Аппаратные средства телекоммуникационных систем

Введение в архитектуру процессорных устройств.

Основные понятие архитектуры процессоров

Аппаратные средства телекоммуникационных систем.

Введение в архитектуру процессорных устройств.

Понятие процессор

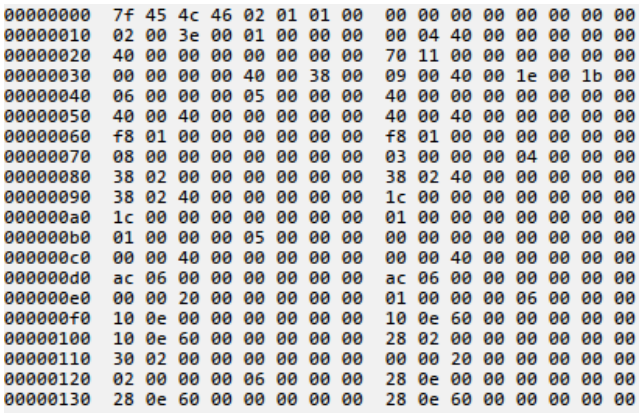
- ***Процессор*** – электронный блок либо интегральная схема (микропроцессор), исполняющая машинные инструкции (код программы), главная часть аппаратного обеспечения компьютера или программируемого логического контроллера.
  - *Устройства типа процессор подчинены т.н.* ***«принципу программного управления»****.*
    - *Процесс реализации функции в устройстве описывается в форме алгоритма, называемого* ***программой****.*

Принцип программного управления.

- любая функция, является последовательностью элементарных действий – **операций**.
- Каждая операция задается **специальной инструкцией или командой**, служащей для настройки процессора на выполнение заданного элементарного действия;
- Программа описывается в терминах команд и логических условий.
- Программа предварительно размещается в памяти устройства, а не вводится команда за командой в процессе его работы.

О машинном коде и языках программирования

- На машинном уровне программа представляет собой набор аппаратно-выполняемых команд – **машинный код**.
  - Примеры таких команд – сложение, умножение, логическое или, перенос значения из одной ячейки памяти в другую.
- *Каждая команда имеет свой кодовый номер и адреса двух ячеек – данных, для выполнения над ними определенного действия.*
  - Такие данные называются операндами.
- Любая команда программы уровня выше машинного (начиная от ассемблера и до современных абстрактных языков) интерпретируется в машинный код для ее выполнения.



```
00000000  7f 45 4c 46 02 01 01 00  00 00 00 00 00 00 00 00
00000010  02 00 3e 00 01 00 00 00  00 04 40 00 00 00 00 00
00000020  40 00 00 00 00 00 00 00  70 11 00 00 00 00 00 00
00000030  00 00 00 00 40 00 38 00  09 00 40 00 1e 00 1b 00
00000040  06 00 00 00 05 00 00 00  40 00 00 00 00 00 00 00
00000050  40 00 40 00 00 00 00 00  40 00 40 00 00 00 00 00
00000060  f8 01 00 00 00 00 00 00  f8 01 00 00 00 00 00 00
00000070  08 00 00 00 00 00 00 00  03 00 00 00 04 00 00 00
00000080  38 02 00 00 00 00 00 00  38 02 40 00 00 00 00 00
00000090  38 02 40 00 00 00 00 00  1c 00 00 00 00 00 00 00
000000a0  1c 00 00 00 00 00 00 00  01 00 00 00 00 00 00 00
000000b0  01 00 00 00 05 00 00 00  00 00 00 00 00 00 00 00
000000c0  00 00 40 00 00 00 00 00  00 00 40 00 00 00 00 00
000000d0  ac 06 00 00 00 00 00 00  ac 06 00 00 00 00 00 00
000000e0  00 00 20 00 00 00 00 00  01 00 00 00 06 00 00 00
000000f0  10 0e 00 00 00 00 00 00  10 0e 60 00 00 00 00 00
00000100  10 0e 60 00 00 00 00 00  28 02 00 00 00 00 00 00
00000110  30 02 00 00 00 00 00 00  00 00 20 00 00 00 00 00
00000120  02 00 00 00 06 00 00 00  28 0e 00 00 00 00 00 00
00000130  28 0e 60 00 00 00 00 00  28 0e 60 00 00 00 00 00
```

Принцип построения ЭВМ

- ***Устройство, объединяющие процессор и периферийные модули называется электронно-вычислительной машиной (ЭВМ)***

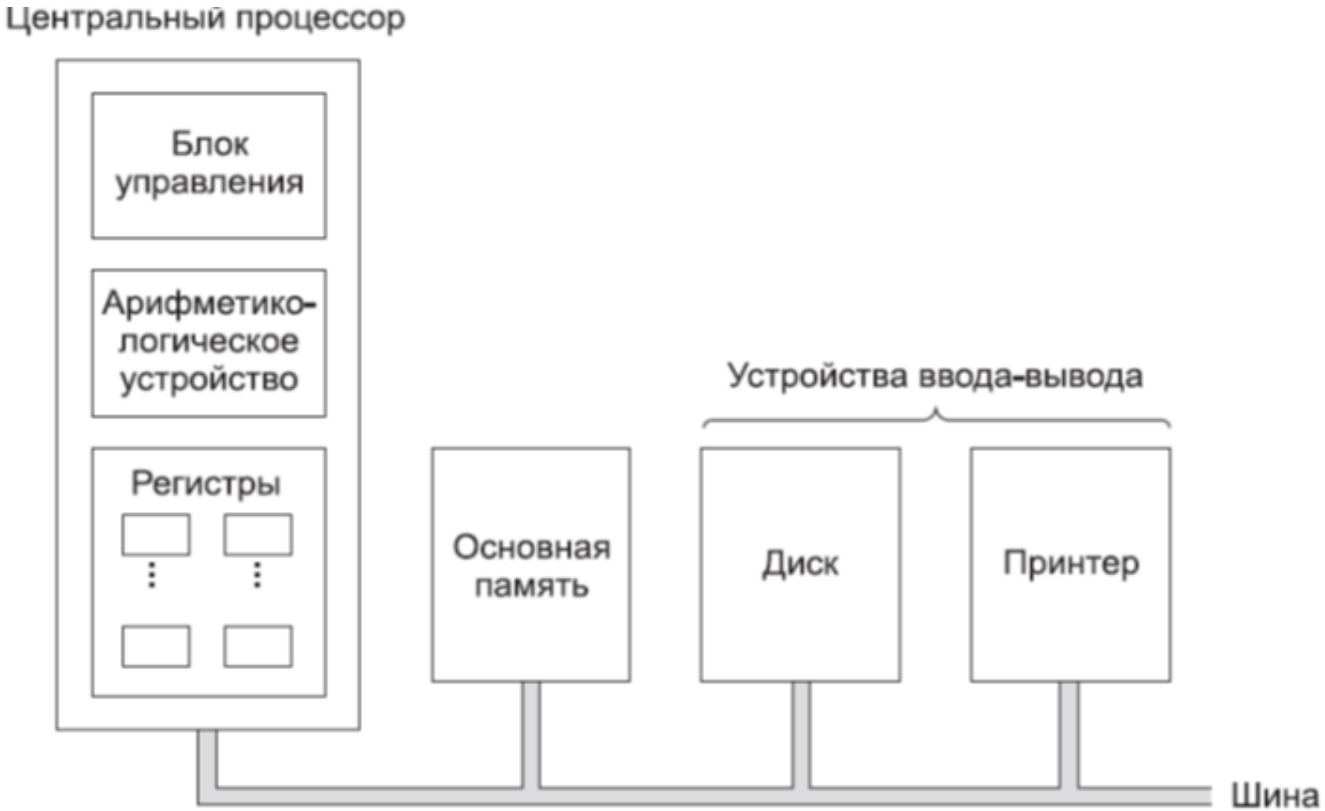


Схема компьютера с одним центральным процессором и двумя устройствами ввода-вывода

Принцип построения ЭВМ

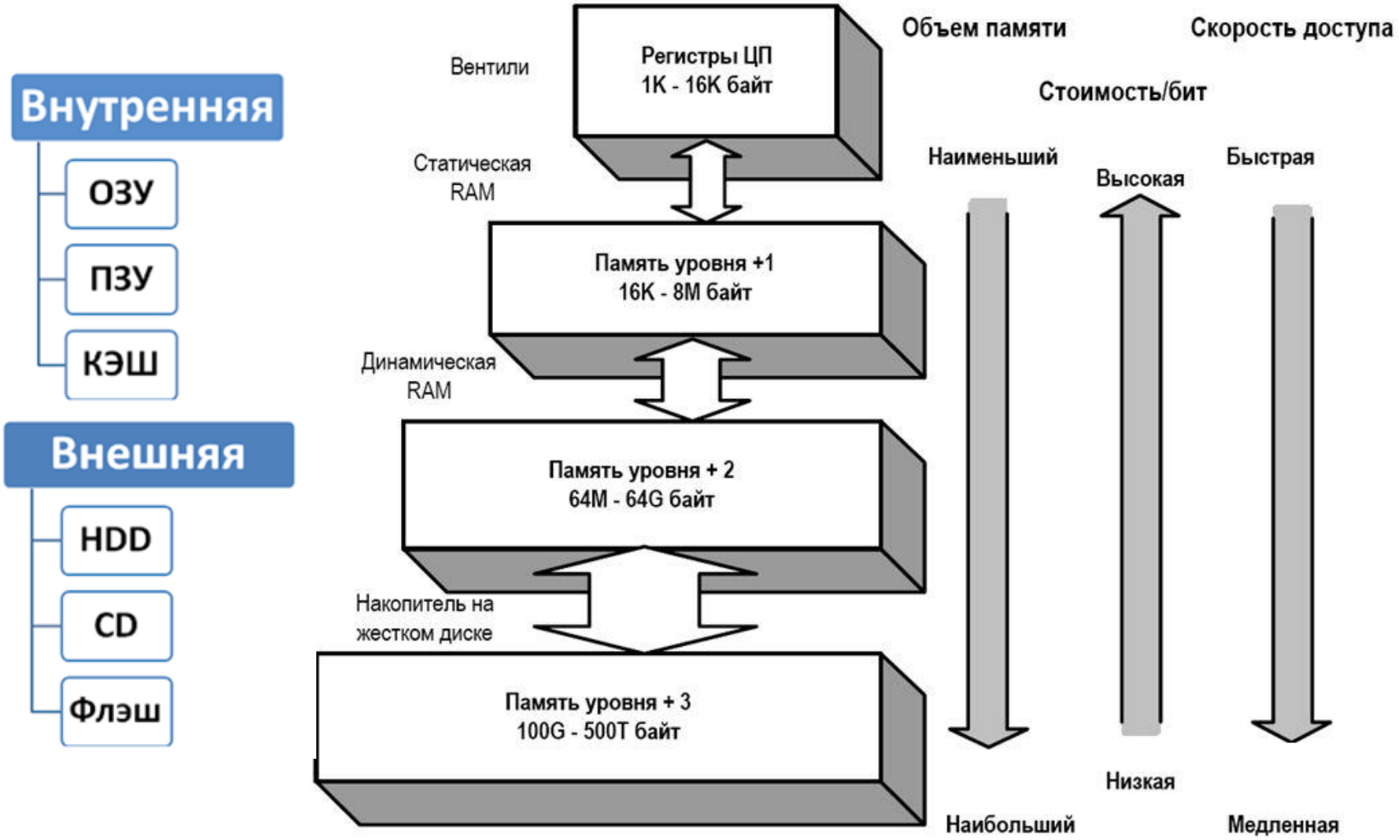
- ***Центральный процессор*** **(АЛУ с блоком устройства управления (УУ))** обладает принцип последовательной передачи управления.
- Набор арифметических, логических и прочих инструкций **АЛУ** насчитывает несколько сотен,
- Процессор имеет **набор регистров в устройстве управления (УУ)**
  - часть регистров доступна для хранения операндов, выполнения действий над ними и формирования адреса инструкций и операндов в памяти.
  - Другая часть регистров используется процессором для служебных (системных) целей,

    доступ к ним может быть ограничен (есть даже программно-невидимые регистры).
- **Все компоненты компьютера представляются для процессора в виде наборов *ячеек памяти* или/и *портов ввода-вывода*,**
  - В ячейки и порты в-в процессор может записывать и/или считывать содержимое.

• *Процессор (один или несколько), память и необходимые элементы, связывающие их между собой и с другими устройствами, называют центральной частью, или ядром, компьютера (или просто центром).*

Иерархия памяти в компьютере

Самая важная характеристика памяти – **латентность** – время доступа к ячейки памяти



Иерархия памяти в компьютере

- ***Оперативная память*** **(ОЗУ)** динамическая память с произвольным доступом.
  - Оперативная память вместе с кэшем всех уровней (в настоящее время — до трех) представляет собой единый массив памяти, доступный процессору для записи и чтения данных.
- ***Постоянная память*** **(ПЗУ)**, из нее можно только считывать команды и данные
- Также ЭВМ имеет некоторые виды специальной памяти (например, видеопамять графического адаптера).
- В любом компьютере есть ***энергонезависимая память***, в которой хранится программа начального запуска компьютера и минимально необходимый набор сервисов (FLASH,**ROM BIOS**).
  - Доступ к внутренней памяти осуществляется по одномерному (линейному) адресу, который представляет собой двоичное число. Доступна для процессора.

Иерархия памяти в компьютере

- ***Внешняя память*** каждая ее ячейка имеет свой адрес внутри *блока*, который, имеет многомерный адрес и может быть считан или записан только целиком.
  - В случае дискового накопителя физический адрес блока является трехмерным — он состоит из номера поверхности (головки), номера цилиндра и номера сектора, но виртуально линейным номером — логическим, адресом блока, а его преобразованием в физический адрес занимается внутренний контроллер накопителя

Периферийные устройства ЭВМ

- ***Устройства хранения данных*** (устройства внешней памяти) — дисковые (магнитные, оптические, магнитооптические), твердотельные (карты, модули и флэш-память). Эти устройства используются для сохранения информации, на энергонезависимых носителях и загрузки этой информации в оперативную память.
- ***Устройства ввода-вывода*** служат для преобразования информации из внутреннего представления компьютера (биты и байты) в форму, понятную ок*ружающим,* и обратно. Под окружающими подразумеваются человек (и другие биологические объекты) и различные технические устройства
- ***Коммуникационные устройства*** служат для передачи информации между компьютерами и/или их частями. Сюда относят модемы (проводные, радио, оптические, инфракрасные...), адаптеры локальных и глобальных сетей.
- ***Консоль.*** *Консолью* компьютера называют его «выступающую часть», обращенную к пользователю. В PC стандартной консолью являются клавиатура (устройство ввода) и дисплей

Классификация ЭВМ

- **Персональные ЭВМ**
  - Настольные персональные компьютеры.
  - Ноутбуки и нетбуки.
  - Однопалатные микрокомпьютеры.
  - Планшетные устройства и смартфоны.
  - Компьютеризированные устройства: фотоаппараты, mp3 плееры, диктофоны, игровые приставки.
- **Серверы**: промышленные серверы, Серверы на базе персональных компьютеров.
- **приемо-передающие устройства**: модемы, точки беспроводного и проводного доступа, устройства беспроводной связи.
- **Межсетевые узлы:** концентраторы, коммутаторы, мосты, шлюзы, маршрутизаторы, межсетевые экраны.
- **Устройства специального назначения.**
  - Бортовые компьютерные системы.
  - Встроенные системы.
  - Диагностические устройства.
  - Контрольно-кассовые аппараты.

Классификация процессоров по видам

- ***Центральные процессоры (CPU). –*** *пример CPU ПК.*
- ***Универсальные микропроцессоры*** используются для построения вычислительных машин и систем связи Такие компьютеры называются контроллерами. (пример Raspberry Pi, Siemens).
- ***Микроконтроллеры (МК)*** используются для управления малогабаритными и дешёвыми устройствами управления и связи они раньше назывались однокристальными микроЭВМ. В микроконтроллерах, в отличие от универсальных микропроцессоров, максимальное внимание уделяется именно габаритам, стоимости и потребляемой энергии.
- ***Сигнальные процессоры (DSP)*** используются для решения задач обработки сигналов. Аппаратная реализация сложных математических операций.
- ***Медийные процессоры*** гибрид DSP и универсальных процессоров и предназначены для обработки аудио сигналов, графики, видеоизображений, а также для решения коммуникационных задач в мультимедиа-компьютерах, игровых приставках, бытовой технике и т.д.

Примеры сопроцессоров

- ***Основные виды сопроцессоров:***
- *Математические сопроцессоры (FPU) -операции с плавающей запятой (имеют 2 ЛУ для мантиссы и экспоненты);*
- *навигационные (с GPS);*
- *Графические (многоядерные, много АЛУ, мало команд другого профиля) ориентация на рендеринг – расчет текстуры по модели;*
- *Коммуникационные (поддержка сетевых интерфейсов и протоколов). Например (Ethernet, или беспроводных, например WiFi и GPRS)*

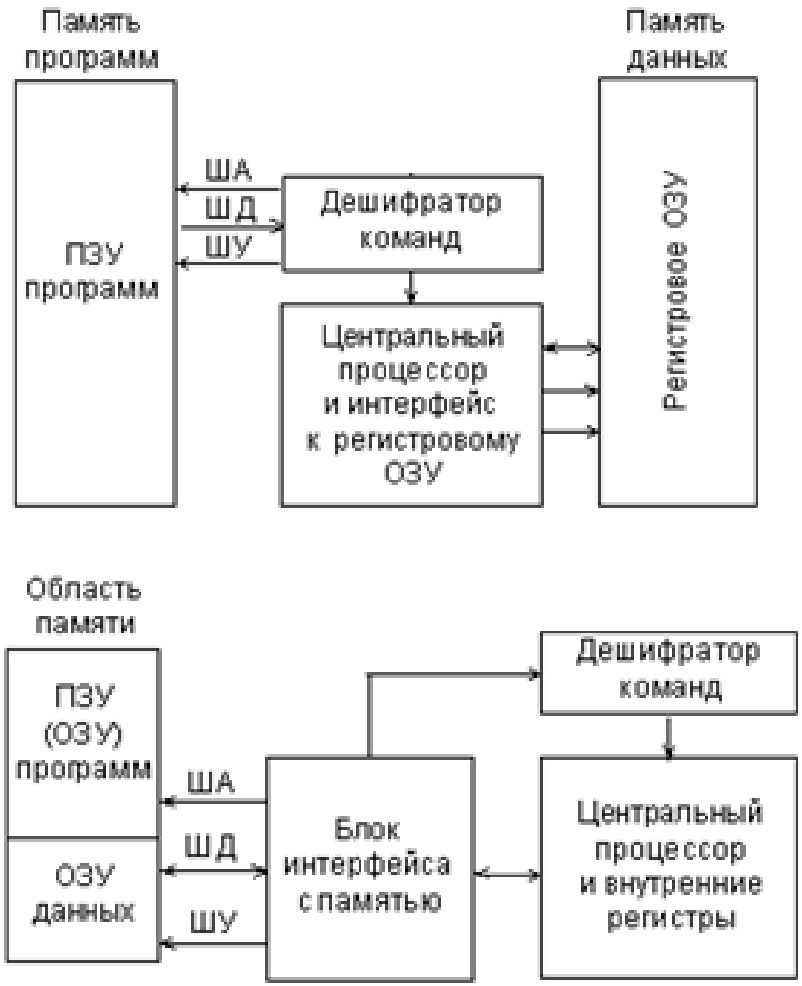
Особенности архитектуры процессоров

Аппаратные средства телекоммуникационных систем.

Введение в архитектуру процессорных устройств.

Архитектуры процессоров. Виды архитектура процессоров

- ***Гарвардская архитектура*** предполагает раздельное использование памяти программ и данных.
- Обычно используют для повышения быстродействия системы за счёт разделения путей доступа к памяти программ и данных.
- Большинство специализированных микропроцессоров (особенно микроконтроллеры) имеют данную архитектуру.
- ***Архитектура фон Неймана*** – предполагает хранение программ и данных в общей памяти.
- Наиболее характерна для процессоров, ориентированных на использование в компьютерах.
- Примером могут служить микропроцессоры семейства x86.



Архитектуры процессоров. Особенности гарвардской архитектуры

- **Применение отдельной небольшой по объему *памяти данных* сокращает длину *команд* и ускоряет поиска информации в *памяти данных*.** Использование единого адресного пространства приводит к увеличению формата *команд* за счет увеличения числа разрядов для адресации операндов.
- Гарвардская архитектура обеспечивает **потенциально более высокую скорость выполнения программы** по сравнению с фон-неймановской **за счет возможности реализации параллельных операций. Выборка следующей команды может происходить одновременно с выполнением предыдущей**, и нет необходимости останавливать процессор на время выборки команды.
- Этот метод реализации операций позволяет обеспечивать выполнение различных команд за одинаковое число тактов, что дает возможность более просто определить время выполнения циклов и критичных участков программы.
- Большинство производителей современных микроконтроллеров используют гарвардскую архитектуру.

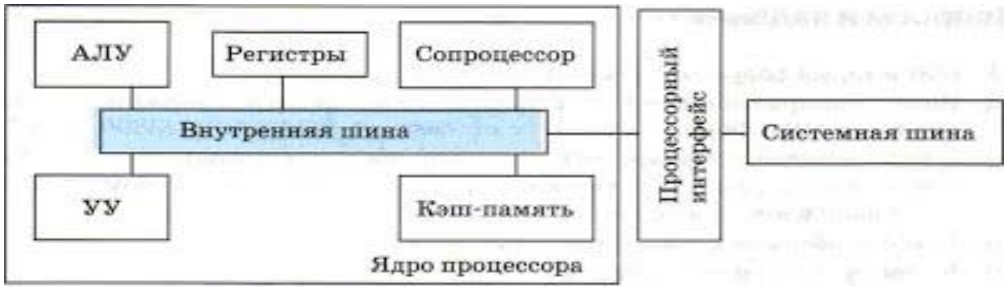
Архитектуры процессоров. Архитектура Фон-Неймана

- **Упрощение устройства процессора**,-обращение к одной общей памяти.
- **Единая область памяти позволяет оперативно перераспределять ресурсы между областями программ и данных**, что повышает гибкость системы.
- **Архитектура фон Неймана последовательная**. Выполняемые действия определяются блоком управления и АЛУ. Центральный процессор выбирает и исполняет команды из памяти последовательно, адрес очередной команды задается «счетчиком адреса» в блоке управления.
- Часто в процессоры встроены **сопроцессоры**, имеющие преимущества при решении определённого рода задач (например, для операций с плавающей запятой).

Блок-схема архитектуры центрального процессора

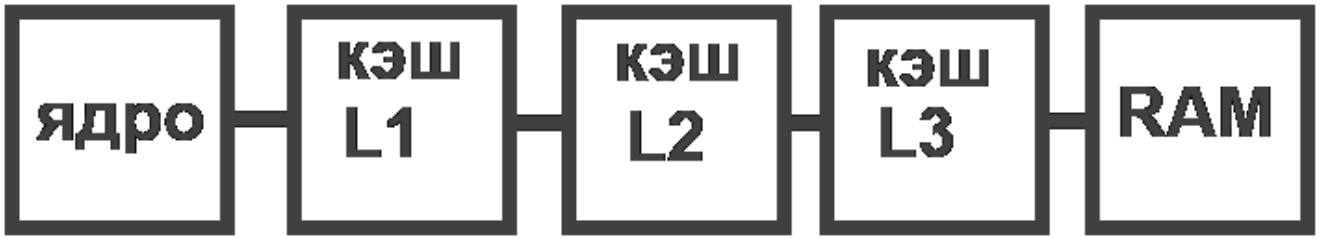
Архитектуры процессоров. Магистральная организация процессов.

- **Магистраль или шина (Bus)** – группа линий передачи информации, объединенных общей функцией.
- **В общем случае у процессору требуется 3 шины – шина адреса, шина данных и шина управления.**
- Для снижения общего количества линий связи магистрали **часто применяется *мультиплексирование*** *шин адреса* и *данных* в разные моменты времени. Для фиксации этих моментов (стробирования) служат специальные сигналы на *шине управления*.
- ***Шина управления (инструкций)*** — это вспомогательная шина по которой передаются **управляющие и служебные сигналы**. Также сигналы с **внешних и внутренних источников**.
- ***Основные функции шины управления - вызов прерываний.***
- На пример, в момент ввода с клавиатуры или достижение определенного значения внутреннего таймера. Предполагается выполнение определённых действий по сигналам прерываний.



Архитектуры процессоров. Кэш память.

- Внутри центрального процессора находится быстрая память небольшого объема для хранения промежуточных результатов и некоторых команд управления – **КЭШ память**.
- Кэш может быть многоуровневый.
  - Часто двухуровневый, для хранения команд и отдельно для хранения данных или трех уровневой с дополнительным уровнем для работы между ядрами.
- Операции чтения и записи с регистрами выполняются очень быстро, поскольку они находятся внутри центрального процессора.
- Кэш-память позволяет держать наиболее часто используемые слова внутри центрального процессора и избегать (медленных) обращений к основной памяти.
  - скорость работы процессора выше скорости операции обращения к памяти и получения от туда данных.
  - За работу Кэш память отвечает специальный контроллер внутри процессора.



Архитектуры процессоров. Регистровая память.

- Каждый процессор для обеспечения гибкости работы имеет набор регистров, отвечающих за определенные настройки процессора (такие как, например, тактовая частота) (**Регистры**).
- Один из самых главных регистров – это **счетчик команд**, в нем указывается, какая по счету последовательная команда должна быть выполнена в настоящее время.
- Также в процессоре имеются регистры, содержащие код текущей команды и регистры операндов для текущей команды.

Архитектуры процессоров. Устройство управления

- **Функции устройства управления (УУ)**
- формирует адрес команды, которая должна быть выполнена
- выдает управляющий сигнал на чтение содержимого соответствующей ячейки запоминающего устройства (ЗУ).
  - Считанная команда передается в УУ.
- По информации, содержащейся в адресных полях команды, УУ формирует адреса операндов и управляющие сигналы для их чтения из ЗУ и передачи в арифметико-логическое устройство (АЛУ).
  - После считывания операндов УУ по коду операции, содержащемуся в команде, выдает в АЛУ сигналы на выполнение операции.
- Полученный результат записывается в ЗУ по адресу приемника результата.
- Признаки результата (знак, наличие переполнения, признак нуля и так далее) поступают в УУ, где записываются в специальный регистр признаков.
- Эта информация может использоваться при выполнении следующих команд программы, например команд условного перехода.

Архитектуры процессоров. Арифметико-логическое устройство (ALU)

- объединяет различные арифметические и логические операции в одном узле. Например, типичное АЛУ может выполнять сложение, вычитание, сравнение величин, операции «И» и «ИЛИ».

АЛУ имеет два регистра операндов
Результат работы АЛУ может быть подан на шины данных или обратно в АЛУ
АЛУ имеет ряд флаг, соответствующих определённым событиям, например переполнению.

Часто к АЛУ добавляют сопроцессор для работы с числами с плавающей запятой

Архитектуры процессоров. Организация наборов команд процессоров.

Программа размещена в памяти команд (ПК). После запуска устройство управления (УУ) начинает выполнять три действия:

1) последовательную выборку команды из памяти команд;
2) декодирование (интерпретацию) кода команды;
3) выполнение операции, соответствующей команде в устройстве обработки (ОУ).

- ***Команда или инструкция*** (Command, Instruction) – двоичный код, служащий для настройки программно-управляемого устройства на выполнение заданной операции.
- ***Система команд*** (Command set) – совокупность всех команд, допустимых для данного программного управляемого устройства.
- ***Программа*** (Program) – последовательность инструкций (команд) и логических условий, реализующих заданный алгоритм.
- **По типам команд процессоры делят на:**
  - ***CISC*** (Complex Instruction Set Computing) с полным на-бором команд;
  - ***RISC*** (Reduced Instruction Set Computing) с сокращенным набором команд;
  - ***MISC*** (Minimal Instruction Set Computer) с минимальным набором команд;
  - ***VLIW (***Very Long Instruction Word) (одна команда выполняется параллельно на нескольких процессорах).

Архитектуры процессоров. CISC система команд

CISC (англ. Complex Instruction Set Computer — «компьютер с полным набором команд») – полная система команд, подразумевает, что все необходимые для машинного языка команды выполняются на аппаратном уровне.

Самый яркий пример CISC архитектуры — это x86 (он же IA-32) и x86_64 (он же AMD64).

- нефиксированная длина команд,
- небольшое число регистров, многие из которых выполняют строго определенную функцию.
- одна команда может быть заменена ей аналогичной, либо группой команд, выполняющих ту же функцию.
- CSIC и RISC процессоры несовместимы.
- CISC система команд исторически появилась первой, по этому большинство процессоров CISC.
  - Процессоры Intel, начиная с процессора 486, содержат RISC-ядро, которое выполняет самые простые (и обычно самые распространенные) команды за один цикл тракта данных, а по обычной технологии CISC интерпретируются более сложные команды. В результате обычные команды выполняются быстро, а более сложные и редкие — медленно.
  - на выполнение даже самой короткой команды из системы CISC обычно тратится 4 такта.

Архитектуры процессоров. RISC система команд

RISC (англ. Reduced Instruction Set Computer — «компьютер с сокращённым набором команд») — архитектура процессора, в котором быстродействие увеличивается за счёт упрощения инструкций декодирование становится более простым, а время выполнения — меньшим.

Первые RISC-процессоры не имели даже инструкций умножения и деления и не поддерживали работу с числами с плавающей запятой.

Примеры RISC-архитектур: PowerPC, серия архитектур ARM (ARM7, ARM9, ARM11, Cortex).

- архитектура имеет постоянную длину команды,
  - Позволяет работать параллельно и конвейером (то есть выполнять больше одной команды за один такт)
- меньшее количество схожих инструкций,
- большее количество регистров.
- содержат набор только простых, чаше всего встречающихся в программах команд (по правилу 20-80)
- Основной недостаток RISC архитектуры — необходимость моделирования сложных команд.
  - Сборка сложных команд производится автоматическая из простых.

Архитектуры процессоров. MISC система команд

MISC (англ. Minimal Instruction Set Computer — «компьютер с минимальным набором команд»).

- более простая архитектура чем RISC, используемая в первую очередь для большего уменьшения итоговой цены и энергопотребления процессора.
- Архитектура MISC строится на стековой вычислительной модели с ограниченным числом команд (примерно 20—30 команд).
  - Может содержать в себе блок RISC, обрабатывающий в себе от 10 базовых команд (+, —, /, *, if, else & etc), из которых формируются более сложные операции над значениями, методом ветвления полученных результатов в ПЗУ.
- Используется в IoT-сегменте и недорогих компьютерах, например, роутерах.
- Недостаток - сложность написания программ под различные процессоры.
  - Все нюансы по подбору методов вычисления и оптимизаций возлагались на плечи программистов.

Архитектуры процессоров. VLIW система команд

VLIW (англ. Very Long Instruction Word — «очень длинная машинная команда») — архитектура процессоров с несколькими вычислительными устройствами

Архитектура VLIW в терминах Intel называется EPIC (на самом деле EPIC имеет отличия в организации параллелизма).

Примеры архитектуры: Intel Itanium (серверные процессоры Intel Core, архитектура IA-64), Эльбрус-3.

- одна инструкция процессора содержит несколько операций, которые должны выполняться параллельно.
  - По сути является архитектурой CISC со своим аналогом спекулятивного исполнения команд, спекуляция выполняется во время компиляции.
- Компиляторы для процессоров этой архитектуры сильно привязаны к конкретным процессорам.
  - Например, в следующем поколении максимальная длина «очень длинной команды» может из условных 256 бит стать 512 бит, и исчезнет совместимость.
  - Ключевым отличием от суперскалярных CISC-процессоров является то, что для них загрузкой исполнительных устройств занимается часть процессора (планировщик), а загрузкой вычислительных устройств для VLIW-процессора занимается компилятор, на что отводится существенно больше времени (качество загрузки и, соответственно, производительность теоретически выше).

Особенности архитектуры современных процессорных систем

Аппаратные средства телекоммуникационных систем.

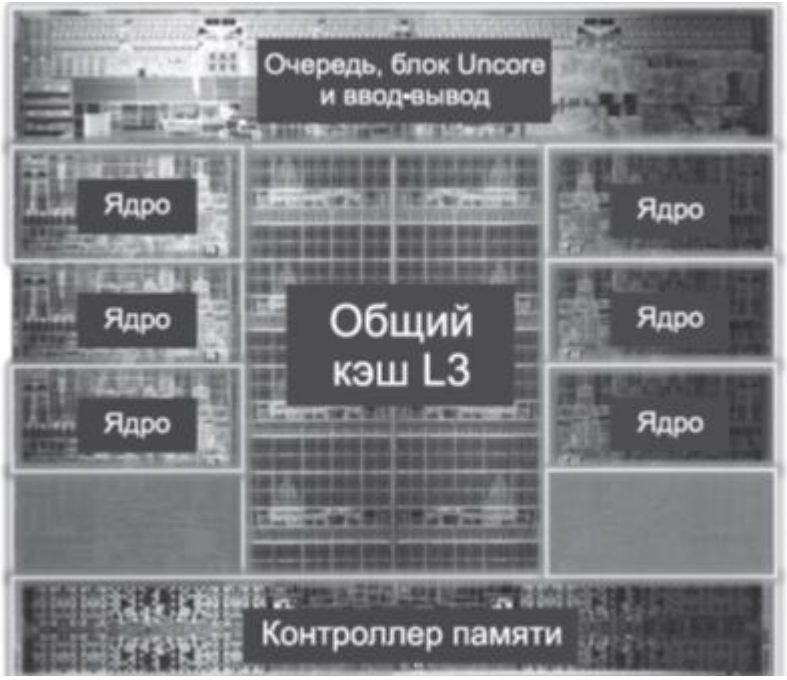
Введение в архитектуру процессорных устройств.

Архитектуры процессоров. Особенности современных архитектур процессоров

- Увеличение количества ядер микропроцессора, коммутация между ядрами.
- Увеличение объема КЭШ памяти и уровней Кэш-а.
- Парализация выполнения команд (Конвейеризированные и суперскалярные архитектуры)
- Спекулятивное выполнение команд.
  - Спекулятивное выполнение команд. Перераспределение команд в пределах одного блока (например цикл или if) и выполнение «тяжелых» команды раньше чем станет известно, понадобится ли она. Такие команды обрабатываются в период ожидания в основной ветке (например ожидания блока расчета float). Недостаток актаки типа Spectra, meltdown и т.п.
- Встроенный контроллер доступа к памяти (MCU) - оптимизация работы с ОЗУ
- Система команд X86-X64 (AMD x64) – расширенная система команд с 64 битной адресацией.
- Параллельное выполнение двух потоков инструкций ядром (hyper threading).
- Производительность зависит от тактовой частоты, IPC и энергопотребления (Instructions Per Clock)
  - IPC количество инструкций, исполняемых CPU за один так, зависит от логической структуры ядра.

Архитектуры процессоров. Примеры. Архитектура современных процессоров Intel

- Каждое ядро имеет собственные кэши 1 и 2 уровня, но также имеется общий кэш 3 уровня (L3), используемый всеми
- *субъядро (uncore)* - компоненты, отвечающие за средства коммуникации :
  - контроллер памяти (memory controller),
  - интерконнект QuickPath (QuickPath links, QPI у INTEL, HyperTransport у AMD), последовательная кэш-шина типа точка-точка для соединения процессоров и для передачи данных между процессором и системной платой.
  - управления энергопитанием (powermanagement),
  - встроенный графический контроллер.



Микросхема Intel Core i7-3960X. Подложка имеет размеры 21×21 мм и содержит 2,27 миллиарда транзисторов

- Некоторые процессоры содержат блок - *Системный агент (System agent)* - содержит многоканальный контроллер памяти, «мосты» PCI-Express, DMI, дисплейные интерфейсы, блок аппаратного декодирования видео.

Архитектуры процессоров. Примеры. Архитектура современных графических процессоров

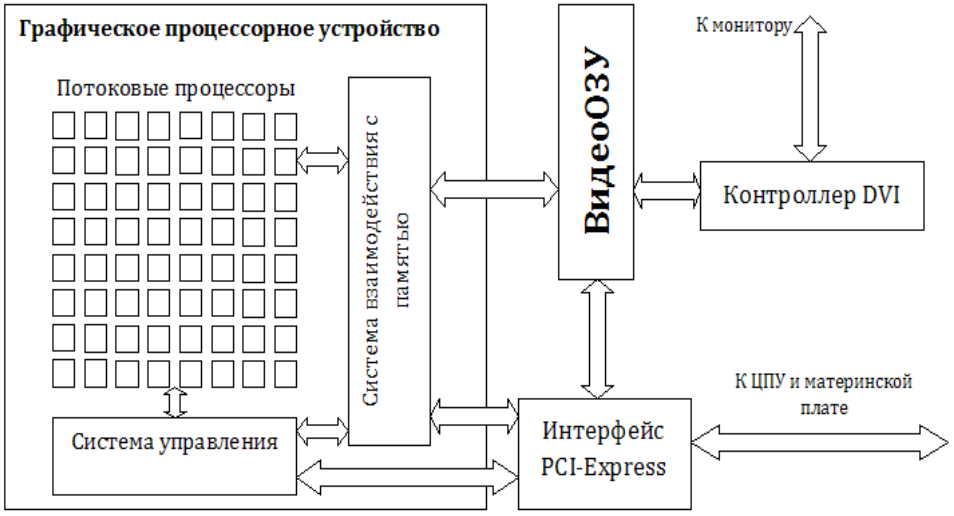
• Содержат набор одинаковых вычислительных устройств (потоковых процессоров, ПП), работающих с общей памятью ГПУ (видео ОЗУ) (SIMD архитектура).

• Все ПП синхронно исполняют один и тот же шейдер.

–За один проход, являющийся этапом вычислений на ГПУ, шейдер исполняется для всех точек двумерного массива.

- Система команд ПП включает арифметические команды для вещественных и целочисленных вычислений и команды обращения к памяти.
- ГПУ выполняют операции асинхронно, в потоках и только с данными на регистрах. Из-за высоких задержек доступа к ОЗУ.

- За переключение потоков отвечает диспетчер потоков, который не является программируемым
- благодаря большому количеству потоковых процессоров высокая производительность.



Архитектуры процессоров. Примеры. Архитектура современных графических процессоров

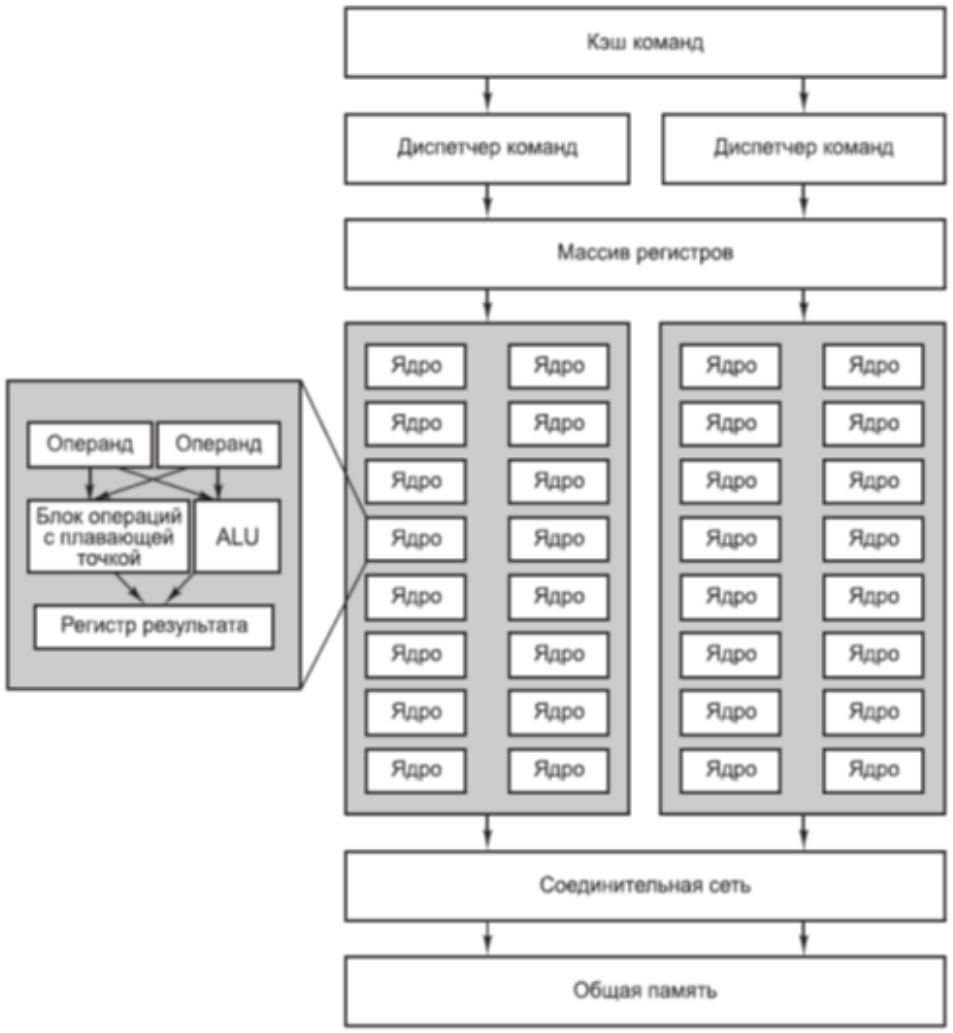
• Низкая скорость чтения из видео ОЗУ в шейдере на ГПУ (высокая латентность).

  чтобы его компенсировать, требуется обрабатывать большое (10000 и более) количество элементов за 1 запуск.

Поддержка аппаратной многопоточности.

Разнородность архитектур.

  Следует учесть, что оптимальные программы для NVidia и AMD будут сильно различаться.



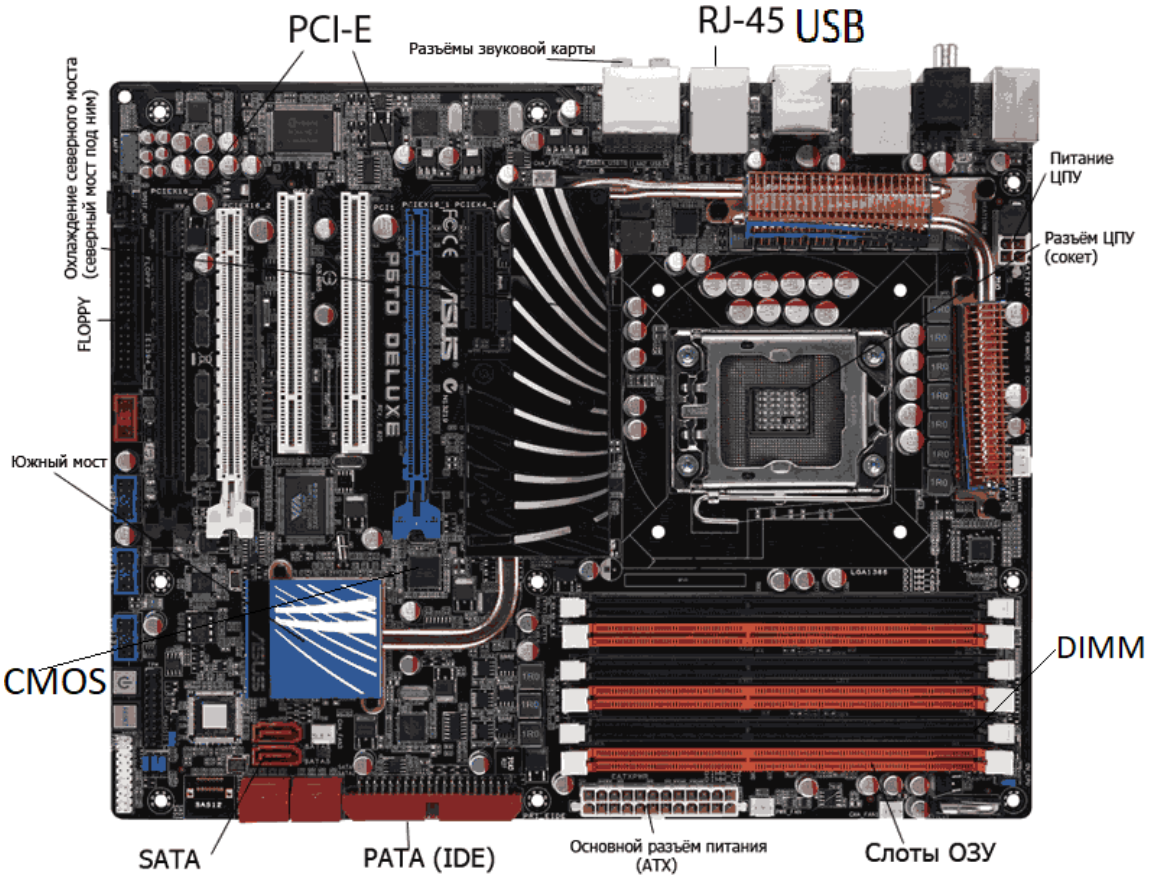
SIMD-ядро графического процессора Fermi

Особенности архитектуры системны плат

Аппаратные средства телекоммуникационных систем. Особенности архитектуры системных плат

Системная плата

Материнская (системная, главная) плата (Motherboard) является основным компонентом каждого ЭВМ. Это элемент, который управляет внутренними связями и с помощью системы прерываний взаимодействует с внешними устройствами.

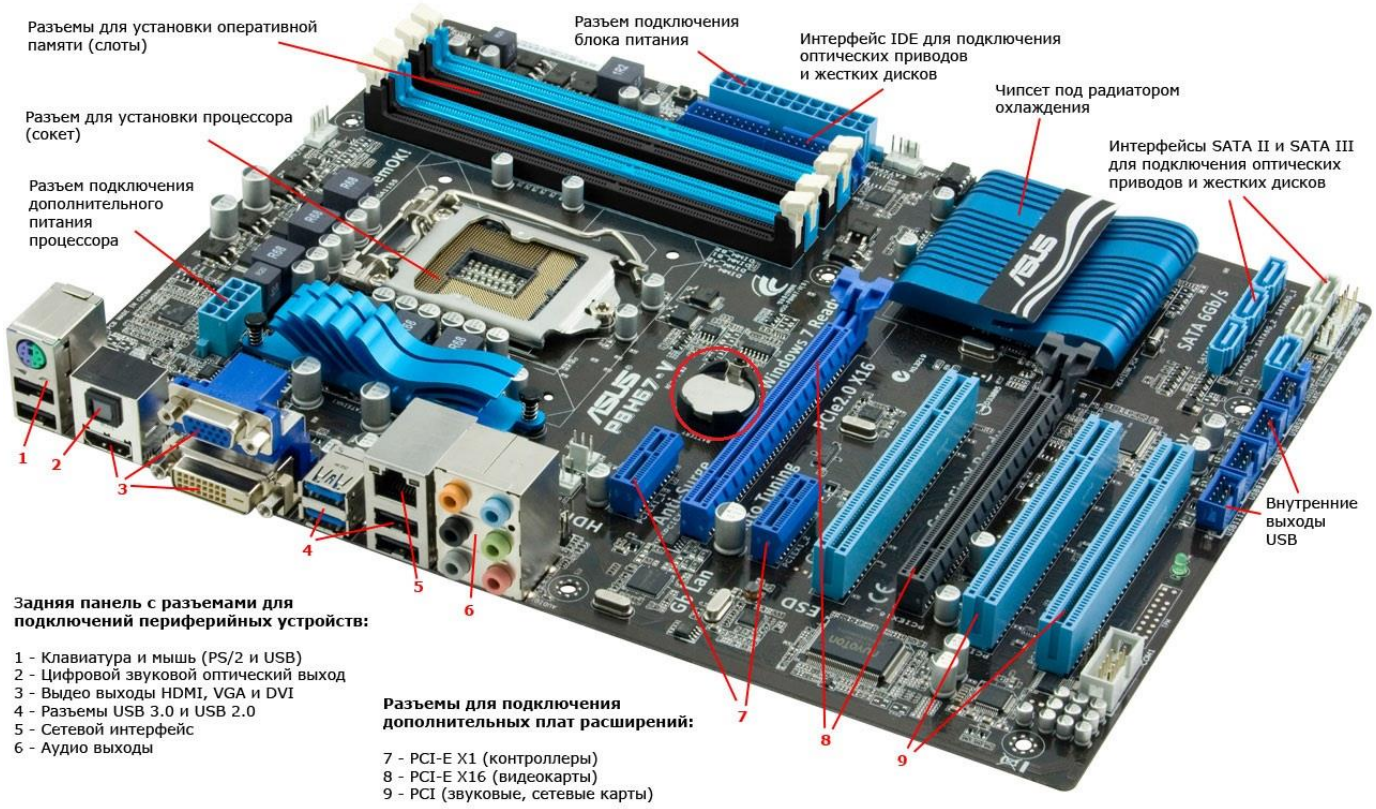


В архитектуру системной платы интегрированы:

- Микросхемы чипсета (chip-set) (северный и южный мост, контроль перываний)
- Микросхема ПЗУ (CMOS), содержащая программу BIOS (UEFI), систему Plug&Play
- Систему магистралей (системная магистраль FBS, QPI, PCI-E, USB и т.д.)
- Разъем (сокет, PCI-E, USB, DIMM и т.д.), и внешние разъемы (USB, RJ-45 и т.д.)
- Платы расширения (сетевая, wi-fi, звуковая и т.д.)

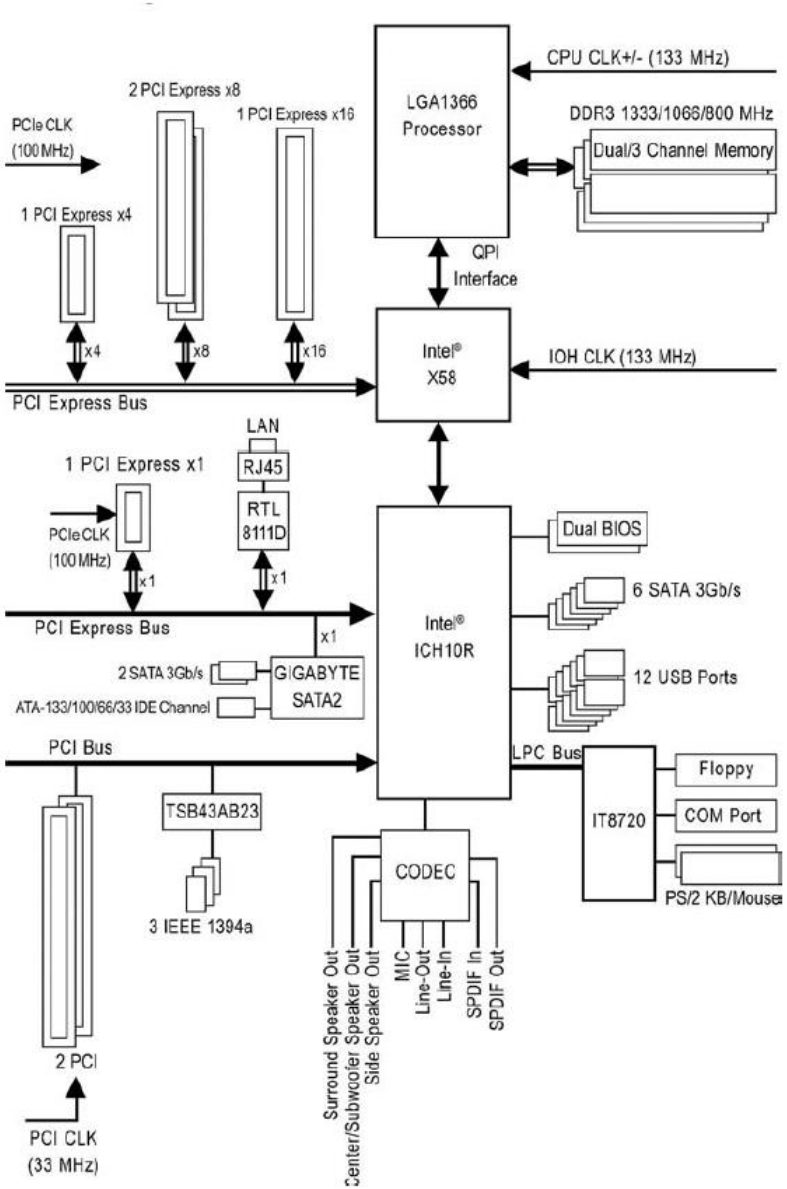
Системная плата

.



Материнская (системная, главная) плата (Motherboard) является основным компонентом каждого ЭВМ. Это элемент, который управляет внутренними связями и с помощью системы прерываний взаимодействует с внешними устройствами.

Системная плата



2. Блок-схема компьютера на чипсете Intel X58

Системная плата

- В архитектуру системной платы интегрированы:
  - **Микросхемы чипсета** (chip-set) (северный и южный мост, в т.ч. порывания Прямой доступ к памяти (DMA) и т.д.)
  - **Микросхема ПЗУ** (CMOS), содержащая программу BIOS(UEFI), систему P&P
  - **Систему магистралей** (системная магистраль (FBS, INTEL(QPI,DMI, FDI), AMD(HT, UMI)), PCI-E, USB и т.д.)
  - Разъем (сокет, socket) процессора,
  - Разъемы модулей оперативной памяти (SIMM, DIMM),
  - Разъемы видеоадаптера (AGP, PCI, PCI-Express),
  - Разъемы для подключения внешних запоминающих устройств (SATA, IDE)
  - Разъемы работы с периферийными устройствами и др. разъемы (USB, COM, IEEE 1394 (FireWire), PS/2 и др.)
  - **Платы расширения** (сетевая, wi-fi, звуковая и т.д.)
- Материнская плата во многом определяет производительность и функциональные возможности компьютера, включая средства оптимальной настройки и мониторинга.
- Основные производители: Intel, ASUSTek, MSI, GigaByte и тп

Системная плата

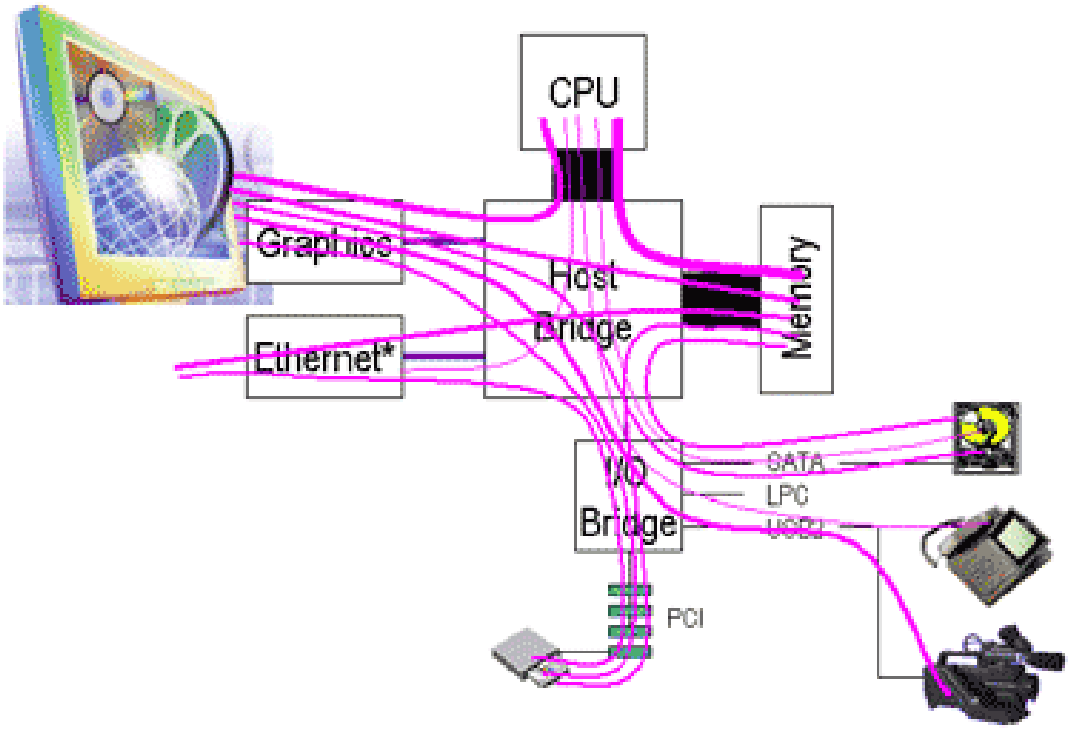
- **Чипсет.** Это связующий элемент системной платы, благодаря которому обеспечивается совместное функционирование центрального процессора, подсистем памяти, устройств ввода-вывода и так далее. Как правило, чипсет имеет северный мост и южный мост.
- **Северный мост** - связь процессора с основными устройствами ЭВМ (ОЗУ, графическая карта)
- **Южный мост** за работа дисковой подсистемы и интерфейсные разъемы
- Иногда мосты объединены в одном чипе.
- **IDE-интерфейс.** Через данный интерфейс
- **Интерфейсы типа ATA (SATA) и IDE.** подключаются внутренние жесткие диски и оптические приводы.
- **Слоты расширения PCI.** В разъемы PCI вставляются звуковые и сетевые карты компьютера.
- **Слоты PCI-Express x16.** Установка графической платы.
- **Слоты PCI-Express x1.** Установка устройств типа Wi-Fi-карты и GSM-модемы, а также различные контроллеры.
- **Разъем для батарейки BIOS.** (CMOS-память, является энергозависимой), для ее питания используется специальная батарейка.

Особенности шинной организации системны плат

Аппаратные средства телекоммуникационных систем. Особенности архитектуры системных плат

Шинная организация платы.

- В современных системных платах предусмотрено несколько шин.
  - шины «процессор-память» (FSB, UMI, DMI);
  - шины ввода/вывода (PCI, PCI-Express, USB);
  - системные шины (DMA).



Виды шин

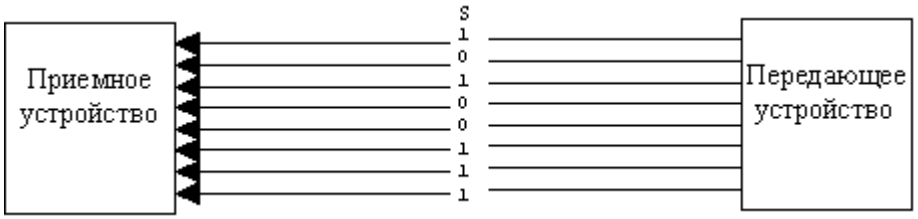
- **По назначению:**
  - специализированные (например IDE, Ethernet)
  - универсальные (например USB, PCI),
- **По числу подключаемых устройств**
  - Выделенные интерфейсы (одно устройство к одному порту)
  - Разделяемые интерфейсы(хабы)
- **По степени синхронности**:
  - **синхронные** (осуществляющими передачу данных только по тактовым импульсам)
  - **асинхронные** (осуществляющими передачу данных в произвольные моменты времени),
  - **С мультиплексированием** (передачу адреса и данных по одним и тем же линиям)
  - **Со схемами арбитража** (то есть способа совместного использования шины несколькими устройствами).
  - **Изохронные** – то есть на каждое устройство выделяется время передачи пакетов сообщений, и не важно сколько их в этот промежуток времени будет передано (пример USB хаб).

Виды шин

- **Шины по методу передачи данных**:
  - **Последовательные** (USB, SATA)
    - Передача пакетов по одному проводнику
    - Возможна организация двух каналов (прием и передача)
    - Данные объединяются в пакеты.
    - Пакет также могут включать служебную информацию.
  - **Параллельные** (PCI, DIMM, PATA)
    - параллельных шинах понятие «ширина шины» соответствует её разрядности – количеству сигнальных линий, количеству одновременно передаваемых битов информации.
    - Возможны отдельные вывода под служебные сигналы
  - **Последовательно-параллельные** (PCI-Express)
    - Несколько последовательных шин
    - для повышения скорости передачи
    - Как правило работают асинхронно.
- **По типу информации:**
  - Дискретные (дискрет. Звуковые карты)
  - Аналоговые (VGA)
  - Цифровые (большинство)

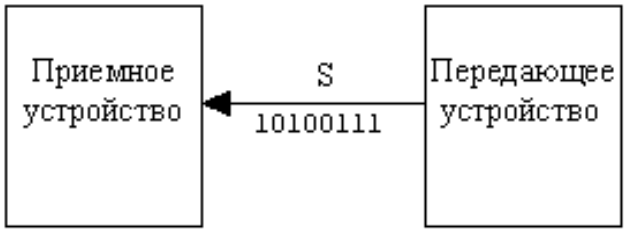
Интерфейсные шины. Параллельные шины.

- Недостатки:
  - Широкая шина данных
  - отдельный тактирующий сигнал.
  - **Рассинхронизация**
    - Разница задержек сигнала между проводниками в шине ограничения на максимально возможную скорость передачи данных.
  - **Взаимное влияние устройств на шине**
    - Помехи, вызванные отражениями и разным время прохождения к различным нагрузкам.
      - Особенно влияют при больших длинах кабелей
      - Шум также может повредить данные.



Интерфейсные шины. Последовательные шины.

- **интерфейсы «точка-точка».**
- **Низкое влияние шумов**
  - *Данные часто передаются по дифференциальной паре.*
    - Внешний шум воздействует на оба проводника в паре, и, таким образом, перестает влиять на передаваемый сигнал.
- **Линии передачи проще соединять, так как помехи взаимного влияния малы.**
- *Тактирующий сигнал не подается в явном виде;*
  - вместо этого, приемник восстанавливает его по временам переключения данных (из 0 в 1 и из 1в 0).
- Хорошие интерфейсы могут работать на скоростях более 10 Гбит/с по медным проводникам, а по оптоволокну –быстрее.



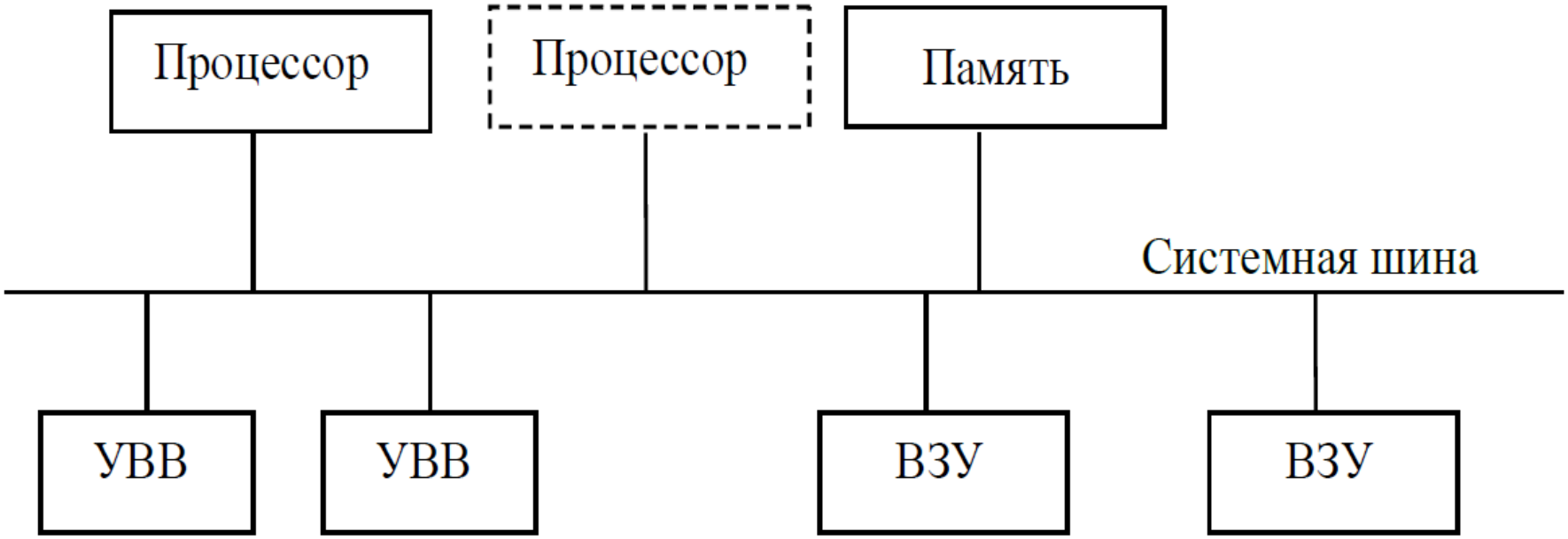
Контроллеры шин

- За распределение порядка передачи данных по шине отвечает особое устройство – **контроллер** (адаптеры) шины.
  - Сложный контроллер может иметь в своем составе и собственный процессор.
  - Если передача данных по шине происходит без участия центрального процессора, то говорят, что осуществляется **прямой доступ к памяти** (Direct Memory Access, **DMA**).
  - *Для взаимодействия с программой (с помощью процессора или сопроцессоров) адаптеры и контроллеры обычно имеют регистры ввода-вывода, управления и состояния.*

Контроллеры шин. Механизм прерываний

- Когда передача данных заканчивается, контроллер выдает **прерывание**, вынуждая центральный процессор приостановить работу текущей программы и начать выполнение особой процедуры.
  - процедура **программой обработки прерываний**
    - процедура, чтобы проверить, нет ли ошибок,
    - в случае обнаружения ошибок процедуедура произведет необходимые действия и сообщит операционной системе, что процесс ввода-вывода завершен.

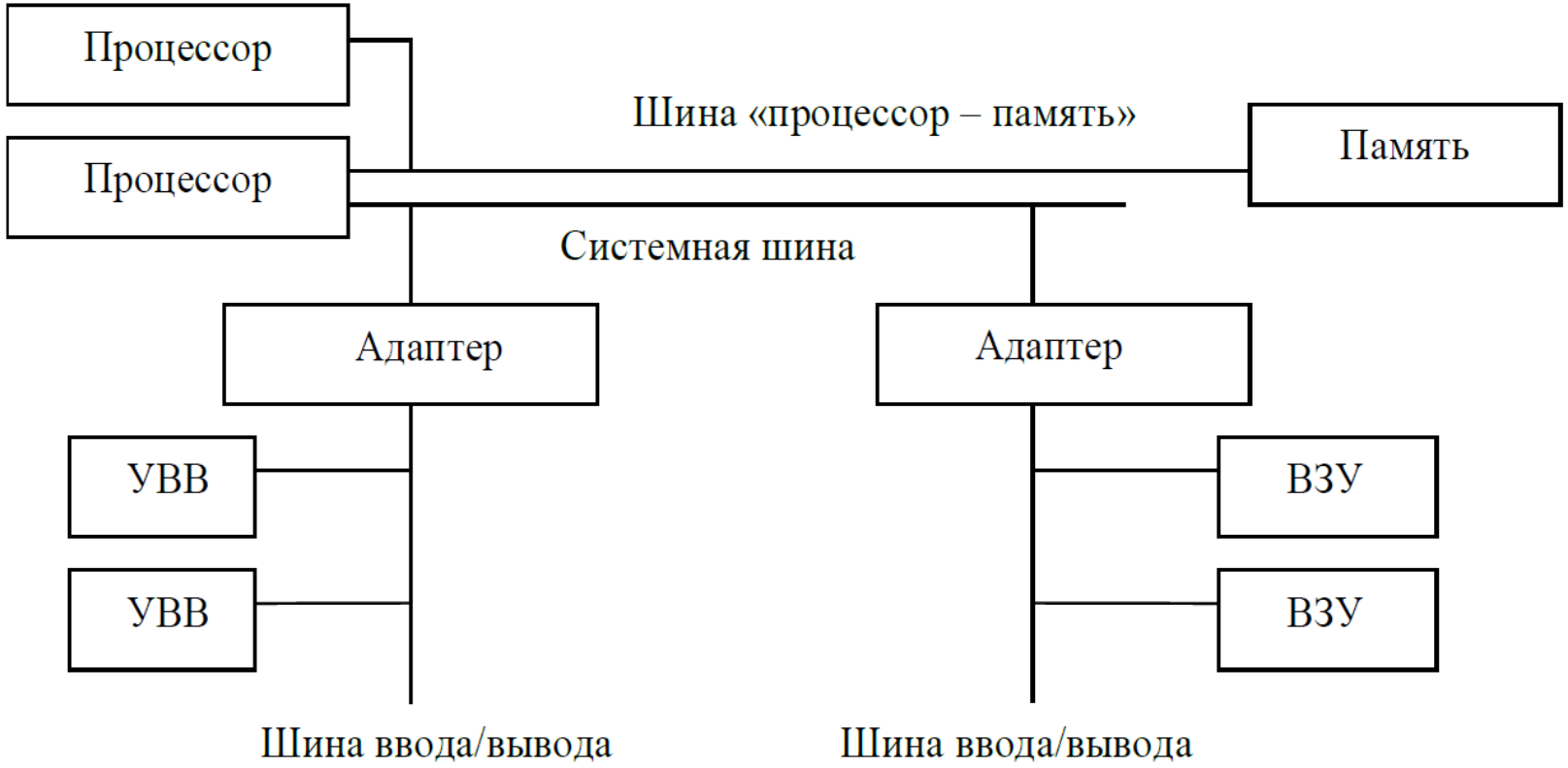
Способы организации шин



Система с одной шиной – низкое быстродействие, строго последовательный доступ
Достоинство – цена, простота

Параметр работы шины — трансферы в секунду, который указывает на количество операций по передаче данных в секунду. Например, 3200 MT/с (мегатрансферы в сек) или 3.2 ГТ/с (гигатрансферы).

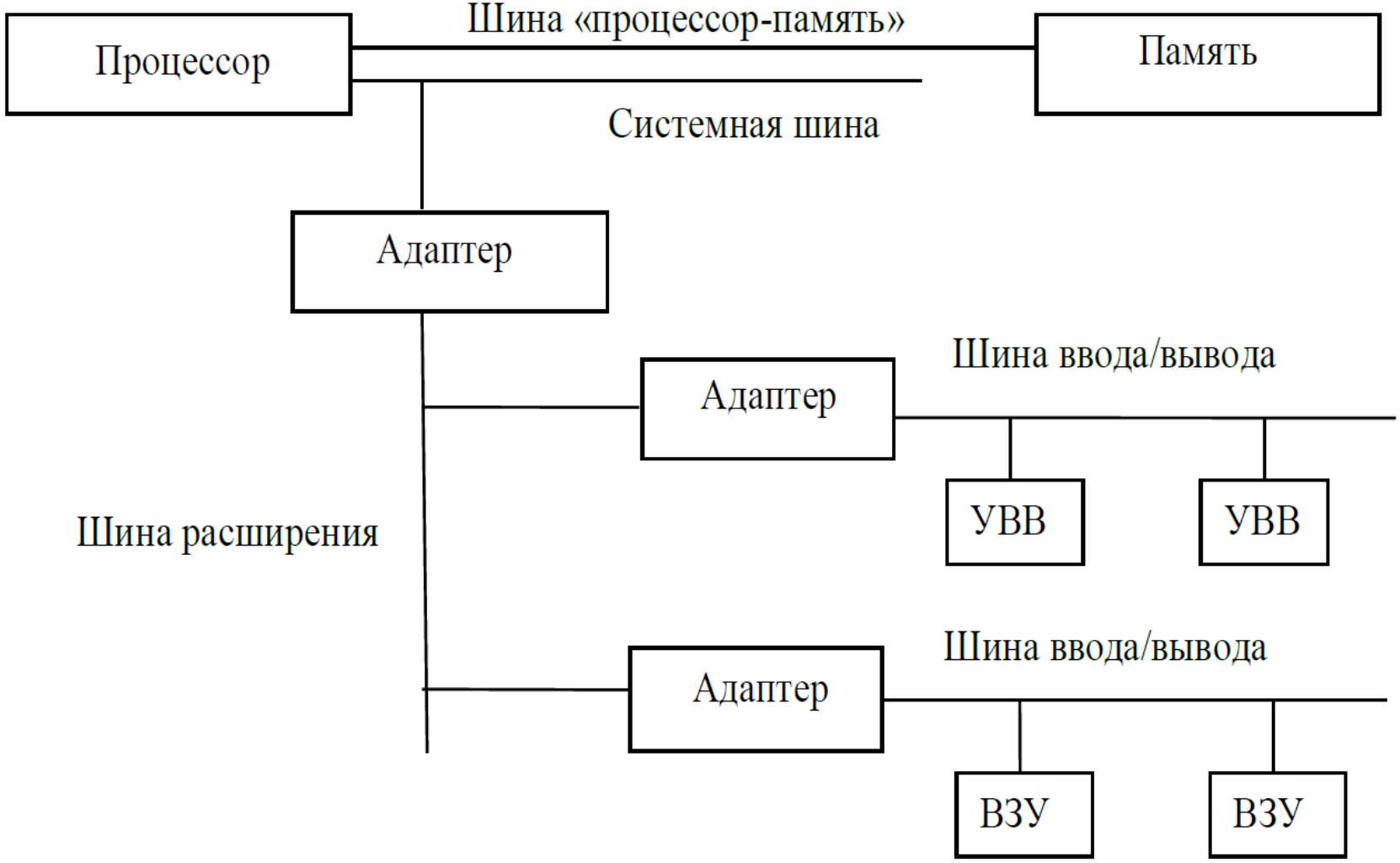
Способы организации шин



Система с двумя шинами – связь через адаптеры, разгрузка шины за счет отдельной магистрали для переферии

Параметр работы шины — трансферы в секунду, который указывает на количество операций по передаче данных в секунду. Например, 3200 МТ/с (мегатрансферы в сек) или 3.2 ГТ/с (гигатрансферы).

Способы организации шин



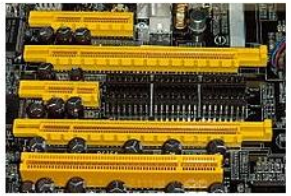
Система с тремя шинами. – Использование шины расширения для разгрузки основных магистралей

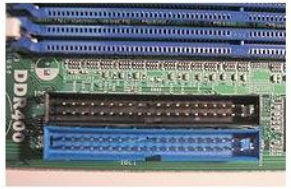
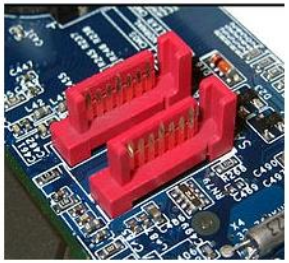
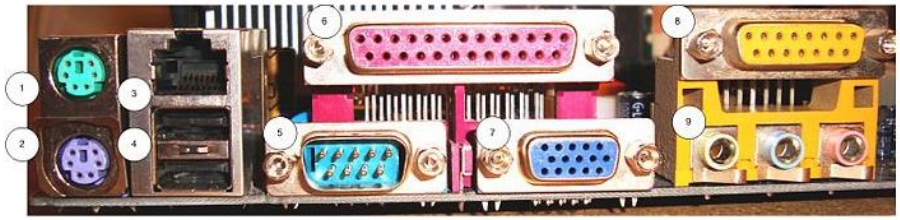
Интерфейсные шины

Аппаратные средства телекоммуникационных систем. Особенности архитектуры системных плат

Интерфейсные шины. Подключение периферийных устройств

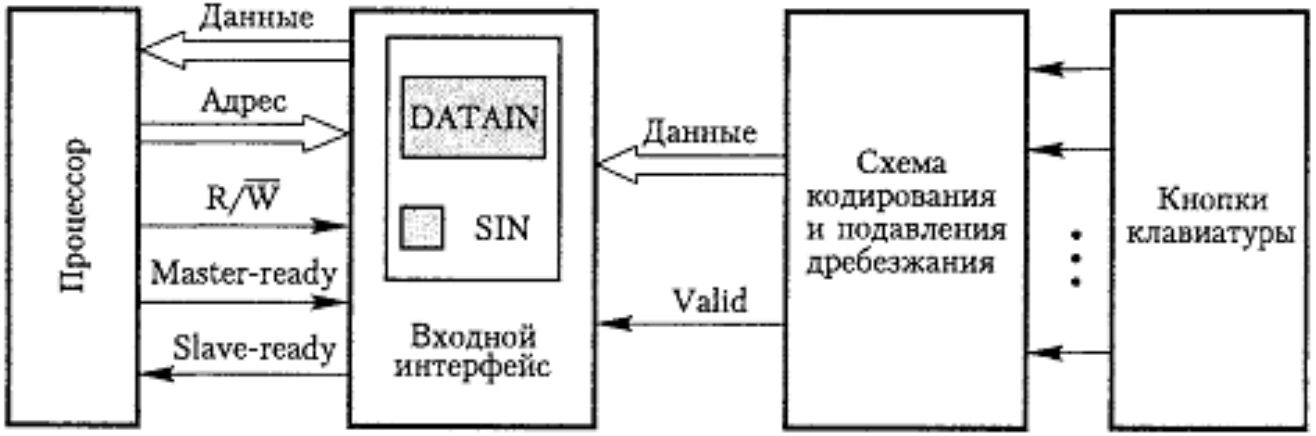
- **Большинство периферийных устройств подключаются через промежуточные периферийные интерфейсы**
- К периферийным устройствам относятся:
  - большинство устройств хранения (дисковые, флэш),
  - устройств ввода-вывода (дисплеи, клавиатуры, мыши, принтеры, плоттеры),
  - коммуникационные устройств (внешние модемы).

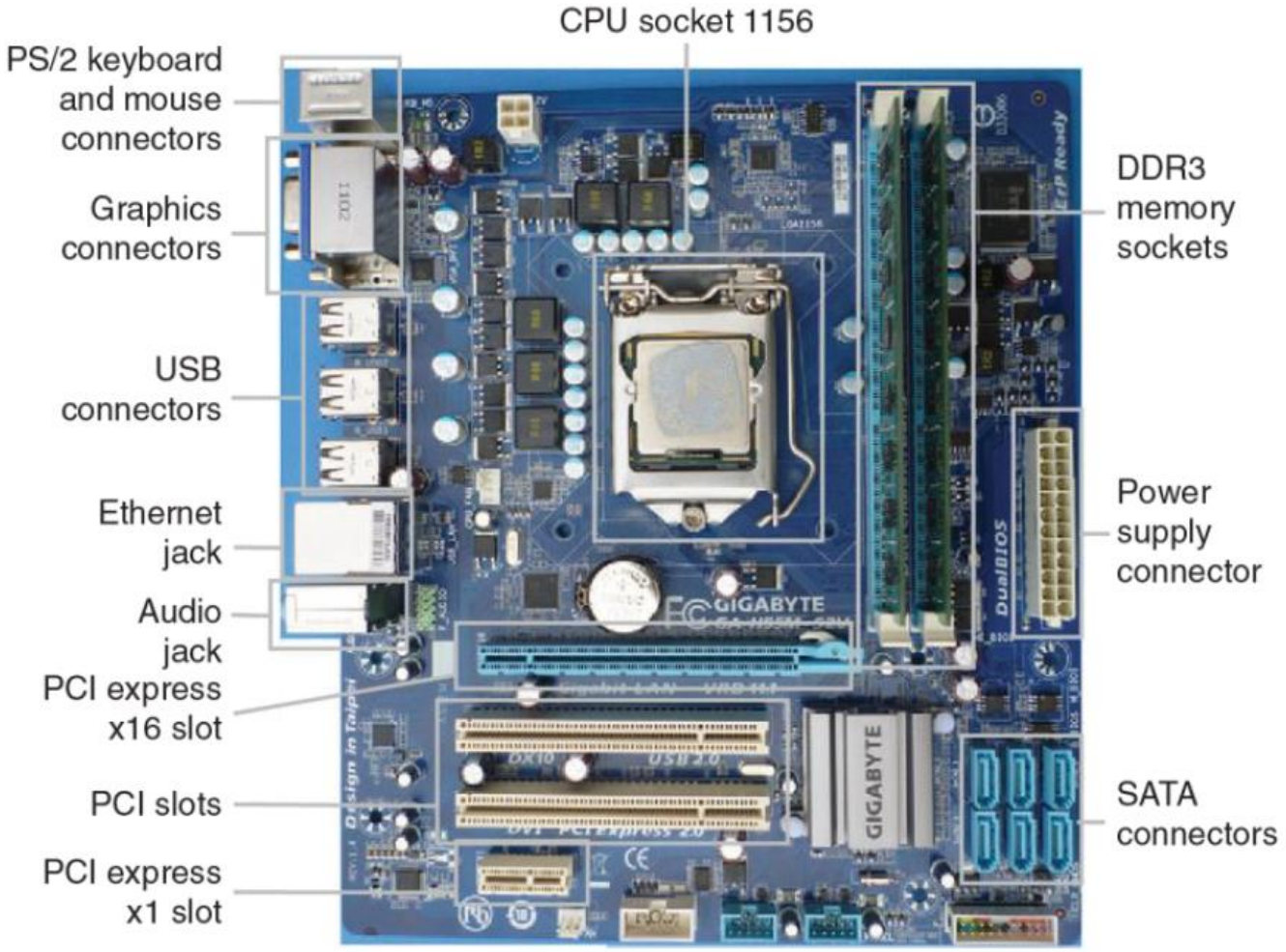





Интерфейсные шины. Подключение периферийных устройств

- подключение периферийных устройств осуществляется через входные интерфейсы
  - *Часто устройства имеют дополнительные контроллеры подключения*
- **Интерфейсы соединены с процессором и/или южным мостом системной платы**
- Устройства соединяются через т.н. шины
  - *Часто шины объединены в т.н. хабы*



Интерфейсные шины. Разъемы интерфейсов на типичной материнской плате



Интерфейсные шины. Подключение периферийных устройств

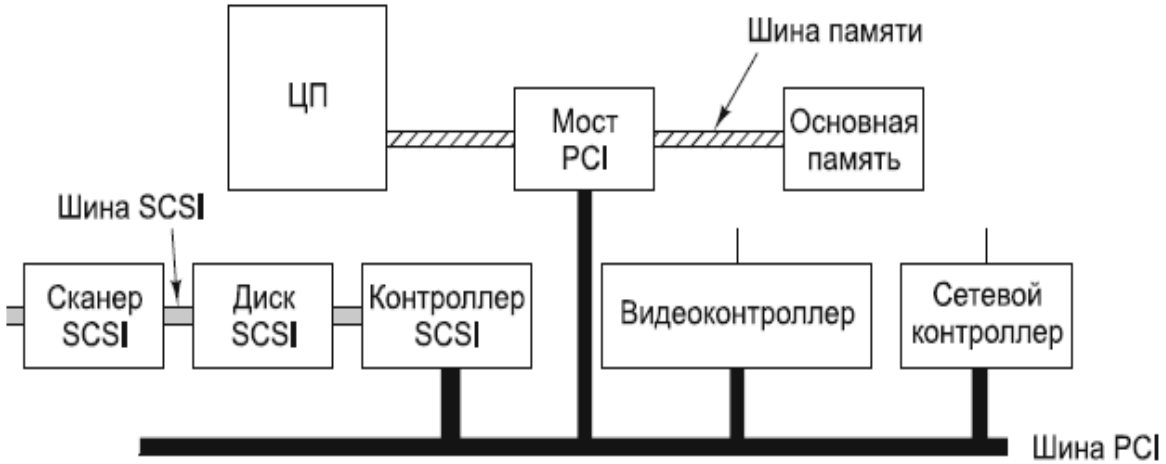
Порядок подключения

- *подсоединение периферийного устройства к узлу с помощью соответствующего кабеля или беспроводного соединения;*
- подключение устройства к источнику питания;
- установка соответствующего драйвера.

Некоторые устройства не предусматривают самонастройки. Драйверы таких устройств устанавливаются после того, как устройство подключается к компьютеру и включается питание.

Драйверы самонастраивающихся устройств в системе уже имеются (PnP). В таком случае при подключении ОС распознает устройство и устанавливает соответствующий драйвер.

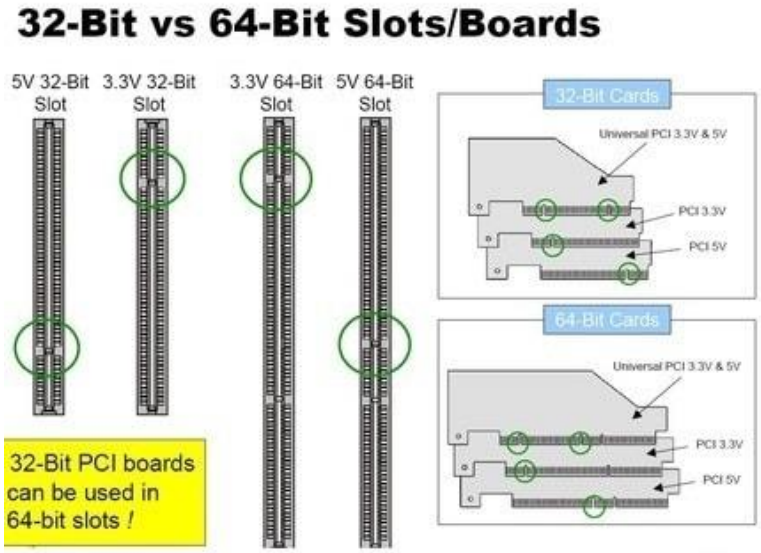
Шина PCI



PCI (Peripheral Component Interconnect — **взаимодействие периферийных компонентов**), разработанная компанией Intel.

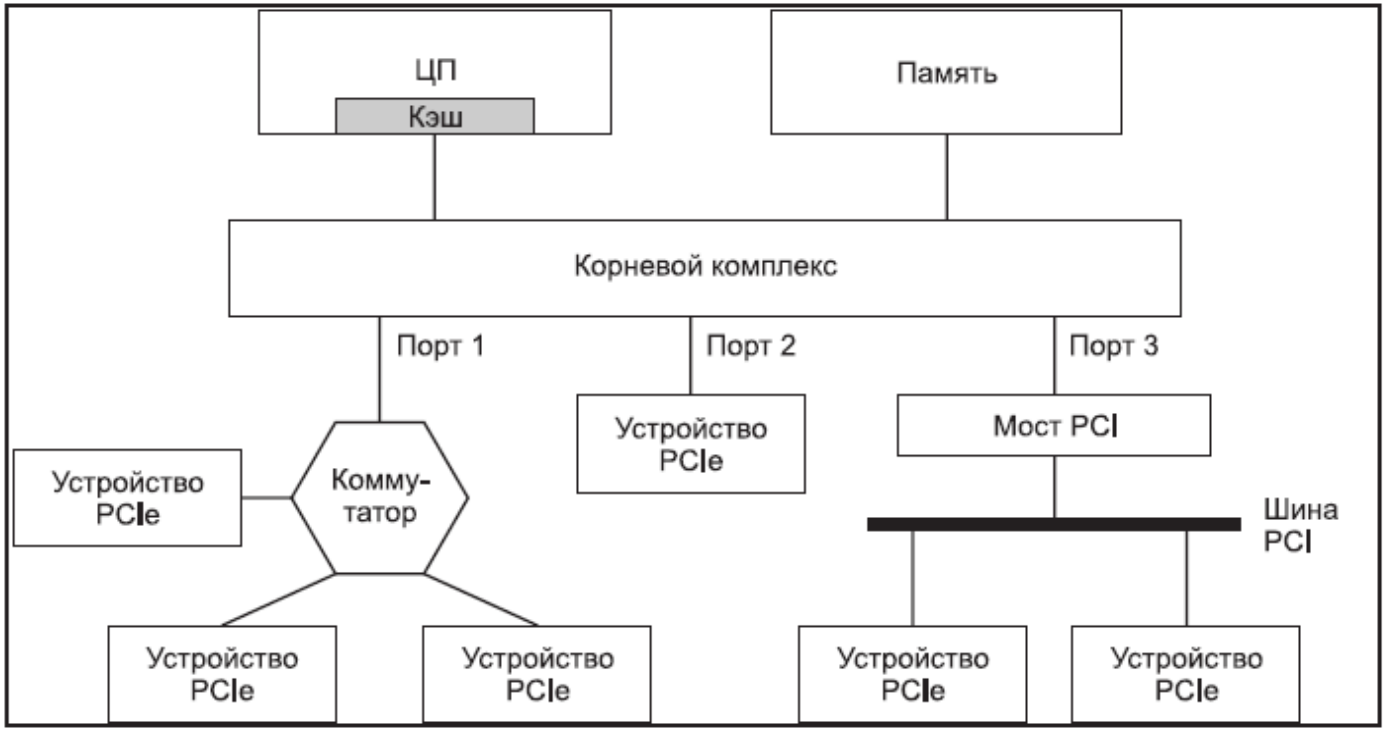
- *Центральный процессор взаимодействует с контроллером памяти по выделенному высокоскоростному соединению.*
- Периферийные устройства подсоединяются прямо к шине PCI
- Шина PCI распознает подключаемые устройства и подключает их по принципу **PLUG&PLAY.**
- **Принцип Bus Mastering**, - способность внешнего устройства при пересылке данных управлять шиной (без участия CPU).
  - *Полная поддержка **multiply bus master** (например, несколько контроллеров жестких дисков могут одновременно работать на шине).*

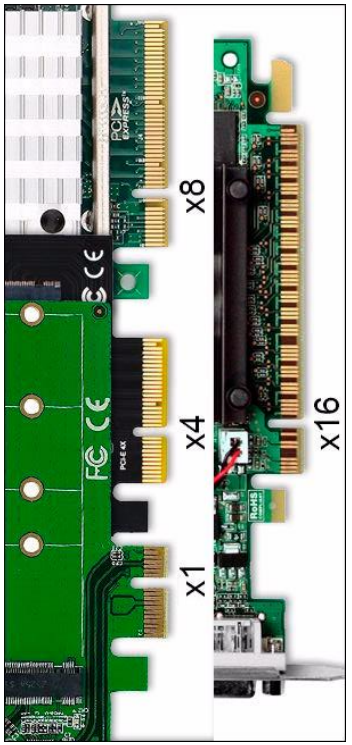
Шина PCI. Характеристики



- **Синхронный 32-х или 64-х разрядный обмен данными.**
- Частота работы шины 33MHz или 66MHz - широкий диапазон пропускных способностей (с использованием пакетного режима):
  - 132 MB/сек при 32-bit/33MHz;
  - До 528 MB/сек при 64-bit/66MHz.
  - А также в PCI-X —1056 MB/сек при 64-bit/133MHz.
- *Комбинирование до 8 функций на одной карте (, видео + звук и т.д.).*
- Шина позволяет устанавливать до 4 слотов расширения, однако возможно использование моста PCI-PCI для увеличения количества карт расширения.
- Возможно подключение логик 5 В и 3.3 В

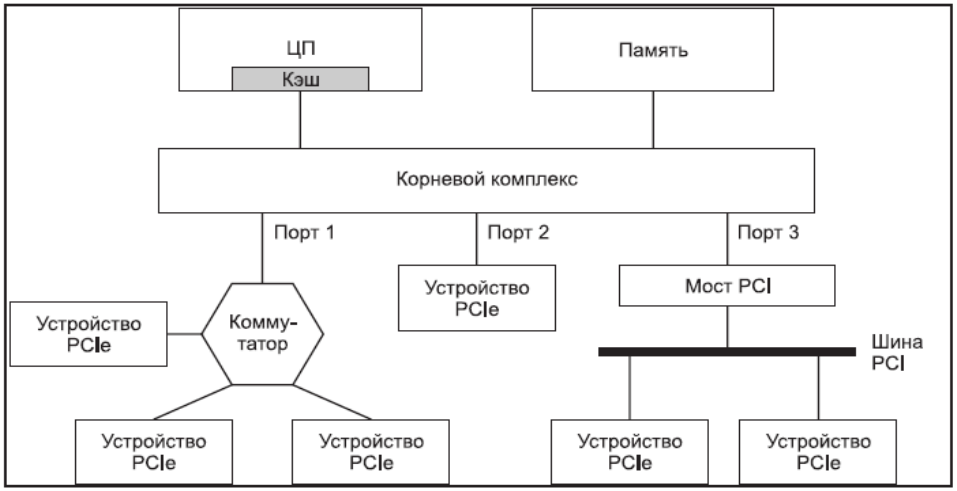
Шина PCI-Express





PCI Express – компьютерная шина, образующая одноранговую сеть, использующая программную модель шины PCI и физический протокол, основанный на последовательной передаче пакетных данных.

Шина PCI-Express. Особенности организации сети

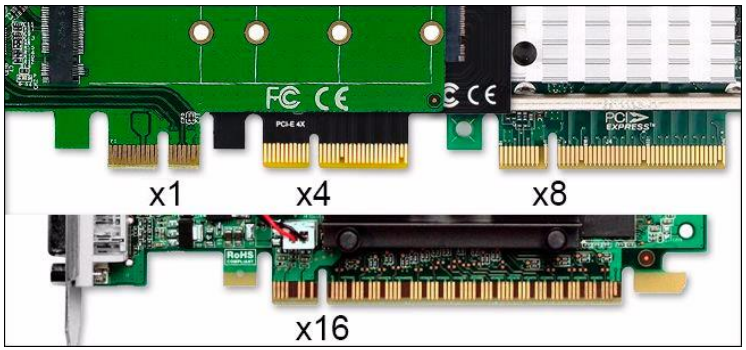


PCI Express – компьютерная шина, использующая программную модель шины PCI и физический протокол, основанный на последовательной передаче пакетных данных.

- **Представляет одноранговую сеть, использующая разрядноособследовательные линии и коммутацию пакетов.**
  - *Устройства взаимодействуют между собой через среду, образованную коммутаторами(соединение типа точка-точка).*
    - применение узких последовательных двухточечных соединений.
  - передача данных пакетами, содержащими как саму посылку, так и системную информацию (протокольная передача данных).

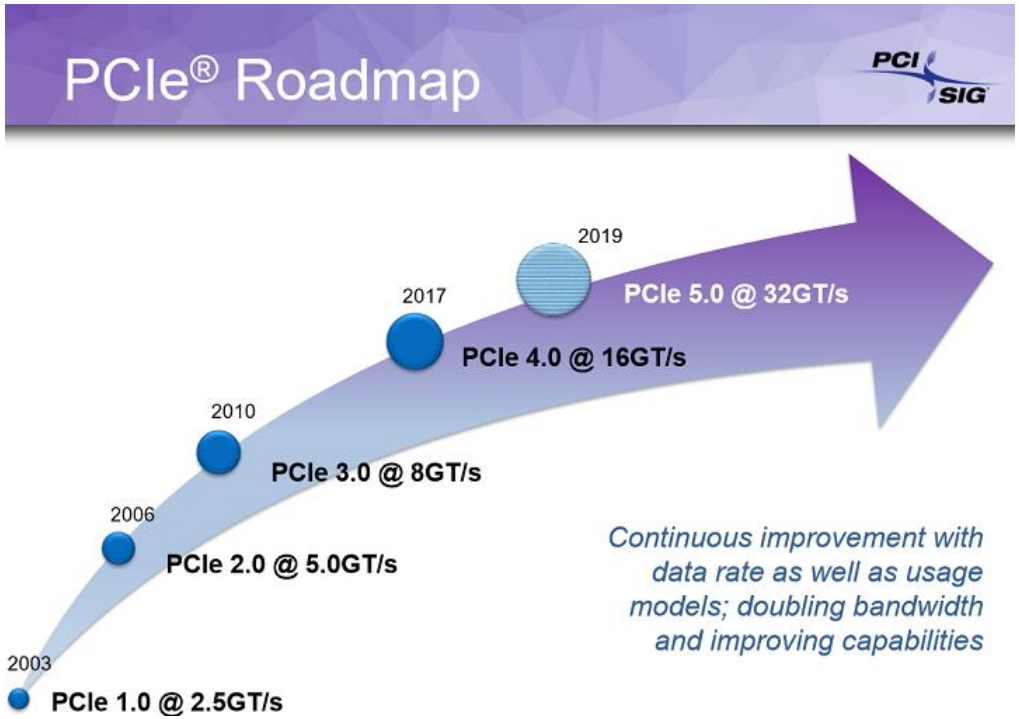
Шина PCI-Express. Особенности

- **Физическая длина соединения до коммутатора до 50 см,**
- *Скорость до 20 Гбит/сек.*
- Режим эмуляции шины PCI (программный уровень).
- К базовому коммутатору можно подключить другой коммутатор,
  - Возможность формирования древовидной структуры повышается степень расширяемости системы.
- Может иметь до 32 проводных пар, называемых трактами (lanes) или дорожками.
  - Тракты работают несинхронно, но расфазировка несущественна.
  - Устройства на шину могут быть подключены по 1, 4, 8 или 16 ленсам.



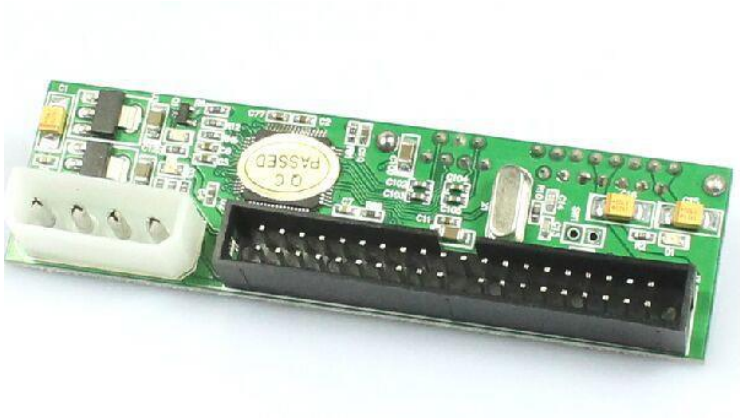
Шина PCI-Express. Особенности

- Причины появления PCI-e 4 – появление новых устройств на шине PCIe, типа SSD
- Увеличение линий и скорости передачи на каждую линию (актуально для серверных систем).
- Увеличение толерантности к палатам расширения (подключение через PCI-e X1, X4)
  - – то есть максимально допустимой скорости при переходниках с таких устройств на PCI-e 16.



IDE (PATA)

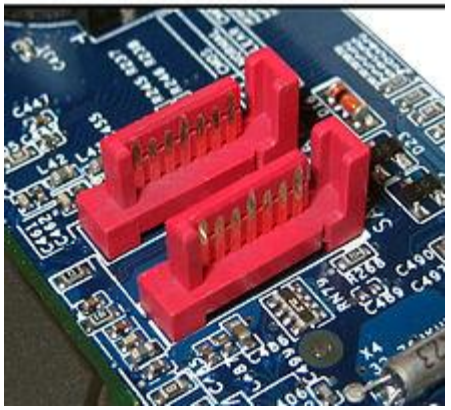
- *интерфейс предназначен только для подключения жестких дисков и других накопителей*
- поддерживает два разъема IDE Primary — Первичный и Secondary — Вторичный,
  - **к каждому из разъемов можно подключать по два устройства (Master и Slave — ведущий и ведомый).**
- Максимальная пропускная способность интерфейса — до 66 Мбайт/с.
  - *Для обеспечения совместимости с накопителями, отличными от жестких дисков, существует протокол обмена данными ATAPI (ATA Packet Interface — Пакетный интерфейс ATA).*



SATA

- SATA (англ. Serial ATA) — последовательный интерфейс обмена данными с накопителями информации.
- SATA является развитием параллельного интерфейса ATA (IDE), который после появления SATA был переименован в PATA (Parallel ATA).

- SATA I 1.5 Гбит / с. Пропускная способность интерфейса - до 150МБ / с.
  SATA II (SATA 3 Гбит / с) ,Пропускная способность интерфейса - до 300МБ / с.
  SATA III (SATA 6 Гбит / с(.Пропускная способность интерфейса 600 МБ / с.
  интерфейсы обратно совместимы.
- SATA e – подключение внешних жестких дисков

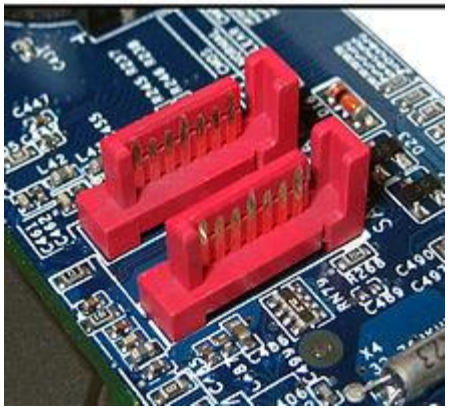


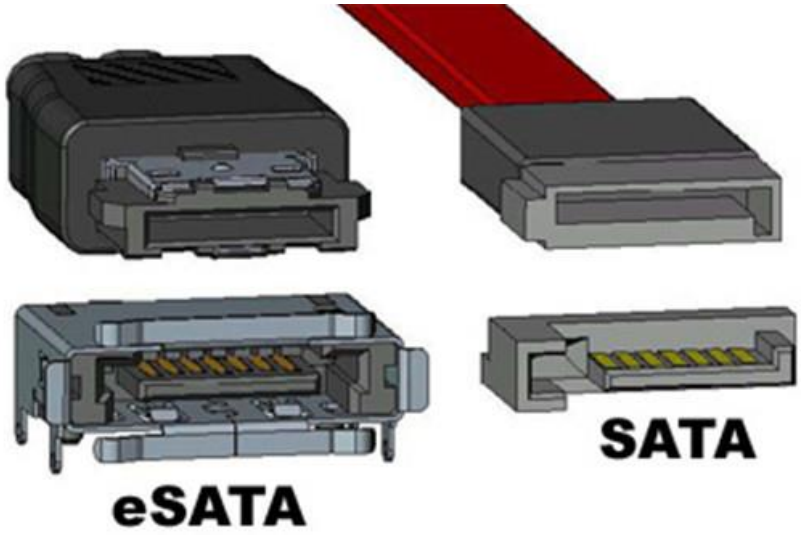
Главное преимуществом SATA перед PATA - использование последовательной шины вместо параллельной. – увеличение помехоустойчивости и повышение скорости передачи данных.

Интерфейс SATA поддерживает все периферийные устройства ATAPI — CD, DVD, и тп, ленты, а также ATA.

SATA

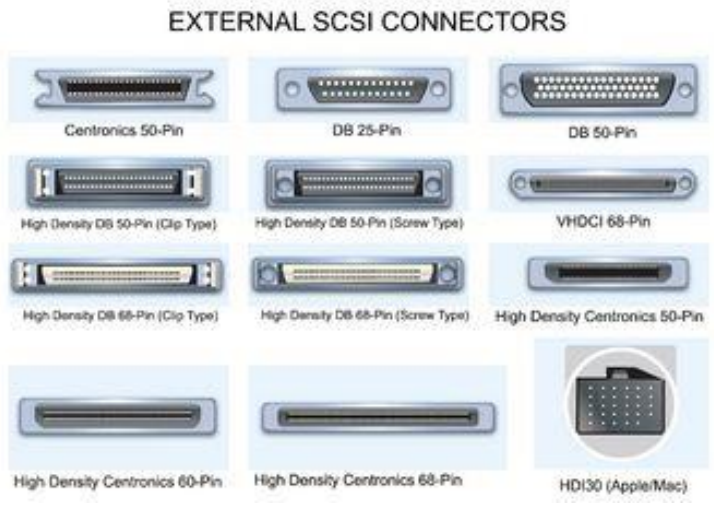
- **Интерфейс SATA обладает высокой пропускной способностью шины и помехоустойчивостью кабеля данных :**
  - меньшее количество линий
  - дифференциальная передача сигналов.
  - Для передачи и приема используются две токовые петли — два замкнутых кольца, через которые циркулируют данные, синхронизированные частотой 1,5 ГГц.
  - Каналы работают в противофазе, в силу чего происходит уничтожение взаимных помех.
  - Система допускает подключение plag and play

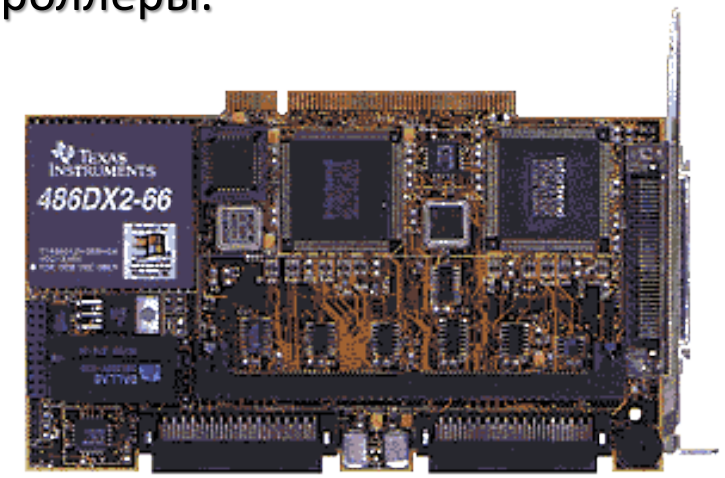




SCSI

- Интерфейс SCSI (Small Computer System Interface — системный интерфейс малых компьютеров, произносится «скази»)
  - *интерфейс, разработанный для объединения в единую систему устройств различного профиля: накопителей на жестких магнитных носителях, сканеров, стримеров, CD-ROM и т.п.*
- **Наиболее широко используется для устройств и систем хранения данных.**
- Устройства SCSI подключаются к шинам пк (PCI) при помощи хост-адаптера
- Устройства, подключенные к SCSI-шине, взаимодействуют друг с другом не напрямую, а через встроенные SCSI-контроллеры.

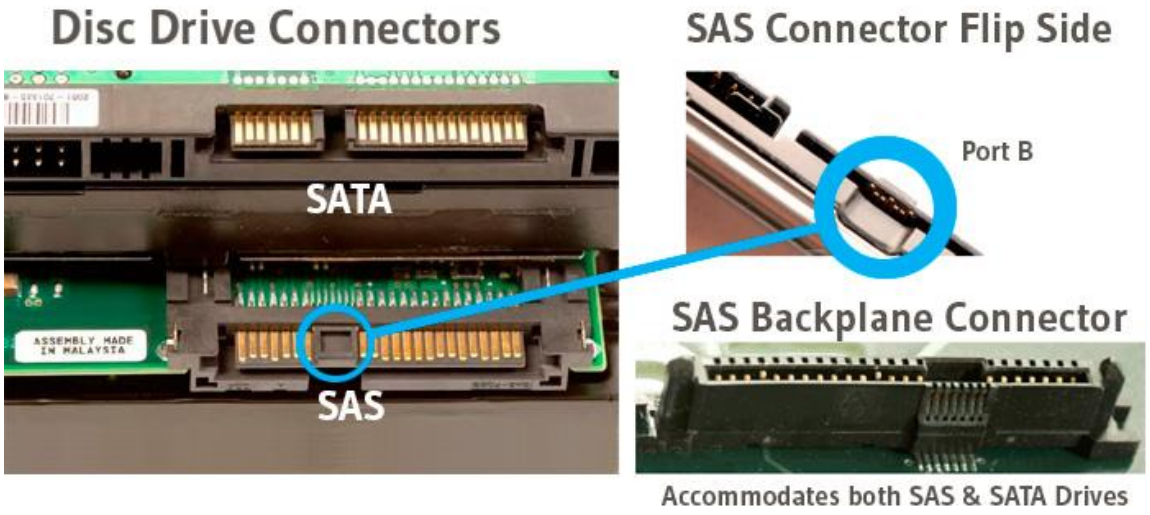




SAS

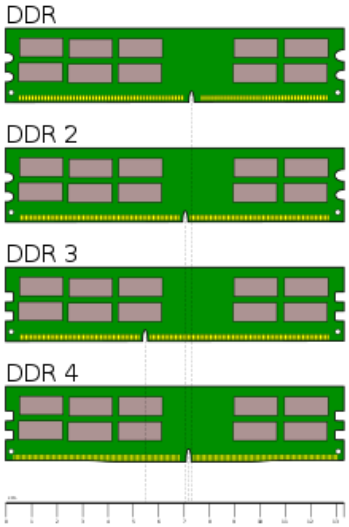
SAS - Последовательный интерфейс типа SCSI

- *Возможность подключение одного устройства по нескольким каналам и поддержка расширителей шины*
  - *Требует наличия специального контроллера SAS*
  - Обладает обратной совместимостью с SATA
- ***Интерфейсы SAS и SCSI используются в основном в серверах из-аз высокой стоимости интерфейса***
  - Наибольшего эффекта от применения можно достигнуть при одновременном выполнении нескольких "тяжелых" приложений или при массовых запросах к данным на устройствах хранения.



Интерфейс DIMM

- **Dual In-line Memory Module, DIMM интерфейс двухстороннего модуля памяти) – используется для подключения оперативной памяти, на сегодня это DDR RAM (double data rate random access memory).**
- Параллельный интерфейс
- *по 120 контактов с двух сторон, (240 в сумме), (288 в DDR4)*
  - 64-разрядная шина данных,
  - 16-разрядная адресная шина с временным мультиплексированием,
  - Тактовая частота сигнала 100-266 МГц
    - Тактирование по переднему и заднему фронту импульсов - DDR

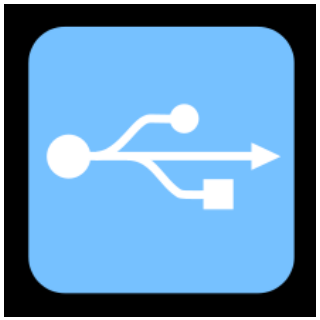


Например, DDR3-1600 использует тактовую частоту памяти в 200 МГц, ввода-вывода – в 800 МГц, и посылает 1600 миллионов слов/сек или 12800 Мбайт/с.

Главная проблема DIMM – латентность – то есть время чтения/записи ячеек памяти

Интерфейс USB

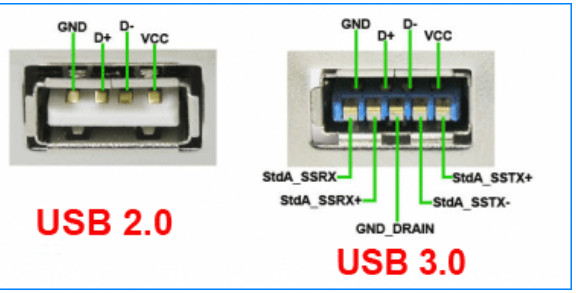
- **USB (Universal Serial Bus — универсальная последовательная шина)**
  - является промышленным стандартом расширения архитектуры PC, ориентированным на интеграцию с телефонией и устройствами бытовой электроники.
- **Ориентированность стандарта:**
  - легкореализуемое расширение периферии ПК;
  - дешевое решение, позволяющее передавать данные со скоростью до 12 Мбит/с (480 Мбит/с USB2, 5, 10, 20 Гбит/с USB3 и USB4);
  - полная поддержка в реальном времени голосовых, аудио- и видеопотоков;
  - гибкость протокола смешанной передачи изохронных данных
  - асинхронных сообщений;
  - обеспечение стандартного интерфейса;
  - Поддержка PnP

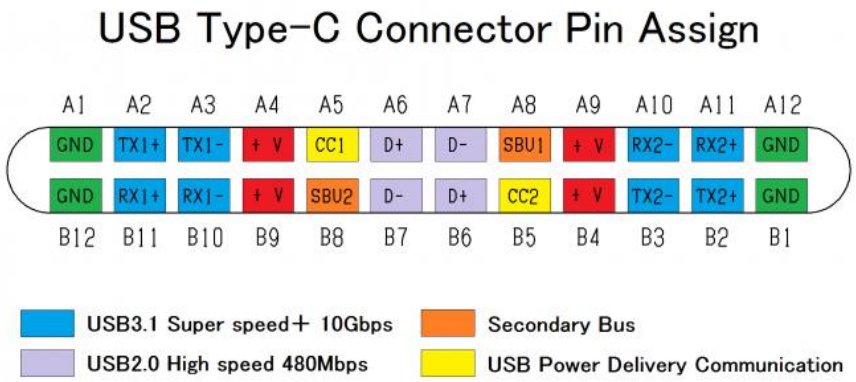


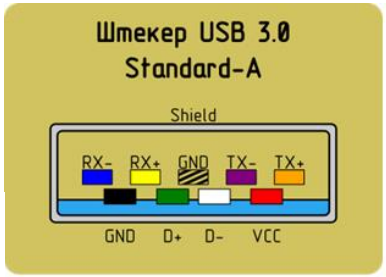
Стандарт USB

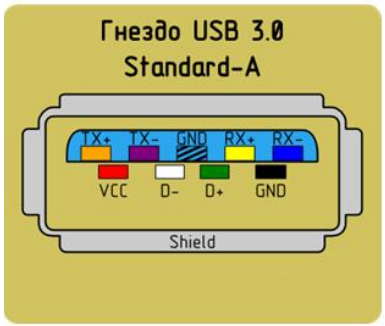
USB1, USB2

- подключения периферийных устройств к шине USB
- четырёхпроводной кабель (USB1, USB2),
  - В стандартах USB3, и более новых используется многопроводной кабель, но при этом структура остается та же и все стандарты остаются совместимыми
- Передача данных по дифференциальным линиям.
- Напряжение 0 и 5В сила тока до 500 мА (USB 3.0 — 900 мА).
  - Интерфейс рассчитан на расстояния до 5 м, и подключения до 5 уровней устройств (либо разветвителей – т.н. «хабов» либо функциональных устройств) .









Промышленные интерфейсы

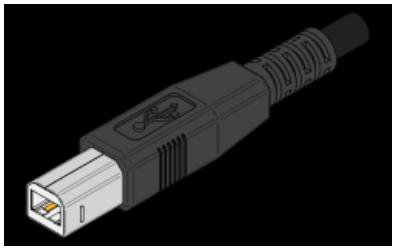
Тип A

USB3 Тип A

Mini USB тип A

micro USB тип A

Тип B



USB3 тип B

Mini USB тип B

micro USB тип B

Тип C

Mini USB3 тип B

micro USB3 тип A

USB. Свойства

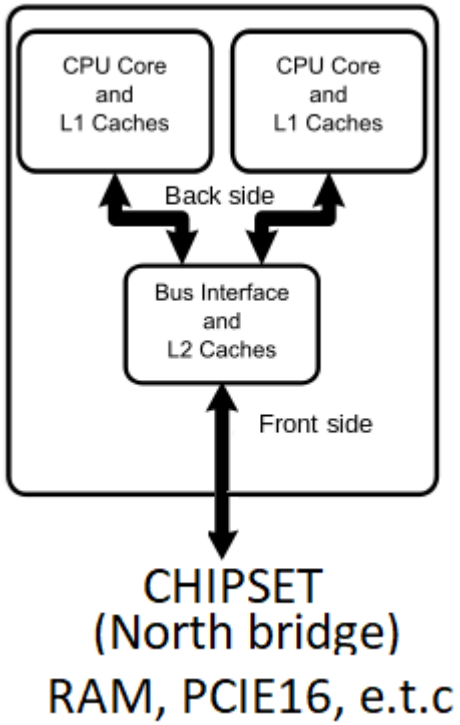
- USB всегда работает от т.н. **корневого хаба** (напр. имеется на системной плате), остальные устройства подключаются либо напрямую либо через другие хабы.
  - Стандарт допускает до 5 уровней устройств от одного хаба.
- **Адресация** — каждое логическое устройство (т.н. функция) имеет свой адрес для работы точка-точка с корневым хабом.
  - Иногда в одном физическом устройстве может быть несколько логических – например точпад и клавиатура
- **Система Plag and Play**— Каждое устройство имеет идентификаторы типа (логической функции - PID) и изготовителя (VID), по ним UEFI должно найти подходящие драйвера;
  - Напр., Human Interface Device, HID (мышки, клавиатуры, игровые манипуляторы и т. п.) Mass Storage («флешки», дисководы).
- **Передача данных** между логическими устройствами (т.н. конечными точками)
  - то есть в одном физическом устройстве может существовать несколько логических каналов данных, при этом каналы могут работать в разных режимах и с разной скоростью.

Шины процессор-память

Аппаратные средства телекоммуникационных систем. Особенности архитектуры системных плат

Шины процессор-чипсет. FSB шина

- **Шина FSB** (Front – Side Bus) - параллельная мультиплексированная процессорная шина.
- FSB соединяет процессор с основной памятью.
- FSB подключается к северному мосту чипсета, который содержит контроллер ОП.
- В некоторых компьютерах для соединения процессора с кэш-памятью второго уровня используется отдельная шина **BSB** (Back- Side Bus).
- FSB является «узким» местом работы пк, задавая тактовую частоты работы.
- Использование технологии DDR (double data rate) – то есть синхронизации как по фонту и спаду (переднему и заднему фронтам).
- Многие устройства имеют свои шины (DMA- direct memory access).



- Асинхронность шин FSB и ОЗУ,
- Опорной частотой для процессора выступает частота тактирования (а не передачи данных) шины FSB,
- частота тактирования шины памяти может задаваться отдельно

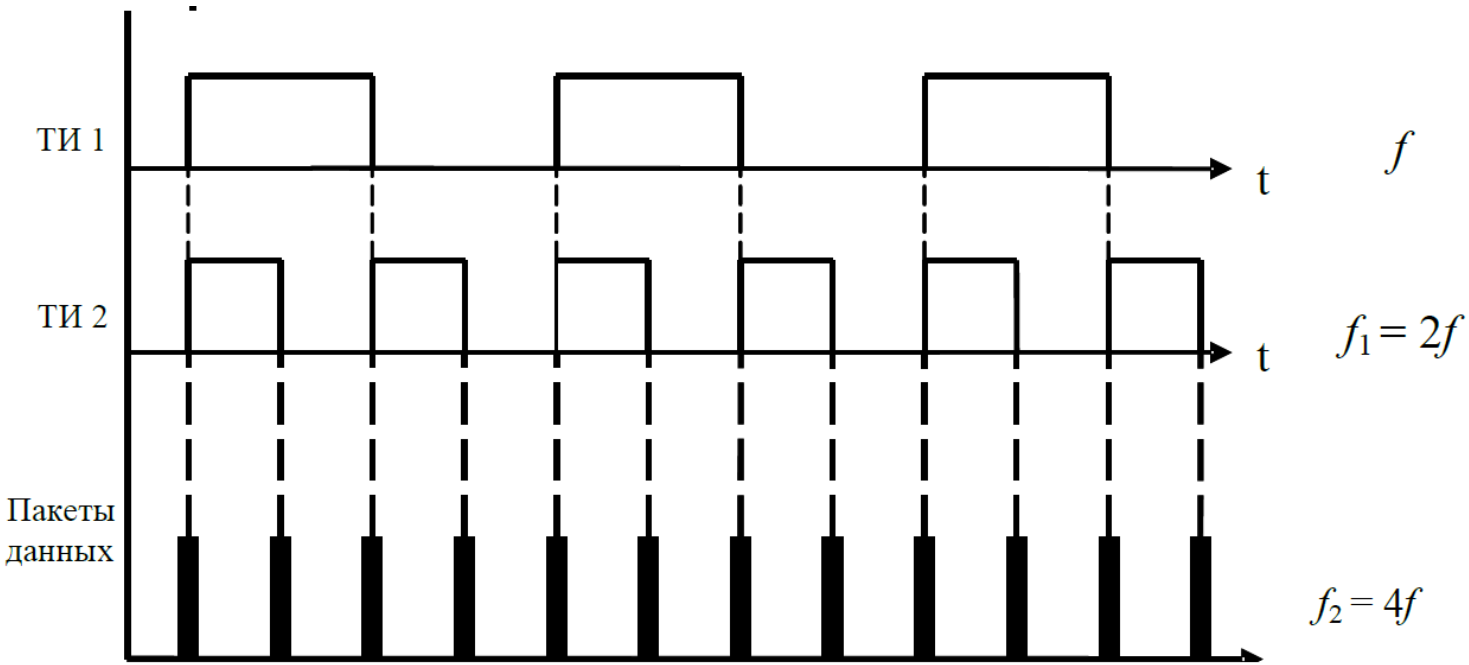
Достоинство – гибкость «разгона» процессора и памяти

Шины процессор-чипсет. FSB шина

Шина FSB – **QPB**, или Quad-Pumped Bus, способна передавать четыре блока данных за такт и два адреса за такт

64 разрядная шина ->256 бит информации за такт

(на самом деле меньше, так как часто данные занимают меньше 64 бит)



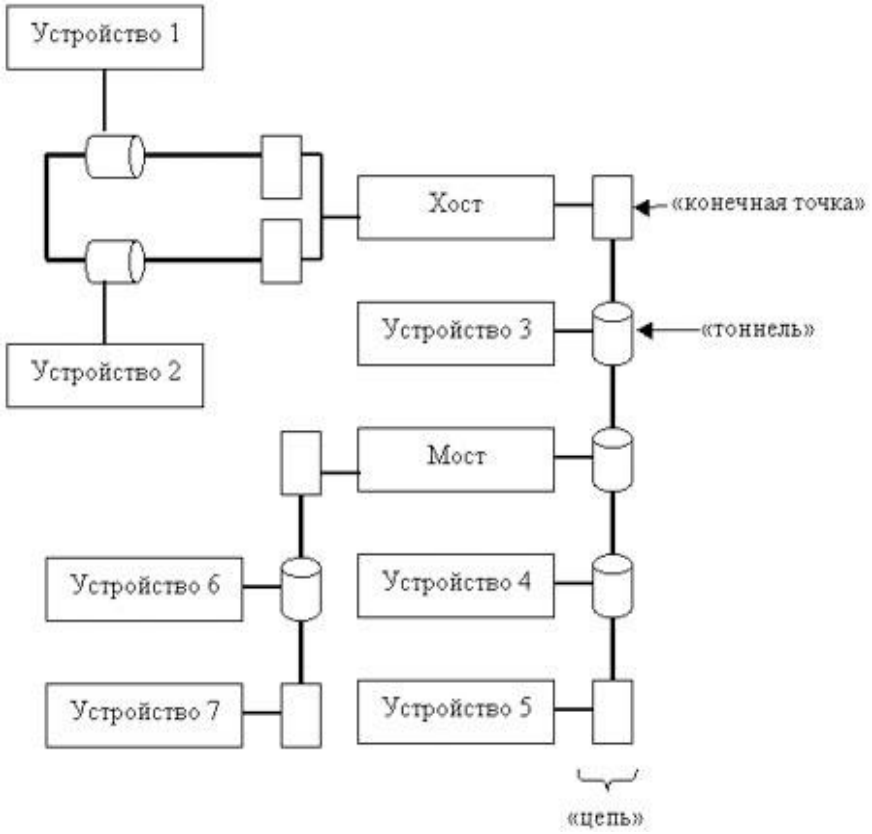
Временная диаграмма шины FSB-QPB

ТИ 1 и ТИ 2 – тактовые импульсы; f – частота ТИ 1; f_1 - частота ТИ 2;

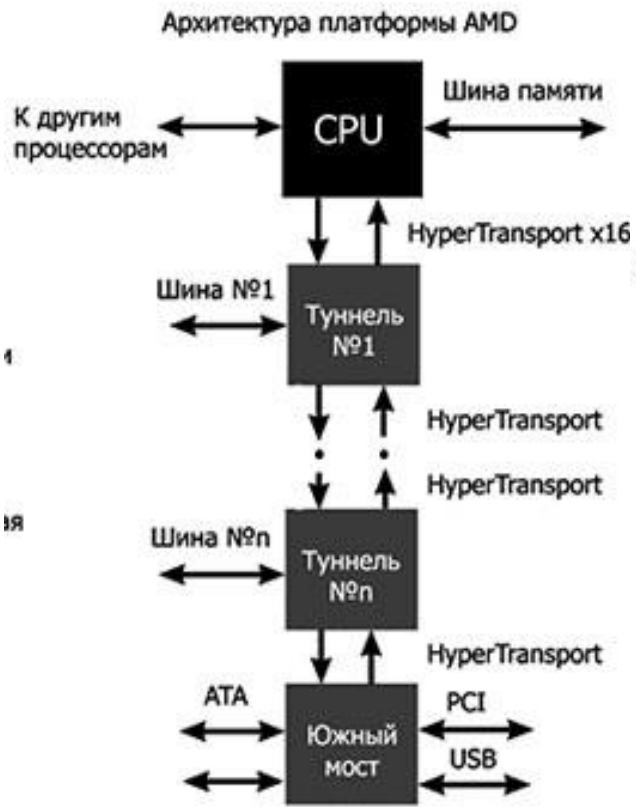
f_2 – частота передачи пакетов данных по шине FSB

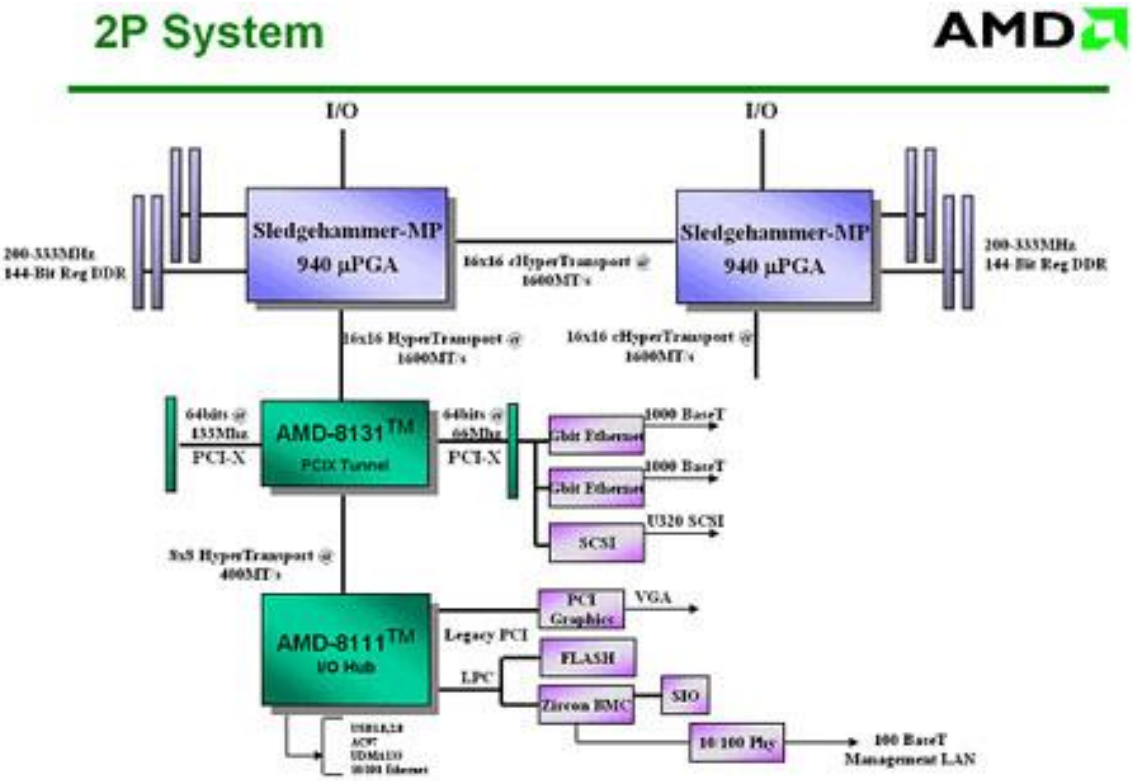
Шины процессор-чипсет. HyperTransport (HT) шина

- Двунаправленная последовательно/параллельная компьютерная шина технология точка-точка.
- **Синхронность** - частота ядра, ОЗУ и шины HyperTransport, привязаны к «шине» тактового генератора (HTT), -является опорной. (регулируются множителями)
- **Топология на основе моста и тоннелей**, объединённых в цепи – последовательное объединение нескольких **туннелей**)
- **Мосты** (выполняет маршрутизацию пакетов между отдельными цепями),
- Архитектура легко масштабируется.
- Автоматическое определение ширины шины
- **DDR**.
- **Позволяет передавать асимметричные потоки данных** к периферийным устройствам и от них



Шины процессор-чипсет. HT шина





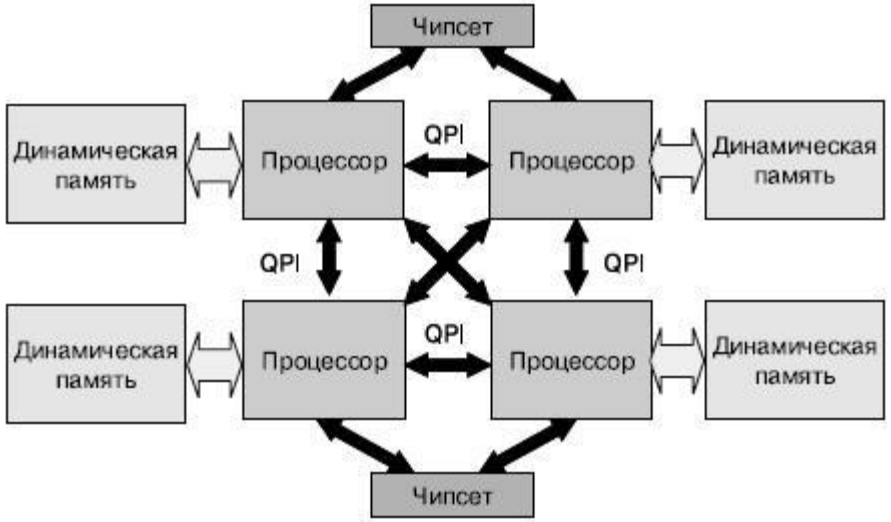
Примеры использования HT:

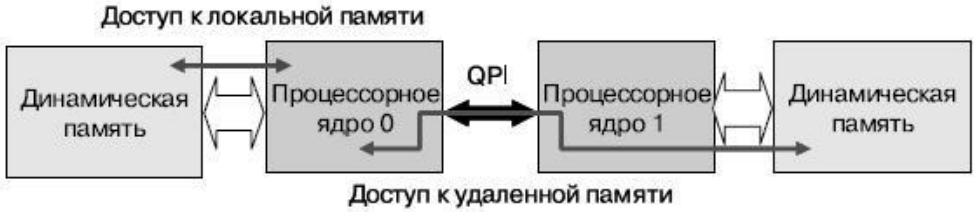
AMD процессоры, чипсеты nForce, ATI Radeon, Xbox, CISCO

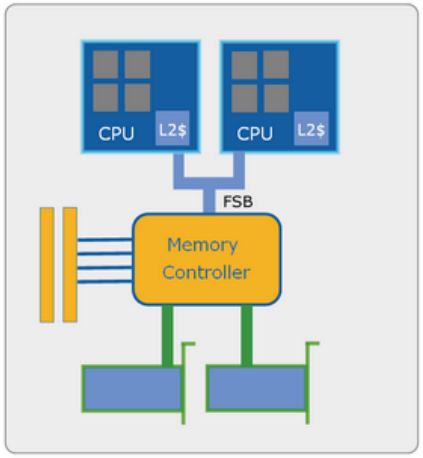
Обеспечивающая высокую скорость при низкой латентности, простота масштабирования устройств

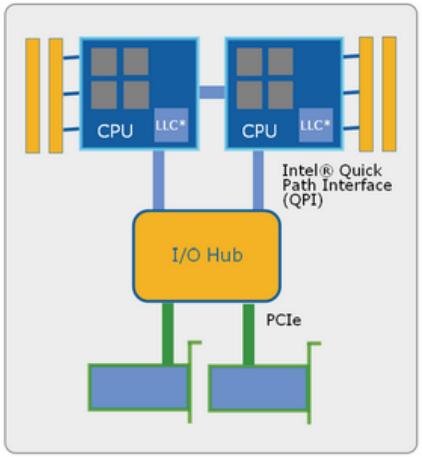
Шины процессор-чипсет. QPI шина

- Служит **для соединения устройств в системе между собой**, а также для «общения» процессоров между собой в многопроцессорных системах.
- **Кэш—когеренстность** (передача кэш-данных в обход оперативной памяти на полной скорости шины).
- **Двунаправленный высокоскоростной обмен данными** между процессором и внешней памятью, а также между процессором и контроллером ввода/вывода
- **Специальные линии контроля ошибок передачи данных.**
- **Параллельное соединение устройств.**
- Шина памяти встроена в процессор.
- В основном используют в серверах.





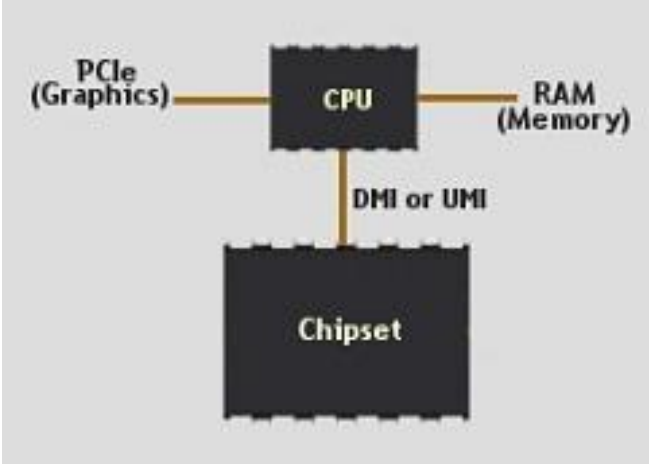




Шины процессор-чипсет. Современные тенденции

Проблема– компенсация латентности доступа к памяти и быстродействующим устройствам.

<u>В современных ЭВМ используют шины типа DMI (Intel) и UMI (AMD), а шины QPI и HT находятся внутри процессора</u>



Особенности:

- Обеспечивается высокая скорость при низкой латентности,
- Технология точка-точка,
- Наличие в процессоре нескольких отдельных шин,
- Специальные шины для непосредственной связи процессора с памятью и хабами PCI-Express
    - **Преимущество** - уменьшение задержек (латентности) при обращении процессора к оперативной памяти, (из пути следования данных по маршруту «процессор – ОЗУ» (и обратно) исключаются такие загруженные элементы, как интерфейсная шина и контроллер северного моста).
- **Синхронизация работы шины единым устройством,** частоты каждого устройства регулируются коэффициентами.

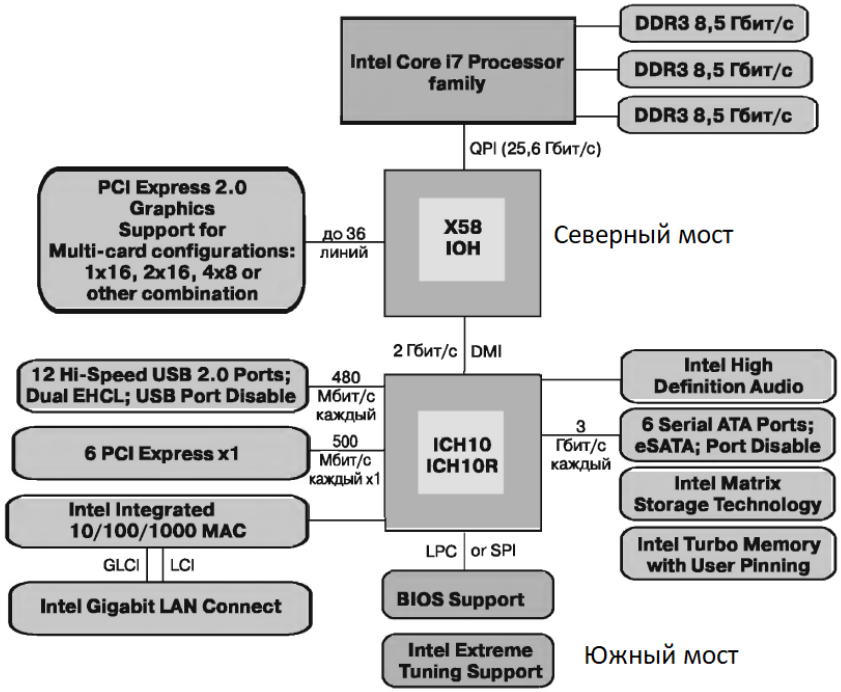
Особенности архитектуры чипсетов

Аппаратные средства телекоммуникационных систем. Особенности архитектуры системных плат

Особенности чипсетов

Архитектура системной платы определяется набором микросхем (chipset):

- таймеры,
- система управления "обвязки" микропроцессора
- контроллеры прерываний
- контроллеры прямого доступа к памяти
- контроллеры связи между памятью и шиной,
- часы реального времени
- клавиатурный контроллер
- контроллеры внешних устройств

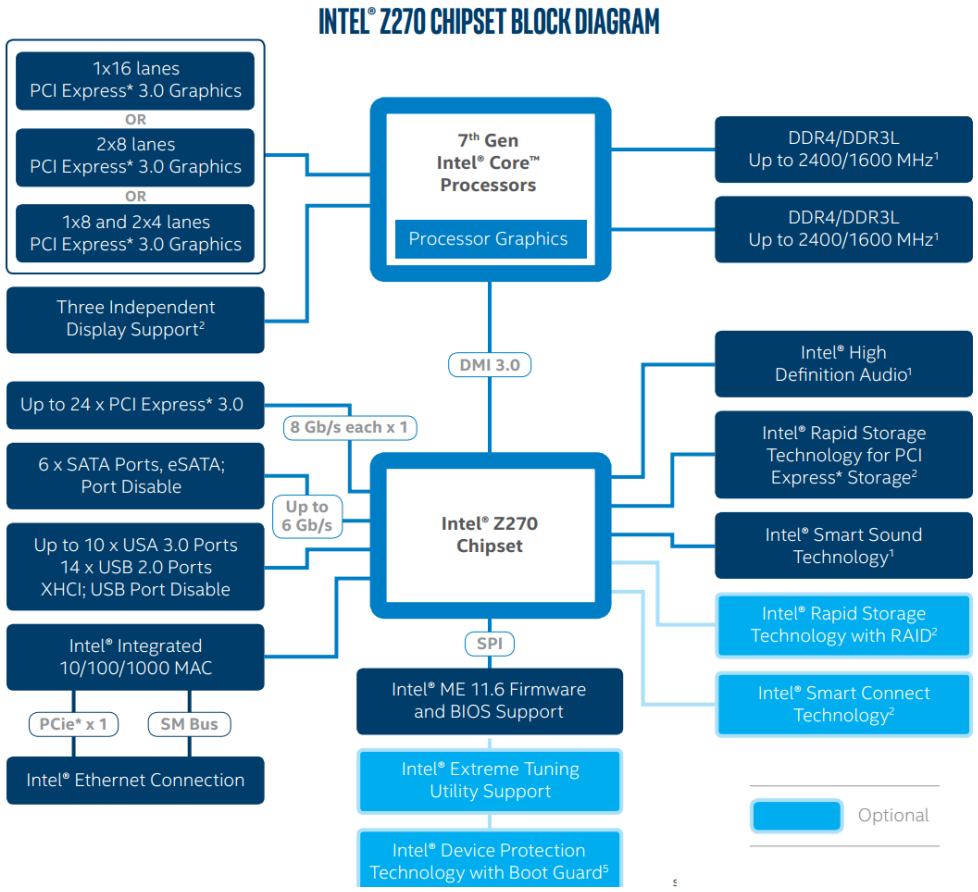


Чипсет определяет основные функциональные возможности платы:

- типы поддерживаемых процессоров,
- структура/объем кэша,
- возможные сочетания типов и объемов модулей памяти,
- поддержка режимов энергосбережения,
- возможность программной настройки параметров

Современные версии чипсетов Intel

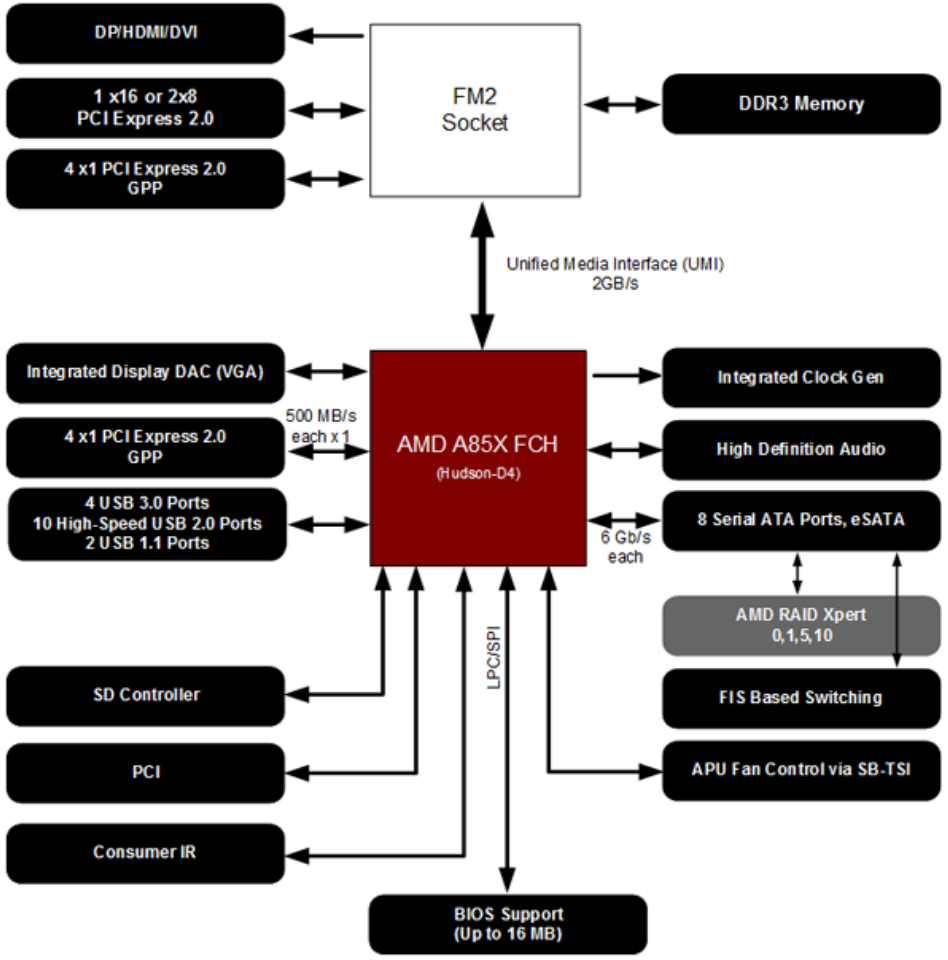
Современные чипсеты
Использование субядра процессора для доступа к главным компонентам ПК (функции северного моста).
Оптимизация частоты процессора (turboboost).
QPI встроена в процессор.
Выделенные линии PCI-e в процессоре.
Создание RAID массивов для хранения данных (с резервированием или проверкой данных).
Поддержка SLI – объединение видеоадаптеров
64 разрядная шина



Фирмы производители чипсетов Intel, а также NVidea, и Asus.

Современные версии чипсетов AMD

Современные чипсеты
Использование субядра процессора для доступа к главным компонентам ПК (функции северного моста).
Оптимизация частоты процессора (turboboost).
HyperTransport встроена в процессор.
Шина работы с процессором UMI
PCI-e16=2xPCI-e8 (CrossFireX)
64 разрядная шина
RAID массивы



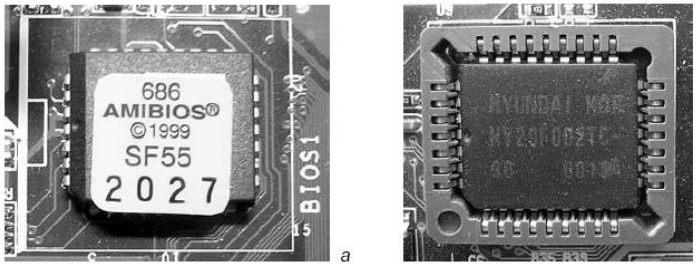
Особенности базовых систем ввода-вывода BIOS и UEFI

Аппаратные средства телекоммуникационных систем. Особенности архитектуры системных плат

Базовая система ввода-вывода (BIOS)

Базовая система ввода-вывода (Basic Input-Output System, BIOS) – система компонентами ЭВМ на основе средств, предоставляемых чипсетом.

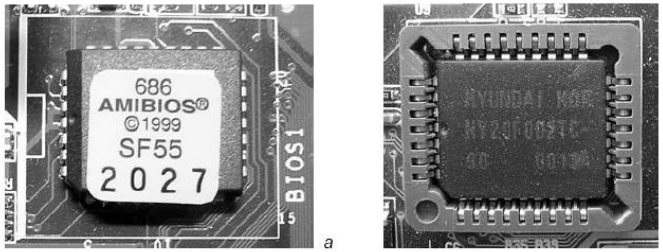
- BIOS представляет собой набор микропрограмм, которые хранятся в постоянной (энергонезависимой) памяти ROM BIOS CMOS или флэш-памяти (Flash) (ПЗУ базовой системы ввода-вывода).
- Системный модуль BIOS должен обслуживать в соответствии со своими функциям все компоненты, установленные на системной плате: процессор, контроллер (памяти (ОЗУ и кэш), прерываний и DMA, системный таймер, системный порт, CMOS RTC, клавиатуры, ЗУ, стандартные периферийных контроллеры и адаптеры, даже если они не установлены на системной плате.



ROM BIOS

Базовая система ввода-вывода (BIOS)

- BIOS находится на самым нижнем уровне ПО, который *обеспечивает изоляцию вышестоящих уровней от подробностей реализации аппаратных средств компьютера.*
- BIOS должен соответствовать конкретной материнской плате.
- BIOS обеспечивает программную поддержку стандартных устройств ЭВМ, конфигурирование аппаратных средств, их диагностику и вызов загрузчика операционной системы.
  - Любые изменения конфигурации (например, информация о новом винчестер, время и дата) записываются в специальную область памяти RAM.
    - Данная область памяти находится в южном мосте чипсета и питается от специальной батарейки.



CMOS ROM BIOS

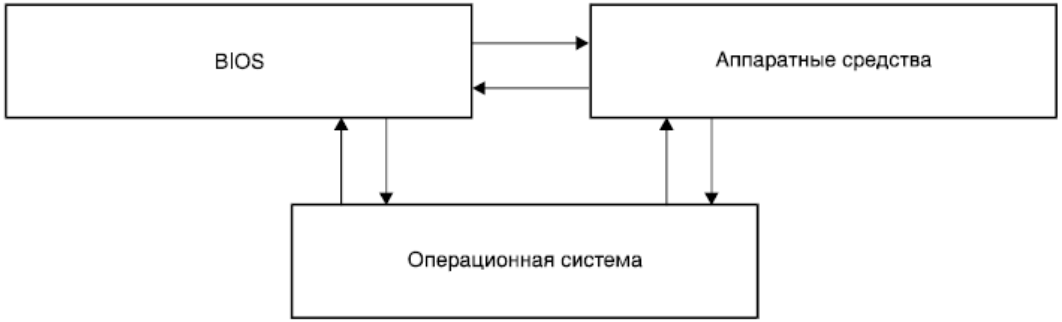
CMOS RAM BIOS и батарейка

Базовая система ввода-вывода (BIOS). Функции

- Инициализация и начальное тестирование аппаратных средств — **POST**;
- Настройка и конфигурирование аппаратных средств и системных ресурсов — **CMOS Setup**;
- Автоматическое распределение системных ресурсов — **PnP BIOS**;
- Идентификация и конфигурирование устройств PCIe и других— **PCI BIOS**;
- Начальная загрузка (первый этап загрузки операционной системы) — **Bootstrap Loader** (Master Boost Recorder, или MBR — главная загрузочная запись;)
- Обслуживание аппаратных прерываний от системных устройств (таймера, клавиатуры, дисков) — **BIOS Hardware Interrupts**;
- Отработка базовых функций программных обращений (сервисов) к системным устройствам — **ROM BIOS Services**;
- Поддержка управляемости конфигурированием — **DMI BIOS**;
- Поддержка управления энергопотреблением и автоматического конфигурирования — например утилиты **APM и ACPI BIOS**.

Базовая система ввода-вывода (BIOS). Plag&Play (PnP)

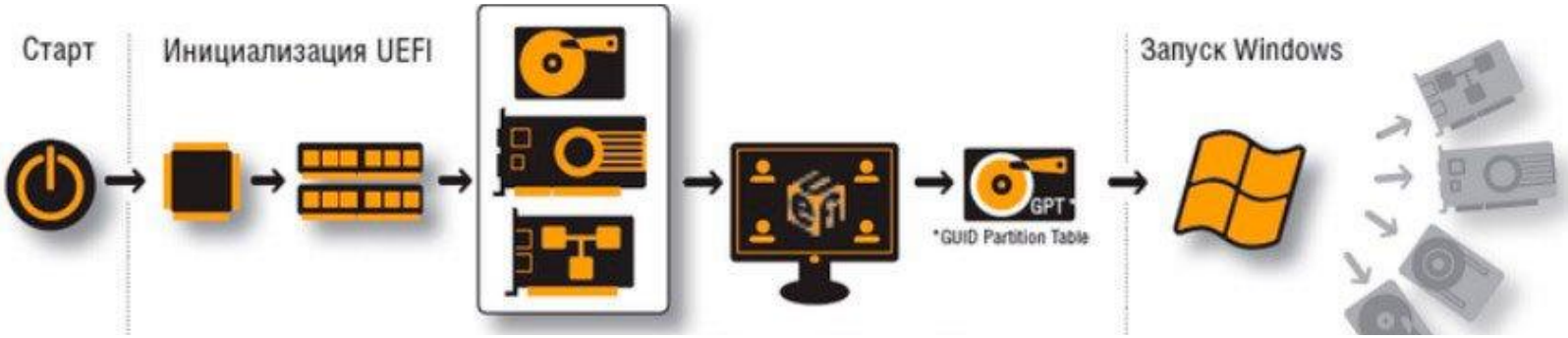
- Стандарт Plag&Play (подключай и работай) позволяет системам и адаптерам, поддерживающим его, автоматически настраивать друг друга и определятся в операционной системе (автоматически определять драйвер).
- Стандарт настраивает для каждого устройства (мышь, клавиатура, платы расширения) :
  - определенное адресное пространство,
  - линии прерываний (IRQ),
  - каналы прямого доступа к памяти (DMA)
  - адреса ввода/вывода (I/O).
- Аппаратные средства, поддерживающие стандарт Plug&Play, информируют BIOS и операционную систему о необходимых им ресурсах и, самонастраиваются на основании полученной информации.
- Plug&Play настраивается в режиме POST.
- Устройства PnP



Базовая система ввода-вывода (BIOS). UEFI-BIOS

Unified Extensible Firmware Interface - стандартизированный расширяемый интерфейс встроенного программного обеспечения – является расширенным BIOS. (изначально EFI от Intel), (UEFI поддерживается начиная с Windows 7 sp1)

BIOS последовательно проверяет все компоненты и ищет загрузчик ОС на ЗУ. Драйвера загружаются в ОС



UEFI проверяет компоненты, инициализирует дайвера, позволяет запускать программы в своей ОС, заранее хранит информацию об загрузчике ОС и о драйверах, ОС может использовать драйвера UEFI

Базовая система ввода-вывода (BIOS). UEFI-BIOS

.

	ХАРАКТЕРИСТИКИ BIOS LEGACY	ХАРАКТЕРИСТИКИ UEFI
Поддерживаемые режимы работы процессора	Режим реальных адресов	Режим реальных адресов, защищенный режим
виртуальная память	Не поддерживает	Поддерживает
Объем ОЗУ	1 Мбайт	Не ограничен
Пространство опционального ПЗУ (Option ROM)	1 Мбайт	Не ограничено
Доступ к регистрам	16-битный	16, 32,64 -битный,
Независимость от архитектуры	Не обеспечивает	Обеспечивает
Язык программирования	Ассемблер	Си/ассемблер
Функция безопасной загрузки	Отсутствует	Присутствует
Таблица разделов жесткого диска	MBR	GPT

Базовая система ввода-вывода (BIOS). Особенности UEFI

- Снижение времени на загрузку
  - параллельной инициализации и хранения информации о драйверах и адресах загрузки ОС
- Загрузка дисков объемом более 2 Тб.
  - BIOS для загрузки использовал MBR (Main Boot Record) - основная загрузочная запись, которая может адресовать 2 Тб пространства, UEFI же использует **GPT (Guid Partition Table)** - это стандарт формата размещения разделов на физическом жестком диске, который позволяет адресовать 9,4 ЗБ (Зеттабайт).
  - возможна загрузка в режиме совместимости с диска с разметкой MBR.
  - По умолчанию файловая система **FAT32 с GPT-разделами.**
  - *Загрузчик UEFI хранится по определенному адресу: efi\boot\bootx64.efi*

BIOS

UEFI

Базовая система ввода-вывода (BIOS). Особенности UEFI

- **графический интерфейс** с поддержкой мыши, встроенные программы,
- **Поддержка криптографии** и других методов защиты.
  Secure boot
  - Безопасная загрузка (проверка ОС на изменения с предыдущей загрузки).
  - Набор подписанных ключей драйверов(аутентификация) (драйвера устройств, ОС, платформы).
  - 4 режима работы ПК- настройка, аудит, пользовательский и расширенный. Режимы отличаются уровнем доверия к ключам.
- Поддержка удаленной работы (**настройки UEFI по сети**).
- **Возможность загрузки UEFI с ЗУ** или по сети
- Менеджер загрузок **– выбор ОС**
- **Поддержка встроенных утилит**, таких как, браузер или иногда подобие Live CD, у каждого производителя свой UEFI

Базовая система ввода-вывода (BIOS). Особенности UEFI

- **Основная идея UEFI** — сделать прошивку модульной и расширяемой.
  - UEFI позволяет расширять прошивку через загрузку образов (драйверов или приложений в формате PE32/PE32+.).
- Расширение, а также идентификация компонентов UEFI выполняется с помощью **GUID-записей**.
  - GUID представляет собой уникальный 128-битный идентификатор, соответствующий тому или иному компоненту прошивки.
- Любое устройство или образ в UEFI имеют собственный протокол обработки.
  - Каждый протокол состоит из GUID и структуры интерфейса протокола.
  - Структура интерфейса протокола содержит функции и данные, которые используются для доступа к тому или иному устройству.
- Управление протоколами обеспечивают специальные службы UEFI (LocateProtocol, OpenProtocol и другие).

Примеры образов UEFI

Structure

Name	Action	Type	Subtype	Text
CDBB7B35-6833-4ED6-9AB2-57D2ACDDF6F0		Volume	FFSv2	
DxeCore		File	DXE core	DxeCore
PcdDxe		File	DXE driver	PcdDxe
ReportStatusCodeRouterRuntimeDxe		File	DXE driver	ReportStatusCodeRouterRuntimeDxe
StatusCodeHandlerRuntimeDxe		File	DXE driver	StatusCodeHandlerRuntimeDxe
ReportStatusCodeRouterSmm		File	SMM module	ReportStatusCodeRouterSmm
StatusCodeHandlerSmm		File	SMM module	StatusCodeHandlerSmm
DatahubStatusCodeHandlerDxe		File	DXE driver	DatahubStatusCodeHandlerDxe
StatusCodeRuntimeDxe		File	DXE driver	StatusCodeRuntimeDxe
07A01ACF-46D5-48DE-A63D-74FA92AA8450		File	DXE driver	GenericIpmi
D14443FF-3626-4BCC-8204-196D11F06BC5		File	SMM module	SmmGenericIpmi
490D0119-4448-440D-8F5C-F58FB53EE057		File	DXE driver	PolicyInitDxe
SectionExtractionDxe		File	DXE driver	SectionExtractionDxe
E0471A15-76DC-4203-8B27-6DB4F8BA644A		File	DXE driver	UbaConfigDatabaseDxe