1. **Алгоритмы поиска. Линейный поиск. Двоичный поиск.**

**Линейный поиск**. Данный алгоритм является простейшим алгоритмом поиска и в отличие, например, от двоичного поиска, не накладывает никаких ограничений на функцию и имеет простейшую реализацию. Поиск значения функции осуществляется простым сравнением очередного рассматриваемого значения (как правило поиск происходит слева направо, т.е.от меньших значений аргумента к большим) и, если значения совпадают (с той или иной точностью), то поиск считается завершенным. В связи с малой эффективностью по сравнению с другими алгоритмами линейный поиск обычно используют только, если отрезок поиска содержит очень мало элементов, тем не менее линейный поиск не требует дополнительной памяти или обработки/анализа функции. Также, линейный поиск часто используется в виде линейных алгоритмов поиска максимума/минимума.

Алгоритм последовательного поиска:

Шаг1. Полагаем, что значение переменной цикла i=0.

Шаг2. Если значение элемента массива x[i] равно значению ключа key, то возвращаем значение, равное номеру искомого элемента, и алгоритм завершает работу. В противном случае значение переменной цикла увеличивается на единицу i=i+1.

Шаг3. Если i<k, где k-число элементов массива х, то выполняется шаг2, в противном случае – работа алгоритма завершена и возвращается значение равное -1. При наличии в массиве нескольких элементов со значением key алгоритм находит только первый из них (с наименьшим индексом).

**Двоичный поиск** (также известен, как метод деления пополам и метод половинного деления) – алгоритм нахождения заданного значения монотонной (невозрастающей или неубывающей) функции. Поиск основывается на теореме о промежуточных значениях. Используется в информатике, вычислительной математике и математическом программировании.

Это поиск заданного элемента на упорядоченном множестве, осуществляемый путем неоднократного деления этого множества на две части таким образом, что искомый элемент попадает в одну из этих частей. Поиск заканчивается при совпадении искомого элемента с элементом, который является границей между частями множества или при отсутствии искомого элемента.

Алгоритм бинарного поиска:

Шаг1. Определить номер среднего элемента массива middle=(high+low)/2.

Шаг2. Если значение среднего элемента массива равно искомому, то возвращаем значение, равное номеру искомого элемента, и алгоритм завершает работу.

Шаг3. Если искомое значение больше значения среднего элемента, то возьмем в качества массива все элементы справа от среднего, иначе возьмет в качестве массива все элементы слева от среднего. Перейдем к Шагу1.

В массиве может встречаться несколько элементов со значениями, равными ключу. Данный алгоритм находит первый совпавший с ключом элемент, который в порядке следования в массиве может быть ни первым,

ни последним среди равных ключу.

1. **Сортировка методом вставки, другие способы сортировки.**
2. **Сортировка методом выбора, другие способы сортировки.**

Процесс упорядочивания информации и называют «сортировкой». Сортировка применяется во всех без исключения областях программирования, будь то базы данных или математические программы. Сортировка массива данных занимает одну из самых важнейших проблем современных организаций. Ведь в каждой организации есть свои БД на сотрудников, которые нужно отсортировать, допустим, по фамилии или по зп, по возрастанию или убыванию.

Чаще всего сортировка применяется для последующего поиска.

Перед тем, как решать вопросы сортировки необходимо знать объем данных, которые необходимо обрабатывать. Есть методы, которые наиболее эффективны при малом количество элементов, но они становятся довольно громоздкими при большом.

Постановка задачи такова: есть набор неупорядоченных данных (массив), задача – выдать те же данные, упорядоченные по некоторому полю (ключу) по возрастанию (убыванию). Обычно данные представляются в виде ключа и некоторой связанной с ним информации. Например, год рождения и фамилия.

Практически каждый алгоритм сортировки можно разбить на три части:

-сравнение, определяющее упорядоченность пары элементов;

- перестановку, меняющую местами пару элементов;

- собственно сортирующий алгоритм, который осуществляет сравнение и перестановку элементов до тех пор, пока все элементы множества не будут упорядочены.

Алгоритмы сортировки оцениваются по скорости выполнения и эффективности использования памяти.

Время – основной параметр, характеризующий быстродействие алгоритма.

Память – ряд алгоритмов требует выделения дополнительной памяти под временное хранение данных.

**Классификация алгоритмов сортировки**

**Сортировка вставками.** Создается новый массив, в который мы последовательно вставляем элементы из исходного массива так, чтобы новый массив был упорядоченным. На каждом шаге алгоритма мы выбираем один из элементов данных и вставляем его на нужную позицию в уже отсортированном списке, до тех пор, пока набор входных данных не будет исчерпан.

Время выполнения алгоритма зависит от входных данных: чем большее множество нужно отсортировать, тем большее время выполняется сортировка. Также на время выполнения влияет исходная упорядоченность массива.

Сортировка вставками эффективна на небольших наборах данных, на наборах данных до десятков элементов может оказаться лучшей. Эффективна на наборах данных, которые уже частично отсортированы. Может сортировать список по мере его получения.

**Сортировка методом выбора.** На первом шаге в массиве ищется самый маленький элемент и меняется местами с первым. На втором шаге ищется самый маленький, начиная со второго, и ставится на 2-е место (второй элемент, естественно, не забываем – ставим его на место, где раньше был самый маленький). И так далее, на i-ом шаге ищется самый маленький, начиная с i-го и ставится на i-е место.

**Метод пузырька.** Метод пузырька так же называют «Пузырьковой сортировкой». Суть сортировки методом пузырька вытекает из названия. Мы находим минимальный элемент (пузырек) в массиве и выставляем его первым элементом массива (поднимает на поверхность). Далее находим следующий минимальный элемент и так же его выставляем вслед за первым элементом. И так будем действовать до самого конца. Таким образом, минимальные элементы всплывают.

Этот алгоритм в исходном списке ищет пары цифр, которые следуют не по порядку и затем меняет их местами. Процесс повторяется до тех пор, пока весь список не будет отсортированным.

**Сортировка Шейкером.** Когда данные сортируются не в оперативной памяти, а на жестком диске, особенно если ключ связан с большим объемом дополнительной информации, то количество перемещений элементов существенно влияет на время работы. Этот алгоритм уменьшает количество таких перемещений, действуя следующим образом: за один проход из всех элементов выбирается минимальный и максимальный. Потом минимальный элемент помещается в начало массива, а максимальный, соответственно, в конец. Далее алгоритм выполняется для остальных данных. Таким образом, за каждый проход два элемента помещаются на свои места, а значит, понадобится N/2 проходов, где N – количество элементов.

**4. Использование списков для моделирования сложных структур данных.**

Часто в серьезных программах надо использовать данные, размер и структура которых должны меняться в процессе работы. Динамические массивы здесь не выручают, поскольку нельзя сказать, сколько памяти надо выделить – это выясняется только в процессе работы. В таких случаях применяют данные особой структуры, которые представляют собой отдельные элементы, связанные с помощью ссылок. Каждый элемент (узел) состоит из двух областей памяти: поля данных и ссылок. Ссылки – это адреса других узлов этого же типа, с которыми данный элемент логически связан. В языке Си для организации ссылок используются переменные-указатели. При добавлении нового узла в такую структуру выделяется новый блок памяти и с помощью ссылок устанавливаются связи этого элемент с уже существующими. Для обозначения конечного элемента в цепи используются нулевые ссылки (NULL).

Линейный список – это конечная последовательность однотипных элементов (узлов), возможно, с повторениями. Количество элементов в последовательности называется длиной списка, причем длина в процессе работы программы может изменяться.

При работе со списками на практике чаще всего приходится выполнять следующие операции:

-найти элемент с заданным свойством;

-определить первый элемент в линейном списке;

-вставить дополнительный элемент до или после указанного узла;

- исключить определенный элемент из списка;

-упорядочить узлы линейного списка в определенном порядке.

Строение списка: набор узлов, объединенных с помощью ссылок.

Однонаправленный линейный список- список, который имеет указатель на начало списка, при этом каждый список имеет указатель на следующий список, а последний список принимает указатель NULL, что говорит о том, что он последний.

Однонаправленный кольцевой список – список, который имеет указатель на начало списка, при этом каждый список имеет указатель на следующий список, а последний список имеет указатель на начало списка.

В зависимости от количества связей между соседними элементами различают односвязные и двусвязные списки. Каждый элемент в списке с двойной связью имеет указатель на следующий элемент списка и указатель на предыдущий элемент списка.

Двунаправленный список отличается двумя основными преимуществами.

Во-первых, список может просматриваться в обоих направлениях. Это не только упрощает сортировку списка, но также позволяет пользователям БД просматривать данные в обоих направлениях.

Во-вторых, список при нарушении одной из связей может быть восстановлен по другой связи. Это свойство имеет смысл использовать при отказах оборудования, приводящих к нарушению списка.

Структура узла:

struct Node{

char word[40]; //слово

int count; //счетчик повторений

Node \*next; //ссылка на следующий элемент

};

Адрес начала списка:

PNode Head=NULL;

Для доступа к списку достаточно знать адрес его головы.

Когда нужны списки?

Задача. В файле записан текст. Нужно записать в другой файл в столбик все слова, встречающиеся в тексте, в алфавитном порядке, и количество повторений для каждого слова.

Проблемы:

**-** количество слов заранее неизвестно;

- количество слов определяется только в конце работы.

Решение – список.

Алгоритм:

- создать список;

- если слова в файле закончились, то стоп.

- прочитать слово и искать его в списке;

- если слово найдено – увеличить счетчик повторений, иначе добавить слово в список;

- перейти к шагу 2.

При работе со списками необходимо уметь создать новый узел, добавить узел в начало списка, в конец списка, после заданного узла, до заданного узла, искать нужный узел в списке, удалить узел.

Функция CreateNode – создает узел.

1. **Использование очередей для моделирования сложных структур данных.**

В зависимости от метода доступа к элементам линейного списка различают разновидности линейных списков называемые стеком, очередью и двусторонней очередью. Очередь – это линейный список, где элементы удаляются из начала списка, а добавляются в конце списка. Двусторонняя очередь – это линейный список, у которого операции добавления и удаления элементов и доступа к элементам возможны как вначале так в конце списка.

Добавление элемента в очереди возможно лишь в конец очереди, выборка – только из начала очереди, при этом выбранный элемент из очереди удаляется.

Очередь в программировании используется, как и в реальной жизни, когда нужно совершить какие-то действия в порядке их поступления, выполнив их последовательно. Примером может служить организация событий в Windows. Когда пользователь оказывает какое-то действие на приложение, то в приложении не вызывается соответствующая процедура (ведь в этот момент приложение может совершать другие действия), а ему присылается сообщение, содержащее информацию о совершенном действии, это сообщение ставится в очередь, и только когда будут обработаны сообщения, пришедшие ранее, приложение выполнит необходимое действие.

Очередь – информационная структура, в которой для добавления элементов доступен только один конец, называемый хвостом, а для удаления – другой, называемый головой.

Типовые операции над очередями:

-добавление элемента в очередь (помещение в хвост);

-удаление элемента из очереди (удаление из головы);

- проверка, пуста ли очередь;

- очистка очереди.

Очередь называют структурой типа FIFO (First In – First Out) – первым пришел, первым ушел. На рисунке изображена очередь из 3-ех элементов.

Добавление элемента -> в б а ->удаление элемента

конец начало

Если максимальный размер очереди заранее известен, его можно реализовать в программе в виде массива.

Если максимальный размер заранее неизвестен или требуется сделать его динамическим, для реализации используют список.

1. **Использование деревьев для моделирования сложных структур данных.**

Дерево – иерархическая структура данных, хранящая набор элементов. Каждый элемент имеет значение и может указывать на ноль или более других элементов. На каждый элемент указывает только один другой элемент. Единственным исключением является корень дерева, на который не указывает ни один элемент. Входящие в дерево элементы называются его вершинами.

Существует два основных типа деревьев. В рекурсивном дереве или неупорядоченном дереве имеет значение лишь структура самого дерева без учета порядка потомков для каждого узла. Дерево, в котором задан порядок (например, каждому ребру, ведущему к потомку, присвоены различные натуральные числа) называется деревом с именованными ребрами или упорядоченным деревом. Упорядоченные деревья являются наиболее распространенными среди древовидных структур. Двоичное дерево поиска – одно из разновидностей упорядоченного дерева.

Существует множество различных способов представления деревьев. Наиболее общий способ представления изображает узлы как записи, расположенные в динамически выделяемой памяти с указателями на своих потомков, предков (или и тех и других), или как элементы массива, связанные между собой отношениями, определенными их позициями в массиве.

Операции:

1. Вставка нового элемента в определенную позицию;
2. Вставка поддерева;
3. Добавление ветви дерева (называется прививкой);
4. Нахождение корневого элемента для любого узла;
5. Нахождение наименьшего общего предка двух вершин;
6. Перебор всех элементов дерева;
7. Перебор элементов ветви дерева;
8. Поиск элемента;
9. Удаление ветви дерева;
10. Удаление поддерева;
11. Удаление элемента.

Применение:

-управление иерархией данных;

- упрощение поиска информации;

- оптимизация программ;

-в качестве технологии компоновки цифровых картинок для получения различных визуальных эффектов и др.

Дерево – структура данных, состоящая из узлов и соединяющих их направленных ребер (дуг), причем в каждый узел (кроме корневого) ведет ровно одна дуга.

Корень – это начальный узел дерева.

Лист – это узел, из которого не выходит ни одной дуги.

С помощью деревьев изображаются отношения подчиненности (иерархия, старший-младший, родитель – ребенок).

Предок узла х – это узел, из которого существует путь по стрелкам в узел х.

Потомок узле х – это узел, в который существует путь по стрелкам из узла х.

Высота дерева – это наибольшее расстояние от корня до листа.

Двоичное (бинарное) дерево – это дерево, в котором каждый узел имеет не более двух сыновей.

Применение двоичных деревьев:

-поиск данных в специально построенных деревьях (БД)

-сортировка данных

-вычисление арифметических выражений

-кодирование

Ключ – это характеристика узла, по которой выполняется поиск.

Обход дерева – это перечисление всех узлов в определенном порядке.

1. **Использование графов для моделирования сложных структур данных.**

Граф – это набор вершин (узлов) и соединяющих их ребер (дуг)

Направленный граф – это граф, в котором все дуги имеют направления.

Цепь – это последовательность ребер, соединяющих две вершины.

Цикл – это цепь из какой-то вершины в нее саму.

Взвешенный граф (сеть) – это граф, в котором каждому ребру приписывается вес (длина).

Графы являются существенным элементом математических моделей в самых разнообразных областях науки и практики. Они помогают наглядно представить взаимоотношения между объектами или событиями в сложных системах. Легко найти примеры графов в самых разнообразных областях науки и практики. Сеть дорог, трубопроводов, электрическая цепь, структурная формула химического соединения, блок-схема программы.

Граф называется:

-связным, если для любых вершин u и v есть путь из u и в v

-сильно связным или ориентировано связным, если он ориентированный, и из любой вершины в любую другую имеется ориентированный путь

-деревом, если он связный и не содержит простых циклов

- полным, если любые его две вершины соединены ребром

-взвешенным, если каждому ребру графа поставлено в соответствие некоторое число, называемое весом ребра и др.

Способы представления графа в информатике:

-Матрица смежности – таблица, где как столбцы, так и строки соответствуют вершинам графа. В каждой ячейке этой матрицы записывается число, определяющее наличие связи от вершины-строки к вершине-столбцу (либо наоборот).

-Список ребер – это тип представления графа в памяти, подразумевающий, что каждое ребро представляется двумя числами – номерами вершин этого ребра. Список ребер более удобен для реализации различных алгоритмов на графах по сравнению с матрицей смежности.

**8.Использование массивов и указателей для моделирования сложных структур данных.**

Массив – это упорядоченный набор данных, для хранения данных одного типа, идентифицируемых с помощью одного или нескольких индексов. В простейшем случае массив имеет постоянную длину и хранит единицы данных одного и того же типа.

Количество используемых индексов массива может быть различным. Массивы с одним индексом называют одномерными, с двумя – двумерными и т.д. Одномерный массив нестрого соответствует вектору в математике, двумерный – матрице. Чаще всего применяются массивы с одним или двумя индексами, реже – с тремя, еще большее количество индексов встречается крайне редко.

Динамическим называется массив, размер которого может меняться во время исполнения программы. Динамические массивы дают возможность более гибкой работы с данными, так как позволяют не прогнозировать хранимые объемы данных, а регулировать размер массива в соответствии с реально необходимыми объемами. Обычные, не динамические массивы называют еще статическими.

Элементы массива располагаются в последовательных ячейках памяти, обозначаются именем массива и индексом. Каждое из значений, составляющих массив, называется элементом массива.

Количество индексов элементов массива определяет размерность массива. По этому признаку массивы делятся на одномерные (линейные), двумерные, трехмерные и тд.

В си можно определить массив любого типа. Int mas[3] описан массив из 3 целых чисел. Нумерация в массивах начинается с 0-го элемента.

Массив можно инициализировать при описании. В этом случае нет необходимости указывать его размер int mas[]={23,25,8}

Создан массив из 3-элементов:

Mas[0]=23;

Mas[1]=25;

Mas[2]=81;

Указатель – это переменная, значением которой является адрес другой переменной. Для описания указателей используется операция косвенной адресации \*. Например, указатель целого типа uk описывается так: int \*uk. Унарная операция &, примененная к некоторой переменной, показывает, что нам нужен адрес этой переменной, а не ее текущее значение. Если переменная uk объявлена как указатель, то оператор присваивания uk=&x означает: «взять адрес переменной х и присвоить его значение переменной-указателю uk».

Унарная операция \* , примененная к указателю, обеспечивает доступ к содержимому ячейки памяти, на которую ссылается указатель. Например, \*uk можно описать словами как «то, что содержится по адресу, на который указывает uk». Указатели могут использоваться в выражениях. Если, например, переменная uk указывает на целое х, то \*uk может во всех случаях использоваться вместо х; так, \*uk+1 увеличивает х на единицу, а \*uk=0 равносильно х=0.

Если uk – некоторый указатель, то uk++ увеличивает его значение и он теперь указывает на следующий, соседний адресуемый объект.

1. **Проблемы и особенности использование текстовых процессоров для автоматизации процессов совместной работы над документами.**
2. **Методы, подходы и технологии повышения производительности в работе с текстовыми процессорами.**

Текстовый процессор – вид прикладной компьютерной программы, предназначенной для производства (включая набор, редактирование, форматирование, иногда печать) любого вида печатной информации. Иногда текстовый процессор называют текстовым редактором второго рода.

Текстовыми процессорами в 1970-е – 1980-е годы называли предназначенные для набора и печати текстов машины индивидуального и офисного использования, состоящие из клавиатуры, встроенного компьютера для простейшего редактирования текста, а также электрического печатного устройства. Позднее наименование «текстовый процессор» стало использоваться для компьютерных программ, предназначенных для аналогичного использования.

Текстовые процессоры, в отличие от текстовых редакторов, имеют больше возможностей для форматирования текста, внедрения в него графики, формул, таблиц и других объектов. Поэтому они могут быть использованы не только для набора текстов, но и для создания различного рода документов, в том числе официальных. Наиболее известным примером текстового процессора является Microsoft Word.

Современные текстовые процессоры предоставляют пользователю широкие возможности по подготовке документов. Это и функции редактирования, допускающие возможность любого изменения, вставки, замены, копирования и перемещения фрагментов в рамках одного документа и между различными документами, контекстового поиска, функции форматирования символов, абзацев, страниц, разделов документа, верстки, проверки грамматики и орфографии, использования списков, таблиц, рисунков, графиков и диаграмм.

Значительное сокращение времени подготовки документов обеспечивают такие средства автоматизации набора текста, как автотекст, автозамена, использование форм, шаблонов и мастеров типовых документов.

Наличие внешней памяти компьютер обеспечивает удобное длительное хранение подготовленных ранее документов, быстрый доступ к ним в любое время.

Существенно упрощают процедуру ввода данных сканеры и голосовые устройства. Существующие системы распознавания текстов, принимаемых со сканера, включают функцию экспорта документа в текстовые редакторы.

Широкий спектр печатающих устройств в сочетании с функциями подготовки документа к печати, предварительного просмотра, обеспечивают получение высококачественных черно-белых и цветных копий.

При работе в локальных и глобальных компьютерных сетях пользователь имеет возможность обмениваться документами с удаленными пользователями, отправляя документы по электронной почте непосредственно из текстового редактора, готовить данные в формате Web-страниц.

Текстовые данные являются наиболее распространенным видом данных при работе с компьютером. Для работы с тексом используют два основных класса программного обеспечения:

-текстовые редакторы;

-текстовые процессоры.

Текстовые редакторы служат в основном для ввода и редактирования (правки) текста. Они не имеют средств для оформления внешнего вида документа и применяются в тех случаях, когда эти средства являются лишними и отвлекают от творческой работы или не нужны (например, при подготовке документов, пересылаемых по электронной почте). При использовании текстового редактора создается текстовый файл, который содержит только коды символов, которые были введены. Это означает, что все текстовые редакторы работают с текстом одинаково. Текст, введенный в одном редакторе, можно редактировать другим редактором, не испытывая при этом никаких затруднений.

Текстовые процессоры используют в тех случаях, когда имеет значение не только содержание текста, но и его внешний вид (например, при подготовке официальных документов). Текстовый процессор позволяет управлять оформлением текста при его выдаче на экран и принтер. Документ, созданный текстовым процессором, содержит не только текст, но и информацию о том, как он должен быть оформлен. Эта информация заключена в невидимых кодах, которые не печатаются ни на экране, ни на бумаге, но влияют на то, как происходит печать. Разные текстовые процессоры используют для оформления текста разные коды (говорят – документы имеют разные форматы). Поэтому перенос форматированных текстовых документов из одного текстового процессора в другой не всегда возможен и не всегда прост. В тех случаях, когда такой перенос сделать не удается, переносят только текст, без кодов форматирования (говорят – перенос с потеряй форматирования), после чего вновь оформляют текст в новом текстовом процессоре.

Что можно делать с помощью текстового процессора?

-набирать текст;

-сохранять текст на диск и загружать текст с диска;

-редактировать (изменять);

-выбирать шрифт и его размер;

-выводить текст на печать, желательно с предварительным просмотром страниц;

-осуществлять поиск и поиск с заменой;

-возможность загружать большие документы;

-возможность одновременного просмотра нескольких документов (многооконный режим);

- наличие буфера для переноса фрагмента документа внутри окна и между окнами;

- форматировать документ( задавать поля, задавать абзацы и отступы, задавать выравнивание текста (по левому, по правому краям, по центру, по ширине), задавать межстрочный интервал, задавать нумерацию страниц, задавать размер страниц, располагать текст в нескольких колонках);

-вставлять в текст графические изображения, таблицы, формулы и т.д.

- осуществлять проверку орфографии.

1. **Общая характеристика и функциональные возможности табличных процессоров.**
2. **Особенности использования табличных процессоров для графического представления данных.**

Табличные процессоры представляют собой двухмерные таблицы, как правило, заранее определенной формы, каждая клетка которой содержит значение некоторой характеристики объекта. Подобные документы являются наиболее распространенными в деятельности различных отделов, служб, предприятий. Примерами этих документов могут служить бухгалтерские ведомости, отчеты, планы, списки и прочее. Такие документы представляются в памяти ЭВМ в виде электронных таблиц.

Отдельные клетки таблиц содержат числовую или текстовую информацию. Числовые данные обычно подлежат математической обработке по определенным математическим зависимостям или графическому представлению. В деятельности многих фирм широко используются такие пакеты, как SuperCalc, Lotus 1-2-3, Excel.

Области применения табличных процессоров достаточно широки. Наиболее простые позволяют обрабатывать табличные данные по формулам, что очень важно при решении задач статистического анализа и при обработке экспериментальных данных. В более сложных процедурах моделирования и прогнозирования требуется решать задачи экстраполяции и интерполяции. Соответственно здесь должны использоваться табличные процессоры с расширенными возможностями.

Все табличные процессоры обеспечивают графическое представление данных. Для этого к ним подключают графические редакторы, обеспечивающие воспроизведение разнообразные графиков, диаграмм: круговых, столбиковых, линейных, трехмерны и т.д.

Электронные таблицы (ЭТ) представляют собой удобный инструмент автоматизации вычислений. Многие расчет, в частности в области бухгалтерского учета, выполняются в табличной форме: балансы, расчетные ведомости, сметы расходов и т.п. Кроме того, решение численными методами целого ряда математических задач удобно выполнять именно в табличной форме. Решения многих вычислительных задач, которые раньше можно было осуществить только с помощью программирования, стало возможно реализовать через математическое моделирование в ЭТ.

Табличный процессор MS EXCEL позволяет:

-решать математические задачи: выполнять разнообразные табличные вычисления, вычислять значения функций, строить графики и диаграммы и т.п.;

-осуществлять численное исследование (что будет, если? Как сделать, чтобы?)

- проводить статистический анализ;

-реализовать функции базы данных – ввод, поиск, сортировку, фильтрацию и анализ данных;

- устанавливать защиту на отдельные фрагменты таблицы, делать их невидимыми;

-наглядно представлять данные в виде диаграмм и графиков;

-вводить и редактировать тексты;

- осуществлять обмен данными с другими программами, например, вставлять текст, рисунки, таблицы, подготовленные в других приложениях.

-осуществлять многотабличные связи.

Диаграмма – это графическое представление числовых данных. Диаграммы упрощают сравнение и восприятие чисел, поэтому они весьма популярны.

Круговая диаграмма показывает как абсолютную величину каждого элемента ряда данных, так и вклад в общую сумму.

В многослойной диаграмме можно представлять более одного ряда данных.

Для построения диаграммы следует выделить любую ячейку из тех, что содержать исходные данные диаграммы. Затем выполнить команду Диаграмма меню Вставка или нажать кнопку Мастер диаграмм на стандартной панели инструментов. С помощью четырех окон диалога мастер диаграмм соберет всю информацию, необходимую для построения диаграммы. Чтобы построить диаграмму, не прибегая к помощи мастера диаграмм, следует выделить ячейку с исходными данными и нажать клавишу F11. Используя установки по умолчанию, Excel создает диаграмму на отдельно листе.

В Excel типы диаграмм делятся на стандартные и нестандартные. При выборе типа диаграммы в диалоговом окне мастера диаграмм в специальной области приводится пример и краткое описание выбранной диаграммы.

Исходные данные диаграммы задаются ссылкой на соответствующий диапазон. Пользователь может задать заголовок диаграммы и каждой из ее осей. При выводе текса в диаграмме Excel использует установленные по умолчанию шрифт, выравнивание и расположение. Наличие и количество осей определяются типом диаграммы. Пользователь может контролировать вывод осей на диаграмме. Если данные для оси Х являются датами, то Excel распознает этот факт и автоматически применяет временное масштабирование к этой оси. Легенда диаграммы – это заголовки рядов, размещаемые по умолчанию в правой части диаграммы. Выбор заголовков рядов производится автоматически, если в выделенные диапазон включены заголовки строк и столбцов. В противном случае ряды именуются как Ряд1, Ряд2 и т.д. Можно также изменить местоположение или вообще удалить легенду с диаграммы. Команды форматирования позволяют изменить используемый в диаграмме шрифт.

Excel может внедрить диаграмму в рабочий лист или поместить ее на отдельном листе диаграммы. При создании диаграммы в существующем рабочем листе ее размеры и положение устанавливаются по умолчанию. Настроить размеры и положение диаграммы можно с помощью мыши.

Диаграмма сохраняется вместе с книгой, в которой она находится. Диаграмма становится доступной, когда открыта книга.

В Excel имеется широкий набор команд, с помощью которых можно изменять внешний вид диаграмм. Форматы из одной диаграммы можно использовать в другой. Для этого следует сначала выделить область диаграммы, форматы которой нужно скопировать, затем выполнить команду Копировать меню Правка, выделить другую диаграмму и выполнить команду Вставить меню Правка.

При форматировании диаграммы можно выполнять следующие действия:

1. Изменять расположение элементов диаграммы.
2. Изменить размеры и переместить область построения. Область построения – это часть диаграммы, в которой отображаются данные.
3. Форматировать текстовые элементы диаграммы (в том числе изменять ориентацию текста).
4. Форматировать и изменять шкалы осей.
5. Задавать вывод и форматирование сетки.
6. Excel позволяет смешивать несколько различных типов диаграмм.
7. Форматировать фоновые области.
8. Настраивать объемные виды диаграммы.
9. Добавлять, удалять, изменять данные в диаграммах, изменять порядок и отображения рядов.

В состав Excel входит специальная компонента Microsoft Map, которую можно использовать для наглядного представления географической информации. В зависимости от используемой карты можно вывести на экран различные конкретные географические подробности, в том числе дороги, города, аэропорты и реки. Microsoft Map является надстройкой и не входит в типовую установку Excel. Для его установки следует запустить программу Setup и добавить этот компонент.

1. **Системы управления базами данных. Характеристика и функциональные возможности СУБД MS Access.**

БД – это информационная модель, позволяющая упорядоченно хранить данные о группе объектов, обладающих одинаковым набором свойств.

Программное обеспечение, предназначенное для работы с БД, называется система управления БД. СУБД используются для упорядоченного хранения обработки больших объемов информации.

СУБД организует хранение информации таким образом, чтобы ее было удобно:

- просматривать;

-пополнять;

- изменять;

- искать нужные сведения;

- делать любые выборки;

- осуществлять сортировку в любом порядке.

Классификация БД:

1. По характеру хранимой информации:

- фактографические (картотеки);

- документальные (архивы).

2. По способу хранения данных:

- централизованные (хранятся на одном компьютере);

-распределенные (используются в локальных и глобальных компьютерных сетях).

3. по структуре организации данных:

-табличные (реляционные),

- иерархические.

Информация в БД структурирована на отдельные записи, которыми называют группу связанных между собой элементов данных. Характер связи между записями определяет два основных типа организации БД: иерархический и реляционный.

В иерархической БД записи упорядочены в определенную последовательность, как ступеньки лестницы, и поиск данных может осуществляться последовательным «спуском» со ступени на ступень. Иерархическая БД по своей структуре соответствует структуре иерархической файловой системы.

Реляционная БД, по сути, представляет собой двумерную таблицу. Столбцы таблицы называют полями: каждое поле характеризуется своим именем и типом данных. Поле БД – это столбец таблицы, содержащий значения определенного свойства.

В реляционной БД используются четыре основных типов полей:

- числовой

- символьный (слова, тексты, коды и т.д.)

- дата (календарные даты в форме «день/месяц/год»)

- логический (принимает два значения: «да» - «нет» или «истина» - «ложь»).

Строки таблицы являются записями об объекте. Запись БД – это строка таблицы, содержащая набор значения определенного свойства, размещенный в полях БД.

Системы управления БД позволяют объединять большие объемы информации и обрабатывать их, сортировать, делать выборки по определенным критериям и т.п.

Современные СУБД дают возможность включать в них не только текстовую и графическую информацию, но и звуковые фрагменты и даже видеоклипы.

Простота использования СУБД позволяет создавать новые БД, не прибегая к программированию, а пользуясь только встроенными функциями. СУБД обеспечивают правильность, полноту и непротиворечивость данных, а также удобный доступ к ним.

Популярные СУБД – FoxPro, MS Access, Paradox.

МА – реляционная СУБД корпорации Microsoft. Благодаря встроенному языку VBA (Visual Basic for Applications), в самом МА можно писать приложения, работающие с БД.

Основные компоненты МА:

-построитель таблиц;

-построитель экранных форм;

-построитель запросов;

-построитель отчетов, выводимых на печать.

Простые программы, которые хранят данные только в одной таблице (Database), часто называют плоскими БД, МА – более сложная программа, которая хранит информацию в несколько связанных между собой таблицах (related) и поэтому называется реляционной БД.

Типы объектов в МА – таблицы, запросы, формы, отчеты, страницы, макросы, модули. Из всех типов объектов только таблицы предназначены для хранения информации. Остальные используются для просмотра, редактирования, обработки и анализа данных – иначе говоря, для обеспечения эффективного доступа к информации.

Поскольку МА входит в состав Microsoft Officе, он обладает многими чертами, характерными для приложений Office, и может обмениваться с ними информацией. Например, работая в МА, можно открывать и редактировать файлы с помощью кнопок, команд и клавиш, а также использовать буфер обмена Office для копирования данных из таких программ, как Microsoft Word или Microsoft Excel.

Запросы служат для извлечения данных из таблиц и представления их пользователю в удобном виде. С помощью запросов выполняют такие операции, как отбор данных, их сортировку и фильтрацию.

Если запросы – это специальные средства для отбора и анализа данных, то формы – это средства для ввода данных. Одновременно с этим в форме можно разместить специальные элементы управления (счетчики, раскрывающиеся списки, переключатели, флажки и прочее) для автоматизации ввода.

Отчеты по свойствам и структуре во многом похожи на формы, но предназначены только для вывода данных.

Страницы – это специальные объекты БД, реализованные в последних версия МА (начиная с МА 2000). Это объект, выполненный в коде HTML, размещаемый на Web-странице. Сам по себе этот объект не является БД, но содержит компоненты, через которые осуществляется связь переданной Web-страницы с БД, остающейся на сервере. Пользуясь этими компонентами, посетитель Web- узла может просматривать записи базы в полях страницы. Таким образом, страницы доступа к данным осуществляют интерфейс между клиентом, сервером и БД, размещенной на сервере.

Макросы и модули предназначены как для автоматизации повторяющихся операций при работе с СУБД, так и для создания новых функций путем программирования. В СУБД МА макросы состоят из последовательности внутренних команд СУБД и являются одним из средств автоматизации работы с базой. Модули создаются средствами внешнего языка программирования, в данном случае языка Visual Basic for Applicatioms.

При создании или открытии файла МА, открывается окно БД. Окно БД является центром управления файлами А. Из этого окна пользователи создают и используют любые объекты БД А или проекта А.

Пользователь имеет возможность изменить настройки, определяющие выводится ли окно БД на экран при открытии файла МА, или нет. Если скрыть окно БД, то необходимо открыть стартовую форму или страницу доступа к данным, чтобы предоставить пользователям возможность переходов по приложению.

Как реляционная СУБД МА обеспечивает доступ ко всем типам данных и позволяет использовать одновременно несколько таблиц БД. Таблицу МА можно связать с данными, хранящимися на ЭВМ или на сервере. С другой стороны, можно использовать таблицы, созданные в среде Paradox или dBASE. Полученные результаты можно быстро и легко связать и объединить с данными электронных таблиц EXCEL.

1. **Проектирование таблиц средствами СУБД MS Access. Понятие конструктора таблиц.**

Прежде чем создавать таблицы, формы и другие объекты необходимо задать структуру БД.

Этапы проектирования БД:

1. Определить цель создания БД, основные ее функции и информацию, которую она должна содержать. БД должна отвечать требованиям тех, кто будет непосредственно с ней работать. Для этого нужно определить темы, которые должна покрывать БД, отчеты, которые она должна выдавать, проанализировать формы, которые в настоящий момент используются для записи данных, сравнить создаваемую БД с хорошо спроектированной, подобной ей базой.
2. Разработать на бумаге структуру таблиц, которые должна содержать БД. При проектировании таблиц, рекомендуется руководствоваться следующими основными принципами:

Информация в таблице не должна дублироваться. Не должно быть повторений и между таблицами. Когда определенная информация хранится только в одной таблице, то и изменять ее придется только в одном месте. Это делает работу более эффективной, а также исключает возможность несовпадения информации в разных таблицах. Каждая таблица должна содержать информацию только на одну тему. Сведения на каждую тему обрабатываются намного легче, если они содержаться в независимых друг от друга таблицах. Например, адреса и заказы клиентов хранятся в разных таблицах, с тем, чтобы при удалении заказа информация о клиенте осталась в БД.

1. Определить необходимые в таблице поля. Каждая таблица содержит информацию на отдельную тему, а каждое поле в таблице содержит отдельные сведения по теме таблицы. Например, в таблице с данными о клиенте могут содержаться поля с названием компании, адресом, городом, страной и номером телефона.
2. Задать ключевое поле. Для того, чтобы МА мог связать данные из разных таблиц, например, данные о клиенте и его заказы, каждая таблица должна содержать поле или набор полей, которые будут задавать индивидуальное значение каждой записи в таблице. Такое поле или набор полей назывют основным ключом.
3. Определить связь между таблицами.

В МА поддерживаются два способа создания БД. Имеется возможность создать пустую БД, а затем добавить в нее таблицы, формы, отчеты и другие объекты. Имеется также возможность создать БД с помощью мастера.

Таблица хранит сведения по конкретному вопросу, например, таблица «Товары» содержит сведения только о товарах, а таблица «Поставщики» - только о компаниях, поставляющих товары. Данные в таблице организованы в столбцы (поля) и в строки (записи).

В новой версии МА существуют четыре режима работы с таблицами: режим Таблицы, режим Конструктора, режим Сводной таблицы и режим Свободной диаграммы.

В режиме Таблицы осуществляется работа с данными, находящимися в таблице: просмотр, редактирование, добавление, сортировка и т.п. В режиме Конструктора создается или модифицируется структура таблицы, т.е. задаются имена полей таблицы и их типы, поля описываются, задаются их свойства. В режиме Сводной таблицы и Сводной диаграммы удобно выполнять анализ данных. Существует также дополнительный режим – режим Предварительного просмотра, который позволяет увидеть расположение данных на листе перед осуществлением печати таблицы.

В МА используются три способа создания таблиц: путем ввода данных, с помощью Конструктора таблиц и с помощью Мастера создания таблиц. Обычно создание таблиц путем ввода данных используют только тогда, когда структура таблицы очень проста, например справочник. Использование Мастера таблиц оправдано, если нужно создать какую-то типовую таблицу, пользуясь шаблонами, которые он предложит.

Создавая БД в режиме таблицы, определяем только имя каждого поля. МА, исходя из тех данных, которые вносим в первую запись поля, присвоит каждому полю соответствующий тип. Когда создаете таблицу в режиме конструктора таблицы, то имеет больше возможностей в определении свойств каждого поля. Сюда относится его длина и тип данных, которые будут в нем хранится. Режим конструктора позволяет установить свойства, необходимые для каждой конкретной БД.

Окно конструктора таблиц разделяется на две области. В верхней области отображается сетка, каждая строка которой описывает один столбец БД. Для каждого столбца отображаются его основные характеристики: имя столбца, тип данных, длина и параметр допустимости пустых значений.

В нижней области окна конструктора таблиц отображаются дополнительные характеристики каждого столбца, выделенного в верхней области: размер поля, формат поля, выравнивание текста и др.

1. **Создание форм в СУБД MS Access.**

Форма – это объект БД, предназначенный для ввода и отображения информации. Работа с формами может происходить в трех режимах: в режиме Формы, в режиме Таблицы, в режиме Конструктора. В режимах Формы и Таблицы можно осуществлять добавление, удаление и редактирование записей в таблице или в запросе, являющемся источником данных для форм. В режиме Конструктора можно производить изменения внешнего вида формы, добавление и удаление элементов управления.

В МА можно создавать формы следующих видов:

- форма в столбец или полноэкранная форма;

- ленточная форма;

- табличная форма;

- форма главная/подчиненная;

- сводная таблица;

- форма-диаграмма.

Форма в столбец чаще всего используется для ввода и редактирования данных. Табличная форма отображает данные в режиме таблицы.

Любая форма может включать следующие разделы:

- заголовок формы

- верхний колонтитул – раздел отображается только в режиме предварительного просмотра и обычно содержит заголовки столбцов

- область данных

- нижний колонтитул – раздел отображается только в режиме предварительного просмотра в нижней части экранной страницы и обычно содержит номер страницы, дату и т.д.

- примечание.

Как и любой объект БД форма имеет свойства. Окно свойств выделенного объекта содержит следующие вкладки:

-макет;

-данные;

-события;

-другие.

Основные свойства формы:

- подпись – позволяет задать название формы, которое будет выводиться в области заголовка;

- режим по умолчанию – определяет режим открытия формы (простая, ленточная, табличная формы);

- допустимые режимы – свойство, которое определяет, можно ли с помощью команд меню Вид переходить из режима формы в режим конструктора;

- свойства полосы прокрутки, область выделения, кнопки перехода, разделительные линии, кнопка оконного меню, размеров окна, кнопка закрытия, кнопка контекстной справки, тип границы – определяют, будут ли выводится эти элементы в окно формы;

- свойства разрешить добавления, разрешить удаления, разрешить изменения – определяют, можно ли пользователю редактировать данные через форму. Эти свойства могут принимать значения Да/Нет.

- ввод данных – определяет режим открытия формы и принимает значения Да/Нет. Режим Да – открытие формы только для добавления новых записей. Режим Нет – просмотр существующих записей и добавление новых.

- блокировка записей – определяет способы блокировки записей в режиме многопользовательской работы с БД.

Для создания форм в МА используются следующие виды:

- автоформа – автоматизированное средство для создания форм трех стандартных типов: в столбец, ленточная, табличная. При этом в форму вставляются все поля источника данных.

- мастер форм – программное средство, которое позволяет создавать структуру одного из трех стандартных типов формы в режиме диалога с разработчиком формы. При этом в форму вставляются выбранные пользователем поля из источника данных.

- конструктор форм – позволяет конструировать форму пользователем в режиме конструктора форм.

Самым удобным способом создания новой формы является следующая: форма создается с использованием автоформы или мастером форм, а затем дорабатывается в режиме конструктора.

Источником данных формы является одна или несколько связанных таблиц и/или запросов.

МА предоставляет возможность вводить данные как непосредственно в таблицу, так и с помощью форм. Форма в БД – это структурированное окно, которое можно представить так, чтобы оно повторяло форму бланка. Формы создаются из набора отдельных элементов управления.

Внешний вид формы выбирается в зависимости от того, с какой целью она создается.

Алгоритм создания форм следующий:

- открыть окно БД

- в окне БД выбрать вкладку формы

- щелкнуть на пиктограмме Создать, расположенной на панели инструментов окна БД

- в появившемся диалоговом окне «Новая форма» выбрать способ создания формы и источник данных

- щелкнуть на кнопке ОК.

1. **Создание запросов в СУБД MS Access. Виды запросов.**

Запрос – это средство выбора необходимой информации из базы данных. Вопрос, сформированный по отношению к базе данных, и есть запрос. Применяются два типа запросов: по образцу и структурированный язык запросов (SQL).

Запрос по образцу – средство для отыскания необходимой информации в базе данных. Он формируется не на специальном языке, а путем заполнения бланка запроса в окне Конструктора запросов.

SQL – запросы – это запросы, которые составляются (программистами) из последовательностей SQL – инструкций. Эти инструкции задают, что надо сделать с входным набором данных для генерации выходного набора.

Все запросы Access строит на основе SQL –запросов. Чтобы посмотреть их, необходимо в активном окне проектирования запроса выполнить команду Вид/SQL.

Существует несколько типов запросов: на выборку, на обновление, на добавление, на удаление, перекрестный запрос, создание таблиц. Наиболее распространенными является запрос на выборку. Запросы на выборку используются для отбора нужной пользователю информации, содержащейся в таблицах. Они создаются только для связанных таблиц.

С помощью конструктора можно создать следующие виды запросов:

Простой

По условию

Параметрические

Итоговые

С вычисляемыми полями

Чтобы вызвать Конструктор запросов, необходимо перейти в окно базы данных. В окне база данных необходимо выбрать вкладку Запросы и дважды щелкнуть на пиктограмме Создание запроса в режиме конструктора. Появится активное окно Добавление таблицы на фоне неактивного окна «Запрос: запрос на выборку».  
В окне Добавление таблицы следует выбрать таблицу – источник или несколько таблиц из представленного списка таблиц, на основе которых будет проводиться выбор данных, и щелкнуть на кнопке Добавить. После этого закрыть окно Добавление таблицы, окно «Запрос: запрос на выборку» станет активным.  
Окно Конструктора состоит из двух частей – верхней и нижней. В верхней части окна размещается схема данных запроса, которая содержит список таблиц – источников и отражает связь между ними.  
В нижней части окна находится Бланк построения запроса QBE (Query by Example), в котором каждая строка выполняет определенную функцию:

1. Поле – указывает имена полей, которые участвуют в запросе

2. Имя таблицы – имя таблицы, с которой выбрано это поле

3. Сортировка – указывает тип сортировки

4. Вывод на экран – устанавливает флажок просмотра поля на экране

5. Условия отбора  - задаются критерии поиска

6. Или – задаются дополнительные критерии отбора

В окне  «Запрос: запрос на выборку» с помощью инструментов формируем query:

1. Выбрать таблицу – источник, из которой производится выборка записей.

2. Переместить имена полей с источника в Бланк запроса. Например, из таблицы Группы студентов отбуксировать поле Название в первое поле Бланка запросов, из таблицы Студенты отбуксировать поле Фамилии во второе поле Бланка запросов, а из таблицы Успеваемость отбуксировать поле Оценка в третье поле и из таблицы Дисциплины отбуксировать поле Название в четвертое поле Бланка запросов.

1. Задать принцип сортировки. Курсор мыши переместить в строку Сортировка для любого поля, появится кнопка открытия списка режимов сортировки: по возрастанию и по убыванию. Например, установить в поле Фамилия режим сортировки – по возрастанию.

2. В строке вывод на экран автоматически устанавливается флажок просмотра найденной информации в поле.

3. В строке "Условия" отбора и строке "Или" необходимо ввести условия ограниченного поиска – критерии поиска. Например, в поле Оценка ввести  - "отл/A", т.е. отображать все фамилии студентов, которые получили оценки отл/A.

4. После завершения формирования запроса закрыть окно Запрос на выборку. Откроется окно диалога Сохранить – ответить Да (ввести имя созданного запроса, например, Образец запроса в режиме Конструктор) и щелкнуть ОК и вернуться в окно базы данных. Чтобы открыть query из окна базы данных, необходимо выделить имя запроса и щелкнуть кнопку Открыть, на экране появится окно запрос на выборку с требуемым именем.

Параметрические запросы  
Запросы, представляющие собой варианты базового запроса и незначительно отличающиеся друг от друга, называются параметрическими. В параметрическом запросе указывается критерий, который может изменяться по заказу пользователя.  
Последовательность создания параметрического запроса:

1. Создать query в режиме конструктора или открыть существующий запрос в режиме конструктора, например «Образец запроса в режиме Конструктор».

2. В Бланк запроса в строке Условия отбора ввести условие отбора в виде приглашения в квадратных скобках, например [Введите фамилию]

3. Закрыть окно Запрос на выборку, на вопрос о сохранении изменения ответить – Да. Вернуться в окно базы данных, где созданный query будет выделен.

4. Выполнить query, щелкнув по кнопке: Открыть. В появившемся на экране окне диалога «Введите значение параметра» надо ввести, например фамилию студента, информацию об успеваемости которого необходимо получить, выполнить щелчок по кнопке ОК.

**17.Создание отчетов в СУБД MS Access.**

**Отчет** – это форматированное представление данных, которое выводится на экран, в печать или файл. Они позволяют извлечь из базы нужные сведения и представить их в виде, удобном для восприятия, а также предоставляют широкие возможности для обобщения и анализа данных.  
При печати таблиц и запросов информация выдается практически в том виде, в котором хранится. Часто возникает необходимость представить данные в виде отчетов, которые имеют традиционный вид и легко читаются. Подробный отчет включает всю информацию из таблицы или запроса, но содержит заголовки и разбит на страницы с указанием верхних и нижних колонтитулов.

**Структура отчета в режиме Конструктора**

Microsoft Access отображает в отчете данные из запроса или таблицы, добавляя к ним текстовые элементы, которые упрощают его восприятие.  
К числу таких элементов относятся:

1. Заголовок. Этот раздел печатается только в верхней части первой страницы отчета. Используется для вывода данных, таких как текст заголовка отчета, дата или констатирующая часть текста документа, которые следует напечатать один раз в начале отчета. Для добавления или удаления области заголовка отчета необходимо выбрать в меню Вид команду Заголовок/примечание отчета.

2. Верхний колонтитул. Используется для вывода данных, таких как заголовки столбцов, даты или номера страниц, печатающихся сверху на каждой странице отчета. Для добавления или удаления верхнего колонтитула необходимо выбрать в меню Вид команду Колонтитулы. Microsoft Access добавляет верхний и нижний колонтитулы одновременно. Чтобы скрыть один из колонтитулов, нужно задать для его свойства Высота значение 0.

3. Область данных, расположенная между верхним и нижним колонтитулами страницы. Содержит основной текст отчета. В этом разделе появляются данные, распечатываемые для каждой из тех записей в таблице или запросе, на которых основан отчет. Для размещения в области данных элементов управления используют список полей и панель элементов. Чтобы скрыть область данных, нужно задать для свойства раздела Высота значение 0.

4. Нижний колонтитул. Этот раздел появляется в нижней части каждой страницы. Используется для вывода данных, таких как итоговые значения, даты или номера страницы, печатающихся снизу на каждой странице отчета.

5. Примечание. Используется для вывода данных, таких как текст заключения, общие итоговые значения или подпись, которые следует напечатать один раз в конце отчета. Несмотря на то, что в режиме Конструктора раздел "Примечание" отчета находится внизу отчета, он печатается над нижним колонтитулом страницы на последней странице отчета. Для добавления или удаления области примечаний отчета необходимо выбрать в меню Вид команду Заголовок/примечание отчета. Microsoft Access одновременно добавляет и удаляет области заголовка и примечаний отчета

**Способы создания отчета**

В Microsoft Access можно создавать отчеты различными способами:

1. Конструктор

2. Мастер отчетов

3. Автоотчет: в столбец

4. Автоотчет: ленточный

5. Мастер диаграмм

6. Почтовые наклейки

Мастер позволяет создавать отчеты с группировкой записей и представляет собой простейший способ создания отчетов. Он помещает выбранные поля в отчет и предлагает шесть стилей его оформления. После завершения работы Мастера полученный отчет можно доработать в режиме Конструктора. Воспользовавшись функцией Автоотчет, можно быстро создавать отчеты, а затем вносить в них некоторые изменения.

Для создания Автоотчета необходимо выполнить следующие действия:

1. В окне базы данных щелкнуть на вкладке Отчеты и затем щелкнуть на кнопке Создать. Появится диалоговое окно Новый отчет.

2. Выделить в списке пункт Автоотчет: в столбец или Автоотчет: ленточный.

3. В поле источника данных щелкнуть на стрелке и выбрать в качестве источника данных таблицу или запрос.

4. Щелкнуть на кнопке ОК.

5. Мастер автоотчета создает автоотчет в столбец или ленточный (по выбору пользователя), и открывает его в режиме Предварительного просмотра, который позволяет увидеть, как будет выглядеть отчет в распечатанном виде.

6. В меню Файл щелкнуть на команде Сохранить. В окне Сохранение в поле Имя отчета указать название отчета и щелкнуть на кнопке ОК.

**18. Характеристика и функциональные возможности PowerPoint**

**Microsoft PowerPoint** (полное название — **Microsoft Office PowerPoint**) — программа для создания и проведения [презентаций](http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B5%D0%B7%D0%B5%D0%BD%D1%82%D0%B0%D1%86%D0%B8%D1%8F_%28%D1%81%D0%BF%D0%BE%D1%81%D0%BE%D0%B1_%D0%BF%D1%80%D0%B5%D0%B4%D1%81%D1%82%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8%29), являющаяся частью [Microsoft Office](http://ru.wikipedia.org/wiki/Microsoft_Office) и доступная в редакциях для операционных систем [Microsoft Windows](http://ru.wikipedia.org/wiki/Microsoft_Windows) и [Mac OS](http://ru.wikipedia.org/wiki/Mac_OS).

Программа MS PowerPoint является специализированным средством автоматизации для создания и оформления презентаций, призванных наглядно представить работы исполнителя группе других людей. Программа обеспечивает разработку электронных документов особого рода, отличающихся комплексным мультимедийным содержанием и особыми возможностями воспроизведения. MS PowerPoint позволяет разрабатывать следующие документы:

1. презентации, рассчитанные на распечатку на прозрачной пленке с целью их демонстрации через оптический проектор;
2. презентации, рассчитанные на распечатку на 35-мм диапозитивной фотопленке с целью их демонстрации через оптический слайд-проектор;
3. презентации, рассчитанные на воспроизведение через компьютерный проектор;
4. материалы презентации для автономного показа на экране компьютера;
5. материалы презентации для публикации в сетевом окружении с последующим автономным просмотром;
6. материалы презентации для рассылки по электронной почте с последующим автономным просмотром адресатами;
7. материалы презентации для распечатки на бумаге с целью последующей раздачи.

Любой документ MS PowerPoint представляет собой набор отдельных, но взаимосвязанных кадров, называемых **слайдами**. Каждый слайд в документе имеет собственный уникальный номер, присваиваемый по умолчанию в зависимости от места слайда. Последовательность слайдов в документе линейная. Слайды могут содержать объекты самого разного типа, например: фон, текст, таблицы, графические изображения и т.д. При этом на каждом слайде присутствует как минимум один объект - фон, который является обязательным элементом любого слайда.

1. **Типовые ошибки при создании презентаций.**

Общие принципы:

-оформление не должно мешать восприятию материала;

-любой прием (цвет, фон, тень, рамка, рисунок, список) должен быть обоснован и должен работать на главную идею презентации;

- не надо повторять целиком текст, который будет сказан, только опорные моменты.

Необходимо:

- излагать материал просто и понятно;

- текст должен без труда читаться;

- не должно быть очень много текста;

- иллюстрации по теме;

- красивое оформление, помогающее раскрыть тему.

Все ошибки можно разделить на две категории: стратегические и тактические. Начнем с трех основных стратегических ошибок.

Ошибка первая, самая важная. В презентации отсутствует единое идейное наполнение. Рекомендуется перед тем, как составить презентацию, сформулировать на листочке: какие именно идеи (а их не должно быть больше трех) вы хотели донести до слушателей. И составляя каждый слайд, проверять – насколько он работает на донесение этих идей до аудитории.

Ошибка вторая. Идеи, которые вы сформулировали, должны быть интересны и значимы для аудитории.

Ошибка третья – нежелание посвятить аудиторию в структуру презентации. Перед началом выступления нужно познакомить аудиторию с планом рассказа – чтобы слушателям было проще следить за мыслью и примерно представлять общее содержание.

Тактические ошибки. Ошибка первая. Информации слишком много. В эту группу ошибок попадает нагромождение информации на одном слайде, с чрезмерным цветовым и шрифтовым оформлением.

Вторая тактическая ошибка является противоположностью первой и заключается в непредоставлении аудитории важной информации по теме слайда или сообщения в целом.

Типичные недостатки структуры и формы представления информации:

- отсутствие титульного слайда, содержащего: название проекта, сведения об авторе, дату разработки идр.

-отсутствия введения, в котором представлены: цели и задачи изучения темы, краткая характеристика содержания.

- отсутствие Оглавления.

- отсутствие логического завершения презентации, содержащего: заключение, обобщения, выводы.

- перегрузка слайдов подробной текстовой информацией;

- неравномерное и нерациональное использование пространства на слайде.

-отсутствие связи фона презентации с содержанием.

Часто встречающиеся ошибки стиля и оформления:

- орфографические и стилистические ошибки;

- отсутствие единства стиля страниц;

- неудачный выбор цветовой гаммы: использование слишком ярких и утомительных цветов, использование в дизайне более 3 базовых цветом, использование темного фона со светлым текстом;

- использование разных фонов на слайдах в рамках одной презентации;

- отсутствие полей на слайдах;

- использование рисунков, фотографий плохого качества и с искажениями пропорций.

- использование слишком мелкого шрифта;

- использование шрифтов существенно разного размера на соседних слайдах;

- использование шрифта с засечками, затрудняющего восприятие информации;

- отсутствия должного выравнивания текста;

- слишком быстрая смена слайдов и анимационных эффектов (при автоматической настройке презентации).

1. **Структура HTML документа. Вывод и форматирование текста. Понятие гиперссылки.**

НТМL (от англ. HyperText Markup Language – «язык разметки гипертекста») – стандартный язык разметки документов во Всемирной паутине. Большинство веб-страниц создаются при помощи языка HTML. Язык HTML интерпретируется браузером и отображается в виде документа в удобной для человека форме.

Язык HTML был разработан британским ученым Тимом Бернерсом-Ли приблизительнов 1989-1991 годах в стенах Европейского совета по ядерным исследованиям в Женеве (Швейцария). HTML создавался как язык для обмена научной и технической документацией. С помощью HTML можно легко создавать относительно простой, но красиво оформленный документ. Позже были добавлены мультимедийные возможности.

Любой документ на языке HTML представляет собой набор элементов, причем начало и конец каждого элемента обозначается специальными пометками – тегами. Элементы могут быть пустыми, то есть не содержащими никакого текста и других данных (например, тег перевода строки <br>). В этом случае обычно не указывается закрывающий тег. Кроме того, элементы могут иметь атрибуты, определяющие какие- либо их свойства (например, размер шрифта для элемента font). Атрибуты указываются в открывающем теге.

Регистр, в котором набрано имя элемента и имена атрибутов, в HTML значения не имеет. Элементы могут быть вложенными. Например, <b>этот текст будет полужирным,<i>а этот – еще и курсивным</i></b>.

Кроме элементов, в HTML-документах есть и сущности – специальные символы. Сущности начинаются с символа амперсанда и имеют вид &имя. Например, &copy – знак авторского права. Как правило, сущности используются для представления символов, отсутствующих в кодировке документа, или же для представления «специальных» символов: &amp –амперсанда, &lt – символа «меньше» и &gt – символа больше, которые некорректно записывать «обычным» образом, из-за их особого значения в HTML.

Каждый HTML- документ, отвечающий спецификации HTML какой-либо версии, должен начинаться со строки объявления версии HTML <!DOCTYPE…>. Если эта строка не указана, т добиться корректного отображения документа в браузере становится труднее. Далее обозначается начало и конец документа тегами <html> и </html> соответственно. Внутри этих тегов должны находиться теги заголовка <head></head> и тела (<body></body>) документа.

Заголовок HTML-документа является необязательным элементом разметки. Элемент разметки TITLE служит для именования окна браузера, в котором просматривают документ. Состоит контейнер из тега начала, содержания и тега конца. Наличие тега конца обязательно. Тег начала элемента не имеет специфических атрибутов.

**Вывод и форматирование текста**. Чтобы отобразить неотформатированный текст, достаточно просто ввести его между тегами начала и конца документа <body></body>. При обработке такой страницы браузер найдет и выведет весь этот текст. Если необходимо, чтобы к тексту было применено какое-либо форматирование, например, выделение <b>полужирным</b> или <i>курсивом</i>, необходимо использовать соответствующие теги форматирования. При этом форматируемый текст помещается между тегами.

Также для выделения текста используются теги <strong> и <em>, данные теги являются контейнерами и требуют закрывающегося тега. Тег <strong> сообщает браузеру, что на заключенном в нем тексте необходимо сделать сильное ударение. Обычно визуальные браузеры отображают содержимое данного тега полужирным шрифтом, но это может быть легко изменено с помощью таблицы стилей. Так как данный тег является структурным, он несет смысловую нагрузку, в отличие от тега <b>, который лишь форматирует текст полужирным, то его использовать предпочтительней. Тег <em> тоже акцентирует внимание на заключенном внутри тексте, но он считается менее сильным ударением. Отображается он, как правило, курсивом. По тем же причинам использовать <em> предпочтительней, чем применение <i>.

Еще одной парой тегов форматирования являются теги <big> и <small>. Первый выводит текст увеличенным по сравнению со стандартным, а второй уменьшенным. По поводу применения тега <small> следует сделать одно замечание: на разных компьютерах установлено различное разрешение экрана и в браузере может быть установлен различный размер основного шрифта и сильное уменьшение текста может сделать текст не читаемым.

Другой парой полезных тегов являются <sup> - верхний индекс и <sub> - нижний индекс, которые могут быть полезными при написании математических и химических формул.

В некоторых случаях, например для вывода кода программ, полезным будет использование тега <pre>, который сообщает браузеру, что находящийся внутри текст должен быть выведен как есть. При этом будут сохранены все пробелы, переносы строк и прочие символы, которые обычно при выводе браузером не отображаются.

**Понятие гиперссылки.** Гиперссылка – часть гипертекстового документа, ссылающегося на другой элемент (команда, текст, заголовок, примечание, изображение) в самом документе, на другой объект (файл, директория, приложение), расположенный на локальном диске или в компьютерной сети.

Гиперссылка может быть добавлена к любому элементу гипертекстового документа и обычно выделяется графически. В HTML- документах текстовые ссылки по умолчанию выделяются синим цветом, при наведении на них курсором мыши в окне браузера изменяются, например, меняют цвет или выделяются подчеркиванием. При навигации в браузере с помощью клавиатуры текстовые и графические ссылки выделяются прямоугольной пунктирной рамочкой. Посещенная ранее ссылка обычно выделяется цветом, отличным от цвета непосещенной ссылки.

«Битой» ссылкой называют такую гиперссылку, которая ссылается на отсутствующий по каким-либо причинам объект, например, если документ или файл удален или перемещен администратором ресурса, на котором он был расположен, или если сам ресурс недоступен. Обычно в таком случае на странице появляется сообщение с кодом ошибки.

Для определения ссылки в HTML используется тег <a>, структура которого имеет вид <a href=”filename»> Текст ссылки </a>, где «filename» - имя файла или адрес в Интернете, на который необходимо сослаться, а «Текст ссылки» - текст гипертекстовой ссылки, который будет непосредственно показан в HTML-документе.

1. **Язык расширенной разметки XML. Корректные и валидные XML-документы.**

Икс-эм-эль – расширяемый язык разметки, фактически представляющий собой свод общих синтаксических правил. XML – текстовый формат, предназначенный для хранения структурированных данных, для обмена информацией между программами, а также для создания на ого основе более специализированных языков разметки (например, XHTML).

XML – это потомок HTML. Разница в том, что HTML имеет четко определенные теги, новые теги появляются лишь по воле разработчиков стандартов и браузеров. В XML совсем другая картина: количество предустановленных (служебных) тегов минимизировано, и программист волен использовать собственные теги.

Годом рождения XML можно считать 1996 год, в конце которого появился черновой вариант спецификации языка, или 1998 год, когда эта спецификация была утверждена.

Первая строка XML-документа называется объявление XML – это строка, указывающая версию XML. В версии 1.0 объявление XML может быть опущено, в версии 1.1 оно обязательно. Также может быть указана кодировка символов.

Важнейшее обязательное синтаксическое требование заключается в том, что документ имеет только один корневой элемент. Это означает, что текст или другие данные всего документа должны быть расположены между единственным начальным корневым тегом и соответствующим ему конечным тегом.

Следующий простейший пример – правильно построенный документ XML:

<book>Это книга: «Книжечка»</book>

Следующий пример не является корректным XML-документом, потому что имеет два корневых элемента:

<thing>Сущность №1</thing>

<thing>Сущность №2</thing>

В любом месте дерева может быть размещен элемент-комментарий. XML-комментарии размещаются внутри специального тега, начинающегося с символов <!—и заканчивающегося символами -- >. Два знака дефис (- -) внутри комментария присутствовать не могут. Теги внутри комментария обрабатываться не должны.

XML- документ состоит из элементов, некоторые из которых имеют атрибуты и содержимое. Элемент обычно состоит из открывающего и закрывающего тегов, обрамляющих текст и другие элементы. Открывающий тег состоит из имени элемента в угловых скобках, например, <step>, а закрывающий тег состоит из того же имени в угловых скобках, но перед именем еще добавляется косая черта, например </step>. Имена элементов, как и имена атрибутов, не могут содержать пробелы.

Содержимым элемента называется все, что расположено между открывающим и закрывающими тегами, включая текст и другие элементы.

Кроме содержания у элемента могут быть атрибуты – пары имя-значение, добавляемые в открывающий тег после названия элемента. Значения атрибутов всегда заключаются в кавычки (одинарные или двойные), одно и то же имя атрибута не может встречаться дважды в одном элементе. Не рекомендуется использовать разные типы кавычек для значений атрибутов одного тега.

В XML определены два метода записи специальных символов: ссылка на сущность и ссылка по номеру символа.

Сущностью в XML называются именованные данные, обычно текстовые, в частности, спецсимволы. Ссылка на сущность указывается в том месте, где должна быть сущность и состоит из амперсанда (&), имени сущности и точки с запятой (;).

В XML есть несколько предопределенных сущностей, такие как lt(ссылать на нее можно написав &lt;) для левой угловой скобки и amp (ссылка - &amp;) для амперсанда. Возможно также определять собственные сущности.

Ссылка по номеру символа выглядит как ссылка на сущность, но вместо имени сущности указывается символ # и число (в десятичной или шестнадцатеричной записи), являющееся номером символа в кодовой таблице Юникод.

Стандартом определены два уровня правильности документа XML:

1. Правильно построенный соответствует всем общим правилам синтаксиса XML. И если, например, начальный тег не имеет соответствующего ему конечного тега, то это неправильно построенный документ XML. Документ, который неправильно построен, не может считаться документом XML. XML-процессор не должен обрабатывать его обычным образом и обязан классифицировать ситуацию как фатальная ошибка.
2. Действительный (англ. valid). Действительный документ дополнительно соответствует некоторым семантическим правилам. Это более строгая дополнительная проверка корректности документа на соответствие заранее определенным, но уже внешним правилам, в целях минимизации количества ошибок. Эти правила могут быть разработаны как самим пользователем, так и сторонними разработчиками. Обычно такие правила хранятся в специальных файлах – схемах, где самым подробным образом описана структура документа, все допустимые названия элементов, атрибутов и многое другое. И если документ, например, содержит не определенное заранее в схемах название элемента, то XML-документ считается недействительным; проверяющий XML-процессор при проверке на соответствие правилам и схемам обязан сообщить об ошибке.
3. **JavaScript и объектная модель документа. Ключевые объекты.**

При генерации страниц в Web возникает дилемма, связанная с архитектурой «клиент-сервер». Страницы можно генерировать как на стороне клиента, так и на стороне сервера. В 1995 году специалисты компании Netscape создали механизм управления страницами на клиентской стороне, разработав язык программирования JS. Т.о. JS – это язык управления сценариями просмотра гипертекстовых страниц Web на стороне клиента. Основная идея JS состоит в возможности изменения значений атрибутов HTML-контейнеров и свойств среды отображении в процессе просмотра HTML- страницы пользователем. При этом перезагрузки страницы не происходит. На практике это выражается в том, что можно, например, изменить цвет фона страницы или интегрированную в документ картинку, открыть новое окно или выдать предупреждение.

JS – объетно-ориентированный скриптовый язык программирования. Наиболее широкое применение находит в браузерах как язык сценариев для придания интерактивности веб-страницам. На JS оказали влияние многие языки, при разработке была цель сделать язык похожим на Java, но при этом легким для использования непрограммистами.

JS используется для написания прикладного ПО. Одним из ярких примеров является Mozilla Firefox, 57% исходного кода которого написано на JS. JS используется в офисных приложениях для автоматизации рутинных действий, написания макросов.

На сегодняшний день поддержку JS обеспечивают современные версии всех наиболее часто используемых браузеров: IE, Mozilla Firefox, Opera

Синтаксис языка JS во многом напоминает синтаксис Си и Java. В JS:

- все идентификаторы регистрозависимы;

- в названиях переменных можно использовать буквы, подчеркивание, символ доллара, арабские цифры;

- названия переменных не могут начинаться с цифры;

- для оформления однострочных комментариев используются //, многострочные и внутристрочные комментарии начинаются с /\* и заканчиваются \*/.

Для добавления JS-код на страницу, можно использовать теги <script></script>.

Исполняет JS-код браузер. В него встроен интерпретатор JS.

DOM (Document Object Model – объектная модель документа) – не зависящий от платформы и языка программный интерфейс, позволяющий программам и скриптам получить доступ к содержимому HTML, XHTML, XNL- документов, а также изменять содержимое, структуру и оформление таких документов.

Учитывая существование различных реализаций DOM в веб-браузерах, среди программистов распространена привычка проверять работоспособность тех или иных возможностей DOM для каждого конкретного браузера, и только потом использовать их. Из-за несовместимости браузеров использование DOM иногда приводит к трудностям HTML-верстки и низкой надежности страниц.

Объектная модель документа является стандартом, предложенным веб-консорциумом, и регламентирует способ представления содержимого документа (в частности веб-страницы) в виде набора объектов. Под содержимым понимается все, что может находиться на веб-странице: рисунки, ссылки, абзацы, текст и т.д. В отличие от объектной модели браузера, которая уникальна для каждого браузера, объектная модель документа является стандартом и должна поддерживаться всеми браузерами. И хотя на практике поддержка DOM реализована не в полной мере, тем не менее необходимо стремиться следовать требованиям этого стандарта как производителям браузеров, так и разработчикам веб-сайтов.

Следует заметить, что DOM может применяться не только в веб-страницах, но и в любых других документах.

DOM является развивающимся стандартом и разбит на три уровня. Первый уровень является первой версией стандарта и пока что единственной законченной. Он состоит из двух разделов: первый является ядром и определяет принципы манипуляции со структурой документа (генерация и навигация), а второй посвящен представлению в DOM элементов HTML, определяемых одноименными тегами. Второй и третий уровни описывают модель событий, дополняют таблицы стилей, проходы по структуре.

В DOM документ представляется в виде древовидной структуры, являющейся одной из наиболее употребительных структур в программировании. В модели DOM к элементу можно обратиться непосредственно по его идентификатору id.

Объект в JS – наиболее важная единица, используемая в языке программирования JS, это самый главный тип данных. Большая часть работы с объектами в JS сводится к работе со встроенными объектами, т.к. создание собственных объектов не является респектабельным ввиду того, что они смогут работать только в пределах одной единственной страницы.

JS – это язык программирования, основанный на объектах. Все объекты, доступные сценарию на языке JS, подразделяются на три группы:

- встроенные объекты исполняющей системы;

- объекты среды, в которой исполняется сценарий (т.е. либо объекты клиента, либо объекты сервера);

- пользовательские объекты, создаваемые сценарием в процессе его выполнения.

Объект в JS – это неупорядоченный набор свойств. Для доступа к свойству объекта используется синтаксис:

имя\_объекта.имя\_свойства

**Основные объекты:**

**Array (массив)** – собрание элементов данных, расположенных в определенном порядке, что-то вроде картотеки, состоящей из множества ящиков. Каждый такой «ящик» имеет имя, которое называется индексом. Обычно значения индексов начинаются с 0 и последовательно увеличиваются на единицу. Размещаются значения индексов в квадратных скобках после имени массива.

**Length** обозначает число элементов в массиве.

**Prototype** – функция, позволяющая назначать объекту новые свойства и методы.

1. **Классификация и действие вирусов.**

**24. Вредоносное ПО. Виды и особенности.**

Вредоносная программа – это любое программно обеспечение, предназначенное для обеспечения получения несанкционированного доступа к информации, хранимой на ЭВМ, с целью причинения вреда (ущерба) владельцу информации.

Наиболее распространенным видами вредоносных программ являются трояны, черви и вирусы.

Троян – вредоносная программа, используемая злоумышленниками для сбора информации, ее разрушения или модификации, нарушения работоспособности компьютера или использования его ресурсов в неблаговидных целях. К троянским коням обычно относят программы, которые внедряются в систему и скрытно от пользователя выполняют заложенные в них злоумышленником действия. Это очень разнообразный класс вредоносного ПО. В первую очередь их различают по типу действия. Среди них есть программы, позволяющие злоумышленникам осуществлять удаленное управление зараженным компьютером, показывающие рекламу, направляющие пользователей на различные сайты, загружающие и устанавливающие в систему другое вредоносное ПО, рассылка спама, участие в DOS-атаках.

Одним из способом распространения троянских коней являются веб-страницы с внедренными в них специальными скриптами. Благодаря существующим в разных браузерах уязвимостям при посещении такого сайта вредоносное ПО автоматически загружается на компьютер и внедряется в систему.

Компьютерный вирус – разновидность компьютерной программы, отличительной особенностью которой является способность к размножению (саморепликации). В дополнение к этому он может повреждать или полностью уничтожать данные, подконтрольные пользователю, от имени которого была запущена зараженная программа. Среди компьютерных вирусов есть как совершенно безобидные (программы-шутки), так и очень опасные, способные обрушить систему, уничтожить все документы на жестком диске. Распространяются они в большинстве случаев с помощью мобильных накопителей информации (CD и DVD-диски, флеш-карты, внешние винчестеры).

В первое время пальму первенства по широте распространения надежно удерживали вирусы, поражающие исполняемые файлы. Однако сегодня они уступили ее макровирусам. Это вредоносное ПО представляет собой макросы, внедряющиеся в различные документы (особенно сильно этим страдают документы Microsoft Office) и выполняющие определенные деструктивные действия.

Сетевой червь – разновидность самовоспроизводящейся компьютерной программы, распространяющейся в локальных и глобальных компьютерных сетях. Для этого они используют разные способы. Еще недавно самым популярным из них была рассылка по Email (как вариант, различные менеджеры ICQ, IRC), ссылки на файл, размещенный на веб-странице. Внедряясь в систему, сетевой червь самостоятельно отправлял письма со своей копией на почтовые ящики из адресной книги зараженного компьютера. Сетевые черви известны тем, что несколько раз устраивали настоящие эпидемии, охватывающие весь земной шар.

Однако в последнее время все больше и больше вирусов переходя на автоматическое внедрение, используя при этом «дыры» в клиентах и самой операционной системе.

Обнаружить присутствие сетевого червя можно по трем основным признакам. Первый – большое количество исходящих TCP/IP-пакетов, которые рассылаются постоянно или через более-менее определенные промежутки времени. Второй – подозрительное содержимое TCP/IP-пакетов. Однако для конечного пользователя наибольшую пользу представляет собой третий признак – необычная структура потребляемого трафика. Необъяснимое увеличение потребляемого или резкое увеличение доли исходящего трафика почти наверняка указывает на наличие вредоносного ПО.

Вредоносные программы чаще всего проникают на компьютер через Интернет или по электронной почте.

Симптомы заражения:

- автоматическое открытие окон с незнакомым содержанием при запуске компьютера;

- блокировка доступа к официальным сайтам антивирусных компаний;

- появление новых неизвестных процессов в окне «Процессы» диспетчера задач Windows;

- появление в ветках реестра, отвечающих за автозапуск, новых записей;

- запрет на изменение настроек компьютера в учетной записи администратора;

- невозможность запустить исполняемый файл (выдается сообщение об ошибке);

- появление всплывающих окон или системных сообщение с непривычным тексом, в том числе содержащих неизвестные веб-адреса;

- перезапуск компьютера во время старта какой-либо программы;

- случайное или беспорядочное отключение компьютера;

- случайное аварийное завершение программ и др.

Методы защиты от вредоносных программ:

- использовать современные ОС, не дающие изменять важные файлы без ведома пользователя;

- своевременно устанавливать обновления;

- использование антивирусных программ;

- ограничить физический доступ к компьютеру посторонних лиц;

- стараться работать на ПК под правами пользователя, а не администратора, что не позволит большинству вредоносных программ инсталлировать на ПК;

- использовать внешние носители информации только от проверенных источников;

- не открывать компьютерные файлы, полученные от ненадежных источников.

1. **Методы работы и основные компоненты антивирусного ПО.**

Антивирусная программа – любая программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления зараженных (модифицированных) такими программами файлов, а также для профилактики – предотвращения заражения файлов и ОС вредоносным кодом.

Современные антивирусные программы обычно состоят из нескольких модулей:

1. Антивирусный монитор работает постоянно, проверяя все открываемые файлы.
2. Антивирусный сканер проверяет систему только тогда, когда пользователь сам пожелает.
3. Веб-экран защищает компьютер от вторжения вирусов, скриптов и несанкционированного вторжения при серфинге в Интернет.
4. Модуль защиты электронной почты проверяет все приходящие письма на наличие вредоносных элементов и спама.
5. Модуль автоматического обновления производит обновление антивирусной базы с сервера фирмы- производителя этого антивируса. В связи с постоянным появлением новых образцов вирусов данных модуль должен запускаться как можно чаще, а лучше оставить его работать постоянно.
6. Планировщик организует запуск тех или иных задач по расписанию. Например, обновление раз в час, сканирование диска С раз в неделю.
7. Всю работу организует обычно отдельный модель, который называют Центром управления. Как правило, через центр управления можно управлять любым модулем – отключать, принудительно запускать и прочее.

Из всех методов антивирусной защиты можно выделить две основные группы:

Сигнатурные методы – точные методы обнаружения вирусов, основанные на сравнении файла с известными образцами вирусов.

Эвристические методы – приблизительные методы обнаружения, которые позволяют с определенной вероятность предположить, что файл заражен.

СИГНАТУРНЫЙ АНАЛИЗ. Сигнатурный анализ заключается в выявлении характерных идентифицирующих черт каждого вируса и поиска вирусов путем сравнения файлов с выявленными чертами. Сигнатурой вируса будет считаться совокупность черт, позволяющих однозначно идентифицировать наличие вируса в файле. Все вместе сигнатуры известных вирусов составляют антивирусную базу.

Задачу выделения сигнатур, как правило, решают люди – эксперты в области компьютерной вирусологии, способные выделить код вируса из кода программы и сформулировать его характерные черты в форме, наиболее удобной для поиска.

Практически в каждой компании, выпускающей антивирусы, есть своя группа экспертов, выполняющая анализ новых вирусов и пополняющая антивирусную базу новыми сигнатурами. По этой причине антивирусные базы в разных антивирусах отличаются. Тем не менее, между антивирусными компаниями существует договоренность об обмене образцами вирусов, а значит рано или поздно сигнатура нового вируса попадет в антивирусных базы практически всех антивирусов. Лучшим же антивирусом будет тот, для которого сигнатура нового вируса была выпущена раньше всех.

Одно из распространенных заблуждений насчет сигнатур заключается в том, что каждая сигнатура соответствует ровно одному вирусу или вредоносной программе. И как следствие, антивирусная база с большим количеством сигнатур позволяет обнаруживать больше вирусов. На самом деле это не так. Очень часто для обнаружения семейства похожих вирусов используется одна сигнатура, и поэтому считать, что количество сигнатур равно количеству обнаруживаемых вирусов, уже нельзя.

Соотношение количества сигнатур и количества известных вирусов для каждой антивирусной базы свое и вполне может оказаться, что база с меньшим количеством сигнатур в действительности содержит информацию о большем количестве вирусов.

Важное дополнительное свойство сигнатур – точное и гарантированное определение типа вируса. Это свойство позволяет занести в базу не только сами сигнатуры, но и способы лечения вируса.

Другое важное, но уже отрицательное свойство – для получения сигнатуры необходимо иметь образец вируса. Следовательно, сигнатурный метод непригоден для защиты от новых вирусов, т.к. до тех пор пока вирус не попал на анализ к экспертам, создать его сигнатуру невозможно. Именно поэтому все наиболее крупные эпидемии вызываются новыми вирусами. С момента появления вируса в сети Интернет до выпуска первых сигнатур обычно проходит несколько часов, и все это время вирус способен заражать компьютеры.

**Эвристический анализ.** Суть эвристических методов состоит в том, что решение проблемы основывается на некоторых правдоподобных предположениях, а не на строгих выводах из имеющихся фактов и предпосылок.

**Эвристические методы.** **Поиск вирусов, похожих на известные.**

Если сигнатурный метод основан на выделении характерных признаков вируса и поиске этих признаков в проверяемых файлах, то эвристический анализ основывается на предположении, что новые вирусы часто оказываются похожи на какие-либо из уже известных. Основанный на таком предположении эвристический метод заключается в поиске файлов, которые не полностью, но очень близко соответствуют сигнатурам известных вирусов.

Положительным эффектом от использования этого метода является возможность обнаружить новые вирусы еще до того, как для них будут выделены сигнатуры. Отрицательные стороны:

-вероятность ошибочно определить в файле вируса, когда на само деле файл чист – такие события называются ложными срабатываниями.

- невозможность лечения – и в силу возможных ложных срабатываний, и в силу возможного неточного определения типа вируса, попытка лечения может привести к большим потерям информации, чем сам вирус.

- низкая эффективность – против действительно новаторских вирусов, вызывающих наиболее масштабные эпидемии, этот вид эвристического анализа малопригоден.

**Поиск вирусов, выполняющих подозрительные действия**

Метод основан на выделении основных вредоносных действий, таких как, например:

- удаление файла;

- запись в файл;

- запись в определенные области системного реестра;

- перехват данных вводимых с клавиатуры;

- рассылки писем и др.

**26.Принципы защиты серверов и клиентских компьютеров от вредоносного ПО**

Абсолютной защиты от вредоносных программ не существует: от «эксплойтов [нулевого дня](http://ru.wikipedia.org/w/index.php?title=%D0%A3%D1%8F%D0%B7%D0%B2%D0%B8%D0%BC%D0%BE%D1%81%D1%82%D1%8C_%D0%BD%D1%83%D0%BB%D0%B5%D0%B2%D0%BE%D0%B3%D0%BE_%D0%B4%D0%BD%D1%8F&action=edit&redlink=1)» наподобие [Sasser](http://ru.wikipedia.org/wiki/Sasser) или [Conficker](http://ru.wikipedia.org/wiki/Conficker) не застрахован никто. Но с помощью некоторых мер можно существенно снизить риск заражения вредоносными программами. Ниже перечислены основные и наиболее эффективные меры для повышения безопасности:

* использовать современные операционные системы, не дающие изменять важные файлы без ведома пользователя;
* своевременно устанавливать обновления;
* если существует режим автоматического обновления, включить его;
* помимо антивирусных продуктов, использующих сигнатурные методы поиска вредоносных программ, использовать программное обеспечение, обеспечивающее [проактивную защиту](http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B0%D0%BA%D1%82%D0%B8%D0%B2%D0%BD%D0%B0%D1%8F_%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B0) от угроз (необходимость использования [проактивной защиты](http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B0%D0%BA%D1%82%D0%B8%D0%B2%D0%BD%D0%B0%D1%8F_%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B0) обуславливается тем, что сигнатурный антивирус не замечает новые угрозы, еще не внесенные в антивирусные базы);
* постоянно работать на персональном компьютере исключительно под правами пользователя, а не администратора, что не позволит большинству вредоносных программ инсталлироваться на персональном компьютере;
* ограничить физический доступ к компьютеру посторонних лиц;
* использовать внешние носители информации только от проверенных источников;
* не открывать компьютерные файлы, полученные от ненадёжных источников;
* использовать персональный Firewall (аппаратный или программный), контролирующий выход в сеть Интернет с персонального компьютера на основании политик, которые устанавливает сам пользователь;

1. **Правила и принципы защиты от вредоносного ПО.**

Для защиты компьютера от заражения вирусами, прежде всего, необходимо установить антивирусное программное обеспечение. Сегодня используется несколько методик обнаружения и защиты от вирусов:

- сканирование; Самая простая методика поиска вирусов заключается в том, что антивирусная программа последовательно просматривает проверяемые файлы в поиске сигнатур известных вирусов. Под сигнатурой понимается уникальная последовательность байт, принадлежащих вирусу, и не встречающаяся в других программах. Антивирусные программы-сканеры способны найти только уже известные и изученные вирусы, для которых была определена сигнатура.

- использование антивирусных мониторов; Целый класс антивирусных программ, которые постоянно находятся в памяти компьютера, и отслеживают все подозрительные действия, выполняемые другими программами. Монитор автоматически проверяет все запускаемые программы, создаваемые, открываемые и сохраняемые документы, файлы программ и документов, полученные через Интернет или скопированные на жесткий диск с дискеты и компакт диска. Антивирусный монитор сообщит пользователю, если какая-либо программа попытается выполнить потенциально опасное действие.

- обнаружение изменений;

- использование антивирусов, встроенных в BIOS компьютера. В системные платы компьютера тоже встраивают простейшие средства защиты от вирусов. Эти средства позволяют контролировать все обращения к главной загрузочной записи жестких дисков, а также к загрузочным секторам дисков и дискет. Если какая-либо программа попытается изменить содержимое загрузочных секторов, срабатывает защита и пользователь получает соответствующее предупреждение.

Кроме того, практически все антивирусные программы обеспечивают автоматическое восстановление зараженных программ и загрузочных секторов, если это возможно.

Для того, чтобы антивирусные программы эффективно выполняли свои функции, необходимо строго соблюдать рекомендации по их применению, описанные в документации. Особое внимание следует обратить на необходимость регулярного обновления вирусных баз данных. Современные антивирусы умеют загружать файлы обновлений через Интернет или по локальной сети.

Одними из самых популярных антивирусов являются антивирус Касперского, доктор WEB.

Для того, чтобы сформулировать основные принципы антивирусной политики безопасности необходимо вспомнить следующие основные моменты, относящиеся к вирусной атаке:

1. Вирусная атака состоит из двух фаз – фаза заражения и фаза распространения (и, возможно, выполнения деструктивных действий).
2. Современные вирусы часто распространяются не только с помощью исполняемых файлов, но и с помощью файлов-документов популярных программ.
3. Современные вирус при атаке часто используют возможности сети Intenet.

Для предотвращения вирусных атак рекомендуется выполнять следующие действия:

- соответствующим образом сконфигурировать антивирусное программное обеспечение.

Сканирование в режиме реального времени, в фоновом и аналоговом режиме должно быть разрешено.

При старте системы должны сканироваться память, загрузочный сектор и системные файлы.

Своевременно обновлять вирусные БД.

Желательно сканировать все типы файлов или как минимум \*.com, \*.exe.

- использовать только лицензионное программное обеспечение. Программное обеспечение, полученное из неизвестного источника, может быть троянским или зараженным вирусом.

-ограничить набор программ, которые пользователь способен установить в системе. Особо следует обратить внимание на различные сервисы интернет и, в первую очередь, на программы передачи сообщений, такие как IRC, ICQ. Данные программы могут передавать файлы и служить источником заражения системы.

- кроме того, желательно устранить известные уязвимости в ПО. Известные уязвимости обычно публикуются в списках рассылки интернет, а так на специальных сайтах.

-контролировать использование внешних носителей информации. В идеале вся информация на них должна быть проверена на наличие вирусов до того, как к ней будет осуществляться доступ со стороны пользователей ПК.

-для защиты от проникновения вирусов через сообщения электронной почты нужно:

-никогда не открывать сразу почтовые вложения в пришедшем почтовом сообщении;

- создать «карантинный» катало – сохранять почтовые вложения в определенном «карантинном» каталоге;

-если отправитель сообщения неизвестен, то сообщение с вложением может быть даже удалено.

-перед открытием вложения всегда проверить его с помощью антивирусного ПО.

-устранить возможные уязвимости в клиентском почтовом ПО.

**28. Операционные системы. Понятие и основные функции ОС. Классификация.**

[Операционная система](http://ru.wikipedia.org/wiki/%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0) — комплекс [программ](http://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0), обеспечивающий управление аппаратными средствами [компьютера](http://ru.wikipedia.org/wiki/%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80), организующий работу с [файлами](http://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB) и выполнение [прикладных программ](http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B8%D0%BA%D0%BB%D0%B0%D0%B4%D0%BD%D0%BE%D0%B5_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5), осуществляющий ввод и вывод [данных](http://ru.wikipedia.org/wiki/%D0%94%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5).

Общими словами, операционная система — это первый и основной набор программ, загружающийся в компьютер. Помимо вышеуказанных функций ОС может осуществлять и другие, например предоставление общего пользовательского [интерфейса](http://ru.wikipedia.org/wiki/%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D1%84%D0%B5%D0%B9%D1%81) и т.п.

Сегодня наиболее известными операционными системами являются ОС семейства [Microsoft](http://ru.wikipedia.org/wiki/Microsoft) [Windows](http://ru.wikipedia.org/wiki/Windows) и [UNIX](http://ru.wikipedia.org/wiki/UNIX)-подобные системы.

## Функции

Интерфейсные функции:

* Управление аппаратными средствами, устройствами ввода- вывода
* Файловая система
* Поддержка многозадачности (разделение использования памяти, времени выполнения)
* Ограничение доступа, многопользовательский режим работы (если взять к примеру ДОС, то он не может быть многопользовательским)
* Сеть (взять спектрум в пример...)

Внутренние функции:

* Обработка прерываний
* Виртуальная память
* "Планировщик" задач
* Буферы ввода- вывода
* Обслуживание драйверов устройств
* Операционные системы различаются особенностями реализации алгоритмов управления ресурсами компьютера, областями использования.  
  Так, в зависимости от алгоритма управления процессором, операционные системы делятся на:
*  Однозадачные и многозадачные
*  Однопользовательские и многопользовательские
*  Однопроцессорные и многопроцессорные системы
*  Локальные и сетевые.
* По числу одновременно выполняемых задач операционные системы делятся на два класса:
*  Однозадачные (MS DOS)
*  Многозадачные (OS/2, Unix, Windows)
* В однозадачных системах используются средства управления периферийными устройствами, средства управления файлами, средства общения с пользователями. Многозадачные ОС используют все средства, которые характерны для однозадачных,  и, кроме того, управляют разделением совместно используемых ресурсов: процессор, ОЗУ, файлы и внешние устройства.
* В зависимости от областей использования многозадачные ОС подразделяются на три типа:
*  Системы пакетной обработки (ОС ЕС)
*  Системы с разделением времени (Unix, Linux, Windows)
*  Системы реального времени (RT11)
* Системы пакетной обработки предназначены для решения задач, которые не требуют быстрого получения результатов. Главной целью ОС пакетной обработки является максимальная пропускная способность или решение максимального числа задач в единицу времени.  
    
  Эти системы  обеспечивают высокую производительность при обработке больших объемов информации, но снижают эффективность работы пользователя в интерактивном режиме.   
  В системах с разделением времени для выполнения каждой задачи выделяется небольшой промежуток времени, и ни одна задача не занимает процессор надолго. Если этот промежуток времени выбран минимальным, то создается видимость одновременного выполнения нескольких задач. Эти системы обладают меньшей пропускной способностью, но обеспечивают высокую эффективность работы пользователя в интерактивном режиме.   
  Системы реального времени применяются  для управления технологическим процессом или техническим объектом, например, летательным объектом, станком и т.д.  
  По числу одновременно работающих пользователей на ЭВМ ОС разделяются на однопользовательские (MS DOS) и многопользовательские (Unix, Linux, Windows 95 - XP)  
  В многопользовательских ОС каждый пользователь настраивает для себя интерфейс пользователя, т.е. может создать собственные наборы ярлыков, группы программ, задать индивидуальную цветовую схему, переместить в удобное место панель задач и добавить в меню Пуск новые пункты.  
  В многопользовательских ОС существуют средства защиты информации каждого пользователя от несанкционированного доступа других пользователей.  
  Многопроцессорные и однопроцессорные операционные системы. Одним из важных свойств ОС является наличие в ней средств поддержки многопроцессорной обработки  данных. Такие средства существуют в OS/2, Net Ware, Widows NT.По способу организации вычислительного процесса эти ОС могут быть разделены на асимметричные и симметричные.  
  Одним из важнейших признаков классификации ЭВМ является разделение их на локальные и сетевые. Локальные ОС применяются на автономных ПК или ПК, которые используются в компьютерных сетях в качестве клиента.  
  В состав локальных ОС входит клиентская часть ПО для доступа к удаленным ресурсам и услугам. Сетевые ОС предназначены для управления ресурсами ПК включенных в сеть с целью совместного использования ресурсов. Они представляют мощные средства разграничения доступа к информации, ее целостности и другие возможности использования сетевых ресурсов.

**29. Классификация сетей. Структура и принципы работы локальных и глобальных сетей.**

**Компьютерная сеть** (КС) являет собой систему распределенной обработки информации, которая составляет как минимум из двух компьютеров, взаимодействующих между собой с помощью специальных средств связи. Или другими словами сеть являет собой совокупность соединенных друг с другом ПК и других вычислительных устройств, таких как принтеры, факсимильные аппараты и модемы. Сеть дает возможность отдельным сотрудникам организации взаимодействовать друг с другом и обращаться к совместно используемым ресурсам; позволяет им получать доступ к данным, что сохраняется на персональных компьютерах в удаленных офисах, и устанавливать связь с поставщиками.

Для классификации компьютерных сетей используются разные признаки, выбор которых заключается в том, чтобы выделить из существующего многообразия такие, которые позволили бы обеспечить данной классификационной схеме такие обязательные качества:  
-  возможность классификации всех, как существующих, так и перспективных, КС;  
-  дифференциацию существенно разных сетей;  
-  однозначность классификации любой компьютерной сети;  
- наглядность, простоту и практическую целесообразность классификационной схемы.  
Определенное несоответствие этих требований делает задание выбору рациональной схемы классификации КС достаточно сложной, такой, которая не нашла до этого времени однозначного решения. В основном КС классифицируют за признаками структурной и функциональной организации.

По назначению КС распределяются на:

1. вычислительные;  
2. информационные;  
3. смешанные (информационно-вычислительные).

Вычислительные сети предназначены главным образом для решения заданий пользователей с обменом данными между их абонентами. Информационные сети ориентированы в основном на предоставление информационных услуг пользователям. Смешанные сети совмещают функции первых двух.

По типа компьютеров, которые входят в состав КС, различают:

1. однородные компьютерные сети, которые состоят из программно общих ЭВМ;  
2.  неоднородные, в состав которых входят программно-несовместительные компьютеры.

Особенное значение занимает классификация **по территориальному признаку**, то есть по величине территории, что покрывает сеть. И для этого есть весомые причины, потому что отличия технологий локальных и глобальных сетей очень значительные, невзирая на их постоянное сближение.   
Классифицируя сети по территориальному признаку, различают:

1. локальные (LocalAreaNetworks– LAN) сети;   
2. глобальные (WideAreaNetworks– WAN) сети;   
3. городские (MetropolitanAreaNetworks– MAN) сети.

**LAN**– сосредоточены на территории не больше 1–2 км; построенные с использованием дорогих высококачественных линий связи, которые позволяют, применяя простые методы передачи данных, достигать высоких скоростей обмена данными порядка 100 Мбит/с, предоставленные услуги отличаются широкой разнообразностью и обычно предусматривают реализацию в режиме on-line.   
**WAN**– совмещают компьютеры, рассредоточенные на расстоянии сотен и тысяч километров. Часто используются уже существующие не очень качественные линии связи. Больше низкие, чем в локальных сетях, скорости передачи данных (десятки килобит в секунду) ограничивают набор предоставленных услуг передачей файлов, преимущественно не в оперативном, а в фоновом режиме, с использованием электронной почты. Для стойкой передачи дискретных данных применяются более сложные методы и оборудование, чем в локальных сетях.   
**MAN**– занимают промежуточное положение между локальными и глобальными сетями. При достаточно больших расстояниях между узлами (десятки километров) они имеют качественные линии связи и высоких скоростей обмена, иногда даже больше высокими, чем в классических локальных сетях. Как и в случае локальных сетей, при построении MANуже существующие линии связи не используются, а прокладываются заново.   
Также дополнительно выделяют:  
4. кампусные сети (Campus Area Network – CAN), которые совмещают значительно удаленные друг от друга абонентские системы или локальные сети, но еще не требуют отдаленных коммуникаций через телефонные линии и модемы;   
5. широкомасштабные сети (WideAreaNetwork – WAN), которые используют отдаленные мосты и маршрутизаторы с возможно невысокими скоростями передачи данных.

Отличительные **признаки локальной сети**:

1. высокая скорость передачи, большая пропускная способность;   
2. низкий уровень ошибок передачи (или, что то же, высококачественные каналы связи). Допустимая вероятность ошибок передачи данных должна быть порядку 10-7 – 10-8;   
3. эффективный, быстродействующий механизм управления обменом;   
4. ограничено, точно определенное число компьютеров, которые подключаются к сети.

Глобальные сети отличаются от локальных тем, которые рассчитаны на неограниченное число абонентов и используют, как правило, не слишком качественные каналы связи и сравнительно низкую скорость передачи, а механизм управления обменом, у них в принципе не может быть гарантировано скорым. В глобальных сетях намного более важное не качество связи, а сам факт ее существования.  
Правда, в настоящий момент уже нельзя провести четкий и однозначный предел между локальными и глобальными сетями. Большинство локальных сетей имеют выход в глобальную сеть, но характер переданной информации, принципы организации обмена, режимы доступа, к ресурсам внутри локальной сети, как правило, сильно отличаются от тех, что принято в глобальной сети. И хотя все компьютеры локальной сети в данном случае включены также и в глобальную сеть, специфику локальной сети это не отменяет. Возможность выхода в глобальную сеть остается всего лишь одним из ресурсов, поделенные пользователями локальной сети.  
Следующей не менее распространенной классификацией есть классификация КС по типа топологии.

1. **Понятие Интернет и протоколов.**

Интернет – всемирная система объединенных компьютерных сетей, построенная на использовании протокола IP и маршрутизации пакетов данных. Часто упоминается как «Всемирная сеть» и «Глобальная сеть». К середине 2008 года число пользователей, регулярно использующих Интернет, составило около 1.5 млрд человек (около четверти населения Земли).

История. После запуска Советским Союзом искусственного спутника Земли в 1957 году Министерство обороны США посчитало, что на случай войны Америке нужна надежная система передачи информации. Агентство передовых оборонных исследовательских проектов США предложили для этого разработать компьютерную сеть. Разработка такой сети была поручена Калифорнийскому университету в Лос-Анджелесе, Стэндфордскому исследовательскому центру, Университету штата Юта и Университету штата Калифорния в Санта-Барбаре. Компьютерная сеть была названа ARPANET (Advanced Research Projects Agency Network - Новейшая Сеть Агентства Научно-исследовательских работ), и в 1969 году в рамках проекта сеть объединила четыре указанных научных учреждения. Все работы финансировались Министерством обороны США. Затем сеть ARPANET начала активно расти и развиваться, ее начали использовать ученые из разных областей науки.

29 октября 1969 года между двумя первыми узлами сети ARPANET, находящимся на расстоянии в 640 км – в Калифорнийском университете Лос-Анджелеса и в Стэндфордском исследовательском институте провели сеанс связи. Это дату можно считать днем рождения Интернета.

К 1971 году была разработана первая программа для отправки электронной почты по сети. Эта программа сразу стала очень популярна. В 1973 году к сети были подключены через трансатлантический телефонный кабель первые иностранные организации из Великобритании и Норвегии, сеть стала международной.

В 1970-х годах сеть в основном использовалась для пересылки электронной почты, тогда же появились первые списки почтовой рассылки, новостные группы и доски объявлений. Однако в то время сеть еще не могла легко взаимодействовать с другими сетями, построенными на других технических стандартах. К концу 1970-х годов начали бурно развиваться протоколы передачи данных, которые были стандартизированы в 1982-1983 годах. 1 января 1983 года есть ARPANET перешла с протокола NCP на TCP/IP, который успешно применяется до сих пор для объединения сетей. Именно в 1983 году термин «Интернет» закрепился за сетью ARPANET.

В 1984 году была разработана система доменных имен (Domain Name System, DNS). В 1988 году был разработан протокол Internet Relay Chat (IRC), благодаря чему в Интернете стало возможно общение в реальном времени. В 1989 году в Европе родилась концепция Всемирной паутины. В течение двух лет был разработан протокол HTTP, язык HTML. В 1990 было зафиксировано первое подключение к Интернету по телефонной линии.

В настоящее время подключиться к Интернет можно через спутники связи, радио-каналы, кабельное телевидение, телефон, сотовую связь, специальные оптико-волоконные линии или электропровода.

Интернет состоит из многих тысяч корпоративных, научных, правительственных и домашних компьютерных сетей. Объединение сетей разной архитектуры и топологии стало возможно благодаря протоколу IP (Internet Protocol) и принципу маршрутизации пакетов данных.

Протокол в данном случае – это, образно говоря, «язык», используемый компьютерами для обмена данными при работе в сети. Чтобы различные компьютеры сети могли взаимодействовать, они должны «разговаривать» на одном «языке», то есть использовать один и тот же протокол. Проще говоря, протокол – это правила передачи данных между узлами компьютерной сети. Систему протоколов Интернет называют «стеком протоколов TCP/IP»

Пример протокола, еще не стандартизированного, но уже очень популярного в Интернет:

BitTorrent. Этот протокол нужен для обмена файлами.

Стек протоколов TCP/IP включает в себя протоколы четырех уровней:

1. Прикладного (application)
2. Транспортного (transport)
3. Сетевого (internet)
4. Уровня доступа к среде (network access).

**31. Именование в компьютерных сетях и основные технологии**

Когда при деловом общении представители двух фирм обмениваются визитками, то в них (визитках) обязательно будут указаны адрес электронной почты и имя корпоративного Web-узла компании. При этом можно также услышать, как собеседники обмениваются "интернет-адресами" ("электронными адресами") компаний. Во всех выше перечисленных случаях так или иначе речь идет об использовании доменных имен.

В адресе электронной почты формально доменным именем можно считать то, что написано после символа коммерческого ат - "@". Например, в [user@corp.ru](mailto:user@corp.ru) доменное имя почтового узла - corp.ru.

Имя Web-узла - это доменное имя этого узла. Например, Web-узел компании Microsoft имеет доменное имя Microsoft.com.

В большинстве случаев при поиске информации в Сети мы перебираем доменные имена или следуем по ссылкам, в нотации которых опять же используются доменные имена.

Довольно часто наряду со словосочетанием "интернет-адрес" употребляют "доменный адрес". Вообще говоря, ни того, ни другого понятий в сетях TCP/IP не существует. Есть числовая адресация, которая опирается на IP-адреса, (группа из 4-ех чисел, разделенных символом ".") и Internet-сервис службы доменных имен (Domain Name System - DNS).

Числовая адресация удобна для компьютерной обработки таблиц маршрутов, но совершенно (здесь мы несколько утрируем) не приемлема для использования ее человеком. Запомнить наборы цифр гораздо труднее, чем мнемонические осмысленные имена.

Тем не менее, установка соединений для обмена информацией в Интернет осуществляется по IP-адресам. Символьные имена системы доменных имен - суть сервис, который помогает найти необходимые для установки соединения IP-адреса узлов сети.

Тем не менее, для многих пользователей именно доменное имя выступает в роли адреса информационного ресурса. В практике администрирования локальных сетей нередки ситуации, когда пользователи жалуются администратору сети на недоступность того или иного сайта или долгую загрузку страниц. Причина может крыться не в том, что сегмент сети потерял связь с остальной сетью, а в плохой работе DNS - нет IP-адреса, нет и соединения.

DNS существовала не с момента рождения TCP/IP сетей. Поначалу для облегчения взаимодействия с удаленными информационными ресурсами в Интернет стали использовать таблицы соответствия числовых адресов именам машин.

Авторство создания этих таблиц принадлежит доктору Постелю (Dr. Jon Postel - автор многих RFC - Request For Comments). Именно он первым поддерживал файл hosts.txt, который можно было получить по FTP.

Современные операционные системы тоже поддерживают таблицы соответствия IP-адреса и имени машины (точнее хоста) - это файлы с именем hosts. Если речь идет о системе типа Unix, то этот файл расположен в директории /etc и имеет следующий вид:

127.0.0.1 localhost

144.206.130.137 polyn Polyn polyn.net.kiae.su polyn.kiae.su

144.206.160.32 polyn Polyn polyn.net.kiae.su polyn.kiae.su

144.206.160.40 apollo Apollo www.polyn.kiae.su

Пользователь для обращения к машине может использовать как IP-адрес машины, так и ее имя или синоним (alias). Как видно из примера, синонимов может быть много, и, кроме того, для разных IP-адресов может быть указано одно и то же имя.

Напомним еще раз, что по самому мнемоническому имени никакого доступа к ресурсу получить нельзя. Процедура использования имени заключается в следующем:

* сначала по имени в файле hosts находят IP-адрес,
* затем по IP-адресу устанавливают соединение с удаленным информационным ресурсом.

Обращения, приведенные ниже аналогичны по своему результату - инициированию сеанса telnet с машиной Apollo:

telnet 144.206.160.40

или

telnet Apollo

или

telnet www.polyn.kiae.su

В локальных сетях файлы hosts используются достаточно успешно до сих пор. Практически все операционные системы от различных клонов Unix до Windows последних версий поддерживают эту систему соответствия IP-адресов именам хостов.

Однако такой способ использования символьных имен был хорош до тех пор, пока Интернет был маленьким. По мере роста Сети стало затруднительным держать большие согласованные списки имен на каждом компьютере. Главной проблемой стал даже не размер списка соответствий, сколько синхронизация его содержимого. Для того, что бы решить эту проблему, была придумана DNS.

DNS была описана Полом Мокапетрисом (Paul Mockapetris ) в 1984. Это два документа: RFC-882 и RFC-883 (Позже эти документы были заменены на RFC-1034 и RFC-1035). Пол Мокапетрис написал и реализацию DNS - программу JEEVES для ОС Tops-20. Именно на нее в RFC-1031 предлагается перейти администраторам машин с ОС Tops-20 сети MILNET. Не будем подробно излагать содержание RFC-1034 и RFC-1035. Ограничимся только основными понятиями.

Роль имени (доменного имени) в процессе установки соединения осталось прежним. Это значит, что главное, для чего оно нужно, - получение IP адреса. Соответственно этой роли, любая реализация DNS является прикладным процессом, который работает над стеком протоколов межсетевого обмена TCP/IP. Таким образом, базовым элементом адресации в сетях TCP/IP остался IP-адрес, а доменное именование (система доменных имен) выполняет роль вспомогательного сервиса.

Система доменных имен строится по иерархическому принципу. Точнее по принципу вложенных друг в друга множеств. Корень системы называется "root" (дословно переводится как "корень") и никак не обозначается (имеет пустое имя согласно RFC-1034).

Часто пишут, что обозначение корневого домена - символ ".", но это не так, точка - разделитель компонентов доменного имени, а т.к. у корневого домена нет обозначения, то полное доменное имя кончается точкой. Тем не менее символ "." достаточно прочно закрепился в литературе в качестве обозначения корневого домена. От части это вызвано тем, что в файлах конфигурации серверов DNS именно этот символ указывается в поле имени домена (поле NAME согласно RFC-1035) в записях описания ресурсов, когда речь идет о корневом домене.

Корень - это все множество хостов Интернет. Данное множество подразделяется на домены первого или верхнего уровня (top-level или TLD). Домен ru, например, соответствует множеству хостов российской части Интернет. Домены верхнего уровня дробятся на более мелкие домены, например, корпоративные.

В 80-е годы были определены первые домены первого уровня (top-level): gov, mil, edu, com, net. Позднее, когда сеть перешагнула национальные границы США появились национальные домены типа: uk, jp, au, ch, и т.п. Для СССР также был выделен домен su. После 1991 года, когда республики Союза стали суверенными, многие из них получили свои собственные домены: ua, ru, la, li, и т.п.

Однако Интернет не СССР, и просто так выбросить домен su из системы доменных имен нельзя. На основе доменных имен строятся адреса электронной почты и доступ ко многим другим информационным ресурсам Интернет. Поэтому гораздо проще оказалось ввести новый домен к существующему, чем заменить его.

Если быть более точным, то новых имен с расширением su в настоящее время ни один провайдер не выделяет (делегирует). Однако у многих существует желание возобновить процесс делегирования доменов в зоне SU.

Со списком доменов первого уровня (top-level) и их типами можно ознакомиться, например, в материале "[Общая информация о системе доменных имен](http://info.nic.ru/st/8/out_74.shtml)".

Как уже было сказано, вслед за доменами первого уровня(top-level) следуют домены, определяющие либо регионы (msk), либо организации (kiae). В настоящее время практически любая организация может получить свой собственный домен второго уровня. Для этого надо направить заявку провайдеру и получить уведомление о регистрации (см. "Как получить домен").

Далее идут следующие уровни иерархии, которые могут быть закреплены либо за небольшими организациями, либо за подразделениями больших организаций.

**32. Основные сервисы Интернет. Доменная система имен.**

Постоянное развитие информационных технологий приводит к появлению разнообразных информационных ресурсов, отличающихся друг от друга формами представления и методами обработки составляющих их информационных объектов. Поэтому в настоящее время в Интернет существует достаточно большое количество сервисов, обеспечивающих работу со всем спектром ресурсов. Наиболее известными среди них являются:

* электронная почта (E-mail), обеспечивающая возможность обмена сообщениями одного человека с одним или несколькими абонентами;
* телеконференции, или группы новостей (Usenet), обеспечивающие возможность коллективного обмена сообщениями;
* сервис FTP – система файловых архивов, обеспечивающая хранение и пересылку файлов различных типов;
* сервис Telnet, предназначенный для управления удаленными компьютерами в терминальном режиме;
* World Wide Web (WWW, W3) – гипертекстовая (гипермедиа) система, предназначенная для интеграции различных сетевых ресурсов в единое информационное пространство;
* сервис DNS, или система доменных имен, обеспечивающий возможность использования для адресации узлов сети мнемонических имен вместо числовых адресов;
* сервис IRC, предназначенный для поддержки текстового общения в реальном времени (chat);

Перечисленные выше сервисы относятся к стандартным. Это означает, что принципы построения клиентского и серверного программного обеспечения, а также протоколы взаимодействия сформулированы в виде международных стандартов. Следовательно, разработчики программного обеспечения при практической реализации обязаны выдерживать общие технические требования.   
Наряду со стандартными сервисами существуют и нестандартные, представляющие собой оригинальную разработку той или иной компании. В качестве примера можно привести различные системы типа Instant Messenger (своеобразные Интернет-пейджеры – ICQ, AOl, Demos on-line и т.п.), системы Интернет-телефонии, трансляции радио и видео и т.д. Важной особенностью таких систем является отсутствие международных стандартов, что может привести к возникновению технических конфликтов с другими подобными сервисами.

DNS(Domain Name System) - это распределенная база данных, которая содержит информацию о компьютерах, включенных в сеть Internet. Характер данных зависит от конкретной машины, но чаще всего информация включает имя машины, IP-адрес и данные для маршрутизации почты. Для удобства,большинство компьютеров имеют имена. Доменная система имен выполняет несколько задач, но основная ее работа – преобразование им|н компьютеров а IP-адреса и наоборот. Пространство имен DNS имеет вид дерева доменов, с полномочиями, возрастающими по мере приближения к корню дерева. Корень дерева имеет имя "."; под ним находятся домены верхнего уровня (корневые домены). По историческим причинам существует два вида доменов верхнего уровня. В США домены верхнего уровня отражают организационную структуру, и как правило имеют трехбуквенные имена:

.gov - государственные учереждения,

.mil - военные учереждения,

.com - коммерческие организации,

.net - поставщики сетевых услуг,

.org - безприбыльные организации,

.edu - учебные заведения;

Для доменов вне США, в соответствии с териториальным расположением используются двухбуквенные коды страм ISO. Например:

www.spm.ru - в России

www.berlin.de - а Германии

www.hotsex.nl - в Нидерландах

и т.д.

**33. Техническое и программное обеспечение вычислительных систем**

***Техническое обеспечение*** - это комплекс технических средств, предназначенных для работы информационной системы, а также соответствующая документация на эти средства и технологические процессы.   
Эволюция технического обеспечения, которое включает в себя аппаратные средства, средства коммуникации, программное обеспечение, проходит неравномерно, скачкообразно. Развитие компьютерной техники пока происходит в геометрической прогрессии. Каждые четыре года происходит удвоение производительности компьютеров.   
Классификация компьютерных технологий по типу пользовательского интерфейса (как взаимодействует пользователь технологии с компьютером) - пакетные, диалоговые, сетевые. В первом случае пользователь получает только результаты работы технологии, в остальных он взаимодействует с ней на индивидуальном компьютере или компьютере, подключенном к сети ЭВМ.   
Современные технические средства обеспечения управления информационными ресурсами по своему составу и функциональным возможностям весьма разнообразны. Средства вычислительной техники, средства коммуникационной техники, средства организационной техники.   
Компьютерная техника предназначена, в основном, для реализации комплексных технологий обработки и хранения информации и является базой интеграции всех современных технических средств обеспечения управления информационными ресурсами.   
Коммуникационная техника предназначена, в основном, для реализации технологий передачи информации и предполагает как автономное функционирование, так и функционирование в комплексе со средствами компьютерной техники.   
Организационная техника предназначена для реализации технологий хранения, представления и использования информации, а также для выполнения различных вспомогательных операций в рамках тех или иных технологий информационной поддержки управленческой деятельности.   
Программные средства автоматизации офиса делятся на системные и прикладные программы.   
К системным программам относятся: тестовые и диагностические программы, антивирусные программы, операционные системы, командно-файловые процессоры.   
Тестовые и диагностические программы предназначены для проверки работоспособности отдельных узлов компьютера и компонентов программно-файловых систем и, возможно, для устранения выявленных неисправностей.   
Антивирусные программы предназначены для выявления и, возможно, устранения вирусных программ, нарушающих нормальную работу вычислительной системы.   
Операционные системы являются основными системными программными комплексами, выполняющими следующие основные функции: тестирование работоспособности вычислительной системы и ее настройку при первоначальном включении; обеспечение синхронного и эффективного взаимодействия всех аппаратных и программных компонентов вычислительной системы в процессе ее функционирования; обеспечение эффективного взаимодействия пользователя с вычислительной системой.

1. **Классификация файловых систем. Файловые системы FAT, NTFS. Технические средства персонального компьютера (ПК)**

Файловая система – порядок, определяющий способ организации, хранения и именования данных на носителях информации в компьютерах, а также в другом электронном оборудовании: цифровых фотоаппаратах, мобильных телефонах и т.п. Файловая система определяет формат содержимого и физического хранения информации, которую принято группировать в виде файлов. Конкретная файловая система определяет размер имени файла (папки), максимальный возможный размер файла и раздела, набор атрибутов файла. Некоторые файловые системы предоставляют сервисные возможности, например, разграничение доступа или шифрование файлов.

Когда прикладная программа обращается к файлу, она не имеет никакого представления о том. Каким образом расположена информация в конкретном файле, так же, как и на каком физическом носителе (СД, жестком диске, флеш-памяти и др) он записан. Все, что знает программа – это имя файла, его размер и атрибуты. Эти данные она получает от драйвера файловой системы. Именно файловая система устанавливает, где и как будет записан файл на физическом носителе.

С точки зрения операционной системы, весь диск представляет собой набор кластером. Драйверы файловой системы организуют кластеры в файлы и каталоги (реально являющиеся файлами, содержащими список файлов в этом каталоге). Эти же драйверы отслеживают, какие из кластеров в настоящее время используются, какие свободны, какие помечены как неисправные.

**По предназначению файловые системы можно классифицировать:**

**-**для носителей с произвольным доступом (например, жесткий диск): FAT32, ext2 и др. Поскольку доступ к дискам в разы медленнее, чем доступ к оперативной памяти, для прироста производительности во многих файловых системах применяется асинхронная запись изменений на диск.

- для носителей с последовательным доступом (например, магнитные ленты): QIC

- для оптических носителей – CD и DVD: ISO9660, HFS, UDF

- виртуальные файловые системы: AEFS

- сетевые файловые системы: NFS, CIFS

-для флэш-памяти: ExtremeFFS, exFAT

Основные функции любой файловой системы нацелены на решение следующих задач:

1. Именование файлов;
2. Программный интерфейс работы с файлами для приложений;
3. Организация устойчивости файловой системы к сбоям питания, ошибкам аппаратных и программных средств;
4. Содержание параметров файла, необходимых для правильного его взаимодействия с другими объектами системы (ядро, приложения и пр.).

В многопользовательских системах появляется еще одна задача: защита файлов одного пользователя от несанкционированного доступа другого пользователя, а также обеспечение совместной работы с файлами, к примеру, при открытии файла одним из пользователей, для других этот же файл временно будет доступен в режиме «только чтение».

**Файловая система fat**

FAT - (с англ.таблица размещения файлов) – этот термин относится к одному из способов организации файловой системы на диске. Эта таблица хранит информацию о файлах на жестком диске в виде последовательности чисел, определяющих, где находится каждая часть каждого файла. С ее помощью операционная система выясняет, какие кластеры занимает нужный файл. FAT – является самой распространенной файловой системой и поддерживается подавляющим большинством операционных систем. Сначала FAT была 12-разрядной и позволяла работать с дискетами и логическими дисками объемом не более 16 Мбайт. В MS-DOS версии 3.0 таблица FAT стала 16-разрадной для поддержки дисков большей емкости, а для дисков объемом до 2 047 Гбайт используется 32-разрядная таблица FAT.

Была разработана Биллом Гейтсом и Марком Макдональдом в 1977 году.

Сейчас существуют три типа файловой системы FAT:

1. FAT12 – поддерживает очень небольшие объемы дисков, поэтому сейчас она применяется только на дискетах.
2. FAT16 – используется на винчестерах и поддерживает диски объемом до 2Гб, поэтому сейчас данная файловая система практически не используется.
3. FAT32 – теоретически поддерживаются диски объемом до 2Гб. Данная файловая система сейчас достаточно популярна, хотя в последние годы многие пользователи Windows XP предпочитают использовать NTFS.

Структура: загрузочный сектор, таблица размещения файлов, корневой каталог, область данных.

**Загрузочный сектор.** В начале раздела диска с файловой системой FAT располагается загрузочный сектор. Он необходим для начальной загрузки компьютера. Так же в нем располагается информация о параметрах данного раздела.

**Таблица размещения файлов.** Вся область данных диска разделена на кластеры – блоки, размер которых задается при форматировании диска. На дискете, например, размер кластера равен 512-ти байтам. А на современных винчестерах с объемом диска более 32Гб размер кластера равен 32Кб. Каждый файл и каталог занимает один или несколько кластеров. Таким образом, образуются цепочки кластеров.

В таблице размещения файлов каждый кластер помечается специальным образом. Размер метки в битах для каждого кластера указывается в названии файловой системы. Т.е. для файловой системы FAT16 размер метки будет равен 16-ти байтам, для FAT32 – 32 и т.д.

Всего существует три типа меток для кластеров:

-свободный кластер – кластер, в который будут записываться новые файлы и каталоги.

-занятый кластер – в метке указывается следующий кластер в цепочке. Если цепочка кластеров заканчивается, то кластер помечается особой меткой.

-BAD-блок – кластер с ошибками доступа. Помечается при форматировании диска, чтобы исключить в последующем доступ к нему.

Повреждение таблицы размещения файлов полностью уничтожает структуру файловой системы, поэтому на диске всегда хранится две копии таблицы.

**Корневой каталог.** Область диска, в котором располагается информация о корневом каталоге. Размер ее ограничен, поэтому в корневом каталоге диска может находиться не более 512-ти файлов и подкаталогов.

**Область данных.** Оставшаяся часть раздела, на которой размещается содержимое файлов и каталогов.

Сейчас основным конкурентом файловой системы FAT32 является NTFS. Файловая система NTFS получила популярность с распространением ОС Windows XP.

Основным преимуществом файловой системы FAT32 является ее простота и совместимость со старыми ОС. Для этой файловой системы существует большое количество подробной документации. Существует ограничение на максимальный размер файла – 4 Гб. Сбои в системе часто приводят к повреждениям одного или нескольких файлов. Однако, при серьезных повреждениях, восстановить информацию гораздо проще, чем в случае с NTFS.

Основными преимуществами файловой системы NTFS является ее защищенность от несанкционированного доступа. В этой файловой системе отсутствуют ограничения на размер файлов и каталогов. Так же ее особенность является журналирование – запись всех операций перед их выполнением в специальный журнал. В случае, если во время выполнения операций с файловой системой произойдет сбой (зависание ОС, отключение электричества и т.п.), то она на основе записей в журнале сможет вернуть себя в прежнее состояние. Однако, в случае серьезного сбоя восстановить информацию будет очень сложно, подчас невозможно. Причиной тому является отсутствие официальной документации файловой системы от Майкрософт. Так же недостатком NTFS является несовместимость со старыми версиями ОС (Windows 95, 98).

**NTFS** (от англ. файловая система новой технологии) – стандартная файловая система для ОС Microsoft Windows NT. NTFS имеет встроенные возможности разграничивать доступ к данным для различных пользователей и групп пользователей, а также назначать квоты (ограничения на максимальный объем дискового пространства, занимаемый теми или иными пользователями).

ПК называют сравнительно недорогой универсальный микрокопьютер, рассчитанный на одного пользователя. Компьютер можно собирать из отдельных узлов и деталей, разработанных и изготовленных независимыми фирмами-изгтовителями.

Компьютер легко расширяется и модернизируется за счет наличия внутренних расширительных гнезд, в которые пользователь может вставлять разнообразные устройства, удовлетворяющие заданному стандарту, и тем самым устанавливать конфигурацию своей машины в соответствии со своими личными предпочтениями.

Для того, чтобы соединить друг с другом различные устройства компьютера, они должны иметь одинаковый интерфейс.

Каждый из функциональных элементов (память, монитор или другое устройство) связан с шиной определенного типа – адресной, управляющей или шиной данных.

Для согласования интерфейсов периферийные устройства подключаются к шине не напрямую, а через свои контроллеры (адаптеры) и порты примерно по такой схеме: устройство-контроллер или адаптер-порт-шина.

Контроллеры и адаптеры представляют собой наборы электронных цепей, которыми снабжаются устройства компьютера с целью совместимости их интерфейсов. Контроллеры, кроме этого, осуществляют непосредственное управление периферийными устройствами по запросам микропероцессора.

Порты устройства представляют собой некие электронные схемы, содержащие один или несколько регистров ввода-вывода и позволяющие подключать периферийные устройства компьютера к внешним шинам микропроцессора. Портами также называют устройства стандартного интерфейса: последовательный, параллельный и игровой порты.

Последовательный порт обменивается данными с процессором побайтно, а с внешними устройствами – побитно. Параллельный порт получает и посылает данные побайтно.

К последовательному порту обычно подсоединяют медленно действующие или достаточно удаленные устройства, такие, как мышь и модем. К параллельному порту подсоединяют более «быстрые» устройства – принтер и сканер. Через игровой порт подсоединяется джойстик. Клавиатура и монитор подключаются к своим специализированным портам, которые представляют собой просто разъемы.

Основные электронные компоненты, определяющие архитектуру процессора, размещаются на основной плате компьютера, которая называется системной или материнской. А контроллеры и адаптеры дополнительных устройств, либо сами эти устройства, выполняются в виде плат расширения и подключаются к шине с помощью разъемов расширения, называемых также слотами расширения.

Современный персональный компьютер состоит из нескольких основных конструктивных компонент:

-системного блока;

-монитора;

-клавиатуры;

-манипуляторов.

В системном блоке размещаются:

-блок питания;

-накопитель на жестких магнитных дисках;

-накопитель на гибких магнитных дисках;

-системная плата;

-платы расширения;

-накопить CD-ROM и др.

**35. Программные и программно-аппаратные методы и средства защиты информации**

**П**рограммными называются средства защиты данных, функционирующие в составе программного обеспечения. Среди них можно выделить и подробнее рассмотреть следующие:

* средства архивации данных;
* антивирусные программы;
* криптографические средства;
* средства идентификации и аутентификации пользователей;
* средства управления доступом;
* протоколирование и аудит.

**К**ак примеры комбинаций вышеперечисленных мер можно привести:

* защиту баз данных;
* защиту информации при работе в компьютерных сетях.

**Средства архивации информации**

**И**ногда резервные копии информации приходится выполнять при общей ограниченности ресурсов размещения данных, например владельцам персональных компьютеров. В этих случаях используют программную архивацию. Архивация это слияние нескольких файлов и даже каталогов в единый файл — архив, одновременно с сокращением общего объема исходных файлов путем устранения избыточности, но без потерь информации, т. е. с возможностью точного восстановления исходных файлов. Действие большинства средств архивации основано на использовании алгоритмов сжатия, предложенных в 80-х гг. Абрахамом Лемпелем и Якобом Зивом. Наиболее известны и популярны следующие архивные форматы:

* ZIP, ARJ для операционных систем DOS и Windows;
* TAR для операционной системы Unix;
* межплатформный формат JAR (Java ARchive);
* RAR (все время растет популярность этого нового формата, так как разработаны программы позволяющие использовать его в операционных системах DOS, Windows и Unix).

**П**ользователю следует лишь выбрать для себя подходящую программу, обеспечивающую работу с выбранным форматом, путем оценки ее характеристик – быстродействия, степени сжатия, совместимости с большим количеством форматов, удобности интерфейса, выбора операционной системы и т.д.. Список таких программ очень велик – PKZIP, PKUNZIP, ARJ, RAR, WinZip, WinArj, ZipMagic, WinRar и много других. Большинство из этих программ не надо специально покупать, так как они предлагаются как программы условно-бесплатные (Shareware) или свободного распространения (Freeware). Также очень важно установить постоянный график проведения таких работ по архивации данных или выполнять их после большого обновления данных.

**Антивирусные программы**

**Э**то программы разработанные для защиты информации от вирусов. Неискушенные пользователи обычно считают, что компьютерный вирус - это специально написанная небольшая по размерам программа, которая может "приписывать" себя к другим программам (т.е. "заражать" их), а также выполнять нежелательные различные действия на компьютере. Специалисты по компьютерной вирусологии определяют, что ОБЯЗАТЕЛЬНЫМ (НЕОБХОДИМЫМ) СВОЙСТВОМ КОМПЬЮТЕРНОГО ВИРУСА является возможность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению. Следует отметить, что это условие не является достаточным т.е. окончательным. Вот почему точного определения вируса нет до сих пор, и вряд ли оно появится в обозримом будущем. Следовательно, нет точно определенного закона, по которому “хорошие” файлы можно отличить от “вирусов”. Более того, иногда даже для конкретного файла довольно сложно определить, является он вирусом или нет.

Программно-аппаратные методы:

**USB-ключ**

 Принцип работы USB-ключа заключается в следующем: после инсталляции специальной программы компьютер не включится до тех пор, пока USB-ключ не будет вставлен в специальный порт. Порой сам ключ выступает как носитель информации небольшого объема, в памяти которого, кстати, можно хранить свой пароль.

 Использование USB-ключа дает пользователю ряд преимуществ.

 Во-первых, используется **более сложный пароль**, который автоматически передается в систему.

 Во-вторых, больше **не надо отвлекаться на пароли**, если нужно на некоторое время отойти от компьютера. Вытащите ключ, и ПК заблокируется автоматически. По возвращении просто вставьте ключ на место.

 В-третьих, можно использовать **один USB-ключ для доступа** к рабочему и домашнему компьютеру.

 И, наконец, один из самых важных моментов – ключ практически **невозможно подделать**.

**Как защитить ноутбук**

**Замок Кенсингтона**

 Одно из самых простых и распространенных устройств, подходящее рядовому пользователю по качеству и цене. Если вы работаете с ноутбуком в офисе или на выездной презентации, но нужно срочно куда-либо отойти, замок Кенсингтона (Kensington Lock) - идеальный вариант защиты ноутбука от хищения. Как он действует? При помощи маленького металлического троса компьютер крепится к тяжелому стационарному предмету. Унести компьютер просто невозможно, единственный минус этого способа защиты - неудобство при переноске ноутбука, например, по комнате. Каждый раз трос нужно отсоединять.

**Сигнализация**

 Еще один вид защиты – сигнализация и все ее разновидности. Способов защиты на основе сигнализации множество, как и вариантов условий ее срабатывания. Например, она может сработать, если ноутбук куда-либо переместился или его удалили из определенной зоны.

**Сканер отпечатков пальцев**

 В последнее время большую популярность приобрели биометрические сенсоры, или считыватели отпечатков пальцев. Это отличный способ защиты: отпечаток почти невозможно подделать или потерять, к тому же он всегда с вами.

 Но, как и у прочих способов защиты, у биометрических сенсоров есть свои недостатки. Например, сенсор может просто не распознать отпечаток. Чтобы этого не произошло, можно снизить порог чувствительности устройства. Но, к сожалению, это приводит к снижению безопасности.

 Для ноутбуков, не имеющих встроенного сканера отпечатков пальца, можно отдельно приобрести биометрический сканер, выполненный в виде обычной флешки. Помимо повышения безопасности данных, защищенных таким способом, данное решение обладает «побочным» преимуществом – вынув сканер из USB-порта, вы оставите с носом злодея, который за долгие зимние вечера сумел-таки подделать ваш отпечаток пальца.

**36. Понятие, цели и принципы информационной безопасности.**

Под информационной безопасностью понимается защищенность информации и поддерживающей ее инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцами или поддерживающей инфраструктуре.

Действия, которые могут нанести ущерб информационной безопасности организации, можно разделить на несколько категорий:

- действия, осуществляемые авторизованными пользователями. В эту категорию попадают: целенаправленная кража или уничтожение данных на рабочей станции или сервере; повреждение данных пользователей в результате неосторожных действий.

- «электронные методы воздействия, осуществляемые хакерами. Под хакерами понимаются люди, занимающиеся компьютерными преступлениями как профессионально (в том числе в рамках конкурентной борьбы), так и просто из любопытства. К таким методам относятся: несанкционированное проникновение в компьютерные сети; DOS-атаки.

Целью несанкционированного проникновения извне в сеть предприятия может быть нанесение вреда (уничтожение данных), кража конфиденциальной информации и использование ее в незаконных целях, кража средств со счетов и др.

Атака типа DOS (с англ. «отказ в обслуживании) – это внешняя атака на узлы сети предприятия, отвечающие за ее безопасную и эффективную работы (файловые, почтовые сервера). Злоумышленники организуют массированную отправку пакетов данных на эти узлы, чтобы вызвать их перезагрузку и, в итоге, на какое-то время вывести их из строя. Это, как правило, влечет за собой нарушения в бизнес-процессах компании-жертвы, потерю клиентов, ущерб репутации и т.п.

- компьютерные вирусы и др.вредоносные программы. Проникновение вируса на узлы корпоративной сети может привести к нарушению их функционирования, потерям рабочего времени, утрате данных, краже конфиденциальной информации и даже прямым хищениям финансовых средств.

- спам. Электронная почта в последнее время стала главным каналом распространения вредоносных программ; спам отнимает массу времени на просмотр и последующее удаление сообщений, вместе со спамом нередко удаляется важная корреспонденция.

- естественные угрозы. На информационную безопасность компании могут влиять разнообразные внешние факторы: причиной потери данных может стать неправильное хранение, кража компьютеров и носителей, форс-мажорные обстоятельства и др.

Основные цели защиты информации:

- обеспечение физической целостности; Физическая целостность информации в ПК зависит от целостности самой ПК, целостности дисков и дискет, целостности информации на дисках, дискетах и полях оперативной памяти. В широком спектре угроз целостности, информации в ПК следует обратить особое внимание на угрозы, связанные с недостаточно высокой квалификацией большого числа владельцев ПК. В этом плане особо опасной представляется возможность уничтожения или искажения данных на жестком диске (винчестере), на котором могут накапливаться очень большие объемы данных, самим пользователем.

- предупреждение несанкционированного получения информации; Данная цель защиты приобретает особую актуальность в тех случаях, когда хранимая информация содержит тайну того или иного характера (государственную, коммерческую и т.п.).

- предупреждение несанкционированной модификации; Действие вредоносных программ (компьютерных вирусов), которые могут разрушать или уничтожать программы или массивы данных. Данная опасность приобретается актуальность в связи с тем, что среди владельцев ПК общепринятой становится практика обмена дискетами. В получаемой дискете может содержаться вирус.

- предупреждение несанкционированного копирования. Актуальность данной разновидности защиты определяется следующими тремя обстоятельствами: накопленные массивы информации все больше становятся товаром; все более широкое распространение получает торговля компьютерными программами; оптические дисководы с перезаписью создают весьма благоприятные условия для широкомасштабного копирования информации.

На сегодняшний день сформулировано три базовых принципа, которые должна обеспечивать информационная безопасность:

- целостность данных – защита от сбоев, ведущих к потере информации, а также защита от неавторизованного создания и уничтожения данных;

- конфиденциальность информации;

- доступность информации для всех авторизованных пользователей.

**37. Классификация угроз и уязвимостей в информационной безопасности**

Классификация угроз. Угрозами информационной безопасности называются потенциальные источники нежелательных событий, которые могут нанести ущерб ресурсам информационной системы. Все угрозы безопасности, направленные против программных и технических средств информационной системы, в конечном итоге оказывают влияние на безопасность информационных ресурсов и приводят к нарушению основных свойств хранимой и обрабатываемой информации. Как правило, угрозы информационной безопасности различаются по способу их реализации.

Исходя из этого можно выделить следующие основные классы угроз безопасности, направленных против информационных ресурсов:  
• угрозы, реализуемые либо воздействием на программное обеспечение и конфигурационную информацию системы, либо посредством некорректного использования системного и прикладного программного обеспечения;  
• угрозы, связанные с выходом из строя технических средств системы, приводящим к полному или частичному разрушению информации, хранящейся и обрабатываемой в системе;  
• угрозы, обусловленные человеческим фактором и связанные с некорректным использованием сотрудниками программного обеспечения или с воздействием на технические средства, в большей степени зависят от действий и "особенностей" морального поведения сотрудников;  
• угрозы, вызванные перехватом побочных электромагнитных излучений и наводок, возникающих при работе технических средств системы, с использованием специализированных средств технической разведки.

Угрозы с использованием программных средств. Наиболее многочисленный класс угроз конфиденциальности, целостности и доступности информационных ресурсов связан с получением внутренними и внешними нарушителями логического доступа к информации с использованием возможностей, предоставляемых общесистемным и прикладным программным обеспечением. Большинство рассматриваемых в этом классе угроз реализуется путем локальных или удаленных атак на информационные ресурсы системы внутренними и внешними нарушителями. Результатом осуществления этих угроз становится несанкционированный доступ к данным, управляющей информации, хранящейся на рабочем месте администратора системы, конфигурационной информации технических средств, а также к сведениям, передаваемым по каналам связи.

В этом классе выделяются следующие основные угрозы:  
• Угрозы техническим средствам. Угрозы использование сотрудниками чужого идентификатора;  
• использование чужого идентификатора поставщиками услуг;  
• использование чужого идентификатора посторонними;  
• несанкционированный доступ к приложению;  
• внедрение вредоносного программного обеспечения;  
• злоупотребление системными ресурсами;  
• отказ от подтверждения авторства передаваемой информации;  
• ошибки при маршрутизации;  
• использование телекоммуникаций для несанкционированного доступа сотрудниками организации, поставщиком услуг, посторонними лицами;  
• неисправность средств сетевого управления, управляющих или сетевых серверов;  
• сбои системного и сетевого программного обеспечения;  
• сбои прикладного программного обеспечения.

Связь доступности и целостности информации (хранимой, обрабатываемой и передаваемой по каналам связи) связаны с физическими повреждениями и отказами технических средств системы и вспомогательных коммуникаций. Последствия реализации этого класса угроз могут привести к полному или частичному разрушению информации, отказу в обслуживании пользователей и их запросов к системе, невозможности вывода или передачи информации.

В этом классе выделяются следующие основные угрозы:  
• пожар;  
• затопление;  
• природные катаклизмы;  
• неисправности сетевого сервера, накопительного устройства, печатающих устройств, сетевых распределяющих компонентов, сетевых шлюзов, сетевых интерфейсов, электропитания, кондиционеров.

Угрозы, обусловленные человеческим фактором. Угрозы возникают вследствие умышленных или неумышленных действий персонала или посторонних лиц, приводящих к выходу из строя либо нештатной работе программных или технических средств информационной системы.

В этом классе выделяются следующие основные угрозы:  
1. ошибки операторов (ошибки администраторов при конфигурировании системы);  
2. ошибки пользователей при работе с системой;  
3. ошибки при работах с программным обеспечением (ошибки администраторов при проведении профилактических работ);  
4. ошибки при работах с оборудованием (ошибки сотрудников службы технической поддержки при проведении профилактических работ);  
5. кражи со стороны сотрудников.

**38. Меры и основные сервисы обеспечения информационной безопасности**

Одним из наиболее эффективных методов обеспечения информационной безопасности являются организационно-технические методы.  
Что такое организационно-технические методы обеспечения информационной безопасности? Прежде всего, создание и совершенствование системы обеспечения информационной безопасности, разработка, использование и совершенствование СЗИ и методов контроля их эффективности.   
Этот этап тесно связан с правовыми методами защиты информации, такими как лицензирование (деятельности в области защиты информации), сертификация средств защиты информации и применение уже сертифицированных, и аттестация объектов информатизации по требованиям безопасности информации.   
А так же организационно технические методы связаны с экономическими, включающими в себя разработку программ обеспечения информационной безопасности Российской Федерации, определение порядка их финансирования, совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков.  
Защита информации всегда является комплексным мероприятием. В совокупности, организационные и технические мероприятия позволяют предотвратить утечку информации по техническим каналам, предотвратить несанкционированный доступ к защищаемым ресурсам, что в свою очередь обеспечивает целостность и доступность информации при ее обработке, передаче и хранении. Так же техническими мероприятиями могут быть выявлены специальные электронные устройства перехвата информации, установленные в технические средства и защищаемое помещение.  
Меры по охране конфиденциальности информации, составляющей коммерческую тайну (ФЗ 2004 г. № 98-ФЗ)

* определение перечня информации, составляющей коммерческую тайну;
* ограничение доступа к информации, составляющей коммерческую тайну,
* путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
* учёт лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;
* регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
* нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа "Коммерческая тайна" с указанием обладателя этой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Если говорить об экономической стороне защиты информации, всегда важно одно правило – стоимость системы защиты информации не должна превышать стоимость этой информации. Но это не единственное «но» в этом вопросе.   
Нецелесообразно защищать всю информацию, какую можем, и все каналы информации какие только есть. Для этого необходимо определить объект защиты.  
Основными объектами защиты являются речевая информация и информация обрабатываемая техническими средствами. Так же информация может быть представлена в виде физических полей, информативных электрических сигналов, носителей на бумажной, магнитной, магнито-оптической и иной основе. В связи с этим защите подлежат средства и системы информатизации, участвующие в обработке защищаемой информации (ОТСС), технические средства и системы, не обрабатывающие непосредственно информацию, но размещенные в помещениях, где она обрабатывается (ВТСС) и защищаемые помещения.

* [Организационные и организационно-технические мероприятия](http://dehack.ru/metod_infbezop/org_tech_mp/)
* [Мероприятия по защите речевой информации](http://dehack.ru/metod_infbezop/zashita_akust/)
* [Штатные средства защиты операционных систем](http://dehack.ru/metod_infbezop/szi_v_OS/)

Только авторизованные пользователи могут оставлять комментарии - [авторизация](http://dehack.ru/login/), а если Вы впервые, то [нужно зарегистрироваться в системе](http://dehack.ru/registration/)

**39. Защита информации в компьютерных сетях: компьютерные и сетевые атаки, классификация**

С помощью таких программ, как WinNuke, Papa Smurf и Teardrop злоумышленники могут атаковать ваши компьютеры и нанести вам ущерб. Согласно опросу за 1999 год Института Компьютерной Безопасности и ФБР о компьютерных преступлениях 57 процентов опрошенных организаций сообщили, что считают соединения их сетей с Интернет "местом, откуда часто организуются атаки". 30 процентов опрошенных сообщило, что имели место случаи проникновения в их сети, а 26 процентов сказали, что в ходе атак происходила кража конфиденциальной информации. Федеральный центр по борьбе с компьютерными преступдениями в США - FedCIRC сообщил, что в 1998 году атакам подверглось около 130000 государственных сетей с 1100000 компьютерами.   
**Классификация компьютерных атак**   
Когда мы говорим "компьютерная атака", мы имеем в виду запуск людьми программ для получения неавторизованного доступа к компьютеру. Формы организации атак весьма разнообразны, но в целом все они принадлежат к одной из следующих категорий:  
Удаленное проникновение в компьютер: программы, которые получают неавторизованный доступ к другому компьютеру через Интернет (или локальную сеть) Локальное проникновение в компьютер: программы, которые получают неавторизованный доступ к компьютеру, на котором они работают. Удаленное блокирование компьютера: программы, которые через Интернет (или сеть) блокируют работу всего удаленного компьютера или отдельной программы на нем (для восстановления работоспособности чаще всего компьютер надо перезагрузить) Локальное блокирование компьютера: программы, которые блокируют работу компьютера, на котором они работают Сетевые сканеры: программы, которые осуществляют сбор информации о сети, чтобы определить, какие из компьютеров и программ, работающих на них, потенциально уязвимы к атакам. Сканеры уязвимых мест программ: программы, проверяют большие группы компьютеров в Интернете в поисках компьютеров, уязвимых к тому или иному конкретному виду атаки. Вскрыватели паролей: программы, которые обнаруживают легко угадываемые пароли в зашифрованных файлах паролей. Сейчас компьютеры могут угадывать пароли так быстро, что казалось бы сложные пароли могут быть угаданы. Сетевые анализаторы (снифферы): программы, которые слушают сетевой трафик. Часто в них имеются возможности автоматического выделения имен пользователей, паролей и номеров кредитных карт из трафика.   
**Как защититься от большинства компьютерных атак**   
Защита сети от компьтерных атак - это постоянная и нетривиальная задача; но ряд простых средств защиты смогут остановить большинство попыток проникновения в сеть. Например, хорошо сконфигурированный межсетевой экран и антивирусные программы, установленные на всех рабочих станциях, смогут сделать невозможными большинство компьютерных атак. Ниже мы кратко опишем 14 различных средств защиты, реализация которых поможет защитить вашу сеть.Оперативная установка исправлений для программ (Patching) Компании часто выпускают исправления программ, чтобы ликвидировать неблагоприятные последствия ошибок в них. Если не внести исправления в программы, впоследствии атакующий может воспользоваться этими ошибками и проникнуть в ваш компьютер. Системные администраторы должны защищать самые важные свои системы, оперативно устанавливая исправления для программ на них. Тем не менее, установить исправления для программ на всех хостах в сети трудно, так как исправления могут появляться достаточно часто. В этом случае надо обязательно вносить исправления в программы на самых важных хостах, а кроме этого установить на них другие средства защиты, описанные ниже. Обычно исправления должны получаться ТОЛЬКО от производителей программ. Обнаружение вирусов и троянских коней Хорошие антивирусные программы - незаменимое средство для повышения безопасности в любой сети. Они наблюдают за работой компьютеров и выявляют на них вредоносные программы. Единственной проблемой, возникающей из-за них, является то, что для максимальной эффективности они должны быть установлены на всех компьютерах в сети. На установку антивирусных программ на всех компьютерах и регулярное обновление антивирусных баз в них может уходить достаточно много времени - но иначе это средство не будет эффективным. Пользователей следует учить, как им самим делать эти обновления, но при этом нельзя полностью полагаться на них. Помимо обычной антивирусной программе на каждом компьютере мы рекомендуем, чтобы организации сканировали приложения к электронным письмам на почтовом сервере. Таким образом можно обнаружить большинство вирусов до того, как они достигнут машин пользователей. Межсетевые экраны Межсетевые экраны (firewalls) - это самое важное средство защиты сети организации. Они контролируют сетевой трафик, входящий в сеть и выходящий из нее. Межсетевой экран может блокировать передачу в сеть какого-либо вида трафика или выполнять те или иные проверки другого вида трафика. Хорошо сконфигуированный межсетевой экран в состоянии остановить большинство известных компьютерных атак. Вскрыватели паролей (Password Crackers) Хакеры часто используют малоизвестные уязвимые места в компьютерах для того, чтобы украсть файлы с зашифрованными паролями. Затем они используют специальные программы для вскрытия паролей, которые могут обнаружить слабые пароли в этих зашифрованных файлах. Как только слабый пароль обнаружен, атакующий может войти в компьютер, как обычный пользователь и использовать разнообразные приемы для получения полного доступа к вашему компьютеру и вашей сети. Хотя это средство используются злоумышленниками, оно будет также полезно и системным администраторам. Они должны периодически запускать эти программы на свои зашифрованные файлы паролей, чтобы своевременно обнаружить слабые пароли. Шифрование Атакующие часто проникают в сети с помощью прослушивания сетевого трафика в наиболее важных местах и выделения из него имен пользователей и их паролей. Поэтому соединения с удаленными машинами, защищаемые с помощью пароля, должны быть зашифрованы. Это особенно важно в тех случаях, если соединение осуществляется по Интернет или с важным сервером. Имеется ряд коммерческих и бесплатных программ для шифрования трафика TCP/IP (наиболее известен SSH). Сканеры уязвимых мест Это программы, которые сканируют сеть в поисках компьютеров, уязвимых к определенным видам атак. Сканеры имеют большую базу данных уязвимых мест, которую они используют при проверке того или иного компьютера на наличие у него уязвимых мест. Имеются как коммерческие, так и бесплатные сканеры. Грамотное конфигурирование компьютеров в отношении безопасности Компьютеры с заново установленными операционными системами часто уязвимы к атакам. Причина этого заключается в том, что при начальной установке операционной системы обычно разрешаются все сетевые средства и часто разрешаются небезопасным образом. Это позволяет атакующему использовать много способов для организации атаки на машину. Все ненужные сетевые средства должны быть отключены. Боевые диалеры(war dialer) Пользователи часто обходят средства защиты сети организации, разрешая своим компьютерам принимать входящие телефонные звонки. Пользователь перед уходом с работы включает модем и соответствующим образом настраивает программы на компьютере, после чего он может позвонить по модему из дома и использовать корпоративную сеть. Атакующие могут использовать программы-боевые диалеры для обзвонки большого числа телефонных номеров в поисках компьютеров, обрабатывающих входящие звонки. Так как пользователи обычно конфигурируют свои компьютеры сами, они часто оказываются плохо защищенными и дают атакующему еще одну возможность для организации атаки на сеть. Системные администраторы должны регулярно использовать боевые диалеры для проверки телефонных номеров своих пользователей и обнаружения сконфигурированных подобным образом компьютеров. Имеются как коммерческие, так и свободно распространяемые боевые диалеры. Рекомендации по безопасности (security advisories) Рекомендации по безопасности - это предупреждения, публикуемые группами по борьбе с компьютерными преступлениями и производителями программ о недавно обнаруженных уязвимых местах. Рекомендации обычно описывают самые серьезные угрозы, возникающие из-за этих уязвимых мест и поэтому являются занимающими мало времени на чтение, но очень полезными. Они описывают в-целом угрозу и дают довольно конкретные советы о том, что нужно сделать для устранения данного узявимого места. Найти их можно в ряде мест, но двумя самыми полезными являются те рекомендации, которые публикует группа по борьбе с компьютерными преступлениями [*CIAC*](http://ciac.llnl.gov) и [*CERT*](http://www.cert.org) Средства обнаружения атак (Intrusion Detection) Системы обнаружения атак оперативно обнаруживают компьютерные атаки. Они могут быть установлены за межсетевым экраном, чтобы обнаруживать атаки, организуемые изнутри сети. Или они могут быть установлены перед межсетевым экраном, чтобы обнаруживать атаки на межсетевой экран. Средства этого типа могут иметь разнообразные возможности. Имеется [*статья об их использовании и видах систем обнаружения атак*](http://www.icsa.net) Средства выявления топологии сети и сканеры портов Эти программы позволяют составить полную картину того, как устроена ваша сеть и какие компьютеры в ней работают, а также выявить все сервисы, которые работают на каждой машине. Атакующие используют эти средства для выявления уязвимых компьютеров и программ на них. Системные администраторы должны использовать эти средства для наблюдения за тем, какие программы и на каких компьютерах работают в их сети. С их помощью можно обнаружить неправильно сконфигурированные программы на компьютерах и установить исправления на них. Группа по расследованию происшествий с безопасностью В каждой сети, независимо от того, насколько она безопасна, происходят какие-либо события, связанные с безопасностью (может быть даже ложные тревоги). Сотрудники организации должны заранее знать, что нужно делать в том или ином случае. Важно заранее определить следующие моменты - когда вызывать правоохранительные органы, когда вызывать сотрудников группы по борьбе с компьютерными преступлениями, когда следует отключить сеть от Интернет, и что делать в случае компрометации важного сервера. [*CERT*](http://www.cert.org) предоставляет общие консультации в рамках США. FedCIRC отвечает за консультирование гражданских государственных учреждений в США. Политики безопасностиСистема сетевой безопасности насколько сильна, насколько сильно защищено самое слабое ее место. Если в рамках одной организации имеется несколько сетей с различными политиками безопасности, то одна сеть может быть скомпрометирована из-за плохой безопасности другой сети. Организации должны написать политику безопасности, в которой определялся бы ожидаемый уровень защиты, который должен быть везде единообразно реализован. Самым важным аспектом политики является выработка единых требований к тому, какой трафик должен пропускаться через межсетевые экраны сети. Также политика должна определять как и какие средства защиты (например, средства обнаружения атак или сканеры уязвимых мест) должны использоваться в сети. Для достижения единого уровня безопасности политика должна определять стандартные безопасные конфигурации для различных типов компьютеров. Тестирование межсетевых экранов и WWW-серверов на устойчивость к попыткам их блокирования Атаки на блокирование компьютера распространены в Интернет. Атакующие постоянно выводят из строя WWW-сайты, перегружают компьютеры или переполняют сети бессмысленными пакетами. Атаки этого типа могут быть очень серьезными, особенно если атакующий настолько умен, что организовал продолжительную атаку, у которой не выявить источник. Сети, заботящиеся о безопасности, могут организовать атаки против себя сами, чтобы определить, какой ущерб может быть нанесен им. Мы рекомендуем проводить этот вид анализа на уязвимость только опытным системным администраторам или специальным консультантам.

**40. Использование межсетевых экранов и политик сетевых безопасностей для защиты информации в компьютерных системах**

**Межсетевой экран** или **сетевой экран** — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Основной задачей сетевого экрана является защита [компьютерных сетей](http://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C) или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

Сетевые экраны подразделяются на различные типы в зависимости от следующих характеристик:

* обеспечивает ли экран соединение между одним узлом и сетью или между двумя или более различными сетями;
* на уровне каких сетевых протоколов происходит контроль потока данных;
* отслеживаются ли состояния активных соединений или нет.

В зависимости от охвата контролируемых потоков данных сетевые экраны делятся на:

* *традиционный сетевой* (или *межсетевой*) *экран* — программа (или неотъемлемая часть операционной системы) на шлюзе (сервере передающем трафик между сетями) или аппаратное решение, контролирующие входящие и исходящие потоки данных между подключенными сетями.
* [*персональный сетевой экран*](http://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D1%84%D0%B0%D0%B9%D1%80%D0%B2%D0%BE%D0%BB) — программа, установленная на пользовательском компьютере и предназначенная для защиты от несанкционированного доступа только этого компьютера.

Вырожденный случай — использование традиционного сетевого экрана сервером, для ограничения доступа к собственным ресурсам.

В зависимости от уровня, на котором происходит контроль доступа, существует разделение на сетевые экраны, работающие на:

* *сетевом уровне*, когда фильтрация происходит на основе адресов отправителя и получателя пакетов, номеров портов транспортного уровня модели OSI и статических правил, заданных администратором;
* *сеансовом уровне* (также известные как [*stateful*](http://ru.wikipedia.org/w/index.php?title=Stateful_Packet_Inspection&action=edit&redlink=1)) — отслеживающие сеансы между приложениями, не пропускающие пакеты нарушающих спецификации TCP/IP, часто используемых в злонамеренных операциях — сканировании ресурсов, взломах через неправильные реализации TCP/IP, обрыв/замедление соединений, инъекция данных.
* *уровне приложений*, фильтрация на основании анализа данных приложения, передаваемых внутри пакета. Такие типы экранов позволяют блокировать передачу нежелательной и потенциально опасной информации на основании политик и настроек.

Некоторые решения, относимые к сетевым экранам уровня приложения, представляют собой [прокси-серверы](http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%BA%D1%81%D0%B8-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80) с некоторыми возможностями сетевого экрана, реализуя прозрачные прокси-серверы, со специализацией по протоколам. Возможности прокси-сервера и многопротокольная специализация делают фильтрацию значительно более гибкой, чем на классических сетевых экранах, но такие приложения имеют все недостатки прокси-серверов (например, анонимизация трафика).

В зависимости от отслеживания активных соединений сетевые экраны бывают:

* *stateless* (простая фильтрация), которые не отслеживают текущие соединения (например, [TCP](http://ru.wikipedia.org/wiki/TCP)), а фильтруют поток данных исключительно на основе статических правил;
* *stateful,* [*stateful packet inspection (SPI)*](http://ru.wikipedia.org/w/index.php?title=Stateful_Packet_Inspection&action=edit&redlink=1) (фильтрация с учётом контекста), с отслеживанием текущих соединений и пропуском только таких пакетов, которые удовлетворяют логике и алгоритмам работы соответствующих [протоколов](http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D0%BF%D0%B5%D1%80%D0%B5%D0%B4%D0%B0%D1%87%D0%B8_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85) и приложений. Такие типы сетевых экранов позволяют эффективнее бороться с различными видами [DoS-атак](http://ru.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0) и уязвимостями некоторых сетевых протоколов. Кроме того, они обеспечивают функционирование таких протоколов, как [H.323](http://ru.wikipedia.org/wiki/H.323), [SIP](http://ru.wikipedia.org/wiki/SIP), [FTP](http://ru.wikipedia.org/wiki/FTP) и т. п., которые используют сложные схемы передачи данных между адресатами, плохо поддающиеся описанию статическими правилами, и, зачастую, несовместимых со стандартными, *stateless* сетевыми экранами.

**Типичные возможности**

* фильтрация доступа к заведомо незащищенным службам;
* препятствование получению закрытой информации из защищенной подсети, а также внедрению в защищенную подсеть ложных данных с помощью уязвимых служб;
* контроль доступа к узлам сети;
* может регистрировать все попытки доступа как извне, так и из внутренней сети, что позволяет вести учёт использования доступа в Internet отдельными узлами сети;
* регламентирование порядка доступа к сети;
* уведомление о подозрительной деятельности, попытках зондирования или атаки на узлы сети или сам экран;

Вследствие защитных ограничений могут быть заблокированы некоторые необходимые пользователю службы, такие как [Telnet](http://ru.wikipedia.org/wiki/Telnet), [FTP](http://ru.wikipedia.org/wiki/FTP), [SMB](http://ru.wikipedia.org/wiki/SMB), [NFS](http://ru.wikipedia.org/wiki/Network_File_System), и так далее. Поэтому настройка файрвола требует участия специалиста по сетевой безопасности. В противном случае вред от неправильного конфигурирования может превысить пользу.

Так же следует отметить, что использование файрвола увеличивает время отклика и снижает пропускную способность, поскольку фильтрация происходит не мгновенно.

Политика сетевой безопасности описывает границы ответственности и отчетности при использовании, сборе и хранении информации. В ней определены ответственные за саму реализацию политики, описывает лиц, к которым она применима. Все служащие компании должны соблюдать политику безопасности,должны сообщать об реальной или возможной опасности своему начальнику. Сетевую безоасность может обеспечить аутентификация информации.

1. **Виртуальные частные сети (VPN). Методы защиты на сетевом уровне.**

**VPN (Virtual Private Network — виртуальная частная сеть)** — технология, при которой происходит безопасный обмен информацией между двумя компьютерами по защищенному виртуальному каналу через сеть общего пользования (Интернет).

Для создания VPN могут использоваться различные протоколы. Необходимая аппаратура: VPN-шлюзы.

По локальной сети пакеты передаются в обычном виде. При обращении к удаленному компьютеру запрос поступает сначала на VPN-шлюз, который обрабатывает и зашифровывает информацию, а затем через Интернет передается другому VPN-шлюзу, обслуживающему локальную сеть получателя. Там информация извлекается, и запрос в обычном виде уходит адресату по локальной сети.

**VPN** ([англ.](http://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *Virtual Private Network* — виртуальная частная сеть) — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, [Интернет](http://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82)). Несмотря на то, что коммуникации осуществляются по сетям с меньшим неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, [инфраструктуры открытых ключей](http://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D1%80%D0%B0%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D0%B0_%D0%BE%D1%82%D0%BA%D1%80%D1%8B%D1%82%D1%8B%D1%85_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9), средств для защиты от повторов и изменений передаваемых по логической сети сообщений).

В зависимости от применяемых протоколов и назначения, VPN может обеспечивать соединения трёх видов: *узел-узел*, *узел-сеть* и *сеть-сеть*.

VPN состоит из двух частей: «внутренняя» (подконтрольная) сеть, которых может быть несколько, и «внешняя» сеть, по которой проходит инкапсулированное соединение (обычно используется [Интернет](http://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82)). Возможно также подключение к виртуальной сети отдельного [компьютера](http://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80). Подключение удалённого пользователя к VPN производится посредством сервера доступа, который подключён как к внутренней, так и к внешней (общедоступной) сети. При подключении удалённого пользователя (либо при установке соединения с другой защищённой сетью) сервер доступа требует прохождения процесса [идентификации](http://ru.wikipedia.org/wiki/%D0%98%D0%B4%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F), а затем процесса [аутентификации](http://ru.wikipedia.org/wiki/%D0%90%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F). После успешного прохождения обоих процессов, удалённый пользователь (удаленная сеть) наделяется полномочиями для работы в сети, то есть происходит процесс [авторизации](http://ru.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F).

Программные средства защиты информации.

* Встроенные средства защиты информации
* [Антивирусная программа](http://ru.wikipedia.org/wiki/%D0%90%D0%BD%D1%82%D0%B8%D0%B2%D0%B8%D1%80%D1%83%D1%81%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0) (антивирус) — программа для обнаружения компьютерных вирусов и лечения инфицированных файлов, а также для профилактики — предотвращения заражения файлов или операционной системы вредоносным кодом.
* Специализированные программные средства защиты информации от несанкционированного доступа обладают в целом лучшими возможностями и характеристиками, чем встроенные средства. Кроме программ шифрования и [криптографических](http://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F) систем, существует много других доступных внешних средств защиты информации.
* [Межсетевые экраны](http://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D0%B6%D1%81%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D1%8D%D0%BA%D1%80%D0%B0%D0%BD) (также называемые брандмауэрами или файрволами — от [нем.](http://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D0%BC%D0%B5%D1%86%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *Brandmauer*, [англ.](http://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *firewall* — «противопожарная стена»). Между локальной и глобальной сетями создаются специальные промежуточные серверы, которые инспектируют и фильтруют весь проходящий через них трафик сетевого/транспортного уровней. Это позволяет резко снизить угрозу несанкционированного доступа извне в корпоративные сети, но не устраняет эту опасность полностью. Более защищенная разновидность метода — это способ маскарада (masquerading), когда весь исходящий из локальной сети трафик посылается от имени firewall-сервера, делая локальную сеть практически невидимой.
* Proxy-servers (proxy — доверенность, доверенное лицо). Весь трафик сетевого/транспортного уровней между локальной и глобальной сетями запрещается полностью — [маршрутизация](http://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F) как таковая отсутствует, а обращения из локальной сети в глобальную происходят через специальные серверы-посредники. Очевидно, что при этом обращения из глобальной сети в локальную становятся невозможными в принципе. Этот метод не дает достаточной защиты против атак на более высоких уровнях — например, на уровне приложения (вирусы, код [Java](http://ru.wikipedia.org/wiki/Java) и [JavaScript](http://ru.wikipedia.org/wiki/JavaScript)).
* [VPN](http://ru.wikipedia.org/wiki/VPN) (виртуальная частная сеть) позволяет передавать секретную информацию через сети, в которых возможно прослушивание трафика посторонними людьми. Используемые технологии: [PPTP](http://ru.wikipedia.org/wiki/PPTP), [PPPoE](http://ru.wikipedia.org/wiki/PPPoE), [IPSec](http://ru.wikipedia.org/wiki/IPSec).

**42. Аудит безопасности компьютерных сетей: уровни, цели и показатели**

**Что такое „аудит безопасности”**

Фраза «проверка безопасности» употребляется взаимозаменяемо с фразой «аудит компьютерной безопасности», хотя эти понятия отличаются. Проверка безопасности (pen-test) - это узко направленная проверка наличия брешей в критических ресурсах, таких как межсетевая защита или Web сервер. Проверяющие безопасность могут рассматривать лишь один сервис на сетевом ресурсе. Они обычно работают извне с минимальной информацией о данной сети для того, чтобы как можно более реалистично симулировать возможную атаку хакера.

С другой стороны, аудит компьютерной безопасности – это систематическая оценка того, как устроена политика безопасности данной организации. Аудиторы компьютерной безопасности работают с полным владением информацией об организации, ее внутренней структуре, для того, чтобы исследовать ресурсы, которые должны состоять под аудитом.

Аудит безопасности является частью процесса определения и управления эффективными политиками безопасности, и это не просто разговоры и конференции. Аудит безопасности касается каждого, кто использует ресурсы внутри организации. Он предоставляет все возможности для проверки безопасности вашей фирмы.

Аудиторы компьютерной безопасности осуществляют проверку посредством личных опросов, сканирований на наличие уязвимостей, проверки настройки операционной системы, анализа открытых сетевых ресурсов, истории данных. Они в первую очередь исследуют использование политик безопасности – основу любой эффективной стратегии безопасности организации. Далее следуют вопросы, на которые аудит безопасности должен найти ответ:

* Насколько сложно подобрать пароль?
* Используется ли ACLs на сетевых ресурсах для контроля доступа к данным?
* Ведется ли аудит доступа к данным?
* Просматриваются ли логи аудита?
* Соответствуют ли настройки безопасности операционной системы общепринятой практике безопасности
* Устранены ли все ненужные приложения и сервисы на каждой системе?
* Пропатчены ли операционные системы и коммерческие приложения до нужного уровня?
* Как хранятся копии данных, кто имеет к ним доступ, проводится ли сохранение данных регулярно?
* Разработан ли план восстановления данных в случае инцидента? Проводились ли тренировки по восстановлению данных?
* Есть ли в наличии криптографические утилиты для шифрования данных и настроены ли они должным образом?
* Были ли написаны используемые программы с учетом безопасности?
* Каким образом проводилось тестирование этих программ на предмет наличия брешей в их безопасности?
* Каким образом ведется аудит изменений кода и конфигураций на каждом уровне? Как просматриваются эти записи и кто ответственный за проведение их просмотра?

Это лишь несколько вопросов, на которые следует обратить внимание при проведении аудита безопасности. Отвечая честно и точно на эти вопросы, организация может представить реальную картину безопасности своей жизненно важной информации.

**Определение политик безопасности**

Аудит безопасности – это, по существу, оценка эффективности применения политик безопасности внутри организации. Конечно, предполагается, что организация уделяет внимание политике безопасности, что, к сожалению, не всегда является таковым. Даже сейчас во многих организациях не существует четко сформулированной политики. Политики безопасности являются средствами стандартизации практики безопасности посредством их документирования (в письменной форме) и соглашения со стороны сотрудников, прочитавших и подписавшихся под ними. Если не существует написанных политик безопасности, или они неформальны, то это может привести к их неправильному пониманию и невыполнению сотрудниками. Проведение политики безопасности должно требовать ознакомление и согласие в письменной форме с оными. Наличие политик безопасности не затрагивает вопрос компетентности работников, а скорее дает уверенность в том, что каждый работник знает, как защитить информацию, и согласен исполнять свое обязательство.

Проблемы часто возникают на рабочих местах между культурой поведения и политиками безопасности. Даже при большой ответственности и осознании ее сотрудники часто предпочитают удобство безопасности. Например, сотрудники знают, что должны выбирать трудно угадываемые пароли, но они также хотят, чтобы эти пароли были всегда под рукой. Каждый аудитор знает, что следует проверить, не наклеены ли бумажки с паролем на мониторе, и не прячет ли работник свой пароль под клавиатурой (почему-то многие сотрудники убеждены, что это – самое безопасное место). Также каждый аккаунт администратора должен иметь пароль; часто из-за спешки установка пароля откладывается на потом, что приводит к появлению уязвимой системы в сети.

Целью аудита безопасности является поиск слабины в политиках безопасности и рекомендации по их решению. Политика должна быть также объектом внимательного рассмотрения. Действительно ли это существующий документ, точно описывающий способы ежедневной защиты организацией ИТ ресурсов? Отражает ли политика производственные стандарты используемых ИТ ресурсов внутри организации?

**Предварительный аудит.**

Прежде чем аудиторы компьютерной безопасности приступят к предварительному аудиту, им следует проделать большое количество организационных работ. Они должны быть знакомы с объектом аудита. Вместе с анализом результатов раннее проведенных аудитов, аудиторам следует взять на вооружение некоторые инструменты, к которым они впоследствии обратятся. Первый – это предварительное знакомство с фирмой; техническое описание хостов системы, включающее управление и данные о пользователях. Такая информация может быть устаревшей, но, тем не менее, давать общее представление о системе. Общие сведения касательно безопасности могут быть использованы при дальнейшем знакомстве с предприятием. Эти сведения являются естественно субъективными, но они полезны, так как позволяют создать общую картину, построенную на практике. Аудиторам часто задают вопросы о средствах и методах оценки ситуации при контроле за ИТ ресурсами. К таковым относятся: средства управления, средства контроля доступа/аутентификации, безопасность на физическом уровне, внешний доступ к системе, средства и методы администрирования системы, соединение с внешними сетями, удаленный доступ, ответственность за инцидент, предварительное планирование.

Анализ фирмы и сведения о безопасности должны быть четко описаны с определенным количеством ответов на специфические требования. Они должны быть пронумерованы по возрастанию от менее (без особых требований) к более желанным (с особыми требованиями и документацией). И те, и другие должны иметь электронные коммерческие соглашения о пригодности для клиентской организации. Например, компании, выпускающие кредитные карточки имеют перечень соглашений о безопасности для своих продуктов. Эти соглашения включают в себя сетевую безопасность, безопасность операционной системы и приложений, а также защиту на физическом уровне.

Аудиторы, в основном внутренние аудиторы, должны рассмотреть предыдущие инциденты в клиентской организации, связанные с безопасностью с целью установить слабые места в организации безопасности. Также должны быть проанализированы настоящие условия во избежания повторения неприятных инцидентов. Если аудиторы проверяют систему, позволяющую выход в Интернет, им следует обратить внимание на логи IDS/Фаерволов. Отображают ли эти логи попытки воспользоваться уязвимостями системы? Может ли для этого существовать какая-то причина (например, ошибка в настройках фаервола), по которой эти попытки могут иметь место. Возможно ли это проверить?

Из-за большого объема данных, которые подлежат проверке, аудиторы захотят работать с клиентами напрямую, чтобы определить масштаб работ для аудита. Факторы, влияющие на это: бизнес план фирмы, способ защиты данных и значение/важность этих данных для организации, предыдущие инциденты, время для проведения аудита и талант/компетентность аудиторов. Профессиональные аудиторы захотят четко определить масштаб работ, соглашенный с клиентом.

Далее аудиторы разрабатывают план, согласно которому будет приводиться аудит, персонал, с которым будут работать аудиторы и инструменты аудита. Затем они обсуждают план с агентством. После этого аудиторы обсуждают цель аудита с персоналом и согласуют некоторые детали, такие как время проведения аудита, требующиеся средства и влияние аудита на повседневную работу. Далее, аудиторы должны убедиться в том, что цели аудита поняты персоналом.

**Аудит**

По прибытии на фирму, аудиторы не должны мешать ведению бизнеса во время проверки. Им следует провести инструктаж, в котором аудиторы снова подчеркнут масштаб своей работы и их планы. Любые вопросы, возникшие у сотрудников фирмы, должны быть разъяснены, и в конце беседы подведены итоги настоящей цели аудита.

Аудиторы должны быть строгими и беспристрастными и проводить аудит согласно стандартам и методам. Во время аудита они будут собирать данные о физической безопасности компьютеров и проводить интервью. Они могут произвести оценку уязвимости сети, безопасности операционных систем и приложений, оценку контроля за доступом и другие вычисления. Во время процесса проверки аудиторам следует придерживаться заранее определенного плана, и в то же время быть готовыми к неожиданным проблемам. Они должны действовать между сложившимися понятиями или ожиданиями того, что они должны найти и того, что есть на самом деле.

**Проведение заключительного инструктажа**

После окончания проверки, аудиторы проведут заключительный инструктаж, убеждаясь в том, что руководство в курсе всех проблем, которые должны быть решены немедленно. На вопросы от руководства следует отвечать в нормальной манере, чтобы не создать плохого впечатления об аудите. Следует подчеркнуть, что аудиторы не способны в данный момент дать четкие ответы на поставленные вопросы. Все окончательные выводы будут сделаны после окончательных анализов результатов аудита.

**Обратно в офис**

Возвратившись в офис, аудиторы начнут объединять свои записи для проверки и анализировать собранные данные с помощью оценочных инструментов. Должно состояться первое собрание, для того, чтобы подбить отчет результатов аудита. На этом собрании аудиторы могут определить области проблем и возможные решения. Аудиторский отчет может быть составлен в нескольких формах, но текст отчета должен быть простым и прямолинейным, содержащим конкретные данные о найденных проблемах вместе с решениями по устранению этих недостатков.

Аудиторский отчет может быть составлен в виде заключения, содержащим детали найденного и дополнений, таких как результаты сканирования. При написании отчета следует сначала сделать краткое описание, так как придется вскоре после возвращения дать краткий отчет руководству. Очень важно представлять, что сильные и слабые стороны безопасности должны быть описаны в кратком изложении, чтобы сбалансировать отчет. Далее аудитор может предоставить рапорт, основанный на проверке. Обнаруженные уязвимости должны быть представлены в простой и логичной форме на отдельном листе для каждой обнаруженной уязвимости. На таком листе должна быть описана проблема, ее значение и методы решения. На листе должно остаться место для подтверждения правильных путей аудита и блок для комментариев чтобы оспорить найденное.

**Не заставляйте их ждать**

Отчет должен быть представлен быстро и четко, чтобы заказчик мог исправить проблемы, обнаруженные при аудите. В зависимости от политик компании, аудиторы должны быть готовыми объяснить недостатки и помочь устранить их. Руководство должно вести наблюдение за недостатками, выявленными во время аудита до тех пор, пока они не будут устранены.

**Аудит – это не событие, а процесс**

Следует помнить, что с развитием организации, меры безопасности также должны меняться. С этой точки зрения аудит компьютерной безопасности – это не одноразовая задача, а продолжительные попытки защитить данные. Аудит исследует политику безопасности организации и проводит анализ эффективности этой политики в контексте структуры организации, ее целей и действий. Аудит должен быть построен на прошлой проверке, чтобы помочь вникнуть в политику и исправить уязвимости, обнаруженные в процессе аудита. Инструменты также являются важной частью процесса аудита, так как аудит не будет эффективным без использования последних и самых лучших инструментов поиска уязвимостей, а значимости ему прибавит использование организованной, последовательной, точной информации о данных и анализе, позволяющим нахождение и устранение ошибок.

**43. Этапы проведения инструментальной проверки автоматизированных информационных систем**

Для проверки корректности системных установок (или их неизменности с момента последней проверки) существуют программные продукты класса "сканер безопасности системы". Эти продукты на сегодняшний день существуют для большинства операционных систем и число достигает десятка. В их число входят такие продукты, как ASET (компонент ОС Solaris), KSA (для платформ NetWare и NT), SSS (System Security Scanner) (Unix-платформы ).

**System Security Scanner**

Программа System Security Scanner (S3) предназначена для проведения проверки состояния безопасности на отдельных UNIX-компьютерах и поиска уязвимости ОС как снаружи (по сети с использованием Internet Scanner), так и изнутри (из самой ОС компьютера). При этом проводится проверка прав доступа и прав собственности файлов, конфигураций сетевых сервисов, установок ресурсов пользователей, программ аутентификации и других, связанных с пользователями слабых мест (например, паролей).

*Характеристики*

* Проверка текущей конфигурации

Анализируются особенности конфигурации, которые могут привести к получению несанкционированного доступа. К ним относятся: файлы конфигураций, версии ПО, права доступа и собственники файлов, файлы SUID/SGID, необычные файлы, ресурсы пользователей и групп пользователей, пароли.

* Проверка опасных изменений в системе.

Проводится поиск следов несанкционированного доступа в систему, к которым относятся необычные изменения в текущей конфигурации системы, например, изменения размера, прав доступа или содержания отдельных файлов, либо изменения в установках ресурсов пользователей , а также следов переключения сетевого интерфейса в режимы работы, допускающие передачу данных на внешний компьютер.

* Удобный графический интерфейс пользователя.

S3 предоставляет возможность для конфигурации и запуска сеансов сканирования и создания отчетов по их результатам.

* Удаленное сканирование.

Программа S3 позволяет выполнять проверку удаленных компьютеров в неоднородной распределенной сетевой среде с центрального хоста, используя шифрование сеансов связи.

* Отчеты по результатам проверок.

В создаваемых по результатам сканирования отчетах отражается информация об обнаруженных уязвимых местах проверяемых систем с пояснениями по каждому типу уязвимости и рекомендуемыми действиями по их коррекции. Отчеты могут быть представлены как в HTML-формате, так и в виде стандартного ASCII-текста.

**Средства анализа защищенности сетевых сервисов**

Слабости, заложенные в реализации сетевых сервисов протокола TCP/IP известны достаточно давно. Поскольку именно сетевые сервисы во многих случаях служили объектом атак на распределенные информационные системы, возникла задача автоматизированной проверки сетевых систем на уязвимость со стороны известных атак. Первым продуктом, выполняющим данную функцию был пакет программ SATAN, сделанный F.Venema и распространяемый бесплатно. В состав пакета включены около двух десятков проверок уязвимостей сетевых сервисов. Несмотря на значительное время, прошедшее с момента создания пакета, практическая проверка любой системы с его помощью может быть весьма полезна - даже старые уязвимости не всегда адекватно учитываются администраторами ИС.

Если требования к системе включают периодические проверки по наиболее полному списку уязвимостей (это, например необходимо для межсетевых экранов, где такие проверки должны проводиться периодически), то необходимо использовать более поздние коммерческие продукты сканирования уязвимостей. В качестве примера одного из наиболее продвинутых продуктов этого класса можно привести Internet Scanner SAFEsuite.

Пакет программ Internet Scanner SAFEsuite предназначен для проведения комплексной оценки эффективности политики безопасности на уровне сетевых сервисов. Он предоставляет возможности для идентификации и коррекции более 140 известных слабых мест и постоянного наблюдения за состоянием безопасности для широкого диапазона сетевых устройств - от web-узлов и межсетевых экранов и до серверов и рабочих станций UNIX, Windows 95, Windows NT и всех других устройств работающих с TCP/IP.

Состоит из трех программ: Web Security Scanner, Firewall Scanner, Intranet Scanner.

*Общие характеристики пакета программ Internet Scanner SAFEsuite*

Автоматизированное и конфигурируемое сканирование:

* автоматическая идентификация и создания отчетов по слабым местам
* плановые периодические сканирования или сканирования после определенных событий
* конфигурация сканирования по адресам IP, типам слабых мест, рискам и другим устанавливаемым пользователями критериям
* автоматическая коррекция ключевых слабых мест
* надежность и повторяемость.

Обеспечение безопасности:

* возможность управления рисками
* инвентаризация всех сетевых устройств и идентификация существующих базовых слабых мест
* распределение приоритетов по степеням риска (высокий, средний, низкий)
* анализ и сравнение базовых отчетов для использования в будущих оценках
* создание цепи обратной связи при реализации политики безопасности

Простота пользования:

* графические интерфейсы пользователя Windows NT и Motif UNIX
* создание отчетов HTML с упорядочением по типам слабых мест, классам рисков, именам host и адресам IP
* двухмерная сетевая карта, облегчающая поиск слабых мест
* централизация процедур сканирования, управления и мониторинга

**Web Secure Scanner**

Предназначен для поиска слабых мест безопасности на web-серверах. Обеспечивает аудит ОС, под управлением которой работает web-сервер, программ-приложений, установленных на web-сервере, и CSI scripts в web-приложениях. Проводит тестирование конфигурации web-сервера, оценивает уровень безопасности основной файловой системы и просматривает CSI scripts на наличие слабых мест. По итогам тестирования создается отчет с описанием обнаруженных слабых мест и с рекомендациями по корректирующим действиям.

**Firewall Scanner**

Обеспечивает поиск слабых мест в межсетевых экранах, прежде всего в их конфигурации, и предоставляет рекомендации по их коррекции. Проводит тестирование реакции межсетевых экранов на различные типы попыток нарушения безопасности. Выполняет сканирование сервисов - идентификацию всех сетевых сервисов, доступ к которым осуществляется через межсетевой экран. Firewall Scanner рекомендуется сделать частью установки межсетевого экрана и составной частью программы обеспечения безопасности.

**Intranet Scanner**

Предназначен для автоматического обнаружения потенциальных слабых мест внутри сетей с использованием различных тестов для проверки реакции на несанкционированные проникновения. Обеспечивает проверку различных сетевых устройств, включая UNIX hosts, системы, работающие под Microsoft NT/Windows 95, маршрутизаторы, web-серверы и X-терминалы.

**44, 45. Внутренний и внешний аудит информационных систем**

Внутренний аудит информационной системы – это независимая и объективная оценка защищенности информационной системы от внутреннего несанкционированного воздействия и утечки конфиденциальной информации.

 Внутренний аудит информационной безопасности включает в себя:

* [технический аудит сети](http://www.its-lab.ru/services/audit/network-audit.html);
* [внутренние тесты на проникновение](http://www.its-lab.ru/services/audit/penetration-test.html);
* аудит защищенности от утечки информации и действий инсайдеров;
* аудит корпоративных беспроводных сетей.

**Почему это необходимо?**

 Основные цели проведения внутреннего аудита информационной системы:

* Поиск уязвимостей, позволяющих произвести атаку на информационную систему из внутреннего периметра корпоративной сети.
* Определение надежности и достаточности применяемых систем защиты информационной системы от утечек информации и действий инсайдеров.
* Регулярное отслеживание изменений в информационной системе.
* Получение Заказчиком независимой оценки.
* Соблюдение требований международных стандартов и нормативных документов в сфере информационной безопасности рекомендующие (требующие) периодического или разового проведения аудита информационной безопасности.

Основные задачи проведения внутреннего аудита информационной системы:

* Анализ структуры, функций, используемых технологий обработки и передачи информации в информационной системе.
* Выявление уязвимостей информационной системы с их ранжированием по степени критичности, их идентификация по международным и собственным классификаторам.
* Составление модели нарушителя, применение методики активного аудита для проверки возможности реализации выявленных угроз информационной безопасности.
* Оценка полноты фактически реализованных мер защиты от утечки информации и действий инсайдеров.
* Требования международных стандартов и нормативных документов в сфере информационной безопасности.
* Формирование требований к построению системы защиты конфиденциальных данных от утечки и действий инсайдеров.
* Выработка рекомендаций по повышению эффективности защиты информации в информационной системе.
* Подготовка данных при проведении [комплексного аудита информационной безопасности](http://www.its-lab.ru/services/audit.html).

Внешний аудит информационной системы – это независимая и объективная оценка защищенности информационной системы от внешнего несанкционированного воздействия.

Внешний аудит информационной системы предполагает выполнение:

* [проведение технического аудита сети](http://www.its-lab.ru/services/audit/network-audit.html);
* [внешних тестов на проникновение](http://www.its-lab.ru/services/audit/penetration-test.html);
* [аудита Web-приложений](http://www.its-lab.ru/services/audit/web-audit.html).

**Почему это необходимо?**

Основные цели проведения внешнего аудита информационной системы:

* Поиск уязвимостей, позволяющих произвести внешнюю атаку на информационную систему компании.
* Комплексная оценка защищенности информационной системы, отсутствие или недостатки применяемых систем защиты информации от внешнего несанкционированного воздействия.
* Регулярное отслеживание изменений в информационной системе.
* Получение Заказчиком независимой оценки.
* Соблюдение требований международных стандартов и нормативных документов в сфере информационной безопасности рекомендующие (требующие) периодического или разового проведения аудита информационной безопасности.

Основные задачи проведения внешнего аудита информационной системы:

* Анализ структуры, функций, используемых технологий обработки, хранения и передачи информации в информационной системе.
* Выявление уязвимостей информационной системы с их ранжированием по степени критичности, их идентификация по международным и собственным классификаторам.
* Составление модели нарушителя, применение методики активного аудита для проверки возможности реализации выявленных угроз информационной безопасности.
* Требования международных стандартов и нормативных документов в сфере информационной безопасности.
* Выработка рекомендаций по повышению эффективности защиты информации в информационной системе.
* Подготовка данных при проведении [комплексного аудита информационной безопасности](http://www.its-lab.ru/services/audit.html).

**Методы внешнего аудита**

В ходе активного аудита специалисты Лаборатории ИнформСистем применяют модели нарушителя, согласно которым Заказчик предоставляет нам следующие минимальные привилегии по доступу к  информационной системе: физический доступ внутрь охраняемого периметра или возможность внешнего подключения к информационной системе и Web-ресурсам Заказчика.

Перед началом активного аудита, разрабатывается и совместно с Заказчиком утверждается график проведения работ. Для особо критичных ресурсов Заказчика проверки могут выполняться в нерабочее время для обеспечения непрерывности работы и исключения возможности отказа в обслуживании информационной системы.

Мы предлагаем своим Заказчикам следующую методологию оценки защищенности информационной системы:

* Тестирование методом черного ящика (black box testing).
* Тестирование методом серого ящика (gray box testing).
* Тестирование методом белого ящика (white box testing).

При внешнем аудите информационной системы, могут использоваться следующие модели взаимодействия с Заказчиком:

* ***Black Hat.*** Специалисты Заказчика, отвечающие за информационную безопасность, не информируются о проведении тестов. В таком случае удается проверить уровень оперативной готовности к атакам сетевых администраторов или администраторов информационной безопасности.
* ***White Hat.*** Работы проводятся совместно со специалистами Заказчика. Основная задача сводится к совместному обнаружению возможных уязвимостей и оценке риска проникновения в систему.

**Работы по внешнему аудиту информационной системы включают в себя ряд последовательных этапов:**

* поиск и анализ всей доступной информации;
* проведение технического аудита сети;
* проведение внешних тестов на проникновение;
* проведение аудита Web-приложений;
* инструментальное сканирование, предполагающее использование как специализированных средств, так и специфичных разработок нашей компании;
* детальный анализ вручную;
* анализ и оценка выявленных уязвимостей и выработка рекомендаций;
* подготовка отчета;
* при необходимости, консультирование специалистов Заказчика.

**46. История, форматы, типы мультимедиа приложений**

**Мультимедиа** — комплекс аппаратных и программных средств, позволяющих пользователю работать в диалоговом режиме с разнородными данными (графика, текст, звук, видео), организованными в виде единой информационной среды.

Например, в одном объекте-контейнере ([англ.](http://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *container*) может содержаться [текстовая](http://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D0%BA%D1%81%D1%82), [аудиальная](http://ru.wikipedia.org/wiki/%D0%97%D0%B2%D1%83%D0%BA), [графическая](http://ru.wikipedia.org/wiki/%D0%98%D0%B7%D0%BE%D0%B1%D1%80%D0%B0%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5) и [видео](http://ru.wikipedia.org/wiki/%D0%92%D0%B8%D0%B4%D0%B5%D0%BE) информация, а также, возможно, способ [интерактивного](http://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%B0%D0%BA%D1%82%D0%B8%D0%B2%D0%BD%D0%BE%D1%81%D1%82%D1%8C) взаимодействия с ней.

Термин *мультимедиа* также, зачастую, используется для обозначения носителей информации, позволяющих хранить значительные объемы данных и обеспечивать достаточно быстрый доступ к ним (первыми носителями такого типа были CD — compact disk). В таком случае термин *мультимедиа* означает, что компьютер может использовать такие носители и предоставлять информацию пользователю через все возможные виды данных, такие как аудио, видео, анимация, изображение и другие в дополнение к традиционным способам предоставления информации, таким как текст.

Мультимедиа может быть грубо классифицировано как **линейное** и **нелинейное**.

Аналогом линейного способа представления может являться [кино](http://ru.wikipedia.org/wiki/%D0%9A%D0%B8%D0%BD%D0%B5%D0%BC%D0%B0%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84). [Человек](http://ru.wikipedia.org/wiki/%D0%A7%D0%B5%D0%BB%D0%BE%D0%B2%D0%B5%D0%BA), просматривающий данный документ никаким образом не может повлиять на его вывод.

Нелинейный способ представления информации позволяет человеку участвовать в выводе [информации](http://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F), взаимодействуя каким-либо образом со средством отображения мультимедийных данных. Участие человека в данном процессе также называется «интерактивностью». Такой способ взаимодействия человека и [компьютера](http://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80) наиболее полным образом представлен в категориях [компьютерных игр](http://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D1%82%D0%B5%D0%B3%D0%BE%D1%80%D0%B8%D1%8F:%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D0%B5_%D0%B8%D0%B3%D1%80%D1%8B). Нелинейный способ представления мультимедийных данных иногда называется «гипермедиа».

В качестве примера линейного и нелинейного способа представления [информации](http://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F), можно рассматривать такую ситуацию, как проведение презентации. Если презентация была записана на пленку и показывается аудитории, то при этом способе донесения информации просматривающие данную презентацию не имеют возможности влиять на докладчика. В случае же живой презентации, аудитория имеет возможность задавать докладчику вопросы и взаимодействовать с ним прочим образом, что позволяет докладчику отходить от темы презентации, например поясняя некоторые термины или более подробно освещая спорные части доклада. Таким образом, живая презентация может быть представлена, как нелинейный(интерактивный) способ подачи информации…

1. **Использование мультимедиа: преимущества и недостатки. Перспективы развития.**

Мультимедиа – комплекс аппаратных и программных средств, позволяющих пользователю работать в диалоговом режиме с разнородными данными (графика, текст, звук, видео), организованными в виде единой информационной среды. Основные составляющие мультимедиа: текст, аудио, графическая и видео информация, а также способ интерактивного взаимодействия с ней.

Термин мультимедиа также, зачастую, используется для обозначения носителей информации, позволяющих хранить значительные объемы данных и обеспечивать достаточно быстрый доступ к ним (первыми носителями такого типа были CD). В таком случае термин мультимедиа означает, что компьютер может использовать такие носители и предоставлять информацию пользователю через все возможные виды данных, такие как аудио, видео, анимации, изображение и другие в дополнение к традиционным способам предоставления информации, таким как текст.

Мультимедийные презентации могут быть проведены человеком на сцене, показаны через проектор или же на другом локальном устройстве воспроизведения.

Мультимедийные игры – такие игры, в которых игрок взаимодействует с виртуальной средой, простроенной компьютером. Состояние виртуальной среды передается игроку при помощи различных способов передачи информации (аудиальный, визуальный, тактильный). В настоящее время все игры на компьютере или игровой приставке относятся к мультимедийным играм. Стоит отметить, что в такой тип игр можно играть как в одиночку на локальном компьютере или приставке, так и с другими игроками через локальную или глобальную сеть.

Различные форматы мультимедиа данных можно использовать для упрощения восприятия информации потребителем. Например, предоставить информацию не только в текстовом виде, но и проиллюстрировать ее аудиоданными или видеоклипом. Таким же образом современное искусство может представить повседневные, обыденные вещи в новом виде.

Для того, чтобы выложить видео на YouTube или Яндекс.Видео пользователю не требуется знаний по редактированию видео, кодированию и сжатию информации, знаний по устройству web-серверов. Пользователь просто выбирает локальный файл и тысячи других пользователей видеосервиса имеют возможность просмотреть новый видеоролик.

Мультимедиа находит свое применение в различных областях, включая рекламу, искусство, образование, индустрию развлечений, технику, медицину, математику, бизнес, научные исследования.

В образовании мультимедиа используется для создания компьютерных учебных курсов и справочников, таких как энциклопедии и сборники. В промышленном секторе мультимедиа используют как способ презентации информации для акционеров, руководства и коллег. Мультимедиа также полезно в организации обучения персонала, рекламы и продаж продукта по всему миру. В математических и научных исследованиях мультимедиа в основном используется для моделирования и симуляции. Например: ученый может взглянуть на молекулярную модель какого-либо вещества и манипулировать ею с тем, чтобы получить другое вещество. Врачи также могут получить подготовку с помощью виртуальных операций или симуляторов человеческого тела, пораженного болезнью, распространенной вирусами и бактериями, таким образом пытаясь разработать методики ее предотвращения.

Мультимедийный учебник способе вести с обучаемым такой либо почти такой же диалог, как и преподаватель. В этом учебнике учащийся может увидеть то, что невозможно напечатать на бумаге. Мультимедийный учебник «оживляет» химические молекулы и человеческие органы, позволяя увидеть их такими, какие они есть в реальности, а не в виде условных схем и рисунков. И, что немаловажно в наше время, иллюстративные файлы мультимедийных пособий могут в ряде случаев вполне успешно заменить дорогостоящие коллекции реактивов и препаратов, т.е. принести прямую экономическую выгоду.

Мультимедиа средства – это комплекс аппаратных и программных средств, позволяющих человеку общаться с компьютером, используя самые разные, естественные для себя среды: звук, видео, графику, тексты, анимацию. В широком смысле термин «мультимедиа» означает спектр информационных технологий, использующих различные программные и технические средства с целью наиболее эффективного воздействия на пользователя (ставшего одновременно и читателем, и слушателем, и зрителем).

Одно из самых широких областей применения технология мультимедиа получила в сфере образования, поскольку средства информатизации, основанные на мультимедиа способны, в ряде случаев, существенно повысить эффективность обучения. Экспериментально установлено, что при устном изложении материала обучаемый за минуту воспринимает и способен переработать до одной тысячи условных единиц информации, а при «подключении» органов зрения до 100 тысяч таких единиц.

Положительных аспектов использования информационных и телекоммуникационных технологий в образовании достаточно много. Отрицательные аспекты:

- свертывание социальных контактов;

- сокращение социального взаимодействия и общения, индивидуализм; Индивидуализация ограничивает живое общение учителей и обучаемых, учащихся между собой, предлагая им общение в виде «диалога с компьютером». Обучаемый не получает достаточной практики диалогического общения, формирования и формулирования мысли на профессиональном языке.

- сложные способы представления информации отвлекают учеников от изучаемого материала. Если учащемуся одновременно демонстрируют информацию разных типов, он отвлекается от одних типов информации, чтобы уследить за другими, пропуская важную информацию.

- чрезмерное и неоправданное использование компьютерной техники негативно отражается на здоровье всех участников образовательного процесса.

Средства виртуальной реальности будут развиваться к тому, чтобы воздействовать на как можно больше органов чувств человека. Например, уже сейчас братьями Латыповыми разработана «виртуальная сфера», которая вращается, имитируя передвижение человека в виртуальном мире – таким образом, его движение требует реальных мускульных усилий, а не простого нажатия кнопки или поворота джойстика. Существую проекты, предполагающие насыщение виртуальной реальности соответствующими обстановке запахами.

1. **Почтовые системы. Электронные адреса. Приложение OutlookExpress, TheBat!**

Электронная почта (анг. e-mail,от англ. electronic mail) – технология и предоставляемые ею услуги по пересылке и получению электронных сообщений по компьютерной сети.

Достоинством электронной почты являются: легко воспринимаемые и запоминаемые человеком адреса вида имя\_пользователя@имя\_домена; возможность передачи как простого текста, так и форматированного, а также произвольных файлов; достаточно высокая надежность доставки сообщения.

Недостатки электронной почты: наличие такого явления, как спам (массовые рекламные и вирусные рассылки); теоретическая невозможность гарантированной доставки конкретного письма; возможные задержки доставки сообщения (до нескольких суток), ограничения на размер одного сообщения и на общий размер в почтовом ящике.

В настоящее время любой начинающий пользователь может завести свой бесплатный электронный почтовый ящик, достаточно зарегистрироваться на одном из интернет порталов.

Почтовая система – это технология, предназначенная для работы с e-mail сообщениями на сайте.

Общепринятым в мире протоколом обмена электронной почтой является SMTP (Simple mail transfer protocol – простой протокол передачи почты). Почта передается между узлами с использованием программ пересылки почты (напр. OutlookExpress, TheBat!)

Внутри заданной почтовой системы (обычно находящейся в рамках одной организации) может быть множество почтовых серверов, выполняющих как пересылку почты внутри организации, так и другие, связанные с электронной почтой задачи: фильтрацию спама, проверку вложений антивирусом, обеспечение автоответа, архивация входящей/исходящей почты.

Адрес электронной почты – запись, однозначно идентифицирующая почтовый ящик, в который следует доставить сообщение электронной поты.

Адрес состоит из двух частей, разделенных символом «@». Левая часть указывает имя почтового ящика, часто оно совпадает с логином пользователя. Правая часть адреса указывает доменное имя того сервера, на котором расположен почтовый ящик.

ОЕ – программа для работы с электронной почтой и группами новостей компании Майкрософт. Поставляется в составе операционных систем Windows, а также вместе с браузером Internet Explorer. Название ОЕ предполагает, что эта программа является облегченной версией Microsoft Outlook – органайзера от Майкрософт, который также содержит функции работы с электронной почтой. На самом деле, между этими двумя программами мало общего. Кроме того, Outlook, в отличие от ОЕ, до версии 2007 не имел функцию работы с группами новостей.

ОЕ основана на более раннем программно обеспечении для электронной почты и новостей – пакете Microsoft Internet Mail and News, поставлявшемся с Internet Explorer 3.0.

ОЕ используется как на домашних, так и на офисных компьютерах, но она более удобна для домашних пользователей, которые открывают электронную почту посредством выхода в интернет.

ОЕ работает фактически с любой стандартной Интернет системой:

-простой протокол почтовой передачи (SMTP);

- протокол почтового офиса 3 (POP3);

- протокол Интернет доступа к электронной почте (IMAP).

ОЕ позволяет подобрать фон и графику для сообщений. Встроенные шаблоны предоставляют возможность иллюстрировать сообщения.

ТВ – платная программа для работы с электронной почтой для ОС Windows. Разрабатывается молдавской компанией RITLabs. Программа ТВ популяра среди российских пользователей и пользователей из бывших республик СССР.

Имеет довольно развитую систему фильтрации и сортировки сообщений, а также систему для подключения дополнительных модулей расширения (плагинов), предназначенных (в случае, если это требуется) для интеграции программы защиты от вирусов и спама различных производителей. Необходимые плагины могут поставляться вместе с антивирусом или загружаться с сайта разработчиков этого модуля.

Поддерживает протоколы: SMTP. POP3, IMAP. Поддерживает большое число кодировок. Имеются механизмы для фильтрации сообщений, их автоматической обработки, шаблоны и возможности для организации списков рассылки.

Также в ТВ имеется возможность резервного копирования почтовых сообщений или папки, адресной книги и настроек по запросу пользователя в автоматическом режиме по расписанию. При этом возможна защита резервной копии паролем и добавление комментариев.

Программа может импортировать сообщения и адресную книгу из баз данных других приложений.