Самостоятельная работа №1

***Тема**: «Системная плата»*

***Задание**: Зарисуйте рисунок и распишите назначение шин (на рисунке обозначены .)*

Рис. 1.3. Логическая схема системной платы

новки оперативной памяти, а также контроллеров внешних устройств.

Пропускная способность. Быстродействие устройства зависит от тактовой частоты тактового генератора (обычно измеряется в мегагерцах — МГц) и разрядности, т. е. количества битов данных, которые устройство может обрабатывать или передавать одновременно (измеряется в битах). Дополнительно в устройствах используется внутреннее умножение частоты с разными коэффициентами.

Соответственно, скорость передачи данных (пропускная способность) соединяющих эти устройства шин также должна различаться. Пропускная способность шины данных (измеряется в бит/с) равна произведению разрядности шины (измеряется в битах) и частоты шины (измеряется в Гц = 1/с):

Пропускная способность шины =
= Разрядность шины × Частота шины.

Северный и южный мосты. Для согласования тактовой частоты и разрядности устройств на системной плате устанавливаются специальные микросхемы (их набор называется чипсетом), включающие в себя контроллер оперативной памяти и видеопамяти (так называемый северный мост) и контроллер периферийных устройств (южный мост).

Частота процессора. Северный мост обеспечивает обмен данными с процессором, оперативной памятью и видеопамятью. Частота процессора в несколько раз больше, чем базовая частота магистрали (иногда ее называют шиной FSB от англ. FrontSide Bus). Например, в наиболее быстрых компьютерах (2006 год) частота шины FSB составляет 266 МГц, коэффициент умножения частоты 14, следовательно, частота процессора 266 МГц × 14 ≈ 3,7 ГГц.

Системная шина. Между северным мостом и процессором данные передаются по системной шине с частотой, которая в четыре раза больше частоты шины FSB. Таким образом, процессор может получать и передавать данные с частотой 266 МГц × 4 = 1064 МГц. Так как разрядность системной шины равна разрядности процессора и составляет 64 бита, то пропускная способность системной шины равна:

64 бит × 1064 МГц = 68 096 Мбит/с ≈
≈ 66 Гбит/с ≈ 8 Гбайт/с.

Шина памяти. Обмен данными между процессором и оперативной памятью производится по шине памяти, частота которой может быть меньше, чем частота шины процессора. Например, частота шины памяти может составлять 533 МГц, т. е. оперативная память получает данные в два раза реже, чем процессор. Так как разрядность шины памяти равна разрядности процессора и составляет 64 бита, то пропускная способность шины памяти равна:

64 бит × 533 МГц = 34 112 Мбит/с ≈
≈ 33 Гбит/с ≈ 4 Гбайт/с.

Шины AGP и PCI Express. По мере усложнения графики приложений требования к быстродействию шины, связывающей видеопамять с процессором и оперативной памятью, возрастают. Для подключения видеоплаты к северному мосту может использоваться 32-битовая шина AGP (Accelerated Graphic Port — ускоренный графический порт). Эта шина первоначально передавала данные с частотой 66 МГц, в настоящее время возможно использование шины AGP×8, частота которой 66 МГц × 8 = 528 МГц. В этом случае пропускная способность шины видеоданных составляет:

32 бит × 528 МГц = 16 896 Мбит/с =
= 16,5 Гбит/с ≈ 2 Гбайт/с.

В настоящее время для подключения видеоплаты к северному мосту все большее распространение получает шина PCI

Express (Peripherial Component Interconnect bus Express — ускоренная шина взаимодействия периферийных устройств). Пропускная способность этой шины значительно выше пропускной способности PCI и AGP.

К видеоплате с помощью аналогового разъема VGA (Video Graphics Array — графический видеоадаптер) или цифрового разъема DVI (Digital Visual Interface — цифровой видеоинтерфейс) подключается электронно-лучевой или жидко- кристаллический монитор или проектор.

Шина PCI. К северному мосту подключается по специальной шине южный мост, к которому, в свою очередь, подключаются периферийные устройства. Шина PCI (Peripherial Component Interconnect bus — шина взаимодействия периферийных устройств) обеспечивает обмен информацией с контроллерами периферийных устройств, которые устанавливаются в слоты расширения системной платы.

Наиболее часто эта шина используется для установки устройств доступа к локальной сети (сетевая карта), глобальной сети Интернет (встроенный модем) и беспроводной сети (сетевой адаптер Wi-Fi, произносится «вай-фай», сокр. от Wireless Fidelity — протокол и стандарт на оборудование для широкополосной радиосвязи).

Разрядность шины PCI может составлять 32 бита или 64 бита, а частота — 33 МГц или 66 МГц. Таким образом, максимальная пропускная способность шины PCI составляет:

64 бит × 66 МГц = 4224 Мбит/с = 528 Мбайт/с.

Шина IEEE 1394 (другие названия FireWire, i-Link). Последовательная высокоскоростная шина, предназначенная для обмена цифровой информацией между компьютером и цифровыми устройствами (цифровыми видеокамерами, DVD-плеерами и др.) без потери качества изображения и звука. (Эту функцию может выполнять также контроллер IEEE 1394, который подключается к шине PCI.) Скорость передачи данных по этой шине может достигать 200 Мбайт/с и более.

Шина ATA. Устройства внешней памяти (жесткие диски, CD- и DVD-дисководы) подключаются к южному мосту по шине ATA (англ. Advanced Technology Attachment — шина подключения накопителей). Ранее использовалась параллельная шина PATA (англ. Parallel ATA), скорость передачи данных по которой может достигать 133 Мбайт/с. В настоящее время широкое распространение получила последовательная шина SATA (англ. Serial ATA), скорость передачи данных по которой может достигать 300 Мбайт/с.

Шина USB. Для подключения принтеров, сканеров, цифровых камер и других периферийных устройств обычно используется шина USB (Universal Serial Bus — универсальная последовательная шина). Эта шина обладает пропускной способностью до 60 Мбайт/с и обеспечивает подключение к компьютеру одновременно нескольких периферийных устройств (принтер, сканер, цифровая камера, Web-камера, модем и др.).

Клавиатура и мышь. Клавиатура и мышь подключаются с помощью порта PS/2 или шины USB (в том числе с помощью беспроводного адаптера).

Звук. К южному мосту может подключаться интегрированная в системную плату микросхема, которая обеспечивает обработку цифрового звука (эту функцию может выполнять также звуковая плата, которая подключается к шине PCI). С помощью аудиоразъемов к системной плате могут подключаться микрофон, колонки или наушники.

Самостоятельная работа №2
Тема: «Логическая структура гибкого и жесткого дисков»

Задание:

1. Выписать определения:

из текста «Дискеты»:

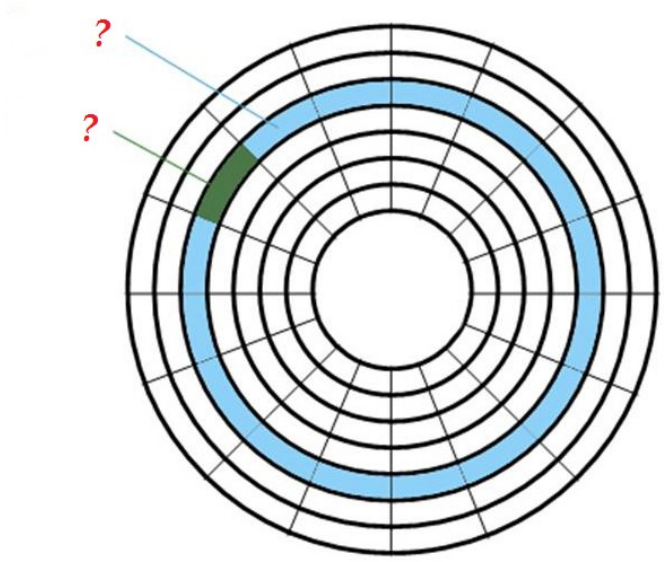
- Дисковод
- Форм-фактор
- Дорожка
- Сектор
- Кластер
- Файл
- Фрагментированный файл

из текста «Жесткие диски»:

- Блин
- Цилиндр
- CHS
- Маркер
- Контрольная сумма
- Низкоуровневое форматирование
- Bad-блок

2. Зарисовать 2 рисунка и подписать обозначения вместо знаков вопроса

Дискеты:



Магнитные диски (МД) относятся к магнитным машинным носителям информации. В качестве запоминающей среды у них используются магнитные материалы со специальными свойствами (с прямоугольной петлей гистерезиса), позволяющими фиксировать два магнитных состояния - два направления намагниченности. Каждому из этих состояний ставятся в соответствие двоичные цифры: 0 и 1. Накопители на МД (НМД) являются наиболее распространенными внешними запоминающими устройствами в ПК. Диски бывают жесткими и гибкими, сменными и встроенными в ПК. Устройство для чтения и записи информации на магнитном диске называется *дисководом*.

Все диски: и магнитные, и оптические характеризуются своим диаметром или, иначе, *форм-фактором.* Наибольшее распространение получили диски с форм-факторами 3,5" (89 мм) и 5,25" (133 мм). Диски с форм-фактором 3,5" при меньших габаритах имеют большую емкость, меньшее время доступа и более высокую скорость чтения данных подряд *(трансфер),* более высокие надежность и долговечность.

Информация на МД записывается и считывается *магнитными головками* вдоль концентрических окружностей - *дорожек (треков).* Количество дорожек на МД и их информационная емкость зависят от типа МД, конструкции накопителя на МД, качества магнитных головок и магнитного покрытия.

Каждая дорожка МД разбита на *сектора*, размером 128, 256, 512 или 1024 байт, но обычно 512 байт данных. Обмен данными между НМД и ОП осуществляется последовательно целым числом секторов. *Кластер* - это минимальная единица размещения информации на диске, состоящая из одного или нескольких смежных секторов дорожки.

При записи и чтении информации МД вращается вокруг своей оси, а механизм управления магнитной головкой подводит ее к дорожке, выбранной для записи или чтения информации.

Данные на дисках хранятся в *файлах,* которые обычно отождествляют с участком (областью, полем) памяти на этих носителях информации.

Файл - это именованная область внешней памяти, выделенная для хранения массива данный.

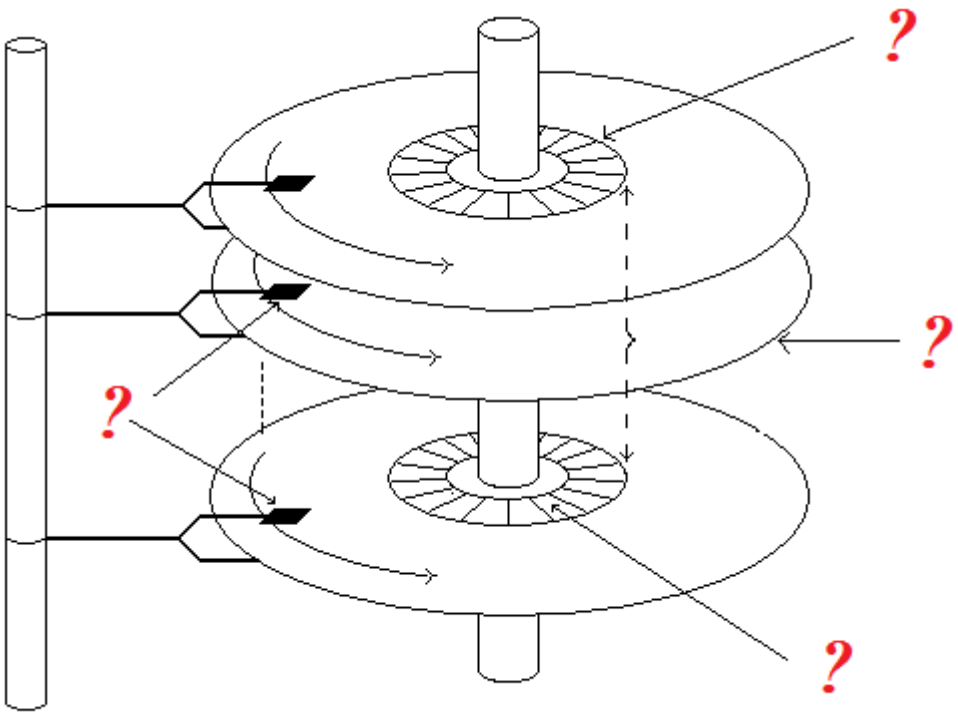
Поле памяти создаваемому файлу выделяется кратным определенному количеству кластеров. Кластеры, выделяемые одному файлу, могут находиться в любом свободном месте дисковой памяти и необязательно являются смежными. Файлы, хранящиеся в разбросанных по диску кластерах, называются *фрагментированными.*

Жесткие диски:

В отличие от «гибкого» диска (дискеты), информация в НЖМД записывается на жёсткие (алюминиевые или стеклянные) пластины, покрытые слоем ферромагнитного материала, чаще всего двуокиси хрома — магнитные диски (блины). В НЖМД используется одна или несколько пластин на одной оси.

HDD — устройство блочное, с произвольной выборкой данных. Означает сие, что информация в нем хранится порциями (блоками), записывать/извлекать ее винчестер может не последовательно (как, например, магнитофон, прокручивая ленту), а произвольно обращаясь к любому из блоков. На круглой поверхности диска организовать блочную структуру можно единственным способом: расчертить на ней концентрические окружности, которые будут пересекать радиальные отрезки. Из школьного курса геометрии известно, что часть дуги, ограниченная двумя радиусами, называется сектор. Так вот, именно сектора являются единицей хранения информации на HDD. Концентрические окружности, именуемые дорожки, — место жизни секторов. Головка чтения/записи переходит с дорожки на дорожку в поиске нужного сектора.

А поскольку у диска две поверхности и у многих винчестеров больше чем один диск, то равноудаленные от центра дорожки на обеих поверхностях каждого диска именуются цилиндром.



Чтобы прочитать или записать данные, контроллер HDD должен понять, в каком из цилиндров, какой головкой чтения/записи обратиться к какому сектору. Поэтому адресация в винчестерах и именуется CHS(Cylinder, Head, Sector).

Именно CHS-адресация определяет геометрию диска: число его дорожек (а значит, и цилиндров) и головок чтения/записи. При этом физическая геометрия диска (о которой знает только его контроллер) частенько не совпадает с его логической геометрией (которую видит BIOS компьютера). BIOS и операционная система видят некий абстрактный диск с одинаковым числом секторов на дорожке (63) и условным числом головок (255), а то и вообще без CHS-адресации — в виде линейного адреса, задаваемого 64-разрядным числом.

Как контроллер HDD определяет, что головка чтения/записи находится над тем или иным физическим сектором? Очень просто. Каждый сектор — многослойный магнитный пирог, и данные пользователя хранятся в его сердцевине объемом 512 байт (в нынешнем году разработчики наконец-то порадовали нас дисками с гигантскими 4096-байтными секторами). Начинается каждый сектор специальной магнитной меткой (маркером), прочитав которую контроллер понимает, что он над сектором. Следующие три метки указывают ему адрес этого сектора в формате CHS. Чтобы убедиться, что сектор не поврежден с момента последнего обращения к нему, за адресом следует поле контрольной суммы (CRC, Cyclic redundancy code — циклический избыточный код). После этого следует пустой байт, чтобы контроллер успел подготовиться к чтению или записи данных, за которым следуют сами данные. После их 512 байт добавлены несколько десятков байт избытка для коррекции ошибок алгоритмом ECC (Error-correcting code — код коррекции ошибок). После снова следует поле CRC, теперь уже для контроля целостности данных. И завершает все пустой байт, за которым следует маркер нового сектора.

Создание такой структуры для всех секторов диска производится на заводе и называется низкоуровневое форматирование (low-level formatting).

Первые винчестеры работали с секторами, в буквальном смысле слова «перешагивая» головками чтения/записи с дорожки на дорожку. Шагали они с помощью специального шагового двигателя, каждый такт работы которого смещал головки на строго определенное расстояние. Но ухищрения разработчиков типа зонной записи, когда размеры дорожек стали разными, привели к тому, что от шаговых двигателей пришлось отказаться в пользу сервоприводов с обратной связью. Для их работы используются специальные магнитные сервометки, которые и дают информацию о текущей позиции головок. Располагаются сервометки вдоль радиальных линий, пересекающих дорожки, и образуют сервоформат диска.

За бешено вращающимися дисками и шныряющими над ними головками, спрятанными в темноте и стерильности гермоблока диска, пристально следит его мозг — контроллер. Фактически — это микрокомпьютер, выполняющий параллельно несколько микропрограмм. Одна из них — трансляция адресов блоков данных, поступающих от операционной системы в формат CHS. И этот микрокод — главный. Но и остальные микропрограммы не менее важны. Они выполняют сервисные функции, с помощью которых контроллер старается защитить диск от угрозы появления на его поверхности bad-блоков – повреждённых секторов.

Самостоятельная работа №3

Тема «Эталонная модель OSI»

- Ответьте на следующие вопросы:
  1. Кем и когда была разработана модель OSI/RM?
  2. Чем обусловлена структура модели OSI/RM?
  3. Сколько уровней в модели OSI/RM, как они называются?
  4. Определяет ли эта модель протоколы, используемые на каждом уровне?
- Распишите назначения каждого уровня модели OSI/RM
- Зарисуйте в тетрадь модель OSI/RM с примерами протоколов.

Эталонная модель OSI (за исключением физической среды) показана на рисунке.

Эта модель основана на разработке Международной организации по стандартизации (International Organization for Standardization, ISO) и является первым шагом к международной стандартизации протоколов, используемых на различных уровнях (Day и Zimmerman, 1983). Затем она была пересмотрена в 1995 году (Day, 1995). Называется эта структура эталонной моделью взаимодействия открытых систем ISO (ISO OSI (Open System Interconnection) Reference Model), поскольку она связывает открытые системы, то есть системы, открытые для связи с другими системами. Для краткости мы будем называть эту модель просто «модель OSI».

Модель OSI имеет семь уровней. Появление именно такой структуры было обусловлено следующими соображениями.

1. Уровень должен создаваться по мере необходимости отдельного уровня абстракции.
2. Каждый уровень должен выполнять строго определенную функцию.

3. Выбор функций для каждого уровня должен осуществляться с учетом создания стандартизированных международных протоколов.
4. Границы между уровнями должны выбираться так, чтобы поток данных между интерфейсами был минимальным.
5. Количество уровней должно быть достаточно большим, чтобы различные функции не объединялись в одном уровне без необходимости, но не слишком высоким, чтобы архитектура не становилась громоздкой.

Далее мы обсудим каждый уровень модели, начиная с самого нижнего. Обратите внимание: модель OSI не является сетевой архитектурой, поскольку она не описывает службы и протоколы, используемые на каждом уровне. Она просто определяет, что должен делать каждый уровень. Тем не менее ISO также разработала стандарты для каждого уровня, хотя эти стандарты не входят в саму эталонную модель. Каждый из них был опубликован как отдельный международный стандарт.

Физический уровень
Физический уровень занимается реальной передачей необработанных битов по каналу связи. При разработке сети необходимо убедиться, что когда одна сторона передает единицу, то принимающая сторона получает также единицу, а не ноль. Принципиальными вопросами здесь являются следующие: какое напряжение должно использоваться для отображения единицы, а какое — для нуля; сколько микросекунд длится бит; может ли передача производиться одновременно в двух направлениях; как устанавливается начальная связь и как она прекращается, когда обе стороны закончили свои задачи; из какого количества проводов должен состоять кабель и какова функция каждого провода. Вопросы разработки в основном связаны с механическими, электрическими и процедурными интерфейсами, а также с физическим носителем, лежащим ниже физического уровня.

Уровень передачи данных
Основная задача уровня передачи данных — быть способным передавать «сырые» данные физического уровня по надежной линии связи, свободной от необнаруженных ошибок с точки зрения вышестоящего сетевого уровня. Уровень выполняет эту задачу при помощи разбиения входных данных на кадры, обычный размер которых колеблется от нескольких сотен до нескольких тысяч байт. Кадры данных передаются последовательно с обработкой кадров подтверждения, отсылаемых обратно получателем.
Еще одна проблема, возникающая на уровне передачи данных (а также и на большей части более высоких уровней), — как не допустить ситуации, когда быстрый передатчик заваливает приемник данными. Должен быть предусмотрен некий механизм регуляции, который информировал бы передатчик о наличии свободного места в буфере приемника на текущий момент. Часто подобное управление объединяется с механизмом обработки ошибок.
В широковещательных сетях существует еще одна проблема уровня передачи данных: как управлять доступом к совместно используемому каналу. Эта проблема разрешается введением специального дополнительного подуровня уровня передачи данных — подуровня доступа к носителю.

Сетевой уровень
Сетевой уровень занимается управлением операциями подсети. Важнейшим моментом здесь является определение маршрутов пересылки пакетов от источника к пункту назначения. Маршруты могут быть жестко заданы в виде таблиц и редко меняться. Кроме того, они могут задаваться в начале каждого соединения, например терминальной сессии. Наконец, они могут быть в высокой степени динамическими, то есть вычисляемыми заново для каждого пакета с учетом текущей загруженности сети.

Если в подсети одновременно присутствует слишком большое количество пакетов, то они могут закрыть дорогу друг другу, образуя заторы в узких местах. Недопущение подобной закупорки также является задачей сетевого уровня. В более общем смысле сетевой уровень занимается предоставлением определенного уровня сервиса (это касается задержек, времени передачи, вопросов синхронизации).
При путешествии пакета из одной сети в другую также может возникнуть ряд проблем. Так, способ адресации, применяемый в одной сети, может отличаться от принятого в другой. Сеть может вообще отказаться принимать пакеты из-за того, что они слишком большого размера. Также могут различаться протоколы, и т. д. Именно сетевой уровень должен разрешать все эти проблемы, позволяя объединять разнородные сети.
В широковещательных сетях проблема маршрутизации очень проста, поэтому в них сетевой уровень очень примитивный или вообще отсутствует.

Транспортный уровень
Основная функция транспортного уровня — принять данные от сеансового уровня, разбить их при необходимости на небольшие части, передать их сетевому уровню и гарантировать, что эти части в правильном виде прибудут по назначению. Кроме того, все это должно быть сделано эффективно и таким образом, чтобы изолировать более высокие уровни от каких-либо изменений в аппаратной технологии.
Транспортный уровень также определяет тип сервиса, предоставляемого сеансовому уровню и, в конечном счете, пользователям сети. Наиболее популярной разновидностью транспортного соединения является защищенный от ошибок канал между двумя узлами, поставляющий сообщения или байты в том порядке, в каком они были отправлены. Однако транспортный уровень может предоставлять и другие типы сервисов, например пересылку отдельных сообщений без гарантии соблюдения порядка их доставки или одновременную отправку сообщения различным адресатам по принципу широковещания. Тип сервиса определяется при установке соединения. (Строго говоря, полностью защищенный от ошибок канал создать невозможно. Говорят лишь о таком канале, уровень ошибок в котором достаточно мал, чтобы ими можно было пренебречь на практике.)
Транспортный уровень является настоящим сквозным уровнем, то есть доставляющим сообщения от источника адресату. Другими словами, программа на машине-источнике поддерживает связь с подобной программой на другой машине при помощи заголовков сообщений и управляющих сообщений. На более низких уровнях для поддержки этого соединения устанавливаются соединения между всеми соседними машинами, через которые проходит маршрут сообщений.

Сеансовый уровень
Сеансовый уровень позволяет пользователям различных компьютеров устанавливать сеансы связи друг с другом. При этом предоставляются различные типы сервисов, среди которых управление диалогом (отслеживание очередности передачи данных), управление маркерами (предотвращение одновременного выполнения критичной операции несколькими системами) и синхронизация (установка служебных меток внутри длинных сообщений, позволяющих после устранения ошибки продолжить передачу с того места, на котором она оборвалась).

Уровень представления
В отличие от более низких уровней, задача которых — достоверная передача битов и байтов, уровень представления занимается по большей части синтаксисом и семантикой передаваемой информации. Чтобы было возможно общение компьютеров с различными представлениями данных, необходимо преобразовывать форматы данных друг в друга, передавая их по сети в неком стандартизированном виде. Уровень представления занимается этими преобразованиями, предоставляя возможность определения и изменения структур данных более высокого уровня (например, записей баз данных).

Прикладной уровень

Прикладной уровень содержит набор популярных протоколов, необходимых пользователям. Одним из наиболее распространенных является протокол передачи гипертекста HTTP (HyperText Transfer Protocol), который составляет основу технологии Всемирной Паутины. Когда браузер запрашивает веб-страницу, он передает ее имя (адрес) и рассчитывает на то, что сервер будет использовать HTTP. Сервер в ответ отсылает страницу. Другие прикладные протоколы используются для передачи файлов, электронной почты, сетевых рассылок.

Самостоятельная работа №4
Тема «Электронно-цифровая подпись»

1.2. Ответьте в тетради на вопросы:

- Что такое ЭЦП?
- Какие условия применения определяет закон о ЭЦП?
- Что обязательно содержит ЭЦП?
- Какие виды ЭЦП существуют?
- Что такое присоединённая электронная подпись?
- Что такое отсоединённая электронная подпись?
- Что такое электронная подпись внутри данных?
- Из каких частей состоит ЭЦП?
- Какие криптографические ключи бывают?
- Где можно получить ЭЦП?
- Из каких этапов состоит процедура получения ЭЦП?
- Где может применяться ЭЦП?

1.3. Зарисуйте схему передачи информации при помощи ЭЦП.

Самый обычный вопрос, который задаётся человеком, впервые столкнувшимся с необходимостью использования электронной подписи, звучит примерно так: «А зачем мне вообще электронная подпись? И нужна ли?»

Электронная подпись может использоваться в нескольких ипостасях. Закон «Об электронной подписи» определяет условия применения электронной подписи как ответственной подписи в документе, аналога собственноручной подписи и печати. Подобным образом электронная подпись используется в системах электронного документооборота различного назначения (организационно-распорядительного, кадрового, законотворческого, торгово-промышленного и прочего).

Однако область применения электронной подписи не ограничивается приведенными областями. Сама по себе, электронная подпись – великолепный механизм обеспечения целостности и подтверждения авторства и актуальности любых данных, представленных в электронном виде.

Электронная подпись поможет проверить целостность электронного письма (e-Mail) и убедиться в надёжности отправителя. Однозначно определит автора статьи, опубликованной в Интернете, и укажет дату публикации. Позволит написать собственное мнение о прочитанном документе в Microsoft Word и прикрепить его в виде «стикера» к файлу, не «испортив» сам файл своими пометками, при этом надёжно привязав такой «стикер» к текущему содержимому документа (при изменении текста документа «стикер» сразу обнаружит, что документ изменялся). Оставит «визитную карточку» о действиях, совершённых в электронном мире, подтвердит полномочия и т.п.

Электронная подпись – является мощным средством контроля подлинности информации в электронном виде, обеспечения целостности электронных данных, подтверждения их авторства и актуальности.

Электронная подпись – это информационный объект, создаваемый для подписываемых данных, позволяющий удостовериться в целостности и аутентичности этих данных.

Распространенное мнение об электронной подписи – «это что-то криптографическое» - верно лишь отчасти. Электронная подпись – это формализованная структура, электронный документ, состоящий из набора обязательных и не обязательных реквизитов – атрибутов электронной подписи. В состав обязательных атрибутов как раз и входит криптографическая часть, обеспечивающая надёжную идентификацию подписываемых данных и гарантирует надёжность источника информации о подписавшем.

Кроме криптографической части, электронная подпись обязательно содержит минимальную информацию о подписавшем и некоторую техническую информацию. Для прикладного использования, электронная подпись может содержать дату и время подписания, сведения для дополнительных механизмов проверки подписи, расширенную информацию о подписавшем, его полномочия и отношение к подписываемым данным, комментарии, файлы, графическое изображение собственноручной подписи и другие, функционально востребованные, данные.

Существуют различные виды электронной подписи.

Электронные подписи могут быть присоединены к подписываемым данным, отсоединены от них или находиться внутри данных. Наиболее часто применяют электронные подписи к данным, хранящимся в файлах, а сама подпись относится ко всему содержимому файла.

• Присоединенная электронная подпись

В случае создания присоединенной подписи создается новый файл электронной подписи, в который помещаются данные подписываемого файла. Этот процесс аналогичен помещению документа в конверт и его опечатыванию. Перед извлечением документа следует убедиться в сохранности печати (для электронной подписи в ее правильности). К достоинствам присоединенной подписи следует отнести простоту дальнейшего манипулирования с подписанными данными, т.к. все они вместе с подписями содержатся в одном файле. Этот файл можно копировать, пересылать и т.п. К недостаткам следует отнести то, что без использования средств СКЗИ уже нельзя прочесть и использовать содержимое файла, точно так же, как нельзя извлечь содержимое конверта, не расклеив его.

• Отсоединенная электронная подпись

При создании отсоединенной подписи файл подписи создается отдельно от подписываемого файла, а сам подписываемый файл никак не изменяется. Достоинством отсоединенной подписи является то, что подписанный файл можно читать, не прибегая к СКЗИ. Только для проверки подписи нужно будет использовать и файл с электронной подписью, и подписанный ей файл. Недостаток отсоединенной подписи - необходимость хранения подписанной информации в виде нескольких файлов (подписанного файла и одного или нескольких файлов с подписями). Последнее обстоятельство существенно осложняет применение подписи, так как при любых манипуляциях с подписанными данными требуется копировать и передавать несколько независимых файлов.

• Электронная подпись внутри данных

Применение электронной подписи этого вида существенно зависит от приложения, которое их использует, например электнонная подпись внутри документа Microsoft Word или Acrobat Reader. Вне приложения, создавшего электронную подпись, без знания структуры его данных проверить подлинность частей данных, подписанных электронной подписью затруднительно.

Электронная цифровая подпись состоит из трех частей:

1. Сертификат
2. Открытый ключ
3. Закрытый ключ

Ключи, как правило, состоят из закодированных символов, а в сертификате находится краткая информация о владельце.

Криптографическая защита информации

При помощи криптографической защиты реализуются конфиденциальность (невозможность прочтения посторонними) и аутентичность (целостность, подлинность, авторство и не отказуемость от него) информации.

Особенностью современной криптографической защиты информации является тот факт, что общедоступность алгоритмов, по которым преобразовывается информация, не влияет на

степень защищённости данных. Криптографические ключи различаются согласно алгоритмам, в которых они используются.

- **Симметричные ключи** — ключи, используемые в симметричных алгоритмах шифрования. Главное свойство симметричных ключей: для выполнения как прямого, так и обратного криптографического преобразования (шифрование - расшифровывание) необходимо использовать один и тот же ключ. С одной стороны, это обеспечивает более высокую конфиденциальность сообщений, с другой стороны, создаёт проблемы распространения ключей в системах с большим количеством пользователей.
- **Асимметричные ключи** — ключи, используемые в асимметричных алгоритмах. Вообще говоря, они являются ключевой парой, поскольку всегда состоят из двух связанных друг с другом ключей:
    - **Закрытый (секретный) ключ** — ключ, известный только своему владельцу. Только сохранение пользователем в тайне своего закрытого ключа гарантирует невозможность подделки злоумышленником документа и электронной подписи от имени заверяющего.
    - **Открытый (публичный) ключ** — ключ, который может быть опубликован и используется для проверки подлинности подписанного документа, а также для предупреждения мошенничества со стороны заверяющего лица в виде отказа его от подписи документа.

Главное свойство ключевой пары: по секретному ключу легко вычисляется открытый ключ, но по известному открытому ключу практически невозможно вычислить секретный.

Перед тем как практически начать применять **электронную подпись** в своей работе, надо создать файлы сертификата и закрытого ключа. Сертификат будет использоваться для проверки подлинности данных подписанных электронной подписью любым человеком, использующим эти данные. А закрытый ключ нужен человеку для формирования электронной подписи подписываемых им данных. При создании сертификатов и ключей используется специальные криптографические программы, которые в принципе есть в составе операционной системы любого компьютера.

Однако, доверять полученному таким образом сертификатам могут только люди, работающие на этом компьютере. Для того чтобы создать и в дальнейшем использовать сертификат, которому будут доверять все, кто будет проверять подлинность электронной подписи, нужна определенная организация, которая обеспечит нормативную, организационную и правовую основу использования выпущенных ею сертификатов. Такой организацией является Удостоверяющий Центр.

1. Договор с Удостоверяющим центром.

Электронная подпись аналогична подписи человека, а для того чтобы убедиться в подлинности документов, подписываемых человеком, любая организация отправляет его сначала к нотариусу, который проверив дееспособность человека удостоверяет его собственноручную подпись на самых различных документах.

Конечно, организация, установив соответствующее программное обеспечение, может организовать собственный Удостоверяющий центр, но при этом следует иметь ввиду, что электронная подпись, наносимые работниками организации, не смогут иметь юридическое значение за пределами этой организации.

Поэтому точно так же, как и при обращении к нотариусам, следует пользоваться услугами внешних аттестованных удостоверяющих центров. Подписав договор с Удостоверяющим Центром организация может получать от него сертификаты для своих работников, которые будут пользоваться электронную подпись.

2. Создание закрытого ключа и получение сертификата.

В процессе создания сертификата каждому из таких работников будет сгенерирован закрытый ключ. Процедура создания ключей может выполняться по-разному.

Ключи могут создаваться в Удостоверяющем центре и передаваться пользователям вместе с сертификатом. Ключи могут создаваться и на рабочем месте пользователя в организации, а открытая часть ключа пересылаться в Удостоверяющий центр для последующего изготовления сертификата.

И ключ, и сертификат хранятся в файлах. Для того, чтобы никто, кроме владельца подписи, не мог воспользоваться закрытым ключом, его обычно записывают на съемный носитель ключа. Его также как банковскую карточку для дополнительной защиты снабжают PIN кодом. И точно также как при операциях с картой, перед тем как воспользоваться ключом для создания электронной подписи надо ввести правильное значение PIN кода.

Именно надежное сохранение пользователем своего закрытого ключа гарантирует невозможность подделки злоумышленником документа и электронной подписи от имени заверяющего документ подписанта.

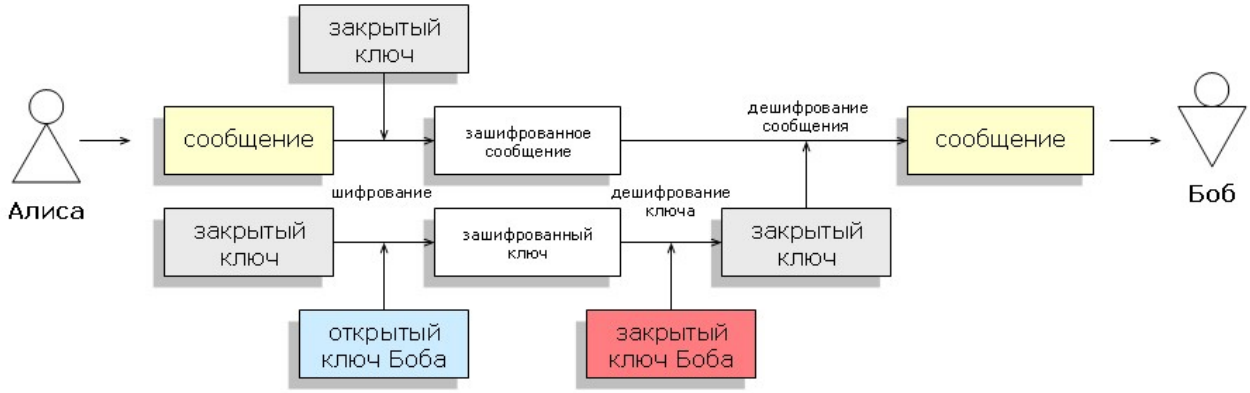
Сертификат содержит всю необходимую информацию для проверки электронной подписи. Данные сертификата открыты и публичны. Поэтому обычно сертификаты хранятся в хранилище операционной системы (в каждом компьютере, в общем сетевом хранилище, в базе данных и т.п.). Конечно, все сертификаты всегда хранятся и в Удостоверяющем центре, точно так же, как и нотариус хранит всю необходимую информацию о человеке, выполнившем у него нотариальное действие.

Получение работником организации закрытого ключа, обеспечение его сохранности и действия с ним обычно регламентируется приказом по организации с утверждением инструктивных материалов. В них регламентируется порядок выпуска сертификатов, применение ключей для подписания документов, получение, замену, сдачу закрытого ключа работниками, и действия выполняемые при компрометации ключа. Последние аналогичны действиям выполняемым при потере банковской карты.

3. Установка криптопровайдера.

Создание электронной подписи представляет собой сложную математическую процедуру и ее выполняют специальные программы – криптопровайдеры. В современных операционных системах криптопровайдеры уже включены в их состав.

Однако в ряде случае законодательство требует применение сертифицированных государственными органами криптопровайдеров. В этом случае их придется покупать и устанавливать на всех машинах, на которых будут подписываться или проверяться электронная подпись. Создание же ключей и получение сертификатов будет возможно только после установки соответствующих криптопровайдеров, так как они будут использоваться в процессе создания ключей и дальнейших процессов формирования и проверки электронной цифровой подписи.



Для реализации механизма взаимного доверия участников обмена удостоверяющий центр имеет центр сертификации, который:

- изготавливает сертификаты открытых ключей;
- создает ключи по обращению участников информационной системы с гарантией сохранения в тайне закрытого ключа;

- приостанавливает и возобновляет действие сертификатов открытых ключей, а также аннулирует их;
- ведет реестр сертификатов открытых ключей, обеспечивает его актуальность и возможность свободного доступа к нему участников информационных систем;
- проверяет уникальность открытых ключей в реестре сертификатов ключей подписей и архиве удостоверяющего центра;
- выдает сертификаты открытых ключей в форме документов на бумажных носителях и (или) в форме электронных документов с информацией об их действии;
- осуществляет по обращениям пользователей сертификатов открытых ключей подтверждение подлинности электронной подписи в электронном документе в отношении выданных им сертификатов открытых ключей;
- может предоставлять участникам информационных систем иные связанные с использованием электронных подписей услуги.

Электронная подпись может применяться в разных областях:

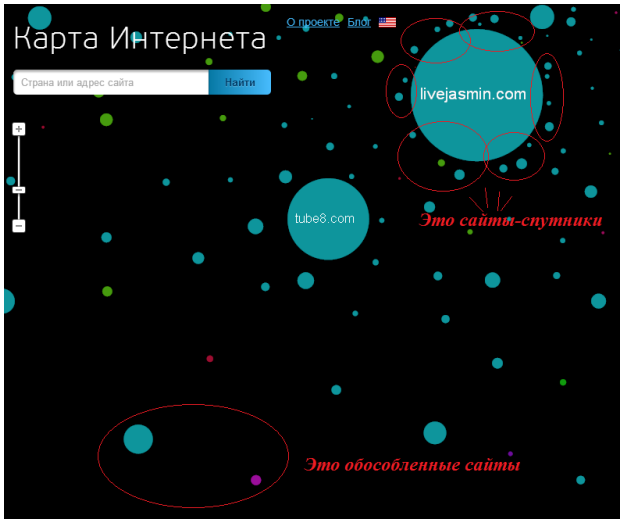
1. электронная подпись может быть использована как ответственная подпись на электронном документе – то есть в качестве аналога собственноручной подписи и/или печати на бумажном документе. В частности, в этой ипостаси электронная подпись используется в системах электронного документооборота разного назначения.
2. Точно также электронная подпись широко используется для подписи программ или отдельных модулей, чтобы пользователь компьютера, загружая эти программы из Интернета, и используя их в работе, мог быть убежден в надежности и корректности их работы и надежности источника получения этих программ.
3. Электронная подпись – это очень надежный инструмент, который позволяет, как установить авторство, так и подтвердить целостность любых данных в электронном виде. Например, полученное вами от, казалось бы, знакомого человека, письмо без электронной подписи может оказаться на самом деле поддельным или содержать искаженную после его отправления информацию. Использование электронной подписи такую возможность исключает. При проверке электронной подписи будет установлено, что документ был изменен после его подписания.
4. При ведении деловой переписки канцеляриями или секретарями разных компаний электронная подпись может служить в качестве «конверта» - на одном конце письмо запечатывают с помощью электронной подписи, а на финише получатель «вскрывает» конверт, предварительно убедившись в полной неприкосновенности и подлинности данных.
5. С помощью электронной подписи можно согласовывать электронные варианты документов (например, договоров) как между различными службами внутри одной организации, так и между разными организациями. В таком случае текст договора будет защищен от несогласованных изменений, а каждая ответственная инстанция должна будет согласовать документ с помощью собственной электронной подписи, подтвердив тем самым свое отношение к нему. Такая подпись безошибочно расскажет не только о том, кто подписал документ, но и укажет дату и время подписи. Если же сотрудник решит отказаться от ответственности за визирование документа или отправку информации в письме, скрепленном его электронной подписью, то электронная подпись легко его уличит. Например, часто договор требуется согласовать с юридическим отделом, бухгалтерией и другими подразделениями компании, и лишь после этого его подпишут руководители обеих сторон. Такое согласование и визирование всеми ответственными службами можно проводить уже сейчас в электронном виде, применяя электронную подпись.

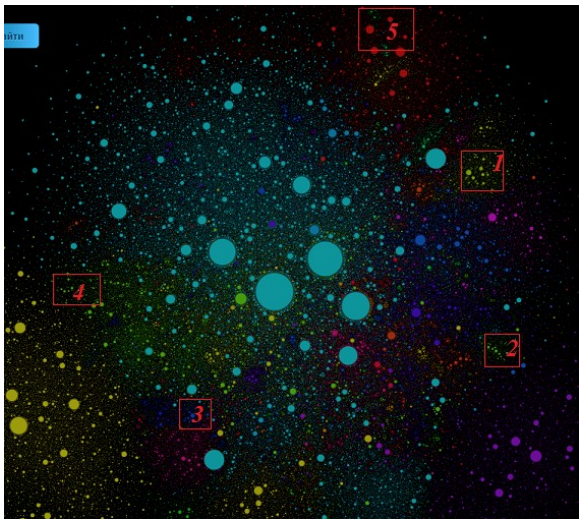
самостоятельная работа №5
Тема «Карта сети Интернет»

1.1. Откройте сайт http://internet-map.net и оцените масштабы сети Интернет.
1.2. Перечислите 5 самых крупных сайтов домена .com (на сайте имеют цвет:)
1.3. Введите названия следующих стран (на английском) в поле поиска в левом верхнем углу и определите цвет страны:

- Япония (Japan)
- Испания (Spain)
- Бразилия (Brazil)
- Канада (Canada)
- Германия (Germany)

1.4. Какой на карте самый крупный обособленный домен? (Отдельная точка на карте не имеющая рядом соседей)





1.5. Спутниками каких сайтов являются:

- gmail.ru
- sevenply.de
- qqmfz.cn
- coordinadorausa.com
- iha.it

1.6. Каким странам принадлежат выделенные сегменты (рис 2)?
1.7. Перечислите 5 самых крупных сайтов домена .ru
1.8. Сравните число связанных сайтов (сайтов спутников) для порталов vkontakte.ru и odnoklassniki.ru