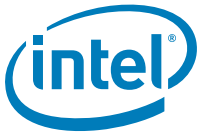


Техническое описание серверных плат на базе семейства наборов микросхем Intel® серии 5000

Код заказа Intel – D38960-004

Версия 1.1

1 июня 2006 года

Подразделение корпоративных платформ и служб

Описание

Дата	Номер версии	Изменения
31 мая 2006	1.1	Первая редакция.

Отказ от ответственности

ИНФОРМАЦИЯ, ПРИВЕДЕННАЯ В ЭТОМ ДОКУМЕНТЕ, СВЯЗАНА С СООТВЕТСТВУЮЩЕЙ ПРОДУКЦИЕЙ INTEL®. Этот документ никоим образом, в том числе процессуальным порядком или иным способом, не предоставляет прямых или косвенных прав на использование интеллектуальной собственности. КОРПОРАЦИЯ INTEL НЕ ПРИНИМАЕТ НА СЕБЯ НИКАКОЙ ОТВЕТСТВЕННОСТИ, СВЕРХ ОГОВОРЕННОЙ В УСТАНОВЛЕННЫХ INTEL УСЛОВИЯХ ПРОДАЖИ ПРОДУКЦИИ ДАННОГО ТИПА. INTEL НЕ ПРИНИМАЕТ НА СЕБЯ НИКАКОЙ ОТВЕТСТВЕННОСТИ И ОБЯЗАТЕЛЬСТВ, ВЫРАЖЕННЫХ ЯВНО ИЛИ ПОДРАЗУМЕВАЕМЫХ, СВЯЗАННЫХ С ПРОДАЖЕЙ И ИСПОЛЬЗОВАНИЕМ ЕЕ ПРОДУКЦИИ, ВКЛЮЧАЯ ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА И ОТВЕТСТВЕННОСТЬ, ОТНОСЯЩИЕСЯ К АДЕКВАТНОСТИ ПРОДУКЦИИ ДЛЯ КОНКРЕТНЫХ ПРИМЕНЕНИЙ, ГАРАНТИИ ПРИБЫЛИ, СОБЛЮДЕНИЮ ПАТЕНТНОГО ПРАВА, АВТОРСКОГО ПРАВА И ПРОЧИХ ПРАВ НА ИНТЕЛЛЕКТУАЛЬНУЮ СОБСТВЕННОСТЬ. Данная продукция Intel не предназначена для использования в области медицины или спасения жизни, а также в системах жизнеобеспечения. Корпорация Intel оставляет за собой право вносить изменения в спецификации продукции и соответствующую документацию в любое время без уведомления.

Разработчики не должны полагаться на отсутствие характеристик или пометки «reserved» или «undefined». Intel оставляет за собой право вносить такие пометки в будущем и не несет никакой ответственности за конфликты или несовместимости, возникающие из-за них.

В настоящем документе содержится информация по продукции, находящейся в стадии разработки. Приведенная информация не является окончательной для данной продукции. Измененная информация будет опубликована после выхода продукции. Перед окончательным выбором конструкции свяжитесь с местным офисом продаж, чтобы убедиться, что у вас имеются самые последние данные.

Техническое описание серверных плат на базе семейства наборов микросхем Intel® серии 5000 может иметь выявленные конструкционные дефекты или ошибки, известные как список выявленных недостатков (errata). Эти дефекты могут влиять на характеристики продукции и быть причиной их несоответствия опубликованным спецификациям. Сведения о выявленных погрешностях и отклонениях предоставляются по требованию.

Настоящий документ и описываемое в нем программное обеспечение поставляется только в рамках программы лицензирования и может использоваться или копироваться только в соответствии с условиями лицензии. Информация, содержащаяся в настоящем пособии, предназначена для использования исключительно в информационных целях, может быть изменена без предварительного предупреждения, и не должна рассматриваться как обязательство корпорации Intel. Корпорация Intel не несет никакой ответственности за любые неточности или ошибки, которые могут содержаться в настоящем документе или в любом программном обеспечении, поставляемом в комплекте с настоящим документом.

Содержание

Список рисунков

Список таблиц

Данная страница преднамеренно оставлена пустой

1. Введение

В этой таблице представлена информация о функциональных возможностях и регулятивная информация, общая для серверных плат Intel® и плат Intel® для рабочих станций с набором микросхем серии Intel® 5000. Это сопроводительный документ, содержащий технические характеристики продукции, которые имеет каждая серверная плата или плата для рабочих станций на базе набора микросхем Intel® 5000 MCH. Чтобы полностью понять функциональные возможности конкретной серверной платы или платы для рабочих станций на базе этого набора микросхем, Вам необходимо использовать эту таблицу и технические характеристики продукции, доступные для Вашей серверной платы или платы для рабочих станций.

Этот документ предназначен для тех, кто хочет получить более подробную информацию о системных платах для серверов или рабочих станций, чем та, которая приведена в руководствах для пользователя или в технических характеристиках конкретной платы. Цель этого технического документа – обеспечить пользователей информацией об особенностях этой серверной платы.

1.1 Обзор серверной продукции

В этом документе содержится информация о конкретных системных платах Intel® для серверов и рабочих станций. Если не указано иное, все ссылки на «системные платы Intel» или на «системные платы» относятся ко всем системным платам для серверов и рабочих станций, в которых используется этот набор микросхем.

1.2 Оглавление

Настоящий документ состоит из следующих глав

- Глава 1 – Введение
- Глава 2 – Функциональная архитектура
- Глава 3 – BIOS
- Глава 4 – Управление системой
- Глава 5 – Обработка ошибок и сообщения об ошибках

2. Функциональная архитектура

В данной главе содержится подробное описание функций, распределенных между архитектурными блоками Intel® 5000 MCH. На следующей странице приведена схема функциональной архитектуры набора микросхем.

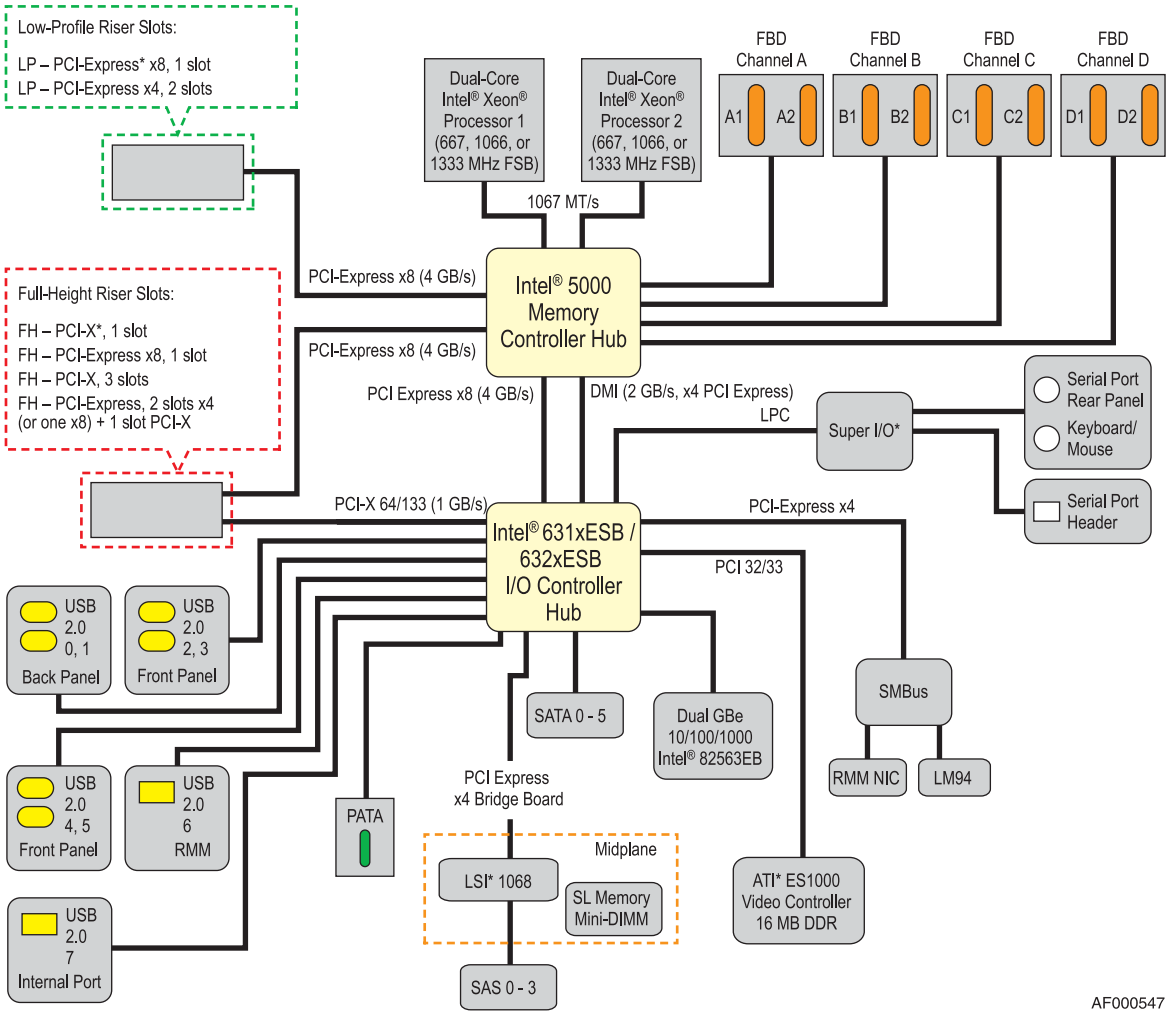


Рисунок 1. Функциональная архитектура

2.1 Компоненты Intel® 5000 MCH

Набор микросхем включает два компонента, которые совместно обеспечивают интерфейс между всеми основными подсистемами системных плат Intel® для серверов и рабочих станций. Эти подсистемы включают процессор, память и подсистему ввода/вывода. Компоненты включают в себя:

- Контроллер-концентратор памяти Intel® 5000 (MCH)
- «Южный мост» Intel® Enterprise South Bridge 2 (контроллер-концентратор ввода/вывода Intel® 631xESB / 632xESB)

Следующий подраздел представляет обзор первичных функций и поддерживаемых функций каждого компонента набора микросхем Intel® 5000 MCH используемого платами Intel®. В других разделах этой главы представлены подробности установки каждой подсистемы.

Примечание: *Информация о поддержке конкретных функций содержится в технических характеристиках системных плат Intel® для серверов и рабочих станций, относящихся к Вашей продукции.*

2.1.1 Контроллер-концентратор памяти (Intel® 5000 MCH)

Контроллер-концентратор памяти Intel® 5000 реализован в 1432-контактном корпусе FC-BGA и поддерживает следующие интерфейсы:

- Независимая системная шина с поддержкой двух процессоров, работающая на частотах 667, 1066 или 1333 МГц.
- Четыре полностью буферизованных канала DIMM (FBD) с поддержкой полностью буферизованных модулей памяти DDR2 DIMM (FBDIMM), последовательная шина с 24 дорожками, рабочей пропускной способностью 6,4 ГБ/с (533 МТ/с) и теоретической пиковой пропускной способностью 8 ГБ/с (667 МТ/с) на канал. Это позволяет достичь общей рабочей пропускной способности 25,6 ГБ/с и теоретической пиковой пропускной способности 64,6 ГБ/с при объединении четырех каналов.
- Один порт PCI Express* x8 с совокупной пропускной способностью 4 ГБ/с, имеющий интерфейс с контроллером-концентратором ввода/вывода Intel® 631xESB / 632xESB.
- Один порт PCI Express* x8 с совокупной пропускной способностью 4 ГБ/с, имеющий интерфейс с разъемом x8 PCI Express.
- Один порт PCI Express* x8 с совокупной пропускной способностью 4 ГБ/с, имеющий интерфейс с разъемом x8 PCI Express.
- Один порт PCI Express* x4 с совокупной пропускной способностью 2 ГБ/с, имеющий интерфейс с контроллером-концентратором ввода/вывода Intel® 631xESB / 632xESB.

2.1.1.1 Системная шина

Контроллер-концентратор памяти Intel® 5000 поддерживает однопроцессорные и двухпроцессорные конфигурации для процессоров Intel® Xeon® серии 5000 с кэш-памятью 2x 2 МБ. Контроллер-концентратор памяти Intel® 5000 поддерживает базовую системную шину, работающую на частотах 266 МГц или 333 МГц для наборов микросхем Intel® серии 5000. Интерфейс адресации и запросов передается с двойной частотой при 533 МГЦ, а 64-битный интерфейс данных передается (частично) на учетверенной частоте 1066 МГц. Это обеспечивает подходящий адрес системной шины и скорость передачи данных 8,5 ГБ/с.

2.1.1.2 Обзор подсистемы памяти Intel® 5000 MCH

Intel® 5000 MCH содержит интегрированный контроллер памяти для прямого соединения по четырем каналам с полной буферизацией DDR2 533/667 МГц (по отдельности или в комплекте). Пиковая пропускная способность теоретических данных памяти при использовании технологии FBD 533/667 МГц составляет 6,4 ГБ/с и 8 ГБ/с соответственно.

После того, как все четыре канала памяти были установлены и запущены, они работают в связке. Максимальный поддерживаемый объем памяти FBD DDR2, работающей на частоте 533/667 МГц – 64 ГБ.

Интерфейс контроллера-концентратора памяти Intel® 5000 MCH поддерживает такие функции, как надежность, непрерывность работы, удобство в обслуживании, использовании и управлении (RASUM):

- Осуществляется поддержка зеркального отображения памяти, что позволяет создавать две копии всех данных в подсистеме памяти (одна в каждом канале).
- Резервирование памяти оставляет один модуль DIMM на каждом канале в резерве, который включается при неисправности другого модуля FBDIMM на этом же канале.
- Периодическая чистка памяти аппаратных средств требует поддержки очистки памяти.
- Повторная попытка при обнаружении неустранимых ошибок памяти.
- Функция Intel® x4/x8 Single Device Data Correction (SDDC) используется для обнаружения ошибок памяти и исправления любого количества ошибочных битов в одном устройстве памяти x4/x8.

Примечание: *Резервирование модулей и зеркальное отображение памяти являются взаимоисключающими режимами.*

Примечание: *Функции резервирования и зеркального отражения памяти в настоящее время не поддерживаются, их поддержка будет реализована после начала производства.*

2.1.1.3 Интерфейс PCI Express*

Контроллер-концентратор памяти Intel® 5000 поддерживает высокоскоростной последовательный интерфейс ввода/вывода PCI Express*, обеспечивающий передовой уровень пропускной способности ввода/вывода. Масштабируемый интерфейс PCI Express* контроллера-концентратор памяти Intel® 5000 MCH соответствует *Спецификации Интерфейсов PCI Express*, Вер. 1.0a.*

Контроллер-концентратор памяти Intel® 5000 MCH использует три интерфейса x8 PCI Express*, теоретическая максимальная пропускная способность каждого составляет 4,2 ГБ/с. Каждый из интерфейсов x8 PCI Express* также могут быть сконфигурированы как два независимых интерфейса x4 PCI Express* . Интерфейс/ порт PCI Express* представляет собой набор дорожек. Каждая дорожка (x1) состоит из двух чередующихся во всех направлениях дифференциальных (передача и прием). При максимальной скорости контактов данных 2.5 ГБ/с действительная пропускная способность каждой пары составляет 250 МБ/с при условии, что 8/10-разрядное кодирование используется для передачи данных по интерфейсу.

По определению *Спецификации Интерфейсов PCI Express*,* контроллер-концентратор памяти Intel® 5000 MCH является компонентом корневого класса. Интерфейсы PCI Express* контроллера-концентратора памяти Intel® 5000 MCH поддерживают соединение со множеством мостов и устройств отвечающих требованиям той же версии спецификации.

*2.1.1.3.1 Настройка PCI Express**

Для того, чтобы установить соединение между конечными точками PCI Express*, точки принимают участие в ряде последовательных операций, известных как настройка. Данная последовательность устанавливает операционную длину соединений и корректирует асимметрию различных дорожек внутри соединения таким образом, чтобы точки образца данных могли верно забирать образцы данных из соединения.

При использовании порта x8, пары соединений x4 вначале пытаются настроиться самостоятельно, однако, при обнаружении устройства, возвращающего соединение с идентификацией входящей информации, они объединяются в один канал шириной x8. После установки отдельных соединений они определяют самую большую ширину полосы пропускания и начинают снижать скорость при поддерживаемой ширине для успешной установки. В итоге, соединение может установиться в качестве соединения x1.

Хотя ширина полосы пропускания соединения данного размера намного ниже, чем ширина соединения x8 или даже x4, данное соединение обеспечивает взаимодействие между двумя устройствами. Возможен опрос устройства на другом конце канала связи программными средствами, чтобы выяснить, почему оно не может работать с более высокой пропускной способностью. Это невозможно без поддержки пропускной способности x1.

Согласование ширины может происходить только в процессе установки или переустановки, а не во время восстановления системы.

*2.1.1.3.2 Повторный запуск PCI Express**

Интерфейс PCI Express* включает в себя механизм перезапуска на уровне соединения. Ели аппаратные средства обнаруживают сбои при передаче пакета, осуществляется повторная пересылка данного пакета и всех последующих пакетов. Хотя данная процедура вызывает временные перерывы в передаче пакетов, повторная действие помогает поддерживать целостность соединения.

*2.1.1.3.3 Восстановление соединения PCI Express**

При очень большом количестве подобных ошибок аппаратное обеспечение может посчитать качество соединения неудовлетворительным, и в этом случае точки завершения могут провести короткую настроечную последовательность, известную как восстановление. Ширина соединения не может быть согласована повторно, но возможна корректировка асимметрии между дорожками. Эти действия происходят без вмешательства ПО, которому может быть отправлено сообщение.

*2.1.1.3.4 Защита данных PCI Express**

Высокоскоростной последовательный интерфейс PCI Express* использует традиционную защиту с помощью циклического избыточного кода (CRC). Пакеты данных используют 32-разрядную схемы защиты CRC. Сеть Ethernet поддерживает ту же схему CRC-32. Меньшие пакеты соединений используют 16-разрядную схему CRC. Поскольку пакеты поддерживают не все способы кодирования, а только кодирование 8Б/10Б, это обеспечивает еще лучшую защиту данных с обнаружением запрещенных кодов. При обнаружении ошибок во время приема пакетов данных из-за различных помех, данные пакеты могут быть переданы заново. Аппаратная логика поддерживает повторные операции на уровне каналов без вмешательства ПО.

*2.1.1.3.5 Повторная настройка PCI Express**

Если аппаратные средства не могут провести успешное восстановление, тогда соединение автоматически переходит в состояние опроса и запускает полную повторную последовательность настройки. Данная процедура является сложным событием с неявной перезагрузкой нижнего устройства и всех подчиненных устройств, сообщение о котором передается в концентратор контроллеров памяти the Intel® 5000 MCH, как ошибка «Link Down». При запуске преобразования события в ПО поступает сообщение об условии link DL_DOWN condition. Если в процедуре задействовано ПО, значит, данные, вероятнее всего, утеряны и необходимо перезапустить процессы. Это является более предпочтительным, чем демонтирование системы или ее отключение на длительный период времени.

2.1.1.4 Интерфейс Enterprise South Bridge (ESI)

Для связи с контроллером-концентратором памяти (Intel® 5000 MCH) используется интерфейс PCI. Максимальная реализованная пропускная способность этого интерфейса составляет 2 ГБ/с в обоих направлениях одновременно, что в целом составляет 4 ГБ/с. Этот интерфейс PCI Express* совместим со спецификацией *PCI Express Base Specification версии 1.0a*, и поддерживает пропускную способность x4 и x8.

2.1.2 Контроллер-концентратор ввода/вывода Intel® 631xESB/ 632xESB (ESB2)

Контроллер-концентратор ввода/вывода Intel® 631xESB / 632xESB представляет собой многофункциональное устройство, обеспечивающее интерфейс концентратора для доступа к встроенным функциям и системам ввода/вывода, включая:

- Совместимость со спецификацией *PCI Express Base Specification версии 1.0a* с поддержкой четырех корневых портов PCI Express* (поддержка горячего подключения модулей) и двух выходных портов 1x4 (поддержка горячей замены на уровне разъемов)
- Совместим с *дополнением PCI-X к спецификации локальной шины PCI, версия 1.0b*
- Совместим со спецификацией локальной шины PCI, редакция 2.3 с поддержкой работы PCI при 33 МГц
- Совместимость с *PCI Standard Hot-Plug Controller и Subsystem Specification, версия 1.0*
- Поддержка логики управления питанием ACPI 2.0
- Расширенные функции контроллера DMA, контроллера прерываний и таймера
- Интегрированный контроллер IDE с поддержкой Ultra ATA100 / 66 / 33
- Интегрированный контроллер SATA
- Контроллер BMC
- хост-интерфейс USB с поддержкой 8 портов USB 2.0, четырех -контроллеров UHCI и одного высокоскоростного контроллер EHCIUSB
- Совместим со *спецификацией шины системного управления (SMBus), редакция 2.0* с дополнительной поддержкой устройств I^2C
- Поддержка спецификации Audio Codec ‘97, версия 2.3
- Интерфейс LPC

Для каждой функции контроллера-концентратора ввода/вывода Intel® 631xESB / 632xESB имеется отдельный набор регистров конфигурации. После настройки все реестры отображаются в системе, как независимые контроллеры аппаратного обеспечения, использующие один и тот же интерфейс шины PCI.

2.1.2.1 Интерфейс PCI

Интерфейс PCI контроллера-концентратора ввода/вывода Intel® 631xESB / 632xESB поддерживает реализацию 33 МГц, совместимую с версией 2.3. Все сигналы PCI выдерживают напряжение 5 В, за исключением PME#. Интегрированный арбитр шины PCI поддерживает до шести внешних задатчиков шины, а также внутренние запросы контроллера-концентратора ввода/вывода Intel® 631xESB / 632xESB. На плате на базе Intel® 5000 MCH данный интерфейс PCI поддерживает одно встроенное устройство PCI: Видеоконтроллер ATI* ES1000.

2.1.2.2 Интерфейс PCI Express*

Контроллер-концентратор ввода/вывода Intel® 631xESB / 632xESB обеспечивает работу корневых портов PCI Express*, совместимых со спецификацией *PCI Express Base Specification версии 1.0a*. Корневые порты PCI Express можно статически сконфигурировать как четыре порта x1 или соединить между собой, чтобы образовать один порт x4. Каждый порт поддерживает пропускную способность 250 МБ/с в каждом направлении (500 МБ/с одновременно).

В контроллере-концентраторе ввода/вывода Intel® 631xESB / 632xESB реализованы два порта x4 по направлению основного трафика. Максимальная достижимая пропускная способность этого интерфейса составляет 1 ГБ/с в каждом направлении одновременно, или 2 ГБ/с в целом. Эти два порта можно сконфигурировать как один порт PCI Express* x8. Интерфейс PCI Express соответствует спецификации *PCI Express Base Specification версии 1.0a*.

2.1.2.3 Интерфейс шины PCI-X*

В контроллере-концентраторе ввода/вывода Intel® 631xESB / 632xESB реализован интерфейс шины PCI-X*, поддерживающий традиционные шины PCI и PCI-X Mode 1. Интерфейсы PCI-X, реализованные в контроллере-концентраторе ввода/вывода Intel® 631xESB / 632xESB, соответствуют следующей спецификации:

- Дополнение PCI-X к *спецификации локальной шины PCI, версия 1.0b*
- Разделы «Mode 1» приложения «PCI-X Electrical and Mechanical Addendum» (Электрические и механические характеристики PCI-X) к спецификации *PCI Local Bus Specification версии 2.0a*
- Дополнительный протокол PCI-X к спецификации локальной шины PCI, версия *2.0a*

Контроллер-концентратор ввода/вывода Intel® 631xESB / 632xESB поддерживает работу шины PCI на частотах 66 МГц, 100 МГц и 133 МГц.

2.1.2.4 Интерфейс IDE (системная шина Bus Master и синхронный режим передачи данных DMA)

В контроллере-концентраторе ввода/вывода Intel® 631xESB / 632xESB имеется встроенный контроллер IDE с независимым трактом передачи сигнала IDE, поддерживающий до двух устройств IDE. Данные интегрированные функции обеспечивают интерфейс для жестких дисков IDE и устройств ATAPI Каждое устройство IDE может иметь независимый скоростной режим. Интерфейс IDE поддерживает скорость передачи PIO IDE до 16 МБ/с и скорость передачи Ultra ATA до 100 МБ/с. Интерфейс IDE содержит 16x32-разрядные буферы для оптимальной передачи и не поддерживает ресурсы ISA DMA. Тракты передачи сигнала IDE в контроллере-концентраторе ввода/вывода Intel® 631xESB / 632xESB можно сконфигурировать как основной канал и дополнительный канал.

2.1.2.5 Последовательный контроллер ATA (SATA)

Хост-контроллер SATA поддерживает сочетание до шести устройств SATA или до четырех устройств SCSI с последовательным интерфейсом (serial attached SCSI, SAS). Это обеспечивает интерфейс для жестких дисков SATA и устройств ATAPI. Интерфейс SATA поддерживает скорость передачи данных PIO IDE до 16 МБ/с и скорость передачи данных Serial ATA до 3,0 ГБ /с (300 МБ/с).

Система SATA, реализованная в контроллере-концентраторе ввода/вывода Intel® 631xESB / 632xESB, содержит шесть независимых сигнальных портов SATA, которые можно независимо электрически изолировать. Каждое устройство SATA может иметь независимый скоростной режим. Они могут быть сконфигурированные как стандартные первичные и вторичные каналы. К тому же, контроллер-концентратор поддерживает технологию RAID для встроенных серверов Intel®, обеспечивающую чередование данных (RAID уровень 0) для повышения производительности или зеркальное отображение данных (RAID уровень 1) для поддержки отказоустойчивости между двумя драйверами SATA устраняя«узкое место» в виде скорости дисков за счет использования двух независимых контроллеров SATA интегрированных в Intel® 631xESB / 632xESB.

Примечание: *Дополнительная информация содержится в технических характеристиках системных плат Intel® для серверов и рабочих станций, относящихся к Вашей продукции.*

2.1.2.6 Контроллер BMC

Компонент BMC, реализованный в контроллере-концентраторе ввода/вывода Intel® 631xESB / 632xESB, состоит из встроенного контроллера ARC* и связанного с ним периферийного оборудования, и обеспечивает функционирование контроллера управления объединительной панели, необходимое для управлением сервером на базе IPMI. Ниже приведен список аппаратных функций управления, реализованных в контроллере-концентраторе ввода/вывода Intel® 631xESB / 632xESB и используемых BMC:

- Процессор ARC4 с кэш-памятью команд и данных объемом 16 Кб
- 256 Кб внутренней статической памяти SRAM с двумя портами (один порт для доступа к кодам, второй – для доступа ко всем остальным данным)
- Шина расширения, позволяющая подключать внешнее флэш-ПЗУ Flash PROM (синхронное или асинхронное), внешнюю статическую память SRAM или внешнюю синхронную динамическую память SDRAM
- Последовательный флэш-интерфейс
- Пять портов SMB, два из которых поддерживают FML (в ведущем или ведомом режиме)
- Последовательный порт RS-232 (UART)
- Криптографический модуль с поддержкой алгоритмов шифрования AES и RC4, и алгоритмов аутентификации SHA1 и MD5 со встроенным прямым доступом к памяти и поддержкой проверки контрольной суммы
- На шине LPC расположены два интерфейса keyboard controller style (KCS)

- Интерфейс ввода/вывода общего назначения (GPIO)
- Интерфейс MAC CSR
- Интерфейс таймера
- Интерфейс Host DMA

2.1.2.7 Интерфейс LPC

Intel® 631xESB / 632xESB выполняет интерфейс LPC в соответствии со Спецификацией Интерфейса *Low Pin Count, версия 1.1*. Функция моста LPC контроллера-концентратора ввода/вывода 631xESB / 632xESB содержится в устройстве PCI 31: Функция 0. Помимо функции моста LPC, D31:F0 содержит другие функциональные единицы, включая DMA, контроллеры прерываний, таймеры, системы управления питанием, средства управления системой, GPIO и часы реального времени.

2.1.2.8 Модули совместимости (контроллер DMA, таймер/счетчики, контроллер прерываний)

Контроллер DMA содержит логику двух контроллеров DMA 82C37 с семью независимо программируемыми каналами. Аппаратные каналы 0-3 поддерживают 8-битную передачу данных с подсчетом по байтам, а аппаратные каналы 5-7 поддерживают 16-битную передачу данных с подсчетом по словам. Любые два из семи каналов DMA могут быть запрограммированы для поддержки высокоскоростной передачи данных Type-F.

Контроллер-концентратор ввода/вывода Intel® 631xESB/632xESB поддерживает LPC DMA. LPC DMA и PC/PCI DMA используют контроллер DMA контроллера-концентратора ввода/вывода Intel® 631xESB / 632xESB. LPC DMA обрабатывается посредством использования линий LDRQ# от периферийных устройств и специального кодирования на LAD[3:0] от сервера. Интерфейс LPC поддерживает режимы Single, Demand, Verify и Increment. Каналы 0-3 являются восьмибитными. Каналы 5-7 являются 16-битными. Канал 4 зарезервирован для запросов хозяина шины.

Блок таймера/счетчика содержит три счетчика, функции которых аналогичны функциям программируемого таймера интервалов 82C54. Эти три счетчика обеспечивают работу системного таймера и звучание динамика. Генератор с частотой 14,31818 МГц является источником синхронизирующих сигналов для этих трех счетчиков.

Контроллер-концентратор ввода/вывода Intel® 631xESB / 632xESB содержит ISA-совместимый программируемый контроллер прерываний (PIC), обладающий функциональностью двух контроллеров прерываний 82C59. Два контроллера прерываний соединены в виде каскада, делая возможными 14 внешних прерываний и два внутренних прерывания. Кроме того, контроллер-концентратор ввода/вывода поддерживает последовательную схему прерываний. Все регистры этих модулей могут быть считаны и восстановлены. Это необходимо для сохранения и восстановления состояния системы после отключения питания платформы и возобновления подачи питания.

2.1.2.9 Расширенный программируемый контроллер прерываний (APIC)

Помимо стандартного ISA-совместимого программируемого контроллера прерываний (PIC), описанного в предыдущем разделе, контроллер-концентратор ввода/вывода Intel® 631xESB / 632xESB содержит расширенный программируемый контроллер прерываний (APIC).

2.1.2.10 Контроллер USB

В контроллере-концентраторе ввода/вывода Intel® 631xESB / 632xESB реализован усовершенствованный интерфейс хост-контроллера, поддерживающий передачу высокоскоростных сигналов USB. Высокоскоростная шина USB 2.0 поддерживает скорость передачи данных до 480 Мбит/с, что в 40 превышает скорость шины USB. Контроллер-концентратор ввода/вывода также содержит четыре контроллера UHCI, поддерживающие передачу данных по шине USB на полной скорости и на пониженной скорости.

Контроллер-концентратор ввода/вывода Intel® 631xESB / 632xESB поддерживает 8 портов USB 2.0. Скорость всех 8 портов может быть высокой, полной и пониженной.

2.1.2.11 Часы реального времени (RTC)

Intel® 631xESB / 632xESB содержит часы реального времени с ПЗУ 256 байт, совместимые с Motorola* MC146818A, и с резервным питанием от батареи. Часы реального времени выполняют две основные функции: показывают время суток и сохранят системные данные даже при выключенном питании. Часы реального времени работают на кристале в 32,768 КГц и отдельной 3-вольтной литиевой батарее.

Часы реального времени поддерживают два блокируемых объема памяти. При настройке разрядов конфигурационной области, два 8-разрядных объема могут быть заблокированы для чтения и записи. Это предотвратит несанкционированное чтение паролей или другой конфиденциальной системной информации.

2.1.2.12 Контакты ввода/вывода общего назначения (GPIO)

Контакты ввода/вывода общего назначения обеспечиваются для систем индивидуальной конструкции. Количество входов и выходов зависит от конфигурации контроллера-концентратора ввода/вывода Intel® 631xESB / 632xESB. Все неиспользуемые контакты GPI должны быть отжаты, чтобы они находились на установленном уровне и не вызывали проблем.

Примечание: *Дополнительная информация содержится в технических характеристиках системных плат Intel® для серверов и рабочих станций, относящихся к Вашей продукции.*

2.1.2.13 Шина системного управления (SMBus 2.0)

Контроллер-концентратор ввода/вывода Intel® 631xESB / 632xESB содержит интерфейс шины SMBus, обеспечивающий связь процессора с подчиненными устройствами SMBus. Этот интерфейс совместим с большинством устройств I^2C. Также реализованы специальные команды I^2C. Хост-контроллер шины SMBus устройства контроллера-концентартора позволяет процессору устанавливать связь с периферийными устройствами шины SMBus.

Контроллер-концентратор ввода/вывода Intel® 631xESB / 632xESB поддерживает функциональность подчиненных устройств, в том числе протокола Host Notify. Хост-контроллер поддерживает восемь командных протоколов интерфейса SMBus: Quick Command, Send Byte, Receive Byte, Write Byte/Word, Read Byte/Word, Process Call, Block Read/Write и Host Notify.

Дополнительная информация содержится в *спецификации шины системного управления (SMBus), версия 2.0*.

2.2 Подсистема процессора

Вспомогательные схемы подсистемы процессора включают следующие компоненты:

- Два разъема LGA771 (ZIF) для процессора
- Вспомогательная схема системной шины AGTL+
- Логика изменения конфигурации
- Логику определения присутствия модуля процессора
- Функции обнаружения BSEL
- Преобразование уровня сигнала процессора
- Комплект Common enabling kit (CEK) для поддержки работоспособности процессора

2.2.1 Поддержка процессоров

Системные платы Intel®, в которых используется контроллер-концентратор памяти Intel® 5000, поддерживают один или два процессора Intel® Xeon® серии 5000 с тактовыми частотами от 3,67 ГГц и с системной шиной, работающей на частоте 667, 1066 или 1333 МГц. Предыдущие поколения процессоров Intel® Xeon® не поддерживаются данными платами.

2.2.2 Правила установки процессоров

При использовании в системе двух процессоров, оба процессора должны иметь одинаковую версию, базовое напряжение питания и тактовую частоту ядра/системной шины. При использовании в системе только одного процессора, он должен быть установлен в разъем, помеченный CPU1, а другой разъем должен оставаться пустым.

Процессоры должны устанавливаться в последовательном порядке. Сначала следует установить процессор в разъем 1; затем в разъем 2. При однопроцессорной конфигурации не требуется установка терминатора в пустое гнездо процессора.

Конструкция системной платы обеспечивает ток до 130 А на каждый процессор. Процессоры с более высокими требованиями к току не поддерживаются.

2.2.3 EVRD процессора

EVRD11.0, Enterprise Voltage Regulator Down – это преобразователь постоянного тока, удовлетворяющий потребностям электропитания процессоров для серверных платформ. Этот стабилизатор напряжения поддерживает следующие процессоры: Процессоры Intel® серии 5000 и будущие процессорные технологии.

EVRD11.0 включает функциональные изменения по сравнению с предыдущими проектными рекомендациями EVRD.

2.2.4 GTL2007

GTL2007 – настраиваемый преобразователь между двумя процессорами Intel® Xeon® серии 5000, управлением состоянием системы, контроллером-концентратором ввода/вывода Intel® 631xESB / 632xESB и сигналами источника питания LVTTL и GTL. GTL2007 – 12-разрядный преобразователь интерфейсов между подсистемой ввода/вывода набора микросхем с напряжением 3,3 В и двухъядерными процессорами Intel® Xeon® серии 5000 GTL- / GTL / GTL+ I/O. Это устройство предназначено для управления состоянием платформы в двухпроцессорных системах.

2.2.5 Набор Common Enabling Kit для поддержки проектирования

Плата соответствует набору стандартных компонентов Intel® Common Enabling Kit (CEK) для установки процессоров Intel и решению крепления теплоотвода процессора. На заводах Intel серверные платы укомплектовываются пружиной CEK, закрепленной на верхней стороне системной платы под каждым разъемом процессора. Пружина CEK является съемной для использования решений крепления теплоотвода процессора сторонних производителей.

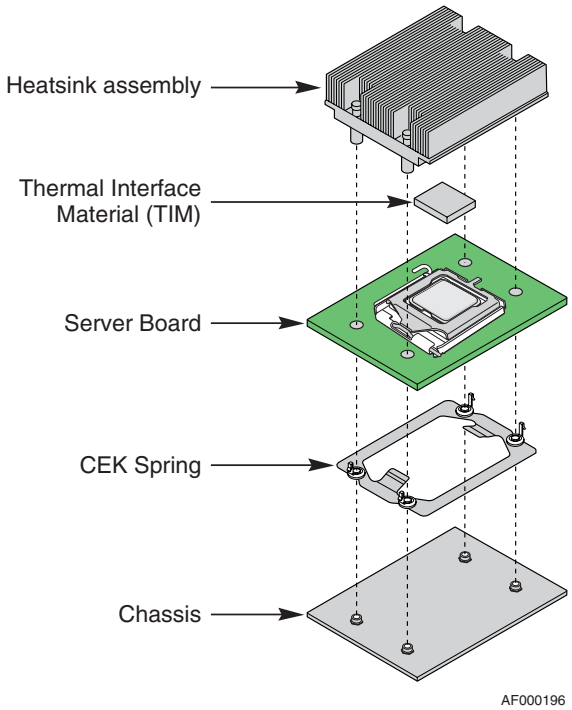


Рисунок 2. Монтаж процессоров с помощью CEK

2.3 Подсистема памяти

Системные платы Intel®, в которых используется контроллер-концентратор памяти Intel® 5000, поддерживают несколько полностью буферизованных (FBD) режимов работы памяти.

- Одноканальный режим (один модуль DIMM)
- Режим одной ветви / двух каналов
- Режим двух ветвей / двух каналов (всего четыре канала)
- Режим резервирования памяти
- Режим зеркалирования памяти

Примечание: *Функции резервирования и зеркального отражения памяти в настоящее время не поддерживаются, их поддержка будет реализована после начала производства.*

Контроллер-концентратор памяти Intel® 5000 – это встроенный контроллер памяти для прямой связи с четырьмя каналами, распределенными на восемь разъемов, поддерживающий буферизованные модули памяти FBDIMM DDR2-533 и DDR2-667 (односторонние и двухсторонние). Пиковая пропускная способность памяти составляет 6,4 ГБ/с при использовании модулей DDR2-533 и 8,0 ГБ/с при использовании модулей DDR2-667.

Пара каналов называется ветвью. Ветвь 0 состоит из каналов A и B, Ветвь 1 состоит из каналов C и D. Модуль DIMM может содержать два ряда. Канал поддерживает максимум восемь каналов.

В режиме работы без зеркалирования два канала DDR2, составляющие ветвь, работают в жёсткой конфигурации, и ветви работают независимо. При режиме зеркального отображения памяти каналы работают в связке при обычных условиях эксплуатации, однако, в условиях сбоя и восстановления системы, каналы работают отдельно.

Контроллер-концентратор памяти Intel® 5000 поддерживает длину пакета импульсов, равную четырем, как в одноканальном, так и в двухканальном режимах. В двухканальном режиме это обеспечивает восемь 64-разрядных участков памяти (64-разрядных строк данных кэша) для каждой операции чтения или записи. В одноканальном режиме для доступа к строке данных кэша необходимы две операции чтения или записи.

Память между 32 ГБ и 32 ГБ минус 512 МБ (мегабайт) не будет доступна для операционной системы. Эта область резервируется для BIOS, конфигурационной области APIC, интерфейса адаптеров PCI и виртуальной видеопамяти. Это означает, что если в системе установлено 32 ГБ памяти, использоваться может только 31,5 ГБ. Набор микросхем должен поддерживать распределение памяти выше 32 ГБ, однако эта память может быть недоступна для операционной системы с ограничением максимального объема памяти в 32 ГБ.

Для загрузки системы BIOS использует выделенную шину I^2C для извлечения информации DIMM, необходимой для программирования реестров памяти Intel® 5000 MCH.

2.3.1 FBDIMM

Интерфейс полностью буферизованной памяти (fully-buffered DIMM, FBDIMM) обеспечивает решение для создания высокосортного канала с высокой емкостью, имеющего ограниченный хост-интерфейс. В интерфейсе FBDIMM используются стандартные модули DRAM, отделенные от канала расширенным буфером памяти (advanced memory buffer, AMB) на модуле DIMM, которые поддерживают большее количество устройств на канал без дополнительной нагрузки на межкомпонентные соединения и влияния на производительность. Максимальное значение емкости памяти остается равным 36 устройствам на DIMM, а общая емкость памяти зависит от плотности битов в DRAM.

FBD – двухточечный интерфейс на базе дифференциальных пар. Интерфейс в основном состоит из 10 дифференциальных пар, идущих в «южном» направлении (выходы контроллера-концентратора памяти Intel® 5000 для связи с модулями DIMM) и 14 дифференциальных пар, идущих в «северном» направлении (входы в контроллер-концентратор памяти Intel® 5000 от модулей DIMM). Контроллер-концентратор памяти Intel® 5000 подключен только к ближайшему модулю FBDIMM в канале и обменивается информацией с буфером AMB этого модуля FBDIMM. Буфер AMB ближайшего модуля FBDIMM обменивается информацией с буфером AMB следующего модуля FBDIMM в канале, и т.д. Такое двухточечное решение позволяет избавиться от проблем, связанных со «шлейфовой» архитектурой, и позволяет увеличивать емкость памяти, не повышая загрузку канала. На рисунке ниже показана топология FBD.

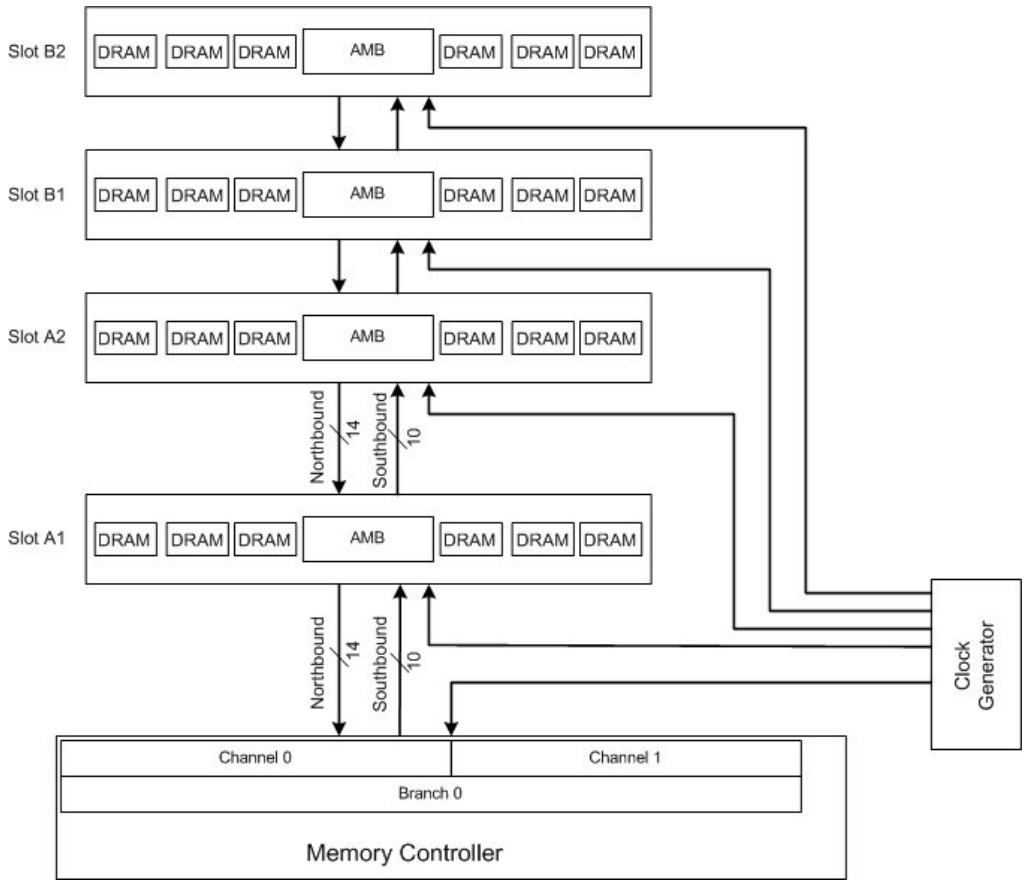


Рисунок 3. Топология FBD

2.3.2 Поддерживаемые модули памяти

Контроллер-концентратор памяти Intel® 5000 поддерживает одноканальный режим работы памяти DIMM, когда только один модуль FBDIMM установлен в разъем DIMM A1. Установка модулей в другие банки DIMM не поддерживается для работы в одноканальном режиме.

Таблица 1 Системные платы для серверов и рабочих станций поддерживают максимальные объемы памяти, которые указаны в Таблице 1. Максимальный объем памяти, поддерживаемый набором микросхем, определяется емкостью модуля DIMM и количеством разъемов DIMM. Минимальный объем памяти, поддерживаемый системой в одноканальном режиме, равен 512 МБ, при этом используется один модуль DIMM, установленный в разъеме DIMM A1.

Примечание: *Проверка модулей памяти корпорацией Intel проводится путем тестирования идентичных модулей памяти во всех разъемах DIMM. При проверке памяти не тестируется одноканальный режим памяти, а также память с модулями DIMM смешанного типа и/или разных производителей.*

Поддерживаются модули DIMM емкостью 512 МБ, 1 ГБ, 2 ГБ и 4 ГБ.

Таблица 1. Объемы модулей памяти DIMM

Использованные SDRAM компоненты / SDRAM технология	512 МБ	1 ГБ	2 ГБ	4 ГБ
X8, одинарный ряд	512 МБ	1 ГБ	2 ГБ	4 ГБ
X8, двойной ряд	1 ГБ	2 ГБ	4 ГБ	8 ГБ
X4, одинарный ряд	512 МБ	1 ГБ	2 ГБ	4 ГБ
X4, помещённый в стек, двойной ряд	1 ГБ	2 ГБ	4 ГБ	8 ГБ

Модули DIMM канала A спарены с модулями DIMM канала B для формирования 4-кратного чередования. Каждая пара модулей DIMM называется банком. Банк может делиться на два ряда при использовании двусторонних модулей DIMM. Если оба модуля DIMM в банке являются односторонними, это означает, что в системе присутствует только один ряд. При использовании двусторонних модулей DIMM говорится, что установлено два ряда.

На системных платах для серверов и рабочих станций имеются восемь разъемов DIMM, или четыре канала DIMM. Оба модуля DIMM в канале должны быть идентичными (т.е. быть изготовлены по одинаковой технологии, иметь одинаковую задержку CAS, одинаковое количество рядов, столбцов и компонентов DRAM, одинаковую рабочую частоту, и т.д.) Хотя модули DIMM в канале должны быть идентичными, BIOS поддерживает модули DIMM различного объема и конфигурации, благодаря чему каналы памяти могут быть разными. Определение объема и конфигурирование памяти гарантируются только для протестированных модулей DIMM, утвержденных корпорацией Intel.

Примечание: *Некоторые платы отличаются по поддерживаемому объему памяти. Дополнительная информация содержится в технических характеристиках системных плат Intel® для серверов и рабочих станций, относящихся к Вашей продукции.*

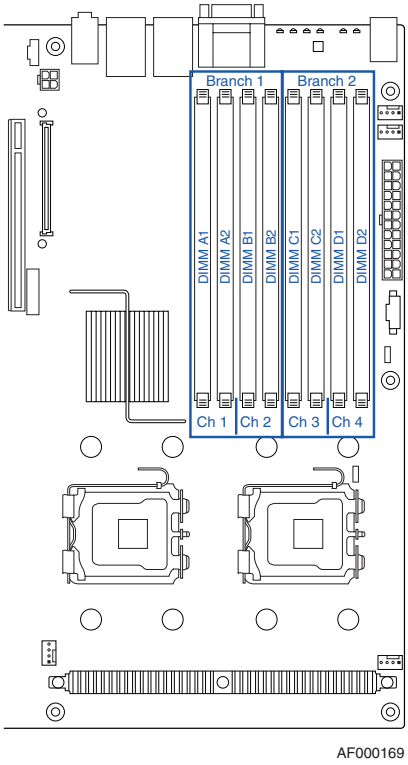


Рисунок 4. Идентификация банков памяти

2.4 Подсистема ввода/вывода

Подсистема ввода/вывода состоит из нескольких компонентов:

- Подсистема PCI
- Поддержка Serial ATA (SATA)
- SCSI с последовательным интерфейсом (Serial-attached SCSI, SAS)
- Поддержка RAID
- Поддержка интерфейса Parallel ATA (PATA)
- Видеоконтроллер
- Сетевой адаптер (NIC)
- Поддержка шины USB 2.0
- Поддержка Super I/O

В данном разделе описываются функции всех интерфейсов ввода/вывода и принципы их работы.

2.4.1 Подсистема PCI

2.4.2 Порядок сканирования

Начиная с нижнего устройства, BIOS использует алгоритм «поиска в глубину» для нумерации шин PCI в соответствии со *Спецификацией локальной шины PCI версия 2.2.* Номер шины увеличивается, когда BIOS обнаруживает устройство связи, не входящее в состав набора микросхем. Поиск продолжается на другой стороне моста до тех пор, пока не будут определены все подчиненные шины. Номера шин PCI могут различаться при каждой загрузке в зависимости от присутствия устройств на мостах PCI. При установке устройства с мостом на шину PCI, все последующие номера шин PCI под текущей шиной увеличиваются на единицу.

Назначение шины осуществляется один раз в начале процедуры загрузки BIOS и никогда не изменяется во время фазы предварительной загрузки.

2.4.3 Назначение ресурсов

Менеджер ресурсов назначает прерывания PIC для всех устройств, доступ к которым будет осуществляться унаследованным программным кодом. BIOS обеспечит правильность настройки реестров PCI BAR и командного реестра для всех устройств, для обеспечения соответствия действиям унаследованных команд BIOS после загрузки в унаследованную ОС. Любой унаследованный программный код не может делать предположения относительно порядка сканирования устройств или порядка, в соответствии с которым им будут выделяться ресурсы.

В унаследованном режиме, BIOS поддерживает вызовы интерфейса INT 1Ah PCI BIOS.

2.4.4 Автоматическое назначение IRQ

BIOS автоматически назначает IRQ системных устройств для обеспечения совместимости. Возможность установки IRQ для устройств вручную отсутствует.

2.4.5 Поддержка дополнительных унаследованных ПЗУ

При выполнении кода поддержки BIOS для унаследованных устройств проверяется наличие унаследованных опциональных ПЗУ в доступном адресуемом пространстве в диапазоне адресов 0C0000h-0DFFFFh, и затем система следует всем унаследованным правилам по отношению к опциональным ПЗУ. Если доступная память имеется в сегменте E, а сегменты C и D уже используются, BIOS также будет использовать теневую память до адреса 0E7FFF. В настройках BIOS можно отключить использование теневой памяти устройствами PCI, расположенными на плате.

2.4.6 EFI PCI API

BIOS поддерживает стандартные протоколы PCI, описанные в спецификации *Extensible Firmware Interface Reference Specification*, версия 1.1.

2.4.7 Унаследованные PCI API

В унаследованном режиме BIOS будет поддерживать функции INT 1Ah, AH = B1h в соответствии со *Спецификацией PCI BIOS* версия 2.1. Системный BIOS поддерживает интерфейс реального режима.

2.4.8 Двойной видеопорт

BIOS поддерживает режим работы с одним и двумя мониторами. Двойной видеорежим отключен по умолчанию.

- В режиме с одним монитором встроенный видеоконтроллер отключается при обнаружении карты расширения.
- В двойном видеорежиме видеоконтроллер на плате доступен и является основным видеоустройством. На внешнюю видеокарту выделяются ресурсы, и она считается вспомогательным видеоустройством.

Дополнительная информация содержится в технических характеристиках системных плат Intel® для серверов и рабочих станций, относящихся к Вашей продукции.

2.4.9 Поддержка интерфейса Parallel ATA (PATA)

Встроенный контроллер IDE контроллера-концентратора ввода/вывода Intel® 631xESB / 632xESB ICH6 поддерживает один канал IDE. Этот канал IDE может использоваться для подключения одного оптического устройства. Каналы IDE могут быть сконфигурированы или отключены/включены с помощью утилиты BIOS Setup.

BIOS поддерживает спецификации ATA/ATAPI версии 6. Она инициализирует интегрированный контроллер IDE в северном мосту набора микросхем (ICH5R) и устройства IDE, подключенные к нему. BIOS производит сканирование устройств IDE и программирует контроллер и устройства на работу в оптимальном режиме. Службы операций чтения/записи для дисков IDE, обеспечиваемые BIOS, используют режим PIO, однако BIOS запрограммирует необходимые реестры Ultra DMA в контроллер IDE так, чтобы операционная система могла использовать режимы Ultra DMA.

BIOS инициализирует и поддерживает устройства стандарта ATAPI (например, дисководы LS-120/240, CD-ROM, CD-RW и DVD).

2.4.9.1 Ultra ATA/100

Интерфейсы IDE протокола DMA Intel® 631xESB / 632xESB переопределяют сигналы на шлейфе IDE, обеспечивая ускорение передачи данных и повышение скорости до 100 МБ/с.

2.4.9.2 Инициализация IDE

BIOS поддерживает спецификацию ATA/ATAPI версии 6. BIOS инициализирует встроенный в набор микросхем (в контроллер-концентратор ввода/вывода Intel® 631xESB / 632xESB) контроллер IDE, а также подключенное к нему устройство IDE. BIOS производит сканирование устройств IDE и программирует контроллер и устройства на работу в оптимальном режиме. Службы операций чтения/записи для дисков IDE, обеспечиваемые BIOS, используют режим PIO, однако BIOS запрограммирует необходимые реестры Ultra DMA в контроллер IDE так, чтобы операционная система могла использовать режимы Ultra DMA.

2.4.10 Поддержка Serial ATA (SATA)

Контроллер integrated Serial ATA (SATA) контроллера-концентратора ввода/вывода Intel® 631xESB / 632xESB поддерживает до шести портов устройств SATA или до четырех портов устройств SAS, расположенных на серверной системной плате. Порты SATA можно включать/отключать и/или настраивать с помощью утилиты BIOS Setup.

BIOS инициализирует и поддерживает устрйоства SATA и устройства PATA. Она инициализирует интегрированный контроллер IDE в северном мосту набора микросхем (ICH5R) и устройства IDE, подключенные к нему. С точки зрения ПО, контроллеры SATA используют тот же интерфейс регистров, что и контроллеры PATA. Горячее подключение дисков SATA во время загрузки не поддерживается BIOS и может привести к неизвестным последствиям.

Функция SATA в контроллере-концентраторе ввода/вывода Intel® 631xESB / 632xESB имеет двойной режим работы, поддерживая различные состояния операционной системы. При использовании ОС с поддержкой Native IDE контроллер-концентратор ввода/вывода Intel® 631xESB / 632xESB I/O имеет отдельные функции PCI для последовательных и параллельных устройств ATA. Для поддержки устаревших операционных систем для последовательных и параллельных портов ATA имеется только одна функция ATA.

Реестр MAP обеспечивает возможность совместного использования функций PCI. При включении совместного использования функций декодирование всех операций ввода/вывода производится через реестры SATA. Запись программного обеспечения в реестр Function Disable Register (D31, F0, смещение F2h, бит 1) приводит к тому, что устройство 31, функция 1(контроллер IDE) скрывается, а его реестры конфигурации не используются. Указатель-реестр возможностей SATA (смещение 34h) изменится, указывая, что MSI не поддерживается в комбинированном режиме.

Контроллер SATA контроллера-концентратора ввода/вывода Intel® 631xESB / 632xESB имеет два набора интерфейсных сигналов, которые могут включаться или отключаться независимо друг от друга. Каждый интерфейс поддерживается независимым контроллером DMA. Контроллер SATA контроллера-концентратора ввода/вывода Intel® 631xESB / 632xESB взаимодействует с подключенными устройствами хранения данных через интерфейс реестров, аналогичный используемому обычными адаптерами IDE. Программное обеспечение сервера следует существующим стандартам и правилам при доступе к интерфейсу реестров и соблюдает стандартные правила командного протокола.

Скорость передачи данных по интерфейсу SATA не зависит от настроек режима UDMA. Скорость передачи данных интерфейса SATA зависит от максимальной скорости шины, вне зависимости от того, об использовании какого режима UDMA сообщается устройством SATA или BIOS.

2.4.11 Функциональная возможность SATA RAID

Дополнительная информация содержится в технических характеристиках системных плат Intel® для серверов и рабочих станций, относящихся к Вашей продукции.

2.4.12 SCSI с последовательным интерфейсом (Serial-attached SCSI)

Дополнительная информация содержится в технических характеристиках системных плат Intel® для серверов и рабочих станций, относящихся к Вашей продукции.

2.4.13 Видеоконтроллер

Дополнительная информация содержится в технических характеристиках системных плат Intel® для серверов и рабочих станций, относящихся к Вашей продукции.

2.4.14 Сетевые адаптеры (NIC)

Серверные системные платы Intel®, в которых используется этот набор микросхем, поддерживают два сетевых адаптера 10Base-T / 100Base / 1000Base-T на базе контроллера Intel® 82563EB. Системные платы Intel® для рабочих станций, в которых используется этот набор микросхем, поддерживают один сетевой адаптер 10Base-T / 100Base / 1000Base-T на базе контроллера Intel® 82564EB.

К сетевым адаптерам подключены два светоиндикатора, расположенные на каждом сетевом адаптере. Левый индикатор соединения/активности указывает на наличие сетевого соединения, а его мигание означает активность сетевого соединения (передачу или прием данных). Правый индикатор скорости указывает, что система работает в режиме 10 Мбит/с (выключен); 100 Мбит/с (горит зеленым) или 1000 Мбит/с (горит желтым). Описание индикаторов приведено в таблице ниже.

Таблица 2. Индикатор состояния NIC2

Цвет индикатора	Состояние индикатора	Состояние сетевого соединения
Зеленый/Желтый (левый)	Не горит	10 мбит/с
	Зеленый	100 мбит/с
	Желтый	1000 мбит/с
Зеленый (правый)	Включен	Активное соединение
	Мигает	Передача / Прием данных

2.4.15 Поддержка USB

В контроллер-концентратор ввода/вывода Intel® 631xESB / 632xESB интегрированы функции контроллера USB, обеспечивающие подключение до восьми портов USB 2.0. Для подключения внутреннего флоппи-дисковода USB предусмотрен один внутренний порт USB 2.0. Также на плате имеется один внутренний коннектор 1x10, поддерживающий подключение 2 дополнительных портов USB 2.0. Возможна маршрутизация портов USB 2.0 через мостовой соединитель платы для обеспечения опционального доступа с передней панели.

2.4.16 Физическая поддержка USB

Во время выполнения процедуры POST (power on self-test) BIOS инициализирует и конфигурирует подсистему USB в соответствии с частью 14 спецификации *Extensible Firmware Interface Reference Specification*, версия 1.1. BIOS может инициализировать и использовать следующие типы устройств USB:

- Клавиатуры, соответствующие спецификации USB
- Мыши, соответствующие спецификации USB
- Устройства хранения данных, соответствующие спецификации USB и использующие только блочный механизм передачи данных

Происходит поиск устройств USB, чтобы определить, требуются ли они для загрузки.

BIOS поддерживает устройства и хост-контроллеры USB 1.1 BIOS конфигурирует устройства и хост-контроллеры USB 2.0 в режиме USB 1.1, т.к. для поддержки режима USB 1.1 необходимы все устройства USB 2.0. Несмотря на то, что скорость передачи данных в режиме USB 1.1 меньше, чем в режиме USB 2.0, разница в скорости не существенна на этапе начальной загрузки. Операционная система может перевести устройства USB в режим USB 2.0, если это будет необходимо. BIOS конфигурирует усовершенствованный интерфейс хост-контроллера (EHCI), чтобы его могла использовать ОС.

На этапе начальной загрузки BIOS автоматически поддерживает горячее подключение и отключение устройств USB. Например, если устройство USB подключается в процессе начальной загрузки, BIOS определяет факт подключения, инициализирует устройство и делает его доступным для пользователя. BIOS инициализирует только контроллеры USB, расположенные на плате. Это не мешает ОС в поддержке любых доступных контроллеров USB, включая расположенные на картах расширения.

2.4.17 Поддержка стандартных разъемов USB

BIOS поддерживает эмуляцию PS/2* для клавиатур и мышей USB. Во время тестирования системы при включении BIOS производит инициализацию и настройку портов концентраторов, а затем производит поиск клавиатуры, мыши и концентраторов USB и включает их.

2.4.18 Суперконтроллер ввода/вывода

Поддержка стандартных устройств ввода/вывода реализована с помощью суперконтроллера ввода/вывода National Semiconductor* PC87427. Суперконтроллер ввода/вывода National Semiconductor* PC87427 содержит все необходимые цепи для управления двумя последовательными портами, одним параллельным портом и PS/2-совместимыми клавиатурой и мышью. Системные платы Intel® для серверов и рабочих станций, в которых используется этот набор микросхем, поддерживают следующее:

- GPIO
- Два последовательных порта
- Съемные диски
- Клавиатура и мышь
- Управление событиями пробуждения
- Поддержка восстановления системы

2.4.18.1 GPIO (Ввод/вывод общего назначения)

В суперконтроллере ввода/вывода National Semiconductor* PC87427 имеются 9 контактов ввода/вывода общего назначения, используемые серверной платой или платой для рабочих станций.

Примечание: *Дополнительная информация содержится в технических характеристиках системных плат Intel® для серверов и рабочих станций, относящихся к Вашей продукции.*

2.4.18.2 Съемные диски

BIOS поддерживает съемные устройства хранения данных в соответствии со списком протестированного аппаратного обеспечения и ОС. BIOS поддерживает загрузку с устройств хранения данных USB, подключенных к порту USB серверного корпуса, например, с миниатюрных устройств USB. BIOS поддерживает устройства хранения данных USB 2.0 с обратной совместимостью со спецификацией USB 1.1.

2.4.18.3 Клавиатура и мышь

На задней стороне серверной платы имеется блок из двух портов PS/2* для подключения клавиатуры и мыши. Каждый порт поддерживает как клавиатуру, так и мышь. Ни один порт не поддерживает горячую установку.

Возможна загрузка системы без подключения клавиатуры или мыши. Если клавиатура подключена, во время выполнения процедуры POST BIOS обнаруживает ее и отображает сообщение «Keyboard Detected» (обнаружена клавиатура) на экране POST.

2.4.18.4 Управление пробуждением

Суперконтроллер ввода/вывода содержит функциональные возможности, позволяющие различным событиям контролировать включение и выключение системы.

Примечание: *Дополнительная информация содержится в технических характеристиках системных плат Intel® для серверов и рабочих станций, относящихся к Вашей продукции.*

2.4.19 Флэш-память BIOS

BIOS поддерживает флэш-память Intel® 28F320C3B. Эта флэш-память представляет собой модуль флэш-памяти емкостью 4 МБ, 2 МБ из которых могут быть перепрограммированы. Флэш-память содержит процедуры инициализации системы, утилиту BIOS Setup и процедуры поддержки выполнения команд. Точная схема может быть изменена по усмотрению корпорации Intel.

Во флэш-ПЗУ имеются необходимые драйверы для периферийных устройств, расположенных на системной плате, включая SCSI, Ethernet и видеоконтроллеры. Утилита обновления флэш-памяти загружает образ BIOS во флэш-память.

2.5 Генерация и распределение синхронизирующих импульсов

Все шины на системных платах Intel® для серверов и рабочих станций, имеющих контроллер-концентратор памяти Intel® 5000, используют синхронный тактовый генератор. Цепь генерации и передачи синхронизирующих импульсов, расположенная на серверной плате, по мере необходимости генерирует частоту синхронизирующих импульсов и уровни напряжения, включая:

- Дифференциальный тактовый генератор с частотой 200 МГц и логическим уровнем 0,7 В. Для процессора 1, процессора 2, отладочного порта и контроллера-концентратора памяти Intel® 5000.
- Дифференциальный тактовый генератор с частотой 100 МГц и логическим уровнем 0,7 В на CK409B. Для буфера тактового генератора DB800.
- Дифференциальный тактовый генератор с частотой 100 МГц и логическим уровнем 0,7 В на DB800. Для устройства PCI Express* используется контроллер-концентратор памяти Intel® 5000, включающий разъем x4 PCI Express. Для устройств SATA используется контроллер-концентратор ввода/вывода Intel® 631xESB / 632xESB ICH6.

- 66 МГц на логических уровнях 3,3 В: для «Северного моста» 5000 и контроллера-концентратора ввода/вывода Intel® 631xESB / 632xESB ICH6.
- 48 МГц на логических уровнях 3,3 В: Для контроллера-концентратора ввода/вывода Intel® 631xESB/632xESB – ICH6 и SIO.
- 33 МГц на логических уровнях 3,3 В: Для контроллера-концентратора ввода/вывода Intel® 631xESB/632xESB – видео, BMC и SIO.
- 14,318 МГц на логических уровнях 2,5 В: Для контроллера-концентратора ввода/вывода Intel® 631xESB/632xESB – ICH6 и видео.
- 10 МГц на логических уровнях 5 В: Для BMC.

Скорость работы разъема PCI-X на карте расширения полной длины определяется используемой картой расширения.

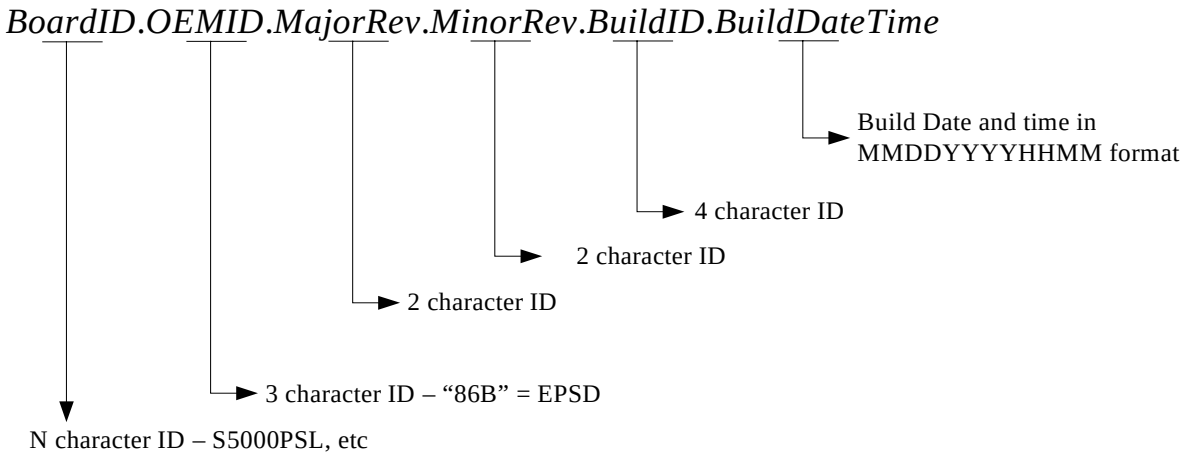
3. BIOS

BIOS реализуется в виде встроенного микрокода, записанного во флэш-памяти. BIOS обеспечивает работу алгоритмов инициализации аппаратных устройств и стандартных PC-совместимых базовых служб ввода/вывода, а также стандартных возможностей серверных плат Intel®. Flash-память также содержит встроенный микрокод для ряда встроенных устройств. Изображения этих устройств не приводятся в этом документе, поскольку они должны поставляться изготовителем.

Система BIOS реализована на основе архитектуры Intel® Platform Innovation Framework for EFI (Рамочная инфраструктура для развития платформ на базе расширяемого микропрограммного интерфейса) и полностью соответствует спецификациям, определенным в документе *Extensible Firmware Interface Reference Specification*, Version 1.1 Далее – просто «Рамочная архитектура».

3.1 Строка идентификации BIOS

Строка идентификации BIOS используется в качестве уникального идентификатора версии BIOS, используемой в сервере. Строка имеет следующий формат:



Например, идентификатор BIOS ID в процедуре POST для BIOS build 3, произведенной 13 августа 2005г в 11ч 56 мин, будет иметь следующее значение:

S5000.86B.01.00.0003.081320051156

Версия BIOS в утилите BIOS Setup будет указана как:

S5000.86B.01.00.0003

Параметр BIOS ID используется для идентификации образа BIOS. Он не предназначен для идентификации системной платы или фазы BIOS. Идентификатор системной платы доступен в структуре SMBIOS type 2. В ней же на основании сведений о выпуске, связанных с образом BIOS, может быть определена и фаза. Системная плата также может быть идентифицирована с помощью утилиты BIOS Setup.

3.2 Процессоры

3.2.1 Идентификационный номер процессора

Ниже приведен перечень процессоров и их идентификаторов (CPU ID), поддерживаемых серверными системными платами Intel® и другими платформами на базе набора микросхем Intel® серии 5000.

- Двухъядерный процессор Intel® Xeon® серии 5000 CPU ID – 00000F6xh
- Двухъядерный процессор Intel® Xeon® LV серии 5000: CPU ID – 000006Fxh

Таблица 3. Поддерживаемые конфигурации процессоров

Семейство процессоров	Скорость системной шины	Тактовая частота ядра	Кэш-память	Ватт	Поддержка
Процессор Intel® Xeon®	533 МГц	Все			Нет
Процессор Intel® Xeon®	800 МГц	Все			Нет
Процессор Intel® Xeon® 5050	667 МГц	3,0 ГГц	2x 2 МБ	95	Да
Процессор Intel® Xeon® 5060	1066 МГц	3,2 ГГц	2x 2 МБ	130	Да
Процессор Intel® Xeon® 5063	1066 МГц	3,2 ГГц	2x 2 МБ	95	Да
Процессор Intel® Xeon® 5080	1066 МГц	3,73 ГГц	2x 2 МБ	130	Да
Процессор Intel® Xeon® 51xx	1333/1066 МГц	подлежит определению	подлежит определению	подлежит определению	Да

3.2.2 Инициализация нескольких процессоров

В процессорах IA-32 на микропрограммном уровне реализован протокол арбитража процедуры назначении процессора, ответственного за инициализацию системы (bootstrap processor, BSP). Процессор, не выступающий в качестве загрузочного, называется прикладным процессором (AP).

Контроллер-концентратор памяти (MCH) набора микросхем Intel® серии 5000 имеет две процессорные системные шины, каждая из которых обслуживает последовательность двухъядерных процессоров Intel® Xeon® 5000. При включении системы из множества доступных ядер процессоров с помощью аппаратно реализованного алгоритма арбитража BSP-процессор назначается на каждой шине. Однако, системе BIOS для выполнения процедуры тестирования при включении питания (power-on self-test, POST) необходим лишь один процессор. Поэтому выбор системного BSP-процессора BIOS осуществляет на основе данных, записанных в регистрах MCH. Определить заранее, какой из процессоров будет выбран, нельзя. BIOS может гарантировать лишь то, что системный BSP-процессор будет назначен. Далее в данном документе термин «BSP» будет употребляться в значении «системный BSP-процессор».

BSP отвечает за выполнение процедуры POST и подготовку сервера к загрузке операционной системы. При загрузке сервера находится в виртуальном проводном режиме, и только BSP может принимать локальные прерывания (INTR от программируемого контроллера прерываний (PIC) и немаскируемые прерывания (NMI)).

Во время загрузки BSP активирует все AP. При активации AP программирует реестры своего диапазона типа памяти (MTRR), приводя их в соответствие с аналогичными реестрами BSP. Все AP выполняют команду остановки (halt) с отключенными локальными прерываниями. Если загрузочный процессор обнаруживает прикладной процессор, т.е. процессор с более низкими характеристиками, или обладает более низким значением CPUID, выбирается наименее функциональный процессор в качестве загрузочного процессора. В режиме управления системой (system management mode, SMM) программа-обработчик ожидает отклика всех процессоров на системное прерывание (system management interrupt, SMI).

3.2.3 Использование процессоров с различными технологическими степпингами

Для обеспечения оптимальной производительности необходимо использовать только идентичные процессоры. Допускается совместное использование процессоров одного семейства с различными номерами, если эти модификации указаны в обновляемых корпорацией Intel спецификациях на процессоры. BIOS не проверяет идентичность номеров процессоров. Информацию о возможных сочетаниях процессоров различных модификаций можно получить в обновлении к спецификации на процессор *Intel® Xeon®*. См. также Таблица 4.

3.2.4 Семейство процессоров смешанной конфигурации

Процессоры различных семейств не могут использоваться совместно. В случае обнаружения процессоров различных семейств контроллеру BMC передается сообщение об ошибке. См. Таблица 4.

3.2.5 Совместное использование процессоров с различными частотами системной шины

Процессоры с различными частотами системной шины не могут использоваться совместно. В случае обнаружения процессоров различных семейств контроллеру BMC передается сообщение об ошибке. См. Таблица 4.

3.2.6 Объем кэш-памяти процессоров смешанной конфигурации

При обнаружении процессоров с различными размерами кэш-памяти контроллеру BMC передается сообщение об ошибке. Объем кэш-памяти всех уровней должен совпадать для всех установленных процессоров. См. Таблица 4.

3.2.7 Обновление микропрограмм

В случае обнаружения процессора, не поддерживающего обновление микропрограмм, контроллеру BMC передается сообщение об ошибке. См. Таблица 4.

Процессоры IA-32 позволяют исправлять определенные фрагменты программных кодов путем загрузки предоставляемых корпорацией Intel блоков данных, известных как обновления микропрограмм. BIOS сохраняет обновления в энергонезависимой памяти и загружает их в каждый процессор во время процедуры POST. BIOS может хранить во флэш-памяти несколько обновлений. Количество хранимых обновлений ограничивается лишь объемом доступной памяти.

3.2.8 Кэш-память процессора

BIOS включает все уровни кэш-памяти процессора на самых ранних возможных этапах процедуры POST. Пользователь не имеет возможность изменять конфигурацию кэш-памяти процессора, ее размер или политику ее использования. Все обнаруженные размеры кэш-памяти фиксируются в структурах SMBIOS типа 7. Кэш-память самого высокого уровня, имеющая самый большой размер, отображается утилитой BIOS Setup.

3.2.9 Совместное использование процессоров различных конфигураций

В приведенной ниже таблице описаны действия, которые предпринимает система в различных ситуациях, возникающих при обнаружении разнородных процессоров. Информация в таблице актуальна для всех серверных системных плат Intel® и других платформ, базирующихся на наборе микросхем Intel®серии 5000. Возможны две категории ошибок:

- **Остановка:** Если загрузка системы возможна, то независимо от значения флага «Post Error Pause» управление передается непосредственно обработчику ошибок.
- **Пауза:** Если параметр «Post Error Pause» активен, то управление передается непосредственно обработчику ошибок. В противном случае система продолжит загрузку без вывода на экран сообщения об ошибке. Значение ошибки фиксируется обработчиком ошибок.

Таблица 4. Совместное использование процессоров различных конфигураций

Ошибка	Критические ошибки	Действия системы
Используются процессоры различных семейств	Остановка	BIOS фиксирует состояние ошибки и реагирует следующим образом: ▪ Ошибка регистрируется в журнале системных событий (SEL) ▪ На передней панели включается светодиодный индикатор «Неисправность системы» ▪ Включаются светодиодные индикаторы «Неисправность CPU» ▪ Процессор не блокируется ▪ Обработчиком ошибок на дисплей выводится сообщение «0194: Processor family mismatch detected» ▪ Производится останов системы
Используются процессоры с разными параметрами кэш-памяти	Остановка	BIOS фиксирует состояние ошибки и реагирует следующим образом: ▪ Ошибка заносится в журнал SEL ▪ На передней панели включается светодиодный индикатор «Неисправность системы» ▪ Включаются светодиодные индикаторы «Неисправность CPU» ▪ Процессор не блокируется ▪ Обработчиком ошибок на дисплей выводится сообщение «0192: Cache size mismatch detected» ▪ Производится останов системы
Используются процессоры с разными тактовыми частотами	Пауза	BIOS фиксирует состояние ошибки и реагирует следующим образом: ▪ Приводит к наименьшему общему знаменателю тактовые частоты всех процессоров ▪ Ошибка заносится в журнал SEL ▪ Обработчиком ошибок на дисплей выводится сообщение «0197: Processor speeds mismatched» ▪ Приостанавливает загрузку системы в ожидании действий пользователя При невозможности установить одинаковые тактовые частоты для всех процессоров ▪ Ошибка заносится в журнал SEL ▪ Обработчиком ошибок на дисплей выводится сообщение «0197: Processor speeds mismatched» ▪ Приостанавливает загрузку системы в ожидании действий пользователя

Ошибка	Критические ошибки	Действия системы
Отсутствует микрокод процессора	Пауза	BIOS фиксирует состояние ошибки и реагирует следующим образом: ▪ Ошибка заносится в журнал SEL ▪ На передней панели включается светодиодный индикатор «Неисправность системы» ▪ Включаются светодиодные индикаторы «Неисправность CPU» ▪ Процессор не блокируется ▪ Обработчиком ошибок на дисплей выводится сообщение «816x: Processor 0x unable to apply microcode update» ▪ Приостанавливает загрузку системы в ожидании действий пользователя
Используются процессоры с разными тактовыми частотами системной шины	Остановка	BIOS фиксирует состояние ошибки и реагирует следующим образом: ▪ Ошибка регистрируется в журнале системных событий (SEL) ▪ На передней панели включается светодиодный индикатор «Неисправность системы» ▪ Включаются светодиодные индикаторы «Неисправность CPU» ▪ Процессор не блокируется ▪ Обработчиком ошибок на дисплей выводится сообщение «0195: Processor System Bus speed mismatch detected» ▪ Производится останов системы

3.2.10 Технология Hyper-Threading

Процессоры Intel® Xeon® поддерживают технологию Hyper-Threading. BIOS определяет процессоры, в которых поддерживается эта технология, и включает данную функцию во время процедуры POST. В утилите BIOS Setup имеется возможность отключения/включения этой возможности. Активируются стандартные настройки.

Для описания виртуальных процессоров BIOS создает дополнительные записи в таблицах ACPI MP. В структуре SMBIOS типа 4 отображаются только установленные физические процессоры. Эта структура не описывает виртуальные процессоры.

Поскольку некоторые операционные системы не могут эффективно использовать технологию Hyper-Threading, BIOS не создает записи для описания виртуальных процессоров в таблицах Спецификации многопроцессорных конфигураций.

3.2.11 Технология Intel SpeedStep®

Процессоры Intel® Xeon® поддерживают функцию Geyserville технологии Intel SpeedStep® Эта функция изменяет тактовую частоту и напряжение процессора так же, как и функция Thermal Monitor 1 (TM1). Использование функции Geyserville возможно только в сочетании с TM1. Выполняя функцию Geyserville, BIOS взаимодействует с функцией TM1.

3.2.12 Технология Intel® Extended Memory 64 (Intel® EM64T)

BIOS данной серверной системной платы:

- Определяет, поддерживает ли процессор технологию Intel® Extended Memory 64 Technology (Intel® EM64T)
- Инициализируют для каждого процессора значение SMBASE
- Определяет в памяти SMRAM область сохранения состояния (State Save Map), используемую каждым процессором
- Во время инициализации подключает, если необходимо, поддержку технологии Intel® EM64T

3.2.13 Функция Execute Disable Bit

Функция Execute Disable Bit (XD bit) является усовершенствованием архитектуры IA-32 Intel®. Процессоры IA-32, поддерживающие функцию Execute Disable Bit, могут предотвращать использование программами-вирусами страниц данных в качестве исполняемого кода. Процессоры IA-32 с поддержкой функции XD bit обеспечивают защиту памяти в следующих режимах:

- Обычный режим защиты, если разрешена расширенная адресация физической памяти (PAE).
- Режим IA-32e. В этом режиме разрешено использование технологии Intel® EM64T, функция PAE также должна быть активна.

Функция XD bit не вносит каких либо новых инструкций. Она лишь требует от операционной системы функционирования в среде с PAE и обеспечения защиты памяти на страничном уровне. Функция XD bit может быть активирована и деактивирована через утилиту BIOS Setup. По умолчанию она включена.

3.2.14 Усовершенствованный режим останова (C1E)

Все процессоры поддерживают режим останова (Halt State, C1), инициируемый командами HLT и MWAIT. Некоторые процессоры с целью еще большего снижения энергопотребления могут переходить в оптимизированный режим C1 так называемый, усовершенствованный режим останова (Enhanced Halt State, C1E) Если C1E разрешен и все логические процессоры одного физического процессора вошли в режим C1, то процессор снижает значение тактовой частоты ядер до значения тактовой частоты системной шины и VID. Переход физического процессора из режима C1 в режим C1E совершается аналогично соответствующему переходу, предусматриваемому технологией Enhanced Intel SpeedStep®. Выполнение таких переходов разрешается после того, как BIOS определит, что все системные процессоры поддерживают режим C1E.

3.2.15 Поддержка многоядерных процессоров

BIOS выполняет следующие операции:

- Инициализирует все ядра процессоров
- Устанавливает обработчики немаскируемых прерываний (NMI) для всех двухъядерных процессоров
- Оставляет проинициализированный AP-процессор в состоянии CLI/HLT
- Инициализирует стек для всех AP-процессоров

BIOS Setup обеспечивает возможность избирательного включения/отключения поддержки многоядерных процессоров. По умолчанию она включена.

Для описания виртуальных процессоров BIOS создает дополнительные записи в таблицах ACPI – многопроцессорные конфигурации. В структуре SMBIOS типа 4 отображаются только установленные физические процессоры. Эта структура не описывает виртуальные процессоры.

BIOS вносит сведения о двухъядерных процессорах в таблицу спецификаций процессоров.

3.2.16 Технология Intel® Virtualization

Технология Intel® Virtualization позволяет различным программным средам использовать общие аппаратные ресурсы Каждая программная среда может включать в себя операционную систему и приложения. Выбор режимов работы системы – с использованием/без использования технологии Intel® Virtualization – осуществляется через BIOS Setup. Стандартной установкой является режим «без использования».

Примечание: *Для того, чтобы изменение статуса использования технологии Intel® Virtualization, выполненное в BIOS Setup, вступило в силу, необходимо произвести выключение-включение системы.*

3.2.17 Акустический контроль скорости вращения вентилятора

Методика, применяемая для контроля температуры процессора, предусматривает также возможность снижения уровня шума посредством управления скоростью вращения вентилятора. Управление скоростью вращения вентилятора осуществляется на основании вычислений температуры процессора, в которых используются два параметра: «TCONTROL offset» и «TCONTROL base». BIOS извлекает из регистра MSR процессора значение «TCONTROL offset» и передает его регистру BMC. Регистр BMC, в свою очередь, из записей показаний температурного датчика извлекает значение параметра «TCONTROL base» и прибавляет его к значению, полученному от BIOS.

3.3 Память

Контроллер MCH набора микросхем Intel® 5000 поддерживает модули памяти DIMM с полной буферизацией (FBDIMM). Он разбивает все установленные на системной плате модули FBDIMM на две независимые группы, называемые ветвями. Каждая ветвь имеет по два канала. В двухканальном режиме для обеспечения синхронности данных в кэш-памяти и корректного вычисления ECC операции с модулями FBDIMM смежных каналов выполняются жестко параллельно. В одноканальном режиме активен только Канал 0.

BIOS может динамически конфигурировать контроллер памяти в соответствии с количеством доступных модулей FBDIMM и выбранным режимом RAS (определяется соотношением надежности, доступности и производительности памяти).

Примечание: *Функции резервирования и зеркального отражения памяти в настоящее время не поддерживаются, их поддержка будет реализована после начала производства.*

3.3.1 Калибровка и конфигурация памяти

BIOS поддерживает модули памяти, имеющие различную емкость и различные характеристики. Возможность использования комбинаций неидентичных модулей FBDIMM распространяется только на протестированные Intel типы модулей. BIOS считывает данные SPD в памяти SEEPROM для каждого модуля памяти, чтобы определить емкость и скорость установленных модулей памяти. С помощью алгоритма калибровки памяти определяется общий объем памяти каждого ряда модулей. BIOS программирует контроллер памяти таким образом, чтобы диапазон памяти доступный для процессора корректно отображался на соответствующие модули или группы модулей FBDIMM.

3.3.2 Коды ошибок POST

Диапазон адресов {0xE0, 0xEF} используется ранними версиями POST для записи информации об ошибках памяти. Последние версии POST используют этот диапазон для записи других системных ошибок.

- При недоступности памяти выполняется останов системы и на светодиодном индикаторе результатов диагностики POST отображается код 0xE1.
- Если система не может установить контакт с модулями FBDIMM, то BIOS берет таймаут случайной длительности и выводит на светодиодный индикатор результатов тестирования POST код 0xE4. Обычно это является признаком аппаратной неисправности.
- Если тесты Memory Intel® Interconnect built in self test (Intel® IBIST) или Memory Link Training оказываются неудачными для одного или нескольких модулей FBDIMM, обслуживаемых одним и тем же FDB-каналом памяти, то BIOS выводит на светодиодный индикатор результатов тестирования POST код 0xE6. Если тесты IBIST оказываются неудачными для всех модулей памяти, то система реагирует так же, как и при недоступности памяти.

Возникновение любой из вышеописанных ошибок сопровождается характерным звуковым сигналом системного динамика. Звуковые коды ошибок памяти описаны в Разделе 5.3.2, POST Code Checkpoints.

3.3.3 Вывод информации о системной памяти

- Если функция «display logo» в BIOS Setup отключена, то BIOS выводит информацию об общем объеме памяти системы на дисплей во время процедуры POST. Общий объем памяти определяется процедурой POST как сумма объемов памяти всех установленных модулей FBDIMM. Сведения об общем объеме памяти также доступны на главной страннице BIOS Setup.
- Кроме того, в BIOS Setup представлена информация об эффективном объеме памяти. Эффективный объем памяти представляет собой суммарный объем памяти FBDIMM всех активных (не отключенных) и не используемых в качестве резервных модулей FBDIMM.
- Если опция «Display Logo» отключена, BIOS выводит на экран информацию об общем объеме памяти системы в конце процедуры POST. Значение этой информации аналогично значению, описанному в предыдущем пункте.
- Для определения общего объема памяти системы BIOS использует сервисную функцию GetMemoryMap(), предоставляемую EFI-интерфейсом,
- а также функции INT 15h и E820h. Более подробную информацию можно получить в спецификации «The Advanced Configuration and Power Interface Specification», Revision 2.0.

Примечание: *Память между 4 ГБ и 4 ГБ минус 1,5 ГБ не будет доступна для операционной системы. Эта область зарезервирована для размещения BIOS, данных конфигурации APIC и виртуальной памяти видеоустройств. См. 3.3.3.1. Память резервируется также для ресурсов шин PCI / PCI Express* / PCI Express. Это означает, что если в системе установлено 4 ГБ памяти, использоваться может только 2,5 ГБ или меньше. Этот набор микросхем позволяет области памяти в неиспользуемый диапазон адресного пространства выше 4 ГБ. Для этого необходимо разрешить операционной системе использовать функцию Physical Address Extensions (PAE).*

3.3.3.1 Резервирование памяти для функций, использующих отображаемое адресное пространство

Область памяти размером 512 МБ в адресном пространстве ниже 4 ГБ всегда резервируется в качестве отображаемого в памяти диапазона ввода/вывода, используемого BIOS (отображается flash-память), процессором и микросхемами управления памятью. Этот диапазон представляется отсутствующим для операционной системы. Кроме того, BIOS создает еще одну область отображаемой памяти, используемую функциями PCI Express*. Эта область включает в себя 1,0 ГБ адресного пространства, необходимого для стандартного размещения данных конфигурации PC Express. При активированной функции PAE операционная системы может использовать этот диапазон или его часть.

3.3.3.2 Функция High-Memory Reclaim

Если в системе установлено 4 ГБ и более физической памяти, то зарезервированная память считается утраченной. Однако, с помощью функции «high-memory reclaim», поддерживаемой набором микросхем Intel® серии 5000, обеспечивается возможность отображения исключенных диапазонов адресного пространства в область системной памяти выше 4 ГБ. Системная память – это память, к которой может адресоваться процессор.

BIOS всегда разрешает использование функции «high-memory reclaim», если обнаруживает, что объем системной памяти составляет 4 ГБ и более . Функция может быть использована, если она поддерживается операционной системой и процессору разрешена расширенная адресация памяти (PAE). Большинство операционных систем поддерживают эту функцию. Для получения информации о возможностях конкретной операционной системы необходимо обратиться к документации на нее.

3.3.4 Совместное использование модулей памяти с различным быстродействием

BIOS позволяет использовать совместно модули памяти, имеющие различное быстродействие. Адаптация модулей выполняется выбором соответствующей комбинации частотных и временных параметров каждого модуля FBDIMM. В этом разделе описывается ожидаемый результат адаптации подсистемы памяти к использованию модулей FBDIMM с различными параметрами быстродействия на тактовой частоте, установленной пользователем.

3.3.4.1 Характеристики модулей FBDIMM

Чтобы правильно запрограммировать модуль FBDIMM для работы с тактовой частотой, установленной пользователем, BIOS обращается в хранилище данных SPD (Serial-presence Data) каждого модуля. В хранилище содержатся следующие параметры, определяющие частотно-временные характеристики модуля:

- Латентность CAS-сигнала (CL)
- Общая тактовая частота
- Аддитивная латентность (AL)
- Задержка чтения буфера (BRD)

Латентность CAS-сигнала и дополнительная латентность – это настраиваемые параметры, извлекаемые BIOS из хранилища данных SPD модулей FBDIMM. Параметр BRD – это средняя вносимая задержка, обусловленная тем, что операция сохранения в буфере AMB данных, считанных из DRAM-памяти, перед направлением их на южную или северную магистраль занимает некоторое конечное время.

3.3.4.2 Базовая тактовая частота и коэффициент передачи

Базовая тактовая частота – это частота интерфейса с памятью, обеспечиваемая набором микросхем Intel® серии 5000. Она определяет скорость выполнения набором микросхем транзакций с памятью. Коэффициент передачи определяет соотношение скоростей интерфейса процессора и интерфейса памяти.

BIOS поддерживает две номинала частот: 533 МГц и 667 МГц. BIOS также обеспечивает автоматический выбор значений базовой тактовой частоты и коэффициента передачи.

Во время сбора информации об установленной в системе памяти BIOS считывает из хранилища SPD каждого модуля FBDIMM значения минимально необходимой латентности. Затем BIOS устанавливает общую тактовую частоту, приемлемую для всех компонентов системы памяти, и конфигурирует сами компоненты в соответствии с выбранной частотой.

3.3.5 Тестирование памяти

3.3.5.1 Интегрированный механизм тестирования памяти Memory BIST

Контроллер MCH набора микросхем Intel® 5000 позволяет использовать комплексный механизм самотестирования памяти Memory Built-in Self Test (BIST). Этот механизм обеспечивает контроль и исправление ошибок данных как на уровне ячеек памяти, так и в процессе передачи данных из модулей FBDIMM.

BIOS использует механизм Memory BIST для выполнения двух специфических операций:

- Добавление к данным контрольных сумм ECC, обеспечивающих возможность проверки соответствия содержимого памяти определенному образу. Этот метод называется алгоритмом базового тестирования памяти. Он обладает низкой способностью обнаружения ошибок.
- Дополнительное тестирование модулей FBDIMM, позволяющее обнаруживать ошибки как при хранении данных в ячейках памяти, так и при передаче данных по магистралям. Этот метод известен как алгоритм расширенного тестирования памяти.

Механизм Memory BIST заменяет традиционные тесты памяти, выполняемые BIOS, и обладает значительно большим, по сравнению с ними, быстродействием. BIOS использует механизм Memory BIST для инициализации памяти по окончании процесса ее обнаружения. BIOS не выполняет встроенное самотестирование (BIST) памяти, когда система выходит из спящего режима S3 (S3 Resume) – для систем, которые поддерживают режим S3.

3.3.6 Механизм Memory Scrub

Система Intel® 5000 MCH включает в себя механизм обнаружения и исправления ошибок памяти «Memory scrub» – проверка памяти с поиском и исправлением ошибок. В активном состоянии этот встроенный компонент периодически проверяет ячейки памяти, находит и исправляет одноразрядные ошибки. Возможны два вида операций по проверке памяти:

- Проверка по требованию – выполняется, когда ошибка обнаруживается в процессе чтения/записи данных.
- Дежурная проверка – превентивный поиск мягких сбоев в заполненной памяти.

Оба вида проверки включены в BIOS по умолчанию.

Проверка невозможна при использовании зеркалирования памяти. Поэтому, если память переходит в режим зеркалирования, BIOS отключает эту функцию.

Примечание: *Функции резервирования и зеркального отражения памяти в настоящее время не поддерживаются, их поддержка будет реализована после начала производства.*

3.3.7 Карта памяти и правила заполнения памяти

Ниже приводится следующая спецификация для разъемов DIMM.

разъемы DIMM	Группа	Линия
DIMM_A1	0	A
DIMM_A2	0	A
DIMM_B1	0	B
DIMM_B2	0	B
DIMM_C1	1	C
DIMM_C2	1	C
DIMM_D1	1	D
DIMM_D2	1	D

Примечание: *Карта памяти и правила заполнения памяти могут различаться в зависимости от изделия. Обратитесь к Технической спецификации сервера или рабочей станции, которая прилагается к Вашему изделию, чтобы получить более полную информацию.*

3.3.7.1 Спецификация подсистемы памяти

- Модули памяти FBDIMM распределяются по разъемам каналов памяти, принадлежащих разным группам.
- Каждая группа может содержать максимум четыре DIMM-разъема для одного канала.
- Каждый канал имеет название A, B, C, и D.
- Каналы A и B составляют группу 0. Каналы C и D входят в группу 1.
- Идентификаторы разъемов DIMM, нанесенные на плату, содержат информацию о канале и, соответственно, группе, к которой относятся модули памяти. Например, DIMM_A1 – первый разъем канала A в группе 0. DIMM_C1 – первый разъем канала C в группе 1.

3.3.7.2 Установка дополнительной памяти

При расширении оперативной памяти следует устанавливать модули FBDIMM с учетом следующих факторов:

- Выбранный режим работы
- Ранее установленные модули FBDIMM
- Характеристики модулей FBDIMM
- Средства оптимизации Intel® 5000 MCH, направленные на повышение пропускной способности FBD

В двухканальном режиме смежные каналы одной группы работают параллельно, что позволяет увеличить пропускную способность FBD. Канал A и канал B работают параллельно если группа 0 настроена для поддержки двухканального режима работы, канал C и канал D работают параллельно, если группа 1 настроена на параллельную работу.

В одноканальном режиме активен только канал A из группы 0. В этом режиме группа 1 всегда отключена. Таким образом, в этом режиме используется только модуль FBDIMM на канале A. Остальные модули памяти FBDIMM отключены.

Ниже перечислены основные правила выбора и настройки памяти для получения наибольшей производительности системы.

- **Правило 1:** Группа каналов 0 всегда имеет преимущество перед группой 1 в определении режима работы. Следовательно, если группа 0 не поддерживает двухканальный режим работы, BIOS настроит систему для работы в одноканальном режиме, независимо от того, какие режимы доступны группе каналов 1.
- **Правило 2:** Заполнение разъема 1 группы 0 модулями FBDIMM обусловливает выбор режима работы. Если DIMM_A1 и DIMM_B1 не могут работать параллельно, то система переходит в одноканальный режим, при котором DIMM_B1 отключается.

- **Правило 3:** Одноканальный режим всегда предпочтительнее двухканального, если конфигурация канала 1 группы 0 несимметрична (если DIMM_A1 и DIMM_B1 не одинаковы).
- **Правило 4:** Разъем DIMM_A1 должен быть заполнен. Помимо этого, BIOS всегда выбирает режим работы, ориентируясь на настройки канала DIMM_A1, чтобы этот разъем использовался. Например, если в группе 0 только канал DIMM_A1 оснащен модулями памяти FBDIMM, то BIOS настроит систему для работы в одноканальном режиме с единственным активным каналом DIMM_ A1, *независимо от количества установленных модулей памяти FBDIMM в группе 1*. Такой метод расширения памяти некорректен, поскольку в этом случае используется не весь установленный объем памяти. Следовательно, такого режима работы необходимо избегать.
- **Правило 5:** Минимальная конфигурация FBDIMM подразумевает установку модуля только на канал DIMM_A1. При этом память работает в одноканальном режиме, и применение функций RAS невозможно.
- **Правило 6:** Минимальное количество модулей FBDIMM для активизации группы 1 – четыре: DIMM_A1, DIMM_B1, DIMM_C1 и DIMM_D1.
- **Правило 7:** Для параллельной работы группы в синхронном режиме (для двухканального режима), модули памяти FBDIMM, принадлежащие смежным каналам группы, должны быть идентичными по технологии, временным характеристикам и объему. Следовательно, для работы в двухканальном режиме DIMM_A1 и DIMM_B1 в группе 1 должны быть идентичны.

  Если модули FBDIMM смежных каналов одной группы не одинаковы, то модуль, установленный в старший канал, будет отключен.
- **Правило 8:** Модули памяти FBDIMM в смежных разъемах одного канала не обязательно должны быть одинаковыми.
- **Правило 9:** Для зеркального отображения памяти должно быть установлено не менее четырех модулей FBDIMM: DIMM_A1, DIMM_B1, DIMM_C1 и DIMM_D1. Зеркалирование памяти требует двухканального режима работы.
- **Правило 10:** Минимальный набор модулей для резервирования – два FBDIMM: DIMM_A1 и DIMM_A2. Минимальный набор модулей для парного резервирования – четыре модуля FBDIMM: DIMM_A1, DIMM_A2, DIMM_B1 и DIMM_B2.

При проверке памяти во время самотестирования после включения питания (процедура POST), BIOS отключает все модули FBDIMM, не соответствующие правилам.

Примечание: *Функции резервирования и зеркального отражения памяти в настоящее время не поддерживаются, их поддержка будет реализована после начала производства.*

3.3.7.3 Примеры установки модулей памяти FBDIMM и правила модернизации

Обратитесь к Технической спецификации сервера или рабочей станции, которая прилагается к вашему изделию, чтобы получить более полную информацию об установке модулей памяти FBDIMM и правилах модернизации.

3.3.8 Режимы работы памяти

Исходя из количества доступных модулей FBDIMM, BIOS выбирает оптимальный режим работы памяти. Настройки, доступные в режиме RAS:

- Одноканальный режим
- Режим с максимальным чередованием (двухканальный режим)
- Режим зеркалирования памяти
- Режим резервирования DIMM (двойные или одинарные FBDIMM)

Особые случаи использования двухканального и одноканального режимов, когда RAS отключен. В одноканальном режиме активен только один канал в каждой группе, смежные каналы отключены. В двухканальном режиме модули памяти FBDIMM смежных каналов каждой группы настроены на максимальное чередование для того, чтобы обеспечить полностью параллельное функционирование.

Примечание: *Функции резервирования и зеркального отражения памяти в настоящее время не поддерживаются, их поддержка будет реализована после начала производства.*

3.3.9 RAS памяти

Примечание: *Функции резервирования и зеркального отражения памяти в настоящее время не поддерживаются, их поддержка будет реализована после начала производства.*

3.3.9.1 Характеристики RAS

Серверные системные платы на основе наборов микросхем серии Intel® 5000 поддерживают следующие возможности RAS памяти:

- Зеркальный набор памяти
- Резервирование памяти
- Автоматическая подстройка нагрузки в зависимости от температуры (Thermal Throttling)
- Intel® Interconnect BIST (Intel® IBIST) для DIMM с полной буферизацией (FBD)

Эти стандартные режимы RAS используются в сочетании с обычными устройствами обнаружения и исправления ошибок и тестирования памяти, что обеспечивает полную поддержку RAS. Некоторые функции RAS реализованы на разных системных платах различным образом.

3.3.9.2 Резервирование памяти

Все версии наборов микросхем серии Intel® 5000 обеспечивают функцию резервирования памяти. Резервирование – это возможность RAS перераспределять модули памяти FBDIMM системной платы. Часть модулей становятся резервными и подключаются к работе взамен неисправных.

Резервное перераспределение памяти не предполагает создание избыточных копий памяти, и система не сможет продолжать работу в случае появления неисправимой ошибки. Цель резервирования памяти – обнаружить неисправные модули FBDIMM до возникновения системного сбоя. Обнаруженный неисправный модуль FBDIMM изолируется и удаляется из набора активных модулей, целостность системы поддерживается при помощи копирования данных из неисправного модуля в один из резервных модулей.

Обратитесь к разделу 3.7.2.1.2, для того чтобы узнать, как эта функция включается в BIOS. Программа установки BIOS укажет, возможно ли резервирование памяти при данной конфигурации памяти.

Примечание: *(Для этого необходимо, чтобы размер резервного модуля FBDIMM был, по крайней мере, не меньше размера самого большого основного модуля FBDIMM) Если резервирование возможно, BIOS проведет резервирование автоматически при следующем включении компьютера. Эта функция не требует дополнительной настройки, ее необходимо только включить в настройках BIOS. При включенной функции резервирования общий объем памяти уменьшается на объем резервных модулей FBDIMM.*

3.3.9.2.1 Резервирование DIMM в двухканальном режиме

При включении резервирования в двухканальном режиме, BIOS может независимо выбрать один физический канал, модуль в котором будет использоваться в качестве резервного, а другой канал использовать как обычный модуль. Такое выборочное резервирование обеспечивает максимальный объем доступной памяти с сохранением функций RAS. Тем не менее, использование модулей FBDIMM с различным числом каналов для резервирования не рекомендуется и может привести к непредсказуемым результатам.

3.3.9.3 Минимальный набор модулей FBDIMM для резервирования

Чтобы использовать функцию резервирования FBDIMM, требуется не менее двух FBDIMM на одном канале в любой группе. Включение резервирования в настройках BIOS приведет к тому, что BIOS сначала попытается задействовать эту функцию в обеих группах, но итоговая конфигурация каждой группы будет зависеть от набора модулей FBDIMM в ней.

Например: Правильные конфигурации для группы 0 – DIMM A1, DIMM A2. Неправильная конфигурация для группы 0 – DIMM A1. Поскольку в данном случае присутствует всего один модуль FBDIMM, невозможно выбрать резервный модуль.

Резервные модули FBDIMM не учитываются в объеме доступной физической памяти в обычном режиме работы. Поле «Доступная память» («Effective Memory») на экране настроек BIOS не отобразит объем памяти, задействованной для резервирования.

Примечание: *Функции резервирования и зеркального отражения памяти в настоящее время не поддерживаются, их поддержка будет реализована после начала производства.*

3.3.9.4 Зеркальное отображение памяти

В отличие от резервирования памяти, конфигурация с зеркалированием представляет собой избыточный образ памяти, позволяющий продолжить работу даже после некоторого количества неисправимых ошибок.

Зеркалирование памяти основано на RAS – в этом случае поддерживаются два идентичных образа памяти, что обеспечивает максимальную избыточность. В серверных системных платах на базе Intel® 5000 MCH зеркалирование происходит между группами 0 и 1: одна из групп содержит первичный образ, а другая – вторичный. Контроллер памяти всегда направляет запросы на чтение первичной группе. В обычных условиях запросы на запись направляются обеим группам.

Поскольку доступная оперативная память разделена на первичный образ и копию этого образа, объем доступной памяти сокращается вдвое. Например, если система с общим объемом модулей FBDIMM 1 ГБ работает в режиме зеркалирования памяти, то будет доступно 512 МБ оперативной памяти, поскольку половина модулей FBDIMM используется для хранения вторичного образа.

Для успешного зеркалирования модули FBDIMM в соответствующих разъемах DIMM различных групп должны быть идентичными по технологии, количеству каналов, временным характеристикам и объему.

В BIOS существует настройка для включения зеркалирования памяти. Когда зеркалирование памяти включено, BIOS пытается соответствующим образом настроить систему памяти. Если набор FBDIMM не подходит для зеркалирования, BIOS отключает зеркалирование и возвращается в режим по умолчанию без использования RAS с максимальным чередованием или в одноканальный режим. При следующей перезагрузке в настройках BIOS сохраняется режим, выбранный автоматически.

Дополнительная информация содержится в технических характеристиках системных плат Intel® для серверов и рабочих станций, относящихся к Вашей продукции.

3.3.9.4.1 Минимальный набор FBDIMM для зеркалирования

Для зеркалирования памяти должны выполняться следующие минимальные требования:

- **Конфигурация групп:** Для зеркалирования требуется активность обеих групп.
- **Настройки чередования:** Для зеркалирования требуется, чтобы чередование на уровне каналов в обеих группах было настроено так, чтобы модули FBDIMM работали синхронно.

Из этих требований следует, что минимальный набор модулей FBDIMM – DIMM_A1, DIMM_B1, DIMM_C1 и DIMM_D1. Дополнительная информация приведена в разделе 3.3.7.

В этом режиме пара DIMM A1-DIMM B1 и пара DIMM_C1-DIMM_D1 работают синхронно в группе 0 и группе 1 соответственно, что отвечает перечисленным требованиям. Таким образом, минимальное количество модулей для зеркалирования равно четырем, и они должны располагаться описанным выше образом. Различающиеся модули FBDIMM или пары модулей будут отключены на уровне BIOS таким образом, чтобы группы были симметричны и сбалансированы.

Примечание: *Функции резервирования и зеркального отражения памяти в настоящее время не поддерживаются, их поддержка будет реализована после начала производства.*

3.3.9.5 Автоматическая подстройка нагрузки в зависимости от температуры (Thermal Throttling)

Наборы микросхем Intel® MCH серии 5000 поддерживают автоматическое переключение уровня электропитания модулей FBDIMM при большой нагрузке на память, например, при работе с приложениями, требовательными к памяти. Это опосредованно приводит к повышению температуры буферов AMB модулей FBDIMM. Управление уровнем питания всегда включено на уровне BIOS.

BIOS передает контроллеру системной платы (BMC) команду, сообщая о режиме работы вентилятора, выбранном в настройках BIOS – низкий уровень шума («acoustic») или высокая производительность («performance»), – после чего передается дополнительная команда для получения настроек этого режима. Для настройки управления уровнем питания и скоростью вращения вентиляторов для памяти и набора микросхем BIOS использует параметры, полученные из записей датчиков температуры (thermal SDR), и установленное в настройках BIOS значение высоты. Если BIOS не удается получить записи датчиков температуры, используются значения температуры по умолчанию, заданные в MRC.

3.3.10 Обработка ошибок памяти

В этом разделе описано поведение BIOS и набора микросхем при обработке и индикации ошибок подсистемы памяти.

3.3.10.1 Классификация ошибок памяти

С точки зрения BIOS существует следующие категории ошибок памяти:

- **Исправимые ошибки ECC:** ошибки, происходящие в ячейках памяти и приводящие к искажению данных в памяти, но исправляемые механизмом ECC, встроенным в набор микросхем.
- **Неисправимые ошибки ECC:** ошибки, происходящие в ячейках памяти и приводящие к искажению данных в памяти. Механизм ECC, встроенный в набор микросхем, обнаруживает эти ошибки, но не может их исправить. Такие ошибки нарушают достоверность данных и являются серьезными ошибками.
- **Невосстановимые или критические ошибки:** ошибки, не распознаваемые стандартным механизмом ECC. К таким ошибкам относятся ошибки, вызванные высокой температурой, ошибки канала FBD и ошибки потока данных. Такие ошибки приводят к катастрофическому сбою системы.

Существует два этапа, на которых могут произойти ошибки памяти:

- В ходе процедуры POST, во время обнаружения памяти
- По окончании процедуры POST или после передачи управления операционной системе

Во время тестирования POST, BIOS при помощи средств встроенного самотестирования (BIST) обнаруживает ошибки памяти и сообщает о них.

- Ошибки конфигурирования RAS памяти

Во время работы операционной системы BIOS обнаруживает исправимые, неисправимые и критические ошибки подсистемы памяти и сообщает о них.

- Потеря функциональности RAS

3.3.10.1.1 Сбойные модули FBDIMM

BIOS обеспечивает обнаружение сбойного или потенциально неисправного модуля FBDIMM. Модуль FBDIMM считается сбойным, если он не проходит тест BIST. BIOS включает встроенные механизмы тестирования памяти в наборах микросхем Intel® серии 5000 во время инициализации памяти при начальном тестировании системы (POST). Цикл встроенного тестирования BIST для памяти обнаруживает неисправные, сбойные и потенциально сбойные модули FBDIMM, затем BIOS помечает эти модули как неисправные и отключает их.

В модулях FBDIMM может произойти сбой в штатном режиме работы. BIOS помечает эти модули как временно отключенные и выполняет другие необходимые служебные действия. Тест BIST для памяти выполняется для всех модулей FBDIMM при каждом запуске системы, за исключением пробуждения из состояния S3.

3.3.10.1.2 Сбойные соединения

Технология FBDIMM является последовательной. В связи с этим, ошибки или сбои могут возникать в последовательном соединении между модулями FBDIMM. Эти ошибки отличаются от ошибок ECC и необязательно возникают в результате сбойных модулей FBDIMM. BIOS ведет историю возникновения ошибок на уровне соединения.

В общем случае, при возникновении ошибки соединения BIOS отключает все модули FBDIMM, использующие это соединение. Если все модули используют одно сбойное соединение, BIOS генерирует код ошибки POST 0xE1, показывающий, что в системе отсутствует работоспособная память, а затем останавливает систему.

Если сбой соединения происходит в штатном режиме работы (после POST), BIOS сигнализирует о критической ошибке и выполняет действия по обработке критических ошибок.

BIOS обрабатывает ошибки памяти в соответствии с набором действий, зависящим от платформы. Каждый из этих наборов действий нацелен на обеспечение полной диагностической поддержки для системного администратора при восстановлении системы после сбоя.

BIOS использует счетчики ошибок в наборах микросхем Intel® серии 5000, а также внутренние программные счетчики для отслеживания количества исправимых и многоразрядных исправимых ошибок, возникающих в штатном режиме работы. Набор микросхем увеличивает эти счетчики при возникновении ошибок. Значения счетчиков ошибок уменьшаются со скоростью (скоростью исправления), задаваемой в BIOS. Благодаря такому поведению счетчиков, они называются «счетчиками типа «дырявое ведро»» (*leaky bucket counters*).

3.3.10.1.3 Счетчики ошибок и пороговые значения

Счетчики типа «дырявое ведро» позволяют измерять частоту возникновения ошибок. BIOS настраивает и использует счетчики и скорость исправления, чтобы отследить потенциально сбойные модули FBDIMM. Потенциально сбойный модуль FBDIMM обычно порождает всплеск ошибок за короткий период времени. Этот всплеск обнаруживается алгоритмом «дырявого ведра». Набор микросхем поддерживает отдельные внутренние счетчики типа «дырявое ведро» для исправимых и многоразрядных исправимых ошибок.

BIOS инициализирует счетчики исправимых ошибок значением 10 для исправимых ошибок ECC. Для модулей каждого ранга поддерживается свой счетчик ошибок. Ранг соответствует паре модулей FBDIMM, расположенных на разных каналах и функционирующих в синхронном режиме.

3.3.10.1.3.1 Поведение BIOS в случае обнаружения исправимых ошибок

Для каждой исправимой ошибки, случившейся до достижения порогового значения, BIOS создает соответствующую запись («Correctable Error») в журнале системных событий (system event log, SEL). Других действий не производится, продолжается нормальное функционирование системы.

Когда пороговое значение достигает 10, BIOS создает запись в SEL, сообщающую об исправимой ошибке. Помимо этого выполняются следующие четыре шага:

1. Если включено резервирование, набор микросхем выполняет аварийное переключение на резервный модуль FBDIMM. В других конфигурациях памяти последующие исправимые ошибки маскируются и не записываются в SEL.
2. BIOS создает в SEL запись о достижении порогового значения («Max Threshold Reached»).
3. BIOS передает контроллеру системной платы сообщение о сбое DIMM («DIMM Failed»). Вслед за этим контроллер системной платы включает светодиоды – индикаторы системного сбоя –, снижает производительность памяти и запускает проверку сбойного модуля FBDIMM.
4. Контроллер системной платы включает светодиод «Сбой DIMM» для сбойного модуля FBDIMM.

3.3.10.1.4 Пороговое значение для счетчиков многоразрядных исправимых ошибок

Набор микросхем устроен таким образом, что пороговое значение для исправимых ошибок используется и для многоразрядных исправимых ошибок. Однако использование уровня толерантности 10 для многоразрядных исправимых ошибок нежелательно, поскольку эти ошибки являются критическими. Поэтому BIOS задает пороговое значение для многоразрядных исправимых ошибок на основе следующих правил:

- **Автоматические повторные попытки при возникновении ошибок памяти:** Набор микросхем автоматически выполняет повторное чтение при возникновении неисправимых ошибок. Если повторная попытка привела к успеху, ситуация классифицируется как многоразрядная исправимая ошибка. Если данные по-прежнему неверны, то это неисправимая ошибка, если контроллер памяти не работает в режиме зеркалирования памяти. Повторное чтение устраняет временные ошибки контрольной суммы, которые могут возникать в пакетах данных, передаваемых по последовательным соединениям FBDIMM между набором микросхем и модулями FBDIMM.
- **Уведомление об ошибках внутри набора микросхем:** Набор микросхем регистрирует возникновение неисправимой ошибки, как во время ее возникновения, так и при последующем сбое во время повторного чтения. Уведомления об обеих ошибках передаются в BIOS независимо.

3.3.10.1.5 Пороговое значение числа критических ошибок FBD

Помимо стандартных ошибок ECC, BIOS отслеживает ошибки протокола FBD, сообщения о которых приходят от набора микросхем. Ошибки протокола FBD приводят к ухудшению параметров оперативной памяти, поэтому они недопустимы ни в каком количестве. В BIOS существует внутренний программный счетчик для ошибок FBD. Пороговое значение этого счетчика равно 1.

3.3.10.1.5.1 Поведение BIOS при возникновении неисправимых ошибок

В случае возникновения неисправимой ошибки BIOS создает в SEL запись о ней («Uncorrectable Error»). BIOS генерирует немаскируемое прерывание (NMI).

3.3.10.1.6 Период действия ошибки

Период действия ошибки (скорость исправления) задает скорость, с которой уменьшаются значения счетчиков типа «дырявое ведро». Время исправления – это интервал времени, который требуется для того, чтобы значение счетчика достигло 0.

Поскольку частота ошибок напрямую связана с объемом модулей FBDIMM, для определения оптимального периода BIOS использует информацию, приведенную в следующей таблице:

Объем FBDIMM	Время исправления (приблизительно)
512 МБ	9 дней
1 ГБ	9 дней
2 ГБ	9 дней
4 ГБ	7 дней

3.3.10.1.7 Повторная попытка при возникновении ошибки

В случае любого сбоя Intel® 5000 MCH осуществляет повтор операции. В режиме зеркалирования операции чтения выполняются только с первичным образом. Операции записи выполняются с обоими образами. Поведение набора микросхем при возникновении ошибки зависит от операции, при которой ошибка была обнаружена изначально.

- Когда набор микросхем сталкивается с неисправимой ошибкой в группе X, отправляется запрос на повтор операции в группу Y. Если повторная операция успешна, происходит исправление данных, работа возобновляется в обычном режиме.
- Если повторная операция с другой группой также заканчивается сбоем, и обе группы дают сбой при повторе, то набор микросхем сбрасывает обе группы и сообщает в BIOS о критической ошибке.

3.3.10.2 Уведомление об ошибках памяти

Уведомление об ошибках памяти происходит при помощи разнообразных элементов, зависящих от платформы.

Элемент платформы	Описание
ECC Event Logging	Когда в штатном режиме работы происходит ошибка памяти, BIOS записывает информацию об ошибке в журнал системных событий в хранилище контроллера системной платы.
Экран диагностики/ ошибки BIOS	В конце тестирования POST менеджер ошибок BIOS сообщает об ошибках, найденных во время теста MemBIST.
Эвуковые сигналы	BIOS издает звуковой сигнал в случаях, когда в системе не установлена память или когда был выявлен сбой соединения во время обнаружения памяти, что привело к отключению всей памяти.
Экран настроек BIOS	Когда модули FBDIMM не проходят тест BIST, или обнаруживаются ошибки конфигурирования RAS, состояние FBDIMM выводится на экране «Advanced | Memory» в настройках BIOS.
Светодиоды «Сбой DIMM»	Системные платы Intel® для серверов и системы на базе набора микросхем Intel® серии 5000 оснащены набором светодиодов, сигнализирующих о сбое модуля памяти – по светодиоду на каждый разъем DIMM. Эти светодиоды используются для обозначения неисправных или сбойных модулей FBDIMM.
Светодиоды «Системный сбой/Состояние системы»	Системные платы Intel® для серверов и системы на базе набора микросхем Intel® серии 5000 поддерживают специальный светодиод на передней панели, сообщающий о состоянии системы. Когда происходит ошибка памяти, влияющая на производительность подсистемы памяти, BIOS посылает контроллеру системной платы запрос на включение светодиода «Системный сбой».
Генерирование NMI	BIOS генерирует немаскируемое прерывание (NMI), чтобы остановить систему после критической ошибки.

3.3.10.2.1 Протоколирование ошибок памяти

Для протоколирования ошибок памяти BIOS посылает контроллеру системной платы команды на запись в журнал системных событий (SEL). Данные форматы ошибок описаны в *Спецификации на интеллектуальный интерфейс управления платформами (Intelligent Platform Management Interface Specification) ,в.2.0*.

Тип датчика	Коды типов датчиков	Смещение	Описание
Память	0x0C	0x08	Ошибка памяти ECC
Память	0x0C	0x09	Ошибка памяти ECC

Данные событий 1	
0x20	Исправимая ошибка ECC
0x21	Неисправимая ошибка ECC
0x25	Достигнуто пороговое значение числа исправимых ошибок ECC
Данные событий 2	
0xFF	
Данные событий 3	
Бит [7:6]	Индекс записи SMBIOS Type16 для системного устройства Memory Array Device. Для серверных системных плат Intel® и систем, использующих набор микросхем Intel® серии 5000 это значение всегда равно 0, что означает использование одного встроенного контроллера памяти.
Бит [5:0]	Индекс записи SMBIOS Type17 для сбойного модуля FBDIMM.

3.3.10.2.2 Уведомление об ошибках теста BIST для памяти

Экран менеджера ошибок в BIOS содержит информацию о сбоях во время теста BIST, случившихся во время последнего тестирования POST.

Таблица 5. Ошибки памяти, отслеживаемые менеджером ошибок

Ошибка	Класс ошибки	Код ошибки	Текст ошибки	Описание
Ошибка конфигурации	Пауза	0x85F0	Не удалось сконфигурировать память для выбранного режима RAS.	BIOS не удалось сконфигурировать подсистему памяти для работы в выбранном режиме RAS.
Не пройден тест BIST для памяти	Пауза	0x852x	DIMM_xx failed Self Test (BIST).	Во время проведения теста BIST для памяти (в ходе POST), BIOS обнаружила, что DIMM_xx не прошел этот тест.

Примечание: x = номер модуля DIMM, не прошедшего тест.

3.3.10.2.3 Светодиоды «Сбой DIMM»

В системных платах Intel® для серверов рядом с каждым разъемом DIMM установлен светодиодный индикатор сбоя. Эти светодиоды включаются, если выявлен сбой модуля FBDIMM в соответствующем разъеме.

Общая модель использования индикаторов сбоя DIMM следующая:

Таблица 6. Светодиоды «Сбой DIMM»

Ошибка	Режим работы	Описание
Модуль FBDIMM прошел тест BIST для памяти во время тестирования POST.	Нет	Около разъема FBDIMM включается светодиод «Сбой DIMM».
Происходит сбой во время тестирования каналов Intel® IBIST (в ходе POST).	Нет	Если на сбойном канале установлено несколько модулей FBDIMM, включаются все соответствующие светодиоды «Сбой DIMM».
Для потенциально сбойного модуля FBDIMM достигнут порог числа исправимых ошибок. (На одном FBDIMM обнаружены десять исправимых ошибок в рамках одного периода действия ошибки).	Система работает в одноканальном режиме.	Когда число ошибок модуля FBDIMM достигает порогового значения (на десятой ошибке), включается светодиод «Сбой DIMM».
Для потенциально сбойного модуля FBDIMM достигнут порог числа исправимых ошибок. (На одном FBDIMM обнаружены десять исправимых ошибок в рамках одного периода действия ошибки).	Система работает в двухканальном режиме.	Когда число ошибок синхронизированной пары модулей FBDIMM достигает порогового значения (на десятой ошибке), включается светодиод «Сбой DIMM» для обоих модулей из пары.
В модуле FBDIMM обнаружена неисправимая ошибка.	Система работает в одноканальном режиме.	Включается светодиод «Сбой DIMM» для сбойного модуля.
В модуле FBDIMM обнаружена неисправимая ошибка.	Система работает в двухканальном режиме.	Включаются светодиоды «Сбой DIMM» для сбойной пары модулей FBDIMM.
Произошла критическая ошибка на уровне соединения каналов или FBD.	Нет	Включаются светодиоды «Сбой DIMM» для всех модулей FBDIMM на одном канале или в одной группе.

Примечание: *Как показано в приведенной выше таблице, когда два модуля FBDIMM работают в синхронном режиме. Если в одном из модулей FBDIMM происходит сбой, BIOS также оповестит о наличии ошибки в парном модуле (включится соответствующий светодиод). Это происходит из-за того, что при работе в этом режиме BIOS не может локализовать сбои на уровне отдельного модуля. Во всех случаях контроллер системной платы включает светодиод после получения сигнала от интеллектуального интерфейса управления платформами (IPMI) через BIOS.*

3.3.10.2.4 Индикаторы состояний системы

Системные платы Intel для серверов оснащены индикатором состояния системы (светодиодом) на передней панели. Этот индикатор показывает множество разных ошибок системы. В приведенной ниже таблице описывается поведение системы при обнаружении ошибок памяти.

Таблица 7. Индикаторы состояний системы

Цвет	Состояние	Критичность	Описание
Не горит	Нет	Не готов	Отключение питания переменного тока
Зеленый / Оранжевый	Мигание	Не готов	Перед подключением питания постоянного тока – 15-20 секунд инициализации контроллера BMC при подаче тока на сервер. Кнопки панели управления отключены до завершения инициализации контроллера BMC
Зеленый	Включен	Система в нормальном состоянии	Система загружена и готова к работе
Зеленый	Мигает	Деградация	Деградация системы ▪ Не удается использовать весь установленный объем памяти (если установлено несколько модулей DIMM) ▪ Устранимые ошибки с переключением на резервный модуль DIMM (резервирование памяти). Это означает, что идет работа на резервном модуле DIMM, т.е. избыточность потеряна. Должен загореться соответствующий индикатор DIMM ▪ В конфигурации с зеркальным набором, когда теряется избыточность ▪ Потеря избыточности блока питания или вентиляторов. Не относится к подсистемам без избыточности ▪ Ошибки соединений PCI-e ▪ Ошибка/отключение процессора – при ошибке одного из двух процессоров ▪ Сигнал вентилятора – Ошибка вентилятора Число рабочих вентиляторов должно быть больше минимального необходимого числа ▪ Превышен некритический порог – Температура и напряжение
Желтый	Мигает	Не критическое	Некритическое оповещение – Возможен сбой системы ▪ Превышен критический порог напряжения ▪ Сигнал перегрева VRD ▪ В системе недостаточно вентиляторов ▪ Превышение порога из 10 устранимых ошибок в режиме без резервирования и без зеркального набора

Цвет	Состояние	Критичность	Описание
Желтый	Включен	Критическое или невосстановимое состояние	Критическое оповещение – Ошибка или отключение системы ▪ Ошибка DIMM при использовании одного модуля DIMM, в системе нет работоспособных модулей памяти ▪ Неустранимая ошибка памяти в режиме без резервирования ▪ Сигнал IERR ▪ Отсутствует процессор Processor 1 ▪ Превышение критических ограничений температуры (CPU ThermTrip, memory TempHi) ▪ Нет сигнала power good – ошибка питания ▪ Ошибка конфигурации процессора (например, несоответствие степпинга)

Светодиодами управляет контроллер системной платы, но информация об ошибках памяти, перечисленных в таблице, поступает к контроллеру от BIOS. О том, каким образом контроллер получает сообщения об ошибках, подробно рассказано в разделе 3.3.10.2.1. За переключение светодиодов в соответствии с уведомлениями, приходящими из BIOS отвечает контроллер системной платы.

3.3.10.2.4.1 Индикатор состояния – Инициализация BMC

При подключении системы к сети и подаче питания 5В режима ожидания для инициализации контроллера BMC на серверной плате требуется 15-20 секунд. В течение этого времени индикатор состояния системы мигает зеленым и оранжевым, а кнопка питания на панели управления отключается для предотвращения включения сервера. После того как контроллер системной платы заканчивает инициализацию, светодиоды состояния перестают мигать, и кнопка питания снова действует.

3.3.10.2.5 Генерирование NMI

BIOS создает немаскируемое прерывание (NMI), чтобы остановить систему, если память не может продолжать нормал ьную работу. В приведенной ниже таблице перечисляются условия, при которых вызывается немаскируемое прерывание.

Таблица 8. Генерирование NMI

Ошибка	Режим работы
Обнаружена неисправимая ошибка в штатном режиме работы.	RAS не используется (один канал или максимальная производительность), или же включен режим резервирования или зеркалирования, но и первичный образ, и копия содержат ошибки.
Происходят критические ошибки FBD во время работы системы.	Все режимы.

3.3.10.3 Ошибки режима зеркалирования

Когда режим зеркалирования доступен, BIOS сообщает об ошибках в соответствии со следующей таблицей:

Таблица 9. Ошибки режима зеркалирования

Событие	Действия
Пользователь выбрал режим зеркалирования, но BIOS не удалось перевести систему в этот режим.	Сообщение об ошибке в менеджере ошибок в конце тестирования POST. Ошибка ID 0x85FD В поле «Текущая конфигурация памяти» («Current Memory Configuration») на закладке «Дополнительные возможности | Память» («Advanced | Memory») в программе настройки BIOS указано «максимальная производительность» («maximum performance») или «одноканальный режим» («single-channel mode»), в зависимости от набора модулей FBDIMM
Исправимые ошибки в первичной или вторичной группе. Количество ошибок меньше порогового значения 10	Запись в SEL с указанием смещения датчика (Sensor Offset) = Исправимая ошибка.
Исправимая ошибка в первичной или вторичной группе, количество таких ошибок в одной группе достигает порогового значения10	Запись в SEL с указанием смещения датчика (Sensor Offset) = Исправимая ошибка. Запись в SEL с с указанием смещения датчика (Sensor Offset) = Пороговое значение числа исправимых ошибок Включается светодиод «Сбой DIMM» для сбойного модуля.
Первая неисправимая ошибка ECC в первичной или вторичной группе	Запись в SEL с указанием смещения датчика (Sensor Offset) = Неисправимая ошибка. Неисправная память отключается. Включается светодиод «Ошибка модуля DIMM» у модуля, в котором произошла ошибка. Вызывается немаскируемое прерывание.

Примечание: *Функции резервирования и зеркального отражения памяти в настоящее время не поддерживаются, их поддержка будет реализована после начала производства.*

Таблица 10. Обработка ошибок памяти в процессе тестирования POST

Сценарий	Сообщение POST	SEL	Состояние индикатора	Обновлено состояние памяти интерфейса IPMI	Работа системы
Неисправимая ошибка в процессе теста BIST для памяти (ошибка оборудования)	Сообщение о неисправимой ошибке, указывающее на размещение модуля FBDIMM	Код POST «Неисправимая ошибка» Код POST «Сбой DIMM» Расположение FBDIMM записано в SEL	Светодиод DIMM: Включен только для сбойного модуля FBDIMM. Индикатор сбоя системы Не включен.	Сбой DIMM = ДА Отключено = ДА	Система продолжает загрузку, если найдена работоспособная память. Если найдена только сбойная память, система издает последовательность звуковых сигналов и отображает диагностическое сообщение POST с помощью светодиодов.
Ошибка теста памяти Intel® IBIST во время POST	Сообщение о неисправимой ошибке, указывающее на размещение модуля (модулей) FBDIMM	Код POST «Неисправимая ошибка» Код POST «Сбой DIMM» Расположение модуля (модулей) FBDIMM записано в SEL	Светодиод DIMM: Включен для всех затронутых FBDIMM. Индикатор сбоя системы Не включен.	Сбой = ДА Отключено = ДА	Система отключит все модули FBDIMM на сбойном канале FBDIMM. Система продолжит нормальное функционирование, если на другом канале или в другой группе будут обнаружены работоспособные модули FBDIMM. Система включит светодиоды «Сбой DIMM» для всех FBDIMM, не прошедших IBIST, начиная с первого, независимо от наличия модулей в разъемах. Это указывает на более серьезный сбой канала или группы.

Таблица 11. Обработка ошибок памяти в штатном режиме, избыточность отсутствует

Сценарий	Сообщение POST	SEL	Состояние индикатора	Обновлено состояние памяти интерфейса IPMI	Работа системы
Штатный режим: Конфигурация != RAS Исправимые ошибки < Пороговое значение	Нет, поскольку BIOS не сохраняет информацию о состоянии памяти между перезагрузками.	Сообщение в SEL об исправимой ошибке с указанием модуля DIMM	Светодиод «Сбой DIMM»: Не включен. Индикатор сбоя системы Не включен.	Нет	Система продолжает работать.
Штатный режим: Конфигурация != RAS Исправимые ошибки >= Пороговое значение	Нет, поскольку BIOS не сохраняет информацию о состоянии памяти между перезагрузками.	Сообщение в SEL об исправимой ошибке Сообщение о достижении порога исправимых ошибок Остановка протоколирования исправимых ошибок	Светодиод DIMM: Включен только для сбойного модуля FBDIMM. Индикатор сбоя системы ▪ Зеленый / мигает: установлено больше одного FBDIMM. ▪ Янтарный / включен: Установлен только один FBDIMM.	Сбой = ДА Отключено = НЕТ	Система продолжает работать, но будет скрывать все исправимые ошибки памяти.
Штатный режим: Конфигурация != RAS UE	Нет, поскольку BIOS не сохраняет информацию о состоянии памяти между перезагрузками.	Сообщение о неисправимой ошибке с указанием модуля FBDIMM	Светодиод «Сбой DIMM»: Включены для синхронизированной пары или для одного модуля в зависимости от режима работы. Индикатор сбоя системы Янтарный / включен.	Сбой = ДА Отключено = ДА	В системе происходит NMI.

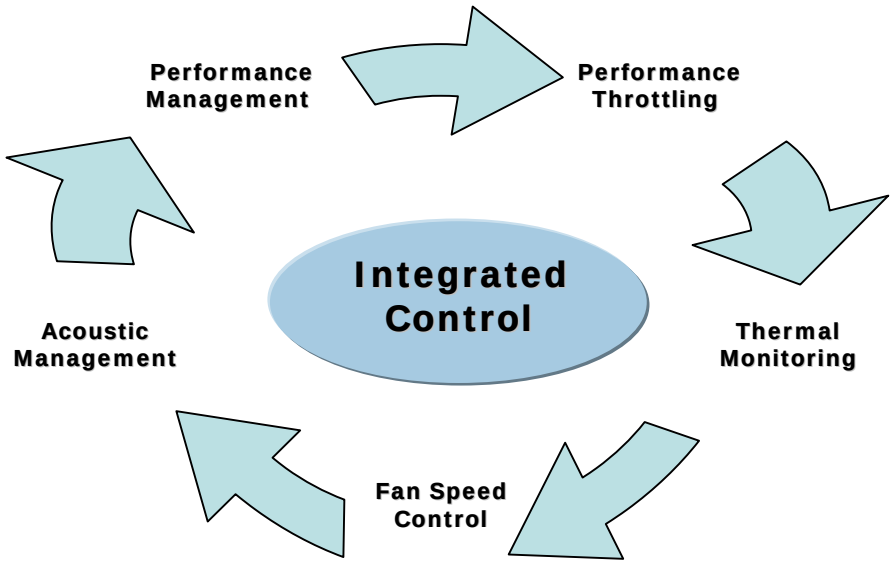
Таблица 12. Обработка ошибок в штатном режиме, включена избыточность

Сценарий	Сообщение POST	SEL	Состояние индикатора	Обновлено состояние памяти интерфейса IPMI	Работа системы
Штатный режим: Конфигурация = Резервирование Исправимые ошибки < Пороговое значение	Нет, поскольку BIOS не сохраняет информацию о состоянии памяти между перезагрузками.	Сообщение в SEL об исправимой ошибке с указанием модуля FBDIMM	Светодиод «Сбой DIMM»: Не включен. Индикатор сбоя системы Не включен.	Нет	Система продолжает работать нормально.
Штатный режим: Конфигурация = Резервирование Исправимые ошибки >= Пороговое значение	Нет, поскольку BIOS не сохраняет информацию о состоянии памяти между перезагрузками.	Сообщение в SEL об исправимой ошибке с указанием модуля FBDIMM Сообщение в SEL о достижении порога ошибок с указанием модуля FBDIMM. Остановка протоколирования исправимых ошибок	Светодиод «Сбой DIMM»: Включены в синхронном режиме для сбойной пары FBDIMM. В одноканальном режиме включен для сбойного FBDIMM. Индикатор сбоя системы Зеленый / мигает:	Сбой = ДА Отключено = ДА Резервирование = Резервирование 1 / 0 Избыточность RAS С избыточностью / Без избыточности	Система продолжает работать нормально. Система переходит в режим без избыточности. BIOS скрывает все исправимые ошибки памяти.
Штатный режим: Конфигурация = Резервирование Состояние: Без избыточности (Post-SFO) UE	Нет, поскольку BIOS не сохраняет информацию о состоянии памяти между перезагрузками.	Сообщение в SEL о неисправимой ошибке с указанием модуля FBDIMM	Светодиод «Сбой DIMM»: В двухканальном режиме включены для пары FBDIMM, иначе для одного FBDIMM. Индикатор сбоя системы Янтарный / включен.	Сбой = ДА	В системе происходит NMI.

Сценарий	Сообщение POST	SEL	Состояние индикатора	Обновлено состояние памяти интерфейса IPMI	Работа системы
Штатный режим: Конфигурация = Резервирование Состояние: С избыточностью (Pre-SFO) UE	Нет, поскольку BIOS не сохраняет информацию о состоянии памяти между перезагрузками.	Сообщение в SEL о неисправимой ошибке с указанием модуля FBDIMM	Светодиод «Сбой DIMM»: В двухканальном режиме включены для пары FBDIMM. Иначе включен для одного FBDIMM. Индикатор сбоя системы Янтарный / включен.	Сбой = ДА	В системе происходит NMI.
Штатный режим: Конфигурация = MIR Состояние: С избыточностью Исправимые ошибки >= Пороговое значение	Нет, поскольку BIOS не сохраняет информацию о состоянии памяти между перезагрузками.	Сообщение в SEL об исправимой ошибке с указанием модуля FBDIMM Сообщение в SEL о достижении порогового значения для исправимых ошибок с указанием FBDIMM	Светодиод «Сбой DIMM»: Включено для сбойной пары. Светодиод системного сбоя: Зеленый / мигает	Сбой = ДА Отключено = НЕТ	Операционная система продолжает работать нормально. BIOS скрывает все исправимые ошибки.
Штатный режим: Конфигурация = MIR, и текущее состояние: С избыточностью UE	Нет, поскольку BIOS не сохраняет информацию о состоянии памяти между перезагрузками.	Сообщение в SEL о неисправимой ошибке с указанием модуля FBDIMM	Светодиод «Сбой DIMM»: Включено для сбойной пары FBDIMM. Индикатор сбоя системы Зеленый / мигает	Сбой = ДА Отключено = ДА для всех FBDIMM сбойной группы	В системе происходит NMI.

3.4 Управление платформой

На этой серверной платформе используются встроенные средства управления платформой, автоматически настраивающие производительность и уровень шума.



Система управления платформой оптимизирует производительность и акустические характеристики благодаря следующим возможностям:

- Управление производительностью
- Регулировка нагрузки
- Мониторинг температуры
- Управление скоростью вентиляторов
- Управление уровнем шума

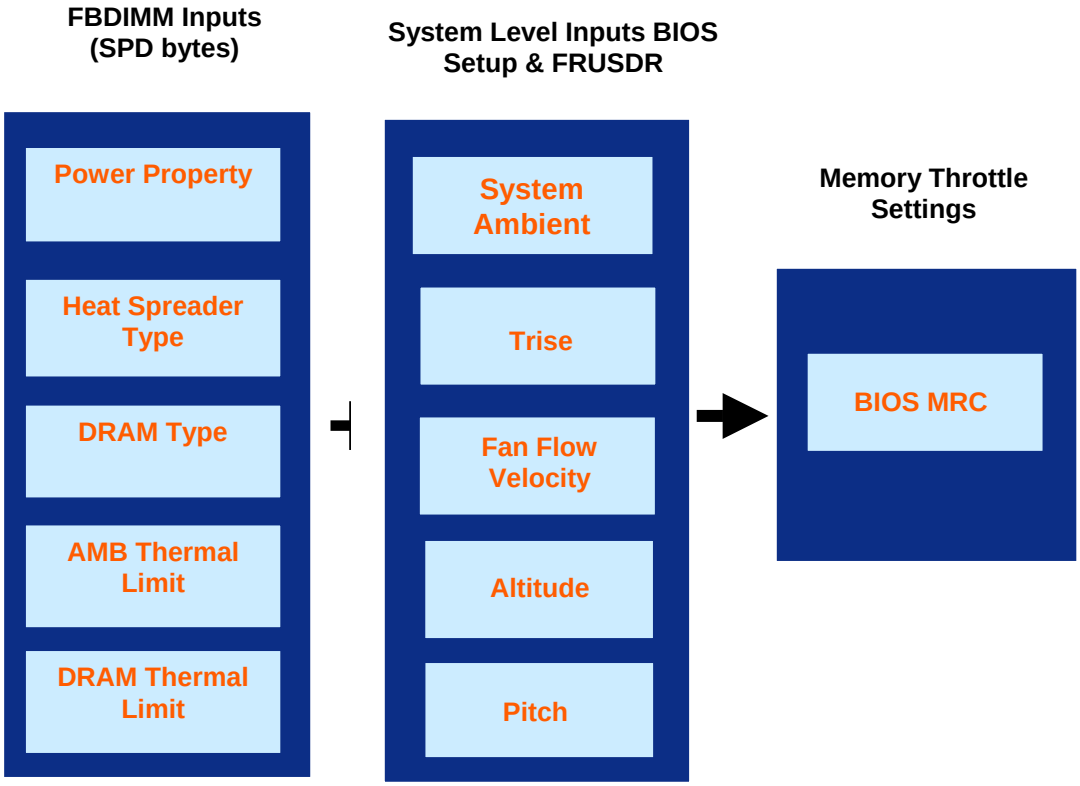
Для управления платформой служат следующие компоненты:

- Контроллер BMC в блоке контроллеров ESB-2
- Микросхема опроса датчиков LM94
- Датчики платформы
- Системные вентиляторы с изменяемой скоростью
- BIOS
- Встроенное ПО контроллера системной платы
- Записи данных датчиков (SDR), загружаемые FRUSDR
- Тип FBDIMM
- Тип процессора

3.4.1 Оптимизация пропускной способности FBDIMM

Регулировка нагрузки на память – непременный атрибут набора микросхем Intel серии 5000, защищающий модули памяти FBDIMM от перегрева. Если при работе установленные модули FB-DIMM разогреваются до заданного для этой платформы температурного лимита, BIOS системы включит управление нагрузкой на память за счет ограничения пропускной способности модулей DIMM, сокращая расход энергии и защищая модули DIMM от перегрева. Управление нагрузкой на память можно свести к минимуму, установив режим «Высокая производительность» (выбран по умолчанию), при этом меняется режим работы вентиляторов – они вращаются с большей скоростью. При запуске платформы в «Малошумном режиме» вентиляторы будут вращаться медленнее, не превышая пределов шума, заданных для этой платформы.

В BIOS используется алгоритм MRC для максимального увеличения пропускной способности памяти при применении оптимизации. Алгоритм MRC использует данные SPD модулей DIMM и данные системного уровня из BIOS и FRUSDR.



3.4.2 Управление скоростью вентиляторов

Скорость вентилятора определяется контроллером BMC в блоке контроллеров ESB-2. При нормальной работе системы контроллер BMC получает информацию из BIOS и отслеживает датчики платформы для определения скорости вентилятора.

Для управления скоростью вентиляторов в контроллер BMC необходимо запрограммировать данные о платформе. Данные о платформы программируются с помощью FRUSDR во время системной интеграции и с помощью BIOS во время работы.

3.4.2.1 Настройка системы с помощью FRUSDR

Программа обновления записей FRUSDR используется для записи данных о конфигурации платформы во встроенную память серверной платы. С помощью этой программы пользователь может выбрать поддерживаемый корпус (Intel или не Intel) и платформу. Основываясь на имеющихся данных, FRUSDR записывает данные датчиков в память NVRAM, и контроллер BMC считывает их при каждом включении системы.

3.4.2.2 Управление скоростью вентиляторов на основании данных BMC и BIOS

Используя данные, запрограммированные в NVRAM с помощью программы FRUSDR, контроллер BMC настроен для мониторинга и управления датчиками и вентиляторами платформы при каждом включении системы. После включения системы контроллер BMC использует дополнительные данные BIOS для определения способа управления вентиляторами.

BIOS передает данные BMC, указывая необходимый режим работы вентиляторов, т.е. бесшумный режим или производительный режим. BIOS использует параметры температурных датчиков SDR, настройки профиля вентиляторов в программе BIOS Setup, а также настройки высоты в BIOS Setup для настройки оптимизации системной памяти и управления скоростью вентиляторов. Если BIOS не может получить данные температурных датчиков SDR, для оптимизации памяти используются стандартные настройки MRC.

Программа <F2> BIOS Setup позволяет устанавливать профиль вентиляторов и режим работы платформы. Для каждого режима работы существует соответствующий профиль, определяющий то, как работают вентиляторы для выполнения поставленных задач. Задачи профилей зависят от типа платформы, выбранного в FRUSDR и <F2> BIOS Setup.

3.4.2.3 Настройка профиля вентилятора в программе BIOS Setup

BIOS использует опции, установленные в программе <F2> BIOS Setup, чтобы определить, какой профиль вентиляторов следует использовать в системе. Для этого служат опции «SET FAN PROFILE» и «ALTITUDE».

Опция «SET FAN PROFILE» может иметь значения «Performance» (по умолчанию) или «Acoustics». Подробное описание различий этих режимов приведено в разделах ниже. Использование акустического режима (Acoustics) может отрицательно повлиять на производительность системы.

Опция «ALTITUDE» определяет настройки производительности памяти, зависящие от различий охлаждающей способности на разных высотах. При большой высоте над уровнем моря производительность памяти необходимо уменьшать из-за разреженности воздуха. Если установить для опции Altitude неверное значение, вентиляторы могут не обеспечить достаточное охлаждение памяти. Если воздушный поток недостаточно охлаждает сервер даже при оптимизации, система может отключиться из-за перегрева.

По умолчанию для опции Altitude установлено значение 301 – 900 метров, которое соответствует большинству рабочих высот для этих серверных платформ.

На схемах ниже показано меню программы BIOS Setup, используемое для настройки требуемого профиля вентилятора.

Пункт настроек	Опция	Текст справки	Комментарий
Установка профиля вентилятора	**Производительность** Акустические характеристики	Выбирает профиль вентилятора для охлаждения системы.	В производительном режиме для охлаждения используются вентиляторы, а пропускная способность памяти не уменьшается.
Высота над уровнем моря	300 М или меньше **301 М – 900 М** Более 900 М	300 М или меньше (<= 980 футов): Оптимальная производительность для серверов, используемых на уровне моря. 301 М – 900 М (980 футов – 2950 футов): Оптимальная производительность для серверов, используемых на средней высоте над уровнем моря. Более 900 М (>2950 футов): Оптимальная производительность для серверов, используемых на большой высоте над уровнем моря.	

***Примечание**: Управление скоростью вентиляторов в корпусах сторонних производителей, установленных в FRUSDR, поддерживается только для вентиляторов процессоров. Контроллеру BMC требуются данные температурных датчиков процессора, чтобы определить необходимую скорость вентиляторов. Остальные вентиляторы системы работают с максимальной скоростью в связи с тем, что переменные для корпусов сторонних производителей и их вентиляторов неизвестны. Таким образом, вне зависимости от того, какой режим установлен для системы, вентиляторы корпуса будут работать с максимальной скоростью все время. В такой конфигурации настройка режима влияет только на производительность памяти (в производительном режиме она выше).*

3.4.2.4 Производительный режим (по умолчанию)

При работе в производительном режиме (по умолчанию), определенные переменные алгоритма управления платформой позволяют увеличивать максимальную производительность системы. При этом скорость вентиляторов программируется более высокой даже при низких температурах рабочей среды. В результате уровень шума платформы увеличивается, однако более активное охлаждение значительно снижает возможность уменьшения пропускной способности памяти и частоту изменения скорости вентиляторов в зависимости от загрузки процессора.

3.4.2.5 Акустический режим

При работе в акустическом режиме, определенные переменные алгоритма управления платформой позволяют устанавливать определенные акустические характеристики платформы. В этом режиме вентиляторы платформы работают на низкой скорости, если процессору не требуется дополнительное охлаждение из-за высокой нагрузки. Оптимизация памяти будет использоваться для обеспечения соблюдений температурных требований.

3.5 Флэш-память

BIOS поддерживает флэш-память Intel® 28F320C3. Эта флэш-память представляет собой модуль флэш-памяти емкостью 4 МБ, 2 МБ из которых могут быть перепрограммированы. Флэш-память содержит процедуры инициализации системы, утилиту BIOS Setup и процедуры поддержки выполнения команд. Точная схема может быть изменена по усмотрению корпорации Intel. Отдельный блок размером 128 КБ выделен для хранения пользовательского кода или индивидуальных заставок.

3.6 Пользовательский интерфейс BIOS

3.6.1 Логотип / Экран диагностики

Экран диагностики/логотипа может иметь одну из двух форм: Если в программе настройки BIOS включен показ логотипа, то логотип появится на экране в качестве заставки. По умолчанию этот параметр включен. Если логотип появляется во время POST, то можно нажать клавишу <Esc> – логотип скроется и появится экран диагностики.

Если во флэш-памяти отсутствует логотип, или если в системной конфигурации отключен режим Display Logo, на экране выводится диагностическая инфомрация.

Экран диагностики содержит следующую информацию:

- BIOS ID. См. Раздел 3.1
- Название системы
- Вся обнаруженная память (общий объем всех установленных модулей FBDIMM)
- Информация о процессоре (фирменная строка Intel, скорость и количество обнаруженных физических процессоров)
- Банк, из которого загружается система
- Типы обнаруженных клавиатур, если есть (подключенных через порт PS/2* и/или USB)
- Устройства «мышь», если есть (подключенные через порт PS/2 и/или USB)

3.7 Утилита BIOS Setup

Программа настройки BIOS работает в текстовом режиме и позволяет пользователю конфигурировать систему и просматривать информацию об оборудовании и текущих настройках платформы. Программа настройки BIOS управляет встроенным оборудованием платформы.

Интерфейс программы настройки BIOS состоит из нескольких страниц, или экранов. Каждая страница содержит информацию или ссылки на другие страницы. На первой странице в программе настройки BIOS – перечень основных категорий, оформленный в виде ссылок на них. Эти ссылки ведут на страницы со специальной информацией о конфигурациях категории.

Следующие разделы описывают вид и поведение программы настройки BIOS.

3.7.1 Работа

Отличительные особенности программа настройки BIOS:

- Локализация Программа настройки BIOS использует стандарт Unicode и может отображать страницы загрузки параметров на любом языке, включенном в стандарт Unicode. Однако BIOS серверной системной платы от Intel доступен только на английском языке.
- Программа настройки BIOS может работать с перенаправлением консольного ввода-вывода для различных стандартов эмуляции терминала. Для обеспечения совместимости эмуляторы терминалов могут ограничить некоторые возможности, например, использование цветов, некоторых клавиш или последовательностей клавиш, или поддержку устройств управления.

3.7.1.1 Устройство страницы настройки

Страница программы настройки BIOS подразделяется на функциональные области. Каждая отображается в своей части экрана и имеет отдельное назначение. Следующие рисунок и таблица перечисляют и описывают все функциональные области.

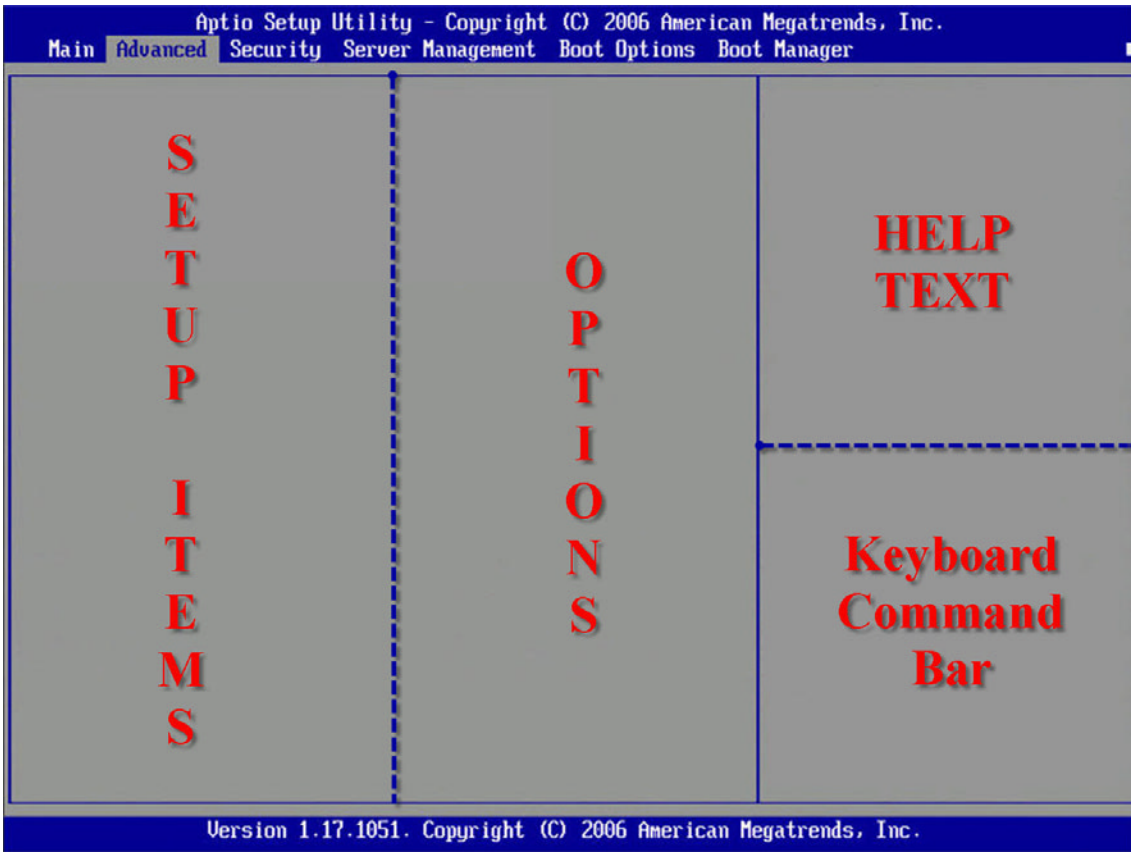


Рисунок 5. Общий вид экрана BIOS

Таблица 13. Устройство страницы настройки BIOS

Функциональная область	Описание
Строка заголовка	Заголовок расположен вверху экрана и содержит название страницы, открытой пользователем в данный момент. Он может также содержать информацию для навигации по странице.
Список пунктов настроек	Список пунктов настроек – это набор управляемых и информационных элементов. Каждый пункт списка занимает левые и центральные колонки в середине экрана. Левая колонка, пункт настройки, отображает предмет настройки. Средняя колонка, дополнительная, содержит информацию или варианты выбора объекта. Пункт настройки может быть гиперссылкой, которая используется для навигации по страницам. Если на экране представлена гиперссылка, то пункт настройки отображается только в части экрана, относящейся к пункту настройки.
Окно информации об элементе	Окно информации об элементе находится в правой части экрана и содержит пояснительные тексты о выделенных пунктах настройки. Дополнительная информация – это назначение и использование элемента, доступные значения, результаты настройки и т.д.
Панель команд с клавиатуры	Информационная панель клавиатуры справа внизу экрана постоянно высвечивает напоминание о специальных клавишах и клавишах навигации. Информационная панель клавиатуры зависит от контекста – она показывает клавиши в зависимости от страницы и режима.
Строка состояния	Строка состояния – это самая нижняя строка на экране. Эта строчка отображает BIOS ID.

3.7.1.2 Вход в утилиту BIOS Setup

Программа настройки BIOS запускается нажатием клавиши <F2> во время загрузки системы, когда на экране высвечивается логотип производителя оборудования или корпорации Intel.

Когда логотип гаснет, на экране появляется следующее сообщение: «press <F2> to enter setup».

3.7.1.3 Команды с клавиатуры

Внизу справа экрана программы настройки BIOS приводится список команд, которыми можно пользоваться при настройке. Эти команды отображаются во всех случаях.

Каждая страница меню содержит ряд элементов. Каждый элемент, кроме информационных, соответствует некоторому настраиваемому полю. В этом поле содержатся параметры, значение которых может задавать пользователь. В зависимости от выбранных параметров безопасности и наличия/отсутствия пароля, параметры элементов могут быть изменяемыми или неизменяемыми. Если их значения неизменяемы, поле для ввода значений элемента недоступно. Оно становится «серым».

На панели команд с клавиатуры содержатся следующие команды:

Таблица 14. BIOS Setup: Панель команд с клавиатуры

Ключ	Option	Описание
<Enter>	Execute Command	Клавиша <Enter> используется для активации подменю если выбранная позиция является подменю или для отображения списка опций если для выбранной позиции существует список опций или для открытия поля ввода данных для таких функций, как время и дата. Если список элементов для выбора доступен, можно выбрать требуемый элемент при помощи клавиши <Enter>, затем покинуть список и вернуться к главному меню.
<Esc>	Exit	Клавиша <Esc> используется для выхода из любого поля. Эта клавиша отменяет нажатие клавиши Enter. При нажатии клавиши <Esc> во время редактирования любого поля или выбора позиции из списка, происходит возврат в меню. При нажатии клавиши <Esc> в любом подменю происходит возврат в родительское меню. При нажатии клавиши <Esc> в любом основном меню появляется окно подтверждения выхода и пользователю будет предложено сохранить изменения. При выборе «No» и нажатии <Enter> или при нажатии клавиши <Esc> пользователь возвращается в меню, открытое до нажатия клавиши <Esc> без изменений настроек. Если вы выбрали «Да» и нажали клавишу <Enter>, настройка завершается и BIOS вновь высвечивает на экране главное меню системы.
↑	Select Item	Стрелка вверх используется для выбора предыдущего значения списка значений или предыдущей опции списка опций меню. После этого выбранная позиция должна быть активирована нажатием клавиши <Enter>.
↓	Select Item	Стрелка вниз используется для выбора следующего значения в списке опций меню или списке значений. После этого выбранная позиция должна быть активирована нажатием клавиши <Enter>.
↔	Выбор пункта меню	Стрелки влево и вправо используются для перемещения между пунктами главного меню. Нажатие этих клавиш не влияет на подменю или список выбора.
<Tab>	Select Field	Клавиша <Tab> используется для перемещения между полями. Например, клавиша <Tab> может использоваться для перемещения с поля часов в поле минут в главном меню.
-	Change Value	Клавиша минус на цифровой клавиатуре используются для изменения значений текущей позиции на предыдущее значение. Эта клавиша позволяет менять значения списка без открытия всего списка.
+	Change Value	Клавиша плюс на цифровой клавиатуре используются для изменения значений текущей позиции на следующее значение. Эта клавиша позволяет менять значения списка без открытия всего списка. На 106-клавишных клавиатурах с японской раскладкой клавиша плюс имеет код сканирования, отличный от клавиши плюс на других клавиатурах, но ее нажатие производит то же воздействие.

Ключ	Option	Описание
<F9>	Setup Defaults	При нажатии клавиши <F9> появляется следующее сообщение: Загрузить оптимизированные настройки? (Да/Нет) При нажатии «Да» (<Y>), все поля будут заполнены значениями, принятыми по умолчанию. При нажатии «Нет» (<N>) или <Esc>, программа вернется к состоянию, в котором находилась до нажатия <F9> без каких-либо изменений в значениях полей элементов.
<F10>	Save and Exit	После нажатия клавиши <F10> появится следующее сообщение: Сохранить настройки и перезагрузиться? (Да/Нет) При нажатии «Да» (<Y>), все изменения будут сохранены, и установка завершится. При нажатии «Нет» (<N>) или <Esc> программа вернется к состоянию, в котором находилась до нажатия клавиши <F10>, без внесения каких-либо изменений.

3.7.1.4 Панель выбора меню

Панель выбора меню расположена в верхней части экрана. Здесь отображены основные пункты меню.

3.7.2 Экран настроек платформы сервера

Следующие разделы описывают экраны, отображающие настройки платформы сервера. В этих разделах, таблицах и цифрах описано содержание каждого экрана. Эти таблицы и рисунки соответствуют следующим правилам:

- Текст и значения колонок «Пункты настроек» «Параметры» и «Помощь» выводятся на экраны установки BIOS.
- Текст, выделенный полужирным шрифтом в колонке «Параметры», описывает настройки по умолчанию. Эти же значения на экране установки полужирным шрифтом не выделяются.
- Текст в колонке «Параметры» отображает доступные варианты значений.
- В колонке «Комментарии» приводится дополнительная информация, которая может оказаться полезной. Эта информация не отображается на экранах установки.
- Если текст заключен в угловые скобки (< >), он может меняться, в зависимости от включенных параметров. Например, <Текущая дата > заменяется на текущую дату.
- Информация в фигурных скобках ({ }) обозначает поля, в которые пользователь должен ввести текст, а не выбирать одно из доступных значений.

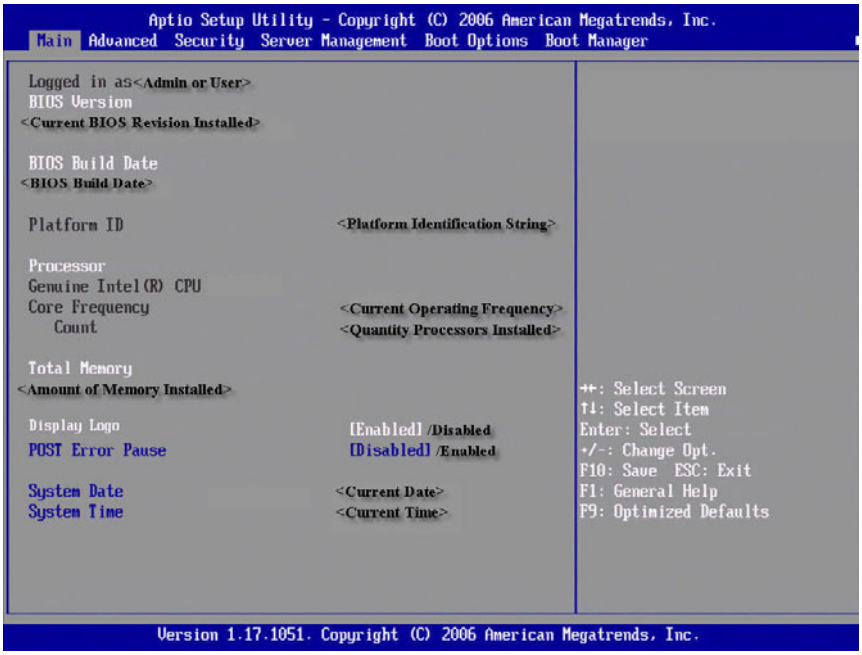


Рисунок 6. Программа установки – вид основного экрана

Таблица 15. Программа установки – поля основного экрана

Пункт настроек	Опции	Текст справки	Комментарии
Версия BIOS	Ввод запрещен		Только информация. Обозначает версию BIOS. ▪ yy = основной номер версии ▪ xx = дополнительный номер версии ▪ zzzz = номер сборки
Дата сборки BIOS	Ввод запрещен		Только информация. Отображает дату сборки BIOS.
ID системы	Ввод запрещен		Только информация. Отображает ID системы. (например: S5000XVN, S5000VSA или S5000PAL)
Процессор			
Тип	Ввод запрещен		Только информация. Обозначает скорость и название процессора Intel.
Тактовая частота ядра	Ввод запрещен		Только информация. Обозначает текущую скорость процессора в гигагерцах или мегагерцах

Пункт настроек	Опции	Текст справки	Комментарии
Счет	Ввод запрещен		Только информация. Количество обнаруженных процессоров.
Общий объем памяти	Ввод запрещен		Только информация. Отображает всю физическую память системы в мегабайтах или гигабайтах. Термин «физическая память» обозначает весь обнаруженный объем памяти в имеющихся модулях FBDIMM.
Отображение логотипа	**Включено** Отключено	Если включено, показывается заставка BIOS. Если выключено, отображаются сообщения BIOS POST.	
POST Error Pause	Включено **Отключено**	При выборе значения «enabled» система ожидает действий пользователя при обнаружении критических ошибок POST. При выборе значения «disabled» система производит загрузку автоматически, если это возможно.	Пауза для POST дает время менеджеру ошибок обнаружить ошибки.
Системная дата	[MM/DD/YYYY]	Значение месяца от 1 до 12. Значение дня от 1 до 31. Значение года от 1998 до 2099.	Дополнительный текст зависит от того, какое субполе выбрано (месяц, день или год).
Системное время	[HH:MM:SS]	Значение часа от 0 до 23. Значения минут от 0 до 59. Значения секунд от 0 до 59.	Дополнительный текст зависит от того, какое субполе выбрано (часы, минуты, секунды).

3.7.2.1 Экран «Дополнительные возможности» (Advanced)

Экран «Дополнительные возможности» предоставляет доступ к настройке нескольких параметров. На этом экране пользователь выбирает параметр, который должен быть настроен. Настройки выполняются на выбранном экране, а не на экране «Дополнительные возможности».

Для доступа к экрану «Дополнительные возможности» из основного экрана следует нажимать стрелку вправо, до тех пор пока не будет выбран экран «Дополнительные возможности».

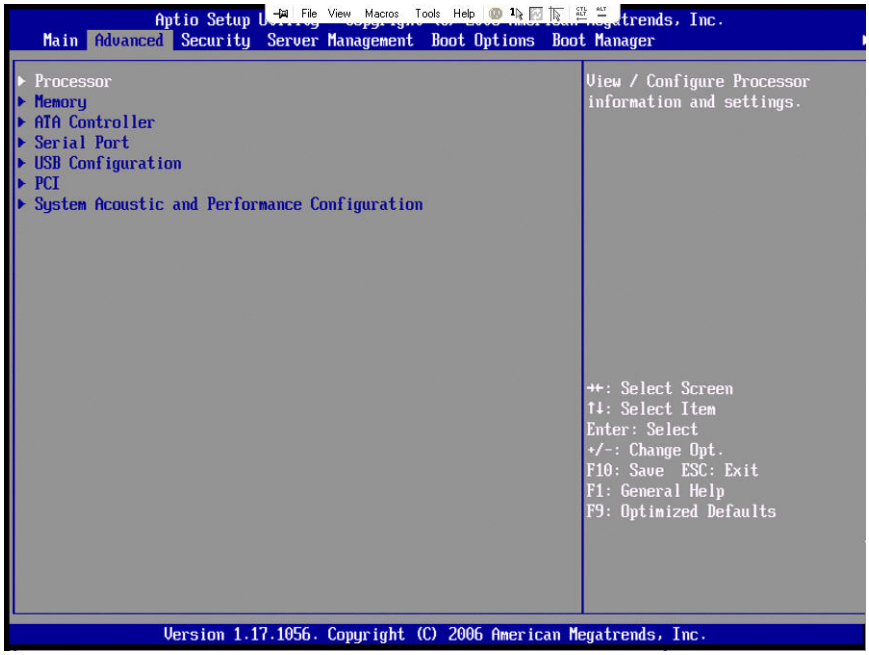


Рисунок 7. Программа настройки – вид экрана «Дополнительные возможности»

3.7.2.1.1 Экран «Процессор» (Processor)

Экран «Процессор» предоставляет пользователю возможность узнать частоту ядра процессора, частоту системной шины, а также включить или выключить некоторые параметры, связанные с процессором. Пользователь также может посмотреть информацию о выбранном процессоре.

Для доступа к этому экрану из основного экрана выберите «Дополнительные возможности» | «Процессор» (Advanced | Processor).

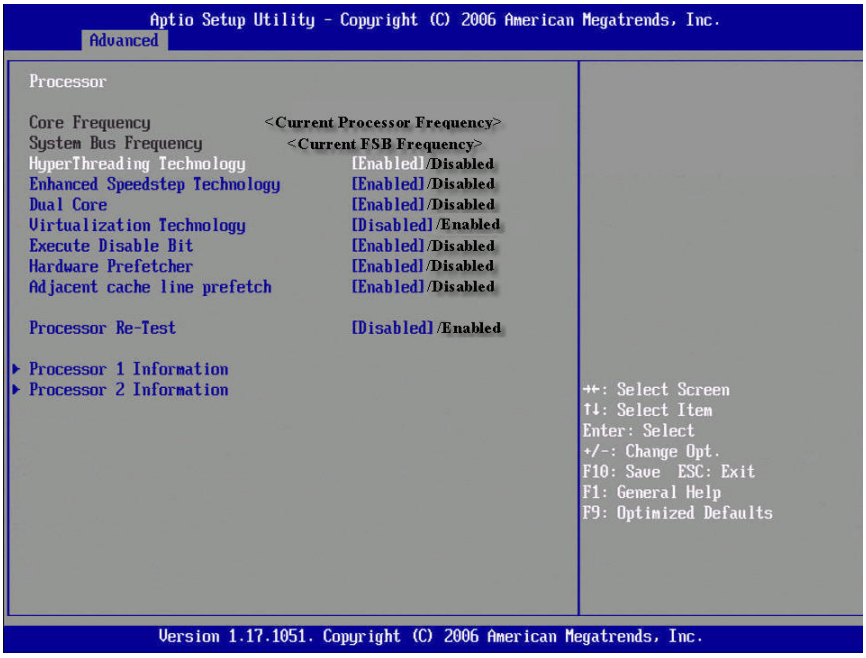


Рисунок 8. Программа настройки – вид экрана «Процессор»

Таблица 16. Программа настройки – поля экрана «Процессор»

Пункт настроек	Опции	Текст справки	Комментарии
Тактовая частота ядра	Ввод запрещен	Частота, на которой работают процессоры.	Только информация.
Частота системной шины	Ввод запрещен	Текущая частота системной шины процессора.	Только информация.
Технология HyperThreading	**Включено** Отключено	Включение и выключение технологии Hyper-Threading на процессорах.	Этот параметр автоматически выключается, когда выключен двухъядерный режим.
Технология Enhanced SpeedStep	**Включено** Отключено	Включение и выключение технологии Enhanced Intel SpeedStep® на процессорах.	
Двухъядерный	**Включено** Отключено	Включение и выключение второго ядра процессора (Ядро 1). Если выключено, технология Hyper-Threading автоматически выключается.	
Технология Virtualization	Включено **Отключено**	Если опция включена, Virtual Machine Monitor может использовать дополнительные возможности оборудования, обеспечиваемые технологией Intel® Virtualization Technology	
Технология Execute Disable Bit	**Включено** Отключено	Если опция отключена, значение флага активации XD-функции всегда возвращается равным нулю	
Hardware Prefetcher (аппаратная предвыборка)	**Включено** Отключено	Разрешает или запрещает использование функции аппаратной предвыборки	
Adjacent Cache Line Prefetch (предвыборка смежных строк кэш-памяти)	**Включено** Отключено	Разрешает или запрещает использование предвыборки смежных строк данных кэш-памяти	
Processor 1 Information (информация о первом процессоре)			Выберите, чтобы просмотреть сведения о первом процессоре. При этом осуществляется переход к другому экрану.
Processor 2 Information (информация о первом процессоре)			Выберите, чтобы просмотреть сведения о втором процессоре. При этом осуществляется переход к другому экрану.

3.7.2.1.1.1 Processor # Information Screen (экран «Processor # Information»)

В экране «Processor # Information» приводятся сведения о конкретном процессоре.

Для перехода в этот экран из экрана «Main» необходимо выбрать Advanced | Processor | Processor # Information, где символ «#» обозначает номер процессора, сведения о котором необходимо получить.

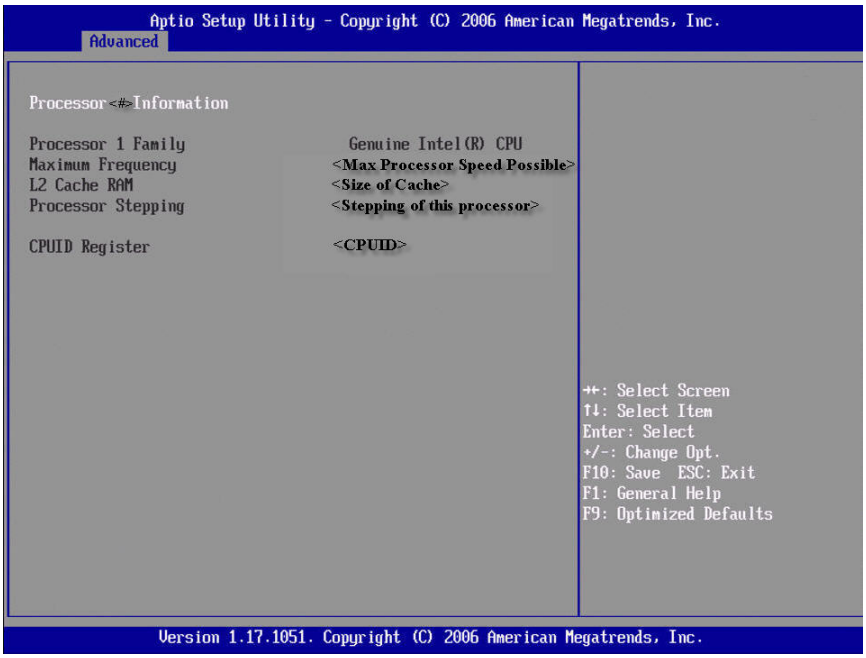


Рисунок 9. Программа настройки – Вид экрана «Specific Processor Information»

Таблица 17. Программа настройки – Поля экрана «Specific Processor Information»

Пункт настроек	Опции	Текст справки	Комментарии
Семейство процессоров	Ввод запрещен	Идентифицирует семейство или поколение процессора	Только информация.
Maximum Frequency (максимальная тактовая частота)	Ввод запрещен	Максимальная тактовая частота, поддерживаемая ядром процессора.	Только информация.
Объем кэш-памяти второго уровня	Ввод запрещен	Size of the processor cache (размер кэш-памяти процессора).	Только информация.
Степпинг процессора	Ввод запрещен	Stepping number of the processor (номер модификации процессора).	Только информация.
CPUID Register (регистр CPUID)	Ввод запрещен	В регистре CPUID содержится детальная информация о семействе, модели и модификации процессора.	Только информация.

3.7.2.1.2 Memory Screen (экран «Memory»)

В экране «Memory» приводятся сведения об установленных системных модулях памяти FBDIMM. В этом экране пользователь может выбрать опцию перехода к экрану «Configure Memory RAS Performance».

Для перехода к экрану «Memory» из экрана «Main» необходимо выбрать Advanced | Memory.

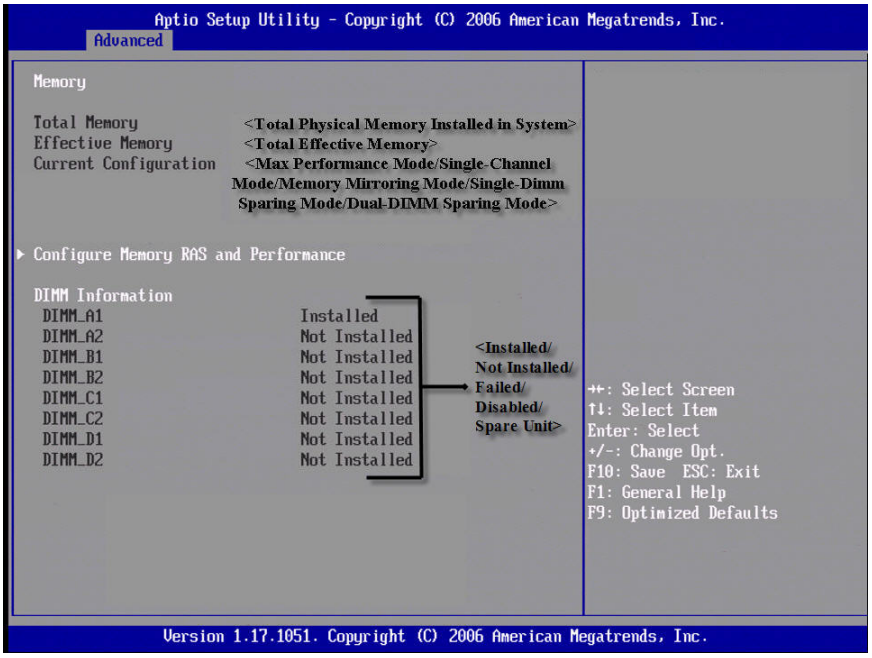


Рисунок 10. Программа настройки – Вид экрана «Memory Configuration»

Таблица 18. Программа настройки – Поля экрана «Memory Configuration»

Пункт настроек	Опции	Текст справки	Комментарии
Общий объем памяти	Ввод запрещен		Только информация. Общий объем памяти установленных в системе модулей FBDIMM, выраженный в МБ или ГБ.
Effective Memory (эффективная память)	Ввод запрещен		Только информация. Объем доступной для операционной системы памяти, выраженный в МБ или ГБ. Эффективная память это разность между общим объемом памяти системы и объемом памяти, зарезервированной для внутреннего использования, обеспечения RAS-резервирования и размещения данных SMRAM. Кроме того, при определении объема эффективной памяти учитывается суммарная емкость модулей FBDIMM, неуспешно выполнивших тест BIST процедуры POST или отключенных BIOS на фазе обнаружения памяти с целью обеспечения оптимальной конфигурации памяти.
Current Configuration (текущая конфигурация)	Ввод запрещен		Только информация. Выводится одно из следующих сообщений: ▪ Режим максимальной производительности: Системная память сконфигурирована для обеспечения оптимальной производительности и эффективности; режим RAS отключен. ▪ Single-channel Mode (одноканальный режим): Системная память функционирует в специальном режиме с пониженной эффективностью. Режим зеркалирования памяти: Системная память сконфигурирована для режима максимальной надежности, обеспечиваемого зеркальным копированием данных. ▪ Single-DIMM Sparing Mode (Режим с одним резервным модулем DIMM): Системная память работает в режиме с резервированием, обеспечиваемым одним модулем FBDIMM. ▪ Dual-DIMM Sparing Mode (Режим с двумя резервными модулями DIMM): Системная память работает в режиме с резервированием, который обеспечивается двумя модулями FBDIMM, функционирующими как единый модуль.

Пункт настроек	Опции	Текст справки	Комментарии
Configure Memory RAS and Performance (настройка режима RAS и производительности системы)		Просмотр настроек текущего режима RAS (от Reliability Accessibility and Serviceability – надежность, доступность и эффективность) и выбор характеристик памяти для улучшения/ручной настройки производительности системы.	Выберите, чтобы перейти к настройке режима RAS и производительности системы. При этом осуществляется переход к другому экрану.
DIMM #	Ввод запрещен		Выводит сведения о статусе всех имеющихся на плате разъемов DIMM. Поле каждого разъема DIMM отражает одно из следующих состояний разъема: ▪ **Установлен:** В данном разъеме установлен модуль FBDIMM. ▪ **Не установлен:** Модуль FBDIMM в данном разъеме отсутствует. ▪ **Сбой:** Модуль FBDIMM, установленный в данном разъеме, неисправен. ▪ **Отключено:** Модуль FBDIMM, установленный в данном разъеме, отключен BIOS в целях обеспечения оптимальной конфигурации памяти. ▪ **Spare Unit (элемент резервирования):** Модуль FBDIMM выполняет функцию резервного элемента для обеспечения работы памяти в режиме RAS.

3.7.2.1.3 Экран «ATA Controller»

Экран «IDE Controller» содержит поля данных для конфигурирования дисководов жестких дисков с интерфейсам PATA и SATA. Он также предоставляет информацию об установленных дисководах жестких дисков.

Для перехода к этому экрану из экрана «Main» следует выбрать Advanced | IDE Controller.

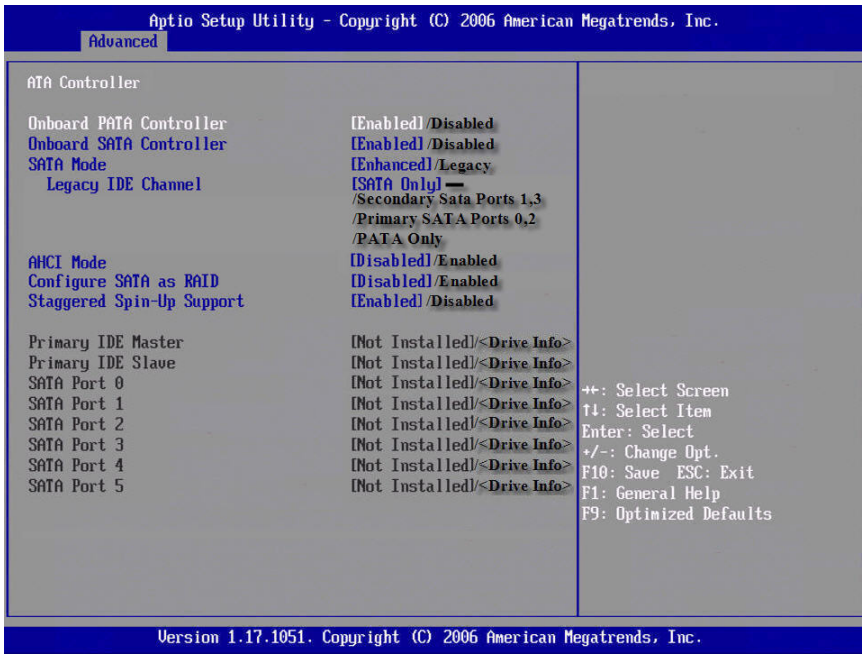


Рисунок 11. Программа настройки – Вид экрана «IDE Controller Configuration»

Таблица 19. Программа настройки – Поля экрана «IDE Controller Configuration»

Пункт настроек	Option	Текст справки	Комментарии
Onboard PATA Controller (встроенный контроллер PATA-интерфейса)	**Включено** Отключено	Справка: Onboard PATA Controller (встроенный контроллер PATA-интерфейса)	
Onboard SATA Controller (встроенный контроллер SATA-интерфейса)	**Включено** Отключено	Справка: Onboard SATA Controller (встроенный контроллер SATA-интерфейса)	Если опция включена, контроллер SATA может быть сконфигурирован для работы в режиме IDE, RAID или AHCI. Режимы RAID и AHCI взаимно исключают друг друга.
SATA Mode (режим SATA)	**Улучшение функций** Стандартные	Справка: SATA Mode (режим SATA)	В стандартном режиме BIOS поддерживает только четыре дисковода. Существует четыре варианта совместного использования дисководов с интерфейсами SATA и PATA в стандартном режиме (см. раздел Legacy IDE Channel ниже). В улучшенном режиме возможности BIOS не ограничиваются стандартной поддержкой четырех PATA-дисководов. Независимо от статуса AHCI-режима BIOS в этом случае поддерживает два PATA и четыре SATA-дисковода (всего шесть дисководов). При включенном режиме AHCI BIOS может работать еще с двумя SATA-дисководами. Режимы AHCI и RAID поддерживаются только в том случае, если для SATA-интерфейса установлен улучшенный режим работы («Enhanced»)

Пункт настроек	Option	Текст справки	Комментарии
Legacy IDE Channel (стандартный канал IDE)	**SATA только** Secondary SATA Ports 1, 3 (вторичные порты 1, 3 интерфейса SATA) Primary SATA Ports 0, 2 (первичные порты 0, 2 интерфейса SATA) PATA только		Присутствуют на экране только в случае, если для SATA-интерфейса установлен стандартный режим. Если выбран режим «SATA only», то четыре SATA-накопителя могут быть инициализированы в системе. Если установлен режим «PATA Only», только два IDE-дисковода могут быть инициализированы. Если выбрана опция «Secondary SATA Ports 1,3», то через PATA-интерфейс будет организован первичный канал, а порты 1 и 3 интерфейса SATA будут эмулировать вторичный канал «Master/Slave» ATA-интерфейса. Если выбрана опция «Primary SATA Ports 0,2», то SATA-порты 0, 2 и оба IDE-порта будут инициализированы в системе
AHCI Mode (режим AHCI)	Включено **Отключено**	Справка: AHCI Mode (режим AHCI)	Недоступен, если установлен стандартный режим SATA-интерфейса или выбран режим RAID. В AHCI-режиме информация о дисководах жестких дисков на экран не выводится, поскольку в этом режиме BIOS не выполняет идентификацию каких бы то ни было дисководов. Задача идентификации и конфигурации дисководов возложена на ПЗУ контроллера AHCI. В программе настройки BIOS информация о дисководах жестких дисков доступна не будет.
Configure SATA as RAID (настройка интерфейса SATA для работы в RAID-режиме)	Включено **Отключено**	Справка: Configure Intel® Embedded RAID Technology II (настройка использования технологии Intel® Embedded RAID Technology II)	Опция недоступна, если активен режим AHCI. Этот режим может быть выбран только в том случае, если контроллер SATA работает в улучшенном режиме.
Staggard Spin Up Support (поддержка Staggard Spin Up)	**Включено** Отключено	Справка: Staggard Spin Up Support (поддержка Staggard Spin Up)	Опция доступна только при активном AHCI-режиме

Пункт настроек	Option	Текст справки	Комментарии
Primary IDE Master	Disabled / Drive information (отключен / информация о диске)		Information only (только для информации)
Primary IDE Slave	Disabled / Drive information (отключен / информация о диске)		Information only (только для информации)
SATA 0	Disabled / Drive information (отключен / информация о диске)		Используется только для информации и недоступно при активном AHCI или RAID-режиме
SATA 1	Disabled / Drive information (отключен / информация о диске)		Это поле используется только для информации и недоступно при активном AHCI или RAID-режиме
SATA 2	Disabled / Drive information (отключен / информация о диске)		Это поле используется только для информации и недоступно при активном AHCI или RAID-режиме
SATA 3	Disabled / Drive information (отключен / информация о диске)		Это поле используется только для информации и недоступно при активном AHCI или RAID-режиме
SATA 4	Disabled / Drive information (отключен / информация о диске)		Это поле используется только для информации и недоступно при активном AHCI или RAID-режиме
SATA 5	Disabled / Drive information (отключен / информация о диске)		Это поле используется только для информации и недоступно при активном AHCI или RAID-режиме

3.7.2.1.4 Mass Storage Screen (экран «Mass Storage»)

Поля для настроек представлены в экране «Mass Storage» только в том случае, если объединительная плата, расположенная в средней или задней части вычислительной системы Intel®, содержит контроллер SAS.

Для перехода к этому экрану из экрана «Main» необходимо выбрать Advanced | Mass Storage.

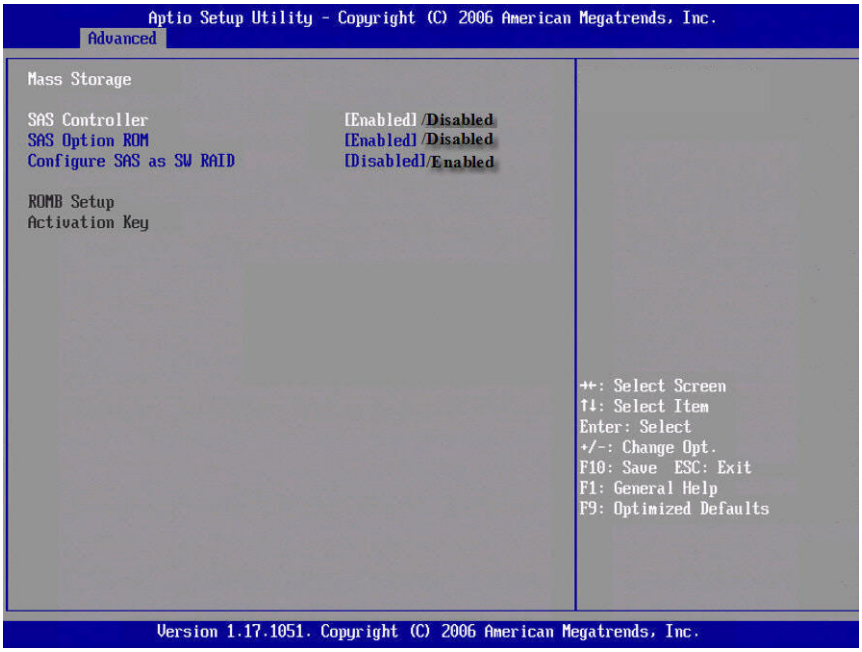


Рисунок 12. Программа настройки – Вид экрана «Mass Storage Configuration»

Таблица 20. Программа настройки – Поля экрана «Mass Storage Configuration»

Пункт настроек	Опции	Текст справки	Комментарии
Контроллер SAS	**Включено** Отключено	Включает или отключает контроллер SAS.	
SAS Option ROM (ПЗУ настроек SAS-контроллера)	**Включено** Отключено	При выборе значения Enabled производится инициализация дополнительного ПЗУ встроенного контроллера SCSI.	Опция недоступна, если устройство отключено или опция ROMB активна.
Enable Intel® SROMBSAS18E (использовать контроллер Intel® SROMBSAS18E)	Включено **Отключено**	Если опция активна, инициализируется контроллер ROMB (RAID On MotherBoard).	Опция недоступна, если отсутствует ключ активации Intel® RAID Key . **ОСТОРОЖНО:** Перед переключением режимов необходимо создать резервные копии данных массива и удалить существующие массивы. В противном случае возможна потеря всех данных. Перед активацией опции ROMB следует сделать резервные копии всех дисков. При переходе в режим RAID все данный на дисках будут утеряны. Для использования режима Intel® RAID On Motherboard необходимы ключ активации Intel® RAID Activation Key и специальный модуль памяти «DIMM for ROMB». Перед включением режима RAID необходимо убедиться в наличии ключа активации и модуля памяти «DIMM for ROMB». Для получения подробной информации о настройке RAID следует обратиться к документации на соответствующее оборудование.
Activation Key (ключ активации)			

3.7.2.1.5 Serial Ports Screen (экран «Serial Ports»)

В экране «Serial Ports» представлены поля для настройки портов Serial A (COM 1) и Serial B (COM2). Для перехода к этому экрану из экрана «Main» необходимо выбрать Advanced | Serial Port.

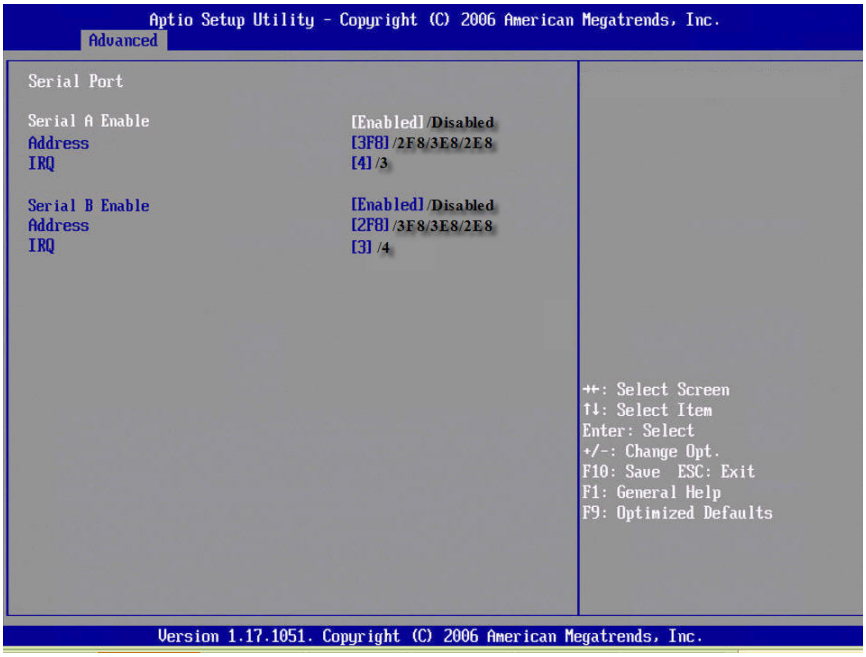


Рисунок 13. Программа настройки – Вид экрана «Serial Port Configuration»

Таблица 21. Программа настройки – Поля экрана «Serial Ports Configuration»

Пункт настроек	Опции	Текст справки	Комментарии
COM1 Enable (активация COM1)	**Включено** Отключено	Активирует или деактивирует порт COM1.	
Адрес	**3F8h** 2F8h 3E8h 2E8h	Выбор базового адреса диапазона ввода/вывода для порта COM1.	
IRQ	3 **4**	Выбор линии запроса прерывания для порта COM1.	
COM2 Enable (активация порта COM2)	**Включено** Отключено	Активирует или деактивирует порт COM1.	
Адрес	3F8h **2F8h** 3E8h 2E8h	Выбор базового адреса диапазона ввода/вывода для порта COM1.	
IRQ	**3** 4	Выбор линии запроса прерывания для порта COM1.	

3.7.2.1.6 USB Configuration Screen (Экран «USB Configuration»)

В экране «USB Configuration» представлены поля для настройки портов контроллера USB.

Для перехода к этому экрану из экрана «Main» необходимо выбрать Advanced | USB Configuration.

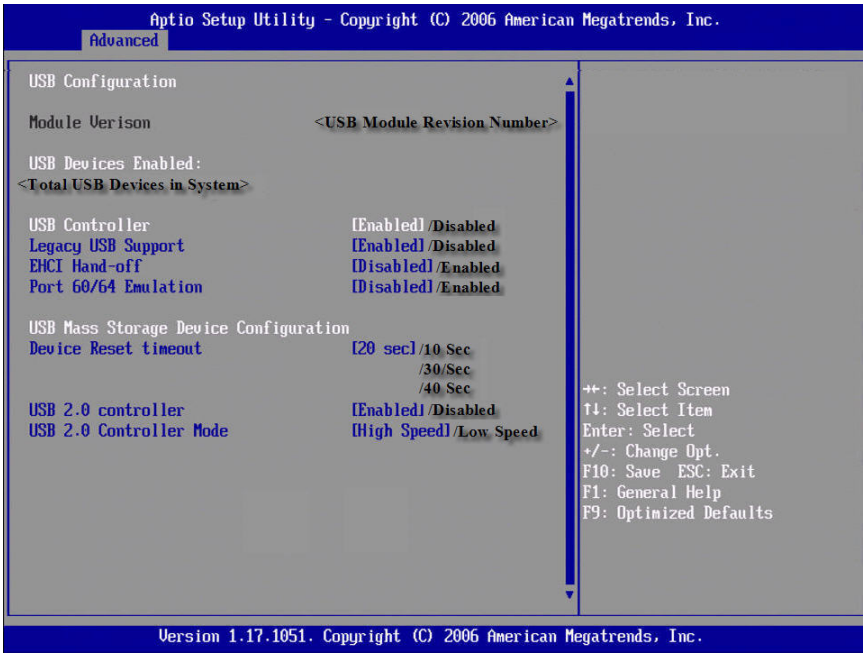


Рисунок 14. Программа настройки – Вид экрана «USB Controller Configuration»

Таблица 22. Программа настройки – Поля экрана «USB Controller Configuration»

Пункт настроек	Опции	Текст справки	Комментарии
Включены устройства с интерфейсом USB:		Выводит сведения о количестве USB-устройств в системе	Information only (только для информации)
USB контроллер	**Включено** Отключено	Если опция отключена, то все контроллеры USB блокируются и становятся недоступными для операционной системы.	
Поддержка стандартных разъемов USB	**Включено** Отключено Автоматически	Активирует стандартную поддержку USB-устройств. Опция AUTO отключает поддержку стандартных устройств с интерфейсом USB, если такие устройства не подключены.	
EHCI Hand-off	Включено **Отключено**	Если операционная система не поддерживает механизм, то включение этой опции позволяет обойти данное ограничение и использовать механизм EHCI Hand-off. Необходимость смены владельца контроллера EHCI определяется драйвером EHCI.	

Пункт настроек	Опции	Текст справки	Комментарии
Port 60/64 Emulation	Включено **Отключено**	Включает поддержку эмуляции порта 60/64h. Данная опция должна быть включена для полной клавиатурной поддержки стандартных устройств с интерфейсом USB для ОС, не поддерживающих USB.	
Hotplug USB floppy («Горячее» подключение USB-дисковода гибких дисков)	Включено Отключено **Автоматически**	Создается образ дисковода гибких дисков, который позднее может быть ассоциирован с физическим дисководом, подключенным во время работы системы. Образ дисковода создается автоматически при условии, что на момент создания USB-дисковод гибких дисков к системе не подключен.	
Device Reset Timeout (таймаут сброса устройства)	10 секунд **20 секунд** 30 секунд 40 секунд	Таймаут выполнения команды USB-накопителя Start Unit.	
USB 2.0 Controller	**Включено** Отключено	Если опция выключена, то все контроллеры USB 2.0 блокируются и становятся недоступны для операционной системы.	
USB 2.0 Controller Mode	**High Speed (высокоскоростной режим)** Low Speed (низкоскоростной режим)	Выберите режим работы контроллера USB 2.0: высокоскоростной или низкоскоростной.	

3.7.2.1.7 PCI Screen (экран «PCI»)

В экране «PCI» представлены поля для настройки PCI-карт расширений, встроенных контроллеров NIC, и видеоресурсов.

Для перехода к этому экрану из экрана «Main» необходимо выбрать Advanced | PCI.

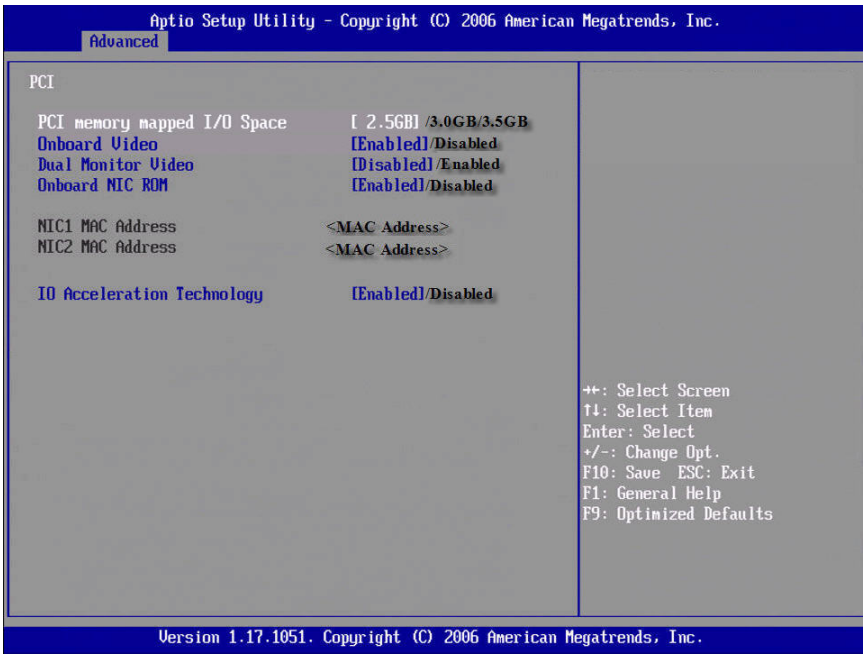


Рисунок 15. Программа настройки – Вид экрана «PCI Configuration»

Таблица 23. Программа настройки – Поля экрана «PCI Configuration»

Пункт настроек	Опции	Текст справки	Комментарии
PCI Memory Mapped I/O Space (отображаемый в память диапазон ввода/вывода устройств PCI)	**2.5 ГБ** 3.0 ГБ 3.5 ГБ	Если опция включена, диапазон адресов, используемый устройствами PCI, отображается в адресное пространство памяти выше 4 ГБ. При этом операционная система должна поддерживать использование памяти выше 4 ГБ.	
Интегрированный графический адаптер	**Включено** Отключено	Разрешает или запрещает использование встроенного видеоконтроллера. Для обеспечения работы двух мониторов опция должна быть включена	При отключенной опции и отсутствии в системе других видео-карт, получить видеоизображение на мониторе будет невозможно.
Поддержка двух мониторов	Включено **Отключено**	При включенной опции встроенный видеоконтроллер может работать совместно с контроллером видео-карты расширения. Встроенный видеоконтроллер будет являться первичным	
On-board NIC ROM (ПЗУ встроенного контроллера NIC)	**Включено** Отключено	Разрешает или запрещает использование ПЗУ контроллера сетевого интерфейса. Если опция отключена, то контроллеры NIC1 и NIC2 не могут быть использованы для загрузки системы	
NIC 1 MAC адрес	Ввод запрещен		Только информация. 12 шестнадцатеричных знаков MAC-адреса.
NIC 2 MAC адрес	Ввод запрещен		Только информация. 12 шестнадцатеричных знаков MAC-адреса.
IO Acceleration Tech	**Включено** Отключено	Разрешает или запрещает встроенным контроллерам NIC использование функции Intel® I/O Acceleration Technology.	

3.7.2.1.8 Акустическая и производительная конфигурации системы

В экране «System Acoustic and Performance Configuration» представлены поля для настройки температурного режима системы.

Для перехода к этому экрану из экрана «Main» необходимо выбрать Advanced | System Acoustic and Performance Configuration.

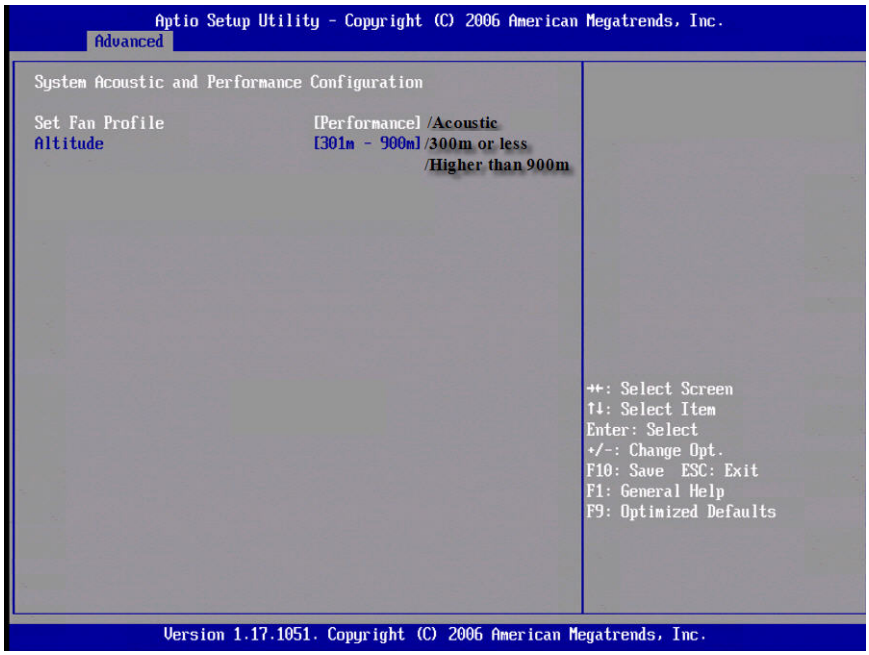


Рисунок 16. Программа настройки – Вид экрана «System Acoustic and Performance Configuration»

Таблица 24. Программа настройки – Поля экрана «System Acoustic and Performance Configuration»

Пункт настроек	Опции	Текст справки	Комментарии
Установка профиля вентилятора	**Производительность** Акустические характеристики	Выбирает профиль вентилятора для охлаждения системы.	В производительном режиме для охлаждения используются вентиляторы, а пропускная способность памяти не уменьшается. В акустическом режиме для снижения уровня шума используется регулирование скорости вращения вентиляторов охлаждения системы.
Высота над уровнем моря	300 м и меньше **301 м – 900 м** Более 900 м	300 м или меньше (<= 980 футов): Оптимальная производительность для серверов, используемых на уровне моря. 301 м – 900 м (980 – 2950 футов): Оптимальная производительность для серверов, используемых на средней высоте над уровнем моря. Более 900 М (>2950 футов): Оптимальная производительность для серверов, используемых на большой высоте над уровнем моря.	

3.7.2.2 Security Screen (экран «Security»)

В экране «Security» представлены поля для активации парольной защиты, выбора пользовательского и администраторского паролей, блокировки кнопок передней панели.

Для перехода к этому экрану из экрана «Main» выберите опцию Security.

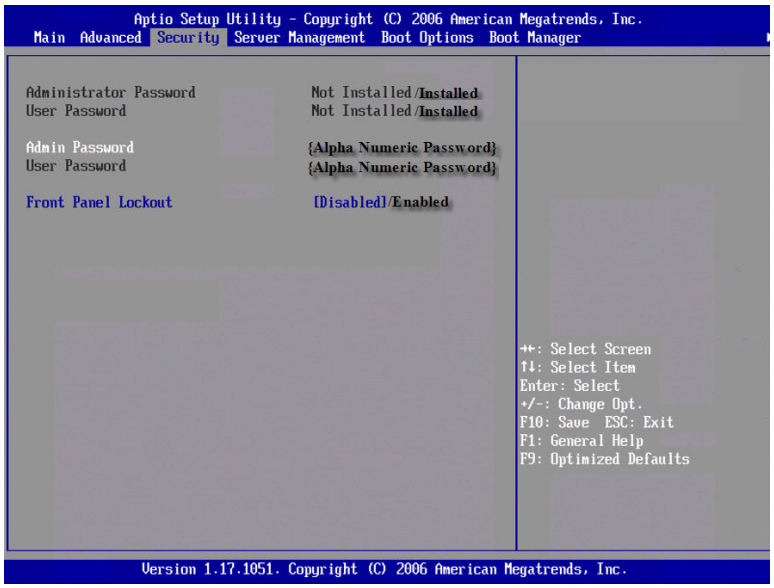


Рисунок 17. Программа настройки – Вид экрана «Security Configuration»

Таблица 25. Программа настройки – Поля экрана «Security Configuration»

Пункт настроек	Опции	Текст справки	Комментарии
Administrator Password (пароль администратора)	Установлен Не установлен	Показывает статус пароля администратора.	Только информация. Пароль администратора отключен, если он не содержит ни одного знака.
Пароль пользователя	Установлен Не установлен	Показывает статус пароля пользователя.	Предназначено только для информации; пароль пользователя отключен, если он не содержит ни одного знака.
Admin Password		Поле ввода пароля администратора; максимальная длина пароля – 7 знаков.	Эта опция предназначена только для контроля доступа к настройкам BIOS. Администратор имеет полный доступ ко всем настройкам. Удаление пароля администратора влечет удаление пароля пользователя.

Пункт настроек	Опции	Текст справки	Комментарии
Пароль пользователя		Поле ввода пароля пользователя; максимальная длина пароля – 7 знаков.	Доступно только в случае, если установлен пароль администратора. Эта опция предназначена для защиты настроек BIOS. Авторизованный пользователь имеет ограниченный доступ к настройкам.
Блокировка передней панели	Включено **Отключено**	Если опция включена, кнопки выключения питания и перезапуска системы, расположенные на передней панели, блокируются. Выключение и перезапуск должны инициироваться через интерфейс управления системой	

3.7.2.3 Server Management Screen (экран «Server Management»)

В экране «Server Management» представлены поля для настройки различных функций управления системой. Кроме того, экран содержит опции перехода к экрану настройки переадресации консоли и экрану системной информации.

Для перехода к этому экрану из экрана «Main» выберите опцию Server Management.

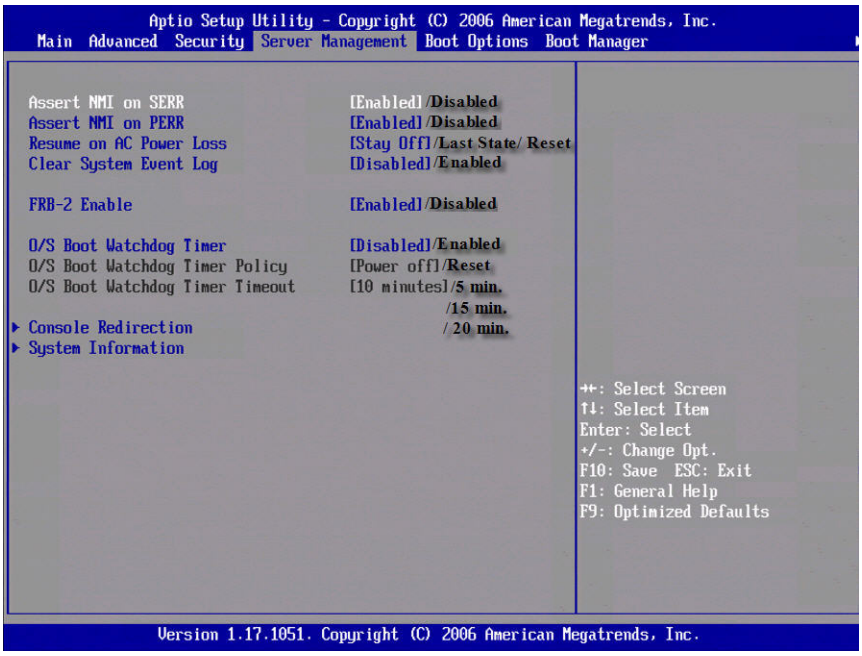


Рисунок 18. Программа настройки – Вид экрана «Server Management Configuration»

Таблица 26. Программа настройки – Поля экрана «Server Management Configuration»

Пункт настроек	Опции	Текст справки	Комментарии
Возобновление работы после отключения питания	**Stay off** Last State (Последнее состояние) Очистить	Возобновление работы после отключения питания	
Clear System Event Log	Включено **Отключено**	Очищает журнал системных событий. После перезагрузки устанавливается значение «Disabled»	
FRB-2 Enable	**Включено** Отключено	При включенной опции контроллер BMC перезагружает систему, если BIOS не заканчивает выполнение процедуры POST до истечения таймера FRB-2.	
O/S Boot Watchdog Timer	Включено **Отключено**	При включенной опции запускается специальный таймер BIOS, который может быть сброшен только приложением Intel Management Software после загрузки операционной системы. Позволяет определить, что загрузка системы завершена успешно; в противном случае – перезапускает систему.	
O/S Boot Watchdog Timer Policy	**Питание выключено** Очистить	O/S Boot Watchdog Timer Policy	
O/S Boot Watchdog Timer Timeout	5 минут 10 минут 15 минут 20 минут	O/S Boot Watchdog Timer Timeout	
Подключение консоли			См. Раздел 3.7.2.4
System Information (информация о системе)			См. Раздел 3.7.2.5

3.7.2.3.1 Console Redirection Screen (экран «Console Redirection»)

Экран Console Redirection позволяет подключать или отключать функцию переадресации консоли и настраивать параметры соответствующего соединения.

Для перехода к этому экрану из экрана «Main» выберите Server Management, В экране «Server Management» выберите опцию Console Redirection.

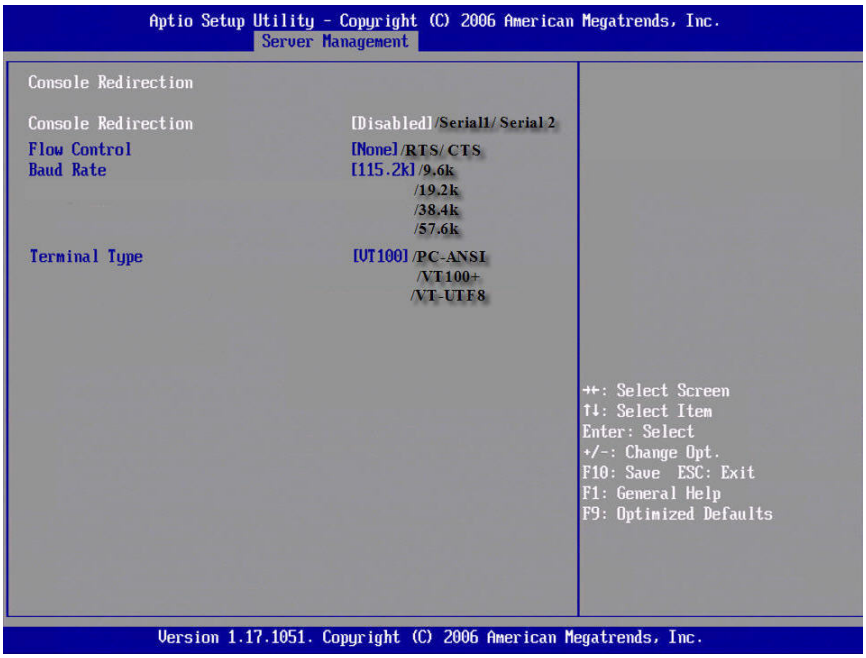


Рисунок 19. Программа настройки – Вид экрана «Console Redirection»

Таблица 27. Программа настройки – Поля экрана «Console Redirection Configuration»

Пункт настроек	Опции	Текст справки	Комментарии
Подключение консоли	**Отключено** **Serial1** **Serial2**	Разрешается или запрещается переадресация консольной информации через последовательное соединение	
Flow Control	**Нет** RTS/CTS	Выбор протокола квитирования, поддерживаемого приложением удаленной консоли	
Baud Rate	9600 19.2K 36.4K 57.6K **115.2K**	Выбор скорости передачи данных по каналу связи с удаленной консолью	
Terminal Type	**VT100** VT100+ VT-UTF8 PC-ANSI	Выбор кодировки символов, поддерживаемой удаленной консолью	

3.7.2.4 Server Management System Information (экран «Server Management System Information»)

В экране «Server Management System Information» представлена информация о типах компонентов, серийных номерах и версиях встроенного программного обеспечения системы.

Для перехода к этому экрану из экрана «Main» выберите Server Management, Выберите опцию System Information в экране «Server Management».

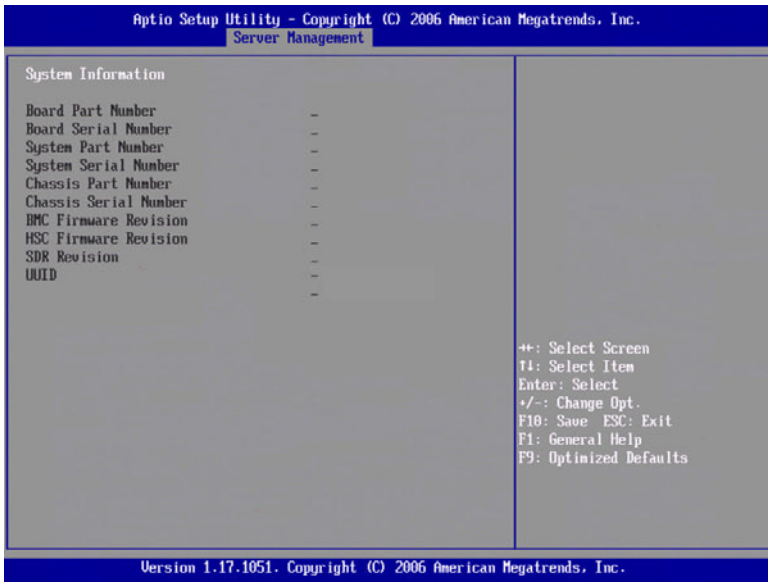


Рисунок 20. Программа настройки – Вид экрана «Server Management System Information»

Таблица 28. Программа настройки – Поля экрана «Server Management System Information»

Пункт настроек	Опции	Текст справки	Комментарии
Номер детали платы	В информационных целях		
Серийный номер платы	В информационных целях		
Номер детали системы	В информационных целях		
Серийный номер системы	В информационных целях		
Chasis Part Number (код типа шасси)	В информационных целях		
Chasis Serial Number (серийный номер шасси)	В информационных целях		
Версия встроенного микрокода BMC	В информационных целях		
HSC Firmware Revision (версия встроенного программного обеспечения контроллера HSC)	В информационных целях		
SDR Revision	В информационных целях		
UUID	В информационных целях		

3.7.2.5 Error Manager Screen (экран «Error Manager»)

Экран «Error Manager» содержит информацию об ошибках, обнаруженных процедурой POST.

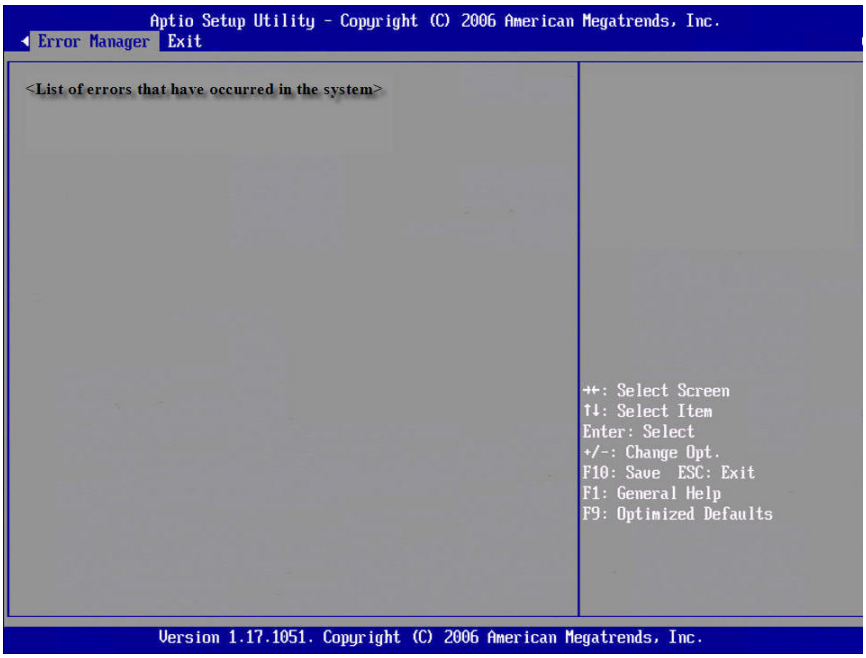


Рисунок 21. Программа настройки – Вид экрана «Error Manager»

Таблица 29. Программа настройки – Поля экрана «Error Manager»

Пункт настроек	Опции	Текст справки	Комментарии
Показывает информацию о системных ошибках			

3.7.2.6 Exit Screen (экран «Exit»)

Экран «Exit» предоставляет пользователю возможность сохранить или отменить изменения, сделанные в других экранах. С помощью этого же экрана можно восстановить заводские настройки системы или сохранить/восстановить определенный пользователем набор стандартных значений. Если выбрана опция Restore Defaults, то будут использованы стандартные значения, выделенные в таблицах этой главы жирным шрифтом. Если выбрана опция Restore User Default Values, то вместо заводских настроек, будут применены настройки, сохраненные пользователем ранее в качестве стандартных.

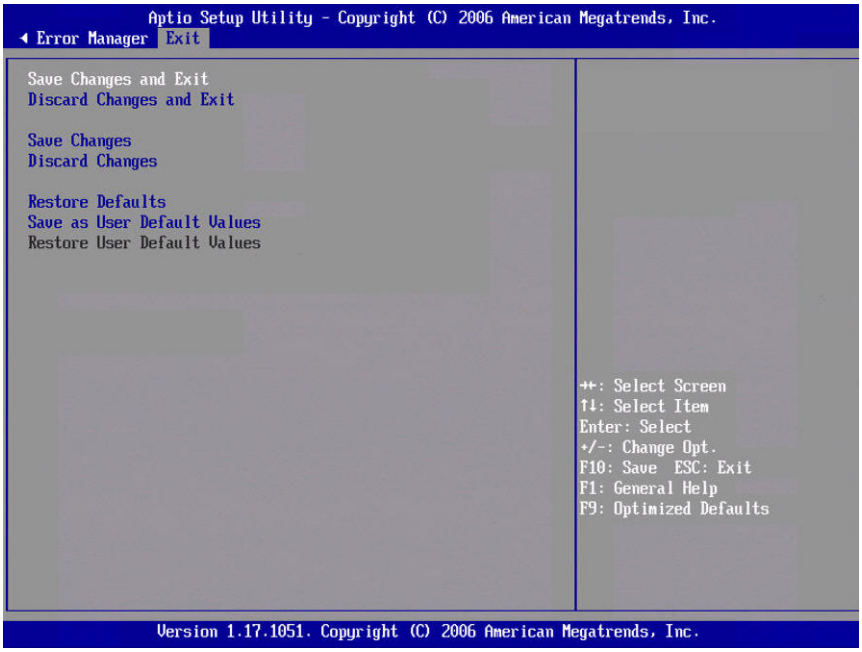


Рисунок 22. Программа настройки – Вид экрана «Exit»

Таблица 30. Программа настройки – Поля экрана «Exit»

Пункт настроек	Текст справки	Комментарии
Save Changes and Exit	Применяются текущие значения параметров и выполняется выход из программы настройки BIOS.	Запрос подтверждения принятия изменений появляется на экране только в том случае, если значения каких-либо полей программы настройки были изменены.
Discard Changes and Exit	Отменяются изменения и выполняется выход из программы настройки BIOS.	Запрос подтверждения принятия изменений появляется на экране только в том случае, если значения каких-либо полей программы настройки были изменены.
Save Changes	Применяются текущие значения параметров и продолжается настройка BIOS.	Запрос подтверждения принятия изменений появляется на экране только в том случае, если значения каких-либо полей программы настройки были изменены.
Discard Changes	Отменяются изменения и продолжается настройка BIOS.	Запрос подтверждения принятия изменений появляется на экране только в том случае, если значения каких-либо полей программы настройки были изменены.
Restore Defaults (восстановить заводские настройки)	Восстанавливаются заводские настройки.	Пользователю предлагается подтвердить выбор данной инструкции. BIOS сможет использовать заводские настройки после перезагрузки.
Save User Default Values (сохранить определенные пользователем стандартные настройки)	Сохраняются текущие значения параметров для их последующего использования.	
Restore User Default Values (восстановить определенные пользователем стандартные настройки)	Восстанавливаются ранее сохраненные пользователем стандартные настройки.	Пользователю предлагается подтвердить выбор данной инструкции.

3.8 Loading BIOS Defaults (загрузка заводских настроек BIOS)

Существуют различные механизмы восстановления стандартной конфигурации системы. Если фиксируется запрос на восстановление исходной конфигурации, то BIOS загружает параметры заводских настроек во время следующего запуска процедуры POST. Запрос на восстановление исходных настроек может быть инициирован одним из нижеприведенных способов:

- Во время работы программы настройки BIOS запрос может быть сгенерирован нажатием клавиши <F9>.
- Запрос на переустановку конфигурации системы может вызываться перемещением конфигурационных перемычки очистки CMOS.

Выполнение следующих действий также влечет за собой загрузку стандартных настроек BIOS:

1. Выключите систему.
2. Переставьте переключатель Clear CMOS с контактов 1-2 на контакты 2-3.
3. Подождите 10 секунд.
4. Переставьте переключатель Clear CMOS с контактов 2-3 на контакты 1-2.
5. Отключите и затем включите снова питание системы.
6. Включите питание системы.

3.9 Security

BIOS поддерживает несколько функций, обеспечивающих безопасности системы В данном разделе описываются эти функции безопасности и рабочая модель.

3.9.1 Рабочая модель

В таблице ниже сведены принципы работы функций безопасности, поддерживаемые BIOS.

Таблица 31. Функции безопасности – Операционная модель

Режим	Метод входа/ событие	Критерий входа	Поведение системы	Критерий выхода	После выхода
Password on boot	Включение питания/ перезагрузка (Reset)	Пароль пользователя в BIOS установлен и используется при загрузке системы. Использование безопасного режима загрузки запрещено в программе настройки BIOS.	Система останавливается и просит ввести пароль пользователя перед сканированием дополнительных ПЗУ. Система находится не в защищенном режиме. Не принимается никакой ввод клавиатуры или мыши, кроме пароля.	Пароль пользователя. Пароль администратора.	Кнопки передней панели разблокированы. Сервер загружается в обычном режиме. Загрузочная последовательность определяется опциями настройки.

3.9.2 Защита паролем

В BIOS используются пароли для предотвращения несанкционированного доступа к серверу. BIOS поддерживает пароли пользователя и администратора. Для того, чтобы установить пароль пользователя, необходимо чтобы был установлен пароль администратора. Максимальная длина пароля составляет 8 символов. В пароле могут использоваться только буквенно-числовые символы (a-z, A-Z, 0-9). Пароль не чувствителен к регистру ввода символов.

После установки пароля он может быть сброшен путем ввода пустого пароля. Пользователь после ввода пароля может изменять дату, время и пароль пользователя. Другие настройки можно изменять только после ввода пароля администратора. Если установлен только один пароль, этот пароль требуется для входа в программу BIOS Setup.

Администратор контролирует все настройки программы BIOS Setup и имеет возможность удалять пароль пользователя.

Если пользователь или администратор три раза подряд в течение одной попытки загрузки системы введет неверный пароль, систем перейдет в состояние останова.
Для выхода из этого состояния необходим перезапуск системы. Такое поведение системы затрудняет «взлом» пароля путем его подбора.

3.9.3 Перемычка очистки пароля

В случае утери пароля пользователя и/или администратора очистку обоих паролей можно произвести, установив перемычку очистки пароля в положение очистки. Во время процедуры POST BIOS определяет положение перемычки очистки пароля и при необходимости очищает любые пароли. Перед заданием нового пароля переключатель удаления пароля должен быть установлен в свое исходное положение.

3.10 Процедуры загрузки обновлении во флэш-память BIOS

3.10.1 Утилита Intel Iflash32 BIOS Update

Утилита Intel Iflash32 BIOS Update предназначена для обновления BIOS в среде DOS.

Загрузите оболочку ROM-DOS и скопируйте файл IFlash32.exe и бинарный файл BIOS (называемый также файлом-капсулой) на загрузочную дискету DOS, компакт-диск или USB-накопитель.

3.10.1.1 Интерфейс командной строки

IFlash32 [File Name] [Options]

- Для получения справки о синтаксисе команды наберите: IFlash32 /h
- Для обновления BIOS: IFlash32 [File Name] /u
- Для отображения информации о файле: IFlash32 [File Name] /i

- Для получения значения BIOS ID: IFlash32 /i
- Для обновления BIOS в неинтерактивном режиме: IFlash32 [FileName] /u /ni
- Для автоматической перезагрузки системы после окончания процедуры обновления BIOS: IFlash32 [FileName] /u /r

Перезагрузите систему после завершения процедуры обновления BIOS.

3.10.2 Программа Intel® One Boot Flash Update Utility

Утилита Intel® One Boot Flash Update запускается из командной строки с помощью команды flashupdt.

Перед запуском необходимо указать рабочий каталог, в котором находится утилита. Во время выполнения утилита использует определенные файлы, которые должны быть расположены в рабочем каталоге.

Для выполнения утилиты Intel® One Boot Flash Update необходимо обладать администраторскими полномочиями в среде Windows* или полномочиями суперпользователя среде Linux.

3.10.2.1 Синтаксис команды

flashupdt [-i] [-u < *URL or path* >] [-c] [-h|?]

Эта команда выполняет загрузку обновлений BIOS или других микропрограмм локального сервера на основе файла конфигурации, входящего в комплект поставки утилиты Intel® One Boot Flash Update.

[–i]	Выводит на экран информацию о текущих версиях BIOS, BMC и SDR. Если опция –i дополнена опцией –u, то утилита выводит информацию о файлах пакета обновления.
[–u]	Выполняет обновление BIOS и встроенного программного обеспечения. Параметр <URL or path> определяет место нахождения файлов, необходимых для выполнения обновления. Значением параметра <URL or path> может быть путь к каталогу в локальной файловой системе, адрес FTP или HTTP -сервера. Пример использования опции –u: –u — Определяет текущий локальный каталог. –u http://<IP адрес или URL>/<путь> — Определяет HTTP-сервер. –u ftp://<логин:пароль>@<имя сервера или IP адресс>/<путь> — Определяет FTP-сервер. Если опция –u используется совместно –i, то обновление не выполняется. Выводится только информация о пакете обновления.
[–c]	Отменяются все не вступившие в силу изменения, внесенные утилитой в BIOS, BMC и SDR. Чтобы прервать операцию обновления независимо от того, выполняется ли она в этот момент или нет, утилита восстанавливает значения внутренних флагов BIOS, BMC и SDR. Обновления FRU вступают в силу немедленно.
[–h|?]	Выводит справочную информацию о команде.

Пример синтаксиса команды:

```
flashupdt –u ftp://ftp.examplesite.com/UpdatePackage/ServerName
flashupdt –u "ftp://ftp.examplesite.com/Update Package/
Server Name"
flashupdt –u
ftp://Kevin:87w09@ftp.examplesite.com/UpdatePackage/ServerName
```

Для ОС Windows*:

```
flashupdt –u c:\UpdatePackage\ServerName
```

Для Linux:

```
flashupdt –u /UpdatePackage/ServerName
```

3.10.2.2 Обновление серверных микропрограмм через удаленное клиентское приложение

Утилита может быть запущена удаленно через безопасное сетевое соединение, использующее приложения Telnet Client и Terminal Services в среде Windows или Telnet Client и Remote Shell в Linux. Для получения информации о процедуре удаленного доступа в систему и об использовании команд следует обращаться к документации на операционную систему.

После завершения удаленного входа в систему, можно использовать команды, описанные выше. При использовании сценария, описывающего рассматриваемые процессы, возможно удаленное обновление нескольких серверов.

3.10.2.3 Удаление утилиты Intel® One Boot Flash Update

В этом разделе описывается процедура удаления утилиты the Intel® One Boot Flash Update.

*3.10.2.3.1 Microsoft Windows**

Для удаления утилиты Intel® One Boot Flash Update в операционной системе Windows* необходимо выполнить следующие операции:

1. Открыть окно командной строки и указать рабочий каталог, содержащий утилиту Intel® One Boot Flash Update:

   ```
   cd C:\<installation directory>\bin\flashupdt
   ```

2. Для удаления драйверов необходимо выполнить следующее:

   ```
   uninstall.cmd
   ```

3. Удалить все находящиеся в каталоге файлы.

4. Перезагрузите сервер.

3.10.2.3.2 Linux

Для удаления утилиты Intel® One Boot Flash Update в операционной системе Linux необходимо выполнить следующие действия:

1. Войти в систему как суперпользователь.
2. Открыть терминал и рабочий каталог, содержащий утилиту Intel® One Boot Flash Update:

   ```
   cd /usr/local/flashupdt
   ```

3. Выполнить следующую команду:

   ```
   /uninstall
   ```

3.11 BIOS Bank Select и One Boot Flash Update

Обновление BIOS с помощью утилиты One Boot Flash Update возможно при условии, что сервер находится во включенном состоянии и функционирует в нормальном режиме.

Обновление BIOS с помощью функции BIOS Bank Select возможно во внештатном режиме работы сервера. Если после обновления будет установлено, что новая версия BIOS в силу каких-либо причин является неработоспособной, то выполняется «откат» к предыдущей работоспособной версии BIOS.

Все серверные системные платы Intel® и другие платформы на базе набора микросхем Intel® серии 5000 снабжены флэш-памятью объемом 4 МБ для размещения BIOS. Эта память разделена на 2 банка по 2 МБ каждый. Один из банков называется «верхний банк», другой – «нижний банк». BIOS может размещаться в любом из банков. Область BIOS, из которой в любой момент времени может быть выполнена загрузка системы, называется первичным разделом BIOS. Оставшаяся область BIOS носит название вторичным разделом BIOS. Все обновления BIOS производятся *только* для вторичного раздела BIOS.

Примечание: *Первичный и вторичный разделы BIOS являются логическими разделами системной флэш-памяти. Они могут размещаться в любом из физических банков памяти.*

Для выполнения процедуры обновления BIOS требуются специальные аппаратные средства и дополнительное пространство во флэш-памяти для утилит BIOS Bank Select и One Boot Flash Update. Переключатель BIOS Bank Select определяет поведение BIOS после завершения онлайн-обновления. В зависимости от позиции переключателя может быть установлен один из двух режимов.

- 1-2 банк 0
- 2-3 Нормальный режим (стандартная позиция)

Обновления BIOS могут быть выполнены в обеих позициях переключателя BIOS Bank Select. Поведение системы в каждом из режимов описано ниже.

3.11.1 Переключатель BIOS Bank Select в позиции «нормальный режим» (замкнуты контакты 2 – 3)

В нормальном режиме новый образ BIOS загружается во вторичный раздел флэш-памяти и после этого верифицируется. Если верификация проходит успешно, BIOS через специальные аппаратные ресурсы уведомляет систему о необходимости загрузки с использованием нового образа BIOS и перезагружает систему. Начинается загрузка новой BIOS. Если загрузка завершается успешно, то обновление BIOS считается выполненным. Если загрузка новой BIOS происходит неудачно, то запускается таймер и выполняется возврат к предыдущему «рабочему» образу BIOS.

1. Загрузите систему при замкнутых контактах 2 и 3 переключателя BIOS Bank Select.
2. Обновите BIOS, используя файл iFlash32.exe или утилиту Intel® One Flash Update.
3. Перезагрузка системы.
4. После этого выполняется проверка работоспособности текущей версии BIOS и производится загрузка системы с новой BIOS.
5. Если загрузка новой BIOS происходит неудачно, то выполняется процедура «отката» и система загружается со старой BIOS.

3.11.2 Переключатель BIOS Bank Select в положении «банк 0» (замкнуты контакты 1 – 2)

При необходимости обновления первичного раздела образа BIOS положение переключателя BIOS Bank Select может быть изменено и система будет вынуждена загружаться из вторичного раздела флэш-памяти.

1. Загрузите систему при замкнутых контактах 1 и 2 переключателя BIOS Bank Select.
2. Обновите BIOS, используя файл iFlash или утилиту Intel® One Boot Flash Update.
3. Перезагрузка системы.
4. Загрузка системы выполняется со старой BIOS.
5. Чтобы использовать новую BIOS необходимо отключить питание системы, переставить переключатель в позицию 2 – 3 и затем снова включить питание системы.
6. Если новая BIOS исправна, то система загружается с использованием нового образа BIOS.
7. Если BIOS повреждена или несовместима «откат» к старому образу BIOS не выполняется. Чтобы загрузить систему со старым образом BIOS, необходимо отключить питание системы, установить переключатель в позицию 1 – 2, затем снова включить питание.

3.12 Двоичный код OEM-компании

Отдельный том энергонезависимой памяти резервируется для использования OEM-производителями. Том памяти OEM предназначен для хранения логотипа OEM-производителя. Обновление тома выполняется независимо от других томов энергонезависимой памяти. В томе OEM содержится также образ файловой системы флэш-памяти. Объем тома OEM – 192 КВ.

3.12.1 Графический логотип

Том OEM энергонезависимой памяти может содержать графический логотип (splash logo) OEM-производителя. Обновление логотипа возможно с помощью утилиты Change Logo. Если OEM-логотип записан в энергонезависимую память, то он используется вместо стандартного логотипа Intel. Логотип может быть идентифицирован по имени файла.

Файл, содержащий логотип, должен соответствовать общим стандартам для графических изображений. Размер изображения не должен превышать 800 x 512 пикселей. Количество цветов – не более 256, хотя на практике, в связи с небольшим размером изображения, используется гораздо меньшее количество цветов.

3.13 Выбор загрузочного устройства

На фазе Boot Device Selection (выбор загрузочного устройства) обеспечивается управление загрузкой системы. Значения переменных, определяющих вариант загрузки системы, устанавливаются автоматически во время инсталляции операционной системы или изменяются пользователем с помощью приложения Boot Maintenance Manager или программы настройки BIOS. Приложение Boot Maintenance Manager позволяет вносить и сохранять изменения в порядок загрузки системы. Существует также возможность ограничить срок действия изменений опции «first boot» периодом одной загрузки системы.

3.13.1 Управление сервером. Выбор загрузочного устройства

Спецификацией IPMI 2.0 определено, что устройства управления серверами должны устанавливать параметры загрузки с помощью соответствующих флагов.

BIOS поддерживает загрузку со следующих устройств:

- PXE
- дисководов жестких дисков (USB, SATA, SAS и PATA)
- USB-дисководов гибких дисков
- USB-карт флэш-памяти
- дисководов компакт-дисков

3.14 Поддержка операционных систем

3.14.1 Совместимость с Windows

Корпорации Intel и Microsoft совместно разрабатывают руководства для системных интеграторов, использующих процессоры Intel и операционные системы Microsoft. Программа *Hardware Design Guide for Microsoft Windows 2000 Server*, Version 3.0 предназначена для платформ, разработанных под операционные системы класса Windows Server.

Эти платформы соответствуют требованиям, предъявляемым приложением *Hardware Design Guide for Microsoft Windows 2000 Server*, Version 3.0 к серверам уровня предприятия.

3.14.2 Расширенный интерфейс управления конфигурацией и питанием (ACPI)

Основная задача ACPI BIOS заключается в создании таблиц ACPI. Процедура POST создает таблицы ACPI и размещает их в расширенной памяти (выше 1 МБ). Расположение этих таблиц передается операционной системе с поддержкой ACPI через серию таблиц, расположенных в памяти. Формат и расположение этих таблиц описаны в открытых спецификациях интерфейса ACPI (*Advanced Configuration and Power Interface Specification*, Revision 1.0b и *Advanced Configuration and Power Interface Specification*, Revision 2.0).

BIOS поддерживает как таблицы ACPI 2.0 так и ACPI 1.0b. Для предотвращения конфликтов с операционной системой без поддержки ACPI, память использованная для таблиц ACPI, помечается как зарезервированная функцией E820h INT 15h.

Согласно спецификации ACPI, ACPI-совместимая операционная система генерирует SMI с целью запроса системы о переключении в режим ACPI. BIOS отвечает тем, что устанавливает конфигурацию системы, обеспечивающую поддержку режима ACPI, и посылает команду контроллеру BMC активировать указанный режим. Система автоматически возвращается в прежний режим после нажатия кнопки reset или выключения и включения питания.

Согласно спецификации ACPI система должна поддерживать хотя бы один режим пониженного энергопотребления – так называемый, спящий режим или режим ожидания. BIOS поддерживает режимы пониженного энергопотребления S0, S1, S3, S4 и S5. Режим S1 рассматривается как базовый спящий режим.

Примечание: *Режим S3 поддерживается только системными платами для рабочих станций Intel® Workstation Board S5000XVN. Для получения подробной информации о поддерживаемых системой режимах пониженного энергопотребления следует обращаться к технической спецификации на используемое оборудование.*

Инициатором выхода рассматриваемой платформы из режима S1, кроме перечисленных в разделе 3.16 источников, может быть USB-устройство.

Состояние источников сигнала активизации контролируется операционной системой, поддерживающей режим ACPI, через соответствующие драйверы. BIOS не имеет прямого контроля над источниками сигнала активации во время загрузки операционной системы в режиме ACPI. Роль BIOS ограничивается передачей операционной системе информации об источниках сигнала активизации и контролем посредством таблицы DSDT (differentiated system description table, дифференциальная таблица описания системы) вторичных битов control / status.

Состояние S5 эквивалентно отключению операционной системы. При переходе в режим S5 информация о состоянии системы не сохраняется.

3.15 Лицевая панель управления

Платформа поддерживает использование кнопок включение/выключение питания), перезапуск системы) и NMI, расположенных на панели управления.

3.15.1 Кнопка питания

BIOS поддерживает использование кнопки power, находящейся на передней панели управления. Нажатие кнопки power инициирует запрос, который затем пересылается контроллером BMC машинам состояния питания ACPI, имеющимся в микросхемах. Эта кнопка управляет контроллером BMC и не связана с блоком питания непосредственно.

- **Включение кнопки питания**
  Контроллер BMC следит за состоянием кнопки power и других аппаратных источников сигнала активизации системы. При изменении состояния любого из источников контроллер BMC запускает процесс перехода системы к активному режиму. Поскольку процессоры не задействуются, BIOS не участвует в этой последовательности. Оборудование системы получает от BMC сигналы power good и reset, после чего переходит в активное состояние.
- **Выключение кнопки power (при незагруженной операционной системе)**
  Прерывание SCI (System Control Interrupt) замаскировано. BIOS регистрирует событие нажатия кнопки power, после чего генерируется прерывание SMI. При получении этого прерывания BIOS выполняет проверку в регистрах микросхем ACPI бита состояния кнопки power. Если бит состояния установлен, то BIOS деактивирует в микросхемах машину состояния питания режима ACPI. BMC ожидает получения сигналов об отключении всех микросхем, после сего отключает общее питание системы. В качестве механизма защиты предусмотрено автоматическое отключение контроллером BMC питания системы по истечению 4 – 5 секунд после получения BIOS запроса на выключение.
- **Выключение кнопки power (при загруженной операционной системе)**
  Нажатие кнопки power во время работы операционной системы, поддерживающей режим ACPI, генерирует посредством прерывания SCI запрос на завершение работы системы. Операционная система сохраняет контроль над системой, а политика операционной системы определяет, в какое состояние сна переходит система, если переходит вообще. В противном случае питание системы выключает BIOS.

3.15.2 Кнопка Reset

Платформа поддерживает использование кнопки reset , находящейся на лицевой панели управления. Нажатие кнопки reset инициирует соответствующий запрос, который контроллер BMC пересылает набору микросхем. BIOS не участвует в обработке события нажатия кнопки reset.

3.15.3 Кнопка NMI (Non-Maskable Interrupt – немаскируемое прерывание)

BIOS поддерживает кнопку NMI на передней контрольной панели. Существуют различные виды лицевых панелей; не всех из них может иметься кнопка NMI. Нажатие кнопки NMI инициирует запрос, на основании которого BMC генерирует прерывание NMI. На фазе загрузки системы это прерывание перехватывается BIOS. После загрузки прерывание NMI перехватывается операционной системой. Если BIOS обнаруживает прерывания NMI на фазе загрузки, то выполняется останов системы. Во время работы сервера под управлением операционной системы прерывание NMI обрабатывается операционной системой.

3.16 Режимы пониженного энергопотребления и активизация системы

3.16.1 Состояния режима сна системы

Платформа поддерживает следующие состояния режима сна ACPI:

- Состояние ACPI S0 (работает)
- Состояние ACPI S1 (режим сна)
- Режим ACPI S3 (приостановка системы)
- Режим ACPI S4 (бездействие системы)
- Режим ACPI S5 (программное выключение)

Примечание: *Режим S3 поддерживается только системными платами для рабочих станций Intel® Workstation Board S5000XVN. Для получения подробной информации о поддерживаемых системой режимах пониженного энергопотребления следует обращаться к технической спецификации на используемое оборудование.*

3.16.2 События, активизирующие систему / Источники прерывания SCI

Серверные системные платы или системные платы для рабочих станция поддерживают в среде ACPI перечисленные ниже источники сигналов активизации системы. Установка и снятие запрета на использования этих источников осуществляется операционной системой:

- Устройства, такие как USB-мышь и клавиатура, подключенные к любому из портов USB, могут инициировать активизацию системы в режимах S1 и S3.
- Последовательный порт может быть сконфигурирован для активизации системы в режимах S1 и S3.

- Карты PCI, такие как сетевые адаптеры, могут инициировать активизацию системы в режиме S1 и S3. При этом карты должны иметь соответствующее аппаратное обеспечение.
- Согласно требованиям спецификации интерфейса ACPI, кнопка power может инициировать активизацию системы в режимах S1 и S3.

3.17 Обработка немаскируемых прерываний

Немаскируемые прерывания генерируются в двух случаях: при нажатии кнопки NMI на лицевой панели и в случае, если BIOS обнаруживает фатальную ошибку и работа системы должна быть остановлена. BIOS устанавливает стандартный обработчик прерываний NMI, выводящий на экран сообщение о системной ошибке и после этого останавливающий систему. Обработчик прерываний NMI, работающий под управлением BIOS, активен только на протяжении процедуры POST. Операционная система во время своей работы устанавливает и использует собственный обработчик прерываний NMI.

Обработчик NMI-прерываний, работающий под BIOS, определяет источник прерывания и перед остановкой системы выводит сообщение о системной ошибке. Возможные типы сообщений перечислены в приведенной ниже таблице.

Таблица 32. Сообщения об ошибках, используемые обработчиком прерываний NMI

Источник прерывания NMI	Сообщение о системной ошибке
Кнопка NMI на передней панели	Front Panel NMI activated – System Halted (Нажата кнопка NMI на лицевой панели – система остановлена)
System Error NMI (системная ошибка)	NMI has been received – System Halted (получено прерывание NMI – система остановлена)

3.18 Функции управления сервером, поддерживаемые BIOS

BIOS поддерживает большое количество функций управления сервером, базирующихся на открытых стандартах, и несколько функций, использующих в своей основе фирменные стандарты. IPMI – отраслевой стандарт, определяющий абстрактные интерфейсы управления платформой. В данной главе рассматривается реализация функций IPMI.

3.19 IPMI

Под интеллектуальным управлением платформой понимаются функции автономного мониторинга и восстановления системы, реализованные на аппаратном и микропрограммном уровнях. Функции управления, такие как инвентаризация системы, регистрация системных событий, диагностика и предоставление информации о состоянии системы, могут выполняться без участия главных процессоров. При этом система может находиться в выключенном состоянии, а выполнение рассматриваемых функций будет обеспечиваться за счет автономного источника. Контроллер BMC (контроллер системной платы) и другие контроллеры выполняют эти задачи независимо от главного процессора. BIOS использует для взаимодействия с контроллерами управления платформой стандартные интерфейсы.

BIOS активирует системный интерфейс с контроллером BMC на ранней стадии процедуры POST. BIOS ведет журнал регистрации системных событий и кодов ошибок, обнаруженных процедурой POST. BIOS передает контроллеру BMC информацию о начале загрузки на ранней стадии процедуры POST. Перечень событий, регистрируемых BIOS, определен стандартом *Intelligent Platform Management Interface Specification*, Version 2.0.

3.20 Подключение консоли

BIOS поддерживает переадресацию интерфейса с видеоустройствами и клавиатурой через последовательный канал связи (последовательный порт). При включении переключения консоли локальный клавиатурный ввод и вывод изображение (для сервера) передаются на локальные соединения клавиатуры и изображения, а также на удаленную консоль через последовательное соединение. Доступен клавиатурный ввод с обоих источников; изображения также передается на оба устройства отображения изображений.

Система также может работать без установленных в систему клавиатуры или мыши; при этом управление системой осуществляется исключительно посредством удаленной консоли. Удаленно могут выполняться различные утилиты, в том числе программа настройки BIOS.

3.20.1 Настройка переадресации через последовательный канал связи

Для выполнения переадресации консоли BIOS не требует отключения графического логотипа. BIOS поддерживает несколько консолей, функционирующих как в графическом, так и в текстовом режимах. Графические консоли могут отображать логотип, тогда как текстовые консоли воспринимают только текстовую информацию.

Переадресация консоли прекращается с началом стандартной загрузки операционной системы. С этого момента за переадресацию консоли отвечает операционная система.

3.20.2 Наборы символов и кодировка

Удаленный терминал в режиме переадресации направляет локальному серверу информацию в символьном виде. В качестве удаленного может использоваться несетевой терминал, имеющий коммуникационную программу и подключенный к серверу через прямое соединение. Кодировка символов соответствует формату VT-UTF8 со следующими расширениями.

3.20.2.1 Выбор комбинаций клавиш

Комбинация клавиш <Del> и <Ctrl> аналогична нажатию клавиши <F2> (Setup). Возможность использования этой комбинации реализована и документирована, но информация о ней не выводится на экран в строке-подсказке системы. Следующие «горячие» клавиши определены для использования только на удаленной консоли. Использование этих клавиш на локальной клавиатуре сервера не поддерживается.

3.20.2.2 Обособленное использование клавиши <Esc> для неструктурированных операций

В документе *Microsoft Headless Design Guidelines* специфика использования клавиши <Esc> в качестве обособленного символа описывается следующим образом:

- Нажатие клавиши <Esc>, сопровождаемое двухсекундной паузой, должно интерпретироваться как одиночная инструкция escape.
- Символ <Esc>, сопровождаемый в течение двухсекундного интервала одним или более символом, должен интерпретироваться как символ <Esc> плюс сопровождающий символ или символы, если эта последовательность не описана в настоящей спецификации.

Escape-последовательность, приведенная в нижеследующей таблице, является последовательностью ввода. Это значит, что она направлена системе BIOS с удаленного терминала.

Таблица 33. Escape-последовательности, используемые при переадресации консоли, для неструктурированных операций

Escape-последовательность	Описание
<Esc>R<Esc>r<Esc>R Это будет выполнено, с установкой по умолчанию значения «отключено».	Удаленный сброс консоли

3.20.3 Ограничения

- Перенаправление консоли BIOS завершается после того, как операционная система с поддержкой EFI вызывает функцию EFI Exit Boot Services. После этого за перенаправление консоли отвечает операционная система.
- Перенаправление BIOS производится в текстовую консоль. Графические данные, например, логотип, не перенаправляются.

3.20.4 Интерфейс управления сервером

Если BIOS определяет, что перенаправление консоли включено, BIOS считывает текущую скорость передачи и передает это значение на соответствующий управляющий контроллер по интеллектуальной шине управления платформами (Intelligent Platform Management Bus – IPMB).

3.21 Последовательный интерфейс IPMI

Система предоставляет последовательный порт, управляемый контроллером системной платы. Мультиплексор, управляемый контроллером системной платы, определяет, подключен ли внешний порт COM1 к контроллеру системной платы или к стандартному последовательному порту Super I/O. Обратитесь к Спецификации на интеллектуальный интерфейс управления платформами (Intelligent Platform Management Interface Specification), версия 2.0, раздел 14 «последовательный/модемный интерфейс IPMI» для получения более подробной информации об этих функциях.

3.21.1 Режимы доступа к каналу

BIOS поддерживает доступ по четырем различным каналам. Подробнее это описано в таблице 6-4 Спецификации на интеллектуальный интерфейс управления платформами (Intelligent Platform Management Interface Specification), версия 2.0.

3.21.2 Взаимодействие с подключенной консолью BIOS

Перенаправление консоли BIOS выполняется согласно спецификации VT-UTF8 на перенаправление консоли в BIOS для серверов Intel. Эта реализация соответствует функциональным требованиям Microsoft Windows 2003* WHQL для бесконсольных серверов. Перенаправление также обеспечивает необходимый уровень обратной совместимости с существующими версиями BIOS Intel для серверов и соответствует архитектурным требованиям к серверам Intel, находящимся в разработке.

BIOS для серверов имеет консоль, взаимодействующую с дисплеем и клавиатурой. BIOS определяет источники и направления входных/выходных данных в виде экранов программы настройки BIOS, экранов менеджера загрузки, теста при загрузке (POST), информационных сообщений, а также горячих клавиш и escape-последовательностей.

Выходные данные направляются на локальный компьютер и отображаются на его мониторе. Этот компьютер должен быть оснащен VGA-дисплеем, работающим в текстовом или графическом режиме. Локальные входные данные могут поступать с USB-клавиатуры. Поддержка мыши не обеспечивается.

Для перенаправления консоли через последовательный порт для каждого сервера потребуется один кабель для последовательного подключения. Кабели от разных серверов могут быть подключены к коммутатору или концентратору последовательных устройств. Таким образом, обеспечивается доступ к каждому из серверов. Системный администратор может удаленно переключаться между серверами и управлять большим количеством серверов.

С помощью функций перенаправления, реализованных в контроллере системной платы на платформах Intel®, последовательный порт UART может быть перенаправлен далее и отображен на сетевое устройство в качестве пакетного последовательного потока байтов. Эта функция контроллера системной платы называется «Перенаправление последовательного порта по локальной сети» (Serial over LAN – SOL). С помощью этой функции оптимизируются требования к размещению серверов и возможностям по управлению ими.

При перенаправлении консоли BIOS доступны дополнительные возможности, если перенаправление осуществляется через тот же последовательный порт, который определен в качестве порта доступа, и если установлен режим доступа «Всегда доступен» (Always Active) или «Перед загрузкой» (Preboot).

Переключение консоли BIOS поддерживает дополнительную контрольную последовательность выхода, которая форсирует выделение порта COM для нужд контроллера BMC. После отправки этой команды порт COM1 присоединяется к порту канала доступа на контроллере системной платы, и данные Super I/O COM1 игнорируются. Благодаря данной функции удаленные пользователи могут осуществлять мониторинг состояния POST, используя стандартные функции переключения консоли BIOS, и далее осуществлять управление перезагрузкой или включением системы, используя функции Channel Mode. Если во время POST происходит сбой, функция контрольного таймера BMC автоматически осуществляет управление портом COM1.

Символьной последовательностью, переключающей мультиплексирующее устройство на последовательный порт BMC, является «ESC O 9» (обозначенный как ^[O9) . Данная последовательность клавиш не входит в число обычных функциональных клавиш ANSI и не будет использоваться терминалом ANSI.

3.22 Wired for Management (WFM)

Wired for Management (WFM) представляет собой всеотраслевую инициативу, задачей которой является повысить общую управляемость систем и снизить общую стоимость владения. WFM позволяет управлять серверами через сеть. Для того чтобы высокоуровневое управляющее программное обеспечение могло соответствовать требованиям базовой спецификации на управление через проводные сети (Wired For Management Baseline Specification), редакция 2.0, системный BIOS поддерживает спецификацию BIOS для управления системами (*System Management BIOS Reference*) версии 2.4.

3.22.1 Поддержка PXE BIOS

BIOS поддерживает реализацию EFI PXE, описанную в главе 15 спецификации на расширяемый интерфейс встроенного ПО (*Extensible Firmware Interface Reference Specification*) версии 1.1. Для использования этих возможностей пользователю необходимо установить драйвер EFI для протокола Simple Network Protocol и драйвер UNDI для используемой сетевой платы. Драйвер UNDI поставляется вместе с сетевой платой. Драйвер протокола Simple Network Protocol можно загрузить по адресу http://developer.intel.com/technology/framework.

BIOS поддерживает старые модули памяти PXE ROM в режиме совместимости и включает необходимые PXE ROM в образ BIOS для встроенных контроллеров. Старые модули PXE ROM требуются для сетевой загрузки операционной системы, не совместимой с EFI.

3.23 BIOS системного управления (SMBIOS)

BIOS обеспечивает поддержку спецификацию BIOS для управления системами (*System Management BIOS Reference)* версии 2.4 в целях создания стандартного интерфейса для управляемых атрибутов, которые должны поддерживаться компьютерными системами с DMI. BIOS обеспечивает этот интерфейс с помощью структур данных, через которые сообщаются системные атрибуты. При помощи SMBIOS системный администратор может информацию о типах, возможностях, состоянии, дате установки и другие сведения о серверных компонентах.

4. Системное управление

4.1 Поддерживаемые функции

В этом разделе представлен общий список функций управления, поддерживаемых контроллерами-концентраторами ввода-вывода системной платы Intel® 631xESB / 632xESB.

4.1.1 Стандартные функции

Эти функции перенесены с предыдущих платформ без изменений или с незначительными изменениями.

4.1.1.1 Функции IPMI 2.0

Обратитесь к спецификации *IPMI 2.0* для получения более подробной информации о функциях, перечисленных в этом разделе.

- Контроллер BMC.
- Контрольный счетчик.
- Поддержка обмена сообщениями – включает передачу команд и поддержку пользователей/сеансов.
- Поддержка функций корпуса – включая включение/выключение питания, системный сброс и поддержку загрузочных флагов BIOS.
- Устройство обработки оповещений – включает обработку оповещений Platform Event Trap (PET) SNMP по локальной сети.
- Фильтрация сообщений платформы (PEF).
- Функции устройства получения событий – контроллер системной платы получает и обрабатывает события от других подсистем платформы.
- Функции инвентаризации резервных модулей (FRU) – контроллер системной платы обеспечивает доступ к резервным модулям (FRU) с помощью команд IPMI FRU.
- Функции ведения системного журнала событий (SEL) – контроллер системной платы поддерживает ведение SEL и обеспечивает доступ к нему.
- Функции хранилища данных, поступающих с датчиков (SDR) – контроллер системной платы обеспечивает хранение данных SDR и доступ к ним.
- Функции сканирования / мониторинга датчиков – контроллер системной платы обеспечивает управление системными датчиками посредством IPMI. Контроллер системной платы опрашивает различные датчики платформы с целью мониторинга состояния системы и информирования о ее состоянии. Контроллер обеспечивает мониторинг программных датчиков, сообщающих о состоянии системы и возникающих событиях, а также, мониторинг аппаратных датчиков.

- Интерфейсы IPMI:
  - Хост-интерфейсы – включая интерфейсы SMS (с поддержкой «очереди входящих сообщений») SMM.
  - Последовательный интерфейс – в базовом и терминальном режиме работы.
  - Интерфейс PCI-SMBus – позволяет платам расширения PCI отправлять контроллеру системной платы команды по протоколу, подобному IPMB.
  - Интерфейс IPMB.
  - Интерфейсы локальной сети – поддерживают IPMI по протоколам локальной сети (RMCP, RMCP+).
  - Serial over LAN (SOL).
  - Синхронизация состояния ACPI – контроллер системной платы отслеживает изменение состояния ACPI (обеспечивается BIOS).
  - Самотестирование контроллера системной платы – контроллер системной платы выполняет самотестирование при инициализации и в процессе работы и сообщает результаты во внешние средства.

4.1.1.2 Не-IPMI функции

В этом разделе перечислены не-IPMI функции, унаследованные от предыдущего поколения серверов.

- Мониторинг системы на основе PSMI 1.44, включая поддержку датчиков power gauge и power nozzle. Платформы предыдущего поколения поддерживали стандарт PSMI 1.42, очень близкий к стандарту PSMI 1.44).
- Поддержка загрузки с восстановлением после отказа (FRB) – FRB2 поддерживается с помощью таймера самоконтроля.
- Обновление встроенного ПО контроллера системной платы в режиме передачи встроенного ПО.
- Интерактивное обновление контроллера системной платы – обновление контроллера системной платы с поддержкой избыточного образа встроенного ПО.
- Сохранение состояния питания.
- На некоторых платформах поддерживается определение вскрытия корпуса.
- Поддержка индикаторов FRU – контроллер системной платы включает индикаторы отказа отдельных компонентов сервера.
- Базовое управление вентиляторами посредством TControl SDR версии 1.
- Мониторинг и поддержка избыточных вентиляторов.
- Мониторинг и поддержка избыточных источников питания.
- «Горячая замена» вентиляторов.
- Тестирование сигналов – контроллер системной платы обеспечивает тестовые команды для установления или получения сигналов о различных состояниях платформы.
- Издание звуковых сигналов – контроллер системной платы передает коды для различных диагностических звуковых сигналов при отказе тех или иных компонентов.

- «Горячая замена» задней панели – контроллер системной платы переводит источник питания в состояние HSC.
- Хранение и получение системных идентификаторов GUID.
- Управление передней панелью – контроллер системной платы управляет состоянием индикаторов ошибки и ID корпуса. Поддерживается блокировка некоторых функций передней панели. Мониторинг нажатия кнопок. ID корпуса может быть включен нажатием кнопки на передней панели или командой.
- Управление источником питания – поддержка датчика источника питания. С помощью этого датчика определяется, было ли отключение вызвано пропаданием питания.
- NMI – команды для установки/получения источника NMI. Поддерживает вызов NMI с помощью таймера самоконтроля, команды IPMI, или нажатия на кнопку NMI на передней панели. Мониторинг системного сигнала NMI.
- Поддержка ARP – контроллер системной платы может отправлять и получать ARP. Это поддерживается с помощью встроенного NIC контроллеров-концентраторов ввода-вывода Intel® 631xESB / 632xESB.
- DHCP – контроллер системной платы может выполнять DHCP. Это поддерживается с помощью встроенного NIC контроллеров-концентраторов ввода-вывода Intel® 631xESB / 632xESB.

4.1.2 Новые возможности

В этом разделе перечислены новые возможности, представленные на серверных системных платах с наборами микросхем Intel® серии 5000.

- Управление уровнем шума – снижение уровня шума достигнуто за счет поддержки профилей вентиляторов с использованием TControl SDR версии 2.
- Синхронизация часов контроллера системной платы с часами реального времени SIO RTC – при старте контроллера системной платы он считывает значение SIO RTC и обновляет значение встроенных часов.
- Управление вентиляторами при вскрытии корпуса – при поступлении сигнала от датчика вскрытия корпуса вентиляторы включаются на полную скорость. Эта функция поддерживается на платформах, оборудованных датчиком вскрытия корпуса.
- Поддержка модуля управления Intel® Remote Management Module (Intel® RMM) Эта плата использует собственный NIC (Intel® RMM NIC), для того чтобы обеспечить расширенные функции управления сервером в дополнение к функциям, реализуемым контроллером системной платы. Реализуются следующие возможности:
  - Использование контроллером системной платы Intel® RMM NIC посредством высокоскоростного управляющего соединения (Fast Management Link – FML). FML в качестве отдельного канала NIC для контроллера системной платы. Контроллер системной платы может с помощью этого интерфейса обеспечивать IPMI по локальной сети и SOL.
  - Передача журналов сообщений контроллером системной платы на Intel® RMM.

4.2 Система питания

Контроллер системной платы не имеет непосредственного подключения к системе управления питанием, но может блокировать действия по управлению питанием, выполняемые с передней панели или из набора микросхем. Контроллер также может инициировать изменение состояния системы питания посредством имитации нажатия кнопки питания на передней панели. Контроллер отслеживает требуемое состояние питания, поступившее из набора микросхем, и текущее состояние питания.

Ниже представлена упрощенная блок-схема, показывающая прохождение сигнала на изменение состояния питания и системный сброс на контроллере-концентраторе ввода-вывода Intel® 631xESB / 632xESB I/O.

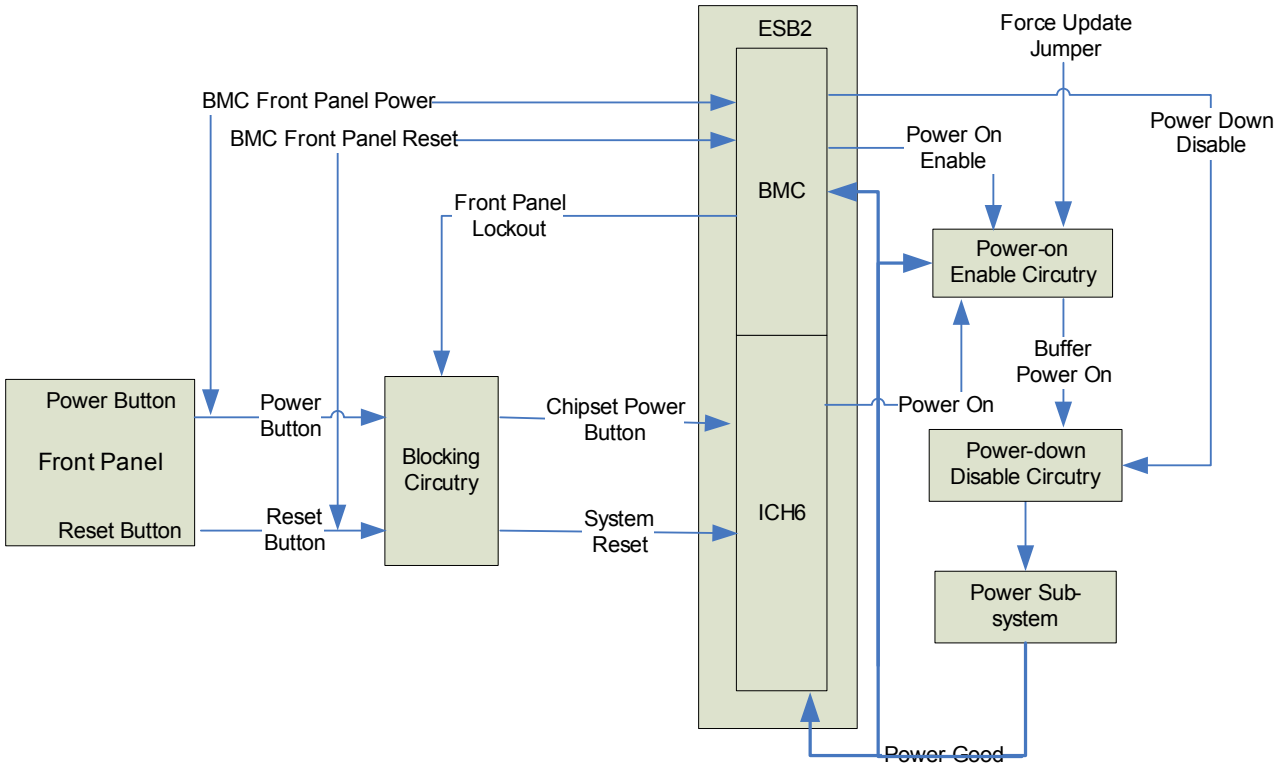


Рисунок 23. Сигналы питания и системного сброса на контроллере-концентраторе ввода-вывода Intel® 631xESB / 632xESB

4.3 Управление системным сбросом с контроллера системной платы

В следующей таблице представлены источники поступления сигнала системного сброса на контроллер системной платы и действия сервера и контроллера системной платы в каждом из случаев.

Таблица 34. Источники сигнала системного сброса и действия при поступлении этого сигнала

Источник перезагрузки	Перезагрузка системы?	Перезагрузка BMC
Включается питание режима ожидания	Нет (система еще не включена)	Да
Контроллер системной платы выходит из режима обновления встроенного ПО	Нет	Да

4.3.1 Контроллер системной платы выходит из режима обновления встроенного ПО

Встроенное ПО контроллера системной платы может быть обновлено с помощью команд обновления встроенного ПО через интерфейс LPC. Контроллер системной платы автоматически входит в режим передачи встроенного ПО при обнаружении сигнала *Force Update* (выполнить обновление) при инициализации, а также при обнаружении ошибки контрольной суммы в коде операции. После выхода из режима обновления встроенного ПО выполняется сброс контроллера системной платы. Контроллер BMC повторно синхронизируется в соответствии с состояниями сигналов управления процессором и питанием в момент его инициализации.

4.4 Инициализация системы

4.4.1 Отказоустойчивая загрузка (FRB)

Fault resilient booting (FRB) – набор алгоритмов BIOS и BMC с аппаратной поддержкой, который, при определенных условиях, позволяет загрузить микропроцессорную систему, даже в случае отказа процессора начальной загрузки (bootstrap processor, BSP).
Если алгоритмы FRB обнаруживают отказ BSP, они отключают отказавший процессор и перезагружают сервер, используя в качестве BSP другой процессор. Платформы Intel® 5000 поддерживают только FRB2 с использованием команд сторожевого таймера.

4.4.1.1 Отключение процессора

Для отключения процессора BMC генерирует соответствующий сигнал Processor Disable и перезагружает систему. Сигнал, используемый для этой цели, зависит от типа процессора.

BMC определяет наличие хотя бы одного доступного процессора. Ожидается, что на платформах, использующих один из наборов микросхем серии Intel® 5000, процессоры будут отключаться только для целей отладки.

4.4.1.2 Идентификация BSP

BSP обеспечивает точную индикацию отключенного процессора (процессоров). Он не показывает, какой процессор является BSP.

4.4.1.3 Разряды причин тайм-аута сторожевого таймера

Для выполнения алгоритмов FRB2 BIOS во время процедуры POST определяет, был ли во время предыдущей попытки загрузки тайм-аут сторожевого таймера BMC. Если он обнаружит, что происходил тайм-аут сторожевого таймера, он определяет, был ли это тайм-аут FRB2, тайм-аут ПО управления системой (system management software, SMS) или преднамеренная плановая полная перезагрузка.

4.4.1.4 FRB2

FRB2 запускает алгоритм FRB, который обеспечивает обнаружение отказов системы, таких как зависание, во время процедуры POST. BIOS использует сторожевой таймер BMC для возможности отката во время процедуры POST. BIOS конфигурирует сторожевой таймер, чтобы показать, что он использует таймер для фазы FRB2 процесса загрузки.

После того как BIOS идентифицировал и сохранил информацию BSP, он устанавливает разряд использования таймера FRB2 и загружает в сторожевой таймер новое значение счетчика времени.

Если счетчик сторожевого таймера обнулится, и при этом установлен разряд использования таймера FRB2, BMC (если он соответствующим образом сконфигурирован) регистрирует событие обнуления счетчика сторожевого таймера, установив в байтах данных события значение «тайм-аут FRB2». Затем BMC запускает полную перезагрузку системы, если в качестве реакции на тайм-аут сторожевого таймера BIOS установил перезагрузку.

BIOS отвечает за отключение значения «тайм-аут FRB2» перед инициализацией сканирования дополнительного ПЗУ и перед выводом запроса пароля для загрузки. Если процессор отказал, и произошло событие «тайм-аут FRB2», BMC перезагружает систему.

BIOS получает от контроллера BMC информацию о состоянии истечения времени контрольного таймера (что является частью его нормальной работы). Если это состояние показывает обнуление счетчика таймера FRB2, BIOS создает запись в системном журнале регистрации событий, которая сообщает об отказе FRB2. В байтах OEM записи о событии содержится последний код ошибки POST, который был сгенерирован во время предыдущей попытки загрузки. Отказ FRB2 не отражается на значении датчика состояния процессора.

Хотя отказ FRB2 вызывает события, которые фиксируются в системном журнале регистрации событий, он не отображается на индикаторах передней панели.

4.5 Интегрированный пользовательский интерфейс передней панели

BMC включает функции интерфейса передней панели и поддерживает модель, совместимую с SSI EB. Индикация на передней панели обеспечивается светодиодными индикаторами.

4.5.1 Световой индикатор питания

Светодиодный индикатор питания зеленого цвета светится, если включено питание системы постоянным током. Светодиодный индикатор питания управляется BIOS. Светодиодный индикатор питания отражает сочетание состояния питания системы постоянным током и состояния интерфейса ACPI. В следующей таблице показаны допустимые состояния.

Таблица 35. Состояния светодиодного индикатора питания

Состояние	Интерфейс ACPI	Световой индикатор питания
Отключен	Нет	Не горит
Питание включено	Нет	Включен
S4 / S5	Да	Не горит
S1 Sleep	Да	Мигает
S3 Sleep	Да	Мигает
S0	Да	Включен

4.5.2 Индикатор состояния системы

Светодиодный индикатор состояния системы является двухцветным. Зеленый цвет (состояние) используется для индикации нормальной работы или работы в условиях ухудшения характеристик. Желтый цвет (отказ) показывает состояние аппаратного обеспечения платформы и перекрывает зеленый цвет.

Когда питание сервера отключено (переход к состоянию отключения питания постоянным током или в режим S5), BMC остается в ждущем режиме и поддерживает состояния датчика и светодиодного индикатора на передней панели, установленные перед событием отключения питания.

После включения питания системы переменным током и появления питания режима ожидания напряжением 5 В, начинается инициализация контроллера BMC, которая занимает 15-20 секунд. В течение этого времени индикатор состояния системы мигает зеленым и оранжевым, а кнопка питания на панели управления отключается для предотвращения включения сервера. После завершения инициализации BMC индикатор состояния прекращает мигать и кнопку питания снова можно использовать для включения сервера.

Примечание: *Светодиодный индикатор состояния системы отображает состояние текущего, самого серьезного отказа. Например, если произошел критический отказ по одной причине и некритический отказ по другой причине, светодиодный индикатор состояния системы будет светиться ярко (состояние критического отказа).*

В следующей таблице показано соответствие состояния платформы и состояния светодиодного индикатора состояния системы.

Таблица 36. Состояния светодиодного индикатора состояния системы

Цвет	Состояние	Критичность	Описание
Не горит	Нет	Не готов	Отключение питания переменного тока
Зеленый / Оранжевый	Мигание	Не готов	Перед подключением питания постоянного тока – 15-20 секунд инициализации контроллера BMC при подаче тока на сервер. До завершения инициализации BMC кнопки панели управления заблокированы.
Зеленый	Включен	Система в нормальном состоянии	Система загружена и готова к работе.
Зеленый	Мигает	Деградация	Деградация системы 1) Не удается использовать весь установленный объем памяти (если установлено несколько модулей DIMM). 2) Количество исправимых ошибок превысило пороговое значение 10, и система переключилась на резервный модуль DIMM (резервирование памяти). Это означает, что идет работа на резервном модуле DIMM, т.е. избыточность потеряна. Должен загореться соответствующий индикатор DIMM. 3) В конфигурации с зеркальным набором, когда теряется избыточность. 4) Потеря избыточности блока питания или вентиляторов. Не относится к подсистемам без избыточности. 5) Ошибки соединений PCI-e 6) Ошибка/отключение процессора – при ошибке одного из двух процессоров 7) Сигнал вентилятора – Ошибка вентилятора Число рабочих вентиляторов должно быть больше минимального необходимого числа 8) Превышен некритический порог – Температура и напряжение

Цвет	Состояние	Критичность	Описание
Желтый	Мигает	Не критическое	Некритическое оповещение – Возможен сбой системы 9) Превышен критический порог напряжения 10) Сигнал перегрева VRD 11) В системе недостаточно вентиляторов 12) Превышение порога из 10 устранимых ошибок в режиме без резервирования и без зеркального набора
Желтый	Включен	Критическое или невосстановимое состояние	Критическое оповещение – Ошибка или отключение системы 13) Ошибка DIMM при использовании одного модуля DIMM, в системе нет работоспособных модулей памяти 14) Неустранимая ошибка памяти в режиме без резервирования 15) Сигнал IERR 16) Отсутствует процессор Processor 1 17) Превышение критических ограничений температуры (CPU ThermTrip, memory TempHi) 18) Нет сигнала power good – ошибка питания 19) Ошибка конфигурации процессора (например, несоответствие степпинга)

Примечание: *Функции резервирования и зеркального отражения памяти в настоящее время не поддерживаются, их поддержка будет реализована после начала производства.*

4.5.3 Световой индикатор идентификации корпуса

Светодиодный индикатор идентификации корпуса обеспечивает визуальную индикацию обслуживаемой системы. Он переключается кнопкой идентификации корпуса.

Таблица 37. Состояния светодиодного индикатора идентификации корпуса

Состояние	Состояние индикатора
Определение активности с помощью кнопки	Включен
Не горит	Не горит

4.5.4 Входы передней панели / корпуса

BMC производит мониторинг кнопок передней панели и других сигналов корпуса. Входные кнопки на передней панели вызывают кратковременное замыкание контактов, которое обрабатывается встроенным ПО процессора BMC.

4.5.4.1 Вскрытие корпуса

Серверные платформы, использующие один из наборов микросхем серии Intel® 5000, поддерживают обнаружение проникновения в корпус. BMC производит мониторинг состояния сигнала проникновения в корпус и делает его доступным. При изменении состояния сигнала проникновения в корпус (если эта опция доступна) BMC генерирует сообщение о событии, связанном с датчиком.

Если сигнал проникновения в корпус активен, BMC повышает скорость всех вентиляторов. Скорость вентиляторов возвращается на предыдущий уровень, когда сигнал проникновения в корпус становится неактивным. Это позволяет обеспечить достаточную вентиляцию в том случае, если технический специалист снимает крышку для обслуживания устройства.

4.5.4.2 Кнопка питания

Сигнал кнопки питания используется для включения и выключения питания системы. Нажатие кнопки вызывает кратковременное замыкание контактов на передней панели. Сигнал направляется к BMC как двунаправленный сигнал, мониторинг которого производится BMC после того, как BMC обработал сигнал. Он также направляется в набор микросхем, блокируя схему, которая позволяет BMC блокировать сигнал. Набор микросхем реагирует на нажатие кнопки, а не на ее отпускание.

Если блокировка передней панели включена и активна, нажатие кнопки питания не вызывает включения или выключения питания системы. Вместо этого будет создана запись в системном журнале регистрации событий. Подробную информацию о защищенном режиме см. в разделе 4.5.5.

4.5.4.3 Кнопка Reset

Активизация на передней панели сигнала перезагрузки для BMC приводит к сбросу и перезагрузке системы, т.к. BMC не заблокировал этот вход. Этот процесс начинается немедленно и не согласуется с ПО и операционной системой.

Кнопка Reset представляет собой быстродействующий контактный выключатель на передней панели. При нажатии кнопки через разъем передней панели направляется сигнал на BMC, отслеживающий и принимающий его.

Если включена блокировка передней панели, нажатие кнопки не приведет к перезагрузке системы. Вместо этого будет создана запись в системном журнале регистрации событий.

4.5.4.4 Диагностическое прерывание (немаскируемое прерывание передней панели)

Как указано в спецификации IPMI 2.0, «диагностическое прерывание – это немаскируемое прерывание или сигнал, для генерации диагностической трассировки и дампов памяти, занимаемой ОС». Для платформ, использующих один из наборов микросхем серии Intel® 5000, это немаскируемое прерывание.

Кнопка диагностического прерывания подключена к контроллеру BMC через разъем передней панели. Нажатие кнопки диагностического прерывания вызывает следующие действия BMC:

- Генерируется сообщение о критическом событии.
- Генерируется импульс системного немаскируемого прерывания.

После того, как BMC сгенерировал немаскируемое прерывание, он не будет выполнять никаких действий до тех пор, пока система не будет перезагружена или выключена.

BMC автоматически сбрасывает флаг сообщения OEM 1 и источник немаскируемого прерывания, когда обнаруживает факт перезагрузки системы или перезагружается сам. Кнопка диагностического прерывания не отключается или не отменяется каким-либо другим образом, если система находится в режиме блокировки передней панели.

4.5.4.5 Идентификация корпуса

Кнопка идентификации корпуса на передней панели позволяет переключать состояние светодиодного индикатора идентификации корпуса. Если этот индикатор не светится, после нажатия кнопки идентификации корпуса он будет светиться. Светодиодный индикатор будет светиться до следующего нажатия кнопки.

4.5.5 Функция блокировки передней панели

Функция блокировки передней панели обеспечивает защиту кнопок передней панели от неавторизованного использования или доступа. Режим блокировки передней панели включается и управляется системным BIOS. Если режим блокировки передней панели разрешен и активен, при нажатии кнопки на передней панели будет сгенерировано событие.

Блокировка передней панели позволяет защитить от неавторизованного использования или доступа определенные кнопки на передней панели. Эта защита включает блокировку кнопок и генерацию сообщений о нарушениях при нажатии кнопки на передней панели в режиме блокировки передней панели. Поддержка доступна только для защиты кнопок питания и перезагрузки на передней панели. Эти кнопки нельзя блокировать отдельно.

Набор кнопок, защищаемых в режиме блокировки передней панели, зависит от состояния питания ACPI.

Таблица 38. Сравнение защищенного режима и состояния ACPI

Состояние ACPI	Кнопка питания	Кнопка Reset	Кнопка диагностического прерывания (Кнопка NMI на передней панели)	Кнопка включения идентификационного индикатора
S0	Защищен	Защищен	Не защищено	Не защищено
S1 / S3	Не защищено	Не защищено	Не защищено	Не защищено
S4 / S5	Не защищено	Не защищено	Не защищено	Не защищено

4.6 Частные шины управления I^2C

BMC управляет несколькими индивидуальными шинами I^2C. BMC является единственным контроллером для этих шин.

4.7 Контрольный счетчик

В BMC имеется сторожевой таймер, полностью совместимый с интерфейсом IPMI 2. Подробная информация содержится в спецификации IPMI. Немаскируемое / диагностическое прерывание, определенное для сторожевого таймера IPMI 2.0 связано с немаскируемыми прерываниями для платформ IA-32. Прерывание SMI перед наступлением тайм-аута сторожевого таймера (или активизация эквивалентного сигнала) не поддерживается платформами, использующими один из наборов микросхем серии Intel® 5000.

4.8 Журнал событий системы (SEL)

В BMC реализована логическая система журнала событий, соответствующая *спецификации IPMI 2.0.* Доступ к SEL может осуществляться по всем каналам связи. Таким образом внеполосные интерфейсы могут получать доступ к информации системного журнала регистрации событий, если сервер выключен.

Для хранения информации о системных событиях BMC выделяет 65536 байт (64 КБ) энергонезависимой памяти. Каждая запись системного журнала регистрации событий дополняется временной отметкой длиной 4 байта, который показывает время удаления записи. Таким образом, длина каждой записи системного журнала регистрации событий равна 20 байт. Это означает, что одновременно может храниться 3276 записей системного журнала регистрации событий. При попытке добавить запись в системный журнал регистрации событий, если в нем уже хранятся 3276 записей, происходит ошибка, и возвращается код завершения «Недостаточно памяти».

4.8.1 Служебные события

При очистке системного журнала регистрации событий могут генерироваться события. BMC поддерживает очередь сообщений о событиях, чтобы предотвратить потерю сообщений. Сообщения, находящиеся в очереди, не затираются.

BMC распознает дубликаты сообщений о событиях, сравнивая порядковый номер и источник сообщения. Дополнительную информацию можно найти в спецификации IPMI 2.0. BMC отбрасывает (фильтрует) дубликаты сообщений о событиях после того, как они будут считаны из очереди сообщений о событиях. Это значит, что в очереди могут находиться дубликаты событий.

4.8.2 Очистка SEL

Очистка системного журнала регистрации событий происходит в фоновом режиме. События, регистрируемые в журнале SEL в процессе удаления, будут находиться в очереди событий до завершения удаления, а затем будут записаны в журнал SEL.

При удалении SEL генерируется событие отключения датчика регистрации событий.

4.8.3 Часы и временные метки

В контроллере BMC имеются внутренние часы с четырехбайтовой временной меткой, которые используются журналом SEL и подсистемой SDR. Приращение импульсов происходит каждую секунду.

4.8.3.1 Инициализация и синхронизация часов

Если питание режима ожидания контроллера BMC отключается, то при восстановлении питания контроллер BMC считывает показания часов реального времени (RTC) суперконтроллера ввода/вывода и использует это значение для обновления внутренних системных часов контроллера. Часы используются для установки временных меток в журнале SEL и программируемого пробуждения системы.

Системные часы, используемые BIOS и операционной системой, основаны на часах реального времени в компоненте ICH набора микросхем Intel® 5000, а не на компоненте SIO, используемом BMC для инициализации часов. В связи с этим возможно существование проблем синхронизации часов BMC и часов реального времени. В некоторых случаях BIOS обновляет часы BMC. Это устраняет возможные проблемы несоответствия, как описано ниже:

- Система загружается: При каждой загрузке системы BIOS проверяет часы BMC и обновляет их, только если их время неточное. Это позволяет сократить число записей в журнале SEL.
- Обработчик SMI: BIOS программирует набор микросхем для генерирования прерываний SMI при выключении операционной системы (переход в режим S3, S4 или S5). Это необходимо для того, чтобы загрузить информацию о состоянии режима сна в контроллер BMC. При отправке прерывания SMI BIOS считывает время с часов реального времени и обновляет часы контроллера BMC.

Когда контроллер BMC принимает команду *Set SEL Time*, он обновляет часы реального времени контроллера SIO в соответствии с системным временем. Это помогает обеспечить синхронизацию часов реального времени контроллера BMC с системными часами реального времени.

При изменении системного времени (например, времени, установленного через интерфейс операционной системы) часы контроллера BMC не синхронизируются повторно до тех пор, пока операционная система не выключает сервер или пока сервер не перезагружается, если происходит внеплановое выключение.

4.9 Хранилище записей показаний датчиков (SDR)

В контроллере BMC используется логическое хранилище SDR, соответствующее *спецификации интеллектуального интерфейса управления платформой IPMI 2.0*. Хранилище SDR доступно по всем коммуникационным каналам. Благодаря этому возможен доступ к информации в хранилище SDR, когда система отключена.

BMC выделяет 65536 байт (64 КБ) памяти долговременного хранения для записей SDR.

4.9.1 Агент инициализации

В контроллер mBMC интегрированы функции агента инициализации в соответствии со Спецификацией интеллектуального интерфейса управления платформами, версия 2,0. Во время инициализации контроллера BMC при загрузке системы производится сканирование хранилища SDR и настройка устройств IPMB с записями контроллера управления. При этом настраиваются пороговые показания датчиков, включается/отключается проверка сообщений о событиях датчиков и включаются/отключаются сами сообщения об событиях датчиков.

В процессе инициализации микроконтроллеры IPMB заново включают генерирование событий. Иногда при этом на контроллер BMC отправляются дублирующие события. Механизм обнаружения и удаления дублирующихся событий в контроллере BMC должен предотвращать регистрацию всех сообщений с дублирующимися событиями.

4.10 Блок инвентаризации FRU

Контроллер управления BMC содержит интерфейс для связи с логическими устройствами FRU в соответствии со *Спецификацией интеллектуального интерфейса управления платформами, версия 2.0.* Эта функция содержит команды, используемые для доступа и управления инвентаризационной информацией FRU. Эти команды могут отправляться через любые интерфейсы.

Контроллер BMC предоставляет устройствам FRU командный доступ к собственному устройству FRU и ко всем устройствам FRU на сервере. Контроллер BMC контролирует соответствие идентификатора устройства FRU физическому устройству. В соответствии со спецификацией IPMI, устройство FRU 0 всегда располагается на серверной плате.

4.11 Генерирование диагностических и звуковых сигналов

BMC при этом может генерировать звуковые коды. Звуковые коды звучат каждый раз при обнаружении проблемы (например, при загрузке), но не непрерывно. Коды, встречающиеся во всех платформах, использующих наборы микросхем Intel® серии 5000, перечислены в таблице ниже. Каждая цифра кода представляется в виде серии гудков, количество которых равняется цифре.

Таблица 39. Звуковые сигналы BMC

Описание	Причина гудка	Датчики	Поддерживается?
1-5-2-1	Процессор: Пустой разъем / ошибка установлена – Нет процессора в разъеме 1	Ошибка установки процессора	Да
1-5-2-2	Процессор: Нет процессоров (только терминаторы)	Нет	Нет
1-5-2-3	Процессор: Ошибка конфигурации, например, несоответствие кода VID	Нет	Нет
1-5-2-4	Процессор: Ошибка конфигурации, например, несоответствие BSEL	Нет	Нет
1-5-4-2	Сбой питания: Неожиданное отключение питания постоянного тока (ошибки управления питанием)	Источник питания – ошибка источника питания	Да
1-5-4-3	Ошибка набора микросхем	Нет	Нет
1-5-4-4	Ошибка управления питанием	Программный сбой управления блоком питания	Да

4.12 NMI

На платформах IA-32 контроллер BMC выполняет функцию мониторинга и генерирования сигнала NMI. При генерировании контроллером BMC диагностического прерывания подается сигнал NMI. Датчики диагностического прерывания с передней панели используются для регистрации событий SEL для диагностического прерывания.

Примечание: *Диагностическое прерывание также называют диагностическим прерыванием передней панели или прерыванием NMI (немаскируемым диагностическим прерыванием).*

4.12.1 Генерирование сигнала

Контроллер BMC генерирует сигнал NMI при определенных условиях. Длительность сигнала NMI, генерированного контроллером BMC, составляет не менее 30 мс. После генерирования сигнала NMI контроллером BMC контроллер BMC не генерирует другой сигнал до перезагрузки или выключения системы. Генерирование сигнала NMI контроллером BMC можно отключить в BIOS. Контроллер BMC генерирует импульсы NMI в следующих случаях:

- Нажатие кнопки диагностического прерывания на передней панели. Для получения дополнительной информации обратитесь к Разделу 4.5.4.4.
- Запись в таблице PEF, соответствующая событию, где запись фильтра указывает на диагностическое прерывание.
- Предварительное время контрольного счетчика истекло, диагностическое прерывание NMI при истечении предварительного времени включено.

4.13 Датчики процессора

Контроллер BMC обеспечивает работу датчиков IPMI для процессоров и сопутствующих компонентов, в том числе стабилизаторов напряжения и вентиляторов. Большинство из этих датчиков устанавливаются для каждого процессора.

Таблица 40. Датчики процессора

Тип датчика	Разъем для процессора	Описание
Статус процессора	Да	Присутствие процессора, наличие ошибок
Температура процессора	Да	Температура самого процессора. Температура на датчике TDIODE или температура, регистрируемая интерфейсом PECI, в зависимости от семейства процессора
Индикация превышения температуры стабилизатора напряжения процессора	Да	Дискретный датчик, показывающий превышение стабилизатором напряжения процессора верхнего порога рабочей температуры
Напряжение процессора	Да	Датчик порогового напряжения стабилизатора напряжения процессора
Превышение ограничений напряжения процессора	Да	Дискретный датчик, показывающий, что напряжение процессора вышло за пределы диапазона
Processor Fan Speed	Да	Скорость вентилятора процессора с теплоотводом (не всегда присутствует в системе)
Управление температурой процессора (Prochot)	Да	Доля времени работы процессора в другом режиме быстродействия в связи с высокой температурой
Ошибка конфигурации процессора	Нет	Неправильная установка процессора в разъем. Это означает, что разъем 1 пустой

4.13.1 Датчики состояния процессора

Контроллер BMC обеспечивает работу датчика IPMI типа «Процессор», отвечающего за мониторинг информации о состоянии каждого разъема процессора, поддерживаемого платформой.

При возникновении любого события (сигнала датчика), за исключением сигнала присутствия процессора, этот сигнал остается активным до одного из следующих событий:

- Включение опции processor retest в программе BIOS setup.
- Выключение и включение питания.

Включение и перезагрузка системы не перезагружают датчики состояния процессора.

Таблица 41. Требования к состоянию процессора

Статус процессора	Обнаружено
IERR	BMC
Температурное нарушение	BMC
FRB2 / ошибка зависания процедуры POST	BIOS[1]
Ошибка конфигурации (например, несоответствие степпингов)	BIOS
Обнаружено присутствие процессора	BMC

Примечание 1: Ошибка не отражается датчиком состояния процессора на платформе, использующей набор микросхем серии Intel® 5000

4.13.1.1 Присутствие процессора

Когда контроллер BMC обнаруживает пустой разъем процессора, он устанавливает бит отключения для состояния процессора в этом разъеме, и удаляет другие биты состояния процессора, в том числе постоянные.

При инициализации контроллера BMC он проверяет наличие процессора. При инициализации контроллера BMC регистрируется одно событие обнаружения для каждого обнаруженного процессора.

4.13.2 Датчик превышения температуры стабилизатора напряжения процессора

Этот датчик отслеживает сигнал, показывающий превышение стабилизатором напряжения процессора верхнего порога рабочей температуры Состояние этого сигнала передается на контроллер системного управления National Semiconductor* LM94, подающий соответствующий сигнал Prochot и понижающий температуру стабилизатора напряжения. Состояние сигнала не передается на подсистему управления вентиляторами. Это отношение построено по принципу 1:1; при подаче сигнала перегрева VRD-hot подается сигнал Prochot.

4.13.3 Мониторинг состояния ThermTrip

Контроллер BMC отвечает за ведение журнала подачи сигнала ThermTrip для каждого процессора. В этом журнале записываются все случаи подачи сигнала ThermTrip с момента последней перезагрузки датчика процессора или тестирования процессоров.

При возникновении такого события контроллер BMC запрашивает статус ThermTrip для каждого процессора. Если контроллер BMC обнаруживает состояние ThermTrip, он устанавливает состояние ThermTrip для соответствующего датчика состояния процессора. После этого системные устройства предпринимают попытку выключить питание датчика.

4.13.4 Поддержка интерфейса PECI

4.13.4.1 Значение температуры PECI

Значение температуры PECI представляет собой отношение текущего значения температуры к пороговой температуре процессора. Это значение всегда составляет не более 0. С увеличением температуры процессора уменьшается модуль отрицательного значения PECI до тех пор, пока оно не достигнет нуля. Когда температура процессора достигает температуру Prochot или превышает ее, значение температуры PECI будет равняться нулю.

4.13.4.1.1 Поддержка PECI датчиками IPMI

- **Два датчика температуры на каждый процессор**: Поскольку эти серверы и рабочие станции должны поддерживать процессоры, работающие в режиме PECI или в режиме без PECI, для каждого процессора используется два датчика температуры IPMI. Один датчик предназначен для PECI, а другой – для термодиодов. Одновременно могут работать только два датчика температуры (PECI или термодиода), в зависимости от того, SDR какого датчика загружены в систему. Процессоры с поддержкой PECI поддерживают только PECI SDR. При переходе с процессоров без поддержки PECI на процессоры с поддержкой PECI необходимо перезагрузить SDR для получения точных показаний температуры.
- **Показания датчиков IPMI для PECI**: Датчики температуры процессора IPMI, отслеживающие термодиоды, передают абсолютное значение температуры. Однако при использовании процессоров с поддержкой PECI датчики температуры процессора IPMI передают относительные значение, не превышающие 0.
- **Обнаружение датчиков PECI:** Датчики PECI имеют код типа (01h) = temperature и максимальное показание датчика 0 градусов Цельсия. Если программному обеспечению требуется определить, является ли датчик температуры датчиком PECI, оно преобразует максимальное значение датчика в SDR и проверяет, равняется ли оно 0 градусов Цельсия.
- **Название датчика PECI:** Датчики PECI в системах Intel S5000 имеют название Px Therm Margin, где «x» – номер процессора в системе. Например: Датчик процессора 1 будет иметь название P1 Therm Margin.
- **Пороговые значения PECI:** Для датчиков PECI не назначаются пороговые значения.

4.13.5 Поддержка PROCHOT

4.13.5.1 Датчик температуры PROCHOT

На этих серверах и рабочих станциях датчик PROCHOT указывает количество времени, в течение которого процессор работает в состоянии пониженного быстродействия за фиксированный срок. При нормальной работе показания этого датчика равняются 0, указывая, что процессор работает в нормальном режиме. При увеличении температуры процессора увеличивается количество времени, проведенное процессором в состоянии пониженного быстродействия, вплоть до уровня 100%.

4.13.5.1.1 Поддержка PROCHOT датчиком IPMI

- **Временной диапазон PROCHOT:** Датчик PROCHOT измеряет процентную долю времени работы отдельного процессора в режиме пониженного быстродействия за период в 5,8 секунд.
- **Обнаружение датчиков PROCHOT:** Датчики PROCHOT имеют код типа (01h) = temperature, но выдают показания в процентах. Это определяется посредством считываний бита 0 поля «sensor units 1» в PROCHOT SDR. Если бит 0 этого байта имеет значение 1b, это означает, что единицей измерения датчика являются проценты. Это стандартный метод, используемый IPMI для определения того, следует ли считывать показания датчика в процентах.
- **Название датчика PROCHOT:** В системах Intel S5000 датчики PROCHOT имеют название Px Therm Ctrl %, где «x» – номер процессора в системе. Например: Датчик процессора 1 будет иметь название P1 Therm Ctrl %.
- **Пороговые значения PROCHOT:** Датчики PROCHOT имеют верхнее пороговое значение и должны рассматриваться, как обычные датчики с пороговым значением.

4.13.6 Мониторинг IERR

Контроллер BMC осуществляет мониторинг сигнала IERR, подаваемого каждым процессором, и приводит его в соответствие с состоянием IERR соответствующего датчика состояния процессора.

4.13.7 Мониторинг динамического напряжения процессора

Процессоры поддерживают динамический режим работы, когда VID процессора могут изменяться по командам программ или при изменении рабочих условий. Контроллер BMC не нуждается в динамическом изменении порогов напряжения для прямого мониторинга напряжения процессора. Однако контроллер системного управления National Semiconductor* LM94 поддерживает мониторинг динамического напряжения. Контроллер BMC считывает реестр состояния контроллера системного управления LM94, который указывает, что напряжение процессора не превышает допустимые ограничения.

4.13.8 Мониторинг температуры процессора

Процессоры, используемые с платформами на базе наборов микросхем Intel® серии 5000 являются двухъядернгыми, и в них используется один физический датчик температуры на каждое ядро. Контроллер BMC объединяет данные датчиков температуры процессора в одном датчик температуры IPMI для каждого разъема процессора. Более высокое значение температуры используется как значение датчика IPMI.

4.13.9 Мониторинг управления температурой процессора (Prochot)

Контроллер BMC выполняет мониторинг управления температурой каждого процессора. Эта функция реализована через контроллер системного управления National Semiconductor* LM94, передающий данные о процентной доле времени, в течение которого подается сигнал *ProcHot* в указанном временном диапазоне. В контроллере BMC эта схема реализована, как пороговый датчик для каждого процессора.

4.13.10 Датчик ошибок установки процессора

Контроллер BMC выполняет только проверку установки процессора в разъем 1. В этом состоянии действует аппаратный запрет на включение питания сервера.

При инициализации контроллера BMC для этого датчика устанавливается отключенное состоянние. После этого контроллер BMC проверяет ошибки установки процессора и устанавливает соответствующее новое значение. При обнаружении ошибки и соответствующей конфигурации SDR регистрируется событие SEL. Контроллер BMC проверяет состояние неисправности и обновляет состояние датчика при каждой попытке включения питания системы. При каждой попытке включения питания постоянного тока при обнаружении ошибки генерируется звуковой сигнал. Звуковые сигналы BMC приведены в Таблица 39.

Примечание: *Это датчик с автоматическим сбросом, но он не сбрасывается при включении питания системы постоянным током или при перезагрузке системы. Правильный метод сброса этого датчика – решение проблемы с помощью отключения источника питания переменного тока сервера, установки процессора в разъем 1 и включения источника питания переменного тока сервера.*

4.14 Стандартное управление вентилятором

Контроллер BMC управляет системными вентиляторами и выполняет мониторинг их работы. Для каждого вентилятора предусмотрен датчик скорости вентилятора, который позволяет обнаружить отказ вентилятора. В некоторых платформах также предусмотрено определение наличия вентиляторов, которое выполняется BMC с помощью датчиков наличия для каждого вентилятора. Дополнительная информация содержится в технических характеристиках системных плат Intel® для серверов и рабочих станций, относящихся к Вашей продукции.

BMC может управлять скоростью вращения некоторых вентиляторов, если предусмотрена такая возможность. Управляемые вентиляторы разделены на группы. Для каждой группы предусмотрен отдельный механизм управления скоростью вращения вентиляторов и отдельная политика управления, которую можно сконфигурировать для каждой группы.

Для группы вентиляторов может быть определен связанный с ней набор датчиков температуры и скорости вращения вентиляторов. Эти датчики используются для определения текущего состояния группы вентиляторов. Группа вентиляторов может иметь три состояния: режим ожидания, рабочий режим и ускоренный режим. В режиме ожидания и в ускоренном режиме вентиляторы вращаются с фиксированной скоростью, которую, однако, можно сконфигурировать. В рабочем режиме вентилятор вращается с переменной скоростью, определяемой политикой группы вентиляторов (см. раздел 4.14.1, Рабочий режим вентиляторов). Для конфигурирования политики группы вентиляторов используется запись OEM списка датчиков SDR (см. раздел 4.14.1).

Примечание: *Дополнительную информацию можно найти в технических характеристиках сервера или рабочей станции, входящих в комплект поставки Вашей продукции.*

Состояние группы вентиляторов определяется несколькими факторами. Ниже перечислены эти факторы в порядке приоритетов, от высшего к низшему:

Ускоренный режим:

- Соответствующий вентилятор находится в критическом или в невосстановимом состоянии в конфигурации вентиляторов без резервирования.
- Группа вентиляторов имеет недостаточное количество ресурсов в конфигурации вентиляторов с резервированием.
- Любой датчик температуры находится в критическом или в невосстановимом состоянии, за исключением датчиков контроля температуры процессора (Processor Thermal Control Monitoring, Prochot) и перегрева VRD (VRDHot).

Режим сна:

- Ускоренный режим недоступен, если система находится в состояниях ожидания ACPI S1 и S3, и контроллер BMC сконфигурирован для перевода групп вентиляторов в режим ожидания.

Номинальный:

- См. Раздел 4.14.1.

4.14.1 Рабочий режим вентиляторов

Возможно задать как фиксированную скорость вращения вентиляторов в группе, так и переменную скорость, управляемую одним или несколькими связанными с этой группой датчиками.

Для конфигурирования датчиков температуры, которые будут связаны с определенной группой вентиляторов, а также для задания отношения (алгоритма) между температурой и значением скорости вращения вентилятора (PWM), используются записи OEM SDR. Несколько записей OEM SDR могут ссылаться на одну и ту же группу вентиляторов и управлять ей, и несколько записей OEM SDR могут ссылаться на одни и те же датчики температуры.

Значение PWM для данной группы вентиляторов рассчитывается с использованием одного или нескольких ступенчатых линейных алгоритмов и алгоритмов фиксации уровня. Переход от одной рассчитанной рабочей скорости вращения вентилятора (значения PWM) к другой происходит плавно, чтобы избежать звукового эффекта при переходе. Длительность перехода устанавливается в записи OEM SDR.

Для каждой группы вентиляторов можно определить несколько аддитивных и фиксирующих алгоритмов управления, которые будут использоваться одновременно. При вычислении общего значения PWM для каждой группы вентиляторов контроллер BMC использует максимальное значение, рассчитанное с помощью определенных для этой группы ступенчатых линейных алгоритмов и суммирует значения, рассчитанные с помощью алгоритмов фиксации, за исключением случаев, когда один из ступенчатых линейных алгоритмов сконфигурирован так, чтобы всегда поддерживать максимальную скорость вращения вентиляторов группы.

Можно задать параметр запаздывания, чтобы минимизировать колебания скорости вращения вентиляторов, а также повысить плавность изменения скорости. Его применение описано ниже вместе с методами изменения скорости вращения вентиляторов. Если унаследованный формат записи TCONTROL SDR не поддерживает установку параметра запаздывания, BMC установит значение запаздывания, равное 0.

4.14.2 Ступенчатые линейные алгоритмы

4.14.2.1 Регулировка скорости вращения вентиляторов

Каждая подзапись TCONTROL в описании ступенчатого линейного алгоритма определяет таблицу соответствия показаний датчиков температуры и скоростей вращения вентилятора. Элементы таблицы необходимо располагать в порядке возрастания температуры. Контроллер BMC просматривает таблицу с конца до тех пор, пока не найдет значение температуры, меньшее или равное текущему показанию датчика температуры. Скорость соответствующего вентилятора в группе вентиляторов, связанной с этой подзаписью, изменится.

Параметр запаздывания применяется к рассчитанной разнице между предыдущим и текущим показаниями датчика. Если эта разница положительная, температура повышается, и заданное положительное значение параметра запаздывания вычитается. В противном случае, если эта разница отрицательная или равна нулю, прибавляется заданное отрицательное значение параметра запаздывания.

Если применение параметра запаздывания изменяет вычисленное значение разницы с положительного на отрицательное, или с отрицательного или нулевого на положительное, используется прошлое вычисленное значение скорости, а не новое. Такой подход отличается от интерпретации запаздывания на основе пороговых показаний датчиков, но все равно достигается желаемый результат - предотвращение колебаний скорости вращения вентилятора.

Основа для определения окончательной скорости вращения вентиляторов каждой группы – максимальное из рассчитанных значений для всех шаговых линейных подзаписей TCONTROL, действующих для активного профиля данной группы. К этому базовому значению прибавляются все значения, рассчитанные по действующим в текущий момент алгоритмам фиксации.

4.14.2.2 Максимальное значение скорости вентиляторов группы

В подзаписях TCONTROL для шаговых линейных алгоритмов может быть установлен флаг, который показывает, что этот алгоритм предусматривает максимальное значение скорости вентиляторов группы. Эти подзаписи не участвуют в расчете скорости вентиляторов, как было описано выше. Вместо этого, скорость вентилятора, вычисленная с помощью таблицы соответствия, сохраняется для ссылок в дальнейшем. После расчета окончательной скорости вращения вентиляторов группы, если необходимо, она может быть снижена до максимального значения, установленного для этой группы. Для подзаписей с установленным максимальным значением скорости для домена параметр запаздывания не применяется.

4.14.3 Фиксирующие алгоритмы

Подзаписи TCONTROL для фиксирующих алгоритмов содержат одно значение температуры, и служат указанием для BMC на увеличение скорости вентиляторов соответствующей группы при необходимости, чтобы поддерживать показание связанного с ней датчика температуры ниже фиксированного значения. Если показание датчика превышает фиксированное значение, скорость вращения вентилятора будет расти во времени до тех пор, пока он не достигнет максимальной скорости, или температура не опустится ниже порогового значения. Если значение температуры упало ниже порогового значения, вклад этого датчика в расчет скорости вращения в течение некоторого времени будет сокращаться, пока не станет равным нулю. Длина шага изменения скорости вращения вентиляторов задается в подзаписях.

Эти подзаписи позволяют указать значение частоты снятия отсчётов ниже значения частоты перерасчета скорости вращения. Такая возможность используется для задания времени, в течение которого группа вентиляторов будет реагировать на изменения, чтобы дождаться усиления охлаждения системы, прежде чем снова увеличивать скорость вращения вентиляторов.

Если указан параметр запаздывания, он применяется только в том случае, когда увеличение скорости сменяется ее уменьшением, и наоборот. Например, если BMC в прошлый раз увеличил скорость вращения вентилятора в соответствии со значением, определенным в данной фиксирующей подзаписи, это выразится в применении заданного отрицательного параметра запаздывания при определении «точки смены направления изменения скорости» и момента начала снижения скорости вентилятора. Если не предпринимается никаких действий, связанных с запаздыванием, контроллер BMC продолжает использовать предыдущее направление.

Сумма рассчитанных значений для всех фиксирующих подзаписей TCONTROL, действующих для активного профиля данной группы, прибавляется к максимальному из всех рассчитанных значений для всех действующих шаговых линейных подзаписей TCONTROL.

4.14.4 Управление вентиляторами в режиме ожидания

С помощью команды *Set ACPI Configuration Mode* контроллер BMC можно сконфигурировать для установки фиксированной скорости вращения всех вентиляторов в режиме ожидания, когда система находится в состоянии S1.

4.14.5 Определение резервных вентиляторов

Контроллер BMC поддерживает мониторинг резервных вентиляторов с помощью датчиков резервирования вентиляторов. Датчик резервирования вентиляторов генерирует события, если связанный с ним набор вентиляторов изменяет режим с резервного на рабочий, и наоборот, в соответствии с количеством и состоянием вентиляторов.

Отказ одного вентилятора или извлечение вентилятора из корпуса, поддерживающего горячую замену вентиляторов, в конфигурации с резервированием вентиляторов является некритическим отказом. Это событие отображается на передней панели.

4.14.6 Горячая замена вентиляторов

Некоторые корпуса и серверные платы поддерживают вентиляторы с горячей заменой. Эти вентиляторы можно извлекать и заменять, не прерывая обычной работы системы. В контроллере BMC используются датчики присутствия вентилятора для каждого вентилятора с возможностью горячей замены. После замены вентилятора временно устанавливается высокая скорость вращения вентиляторов данной группы, чтобы создать импульс для правильного запуска вентилятора.

Примечание: *Дополнительную информацию можно найти в технических характеристиках сервера или рабочей станции, входящих в комплект поставки Вашей продукции.*

4.15 Управление акустическими параметрами

Управление акустическими параметрами предусматривает расширенное управление вентиляторами, чтобы обеспечить оптимальное охлаждение системы и предотвратить избыточное излучение шума.

4.15.1 Профили вентиляторов

В программе настройки параметров BIOS можно установить соответствующие опции, чтобы обеспечить заданный уровень шума за счет снижения производительности системы, или добиться увеличения производительности системы за счет увеличения уровня шума вентиляторов. Это достигается с помощью задания профилей вентиляторов. При начальной загрузке системы BIOS будет опрашивать контроллер BMC о поддерживаемых профилях вентиляторов. BIOS отображает экран с опциями настройки, выбранный BMC.

4.15.2 Взаимодействие с системой теплового управления модулями DIMM

4.15.2.1 Данные теплового профиля

Для BIOS необходима информация о значениях различных параметров, которые будут им использоваться как входные данные при расчетах настроек охлаждения модулей DIMM. Они зависят от того, какой профиль вентилятора активен. BIOS получает от BMC эту информацию, зависящую от платформы, во время начальной загрузки.

BMC хранит ее в записях SDR с данными теплового профиля, что позволяет поместить их в репозиторий SDR контроллера BMC и настраивать для каждой платформы и для каждой группы вентиляторов. В системах с поддержкой множества профилей каждая запись SDR с данными теплового профиля может использоваться для одного или нескольких профилей в данной группе вентиляторов.

4.16 Поддержка PSMI

Платформы на базе наборов микросхем Intel® серии 5000 поддерживает источники питания, совместимые со спецификацией PSMI версии 1.44. Некоторые источники питания могут не поддерживать определенные опциональные функции, такие, как мониторинг тока.

4.17 Мониторинг надежности, готовности и возможностей обслуживания (RAS) системной памяти, и мониторинг ошибок системной шины

Мониторинг ошибок системной памяти и системной шины выполняется системным BIOS. При запуске BIOS опрашивает набор микросхем, чтобы получить информацию об ошибках памяти, которые могли произойти ранее в процессе начальной загрузки. BIOS обновляет состояние конфигурации RAS при запуске, а также позже, во время выполнения. BMC производит мониторинг и запись событий в журнал регистрации событий системы на базе определений в записях SDR. Кроме того, функции BIOS позволяют BMC в процессе работы определять наличие модулей DIMM и их неисправное состояние, а также действующую конфигурацию RAS для памяти (например, резервирование, зеркальное отображение, RAID).

Эти функции поддерживают мониторинг ошибок на шинах, например, на системной шине и шине PCI. Мониторинг выполняется BIOS, который при обнаружении ошибки генерирует критическое прерывание и добавляет записи в журнал регистрации событий системы.

Поддерживаемые датчики описаны ниже.

4.17.1 Датчик тайм-аута SMI (прерывания системного управления)

В системах на базе архитектуры IA-32 контроллер BMC поддерживает датчик тайм-аута SMI (тип датчика OEM (F3h), тип события Discrete (03h)), который срабатывает, если сигнал SMI принимается в течение периода времени, превышающего заданное значение (обычно 90 секунд для платформ S5000). Постоянный прием сигнала SMI означает, что BIOS не может обработать условие, которое вызвало прерывание SMI. Обычно причиной этого является то, что это условие мешает нормальной работе BIOS.

При возникновении тайм-аута SMI контроллер BMC выполняет следующие действия:

- Он принимает сигнал датчика тайм-аута SMI и добавляет в журнал регистрации событий системы запись о событии для этого датчика.
- Затем BMC выполняет аварийное (посмертное) тестирование системы на наличие неисправимых ошибок памяти и системной шины. Все неисправимые ошибки ECC, зафиксированные датчиком памяти, записываются в журнал. Все неисправимые ошибки системной шины, зафиксированные датчиком критических прерываний, записываются в журнал.

Стандартные действия ядра встроенного ПО контроллера BMC – не допустить запуска перезагрузки системы в случае обнаружения тайм-аута SMI. Это относится к платформам S5000.

Контроллер BMC поддерживает датчики, которые сообщают о посмертных ошибках системной памяти, а также о наличии модулей DIMM, об их нерабочем состоянии и о сбоях.

4.17.2 Датчик памяти

BMC поддерживает один или несколько датчиков памяти типа *Memory* (0Ch), которые используются только для генерации событий. Если в процессе обработки тайм-аута SMI контроллер BMC обнаружил ошибки (посмертные), записи об этих событиях добавляются в журнал. Такие события имеют определенный тип (код чтения 6Fh). Поддерживаются следующие смещения для датчиков:

- 01h – неисправимая ошибка ECC

4.17.3 Датчик критических прерываний

BMC использует датчик критических прерываний Critical Interrupt (13h) для сообщений о следующих условиях / событиях:

- Неисправимая ошибка системной шины: Обнаруживается только в процессе обработки тайм-аута SMI (посмертной)
- Кнопка NMI на передней панели / диагностическое прерывание Отслеживается во время нормальной системы

4.17.4 Датчики состояния модулей DIMM

Предусмотрен один датчик состояния модулей DIMM на каждый разъем DIMM. По спецификации IPMI эти датчики имеют тип Slot / Connector (21h) и тип события / код чтения Sensor Specific (6Fh). Поддерживаются следующие смещения:

- 00hСостояние сбоя включено
- 02hУстройство установлено
- 08hУстройство находится в нерабочем состоянии
- 09hВ разъем установлено резервное устройство

BIOS может устанавливать или отменять отдельные смещения для датчиков состояния модулей DIMM с помощью команд *Set DIMM State* и *Get DIMM State*.

Если BMC сконфигурирован соответствующим образом, он будет постоянно сохранять записи о сбое DIMM и нерабочем состоянии в энергонезависимой памяти. Они будут стерты при запуске BMC.

Записи о состоянии не добавляются постоянно.

4.17.4.1 Состояние ошибки

Если BIOS обнаружил неисправимую ошибку ECC, он определяет состояние модуля DIMM и устанавливает соответствующим образом датчик состояния модулей DIMM.

4.17.4.2 Устройство установлено

BIOS выполняет процедуру обнаружения модулей DIMM и устанавливает соответствующим образом датчики состояния модулей DIMM при каждой загрузке системы.

4.17.4.3 Устройство находится в нерабочем состоянии

BIOS может определить, что модуль FBDIMM должен быть отключен, и устанавливает соответствующим образом датчик состояния модуля DIMM.

4.17.4.4 В разъем установлено резервное устройство

Индикация резервных модулей DIMM носит информационных характер и используется функциями резервирования памяти для определения состояния резервных модулей.

4.17.4.5 Сброс смещений

BMC сбрасывает состояния ошибки модуля DIMM и/или нерабочего состояния в следующих случаях:

- BMC получил команду *Set DIMM State*, которая требует сбросить одно или оба этих состояния
- Разъем DIMM становится пустым
- Команда *ReArm Sensor* запускается для этого датчика DIMM
- Запускается команда *ReArm DIMMs*
- Группировка DIMM

4.17.4.6 Группировка DIMM

В следующей таблице описывается группировка FBDIMM.

Рисунок 24. Группировка DIMM

Датчик DIMM	Номер датчика
DIMM 1A	EOh
DIMM 2A	E1h
DIMM 1B	E2h
DIMM 2B	E3h
DIMM 1C	E4h
DIMM 2C	E5h
DIMM 1D	E6h
DIMM 2D	E7h

4.17.5 Мониторинг избыточности системной памяти

Наборы микросхем Intel® серии 5000 поддерживают не только коррекцию одноразрядных ошибок, но и другие функции избыточности памяти, позволяющие заменять неисправные модули DIMM без выключения системы и прерывания работы. Поддержка этих возможностей контроллером BMC описана в разделах ниже.

Примечание: *Дополнительная информация содержится в технических характеристиках системных плат Intel® для серверов и рабочих станций, относящихся к Вашей продукции.*

4.17.5.1 Резервный банк модуля DIMM

В связи с резервированием модулей DIMM в контроллере BMC установлено два датчика для области резервирования DIMM (набора модулей DIMM с общим резервным набором DIMM). Каждой области резервирования присваивается уникальный идентификатор объекта. Оба датчика принадлежат этому объекту.

- Датчик избыточности резервирования DIMM

  Избыточность резервирования определяется BIOS. BIOS передает это состояние контроллеру BMC. Контроллер BMC устанавливает соответствующее состояние датчика для соответствующей области резервирования.

  Датчик имеет тип *Availability Status* (0Bh) и указывает на наличие или отсутствие избыточности области (т.е. на наличие или отсутствие резервных модулей DIMM). Поддерживаются следующие смещения:

  - 00h – Полная избыточность. Модули DIMM и резервные модули в области работают и включены
  - 01h – Избыточность потеряна: Достаточные ресурсы, избыточные модули DIMM в области работают и включены, резервных модулей нет
  - 05h – Нет избыточности: Недостаточно ресурсов
    В области нет работающих модулей DIMM или модули отключены

- Включено резервирование DIMM

  Резервирование DIMM включается BIOS, и соответствующая конфигурация устанавливается в контроллере BMC. Контроллер BMC устанавливает состояние соответствующих датчиков для соответствующей области резервирования.

  Этот датчик используется для передачи информации о включении резервирования для области. Этот датчик имеет тип *Entity Presence* (25h). Состояние этого датчика указывает, следует ли игнорировать датчик избыточности резервирования модулей DIMM. Поддерживаются следующие показания:

  - 00h – Объект присутствует

    Эти показания означают, что функция резервирования DIMM для этой области включена, и соответствующий датчик избыточности резервирования DIMM находится в нужном состоянии. При отсутствии этого сигнала датчик избыточности резервирования DIMM следует игнорировать.

  - 01h – Объект отсутствует

    Этот сигнал означает, что резервирование DIMM недоступно для области, и состояние датчика избыточности резервирования DIMM является недопустимым. Эти показания являются взаимоисключающими с показаниями 00h – Объект присутствует.

Примечание: *Функции резервирования и зеркального отражения памяти в настоящее время не поддерживаются, их поддержка будет реализована после начала производства.*

Примечание: *Дополнительную информацию можно найти в технических характеристиках сервера или рабочей станции, входящих в комплект поставки Вашей продукции.*

4.17.5.2 Зеркальное отображение памяти

Если платформа поддерживает зеркальные наборы памяти, в контроллере BMC реализуется два датчика на каждый зеркальный набор (модули DIMM, формирующие зеркальный набор). У каждой зеркальной области имеется уникальный идентификатор объекта. Оба датчика принадлежат этому объекту.

- Датчик избыточности зеркального набора

  Избыточность зеркального набора определяется BIOS. BIOS передает это состояние контроллеру BMC. Затем контроллер BMC устанавливает состояние соответствующего датчика для соответствующей области зеркального набора.

  Датчик имеет тип *Availability Status* (0Bh) и указывает на наличие или отсутствие избыточности области (т.е. на наличие или отсутствие модулей DIMM в зеркальном наборе). Поддерживаются следующие смещения:

  - 00h – Fully redundant
    Все модули DIMM в зеркальной области работают и включены.
  - 01h – Избыточность потеряна: Достаточные ресурсы
    Один или несколько неисправных модулей DIMM в зеркальной паре
  - 05h – Нет избыточности: Недостаточно ресурсов
    Не функционирующие модули DIMM в обеих зеркальных парах
- Зеркальное отражение памяти включено

  Зеркальное отражение памяти включено в BIOS, и эта конфигурация включена в контроллере BMC. Затем контроллер BMC устанавливает состояние соответствующего датчика для соответствующей области зеркального набора.

  Этот датчик используется для передачи информации о состоянии зеркального набора соответствующей области. Этот датчик имеет тип *Entity Presence* (25h). Состояние этого датчика указывает, следует ли игнорировать датчик избыточности зеркальных наборов памяти. Поддерживаются следующие показания:

  - 00h – Объект присутствует

    Этот сигнал означает, что зеркальное отражение памяти для данной области включено, и соответствующий датчик избыточности зеркальных наборов памяти имеет допустимое состояние. При отсутствии этого сигнала датчик избыточности зеркальных наборов памяти следует игнорировать.
  - 01h – Объект отсутствует

    Этот сигнал означает, что зеркальное отражение памяти для данной области не включено, и соответствующий датчик избыточности зеркальных наборов памяти имеет недопустимое состояние. Этот сигнал является взаимоисключающим с сигналом 00h – Объект присутствует.

Примечание: *Функции резервирования и зеркального отражения памяти в настоящее время не поддерживаются, их поддержка будет реализована после начала производства.*

Примечание: *Дополнительную информацию можно найти в технических характеристиках сервера или рабочей станции, входящих в комплект поставки Вашей продукции.*

4.17.6 Мониторинг системной памяти и загрузка системы

Приведенная ниже последовательность событий описывает процедуру загрузки системы в связи с функцией мониторинга системной памяти.

- При загрузке системы BIOS определяет схему установки DIMM и устанавливает соответствующее состояние контроллера BMC. Контроллер BMC инициализирует состояние датчика DIMM в зависимости от информации о присутствии и неустранимых сбоях.
- BIOS настраивает конфигурацию памяти, при необходимости отключая модули DIMM и настраивая функции избыточности. BIOS передает контроллеру BMC информацию об отключенных модулях и конфигурации избыточности (состоянии компонентов).
- Затем BIOS сообщает контроллеру BMC о состоянии избыточности в соответствии с определением в разделе 4.17.5.1.
- После этого BIOS выполняет тестирование памяти. Для всех ошибок памяти, в результате которых BIOS отключает модули DIMM или генерирует ошибки, BIOS сообщает контроллеру BMC об ошибках DIMM.
- В BIOS должна быть включена функция мониторинга системных ошибок памяти контроллером BMC.

4.18 Поддержка PCI Express*

4.18.1 Датчики соединений PCI Express

В контроллере BMC реализован набор датчиков типа IPMI Critical Interrupt, которые используются для регистрации ошибок канала PCI Express, обнаруженных BIOS. Идентификатор объекта в SDR связывает ошибки PCI Express в соответствии с определениями идентификаторов объектов IPMI.

Когда BIOS обнаруживает ошибку, он передает информацию о ней контроллеру BMC.

При подаче сигнала ошибки на датчик PCI Express* контроллер BMC устанавливает состояние сниженной производительности на индикаторе ошибок на передней панели. Состояние датчика отключается по следующим причинам:

- Датчик перезагружен командой IPMI.
- Система перезагружена или включена.

При отключении состояния датчика отключается состояние индикатора ошибок на передней панели.

4.18.2 BMC с функцией самотестирования

Контроллер BMC выполняет различные тесты в процессе инициализации. При обнаружении ошибки (например, порча SDR контроллера BMC), BMC сохраняет ошибку. Ошибки контроллера BMC или подсистемы контроллера BMC, обнаруженные во время нормальной работы контроллера BMC, также могут сохраняться в системе.

4.19 Управление индикатором FRU / ошибок

Поддерживается несколько наборов индикаторов FRU / POST / ошибок. Некоторые индикаторы контролируются контроллером BMC, а некоторые – BIOS.

Контроллер BMC контролирует следующие индикаторы FRU / ошибок:

- **Индикаторы неисправности вентиляторов:** С каждым вентилятором связан индикатор ошибок вентилятора. Контроллер BMC включает индикатор ошибок вентилятора, если частота вращения соответствующего вентилятора падает ниже минимального уровня. Тахометры вентиляторов сбрасываются вручную. При снижении частоты вращения ниже минимального уровня, индикатор остается включенным до тех пор, пока датчик не перезагружается. Эти датчики перезагружаются при включении питания и перезагрузке системы.
- **Индикаторы ошибки процессора:** Для каждого разъема процессора существует индикатор ошибок процессора. Контроллер BMC включает индикатор ошибки процессора, когда соответствующий датчик состояния процессора обнаруживает ошибку конфигурации процессора или отключение процессора. Датчики состояния процессора перезагружаются вручную, при обнаружении любого из этих состояний индикатор горит LED до тех пор, пока датчик не перезагружается. Эти датчики НЕ перезагружаются при включении питания и перезагрузке системы.

4.20 Поддержка объединительной платы горячей замены (HSBP)

Ниже перечислены операции взаимодействия BMC и HSC.

- Агент инициализации BMC настраивает конфигурацию датчиков HSC. Это происходит при включении или перезагрузке системы.
- Команды могут передаваться от BMC к HSC по шине IPMB. Эта шина обычно используется системным программным обеспечением для доступа к информации о состоянии HSC и для обновления встроенного программного обеспечения HSC.

На объединительную плату горячей замены с контроллером HSC не подается питание, когда система находится в состоянии режима сна S0. Поэтому при включении системы до начала связи с контроллером BMC контроллер HSC должен инициализироваться.

4.21 Поддержка модуля управления Intel® Remote Management Module (Intel® RMM)

Модуль дистанционного управления Intel® Remote Management Module (Intel® RMM) поддерживает удаленное подключение клавиатуры, монитора и мыши (KVM), а также другие расширенные функции. В этом разделе описана поддержка контроллером BMC карт расширения Intel® RMM.

4.21.1 Последовательность обнаружения

Контроллер BMC поддерживает набор команд для установки и получения информации о конфигурации поддержки модулей Intel® RMM серверной платой. Эти команды используются картами расширения при подаче питания на карту. Они запрашивают у контроллера BMC поддержку разъемов для карт расширения.

В модулях Intel® RMM эта информация используется для адаптации поддержки определенных разъемов, для формирования полных описаний доступных вариантов подключения и для изменения конфигурации контроллера BMC в соответствии с собственными требованиями к конфигурации.

Контроллер BMC обеспечивает интерфейс для команд настройки конфигурации при использовании с модулями Intel® RMM. Это выполняется посредством сочетания команд IPMI и IPMI OEM. Контроллер BMC не обрабатывает эту конфигурацию автоматически. Он использует поддержку обнаружения дополнений BMC в модулях Intel® RMM и настраивается в соответствии с требованиями модулей Intel® RMM. Обычно модули Intel® RMM настраиваются с помощью программного обеспечения.

4.21.2 Разделение сетевого трафика

Сетевой трафик системы управления сервером обрабатывается модулем Intel® RMM или контроллером BMC, в зависимости от физической конфигурации системы. Это описывается в двух подразделах ниже. Контроллер BMC обрабатывает трафик IPMI-over-LAN, в том числе трафик SOL, даже если в системе не установлено модулей Intel® RMM. Модули Intel® RMM обрабатывают трафик TCP/IP. Маршрутизация других протоколов базового уровня осуществляется на базе конфигурации контроллера BMC или модуля Intel® RMM.

4.21.2.1 Интерфейс для связи третьего канала сетевого контроллера с модулем Intel® RMM

Модуль Intel® RMM поддерживает выделенный сетевой контроллер. Модуль Intel® RMM отвечает за маршрутизацию сетевых пакетов, полученных через этот интерфейс. Трафик IPMI-over-LAN, в том числе трафик SOL, получаемый модулем Intel® RMM через этот сетевой контроллер, пересылается контроллеру BMC через FML или канал данных SMBus. Модуль Intel® RMM самостоятельно обрабатывает другой трафик системы управления сервером.

Контроллер BMC поддерживает этот режим работы через сетевой интерфейс FNI. Это высокоскоростной последовательный интерфейс, обеспечивающий канал обмена данными между модулем Intel® RMM и контроллером BMC в блоке контроллеров ввода/вывода Intel® 631xESB / 632xESB. Если эта функция включена, контроллер BMC обрабатывает этот поток данных, как третий сетевой канал IPMI в дополнение к двум встроенным сетевым контроллерам блока контроллеров ввода/вывода Intel® 631xESB / 632xESB и ответам IPMI, отправляемым по шине FML. Режим работы FNI отключается при перезагрузке контроллера BMC и потере питания режима ожидания.

Контроллер BMC не требует, чтобы модуль Intel® RMM собирал IP-фрагменты перед пересылкой, однако для этого модуль Intel® RMM должен указать порт UDP или TCP, на который направляется IP-трафик.

4.21.3 Переадресация событий

Контроллер BMC поддерживает отправку уведомлений на модули Intel® RMM при возникновении определенных событий в области контроллера BMC. Эта функция реализована посредством механизма переадресации событий. Переадресация событий – функция переадресации событий позволяет контроллеру BMC пересылать на дополнительный контроллер копию информации о событиях, генерированной BMC или полученной в сообщении *Platform Event*.

В следующих подразделах описывается работа контроллеров BMC при включении функции переадресации ошибок. Формат записи данных о событиях для пересылаемых событий основан на форматах записей событий SEL и OEM SEL, определенных в таблицах 32-1 и 32-2 *Спецификации IPMI 2.0*.

4.21.3.1 Переадресация событий SEL

При генерировании событий BMC SEL любым механизмом, кроме команды *Add SEL Entry*, контроллер BMC отправляет копии этих событий модулю Intel® RMM). Переадресация событий происходит при заполнении журнала BMC SEL.

4.21.3.2 Переадресация изменения состояния BMC

Контроллер BMC отправляет уведомления о других событиях изменения состояния, которые могут интересовать дополнительное зарегистрированное устройство. Контроллер BMC не требует, чтобы дополнительное устройство предпринимало дополнительные действия на базе данных о событиях.

4.21.4 Маршрутизация последовательных команд

Контроллер BMC поддерживает дополнительную команду IPMI, *Set Serial Routing Mux*, которая позволяет передавать дополнительной карте последовательный порт для использования совместно с контроллером BMC. Эта команда позволяет картам расширения или дополнительным контроллерам управления передавать контроллеру BMC маршрутизацию последовательных соединений, а также позволяет контроллеру BMC управлять соединениями. С логической точки зрения это действие можно рассматривать как управление аппаратным мультиплексором (последовательная маршрутизация) с маршрутизацией последовательных сигналов между BMC и картой расширения, хотя данная спецификация не описывает конкретную аппаратную реализацию этой функции.

4.21.4.1 Маршрутизация последовательных сигналов и SOL

Интерфейс SOL может поддерживаться контроллером BMC в соответствии со спецификацией IPMI 2.0 или модулем Intel® RMM через Telnet. Для метода на базе модулей Intel® RMM модули Intel® RMM должны контролировать последовательную мультиплексную передачу контроллера BMC.

Если контроллер BMC использует интерфейс UART при получении команды (например, SOL или EMP), он автоматически прекращает сеанс и последовательный канал отключается.

Маршрутизация сигналов SOL не может выполняться модулем Intel® RMM и контроллером BMC одновременно.

4.21.5 Интерфейсы сообщений

В данном разделе описываются коммуникационные интерфейсы контроллера управления BMC:

- Интерфейс Host SMS по шине LPC / KCS
- Интерфейс Host SMS по шине LPC / KCS
- Интерфейс IPMB I^2C
- PCI SMBus
- Порт аварийного управления (EMP), использующий протокол IPMI over Serial / Modem для удаленного доступа по последовательному интерфейсу.
- Сетевой интерфейс, использующий протоколы IPMI-over-LAN

Эти спецификации описаны в следующих подразделах. В разделе 4.26 описаны базовые характеристики коммуникационных протоколов, использованных в перечисленных выше интерфейсах.

4.22 Управление каналами

Каждому интерфейсу назначается идентификатор канала IPMI 2.0. Существуют команды для настройки уровня прав и режима доступа для каждого канала. В таблице ниже описывается стандартное назначение каналов:

Таблица 42. Стандартное назначение каналов

Идентификатор канала	Интерфейс	Поддержка сеансов
0	IPMB	Нет
1	LAN 1	Да
2	LAN 2 [1]	Да
3	LAN 3 [1] (Intel® RMM / Intel® RMM NIC)	Да
4	EMP (Basic / PPP)	Да
5	Зарезервирован	–
6	PCI SMBus [1]	Нет
7	SMM	Нет
0Eh	Самостоятельный [2]	–
0Fh	SMS / Очередь получения сообщений	Нет

Примечания:

1. Если поддерживается серверной платформой.
2. Реальный канал, использованный для отправки запроса.

4.23 Модель работы пользователя

Контроллер BMC поддерживает пользовательскую модель IPMI 2.0, в том числе *User ID 1*. Поддерживается 15 идентификаторов пользователей. Этим 15 пользователям можно присвоить любой канал.

4.24 Поддержка сессий

Контроллер BMC поддерживает до пяти одновременных сеансов. Они совместно используются всеми каналами на базе сеансов.

4.25 Соединение интерфейсов

Контроллер BMC поддерживает соединение интерфейсов EMP и IPMB, а также LAN и IPMB. Это позволяет запрашивать состояние других интеллектуальных контроллеров корпуса с помощью удаленных программных консолей. Запросы могут направляться контроллерам по шине IPMB, однако запросы, исходящие от шины IPMB, не могут переадресовываться на интерфейсы EMP или LAN.

4.26 Интерфейс связи хоста с контроллером управления BMC

4.26.1 Интерфейс LPC / KCS

В контроллере BMC имеется три интерфейсных порта KCS 8042, соответствующих спецификации IPMI 2.0. Для этих интерфейсов назначены адреса ввода/вывода, и доступ к ним осуществляется через шину LPC в наборе микросхем.

Для этих интерфейсов назначены следующие адреса и модели использования:

Таблица 43. Интерфейсы KCS

Название:	Используется	Адрес
Интерфейс SMS	SMS, BIOS POST и доступ к служебным программам	0CA2h – 0CA3h
Интерфейс SMM	Обработка прерываний SMI для регистрации ошибок	0CA4h – 0CA5h

Контроллер BMC устанавливает более высокий приоритет для передачи через интерфейс SMM. При этом устанавливается минимальная задержка доступа к SMI. Контроллер BMC выступает в качестве моста между интерфейсом ПО для управления сервером (SMS) и IPMB. Реестры интерфейса обеспечивают механизм связи между контроллером BMC и платформой. В большинстве платформ интерфейсы реализованы в виде реестров адресов области ввода/вывода. Интерфейсы состоят из трех наборов из двух реестров шириной 1 байт.

4.26.2 Очередь приема сообщений

Очередь приема сообщений доступна только через интерфейс SMS, поскольку этот интерфейс представляет собой интерфейс платформы BMC / системный интерфейс. Размер очереди зависит от платформы, однако не может составлять меньше двух записей. Очередь не поддерживает рекомендацию IPMI 2.o выделении очередей для каждого канала.

4.26.3 Интерфейс SMS

Интерфейс SMS является платформенным интерфейсом BMC. В контроллере BMC реализован интерфейс SMS KCS, как описано в спецификации IPMI 2.0.

4.26.4 Интерфейс SMM

Интерфейс SMM принадлежит к типу KCS и используется BIOS там, где требуется быстрая реакция, например, обработчиком SMI в BIOS. Для контроллера BMC этот интерфейс является приоритетным по отношению к другим интерфейсам связи.

Интерфейс SMM поддерживает только относительно небольшой набор команд BMC. Код этих команд оптимизирован, что в сочетании с использованием быстрого интерфейса SMM, обеспечивает выполнение команды и ответ на нее в течение одного прерывания BMC.

4.27 Коммуникационный интерфейс IPMB

IPMB представляет собой протокол связи, использующий в качестве физической среды шину I^2C, работающую на скорости 100 КБ/с. Дополнительную информацию о спецификации I^2C можно найти в разделе *Шина I^2C и ее использование.* Реализация IPMB в контроллере BMC совместима с *IPMB 1.0, ред. 1.0.*

Контроллер BMC отправляет и получает сообщения IPMB через интерфейс IPMB. Другие сообщения, полученные через интерфейс IPMB, игнорируются.

Для отправки сообщений запроса IPMB в контроллере BMC реализован интервал времени задержки, составляющий 60 мс с поддержкой до 3 повторных попыток.

4.27.1 Шина PCI SMBus

BMC может использовать шину the PCI SMBus. Контроллер BMC поддерживает отправку сообщений IPMB по шине PCI SMBus. Для этих сообщений модифицирован пакетный формат, что позволяет устранить несоответствие трафика IPMB и SMBus.

Между модифицированным пакетным форматом и стандартным форматом IPMB существуют следующие различия:

- Установлена первая контрольная сумма IPMB 00h.
- Вторая контрольная сумма IPMB заменена кодом PEC, который представляет собой байт контроля ошибок CRC-8.

4.27.2 Контроллер BMC в качестве главного контроллера I^2C на шине IPMB

Контроллер BMC позволяет использовать устройства IPMB в качестве главного устройства шины I^2C. Поддерживаются следующие команды:

- *Send Message:* Эта команда служит для записи данных на устройство I^2C.
- *Master Write-Read I^2C:* Эта команда позволяет выполнять следующие действия:
  - Записывать данные на устройство I^2C, как главное устройство.
  - Считывать данные с устройства I^2C, как главное устройство.
  - Записывать данные на устройство I^2C, как главное устройство, отправлять команду I^2C Repeated Start и считывать определенное число байт с устройства I^2C, как с главного устройства. Сообщения об ошибках приема или передачи на шине I^2C передаются в виде кодов выполнения в ответе команд.

Эти функции поддерживают наиболее распространенные операции главного контроллера шины I^2C. В их число входит доступ к стандартным неинтеллектуальным устройствам шины I^2C, например, к блокам памяти SEEPROM. Команд *Send Message* обычно используется для отправки сообщений IPMB на интеллектуальные устройства, которые используют протокол IPMB.

4.27.3 Маршрутизация LUN в IPMB

Контроллер BMC может получать сообщения IPMB с запросами или ответами. Обработка этих сообщений зависит от номера логического устройства (LUN) назначения в этих сообщениях. Для запросов IPMB LUN устройства назначения соответствует LUN отвечающего устройства. Для ответов IPMB LUN устройства назначения соответствует LUN запрашивающего устройства. Эти сообщения более подробно описываются в таблице ниже. BMC принимает LUN 00b и LUN 10b.

Сообщения IPMB могут иметь размер до 36 байт, включая заголовок IPMB и контрольные суммы.

Таблица 44. Маршрутизация LUN в BMC

LUN	Название:	Обработка сообщений
00b	BMC	Сообщения запросов с этими номерами LUN передаются обработчику команд BMC. Сообщения запросов с этими номерами LUN сравниваются с невыполненными запросами контроллера BMC. В случае соответствия направляется уведомление подсистеме контроллера BMC, отправившей запрос. В противном случае сообщение игнорируется.
01b	Зарезервирован	Зарезервировано – Все сообщения с этими номерами LUN игнорируются.
10b	SMS	Все получаемые сообщения с этими номерами LUN помещаются в очередь приема сообщений. Если этот буфер заполнен целиком, сообщения игнорируются. При этом не выполняется никакой дополнительной обработки.
11b	Зарезервирован	Зарезервировано – Все сообщения с этими номерами LUN игнорируются.

На рисунке 8 показана логическая блок-схема приема сообщений IPMB контроллером BMC.

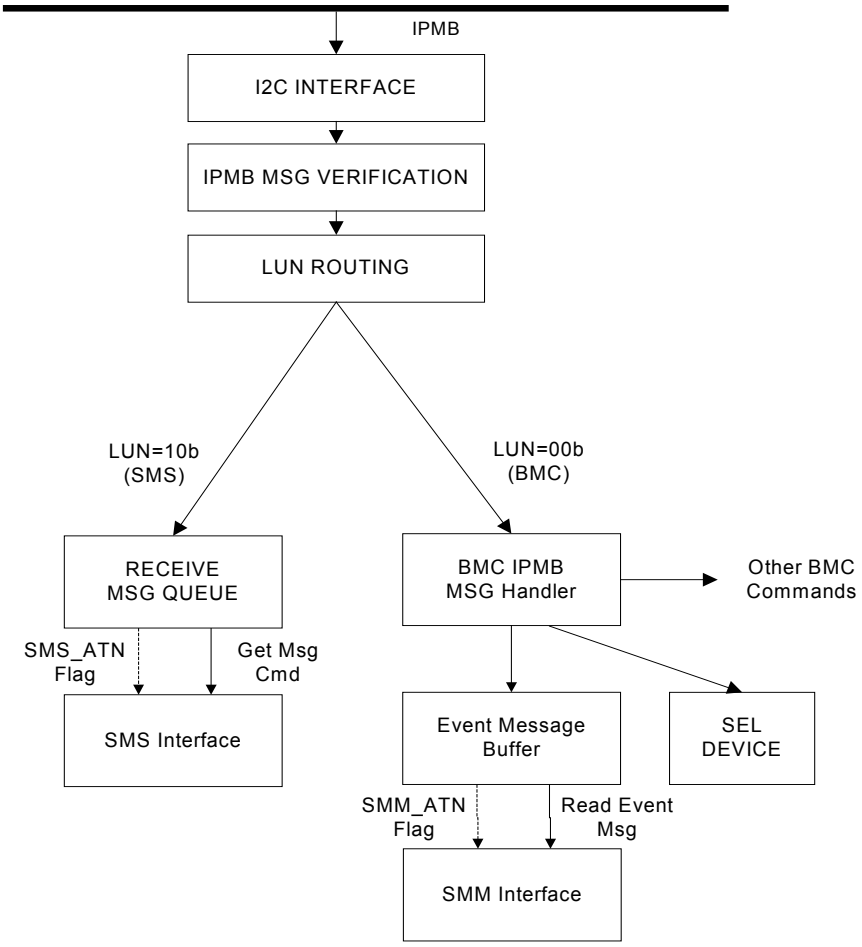


Рисунок 25. Прием сообщений IPMB контроллером BMC

4.28 Интерфейс порта аварийного управления (EMP)

Интерфейс EMP представляет собой реализованный корпорацией Intel интерфейс IPMI 2.0 IPMI over serial. Основная задача постоянно доступного канала RS232 заключается в том, чтобы дать системным администраторам доступ к функциям низкоуровневых средств управления сервером с помощью стандартных средств. Для упрощения использования и обеспечения высокого уровня совместимости с протоколами LAN и IPMB, в этом протоколе реализован ряд функций обоих протоколов.

В версии Intel функция EMP использует интерфейс последовательного порта B на платформе. Контроллер BMC управляет доступом к последовательному порту B (предоставляя его системе или контроллеру BMC). Поддерживаются сигналы установки соединения и сигналы *Ring Indicate* и *Data Carrier Detect*.

Поддерживается базовый режим IPMI over serial, который доступен во всех случаях, независимо от наличия питания постоянного тока. Дополнительную информацию об интерфейсе IPMI over serial / modem можно найти в спецификации IPMI 2.0.

4.28.1 Переключение порта COM2

Как указано в спецификации IPMI 2.0, если порт EMP включен, контроллер BMC будет отслеживать трафик последовательного порта, если порт COM2 контролируется системой. Это требуется для реагирования на запросы переключения порта. Отслеживание трафика последовательного порта выполняется в базовом режиме, хотя распознаваемые последовательности в двух режимах отличаются.

4.28.2 Базовый режим

В базовом режиме используется протокол, передающий запросы IPMI через последовательный порт с минимальным обременением. Прием команд подтверждается контроллером BMC для каждого пакета.

Базовый режим поддерживает типы аутентификации *None* (нет аутентификации) и *Straight Password / Key*. В базовом режиме поддерживается обратный вызов.

4.28.3 Режим терминала

Контроллер BMC поддерживает режим терминала, описанный в спецификации IPMI 2.0. Режим терминала позволяет доставлять сообщения IPMI на контроллер BMC в текстовом формате ASCII через последовательный канал или любой пакетный интерфейс. Сообщения бывают двух видов:

- Сообщения IPMI, закодированные в паре hex-ASCII
- Текстовые команды SYS

4.28.3.1 Ограничения ввода

4.28.3.1.1 Максимальная длина

Контроллер BMC позволяет вводить до 122 символов на строку. Контроллер BMC перестает принимать новые символы и отражать ввод по достижении предельного значения 122 символа. Однако отдельные символы принимаются и обрабатываются даже после достижения ограничения. Это символы <Esc>, <backspace> / <delete>, illegal, и input <newline>.

4.28.3.1.2 Максимальная длина сообщений IPMI

Интерфейс режима терминала поддерживает длину сообщений IPMI до 40 байт.

4.28.3.1.3 Символ непрерывности строки

Символ непрерывности строки поддерживается на последовательном канале только в режиме терминала. Символ непрерывности строки поддерживается для текстовых команд и команд hex-ASCII.

4.28.3.2 Поддержка команд

4.28.3.2.1 Текстовые команды

Контроллер BMC поддерживает все текстовые команды, описанные в спецификации IPMI 2.0, и текстовые команды OEM, описанные в следующей таблице.

Таблица 45. Команды режима терминала

Команда	Запрос/ответ данных	Привилегия	Описание
SYS PWD	В соответствии с определением IPMI 2.0	Обратный вызов	Поддерживаются все определения IPMI для этой команды
SYS TMODE	В соответствии с определением IPMI 2.0	Обратный вызов	
SYS SET BOOT	В соответствии с определением IPMI 2.0	Администратор	
SYS SET BOOTOPT	В соответствии с определением IPMI 2.0	Администратор	
SYS GET BOOTOPT	В соответствии с определением IPMI 2.0	Оператор	
SYS SET TCFG	В соответствии с определением IPMI 2.0	Администратор	Поддерживаются все определения IPMI для этой команды
SYS RESET	В соответствии с определением IPMI 2.0	Оператор	
SYS POWER ON	В соответствии с определением IPMI 2.0	Оператор	
SYS POWER OFF	В соответствии с определением IPMI 2.0	Оператор	
SYS HEALTH QUERY	В соответствии с определением IPMI 2.0	Пользователя	Поддерживаются все определения IPMI для этой команды
XX XX ...	Закодированные команды IPMI в шестнадцатеричном формате ASCII – запрос / отправка данных в соответствии с другими таблицами команд.	Меняются	Привилегии в соответствии с определением кодировки команд IPMI

4.28.3.2.2 Уровни привилегий для текстовых команд

BMC поддерживает схему уровня привилегий для текстовых команд режима терминала в соответствии с Таблица 45.

4.28.3.3 Поддержка объединения мостом

Контроллер BMC поддерживает дополнительную возможность объединения мостом, описанную в спецификации IPMI 2.0.

4.28.4 Неверная обработка пароля

Если через интерфейс EMP последовательно получается три неверных команды *Activate Session,* контроллер BMC отправляет команду отключения в модемном режиме и принимает следующую команду *Activate Session* не ранее, чем через 30 секунд. Контроллер BMC также регистрирует событие Out-of-band Access Password Violation в журнале событий системы при каждом получении ошибочной команды *Activate Session*.

4.28.5 Сообщение Serial Ping

BMC выводит команду IPMI 2.0 *Serial Connection Active* или serial ping через последовательное соединение каждые две секунды, если в параметрах EMP задан базовый режим. Однако сообщение serial ping зависит от типов режимов работы.

4.28.5.1 Автоматическое определение рабочего режима (Connection Mode Enable)

Если включен базовый режим и хотя бы один другой рабочий режим, и контроллер BMC автоматически определяет режим работы, BMC выводит команду serial ping до тех пор, пока не обнаруживается режим работы. Если обнаруживается не базовый режим работы, команда serial ping автоматически отключается. При потере связи, ошибке сеанса или закрытии сеанса команды serial ping автоматически включаются снова в соответствии с параметрами конфигурации EMP.

4.28.5.2 Режим терминала

Если в параметрах конфигурации EMP включен только режим терминала, команда serial ping автоматически отключается, вне зависимости от других параметров конфигурации EMP. При изменении параметров конфигурации EMP действия сообщений serial ping автоматически пересматриваются по мере необходимости.

4.29 Интерфейс локальной сети

В контроллере BMC реализованы модели сообщений IPMI 1.5 и IPMI 2.0. Они обеспечивают связь по локальной сети между контроллером BMC и внешним миром.

Контроллер BMC поддерживает до трех сетевых интерфейсов:

- В двух сетевых интерфейсах используются встроенные сетевые контролеры блока контроллеров ввода/вывода Intel® 631xESB / 632xESB (один канал на каждый встроенный контроллер).
- Один сетевой интерфейс использует дополнительный внешний сетевой контроллер Intel® RMM. Для этого сетевого контроллера требуется дополнительный модуль Intel® Remote Management Module.

Дополнительную информацию о протоколе IPMI-over-LAN можно найти в спецификации IPMI 2.0.

4.29.1 Сообщения IPMI 1.5

Формат пакетов протокола связи включает запросы и ответы IPMI, объединенные в наборе сессий IPMI для аутентификации и в пакете RMCP, помещенном в пакет IP/UDP. Хотя аутентификация обеспечивается, шифрование не обеспечивается, и поэтому изменение некоторых настроек, например, паролей пользователя, не рекомендуется производить через этот интерфейс.

Команды создания сеанса представляют собой команды IPMI, не требующие аутентификации или активации соответствующего сеанса.

Контроллер BMC поддерживает типы аутентификации *None* (нет аутентификации), *Straight Password / Key* и *MD5* по сетевому интерфейсу.

4.29.2 Сообщения IPMI 2.0

Сообщения IPMI 2.0 интегрированы поверх RMCP+ и используют другой протокол создания сессий. Команды сессий определяются RSSP и реализуются на уровне RMCP+, а не на уровне команд IPMI. Аутентификация реализована на уровне RMCP+. RMCP+ обеспечивает шифрование соединений, и поэтому возможна передача конфиденциальных и важных данных.

Контроллер BMC поддерживает следующие шифровальные наборы:

Таблица 46. Поддерживаемые шифровальные наборы RMCP+

ID	Алгоритм аутентификации	Алгоритм(ы) целостности	Алгоритм(ы) конфиденциальности
0	RAKP-none	Нет	Нет
1	RAKP-HMAC-SHA1	Нет	Нет
2	RAKP-HMAC-SHA1	HMAC-SHA1-96	Нет
3	RAKP-HMAC-SHA1	HMAC-SHA1-96	AES-CBC-128
6	RAKP-HMAC-MD5	Нет	Нет
7	RAKP-HMAC-MD5	HMAC-MD5-128	Нет
8	RAKP-HMAC-MD5	HMAC-MD5-128	AES-CBC-128
11	RAKP-HMAC-MD5	MD5-128	Нет
12	RAKP-HMAC-MD5	MD5-128	AES-CBC-128

Для аутентификации пользователей контроллер BMC можно настроить для использования нулевых имен пользователей, так что пароль и ключ проверяются на базе уровня привилегий, а также для использования обычных имен пользователей, так что пароль и ключ проверяются для имени пользователя.

Сообщения IPMI 2.0 поддерживают концепцию типов и идентификаторов полезной нагрузки. Это позволяет передавать другие данные, помимо команд IPMI. Интерфейс IPMI 2.0 Serial-over-LAN реализован, как тип полезной нагрузки.

Таблица 47. Поддерживаемые типы полезной нагрузки RMCP+

Тип полезной нагрузки	Характеристика	IANA
00h	Сообщение IPMI	Нет
01h	Serial-over-LAN	Нет
02h	Определен OEM	Intel (343)
10h – 15h	Настройка сессии	Нет

4.29.3 Встроенные сетевые каналы блока контроллеров ввода/вывода Intel® 631xESB / 632xESB

Хотя встроенные сетевые контроллеры блока контроллеров ввода/вывода Intel® 631xESB / 632xESB совместно используются контроллером BMC и сервером, совместное использование означает, что контроллер BMC и сервер используют одни и те же сетевые контроллеры. Эти общие сетевые контроллеры выделяют отдельный MAC-адрес для использования BMC. В результате эти каналы более напоминают выделенные сетевые каналы, чем общие каналы. IP-адрес сервера всегда отличается от IP-адреса контроллера BMC для определенных встроенных сетевых контроллеров.

Для этих каналов поддержку можно реализовать по каналам IPMI-over-LAN, ARP и DHCP.

Как часть блока контроллеров ввода/вывода, контроллер BMC имеет высокую степень доступа к первичным сетевым интерфейсам. В последующих разделах описывается настройка блока контроллеров ввода/вывода контроллером BMC для реализации этих расширенных возможностей.

Все сетевые функции сетевого канала отключены, если для канала не установлен режим доступа *Always Enabled*.

Если в системе установлен дополнительный модуль Intel® RMM, встроенные сетевые каналы блока контроллеров ввода/вывода настраиваются иначе, чем для сервера, где нет этого устройства. Для получения дополнительной информации см. Раздел 4.21.

4.29.4 Поддержка протокола разрешения адресов

Контроллер BMC может принимать запросы ARP сетевых контроллеров блоков контроллеров ввода/вывода Intel® 631xESB / 632xESB и реагировать на них, а также генерировать запросы ARP.

При первом включении контроллера BMC или при изменении и порче его частной карты хранения генерирование всех запросов ARP отключается.

4.29.5 Поддержка протокола ICMP.

Контроллер BMC поддерживает следующие типы сообщений ICMP, направляемые блоком контроллеров ввода/вывода Intel® 631xESB / 632xESB:

- Запрос эхо (ping) – BMC отправляет ответ эхо
- Destination unreachable – Если сообщение связано с активным соединением контроллера BMC, он закрывает соединение
- Redirect – BMC обновляет свою внутреннюю таблицу маршрутизации
- Запрос временной метки (Timestamp Request) – Контроллер BMC отправляет временную метку

4.29.6 Serial-over-LAN (SOL) 2.0

Контроллер BMC поддерживает интерфейс SOL, определенный в IPMI 2.0. Платформы на базе наборов микросхем Intel® серии 5000 не поддерживают интерфейс Intel SOL предыдущего поколения, называемый теперь SOL 1.0.

В IPMI 2.0 вводится стандарт интерфейса SOL, реализованный как стандартная полезная нагрузка (01h) RMCP+.

5. Сообщения об ошибках и обработка ошибок

В этой главе описываются сообщения об ошибках, коды ошибок и звуковые сигналы. Информацию о роли BIOS в обработке ошибок и взаимодействии между BIOS, оборудованием платформы и встроенным ПО для управления сервером можно найти в главе 4, Системное управление.

5.1 Отказоустойчивая загрузка (FRB)

Отказоустойчивая загрузка (FRB) – эта функция, реализованная Intel для обнаружения и обработки ошибок при загрузке системы. FRB помогает обеспечить загрузку системы даже при ошибке одного или нескольких процессоров во время процедуры POST. При загрузке могут возникать разные ошибки, которые BIOS и BMC могут обнаружить и обработать:

- Ошибка загрузочного процессора (BSP) ошибка POST (контрольный счетчик FRB2)
- Ошибки загрузки ОС
- Ошибки загрузки прикладного процессора (AP)

5.1.1 Ошибки BSP POST (FRB-2)

Процедура FRB-2 использует контрольный счетчик, который можно настроить для перезагрузки системы в случае зависания процедуры POST. В BIOS счетчик FRB-2 установлен на 6 минут.

BIOS отключает контрольный счетчик, прежде чем запрашивать у пользователя загрузочный пароль, при проверке дополнительных ПЗУ и при входе в программу BIOS Setup. Если система зависает во время процедуры POST, контроллер BMC генерирует асинхронную перезагрузку системы (ASR) перед отключением таймера FRB-2.

Контроллер BMC сохраняет биты состояния, которые BIOS может считывать в кодах POST для отключения ранее неисправного процессора, регистрации событий в журнале событий системы и отображения сообщений об ошибках.

5.1.2 Ошибки загрузки операционной системы (загрузочный счетчик ОС)

BIOS представляет дополнительный контрольный счетчик для обеспечения отказоустойчивой загрузки операционной системы. Данная опция отключена по умолчанию. Время счетчика и возможность включения счетчика настраиваются через программу BIOS Setup. Если они включены, BIOS включает загрузочный счетчик ОС в контроллере. После успешной загрузки операционной системы этот счетчик отключается самой операционной системой или приложением.

Осторожно: *Если эта опция включена, а в системе не установлены ОС или приложение для управления сервером, поддерживающие эту функцию, система будет перезагружаться при истечении времени счетчика. Информацию о поддержке этой функции можно найти в документации приложения или ОС.*

5.2 Обработка и регистрация ошибок

В этом разделе описывается обработка ошибок BIOS, а также роль BIOS в обработке ошибок и взаимодействие между BIOS, платформенным оборудованием и ПО для управления сервером при обработке ошибок. Кроме того, в нем рассказывается о методах записи ошибок, и определяются звуковые коды ошибок.

5.2.1 Источники и типы ошибок

Система управления сервером должна правильно и стабильно обрабатывать системные ошибки. Ошибки системы могут, и могут быть разделены на следующие категории:

- Разъемы шины PCI
- Одноразрядные и многоразрядные ошибки памяти
- Датчики
- Ошибки, обнаруживаемые во время тестирования системы при включении, регистрируемые как «ошибки POST»

За управление датчиками управления сервером отвечает контроллер BMC. BMC получает сообщения об ошибках от отдельных датчиков и производит запись событий системы.

5.2.2 Регистрация ошибок обработчиком SMI

Обработчик прерываний SMI обрабатывает и записывает события на системном уровне, являющиеся невидимыми для встроенного микрокода управления сервером. Обработчик SMI выполняет предварительную обработку всех системных ошибок, в том числе тех, которые должны генерировать прерывание NMI.

Обработчик SMI отправляет BMC команду записать событие и предоставляет данные для записи. Например, BIOS программирует генерирование аппаратным обеспечением сигнала SMI в связи с одноразрядной ошибкой и регистрирует расположение неисправного модуля памяти FBDIMM в журнале событий системы (SEL). SMI генерируются системными событиями, обрабатываемыми BIOS. После регистрации ошибки BIOS, при необходимости генерируется прерывание NMI.

5.2.2.1 Ошибки шины PCI

На шине PCI присутствуют два контакта ошибок PERR# и SERR#. Они служат для сообщения об ошибках четности PCI и системных ошибках соответственно. BIOS может быть поручено включить / отключить сообщения об ошибках PERR# и SERR# посредством источника немаскированных прерываний (NMI). Отключение немаскируемых прерываний для ошибок PERR# и/или SERR# также отключает регистрацию соответствующих событий.

В случае ошибки PERR#, хозяин шины PCI может попробовать повторить транзакцию, с которой связана ошибка, или сообщить о ней системе как об ошибке SERR#. Все другие ошибки PCI рассматриваются как ошибки SERR#. Все мосты PCI настроены так, что они генерируют ошибку SERR# на первичном интерфейсе при ошибке SERR# на вторичном интерфейсе, если поддержка ошибок SERR# включена в BIOS Setup. То же самое относится и к PERR#.

5.2.2.2 Ошибки PCI Express*

Критические ошибки PCI Express* регистрируются, как системные ошибки PCI, и генерируют прерывание NMI. Все некритические ошибки PCI Express регистрируются, как ошибки четности PCI.

5.2.2.3 Ошибка шины процессора

BIOS обеспечивает возможности обнаружения и коррекции ошибок процессоров, устанавливая соответствующие биты в MSR или внутри набора микросхем.

В случае неустранимых ошибок на шине процессора не может быть гарантирована соответствующая работа обработчика сигналов SMI; в таком случае обработчик сигналов SMI не сможет произвести регистрацию данных условий. Обработчик запишет ошибки в журнал системных событий только в том случае, если в системе не произошел катастрофический сбой, нарушивший целостность обработчика.

5.2.2.4 Ошибка шины памяти

Оборудование программируется для генерирования прерываний SMI при обнаружении устранимых ошибок данных в массиве памяти. Система обработки прерываний записывает эту ошибку и соответствующий разъем FBDIMM в журнал событий системы. Неустранимые ошибки в памяти передаются SMI, поскольку контроллер BMC не может определить расположение неисправных модулей FBDIMM. Неустранимые ошибки могут привести к порче содержимого SMRAM. Обработчик SMI регистрирует номер неисправного модуля FBDIMM в контроллере BMC, если содержимое SMRAM еще не повреждено. Некоторые платформы не имеют функции определения неисправного модуля памяти FBDIMM ; кроме того, это невозможно на раннем этапе процедуры POST.

5.2.2.5 Ошибка контрольного счетчика ОС

Если драйвер ОС использует контрольный счетчик для обнаружения ошибок оборудования или ПО, и если время этого счетчика истекает, генерируется событие асинхронной перезагрузки (ASR). Это событие эквивалентно аппаратной перезагрузке. При перезагрузки системы часть процедуры POST BIOS может направить контроллеру BMC запрос по событию контрольной перезагрузки и произвести регистрацию данного события в журнале событий системы.

5.2.2.6 События загрузки

Во время тестирования системы при включении BIOS записывает в BMC системную дату и время и производит запись загрузочного события. Приложения, просматривающие журнал событий, не рассматривают событие загрузки как ошибку.

5.2.3 Событие часов временных меток

Контроллер управления BMC поддерживает внутренние четырехбайтовые синхронизирующие импульсы, используемые подсистемами SEL и SDR. Показания часов временных меток меняются каждую секунду.

5.2.3.1 Нет доступа к часам реального времени (RTC)

После перезагрузки контроллера BMC он устанавливает первоначальное значение часов временных меток на 0x00000000, после чего оно увеличивается каждую секунду. События SEL с временными метками от 0x00000000 до 0x140000000 относятся к инициализации BMC.

Во время процедуры POST BIOS сообщает BMC текущее время часов RTC. Контроллер BMC управляет временем, используя аппаратный сигнал, работающий от того же генератора, который обеспечивает работу системных часов реального времени. Если пользователь меняет показания часов реального времени во время работы, SMS отвечает за синхронизацию времени с контроллером BMC.

Примечание: *Контроллер BMC может потерять текущую временную метку при холодной перезагрузке или обновлении встроенного ПО контроллера BMC.*

5.3 Сообщения об ошибках и коды ошибок

BIOS отображает сообщения об ошибках на экране. Перед инициализацией изображения сообщения об ошибках передаются в виде звуковых сигналов. POST-коды ошибок записываются в журнал событий. BIOS отображает коды ошибок POST на экране.

5.3.1 Диагностические индикаторы

При загрузке системы BIOS выполняет ряд процедур настройки платформы, каждой из которых соответствует код POST. Каждый раз при выполнении операций POST BIOS отображает код POST при помощи диагностических индикаторов в задней части серверной платы. При разрешении проблем, связанных с зависанием системы во время процедуры POST, диагностические индикаторы используются для определения последнего процесса, выполненного перед зависанием.

Каждый код POST представлен комбинацией цветов четырех светоиндикаторов. Светоиндикаторы отображают три цвета: зеленый, красный и оранжевый. Коды POST делятся на верхнюю часть байта и нижнюю часть байта. Каждый бит в верхней части представлен красным светоиндикатором; каждый бит в нижней части представлен зеленым светоиндикатором. Если оба бита установлены в верхней и нижней части байта, то загораются красный и зеленый светоиндикаторы, что в результате дает оранжевый цвет. Если оба бита не установлены, светоиндикатор отключен.

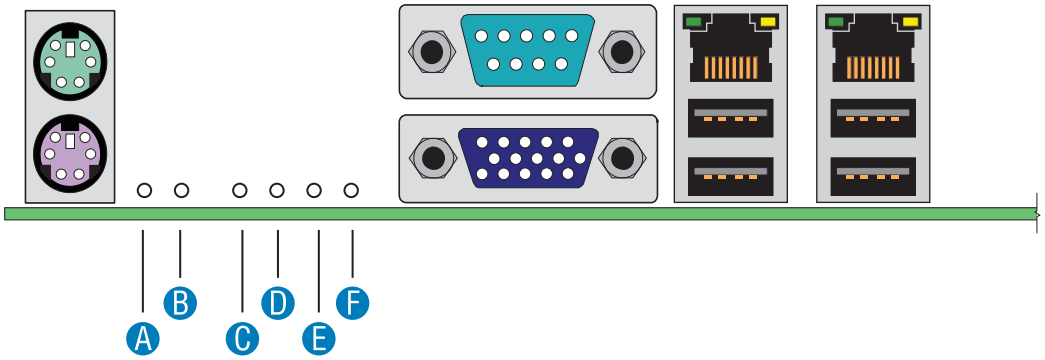
В следующем примере BIOS направляет на светоиндикатор значение ACh. ДекДекод Декодирование светоиндикаторов производится следующим образом:

- Red bits = 1010b = Ah
- Green bits = 1100b = Ch

Поскольку красные биты соответствуют верхней части байта, а зеленые биты соответствуют нижней части байта, то при объединении красные и зеленые биты становятся ACh.

Таблица 48. Индикатор кода процедуры POST (пример)

	8h		4h		2h		1h	
Индикаторы	**Красный**	**Зеленый**	**Красный**	**Зеленый**	**Красный**	**Зеленый**	**Красный**	**Зеленый**
ACh	1	1	0	1	1	0	0	0
Результат	Желтый		Зеленый		Красный		Не горит	
	MSB						LSB	



AF000541

A. Индикатор состояния	D. Bit 1 LED (POST LED)
B. Индикатор идентификации системы	E. Bit 2 LED (POST LED)
C. MSB LED (POST LED)	F. LSB LED (POST LED)

Рисунок 26. Расположение диагностических индикаторов на серверной плате

Примечание: *Подробную информацию по местонахождению диагностических индикаторов на задней панели можно найти в технической спецификации сервера или рабочей станции.*

5.3.2 Контрольные точки POST-кода

Таблица 49. Контрольные точки POST-кода

Контрольная точка	**Расшифровка показаний диагностических индикаторов**				**Описание**
	G=зеленый, R=красный, A=желтый				
	MSB	**Бит 1**	**Бит 2**	**LSB**	
Процессор системы:					
0x10h	Не горит	Не горит	Не горит	R	Включение питания процессора (загрузочного процессора)
0x11h	Не горит	Не горит	Не горит	A	Инициализация кэш-памяти процессора (прикладной процессор)
0x12h	Не горит	Не горит	G	R	Начало инициализации прикладного процессора
0x13h	Не горит	Не горит	G	A	Инициализация SMM

Контрольная точка	Расшифровка показаний диагностических индикаторов				Описание
	G=зеленый, R=красный, A=желтый				
	MSB	**Бит 1**	**Бит 2**	**LSB**	
Набор микросхем					
0x21h	Не горит	Не горит	R	G	Инициализация компонентов набора микросхем
Память					
0x22h	Не горит	Не горит	A	Не горит	Считывание данных конфигурации из памяти (SPD из FBDIMM)
0x23h	Не горит	Не горит	A	G	Определение наличия памяти
0x24h	Не горит	G	R	Не горит	Программирование временных параметров в контроллере памяти
0x25h	Не горит	G	R	G	Конфигурация параметров памяти в контроллере памяти
0x26h	Не горит	G	A	Не горит	Оптимизация настроек контроллера памяти
0x27h	Не горит	G	A	G	Инициализация памяти, например ECC
0x28h	G	Не горит	R	Не горит	Тестирование памяти
Шина PCI					
0x50h	Не горит	R	Не горит	R	Нумерация шин PCI
0x51h	Не горит	R	Не горит	A	Распределение ресурсов между шинами PCI
0x52h	Не горит	R	G	R	Инициализация контроллера Hot Plug PCI
0x53h	Не горит	R	G	A	Зарезервировано для шины PCI
0x54h	Не горит	A	Не горит	R	Зарезервировано для шины PCI
0x55h	Не горит	A	Не горит	A	Зарезервировано для шины PCI
0x56h	Не горит	A	G	R	Зарезервировано для шины PCI
0x57h	Не горит	A	G	A	Зарезервировано для шины PCI
Порт USB					
0x58h	G	R	Не горит	R	Переустановка шины USB
0x59h	G	R	Не горит	A	Зарезервировано для устройств USB
ATA/ATAPI/SATA					
0x5Ah	G	R	G	R	Переустановка шины PATA/SATA и всех устройств
0x5Bh	G	R	G	A	Зарезервировано для ATA
SMBUS					
0x5Ch	G	A	Не горит	R	Переустановка SMBUS
0x5Dh	G	A	Не горит	A	Зарезервировано для SMBUS
Локальная консоль					
0x70h	Не горит	R	R	R	Перезагрузка видеоконтроллера (VGA)
0x71h	Не горит	R	R	A	Отключение видеоконтроллера (VGA)
0x72h	Не горит	R	A	R	Включение видеоконтроллера (VGA)
Удаленная консоль					
0x78h	G	R	R	R	Переустановка контроллера консоли
0x79h	G	R	R	A	Отключение контроллера консоли
0x7Ah	G	R	A	R	Включение контроллера консоли

Контрольная точка	Расшифровка показаний диагностических индикаторов				Описание
	G=зеленый, R=красный, A=желтый				
	MSB	**Бит 1**	**Бит 2**	**LSB**	
Клавиатура (PS2 или USB)					
0x90h	R	Не горит	Не горит	R	Перезагрузка клавиатуры
0x91h	R	Не горит	Не горит	A	Отключить клавиатуру
0x92h	R	Не горит	G	R	Обнаружение присутствия клавиатуры
0x93h	R	Не горит	G	A	Включение клавиатуры
0x94h	R	G	Не горит	R	Очистка входного буфера клавиатуры
0x95h	R	G	Не горит	A	Информация о контроллере клавиатуры – запуск самотестирования (только PS2)
Мышь (PS2 или USB)					
0x98h	A	Не горит	Не горит	R	Переустановка мыши
0x99h	A	Не горит	Не горит	A	Обнаружение мыши
0x9Ah	A	Не горит	G	R	Определение наличия мыши
0x9Bh	A	Не горит	G	A	Включение мыши
Стационарные носители					
0xB0h	R	Не горит	R	R	Перезагрузка устройства хранения данных
0xB1h	R	Не горит	R	A	Отключение устройства хранения данных
0xB2h	R	Не горит	A	R	Обнаружение наличия устройства хранения данных (обнаружение жесткого диска IDE, и т.п.)
0xB3h	R	Не горит	A	A	Включение / настройка стационарного устройства хранения данных
Съемные носители					
0xB8h	A	Не горит	R	R	Перезагрузка съемного дисковода
0xB9h	A	Не горит	R	A	Отключение съемного дисковода
0xBAh	A	Не горит	A	R	Обнаружение съемного дисковода (CD-ROM дисковода IDE, и т.п.)
0xBCh	A	G	R	R	Включение / настройка съемного дисковода
Выбор загрузочного устройства					
0xD0	R	R	Не горит	R	Выбор загрузочных устройств
0xD1	R	R	Не горит	A	Выбор загрузочных устройств
0xD2	R	R	G	R	Выбор загрузочных устройств
0xD3	R	R	G	A	Выбор загрузочных устройств
0xD4	R	A	Не горит	R	Выбор загрузочных устройств
0xD5	R	A	Не горит	A	Выбор загрузочных устройств
0xD6	R	A	G	R	Выбор загрузочных устройств
0xD7	R	A	G	A	Выбор загрузочных устройств
0xD8	A	R	Не горит	R	Выбор загрузочных устройств
0xD9	A	R	Не горит	A	Выбор загрузочных устройств
0XDA	A	R	G	R	Выбор загрузочных устройств
0xDB	A	R	G	A	Выбор загрузочных устройств
0xDC	A	A	Не горит	R	Выбор загрузочных устройств
0xDE	A	A	G	R	Выбор загрузочных устройств
0xDF	A	A	G	A	Выбор загрузочных устройств

Контрольная точка	Расшифровка показаний диагностических индикаторов				Описание
	G=зеленый, R=красный, A=желтый				
	MSB	**Бит 1**	**Бит 2**	**LSB**	
Ядро PEI					
0xE0h	R	R	R	Не горит	Начало распределения модулей предварительной инициализации (PEIM)
0xE2h	R	R	A	Не горит	Память обнаружена, настроена и установлена правильно
0xE1h	R	R	R	G	Зарезервирована для использования модуля инициализации (PEIM)
0xE3h	R	R	A	G	Зарезервирована для использования модуля инициализации (PEIM)
Ядро DXE					
0xE4h	R	A	R	Не горит	Начат этап выполнения драйвера EFI (DXE)
0xE5h	R	A	R	G	Начало распределения драйверов
0xE6h	R	A	A	Не горит	Начало соединения драйверов
Драйверы DXE					
0xE7h	R	A	A	G	Ожидание воода данных пользователем
0xE8h	A	R	R	Не горит	Проверка пароля
0xE9h	A	R	R	G	Вход в утилиту BIOS Setup
0xEAh	A	R	A	Не горит	Обновление флэш-памяти
0xEEh	A	A	A	Не горит	Вызов Int 19. Один звуковой сигнал, если не включена загрузка без вывода информационных сообщений
0xEFh	A	A	A	G	Неустранимая ошибка при загрузке / ошибка выхода из состояния S3
Этап времени исполнения / Загрузка ОС EFI					
0xF4h	R	A	R	R	Вход в режим сна
0xF5h	R	A	R	A	Выход из режима сна
0xF8h	A	R	R	R	Операционная система отправила запрос на закрытие загрузочных служб EFI (ExitBootServices ( ))
0xF9h	A	R	R	A	Операционная система переключилась в режим виртуальной адресации (SetVirtualAddressMap ( ))
0xFAh	A	R	A	R	Операционная система отправила запрос на перезагрузку системы (ResetSystem ( ))
Модуль Pre-EFI Initialization Module (PEIM) / Восстановление					
0x30h	Не горит	Не горит	R	R	Критическое восстановление по запросу пользователя
0x31h	Не горит	Не горит	R	A	Критическое восстановление по запросу ПО (ошибка)
0x34h	Не горит	G	R	R	Загрузка блока критического восстановления
0x35h	Не горит	G	R	A	Передача управления блоку критического восстановления
0x3Fh	G	G	A	A	Не удается завершить критическое восстановление.

5.3.3 Сообщения об ошибках POST и обработка ошибок

При наличии соответствующей возможности BIOS отображает коды хода процедуры POST на мониторе. Эти коды представляют собой строки из 32-разрядных чисел, которые могут сопровождаться комментариями. 32-разрядные числа включают информацию о классе, подклассе и операциях. Поля класса и подкласса указывают на тип инициализируемого оборудования. Поле операций представляет конкретное действие по инициализации. Основываясь на доступной ширине данных для отображения кода процедуры POST, вид отображения этих кодов можно изменять. Чем больше разрядов данных будет доступно, тем подробнее будет информация. Коды хода процедуры POST могут выводиться BIOS или дополнительными ПЗУ.

Раздел «Реакция» в следующей таблице делится на две части:

- **Пауза:** На экране выводится сообщение, в журнале регистрируется ошибка, и для продолжения загрузки требуется команда пользователя. Пользователь может немедленно предпринять действия по устранению проблемы или продолжить загрузку.
- **Остановка:** На экране выводится сообщение, ошибка регистрируется в журнале событий системы, и загрузка системы становится невозможной до устранения ошибки. Пользователь должен заменить неисправный компонент и перезагрузить систему.

Таблица 50. Сообщения об ошибках POST и обработка ошибок

Код ошибки	Сообщение об ошибке	Response
004C	Keyboard/Interface Error	Пауза
0012	CMOS date / time not set	Пауза
5220	Configuration cleared by jumper	Пауза
5221	Passwords cleared by jumper	Пауза
5223	Configuration default loaded	Пауза
0048	Password check failed	Остановка
0141	PCI resource conflict	Пауза
0146	Insufficient memory to shadow PCI ROM	Пауза
8110	Processor 01 internal error (IERR) on last boot	Пауза
8111	Processor 02 internal error (IERR) on last boot	Пауза
8120	Processor 01 thermal trip error on last boot	Пауза
8121	Processor 02 thermal trip error on last boot	Пауза
8130	Processor 01 disabled	Пауза
8131	Processor 02 disabled	Пауза
8160	Processor 01 unable to apply BIOS update	Пауза
8161	Processor 02 unable to apply BIOS update	Пауза
8190	Watchdog timer failed on last boot	Пауза
8198	Operating system boot watchdog timer expired on last boot	Пауза
0192	L3 cache size mismatch	Остановка
0194	CPUID, Processor family are different	Остановка
0195	Front side bus mismatch	Пауза
0197	Processor speeds mismatched	Пауза
8300	Baseboard management controller failed self-test	Пауза
8306	Front panel controller locked	Пауза
8305	Hotswap controller failed	Пауза
84F2	Baseboard management controller failed to respond	Пауза
84F3	Baseboard management controller in update mode	Пауза
84F4	Sensor data record empty	Пауза
84FF	System event log full	Пауза
8500	Memory Component could not be configured in the selected RAS mode	Пауза
8520	DIMM_A1 failed Self Test (BIST)	Пауза
8521	DIMM_A2 failed Self Test (BIST)	Пауза
8522	DIMM_A3 failed Self Test (BIST)	Пауза
8523	DIMM_A4 failed Self Test (BIST)	Пауза
8524	DIMM_B1 failed Self Test (BIST)	Пауза
8525	DIMM_B2 failed Self Test (BIST)	Пауза
8526	DIMM_B3 failed Self Test (BIST)	Пауза
8527	DIMM_B4 failed Self Test (BIST)	Пауза
8528	DIMM_C1 failed Self Test (BIST)	Пауза
8529	DIMM_C2 failed Self Test (BIST)	Пауза
852A	DIMM_C3 failed Self Test (BIST)	Пауза
852B	DIMM_C4 failed Self Test (BIST)	Пауза

Код ошибки	Сообщение об ошибке	Response
852C	DIMM_D1 failed Self Test (BIST)	Пауза
852D	DIMM_D2 failed Self Test (BIST)	Пауза
852E	DIMM_D3 failed Self Test (BIST)	Пауза
852F	DIMM_D4 failed Self Test (BIST)	Пауза
8540	Memory Component lost redundancy during the last boot	Пауза
8580	DIMM_A1 Correctable ECC error encountered	Пауза
8581	DIMM_A2 Correctable ECC error encountered	Пауза
8582	DIMM_A3 Correctable ECC error encountered	Пауза
8583	DIMM_A4 Correctable ECC error encountered	Пауза
8584	DIMM_B1 Correctable ECC error encountered	Пауза
8585	DIMM_B2 Correctable ECC error encountered	Пауза
8586	DIMM_B3 Correctable ECC error encountered	Пауза
8587	DIMM_B4 Correctable ECC error encountered	Пауза
8588	DIMM_C1 Correctable ECC error encountered	Пауза
8589	DIMM_C2 Correctable ECC error encountered	Пауза
858A	DIMM_C3 Correctable ECC error encountered	Пауза
858B	DIMM_C4 Correctable ECC error encountered	Пауза
858C	DIMM_D1 Correctable ECC error encountered	Пауза
858D	DIMM_D2 Correctable ECC error encountered	Пауза
858E	DIMM_D3 Correctable ECC error encountered	Пауза
858F	DIMM_D4 Correctable ECC error encountered	Пауза
8600	Primary and secondary BIOS IDs do not match	Пауза
8601	Override jumper is set to force boot from lower alternate BIOS bank of flash ROM	Пауза
8602	WatchDog timer expired (secondary BIOS may be bad!)	Пауза
8603	Secondary BIOS checksum fail	Пауза

5.3.4 Звуковые сигналы об ошибках во время тестирования системы при включении

В таблице ниже перечислены звуковые сигналы об ошибках, обнаруженных во время тестирования системы при включении. BIOS использует эти коды для информирования пользователей об ошибках до инициализации изображения. Звуковые коды сопровождаются визуальными кодами на диагностических индикаторах.

Таблица 51. Звуковые сигналы об ошибках во время тестирования системы при включении

Звуковые сигналы	Сообщение об ошибке	Коды хода POST	Описание
3	Ошибка памяти		Система была остановлена из-за обнаружения критической ошибки, относящейся к памяти.
6	Ошибка восстановления BIOS		Система обнаружила ошибку BIOS и восстанавливает предыдущую работоспособную версию BIOS.

5.3.5 Опция POST Error Pause

Для ошибок POST отмеченных Пауза, BIOS входит в Менеджер ошибок и ждет пока пользователь не нажмет соответствующую клавишу, и только потом осуществляет загрузку ОС или вход в программу BIOS Setup.

Пользователь может отключить опцию POST Error Pause в меню Main программы BIOS Setup. При отключении опции POST Error Pause, система будет загружать операционную систему без вмешательства пользователя. По умолчанию эта опция включена.

Глоссарий

В данном приложении содержатся термины, используемые в предшествующих главах. Для удобства использования сначала приведены термины, начинающиеся с цифр (например, «82460GX»), а затем остальные термины в алфавитном порядке (например, «ACPI»). Затем в первую очередь вводятся акронимы, а затем идут простые термины.

Термин	Определение
Интерфейс ACPI	Расширенный интерфейс конфигурации и питания
ADC	Аналого-цифровой преобразователь
AP	Процессор приложений
API	Интерфейс API
APIC	Расширенный программируемый контроллер прерываний
ASIC	Специализированная интегральная схема
ASMI	Улучшенный интерфейс управления сервером
ASR	Асинхронная перезагрузка
BIOS	Базовая система ввода/вывода (Basic Input-Output System)
BIST	Встроенный модуль автоматического тестирования
BMC	Контроллер управления шиной
Bridge	Цепь, соединяющая две компьютерные шины и позволяющая агенту одной шины получать доступ к другой шине
BSP	Загрузочный процессор
byte	8 бит
CBC	Контроллер моста между корпусами (микроконтроллер, подключенный к одному или нескольким другим таким контроллерам, вместе эти контроллеры соединяют шины IPMB нескольких корпусов
CEK	Набор CEK
CHAP	Протокол Challenge Handshake Authentication Protocol
CMOS	В настоящей спецификации данный термин означает PC-AT-совместимый участок памяти объемом 128 байт с резервным питанием от батареи, обычно располагающийся на серверной системной плате
DPC	Прямое управление платформой
EEPROM	EEPROM
EHCI	Расширенный интерфейс хост-контроллера
EMP	Порт аварийного управления
EPS	Внешняя спецификация продукции
ESB2	Южный мост ESB2
FBD	Память DIMM с полной буферизацией (FB-DIMM)
FMB	Гибкая системная плата
FRB	Отказоустойчивая загрузка
FRU	Заменяемое устройство (Field Replaceable Unit)
ГБ	1024 МБ
GPIO	Устройства ввода/вывода общего назначения
GTL	Логика приемопередатчика Ганнинга
HSC	HSBP
Гц	Герц (1 цикл/сек.)
I2C	Интегрированная внутренняя шина (Inter Integrated Circuit bus)

Термин	Определение
IA	Архитектура Intel®
IBF	Входной буфер
ICH	Блок контроллеров ввода/вывода
ICMB	Интеллектуальная шина управления корпусом (Intelligent Chassis Management Bus)
IERR	Внутренняя ошибка
IFB	Системы ввода/вывода и мосты для встроенного ПО.
INTR	Прерывание
IP	Протокол Интернет
IPMB	Шина интеллектуального управления платформой
IPMI	Интерфейс интеллектуального управления платформой
IR	Инфракрасный
ITP	Внутренний зонд (In Target Probe)
КБ	1024 байт
KCS	Стиль контроллера клавиатуры (Keyboard Controller Style)
ЛС	Локальная сеть.
LCD	Жидкокристаллический дисплей
Индикатор	Светодиод
LPC	Малое количество контактов (Low pin count)
LUN	Номер логического устройства
MAC	Контроль доступа к среде
МБ	1024 КБ
MCH	Контроллер-концентратор памяти
MD2	Дайджест сообщений 2 – Алгоритм кэширования
MD5	Дайджест сообщений 5 – Алгоритм кэширования – Высокая безопасность
мс	Миллисекунда
MTTR	Реестр типов модулей памяти
Mux	Мультиплексор
NIC	Сетевой адаптер
NMI	Немаскируемый прерыватель
OBF	Выходной буфер
OEM	Изготовитель комплектного оборудования
Ohm	Ом, единица электрического сопротивления
PEF	Фильтрация событий платформы (Platform Event Filtering)
PEP	Сообщение на пейджер о событиях платформы
PIA	Информационная область платформы (настройка встроенного ПО платформы)
PLD	Программируемое логическое устройство
PMI	Прерывание управления платформой
POST	Тестирование системы при включении (Power-on Self Test)
PSMI	Интерфейс управления блоком питания
PWM	Широтно-импульсная модуляция
RAM	Оперативное запоминающее устройство, ОЗУ
RASUM	Надежность, непрерывность работы, эксплуатационная пригодность, удобство и управляемость
RISC	Вычисления с сокращенным набором команд (Reduced instruction set computing)

Термин	Определение
ROM	постоянное запоминающее устройство, ПЗУ
RTC	Часы реального времени (компонент периферийной микросхемы ICH)
SCI	Прерывание системного управления.
SDR	Запись показаний датчика (Sensor Data Record)
5000	Наборы микросхем применяемые в серверных платах.
SECC	Корпус с односторонними контактами
SEEPROM	Последовательная электронно-перепрограммируемая постоянная память
SEL	Журнал событий системы
SIO	Ввод/вывод сервера
SMI	Прерывание управления сервером (SMI имеет самый высокий приоритет среди немаскируемых прерываний)
SMM	Режим управления системой
SMS	Программное обеспечение для управления серверами
SNMP	Простой протокол управления сетью
подлежит определению	Подлежит определению
TIM	Материал теплопроводящей прокладки
UART	Универсальный асинхронный приемопередатчик
UDP	Протокол пользовательских дейтаграмм
UHCI	Интерфейс универсального хост-контроллера
UTC	Универсальный координатор времени
VID	Идентификация уровня напряжения
VRD	Регулятор напряжения (VRD)
Слово	16-битное количество
ZIF	Разъем с нулевым усилием сочленения

Справочная документация

Дополнительную информацию можно получить из следующих документов:

- Спецификация интерфейса ICPI, версия 1.0b. 1996, 1997, 1998. Корпорация Intel, корпорация Microsoft*, Корпорация Toshiba.
- Разработано для теста R18. BIOS/ Встроенное ПО Корпорация Intel.
- Выделение адресов I2C , версия 1.13. 1997. Корпорация Intel.
- Спецификация IPMI 1.0, версия 1,5. 2000. Корпорация Intel, компания Hewlett-Packard, корпорация NEC , корпорация Dell Computer.
- Определение хранения информации FRU для управления платформой, версия 1.0. 1998. Корпорация Intel, компания Hewlett-Packard, корпорация NEC , корпорация Dell Computer. http://developer.intel.com/design/servers/ipmi/spec.htm
- Информационный материал по управлению питания серверов, версия 0.93. 5 ноября 1998 года. Корпорация Intel.
- Спецификация SMBus, корпорация Intel.

Процессор

- AP-485 Идентификация процессоров Intel и функция CPUID. http://www.intel.com/design/xeon/applnots/241618.htm

Набор микросхем

- TBD

Стандарты

- Расширенная спецификация по конфигурированию и интерфейсу питания, версия 1,0b, февраль 1999 года, http://www.acpi.info/
- Спецификация загрузочных CD-дисков El Torito, версия 1.0., http://www.phoenix.com/NR/rdonlyres/98D3219C-9CC9-4DF5-B496-A286D893E36A/0/specscdrom.pdf
- Спецификация Extensible Firmware Interface Reference, версия 1.0., http://www.intel.com/technology/efi/index.htm
- Спецификация Extensible Firmware Interface Reference, версия 1.1, http://www.intel.com/technology/efi/index.htm
- Спецификация IPMI версия 1.5 http://developer.intel.com/design/servers/ipmi/spec.htm
- Спецификация IPMI версия 2,0 http://developer.intel.com/design/servers/ipmi/spec.htm
- Руководство Microsoft по проектированию автоматических устройств. http://www.microsoft.com/whdc/system/platform/64bit/64bitsystems.mspx
- Рекомендации по проектированию сетевых систем, версия 1.0, http://www.intel.com/managedpc/standard
- Руководство по разработке системы PC99, http://www.pcdesguide.com/
- Спецификация локальной шины PCI, версия 2.2, http://www.pcisig.org/

- Спецификация моста PCI-PCI, версия 1.1, http://www.pcisig.org/
- Спецификация PCI BIOS, версия 2.1, http://www.pcisig.org/
- Спецификация управления питанием PCI, версия 1.0, http://www.pcisig.org/
- *Спецификация маршрутизации IRQ на шине PCI*, версия 1.0, корпорация Microsoft.
- Спецификация менеджера памяти POST, версия 1.01, http://www.phoenix.com/NR/rdonlyres/873A00CF-33AC-4775-B77E-08E7B9754993/0/specspmm101.pdf
- Спецификация Plug and Play BIOS, версия 1.0a http://www.microsoft.com/whdc/system/pnppwr/pnp/default.mspx
- Спецификация SMBIOS, версия 2.4, http://www.dmtf.org/standards/published_documents/DSP0134.pdf
- Спецификация EFI, версия 1.10 http://www.intel.com/technology/efi/main_specification.htm
- Спецификация USB, версия 1.1, http://www.intel.com/technology/usb/spec.htm
- Спецификация WFM, версия 2.0, http://www.intel.com/design/archives/wfm/downloads/base20.htm