфере вычислительной техники правоприменительная практика пока не развита, а законотворческий процесс не успевает за развитием технологий, поэтому надёжность работы компьютерных систем во многом опирается на меры самозащиты.

**Список использованной литературы**

1. Караменс В.В., Григ Н.Р. Компьютер: прошлое, настоящее, будущее. М., 2001.
2. Паулин К. Малый толковый словарь по вычислительной технике: перевод с немецкого. М., 1995.
3. Справочник школьника: 5-11 классы. – М.: АСТ-ПРЕСС, 2002.
4. Фигурнов В.Э. IBM РС для пользователя. М., 2002.