**Воронежский институт высоких технологий – АНОО ВПО**

**факультет заочного обучения**

**контрольная работа**

**по дисциплине информатика**

Воронеж 2010

**1. Кодирование различных типов информации**

С помощью набора битов, можно представить любое число и любой знак. В информационных документах широко используются не только русские, но и латинские буквы, цифры, математические знаки и другие специальные знаки, всего их количество составляет примерно 200-250 символов. Поэтому для кодировки всех указанных символов используется восьмиразрядная последовательность цифр 0 и 1. Таким образом, текстовая информация кодируется с помощью кодовой таблицы.

Кодовая таблица – это внутреннее преставление символов в компьютере. Во всем мире в качестве стандарта принята таблица ASCII – Американский стандартный код для обмена информацией. Для хранения двоичного кода одного символа выделен 1 байт = 8 бит.

Следует отметить, что указанный способ кодирования используется тогда, когда к нему не предъявляются дополнительные требования, такие как необходимость указать на возникшую ошибку, исправление ошибки, секретность информации. При специальном кодировании коды получаются длиннее, чем в указанной таблице.

Наиболее просто кодируется числовая информация – она переводится в двоичную систему исчисления.

Для представления графической информации в двоичной форме используется так называемый поточечный способ. На первом этапе вертикальными и горизонтальными линиями делят изображение. Чем больше при этом получилось квадратов, тем точнее будет передана информация о картинке. Как известно из физики, любой цвет может быть представлен в виде суммы различной яркости зеленого, синего, красного цветов. Поэтому информация о каждой клетке должна содержать кодировку значения яркости и количеств зеленого, синего и красного компонентов. Таким образом кодируется растровое изображение – изображение, разбитое на отдельные точки. Объем растрового изображения определяется умножением количества точек на рисунке на информационный объем одной точки, который зависит от количества возможных цветов отображения (для черно-белого изображения информационный объем одной точки равен 1 биту и кодируется двумя цифрами – 0 или 1). Разные цвета и их оттенки получаются за счет наличия или отсутствия трех основных цветов – красного, синего, зеленого и их яркости. Каждая точка на экране кодируется с помощью 4 битов.

Векторное изображение кодируется разбиением рисунка на элементарные отрезки, геометрические фигуры и дуги. Положение этих элементарных объектов определяется координатами точек. Для каждой линии указывается ее тип (сплошная, пунктирная, штрих- пунктирная ), толщина и цвет. Информация о векторном изображении кодируется как обычная буквенно-цифровая и обрабатывается специальными программами.

Звуковая информация может быть представлена последовательностью элементарных звуков и пауз между ними. Вывод звуков из компьютера осуществляется синтезатором речи, который считывает из памяти хранящийся код звука. Речь человека имеет большое разнообразие оттенков, поэтому каждое произнесенное слово должно сравниваться с предварительно занесенным в память компьютера эталоном, и при их совпадении происходит его распознавание и запись.

**2. Состав системного блока**

Системный блок (рис. 1) – основная часть компьютера.



Рис. 1 - Системный блок компьютера

Он состоит из металлического корпуса, в котором располагаются основные компоненты компьютера. С ним соединены кабелями клавиатура, мышь и монитор. Внутри системного блока расположены:

микропроцессор, который выполняет все поступающие команды, производит вычисления и управляет работой всех компонентов компьютера;

оперативная память, предназначенная для временного хранения программ и данных;

системная шина, осуществляющая информационную связь между устройствами компьютера;

материнская плата (рис. 2), на которой находятся микропроцессор, системная шина, оперативная память, коммуникационные разъемы, микросхемы управления различными компонентами компьютера, счётчик времени, системы индикации и защиты;



Рис. 2 - Материнская плата

блок питания (рис. 3), преобразующий электропитание сети в постоянный ток низкого напряжения, подаваемый на электронные схемы компьютера;

вентиляторы для охлаждения греющихся элементов;



Рис. 3 - Блок питания

устройства внешней памяти, к которым относятся накопители на гибких и жестких магнитных дисках, дисковод для CD и DVD-дисков, предназначенные для длительного хранения информации.

Аппаратной основой системного блока является материнская плата - самостоятельный элемент, который управляет внутренними связями и с помощью системы прерываний взаимодействует с внешними устройствами. На материнской плате расположены все важнейшие микросхемы.

Персональные компьютеры делятся на стационарные и портативные. Стационарные обычно устанавливаются рабочем столе. Портативные компьютеры делятся на следующие категории:

переносные (portable), которые имеют небольшую массу и габариты и поддаются транспортировке одним человеком;

наколенные (laptop), выполненные в виде дипломата;

блокнотные (notebook), имеющие габариты большого блокнота;

карманные (pocket), которые помещаются в карман.

В соответствии с вышеприведенной классификацией, системные блоки могут иметь следующие типы корпусов:

Desktop



Tower



Notebook



**3. Топология сетей**

Выделяют следующие основные топологии сетей: шина, кольцо, звезда, дерево.

Топология типа общая ши́на, представляет собой общий кабель (называемый шина или магистраль), к которому подсоединены все рабочие станции. На концах кабеля находятся терминаторы, для предотвращения отражения сигнала.

Топология общая шина предполагает использование одного кабеля, к которому подключаются все компьютеры сети. Отправляемое рабочей станцией сообщение распространяется на все компьютеры сети. Каждая машина проверяет - кому адресовано сообщение и если ей, то обрабатывает его. Принимаются специальные меры для того, чтобы при работе с общим кабелем компьютеры не мешали друг другу передавать и принимать данные.

В топологии «шина» отсутствует центральный абонент, через которого передается вся информация, которая увеличивает ее надежность (ведь при отказе любого центра перестает функционировать вся управляемая этим центром система). Добавление новых абонентов в шину достаточно простое и обычно возможно даже во время работы сети. В большинстве случаев при использовании шины нужно минимальное количество соединительного кабеля по сравнению с другой топологией. Правда, нужно учесть, что к каждому компьютеру (кроме двух крайних) подходит два кабеля, что не всегда удобно.

Шине не страшны отказы отдельных компьютеров, потому что все другие компьютеры сети могут нормально продолжать обмен. Кроме того, так как используется только один кабель, в случае обрыва нарушается работа всей сети. Может показаться, что шине не страшен и обрыв кабеля, поскольку в этом случае остаются две полностью работоспособных шины. Однако из-за особенности распространения электрических сигналов по длинным линиям связи необходимо предусматривать включение на концах шины специальных устройств - Терминаторов.

Без включения терминаторов сигнал отражается от конца линии и искажается так, что связь по сети становится невозможной. Таким образом при разрыве или повреждении кабеля нарушается согласование линии связи, и прекращается обмен даже между теми компьютерами, которые остались соединенными между собой. Короткое замыкание в любой точке кабеля шины выводит из строя всю сеть. Надежность здесь выше, так как выход из строя отдельных компьютеров не нарушит работоспособность сети в целом. При построении больших сетей возникает проблема ограничения на длину связи между узлами, в таком случае сеть разбивают на сегменты. Сегменты соединяются различными устройствами - повторителями, концентраторами или хабами. Например, технология Ethernet позволяет использовать кабель длиной не более 185 метров.

Достоинства:

Небольшое время установки сети;

Дешевизна (требуется меньше кабеля и сетевых устройств);

Простота настройки;

Выход из строя рабочей станции не отражается на работе сети.

Недостатки:

Неполадки в сети, такие как обрыв кабеля и выход из строя терминатора, полностью блокируют работу всей сети;

Сложная локализация неисправностей;

С добавлением новых рабочих станций падает производительность сети.

Кольцо́ - это топология, в которой каждый компьютер соединен линиями связи только с двумя другими: от одного он только получает информацию, а другому только передает. На каждой линии связи, как и в случае звезды, работает только один передатчик и один приемник. Это позволяет отказаться от применения внешних терминаторов.

Работа в сети кольца заключается в том, что каждый компьютер ретранслирует (возобновляет) сигнал, потому затухание сигнала во всем кольце не имеет никакого значения, важно только затухание между соседними компьютерами кольца. Четко выделенного центра в этом случае нет, все компьютеры могут быть одинаковыми. Однако достаточно часто в кольце выделяется специальный абонент, который управляет обменом или контролирует обмен. Понятно, что наличие такого управляющего абонента снижает надежность сети, потому что выход его из строя сразу же парализует весь обмен.

Достоинства

Простота установки;

Практически полное отсутствие дополнительного оборудования;

Возможность устойчивой работы без существенного падения скорости передачи данных при интенсивной загрузке сети, поскольку использование маркера исключает возможность возникновения коллизий.

Недостатки

Выход из строя одной рабочей станции, и другие неполадки (обрыв кабеля), отражаются на работоспособности всей сети;

Сложность конфигурирования и настройки;

Сложность поиска неисправностей.

Звезда́ - базовая топология компьютерной сети, в которой все компьютеры сети присоединены к центральному узлу (обычно сетевой концентратор), образуя физический сегмент сети. Подобный сегмент сети может функционировать как отдельно, так и в составе сложной сетевой топологии (как правило "дерево"). Весь обмен информацией идет исключительно через центральный компьютер, на который таким способом ложится очень большая нагрузка, потому ничем другим, кроме сети, он заниматься не может. Как правило, именно центральный компьютер является самым мощным, и именно на него возлагаются все функции по управлению обменом. Никакие конфликты в сети с топологией звезда в принципе невозможны, потому что управление полностью централизовано.

Достоинства

выход из строя одной рабочей станции не отражается на работе всей сети в целом;

хорошая масштабируемость сети;

лёгкий поиск неисправностей и обрывов в сети;

высокая производительность сети (при условии правильного проектирования);

гибкие возможности администрирования.

Недостатки

выход из строя центрального концентратора обернётся неработоспособностью сети (или сегмента сети) в целом;

для прокладки сети зачастую требуется больше кабеля, чем для большинства других топологий;

конечное число рабочих станций в сети (или сегменте сети) ограничено количеством портов в центральном концентраторе.

Дерево- топология, которая образуется с помощью нескольких топологий типа «общая шина»: они объединяются в дерево с корнем в виде ЭВМ, где размещаются самые важные компоненты сети.

УК-устройство коммутации

Эта топология используется в сложных системах с десятками и сотнями пользователей.

**4. Подключение к Интернет**

Подключиться к Интернету несложно. Прежде всего, необходимо иметь Компьютер.

Модем - аббревиатура слов «модулятор-демодулятор» - это специальное устройство, которое преобразует информацию, поступающую от компьютера, в сигналы, пригодные для передачи по проводной связи (как правило, телефонной линии). Модем выполняет и обратное преобразование (сигналы из линии связи - информация для компьютера).

Линию связи - обычно это телефонный провод.

Договор с провайдером (компания, оказывающая услуги по подключению к Интернету) -иногда такой договор существует в устной форме, или вообще не заключается, или действует в рамках ранее заключенного договора об оказании услуг связи.

Для создания подключения необходимо сделать следующее.

1. Выполнить команду Пуск -> Настройка -> Панель управления - откроется окно Сетевые подключения.

2. В левой части данного окна выбрать параметр Создание нового подключения - откроется окно Мастер новых подключений, в котором нужно нажать кнопку Далее, чтобы появилось следующее окно мастера.

3. Чтобы выбрать тип сетевого подключения, в данном окне необходимо установить переключатель в требуемое положение. Оставьте предлагаемый по умолчанию вариант Подключить к Интернету и нажмите кнопку Далее.

4. В открывшемся окне необходимо выбрать способ подключения к Интернету, и здесь уже возможны варианты. Вполне вероятно, что ваш провайдер будет представлен в предложенном списке поставщиков услуг Интернета или предоставит вам установочный диск. Однако рассмотрим создание подключения вручную, установив переключатель в положение Установить подключение вручную и нажав кнопку Далее, - появится следующее окно мастера.

5. Рассмотрим наиболее типичный пока способ подключения - модемный, установив в данном окне переключатель в положение Через обычный модем и нажав кнопку Далее.

6. В следующем окне в поле Имя поставщика услуг следует указать название интернет-провайдера, можно написать любое слово, оно не имеет значения. Однако нужно учесть, что указанным вами словом будет называться созданное подключение. Написав имя провайдера, нажмите кнопку Далее.

7. В поле Номер телефона необходимо ввести номер, по которому вы будете дозваниваться до провайдера. Данный номер должен предоставить сам провайдер при заключении договора с ним. Введя номер и нажав кнопку Далее, укажите имя пользователя (логин), а также пароль для доступа к Интернету, которые также должны быть предоставлены интернет-провайдером. Нажатие кнопки Далее откроет завершающее окно Мастера новых подключений.

8. В последнем окне мастера не нужны никакие специальные настройки. Можно лишь установить флажок Добавить ярлык подключения на рабочий стол, чтобы в дальнейшем облегчить подключение к Интернету: достаточно будет дважды щелкнуть на значке подключения на Рабочем столе.

9. Далее следует нажать кнопку Готово, чтобы завершить создание нового подключения. Теперь можно осваивать Глобальную сеть. Чтобы подключиться к Интернету, следует выполнить команду меню Пуск Панель управления Сетевые подключения и выбрать требуемое подключение. Двойной щелчок кнопкой мыши на значке подключения на Рабочем столе приведет к тому же результату и откроет окно подключения

**5. FTP**

FTP (англ. File Transfer Protocol - протокол передачи файлов) - протокол, предназначенный для передачи файлов в компьютерных сетях. FTP позволяет подключаться к серверам FTP, просматривать содержимое каталогов и загружать файлы с сервера или на сервер; кроме того, возможен режим передачи файлов между серверами (см. FXP).

FTP является одним из старейших прикладных протоколов, появившимся задолго до HTTP, в 1971 году. До начала 90-х годов на долю FTP приходилось около половины трафика в сети Интернет [источник не указан 535 дней]. Он и сегодня широко используется для распространения ПО и доступа к удалённым хостам.

Протокол FTP относится к протоколам прикладного уровня и для передачи данных использует транспортный протокол TCP. Команды и данные, в отличие от большинства других протоколов передаются по разным портам. Порт 20 используется для передачи данных, порт 21 для передачи команд. В случае, если передача файла была прервана по каким-либо причинам, протокол предусматривает средства для докачки файла, что бывает очень удобно при передаче больших файлов.

Протокол не шифруется, при аутентификации передаются логин и пароль открытым текстом. В случае построения сети с использованием хаба [1] злоумышленник при помощи пассивного сниффера может перехватывать логины и пароли находящихся в том же сегменте сети пользователей FTP, или, при наличии специального ПО, получать передаваемые по FTP файлы без авторизации. Чтобы предотвратить перехват трафика, необходимо использовать протокол шифрования данных SSL, который поддерживается многими современными FTP-серверами и некоторыми FTP-клиентами.

**6. Алгоритм и его свойства**

Слово «Алгоритм» происходит от algorithmi - латинского написания имени аль-Хорезми, под которым в средневековой Европе знали величайшего математика из Хорезма (город в современном Узбекистане) Мухаммеда бен Мусу, жившего в 783-850 гг. В своей книге «Об индийском счете» он сформулировал правила записи натуральных чисел с помощью арабских цифр и правила действий над ними столбиком. В дальнейшем алгоритмом стали называть точное описание действий,однозначно приводящее к получению требуемого результата из исходных данных. Алгоритм может быть предназначен для выполнения его человеком или автоматическим устройством. Создание алгоритма, пусть даже самого простого, - процесс творческий. Он доступен исключительно живым существам, а долгое время считалось, что только человеку. Другое дело - реализация уже имеющегося алгоритма. Ее можно поручить субъекту или объекту, который не обязан вникать в существо дела, а возможно, и не способен его понять. Такой субъект или объект принято называть формальным исполнителем. В роли формального исполнителя может выступать и человек, но в первую очередь – различные автоматические устройства, и компьютер в том числе. Каждый алгоритм создается в расчете на вполне конкретного исполнителя. Те действия, которые может совершать исполнитель, называются его допустимыми действиями. Совокупность допустимых действий образует систему команд исполнителя. Алгоритм должен содержать только те действия, которые допустимы для данного исполнителя.Свойства алгоритма

Данное выше определение алгоритма нельзя считать строгим - не вполне ясно, что такое «точное предписание» или «последовательность действий, обеспечивающая получение требуемого результата». Поэтому обычно формулируют несколько общих свойств алгоритмов, позволяющих отличать алгоритмы от других инструкций.Такими свойствами являются:дискретность (прерывность, раздельность) - алгоритм должен представлять процесс решения задачи как последовательное выполнение простых (или ранее определенных) шагов. Каждое действие, предусмотренное алгоритмом, исполняется только после того, как закончилось исполнение предыдущего;определенность - каждое правило алгоритма должно быть четким, однозначным и не оставлять места для произвола. Благодаря этому свойству выполнение алгоритма носит механический характер и не требует никаких дополнительных указаний или сведений о решаемой задаче;результативность (конечность) - алгоритм должен приводить к решению задачи за конечное число шагов;массовость - алгоритм решения задачи разрабатывается в общем виде, то есть, он должен быть применим для некоторого класса задач, различающихся только исходными данными. При этом исходные данные могут выбираться из некоторой области, которая называется областью применимости алгоритма.

**7. Классификация программного обеспечения**

Програ́ммное обеспе́чение - совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ (ГОСТ 19781-90).

Также - совокупность программ, процедур и правил, а также документации, относящихся к функционированию системы обработки данных (СТ ИСО 2382/1-84).

Программное обеспечение является одним из видов обеспечения вычислительной системы, наряду с техническим (аппаратным), математическим, информационным, лингвистическим, организационным и методическим обеспечением.

В компьютерном сленге часто используется слово софт от английского слова software, которое в этом смысле впервые применил в статье в American Mathematical Monthly математик из Принстонского университета Джон Тьюки (англ. John W. Tukey) в 1958 году.

Программное обеспечение принято по назначению подразделять на системное, прикладное и инструментальное (инструментальные системы), а по способу распространения и использования на несвободное/закрытое, открытое и свободное. Свободное программное обеспечение может распространяться, устанавливаться и использоваться на любых компьютерах дома, в офисах, школах, вузах, а также коммерческих и государственных учреждениях без ограничений.

Системное ПО – это совокупность программ для обеспечения работы компьютера. Системное ПО подразделяется на базовое и сервисное. Системные программы предназначены для управления работой вычислительной системы, выполняют различные вспомогательные функции (копирования, выдачи справок, тестирования, форматирования и т. д).

Базовое ПО включает в себя:

операционные системы;

оболочки;

сетевые операционные системы.

Сервисное ПО включает в себя программы (утилиты):

диагностики;

антивирусные;

обслуживания носителей;

архивирования;

обслуживания сети.

Прикладное ПО – это комплекс программ для решения задач определённого класса конкретной предметной области. Прикладное ПО работает только при наличии системного ПО.

Прикладные программы называют приложениями. Они включает в себя:

текстовые процессоры;

табличные процессоры;

базы данных;

интегрированные пакеты;

системы иллюстративной и деловой графики (графические процессоры);

экспертные системы;

обучающие программы;

программы математических расчетов, моделирования и анализа;

игры;

коммуникационные программы.

Особую группу составляют системы программирования (инструментальные системы), которые являются частью системного ПО, но носят прикладной характер. Системы программирования – это совокупность программ для разработки, отладки и внедрения новых программных продуктов. Системы программирования обычно содержат:

трансляторы;

среду разработки программ;

библиотеки справочных программ (функций, процедур);

отладчики;

редакторы связей и др.

**8. Информационно-поисковые системы и их классификация**

ИПС (информационно-поисковая система) - это система, обеспечивающая поиск и отбор необходимых данных в специальной базе с описаниями источников информации (индексе) на основе информационно-поискового языка и соответствующих правил поиска.

Главной задачей любой ИПС является поиск информации релевантной информационным потребностям пользователя. Очень важно в результате проведенного поиска ничего не потерять, то есть найти все документы, относящиеся к запросу, и не найти ничего лишнего. Поэтому вводится качественная характеристика процедуры поиска - релевантность.

Релевантность - это соответствие результатов поиска сформулированному запросу.

Каждая ИПС предназначена для решения определенного класса задач, для которых характерен свой набор объектов и их признаков. ИПС бывают двух типов:

1. Документографические. В документографических ИПС все хранимые документы индексируются специальным образом, т. е. каждому документу присваивается индивидуальный код, составляющий поисковый образ. Поиск идет не по самим документам, а по их поисковым образам. Именно так ищут книги в больших библиотеках. Сначала отыскивают карточку в каталоге, а затем по номеру, указанному на ней, отыскивается и сама книга.

2. Фактографические. В фактографичеких ИПС хранятся не документы, а факты, относящиеся к какой-либо предметной области. Поиск осуществляется по образцу факта.

Большинство поисковых систем ищут информацию на сайтах Всемирной паутины, но существуют также системы, способные искать файлы на ftp-серверах, товары в интернет-магазинах, а также информацию в группах новостей Usenet.

Популярные поисковые системы

Всеязычные:

Google (34,4 % Русскоязычного сегмента [5])

Bing (0,9 % Русскоязычного сегмента)

Yahoo! (0,2 % Рунета) и принадлежащие этой компании поисковые машины:

Inktomi

AltaVista

Alltheweb

Англоязычные и международные:

AskJeeves (механизм Teoma)

Русскоязычные - большинство «русскоязычных» поисковых систем индексируют и ищут тексты на многих языках - украинском, белорусском, английском и др. Отличаются же они от «всеязычных» систем, индексирующих все документы подряд, тем, что в основном индексируют ресурсы, расположенные в доменных зонах, где доминирует русский язык или другими способами ограничивают своих роботов русскоязычными сайтами.

Яндекс (46,3 % Рунета)

Mail.ru (8,9 % Рунета)

Rambler (3,3 % Рунета)

Nigma (0,5 % Рунета)

Генон (0,1 % Рунета)

Gogo.ru (<0,1 % Рунета)

Aport (<0,1 % Рунета)

**9. Компьютерные вирусы и их классификация**

Компьютерный вирус - это специальная программа, Способная самопроизвольно присоединяться к другим программам и при запуске последних выполнять различные нежелательные действия: порчу файлов и каталогов; искажение результатов вычислений; засорение или стирание памяти; создание помех в работе компьютера. Наличие вирусов проявляется в разных ситуациях.

Некоторые программы перестают работать или начинают работать некорректно.

На экран выводятся посторонние сообщения, сигналы и другие эффекты.

Работа компьютера существенно замедляется.

Структура некоторых файлов оказывается испорченной.

Имеются несколько признаков классификации существующих вирусов:

по среде обитания;

по области поражения;

по особенности алгоритма;

по способу заражения;

по деструктивным возможностям.

По среде обитания различают файловые, загрузочные, макро- и сетевые вирусы.

Файловые вирусы - наиболее распространенный тип вирусов. Эти вирусы внедряются в выполняемые файлы, создают файлы-спутники (companion-вирусы) или используют особенности организации файловой системы (link-вирусы).

Загрузочные вирусы записывают себя в загрузочный сектор диска или в сектор системного загрузчика жесткого диска. Начинают работу при загрузке компьютера и обычно становятся резидентными.

Макровирусы заражают файлы широко используемых пакетов обработки данных. Эти вирусы представляют собой программы, написанные на встроенных в эти пакеты языках программирования. Наибольшее распространение получили макровирусы для приложений Microsoft Office.

Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. Полноценные компьютерные вирусы при этом обладают возможностью запустить на удаленном компьютере свой код на выполнение.

На практике существуют разнообразные сочетания вирусов - например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные секторы дисков, или сетевые макровирусы, которые заражают редактируемые документы и рассылают свои копии по электронной почте.

Как правило, каждый вирус заражает файлы одной или нескольких ОС. Многие загрузочные вирусы также ориентированы на конкретные форматы расположения системных данных в загрузочных секторах дисков. По особенностям алгоритма выделяют резидентные; вирусы, стелс-вирусы, полиморфные и др. Резидентные вирусы способны оставлять свои копии в ОП, перехватывать обработку событий (например, обращение к файлам или дискам) и вызывать при этом процедуры заражения объектов (файлов или секторов). Эти вирусы активны в памяти не только в момент работы зараженной программы, но и после. Резидентные копии таких вирусов жизнеспособны до перезагрузки ОС, даже если на диске уничтожены все зараженные файлы. Если резидентный вирус является также загрузочным и активизируется при загрузке ОС, то даже форматирование диска при наличии в памяти этого вируса его не удаляет.

К разновидности резидентных вирусов следует отнести также макровирусы, поскольку они постоянно присутствуют в памяти компьютера во время работы зараженного редактора.

Стелс-алгоритмы позволяют вирусам полностью или частично скрыть свое присутствие. Наиболее распространенным стелс-алгоритмом является перехват запросов ОС на чтение/запись зараженных объектов. Стелс-вирусы при этом либо временно лечат эти объекты, либо подставляют вместо себя незараженные участки информации. Частично к стелс-вирусам относят небольшую группу макровирусов, хранящих свой основной код не в макросах, а в других областях документа - в его переменных или в Auto-text.

Полиморфность (самошифрование) используется для усложнения процедуры обнаружения вируса. Полиморфные вирусы - это трудно выявляемые вирусы, не имеющие постоянного участка кода. В общем случае два образца одного и того же вируса не имеют совпадений. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

При создании вирусов часто используются нестандартные приемы. Их применение должно максимально затруднить обнаружение и удаление вируса.

По способу заражения различают троянские программы, утилиты скрытого администрирования, Intended-вирусы и т. д.

Троянские программы получили свое название по аналогии с троянским конем. Назначение этих программ - имитация каких-либо полезных программ, новых версий популярных утилит или дополнений к ним. При их записи пользователем на свой компьютер троянские программы активизируются и выполняют нежелательные действия.

Разновидностью троянских программ являются утилиты скрытого администрирования. По своей функциональности и интерфейсу они во многом напоминают системы администрирования компьютеров в сети, разрабатываемые и распространяемые различными фирмами - производителями программных продуктов. При инсталляции эти утилиты самостоятельно устанавливают на компьютере систему скрытого удаленного управления. В результате возникает возможность скрытого управления этим компьютером. Реализуя заложенные алгоритмы, утилиты без ведома пользователя принимают, запускают или отсылают файлы, уничтожают информацию, Эрезагружают компьютер и т. д. Возможно использование этих утилит для обнаружения и передачи паролей и ной конфиденциальной информации, запуска вирусов, ничтожения данных. К Intended-вирусам относятся программы, которые не способны размножаться из-за существующих в них ошибок. К этому классу также можно отнести вирусы, которые размножаются только один раз. Заразив какой-либо файл, они теряют способность к дальнейшему размножению через него.

По деструктивным возможностям вирусы разделяются на:

неопасные, влияние которых ограничивается уменьшением свободной памяти на диске, замедлением работы компьютера, графическим и звуковыми эффектами;

опасные, которые потенциально могут привести к нарушениям в структуре файлов и сбоям в работе компьютера;

очень опасные, в алгоритм которых специально заложены процедуры уничтожения данных и возможность обеспечивать быстрый износ движущихся частей механизмов путем ввода в резонанс и разрушения головок чтения/записи некоторых НЖМД.

**10. Средства защиты от вирусов**

Для защиты от вирусов можно использовать:

Общие средства защиты информации, которые полезны также как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователей;

профилактические меры, позволяющие уменьшить вероятность заражения вирусом;

специализированные программы для защиты от вирусов.

Общие средства защиты информации полезны не только для защиты от вирусов. Имеются две основные разновидности этих методов защиты:

- резервное копирование информации, т. е. создание копий файлов и системных областей дисков на дополнительном носителе;

- разграничение доступа, предотвращающее несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

Несмотря на то, что общие средства защиты информации очень важны для защиты от вирусов, все же их одних недостаточно. Необходимо применять специализированные программы для защиты от вирусов. Эти программы можно разделить на несколько видов:

Программы-детекторы позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов.

Программы-доктора, или фаги, восстанавливают зараженные программы убирая из них тело вируса, т.е. программа возвращается в то состояние, в котором она находилась до заражения вирусом.

Программы-ревизоры сначала запоминают сведения о состоянии программ и системных областей дисков, а затем сравнивают их состояние с исходным. При выявлении несоответствий об этом сообщается пользователю.

Доктора-ревизоры - это гибриды ревизоров и докторов, т.е. программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут автоматически вернуть их в исходное состояние.

Программы-фильтры располагаются резидентно в оперативной памяти компьютера, перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователю. Пользователь может разрешить или запретить выполнение соответствующей операции.

Ни один тип антивирусных программ по отдельности не дает полной защиты от вирусов. Поэтому наилучшей стратегией защиты от вирусов является многоуровневая защита.

Средствами разведки в защите от вирусов являются программы-детекторы, позволяющие проверять вновь полученное программное обеспечение на наличие вирусов.

На первом уровне защиты находятся резидентные программы для защиты от вируса. Эти программы могут первыми сообщить о вирусной атаке и предотвратить заражение программ и диска.

Второй уровень защиты составляют программы-ревизоры, программы-доктора и доктора-ревизоры. Ревизоры обнаруживают нападение тогда, когда вирус сумел пройти сквозь первый уровень. Программы-доктора применяются для восстановления зараженных программ, если ее копий нет в архиве, но они не всегда лечат правильно. Доктора-ревизоры обнаруживают нападение вируса и лечат зараженные файлы, причем контролируют правильность лечения.

Третий уровень защиты - это средства разграничения доступа. Они не позволяют вирусам и неверно работающим программам, даже если они проникли в компьютер, испортить важные данные.

В резерве находятся архивные копии информации и эталонные диски с программными продуктами. Они позволяют восстановить информацию при ее повреждении на жестком диске.

Среди наиболее распространненых российских антивирусных пакетов следует отметить Kaspersky Antivirus, DrWeb, Adinf. Перечисленные средства могут оказать серьёзную помощь в обнаружении вирусов и восстановлении повреждённых файлов, однако не менее важно и соблюдение сравнительно простых правил антивирусной безопасности.

Следует избегать пользоваться нелегальными источниками получения программ. Наименее же опасен законный способ покупки фирменных продуктов.

Осторожно следует относиться к программам, полученным из сети Internet, так как нередки случаи заражения вирусами программ, распространяемых по электронным каналам связи.

Всякий раз, когда дискета побывала в чужом компьютере, необходимо проверить дискету с помощью одного или двух антивирусных средств.

Необходимо прислушиваться к информации о вирусных заболеваниях на компьютерах в своем районе проживания или работы и о наиболее радикальных средствах борьбы с ними. Атакам нового вируса в первую очередь подвергаются компьютеры образовательных учреждений. При передаче программ или данных на своей дискете её следует обязательно защитить от записи.

**Литература**

1. Алексеев Е.Г., Богатырев С.Д. Информатика. Мультимедийный электронный учебник.
2. http://ru.wikipedia.org/wiki/Кольцо\_(топология\_компьютерной\_сети)
3. http://www.klgtu.ru/ru/students/literature/inf\_asu/830.html
4. http://window.edu.ru/window\_catalog/files/r66678/Подключение%20к%20Интернету%20и%20знакомство%20с%20Веб.pdf
5. http://ru.wikipedia.org/wiki/FTP
6. http://emf.ulstu.ru/metod/ITEK/chast\_3.htm