Глава 1

Устройство и принципы работы компьютера

- Что находится внутри системного блока
- Процессор
- Системная плата и чипсет
- Оперативная память
- Шины
- Платы расширения
- Порты
- Устройства хранения информации
- Системные ресурсы и их распределение

Прежде чем приступить к изучению параметров BIOS, следует ближе познакомиться с устройствами, находящимися в системном блоке, и с их взаимодействием между собой.

Что находится внутри системного блока

Персональный компьютер состоит из отдельных устройств и модулей: одни находятся внутри системного блока, другие к нему подключаются. Последние служат для ввода или вывода информации: монитор, принтер, сканер, клавиатура, мышь и др.

Внутри системного блока находятся устройства для обработки и хранения информации (рис. 1.1). В зависимости от конфигурации компьютера они могут быть различными, но большинство типичных системных блоков включает следующие устройства.

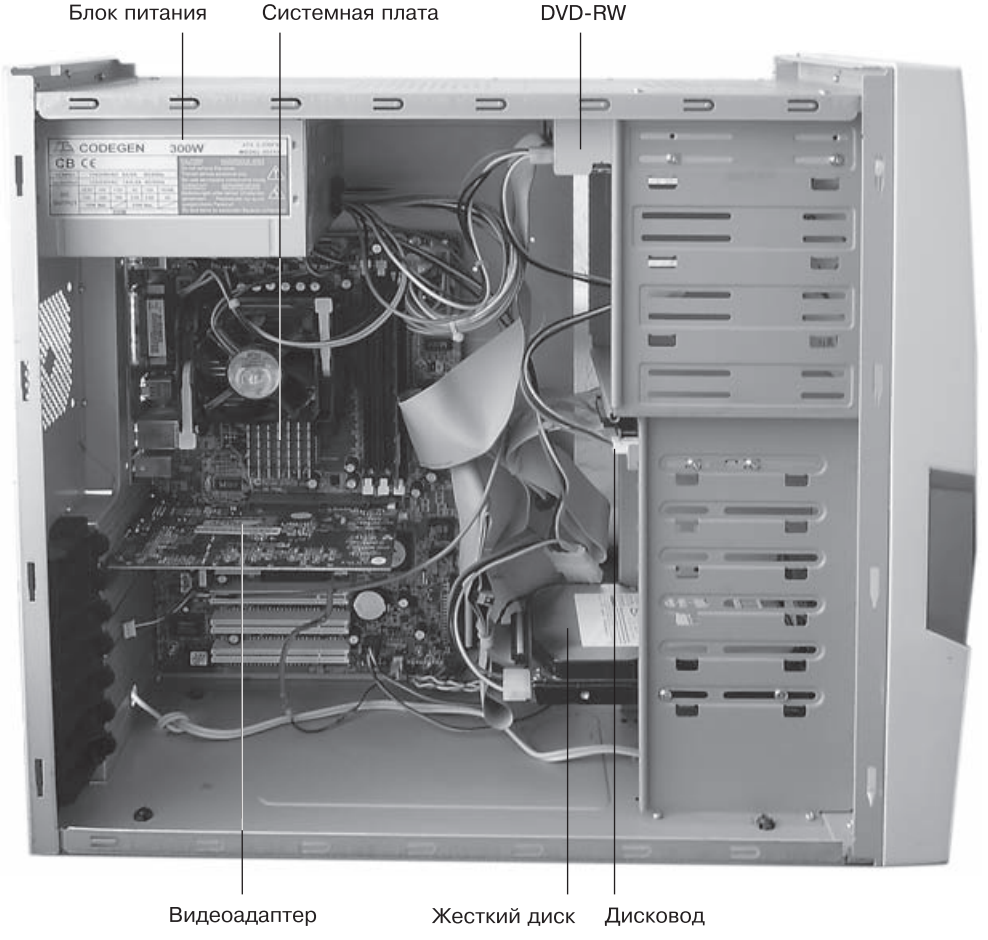

Рис. 1.1. Системный блок типичного персонального компьютера

- **Блок питания.** Вырабатывает стабилизированные напряжения для питания всех устройств, находящихся в системном блоке. От блока питания выходят многочисленные кабели, которые подключаются к системной плате, дисковым накопителям и другим устройствам.
- **Системная, или материнская, плата.** Базовое устройство компьютера для установки процессора, оперативной памяти и плат расширения. К ней подключаются устройства ввода/вывода, дисковые накопители и др. Системная плата обеспечивает их взаимодействие, используя специальный набор микросхем системной логики, или *чипсет* [1]. На системной плате также располагаются другие устройства, например микросхема BIOS, батарейка для питания часов и CMOS (память с автономным питанием), тактовый генератор.
- **Процессор.** Является «сердцем» компьютера и служит для обработки информации по заданной программе.
- **Оперативная память.** Используется для работы операционной системы, программ и для временного хранения текущих данных. Она выполнена в виде модулей, установленных на системную плату, и может хранить информацию только при включенном питании.
- **Видеоадаптер.** Обычно выполняется в виде платы расширения и служит для формирования изображения, которое потом выводится на монитор. Современные видеоадаптеры содержат мощный видеопроцессор и большие объемы видеопамяти, что позволяет формировать трехмерное изображение с высоким разрешением. Для недорогих компьютеров выпускаются системные платы с интегрированным видеоадаптером, и его не нужно устанавливать дополнительно.
- **Жесткий диск.** Основное устройство для хранения информации в компьютере.
- **Дисковод.** Хотя дискеты уже морально устарели, но дисководы для их чтения еще присутствуют в большинстве компьютеров.
- **Привод для CD/DVD.** CD/DVD широко используются для распространения информации, поэтому приводы есть почти в каждом компьютере.
- **Платы расширения.** При необходимости в системный блок можно установить дополнительные устройства, выполненные в виде плат или карт расширения. Примерами таких устройств могут быть модемы, сетевые платы, ТВ-тюнеры и многие другие.

Процессор

В подавляющем большинстве персональных компьютеров используются процессоры, совместимые с процессорами семейства x86 компании Intel. Модели 8086, 286, 386 и 486 были популярны в 1980-х годах, но сегодня представляют лишь

[1] Современные чипсеты выполняют множество различных функций и подробно будут рассмотрены далее.

исторический интерес. Дальнейшим развитием семейства x86 стал появившийся в 1993 году процессор Intel Pentium, затем модели Pentium II/III/IV. С 2006 года компания Intel выпускает процессоры, основанные на архитектуре Intel Core 2, которые являются наиболее популярными на момент выхода книги. Для установки в недорогие компьютеры выпускается процессор Celeron, который являет собой упрощенный вариант соответствующей модели Pentium II/III/IV или Core 2.

В 1980-х годах компания Intel была безоговорочным монополистом на рынке процессоров, но постепенно она утрачивала этот статус в конкурентной борьбе с компанией AMD, а к 2005 году процессоры от AMD даже превосходили по производительности процессоры Intel. С выходом процессоров семейства Core 2 компания Intel вернула себе статус лидера, но процессоры AMD сохранили свою долю в бюджетном сегменте рынка.

Компания AMD начинала с выпуска процессоров, полностью совместимых с Intel 386, 486 и Pentium и устанавливаемых в те же разъемы. Позже AMD разработала собственные процессоры Athlon и Duron, а на момент выхода книги основными моделями процессоров AMD являлись Athlon 64/X2 и новый многоядерный процессор Phenom. Для дешевых компьютеров компания AMD выпускает процессор Sempron.

Современный процессор — это микросхема с несколькими сотнями выводов, которая устанавливается в специальный разъем на системной плате; сверху на нем закрепляется радиатор с вентилятором для охлаждения (его также называют кулером). На рис. 1.2 показан фрагмент системной платы с процессором и кулером, а на рис. 1.3 те же устройства, но в разобранном состоянии. Установка процессора в разъем требует особой осторожности и аккуратности и обычно подробно описана в инструкции к системной плате.

Работа процессора заключается в последовательном выполнении команд из оперативной памяти, и чем больше команд успевает выполнить процессор за секунду, тем выше производительность компьютера в целом. Скорость работы процессора зависит от нескольких параметров: тактовой частоты, количества ядер, объема кэш-памяти и некоторых других. Рассмотрим все параметры процессоров более подробно.

- **Частота FSB.** Для обмена данными с другими устройствами процессор использует шину FSB (Front Side Bus). Во всех современных системах используются технологии, умножающие скорость обмена данными по системной шине, и частота FSB может указываться уже с учетом умножения. Например, для процессора Intel Core 2 Duo E6600 реальная частота FSB составляет 266,6 МГц, а поскольку в большинстве процессоров семейства Intel Core 2 используется четырехкратное умножение частоты FSB, то эффективное значение будет равно $266{,}6 \times 4 = 1066$ МГц. Именно такое значение вы можете встретить в технических характеристиках процессоров и прайс-листах компьютерных магазинов.

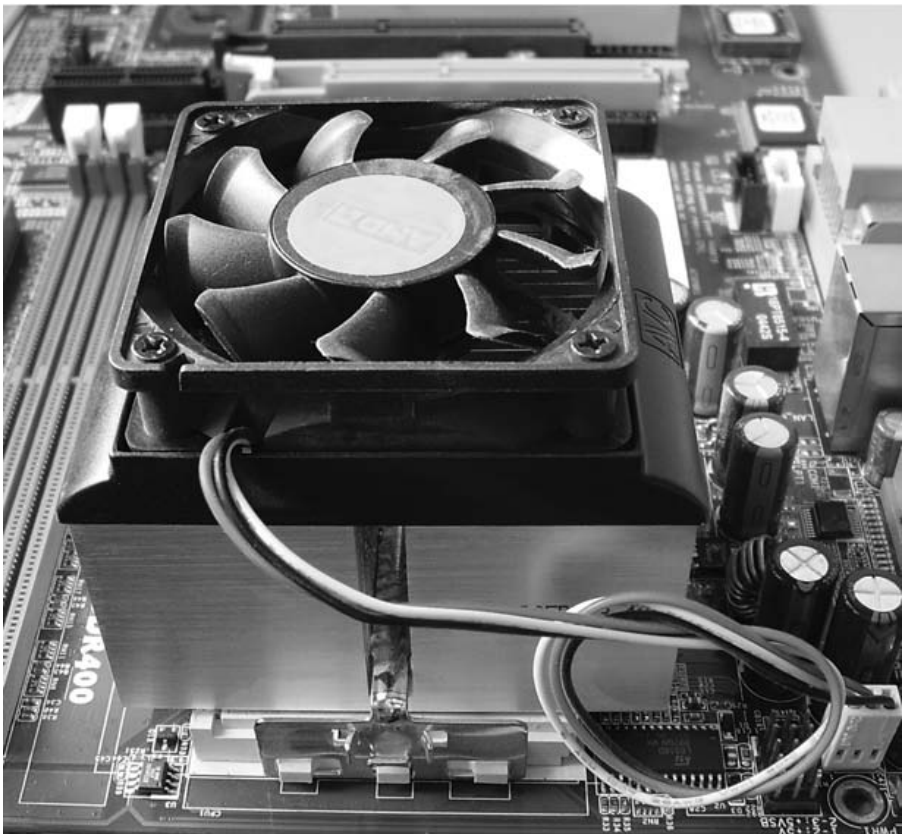

Рис. 1.2. Процессор с закрепленным на нем кулером

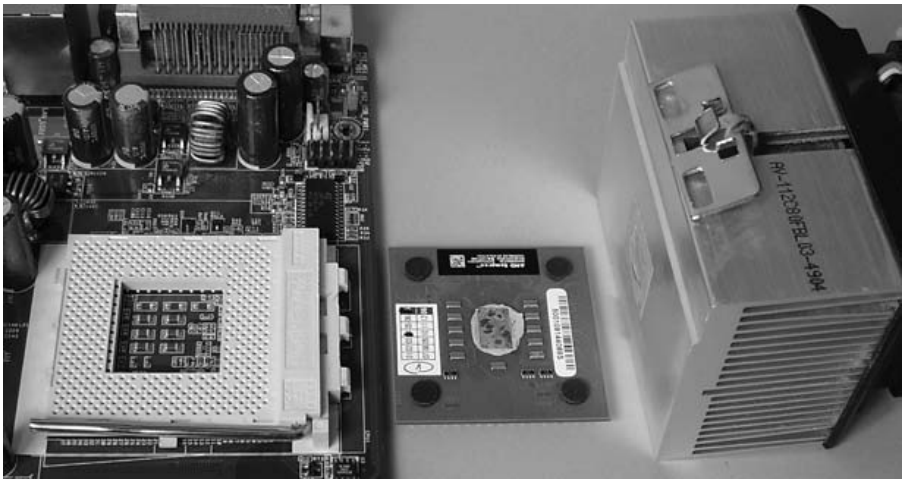

Рис. 1.3. Системная плата, процессор и кулер

Для большинства процессоров AMD Athlon 64/X2 и AMD Phenom частота FSB составляет 200 МГц, а для обмена данными с чипсетом используется шина HT (Hyper Transport), которая работает на частотах, в несколько раз превышающих частоту FSB.

- **Множитель, или коэффициент умножения.** Ядро центрального процессора работает на тактовой частоте, являющейся произведением частоты FSB на коэффициент умножения. Например, для уже упомянутого процессора Intel Core 2 Duo E6600 частота FSB — 266,6 МГц, множитель — 9, в результате тактовая частота будет равна 2400 МГц.
- **Тактовая частота.** Параметр, показывающий реальную частоту работы ядра процессора, которая для современных процессоров может находиться в диапазоне 1,5–4 ГГц. Тактовая частота определяется умножением частоты внешней шины процессора (FSB) на коэффициент умножения.

  Поскольку тактовая частота процессора зависит от шины FSB, есть возможность заставить его работать с большей скоростью, изменив частоту FSB. Эта операция называется разгоном и будет подробно рассмотрена в гл. 17.
- **Количество ядер.** Поскольку тактовые частоты современных процессоров приблизились к физическому пределу, для повышения их производительности применяется объединение нескольких процессорных ядер в одном корпусе. На момент написания книги процессоры с одним ядром (одноядерные) устанавливались только в самые дешевые компьютеры, в большинстве новых компьютеров использовались двуядерные процессоры, а наиболее производительные системы собирались на основе четырехъядерных процессоров.
- **Тип ядра и степпинг.** Современные процессоры умеют выполнять за один такт сразу несколько команд, и этот показатель постоянно увеличивается. При одинаковых значениях тактовой частоты и количестве ядер процессоры с более современной архитектурой будут работать быстрее. Например, процессор Celeron 420 с тактовой частотой 1600 МГц работает приблизительно в два раза быстрее старых моделей Celeron с частотами 1700–2000 МГц.

  Конструкция процессоров и технология их производства постоянно совершенствуются, и одна модель может иметь несколько версий исполнения. Для обозначения внутренней архитектуры процессора разработчики придумывают их ядрам кодовые названия. Например, процессор AMD Sempron 2500+ раньше выпускался на ядре с кодовым названием Thoroughbred-B и имел следующие параметры: частота FSB — 166 МГц, множитель — 10,5, реальная частота — 1750 МГц. Позже эта же модель процессора выпускалась на ядре Palermo, и его характеристики несколько изменились: частота FSB — 200 МГц, множитель — 7, реальная частота — 1400 МГц. Процессоры на более новых ядрах, как правило, обладают лучшими характеристиками, но они и более дорогие.

  Одна и та же версия ядра может претерпеть несколько модификаций, связанных с небольшими усовершенствованиями и исправлением ошибок. Модификации

одного и того же ядра называют *степпингами*; процессор с более высоким степпингом обычно работает стабильнее своих предшественников и меньше греется.

- **Объем кэш-памяти.** Процессор работает значительно быстрее, чем оперативная память, и при обращении к ней ему приходится некоторое время ожидать результата. Чтобы уменьшить время ожидания, непосредственно на кристалле процессора устанавливается небольшой объем очень быстрой памяти, называемой *кэш-памятью*. Она содержит данные, наиболее часто используемые процессором, и обычно работает на его тактовой частоте. Специальные алгоритмы для кэш-памяти позволяют своевременно подгружать нужные процессору данные из оперативной памяти, что увеличивает производительность системы.

  Современные процессоры имеют двухуровневую организацию интегрированной кэш-памяти. У кэш-памяти первого уровня (L1) наивысшая скорость и небольшой объем (обычно 16-64 Кбайт). Кэш-память второго уровня (L2) обладает несколько меньшим быстродействием, а ее объем может составлять от 128 Кбайт до нескольких мегабайт в зависимости от модели процессора. В некоторых процессорах также встречается кэш-память третьего уровня (L3) объемом от 1 Мбайт.

- **Название и номер модели (рейтинг).** При маркировке современных процессоров обычно указывают название модели, по которому можно определить принадлежность процессора к определенному семейству, количество ядер и числовой рейтинг производительности, который позволяет сравнить скорость работы процессоров. Например, маркировка `AMD Athlon 64 X2 4800` обозначает процессор фирмы AMD семейства Athlon 64, который является двуядерным (X2) и имеет рейтинг производительности 4800. При маркировке процессоров могут указываться и дополнительные параметры, например тип разъема для установки, частота FSB, объем кэш-памяти L2 и др.

ВНИМАНИЕ

Компании Intel и AMD используют различные подходы при присвоении номеров моделям, и по этому показателю их сравнивать нельзя. Обозначения процессоров Intel вообще весьма условны, и они не всегда точно отражают реальную производительность.

- **Тип разъема, или форм-фактор.** Каждая модель процессора устанавливается в разъем соответствующего типа и с соответствующим количеством контактов. Приведу перечень наиболее популярных процессорных разъемов последнего десятилетия:
  - Socket 370 — для Pentium II/III, Celeron;
  - Socket 478 — для Pentium 4, Celeron;
  - LGA 775 — для всех процессоров семейства Intel Core 2, а также Pentium 4/D/E, Celeron D;
  - Socket A (462) — для Athlon XP, Duron и некоторых моделей Sempron;

- Socket 754 — для Sempron, Athlon 64;
- Socket 939 — для Athlon 64/FX/X2;
- Socket 940 — для Athlon FX;
- Socket AM2 — для новых моделей Athlon 64/FX/X2, Sempron и процессоров Phenom.

Цифра в названии разъема обозначает количество контактов. Установить процессор в непредназначенный для него разъем нельзя, даже если различие всего в один контакт.

- **Напряжение питания ядра.** Ядро современного процессора питается довольно низким напряжением, порядка 1,2–1,7 В. Для каждой модели есть свое паспортное значение этого напряжения, которое обычно задается автоматически. Ручная регулировка иногда используется при разгоне, но это может привести к перегреву процессора и выходу его из строя.
- **Тепловыделение.** Поскольку процессоры работают на очень высоких частотах, они могут обладать большим тепловыделением, достигающим до 100 Вт и более. Для обозначения потребляемой процессором мощности используется параметр TDP (Thermal Design Power). Производители процессоров используют различные технологии снижения энергопотребления. В наиболее экономичных моделях удается снизить тепловыделение до 20–30 Вт, что особенно важно для ноутбуков.

  Эксплуатация процессора невозможна без системы охлаждения, в качестве которой используются массивные радиаторы с установленными на них вентиляторами.

Для современных процессоров характерен набор дополнительных функций и технологий, расширяющих их возможности.

Процессоры AMD в зависимости от модели могут поддерживать различные технологии.

- **3DNow!, SSE, SSE2, SSE3.** Наборы дополнительных инструкций для процессора, ускоряющих работу с мультимедиа и большими объемами данных.
- **Cool'n'Quiet.** Технология энергосбережения, требующая поддержки со стороны операционной системы (не ниже Windows XP SP2), которая «заставляет» процессор снизить тактовую частоту, если его нагрузка невелика.
- **NX-bit (No Execute).** Технология защиты компьютера от вирусов, запрещающая запуск кода из области данных. Поддерживается операционной системой не ниже Windows XP SP2.
- **AMD64.** Технология, позволяющая выполнять 64-битные инструкции, то есть устанавливать 64-разрядные операционные системы.
- **AMD virtualization (AMD-V).** Аппаратная поддержка одновременной работы нескольких виртуальных машин на одном компьютере. Для реализации этой

технологии понадобится специальная программа — менеджер виртуальных машин, которая будет распределять ресурсы компьютера между несколькими операционными системами. Наличие этой технологии совсем необязательно для установки и запуска виртуальных машин, однако она повышает эффективность работы с ними.

У процессоров Intel дополнительные функции и технологии похожи.

- **MMX, SSE, SSE2, SSE3.** Наборы инструкций для процессора, ускоряющих работу с мультимедиа и большими объемами данных.
- **Технология HT (Hyper-Threading Technology).** Технология, позволяющая выполнять несколько потоков команд одновременно, использовалась только в некоторых процессорах семейства Pentium IV.
- **TM1 (Thermal Monitor 1) и TM2 (Thermal Monitor 2).** Технология защиты процессора от перегрева. В режиме TM1 процессор пропускает несколько рабочих тактов при достижении критической температуры, а в режиме TM2 снижается его тактовая частота.
- **Enhanced Halt State, или C1E.** Режим пониженного энергопотребления, активирующийся при поступлении на процессор команды Halt, то есть если нет полезных задач.
- **EIST (Enhanced Intel SpeedStep Technology).** Технология энергосбережения, аналогичная Cool'n'Quiet, динамически изменяющая с помощью операционной системы тактовую частоту процессора.
- **XD (Execute Disable Bit).** Технология, запрещающая запуск кода из области данных, аналогичная NX-bit.
- **EMT64.** Технология, аналогичная AMD64, позволяющая выполнять 64-битные инструкции.
- **Intel Trusted Execution**. Новая технология защиты от вредоносных программ на аппаратном уровне, которую поддерживают новые модели процессоров семейства Core 2. Для ее реализации требуется поддержка со стороны процессора, чипсета (наличие доверенного платформенного модуля TPM) и операционной системы.
- **VT (Virtualization Technology)**. Аппаратная поддержка одновременной работы нескольких виртуальных машин на одном компьютере, аналогичная AMD-V.

Системная плата и чипсет

Наиболее важные компоненты компьютера располагаются на системной плате, типичный пример которой показан на рис. 1.4. Основа любой системной платы — *чипсет*, то есть набор микросхем, обеспечивающих взаимодействие между процессором, памятью, накопителями и другими устройствами. В его состав входят два основных чипа, которые обычно называются *северным* (*Northbridge*) и *южным*

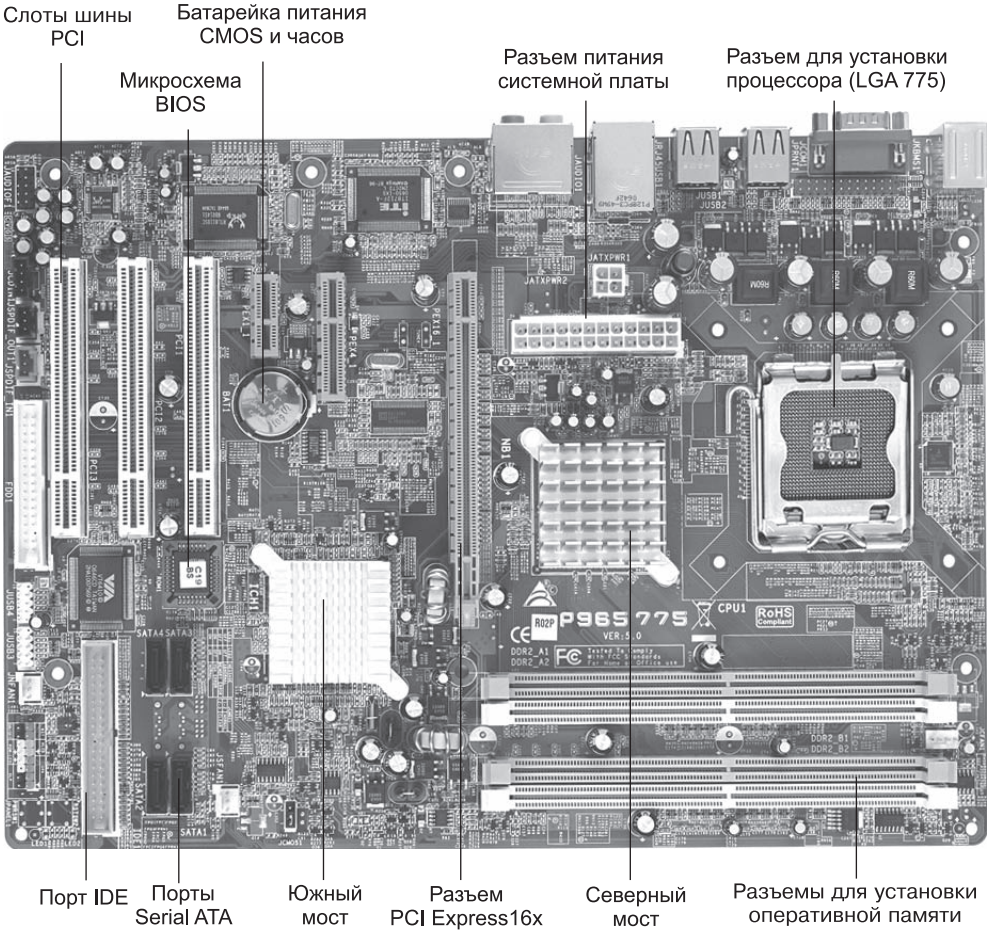

Рис. 1.4. Системная плата

(*Southbridge*) *мостами* (рис. 1.5). Иногда северный мост называют системным контроллером, а южный — функциональным контроллером. В чипсетах для процессоров Intel северный мост обозначается MCH (Memory Controller Hub), а южный — ICH (Input/Output Controller Hub).

Основная задача северного моста — обеспечить связь процессора с оперативной памятью и видеосистемой. Данными процессор и северный мост обмениваются с помощью шины FSB, северный мост и оперативная память — с помощью специальной шины памяти, северный мост и видеосистема — с помощью PCI Express (в устаревших чипсетах — с помощью шины AGP). В некоторых чипсетах в состав северного моста также входит интегрированный видеоадаптер.

Северный мост сильно нагревается во время работы, поэтому для его охлаждения используют радиатор, а в некоторых случаях и вентилятор.

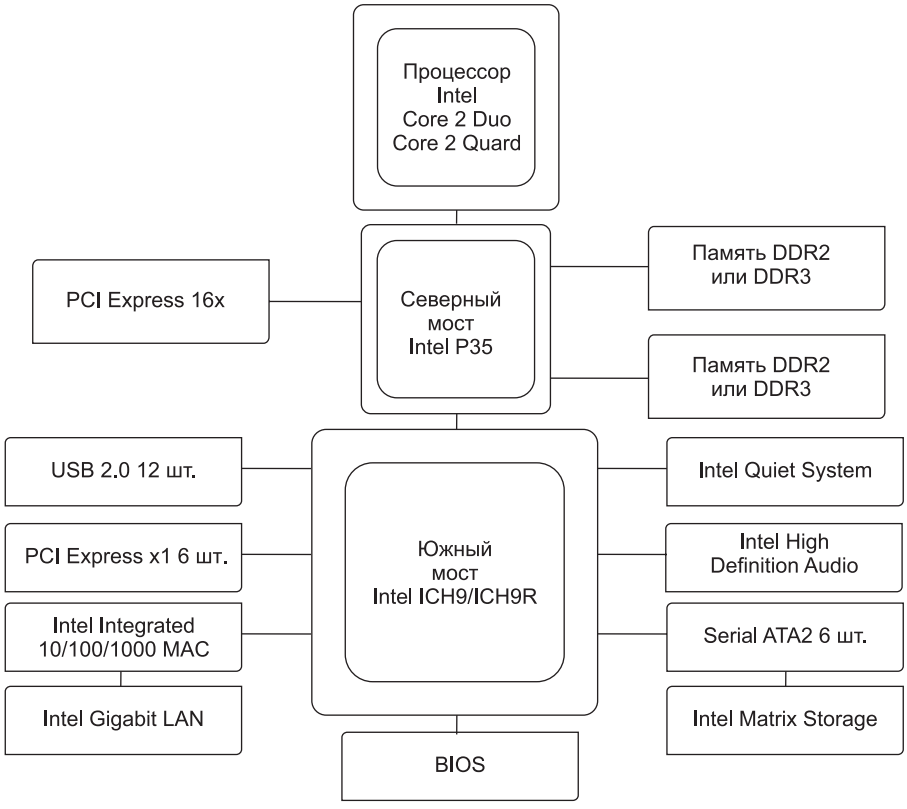

Рис. 1.5. Структурная схема чипсета Intel P35

В чипсетах для процессоров Athlon 64/X2 и Phenom контроллер оперативной памяти интегрирован непосредственно в процессор, а северный мост выполняет функции контроллера PCI Express. Чипсеты для современных процессоров Athlon/Phenom выпускают компании AMD, nVidia и VIA, причем чипсеты nVidia могут состоять всего из одного чипа, который совмещает функции северного и южного мостов.

Южный мост обменивается данными с северным мостом и различными периферийными устройствами. Большинство контроллеров периферийных устройств интегрировано непосредственно в южный мост. Вот функциональный состав типичного южного моста:

- контроллер IDE;
- контроллер Serial ATA/RAID;
- контроллер дисковода;
- контроллер шин PCI и ISA;
- USB-контроллер;

- звуковой контроллер;
- сетевой интерфейс;
- контроллеры портов ввода/вывода.

Кроме того, южный мост взаимодействует с микросхемами BIOS и CMOS[1]. Во многих современных чипсетах микросхема CMOS интегрирована в состав южного моста.

В табл. 1.1 приведены основные характеристики некоторых чипсетов для процессоров семейства Intel Core 2.

Таблица 1.1. Основные характеристики популярных чипсетов для процессоров семейства Intel Core 2

Производитель и марка чипсета	Поддерживаемые частоты шины, МГц	Тип и частота поддерживаемой памяти, МГц	Северный/южный мост	Интегрированный видеоадаптер	Порты для внешнего видеоадаптера
Intel 945GC	533/800	DDR2 533/667	82945GC/ ICH7	GMA 950	PCIEx16
Intel 975X	533/667/800/1066	DDR2 400/533/667/800	82975X/ ICH7	—	1xPCIEx16 2xPCIEx8
Intel P965	533/800/1066	DDR2 533/667/800	82P965/ ICH8	—	PCIEx16
Intel G965	533/800/1066	DDR2 533/667/800	82G965/ ICH8	GMA X3000	PCIEx16
Intel Q965	533/800/1066	DDR2 533/667/800	82Q965/ ICH8	GMA 3000	PCIEx16
Intel P31	800/1066	DDR2 800	82P31/ICH7	—	PCIEx16
Intel G31	800/1066	DDR2 800	82G31/ ICH7	GMA 3100	PCIEx16
Intel G33	800/1066/1333	DDR3 1066/ DDR2 800	82G33/ICH9	GMA 3100	PCIEx16
Intel Q33/ Q35	800/1066/1333	DDR2 800	82Q33(Q35)/ ICH9	GMA 3100	PCIEx16
Intel P35	800/1066/1333	DDR3 1066 DDR2 800	82P35/ ICH9	—	PCIEx16
Intel G35	800/1066/1333	DDR2 800	82G35/ ICH8	GMA X3500	PCIEx16
Intel X38	800/1066/1333	DDR3 1333 DDR2 800	82X38/ ICH9	—	2xPCIEx16 2.0
Intel X48	1066/1333/1600	DDR3 1600/1333/1066	82X48/ ICH9	—	2xPCIEx16 2.0
nVidia 780i	533/800/1066/1333	DDR2 800/667/533	C72+NF200/ MCP55	—	2xPCIEx16 2.0 1x PCIEx1 1.0

[1] Работа с ними будет детально рассмотрена в следующих главах книги.

Производитель и марка чипсета	Поддерживаемые частоты шины, МГц	Тип и частота поддерживаемой памяти, МГц	Северный/южный мост	Интегрированный видеоадаптер	Порты для внешнего видеоадаптера
nVidia 750i	533/800/1066/1333	DDR2 800/667/533	C72+NF200/ MCP55	—	1xPCIEx16 или 2xPCIEx8
nVidia 680i	533/800/1066/1333	DDR2 800/667/533	C55/MCP55	—	2xPCIEx16
nVidia 650i	533/800/1066/1333	DDR2 800/667/533	C55/MCP55	—	1xPCIEx16 или 2xPCIEx8
nVidia 590i	533/800/1066	DDR2 667/533/400	C19/ MCP51	—	2xPCIEx16
nVidia 570i	533/800/1066	DDR2 667/533/400	C19/MCP51	—	1xPCIEx16 или 2xPCIEx8
VIA PT890	533/800/1066	DDR2 533/400 DDR 400/33/266	PT890/ VT8237	—	PCIEx16
VIA PT880	533/800/1066	DDR2 533/400 DDR 400/33/266	PT880/ VT8237	—	PCIEx16/ AGP8x
VIA P4M900	533/800/1066	DDR2 533/400 DDR 400/333/266	P4M890/ VT8251	Chrome9	PCIEx16
VIA P4M890	533/800/1066	DDR2 533/400 DDR 400/333/266	P4M890/ VT8237	Uni-Chrome Pro	PCIEx16
SiS 671	533/800	DDR2 667/533/400	SIS671/968	Mirage 3	PCIEx16
SiS 672	533/800/1066	DDR2 667/533/400	SIS672/968	Mirage 3+	PCIEx16

Оперативная память

Оперативная память — один из важнейших компонентов системы, она необходима для работы операционной системы и приложений, для обработки и временного хранения данных. Оперативная память не позволяет хранить информацию после выключения питания, но она работает намного быстрее жестких дисков и других устройств. Любая программа сначала загружается с жесткого диска в оперативную память и лишь затем начинает работу. Объем оперативной памяти существенно влияет на общую производительность системы, и его увеличение — наиболее простой и популярный метод модернизации компьютера.

Для оперативной памяти может использоваться обозначение *ОЗУ* (оперативное запоминающее устройство) или *RAM* (Random Access Memory — память с произвольным доступом).