

МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ВЫПОЛНЕНИЮ
ЛАБОРАТОРНОЙ РАБОТЫ №3
«Базовая система ввода-вывода (BIOS)»
по дисциплине «**Архитектура аппаратных средств**»

Введение

Время выполнения лабораторной работы (аудиторные часы) – 4 часа

Время самостоятельной работы студента (дополнительные часы) – 4 часа

Минимальная оценка – 3 балла.

Максимальная оценка – 3 балла.

Цель работы: знакомство студентов с базовой системой ввода-вывода БСВВ (BIOS).
Приобретение практических навыков работы с BIOS.

Оборудование и программное обеспечение: системный блок, клавиатура, мышь, монитор.

1 Теоретические сведения

1.1 Базовая система ввода-вывода (BIOS)

BIOS (basic input/output system, базовая система ввода-вывода) – это встроенное в компьютер программное обеспечение, которое ему доступно без обращения к диску. Конструктивно BIOS представляет собой микросхему памяти, информация в которой не стирается даже после выключения питания. На персональных компьютерах BIOS содержит код, необходимый для управления клавиатурой, видеокартой, дисками, портами и другими устройствами.

BIOS является ключевым элементом системной платы, без которого все ее компоненты представляют собой лишь набор дорогих «железок». BIOS, пользуясь средствами, предоставляемыми чипсетом, управляет всеми компонентами и ресурсами системной платы. Из этого следует, что используемая версия BIOS в значительной степени привязана к чипсету, и, кроме того, она должна «знать» особенности применяемых компонентов (процессор, память, интегрированные контроллеры). Код BIOS хранится в микросхеме энергонезависимой постоянной памяти (ROM BIOS) или флэш-памяти (Flash BIOS).

Функционирование компьютера. Начальный запуск и самотестирование POST. При включении блок питания вырабатывает сигнал аппаратного сброса, приводящего все узлы в исходное состояние. Этот же сигнал вырабатывается и при нажатии кнопки Reset. Во время действия сигнала аппаратного сброса процессор пассивен – он не управляет системной шиной. Процессор подготавливается к работе, воспринимая со своих выводов сигналы, задающие его конфигурацию (коэффициент умножения, роль в многопроцессорных системах и некоторые другие параметры). Внутренний кэш очищается, регистры (не все) приводятся в определенное состояние. Сигнал сброса поступает на все устройства (контроллеры и адаптеры), нуждающиеся в переводе в исходное состояние и находящиеся на системной плате или подключаемые к шинам расширения. После окончания сигнала процессор по определенному адресу выбирает из памяти и исполняет первую инструкцию – управление передается на точку входа в программу инициализации компьютера **POST (Power-On Self-Test – самотестирование при включении)**. Первым делом мо выполнить инициализацию процессора – установить значения некоторых регистров. После сброса процессор всегда начинает работу в реальном режиме (совместимом с Intel 8086/88). Далее происходят проверка работоспособности и инициализация подсистем компьютера. Эта «раскрутка» выполняется в несколько этапов, причем постепенно в работу вовлекаются протестированные подсистемы. Ниже представлена обычная последовательность шагов теста POST:

- 1) Тестирование регистров процессора.
- 2) Проверка контрольной суммы ROM BIOS.
- 3) Проверка и инициализация таймера 8253/8254, портов 8255. После этого шага становится доступной звуковая диагностика.
- 4) Проверка и инициализация контроллеров прямого доступа к памяти DMA 8237.
- 5) Проверка регенерации памяти.
- 6) Тестирование 64 Кбайт нижней памяти.
- 7) Загрузка векторов прерывания и стека в нижнюю область памяти.

- 8) Инициализация видеоконтроллера – на экране появляется заставка Video BIOS, обычно с указанием модели видеокарты и объемом установленной видеопамати. После успеха этого шага изображение на экране сменяется заставкой системного модуля BIOS со счетчиком объема тестируемой динамической памяти. Теперь диагностические сообщения выводятся на экран. POST продолжает работу.
- 9) Тестирование полного объема ОЗУ.
- 10) Тестирование клавиатуры.
- 11) Тестирование CMOS-памяти и часов.
- 12) Инициализация различных портов (COM, LPT, USB).
- 13) Инициализация и тест контроллера НГМД.
- 14) Инициализация и тест контроллера НЖМД.
- 15) Сканирование области дополнительной памяти ROM BIOS.
- 16) Вызов Bootstrap (прерывание Int 19h) – загрузка операционной системы, при невозможности осуществляется попытка запуска ROM Basic (Int 18h), при неудаче – останов процессора с сообщением System Halted (система остановлена).

Для процессоров, начиная с шестого поколения (Intel Pentium и выше), у POST есть дополнительная забота – загрузить «заплатки» микропрограмм самого процессора. Эти заплатки позволяют исправлять некоторые ошибки, выявленные в процессорах определенных моделей и партий выпуска. Без них основные функции процессор, конечно, выполнять будет, но в современных сложных операционных системах и приложениях, как говорится, возможны варианты. Информация о том, какие заплатки требуются конкретному процессору, и сами заплатки хранятся в ROM BIOS. Если BIOS про установленный процессор (какой именно процессор установлен, POST может определить программно) «ничего не знает», то и заплатки не загрузит. По этой причине может потребоваться обновление версии BIOS.

В процессе выполнения программа POST отыскивает модули расширений ROM BIOS – сначала в известном месте (по адресу C0000h) ищется ROM BIOS графической карты, а позже ищутся модули карт расширения (в зоне C8000-F4000K). Найденные модули инициализируются, при этом могут переопределяться векторы прерываний, по которым вызываются некоторые сервисы BIOS.

К моменту окончания теста POST все стандартные устройства (клавиатура, дисплей, диски, порты) приводятся в состояние готовности к работе в стандартном режиме по умолчанию, часть настроек может выполняться в соответствии с выбранными установками CMOS Setup. Список обнаруженных устройств и их основные параметры могут отображаться в таблице на экране, но возможна и такая настройка CMOS Setup, при которой экран будет пустым до появления логотипа (или текстового сообщения) загружаемой ОС.

Загрузка ОС и прикладных программ. Последним шагом программы POST является выполнение *процедуры начальной загрузки* (bootstrap loader), которая вызывается как программное прерывание Int 19h BIOS. Ее задача довольно скромная – с выбранного устройства загрузить в память один блок (сектор) данных, и если он похож на загрузчик – передать ему управление. Напомним, что «передать управление» означает выполнить инструкцию перехода на адрес точки входа в программу, загруженную в оперативную память. На этом деятельность POST заканчивается, и компьютер переходит под управление загружаемого ПО (обычно это операционная система)

Системный модуль ROM BIOS. Системный модуль ROM BIOS (System ROM BIOS) обеспечивает программную поддержку стандартным устройств ПК, конфигурирование аппаратных средств, их диагностику и вызов загрузчика операционной системы. Системный модуль ROM BIOS в значительной степени привязан к конкретной реализации системной платы, поскольку именно ему приходится программировать все микросхемы чипсета системной платы. Функции BIOS разделяются на следующие группы:

- 1) Инициализация и начальное тестирование аппаратных средств (POST).
- 2) Настройка и конфигурирование аппаратных средств и системных ресурсов (CMOS Setup).
- 3) Автоматическое распределение системных ресурсов (Plug and Play BIOS, PnP BIOS) – отвечает за разрешение конфликтов на этапе выполнения POST, поддержка конфигурирования в рабочем режиме и т.п.
- 4) Идентификация и конфигурирование устройств PCI (PCI BIOS).
- 5) Начальная загрузка (первый этап загрузки ОС) (Bootstrap Loader);

6) Обслуживание аппаратных прерываний от системных устройств (таймера, клавиатуры, дисков) (BIOS Hardware Interrupts).

7) Обработка базовых функций программных обращений (сервисов) к системным устройствам (ROM BIOS Services).

8) Поддержка управляемости конфигурированием (Desktop Management Interface BIOS, DMI BIOS) – интерфейс управления настольными компьютерами (DMI) служит для удаленного администрирования компьютеров.

9) Поддержка управления энергопотреблением и автоматического конфигурирования (Advanced Power Management и Advanced Configuration and Power Interface BIOS, APM и ACPM BIOS). Интерфейс ACPI позволяет операционной системе управлять конфигурированием и энергопотреблением устройств и компьютера в целом. Он определяет аппаратные и программные интерфейсы, а также наборы данных (таблицы).

Все эти функции (или их часть) исполняет системный модуль BIOS, хранящийся в микросхеме ПЗУ или флэш-памяти на системной плате. Большинство сервисных функций выполняется в 16-битном режиме, хотя некоторые функции могут иметь и альтернативные вызовы для 32-битного исполнения.

Поскольку содержимое флэш-BIOS может быть изменено прямо в компьютере, возникает опасность полной потери работоспособности компьютера при занесении некорректной «прошивки» или под действием вируса. С разрушенным модулем BIOS компьютер не может запуститься. Для предотвращения таких ситуаций применяют различные способы защиты, одним из которых может быть установка «резервной» версии BIOS (дублирование микросхемы ПЗУ) или возможность «прошивки» микросхемы BIOS через определенный порт USB на задней панели ввода-вывода материнской платы. Правда подобные возможности реализуются не на всех материнских платах.

1.2 Конфигурация BIOS

Конфигурация BIOS (**BIOS Setup**, или **Setup**) является важной, но при этом малоизвестной областью. Фирмы-производители не предоставляют по Setup никакой подробной технической информации, справедливо полагая, что рядовому пользователю это совершенно не надо. Доля смысла в этом есть: изменяя установки BIOS, можно довести компьютер до полностью нерабочего состояния. В лучшем случае компьютер перестанет загружаться, в самом худшем – может испортиться какой-нибудь внутренний компонент. Но бывают случаи, когда произвести настройку просто необходимо. Например, при установке нового жесткого диска или какого-либо другого оборудования.

Все необходимые установки содержатся именно в BIOS. Однако существует некоторая информация о компьютере, которая может меняться. Например, информация о жестком диске, способе начального тестирования памяти, реакции на ошибки и т. д. Все параметры, которые меняются, находятся в микросхеме CMOS. Эта микросхема тоже хранит все установки при выключенном питании.

Чтобы изменять основные установки компьютера, нужно воспользоваться утилитой **BIOS Setup**.

Существует много фирм, выпускающих свои версии BIOS (наиболее известные среди них фирмы AMI и AWARD). Поэтому, чтобы попасть в настройки, нужно узнать какая именно версия BIOS используется и в зависимости от этого нажать определенную клавишу (или комбинацию) на клавиатуре (обычно это клавиши Del, F1, F2).

Несмотря на различные версии BIOS, интерфейс которых может отличаться, параметры для изменения в пределах одного поколения процессоров (и чипсетов) не сильно отличаются, поэтому, разобравшись с настройками одного BIOS`а в дальнейшем можно будет просто "работать" и с другими версиями.

Пример главного меню AMI BIOS представлен на рисунке 1.

Данный BIOS стоит из шести разделов, в которых сгруппированы настройки:

1) Раздел **Main** – отвечает за настройку даты/времени, просмотра и конфигурирования работы дисковых накопителей, а так же за просмотр системной информации о компьютере (объем установленной памяти, тип процессора).

2) Раздел **Advanced** – в нем осуществляется "тонкая" подстройка параметров чипсета, накопителей, интегрированных периферийных устройств (звуковой, сетевой карты) и выделение

прерываний различным устройствам, В нем же отображается температура и напряжение основных компонент (процессора, материнской платы).

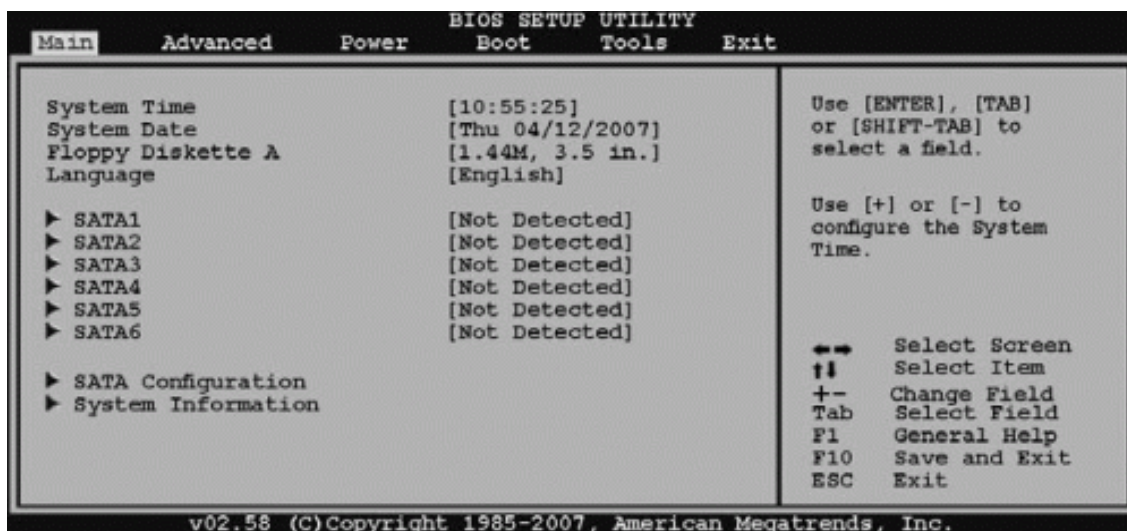


Рис. 1. Настройки AMI BIOS

3) Раздел **Power** – предназначен для установки различных режимов работы материнской платы, процессора, видеокарты, связанных с питанием.

4) В разделе **Boot** возможно определить с какого из устройств будет производиться загрузка операционной системы (HDD, CD-ROM, USB, по сети и т.п.).

5) Раздел **Tools** – в разных версиях может иметь другие названия и обычно содержит параметры, заложенные производителем материнской платы, например возможность выбора частоты шины, памяти, сохранение профилей с настройками и т.п.

6) Раздел **Exit** – обычно содержит типовые опции: сохранить настройки, выйти без сохранения, загрузить заводские настройки.

1.3 Диагностика POST

В процессе включения компьютера, при возникновении какой-то неисправности, можно услышать сигналы, идущие от материнской платы. Это происходит работа системы POST, которая сообщает о состоянии процесса диагностики.

В зависимости от модели BIOS (IBM BIOS, AMI BIOS, AWARD BIOS, Phoenix BIOS) трактовка звуковых сигналов (причина неисправности) может отличаться. В таблице 1 приведен пример для AWARD BIOS.

Таблица 1. Значение звуковых сигналов AWARD BIOS

Вид звукового сигнала	Значение звукового сигнала
Один короткий	Нормальное завершение POST, все О.К.
Отсутствует	Неисправен блок питания
Один сигнал и пустой экран	Неисправна видеосистема
Один длинный и два коротких	Неисправна видеосистема
Один длинный и три коротких	Не подключен монитор
Два коротких	Любая несущественная ошибка
Три длинных	Неисправна материнская плата (ошибка контроллера клавиатуры)

В некоторых системных платах возможна реализация **речевой звуковой диагностики** (voice diagnostics), т.е. неисправность сообщается через системный динамик. Язык выбирается в CMOS Setup.

В современных материнских платах диагностика POST осуществляется посредством вывода на POST-индикаторы кода, по которому можно определить текущую стадию тестирования. Тестирование начинается с кода 00h (подготовка к запуску системы) и заканчивается FFh (завершение пост кода). Если система остановилась на каком-то значении, то, в зависимости от версии BIOS и производителя материнской платы, выдается соответствующий код ошибки (проблема с этим этапом тестирования, например 04h – проблема с инициализацией памяти).

Если на материнской плате нет POST-индикации, то есть специальные модули, устанавливаемые в слот расширения PCI/PCI-E, через которые можно определить код ошибки или текущий процесс прохождения POST (рисунок 2).



Рис. 2 Платы POST-индикации кода ошибки

1.4 UEFI BIOS

Основная проблема "старых" версий BIOS – это 16-битный исполняемый код и аппаратные ограничения архитектуры IBM PC/AT. Например, с увеличением емкости дисковых накопителей возникла проблема загрузки операционной системы с жестких дисков, имеющие объем более 2 Тбайт и как следствие, необходимость использовать дополнительный жесткий диск. Все это привело к активному переходу на **UEFI (Unified Extensible Firmware Interface) BIOS** – интерфейс между операционной системой и микропрограммами, управляющими низкоуровневыми функциями оборудования (рисунок 3).



Рис. 3. UEFI BIOS материнской платы компании Asus

По-сути UEFI BIOS сейчас представляет собой миниатюрную операционную систему с графической оболочкой, которая включает в себя таблицу данных с информацией о платформе, различные сервисы, предоставляемые основной операционной системе и поддерживает расширения BIOS, например ACPI.

Большинство из производителей для удобства пользователей предлагают переход от графического интерфейса UEFI BIOS к "старому", более привычному "псевдо-текстовому" BIOS, но функционал от этого не меняется.

Пример содержания UEFI BIOS [для материнских плат MSI](#).

2. Задание на проведение лабораторной работы

1. Зайдите в настройки BIOS на материнской плате
2. Определите в BIOS имеющиеся диски и конфигурацию компьютера.
3. Установите дату и время через BIOS.
4. Попробуйте выбрать вариант загрузки операционной системы через USB-флешку.

3. Отчет по лабораторной работе

Отчет по выполненной работе производится в виде показа выполненных заданий и устного ответа на контрольные вопросы.

4. Контрольные вопросы к лабораторной работе

1. Что такое BIOS?
2. Опишите функции BIOS
3. Что такое POST?
4. За что отвечает POST?
5. Для чего нужна начальная загрузка?
6. Назначение системного модуля ROM BIOS?
7. Назначение DMI?
8. Назначение ACPI?
9. Что хранится в ROM BIOS?
10. Назначение BIOS Setup?
11. За что отвечает CMOS Setup?
12. Какие настройки имеются в CMOS Setup?
13. Что такое UEFI BIOS?
14. Что можно сделать с помощью UEFI BIOS?