Руководство пользователя

Серия QSRV E-R/P-R

Оглавление

Заявление

Заявление об авторских и исключительных правах

Это руководство, включая, но не ограничиваясь всей содержащейся в нем информацией, защищено положениями законодательства об исключительных и авторских правах. Без разрешения QTECH никто не может заниматься какими-либо действиями, такими как имитация, копирование, извлечение информации, пересылка или другие формы использования.

Отказ от ответственности

Настоящее руководство предназначено для справочных целей при использовании программно-аппаратного комплекса (устройства).

QTECH предоставляет это руководство "как есть" и в той мере, в какой это разрешено законом, не дает никаких явных или подразумеваемых гарантий, включая, помимо прочего, товарную пригодность, пригодность для определенной цели, ненарушение каких-либо прав других лиц и любые гарантии относительно использования или невозможности использования этого руководства. QTECH также не дает никаких гарантий относительно точности или надежности любой информации, полученной с помощью этого руководства.

Из-за обновлений версии продукта или по другим причинам содержимое этого руководства может периодически обновляться. QTECH оставляет за собой право вносить изменения в содержание настоящего руководства в любое время без предварительного уведомления.

Если не указано иное, это руководство предоставляется исключительно в качестве руководства по использованию, и пользователи несут все риски, связанные с использованием этого руководства.

Заявление о товарном знаке

Microsoft® и Windows являются товарными знаками группы компаний Microsoft.

Linux® является зарегистрированной торговой маркой Linus Torvalds.

Aspeed® является торговой маркой ASPEED Technology Inc.

QTECH® является торговой маркой ООО «КЬЮТЭК».

Права собственности на другие товарные знаки принадлежат их владельцам.

1. ВВЕДЕНИЕ

В этой главе приведен краткий обзор функций и особенностей серверной платформы QTECH серии QSRV E-R/P-R.

В дополнение к материнской плате и корпусу перечислены несколько важных конструктивных частей, входящих в систему.

Таблица 1. Перечень основных частей

Описание	Количество
Радиатор процессора	1–2
Вентиляторы	3
Держатель HDD с горячей заменой	12
Объединительная плата HDD	3
Комплект установочных рельсов	1

1.1. Распаковка системы

Осмотрите коробку, в которой была доставлена серверная платформа **QTECH серии QSRV E-R/P-R**, и обратите внимание, если упаковка была повреждена каким-либо образом. Если какое-либо оборудование окажется повреждённым, подайте заявление о возмещении ущерба перевозчику, который его доставил.

Определите подходящее место для стойки, в которой будет установлена серверная платформа. Она должна располагаться в чистом, без пыли, хорошо вентилируемом помещении. Избегайте помещений со сторонним выделением тепла и находящихся в области электрических шумов и электромагнитные полей. Также необходима розетка переменного тока с заземлением.

2. ОПИСАНИЕ КОРПУСА

В данной главе описывается стандартный корпус 2U производимый компанией QTECH, который включает в себя: систему охлаждения, систему для быстрой замены дисков, бэкплейн дисков или экспандер, панель индикации и управления, панель USB 3.0.

Рисунок 2-1. Внешний вид корпуса

2.1. Характеристики корпуса

Таблица 2. Характеристики корпуса

Формфактор корпуса	**2U**
Типоразмер диска	3,5 дюйма
Поддержка дисков SAS/SATA 12 Гбит	да
Поддержка бэкплэйном SGPIO Bus	да
Количество жестких дисков	до 12
Количество и тип плат расширения	2FS+1HS
USB 3.0 на фронтальной панели	2
Плата управления и индикации	да
Размер поддерживаемых вентиляторов	80×80×38 мм
Быстрая замена вентиляторов	да
Количество вентиляторов	3 шт

Формфактор корпуса	2U
Рабочие температуры	+10 °C – +35 °C
Габариты	88×435×657 мм
Гарантия	1 год

2.2. Компоненты корпуса

2.2.1. Передняя панель корпуса

На передней панели корпуса находятся:

- 12 кассет для горячей замены дисков (от 4 до 12 в зависимости от исполнения);
- панели индикации и управления;
- 2 порта USB 3.0;
- ручки для выдвижения корпуса из стойки, с отверстием для доступа к кронштейну;
- кронштейн крепления к стойке.

Рисунок 2-2. Передняя панель корпуса

2.2.1.1. Панель индикации и управления

На панели индикации находятся и кнопки управления.

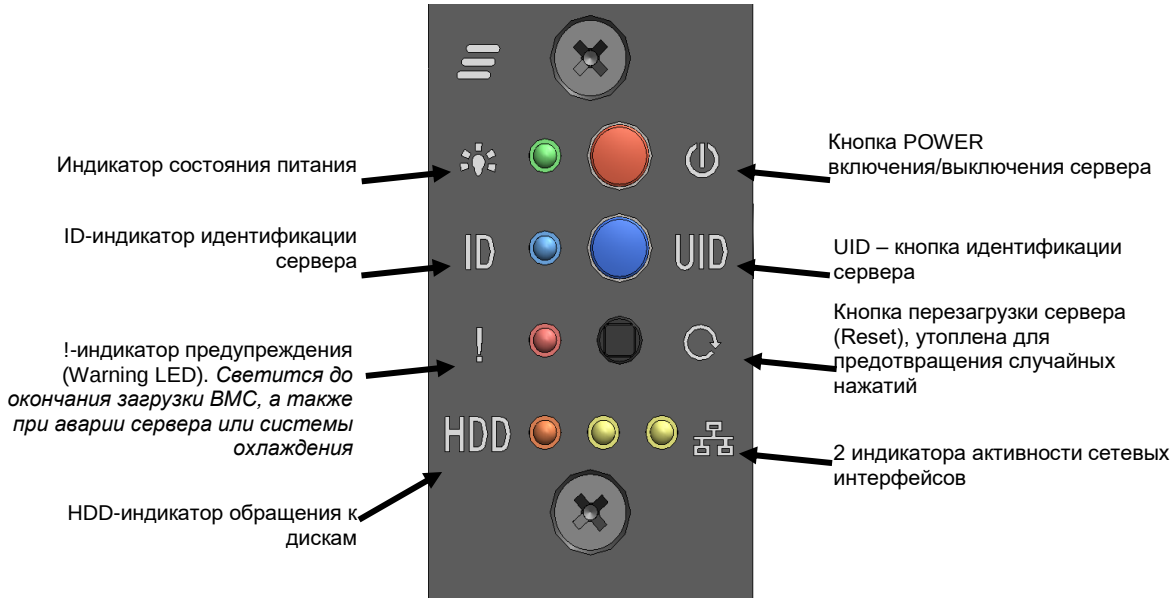


Рисунок 2-3. Панель индикации и управления

2.2.1.2. Индикатор активности накопительного устройства

На передней панели кассеты жестких дисков имеется два индикатора оранжевого и зеленого цвета. Режим работы и комбинации свечения индикаторов определяется стандартом.

Рисунок 2-4. Внешний вид модуля SAS/SATA жестких дисков

2.2.1.3. Кассеты жестких дисков

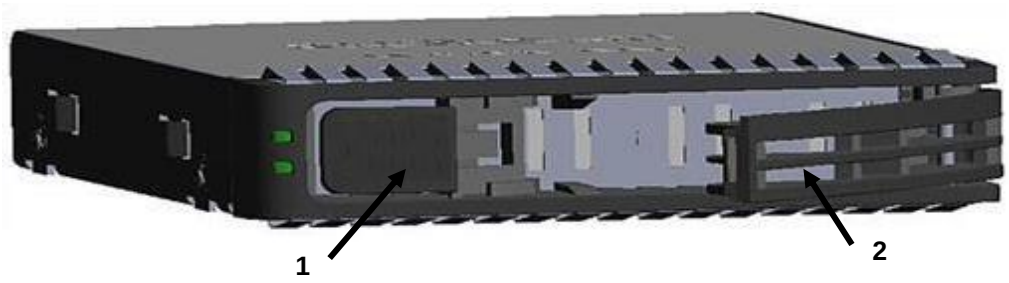


Рисунок 2-5. Кассета жесткого диска SAS/SATA

2.2.1.3.1. Извлечение и установка кассет:

Чтобы вынуть кассету с жестким диском:

- нажмите кнопку **1**, что приведет к откидыванию ручки **2**;
- для выдвижения кассеты потяните за ручку **2**. Чтобы вставить кассету жесткого диска;
- аккуратно вставьте кассету с открытой ручкой **2** в отсек и задвиньте его внутрь до упора;
- закройте ручку **2** до фиксации.

2.2.1.3.2. Установка жесткого диска 3,5 дюйма в кассету

Демонтируйте заглушку диска, сохраните винты крепления заглушки. Сориентируйте диск так чтоб разъем подключения находился сзади, разместите диск так чтобы совпали крепежные отверстия на нижней части с отверстиями кассеты, и зафиксируйте диск винтами, идущими в комплекте поставки.

Для установки диска 2.5 дюйма используйте винты, крепящие заглушку диска.

ВНИМАНИЕ: ДЛЯ ОБЕСПЕЧЕНИЯ ТЕПЛОВЫХ РЕЖИМОВ ВСЕХ ДИСКОВ, В КАССЕТЫ ЖЕСТКИХ ДИСКОВ ДОЛЖНЫ БЫТЬ ВСТАВЛЕНЫ НАКОПИТЕЛИ (SSD ИЛИ HDD) ИЛИ УСТАНОВЛЕНЫ ЗАГЛУШКИ, ПОСТАВЛЯЕМЫЕ С КАССЕТОЙ.

2.2.2. Задняя панель корпуса

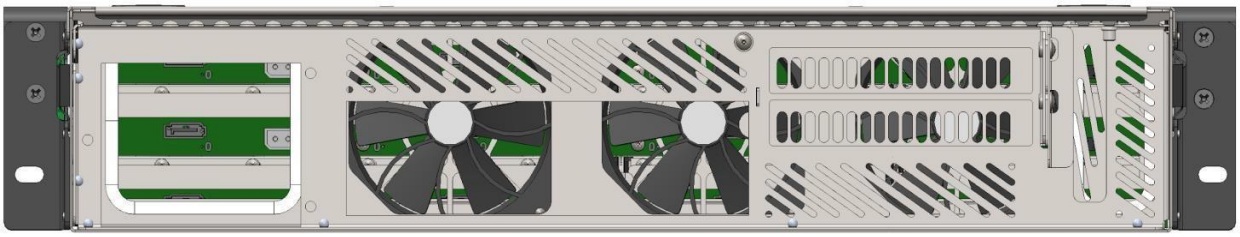


Рисунок 2-6. Задняя панель корпуса

В корпусе может быть установлено 2 полноформатные карты расширения (устанавливаются через слот и крепятся винтом с правой стороны) и 1 полуформатная карта расширения, которая устанавливается непосредственно в PCIe-разъем материнской платы. Для удобства монтажа карт 2FS предусмотрено отверстия сбоку для заведения отвертки.

Корпус рассчитан на установку несъемного блока питания 550 – 1800 Вт.

2.2.3. Система охлаждения

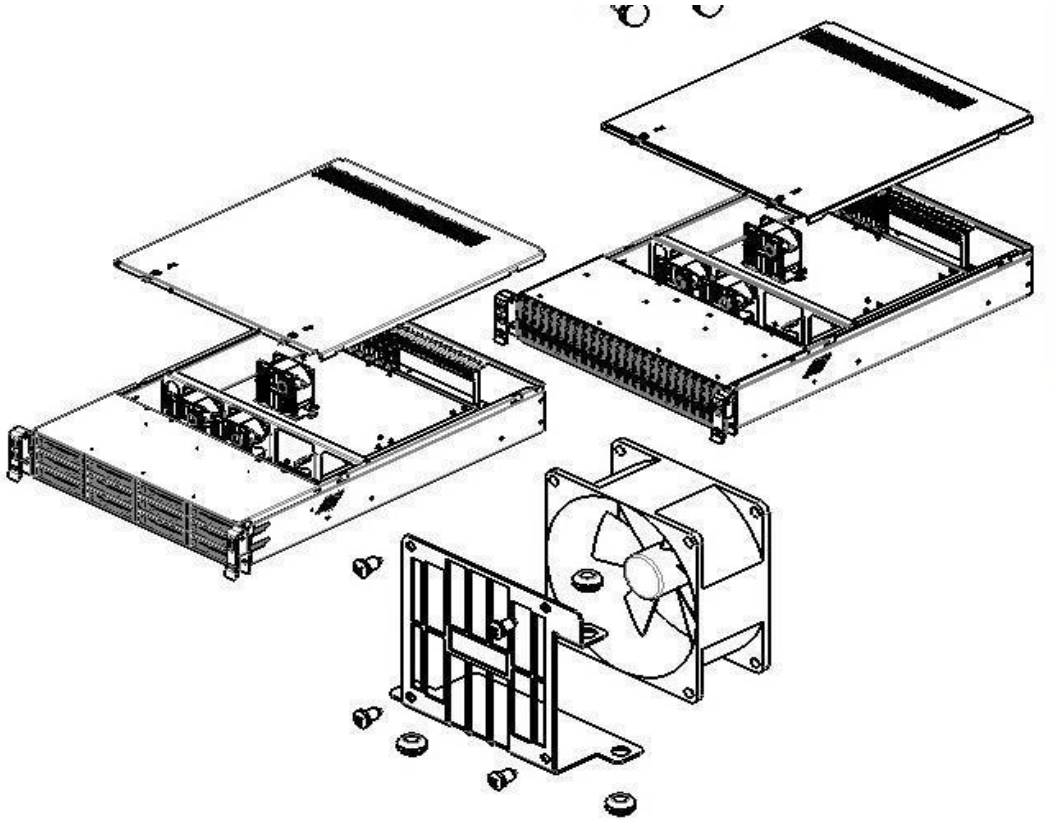


Рисунок 2-7. Система охлаждения

Система охлаждения корпуса обеспечивают возможность функционирования двухпроцессорной системы в диапазоне внешних температур от плюс 10 °С до плюс 35 °С. Температурное состояние системы поддерживается установкой и функциональностью трех 80 мм вентиляторов.

ВНИМАНИЕ: ДЛЯ ОБЕСПЕЧЕНИЯ ТЕПЛОВЫХ РЕЖИМОВ ДИСКОВ, В КАССЕТЫ ЖЕСТКИХ ДИСКОВ ДОЛЖНЫ БЫТЬ ВСТАВЛЕНЫ НАКОПИТЕЛИ (SSD ИЛИ HDD) ИЛИ УСТАНОВЛЕНЫ ЗАГЛУШКИ, ПОСТАВЛЯЕМЫЕ С КАССЕТОЙ.

2.2.3.1.1. Системные вентиляторы

- Каждый вентиляторный модуль обладает демпфирующим эффектом для минимизации вибраций серверного корпуса.

Скорость каждого вентилятора контролируется контроллером, интегрированного в материнскую плату. При достижении предельно высоких или низких значений температурных параметров программно-аппаратные средства контроллера увеличивают или уменьшают скорость определенного вентилятора для регулирования температурных показателей системы.

- С каждого вентилятора в систему менеджмента поступает сигнал от тахометра, что позволяет контролировать его состояние.

В корпус устанавливается до трех вентиляторов. Для замены вентилятора следует выкрутить фиксирующий винт в кассете вентилятора, вытащить разъем из материнской платы и извлечь кассету с вентилятором (Рисунок 2-7). Установку кассеты с новым вентилятором производить в обратной последовательности. Замена вентилятора в кассете производится путем откручивания 4-х винтов. При установке вентилятора в кассету соблюдайте порядок установки, согласно указателю направления движения потока воздуха на вентиляторе. Направление потока воздуха необходимо направлять в заднюю часть корпуса. Вентилятор в кассете нужно установить так чтобы его кабель располагался в соответствии с панелью вентиляторов.

При сборке серверов на “горячих” процессорах рекомендуется подключать вентилятор, находящийся напротив наиболее греющегося процессора, с помощью удлинительного кабеля (в комплекте не поставляется), в разъем FAN_CPU контролирующий обороты для этого процессора.

2.3. Эксплуатация корпуса

2.3.1. Эксплуатационные требования

Сервер предназначен для эксплуатации в закрытом помещении с контролируемой температурой воздуха и следующими условиями:

- температура окружающего воздуха от плюс 10 °С до плюс 35 °С;
- относительная влажность воздуха от 20 % до 80 %;
- атмосферное давление от 85 до 105 кПа;
- согласно «Правилам устройства электроустановок», сопротивление заземляющего контура должно быть не более 4 Ом;
- напряженность внешнего электрического поля согласно ГОСТ 63254-76 не более 0,3 В/м;
- напряженность внешнего магнитного поля не более 200 А/м;
- запыленность окружающего воздуха согласно ГОСТ 16325-76 не более 0,75 мг/м^2;
- в окружающей среде не должно быть паров агрессивных жидкостей и веществ, вызывающих коррозию.

2.3.2. Меры безопасности

Конструкция корпуса обеспечивает надежную защиту специалиста от поражения электрическим током: применение надежных изоляционных материалов и использование кабелей электропитания с заземляющими проводниками.

Обязательно отключайте корпус и все присоединенные устройства от сети путем извлечения сетевых вилок из розеток при любых работах, связанных с открытием корпуса. Помните, что погасший индикатор питания не означает полного снятия напряжения с устройства — блок питания может находиться в дежурном режиме.

Не дотрагивайтесь до вращающихся вентиляторов системы охлаждения корпуса, дождитесь их полной остановки.

3. УСТАНОВКА СИСТЕМЫ

3.1. Обзор

В этой главе содержатся рекомендации и инструкции по установке вашей системы в серверной стойке. Если ваша система еще не полностью интегрирована с процессорами, системной памятью и т. д., обратитесь к Главе 5 за подробной информацией об установке этих конкретных компонентов.

ПРЕДУПРЕЖДЕНИЕ: **ЭЛЕКТРОСТАТИЧЕСКИЙ РАЗРЯД (ESD) МОЖЕТ ПОВРЕДИТЬ ЭЛЕКТРОННЫЕ КОМПОНЕНТЫ. ВО ИЗБЕЖАНИЕ ПОВРЕЖДЕНИЯ ЭЛЕМЕНТОВ, РАСПОЛОЖЕННЫХ НА ПЕЧАТНЫХ ПЛАТАХ, ВАЖНО ИСПОЛЬЗОВАТЬ ЗАЗЕМЛЕННЫЙ БРАСЛЕТ, УДЕРЖИВАТЬ ВСЕ ПЕЧАТНЫЕ ПЛАТЫ ТОЛЬКО ПО КРАЯМ И ХРАНИТЬ ИХ В АНТИСТАТИЧЕСКИХ МЕШКАХ, ЕСЛИ ОНИ НЕ ИСПОЛЬЗУЮТСЯ.**

3.2. Подготовка к установке

Коробка, в которой поставляется система, должна включать части, необходимые для установки в стойку (монтажные рельсы). Прежде чем приступить к установке, прочитайте этот раздел целиком.

3.2.1. Выбор места установки

- Система должна быть расположена в чистом, без пыли, хорошо проветриваемом помещении. Избегайте помещений с посторонним выделением тепла и подверженным электрическим шумам и электромагнитные поля.
- Оставьте достаточно свободного пространства перед стойкой, чтобы вы могли полностью открыть переднюю дверцу (~ 60 см) и приблизительно 75 см зазора от задней части стойки, чтобы обеспечить достаточное пространство для воздушного потока и доступа при обслуживании.
- Этот продукт следует устанавливать только в местах с ограниченным доступом (специальные комнаты для оборудования, шкафы для обслуживания и т. д.).

3.2.2. Меры предосторожности при работе с монтажной стойкой

- Убедитесь, что выравнивающие ножки в нижней части стойки уперты в пол, так что на них приходится полный вес стойки.
- В установках с одной стойкой, к стойке должны быть прикреплены стабилизаторы. В случае с несколькими стойками стойки должны быть соединены между собой.
- Всегда проверяйте стабильность стойки перед тем, как выдвинуть сервер или другой компонент из стойки.
- Вы должны устанавливать только один сервер или компонент за раз — одновременная установка двух или более компонентов в стойку может привести к тому, что стойка потеряет устойчивость.

3.2.3. Меры предосторожности при работе с серверной платформой

- Перед установкой рельсов определите размещение каждого компонента в стойке.
- Сначала установите самые тяжелые серверные компоненты в нижней части стойки, а затем продвигайтесь вверх.

- Используйте источник бесперебойного питания (ИБП), чтобы защитить сервер от скачков и перепадов напряжения и поддерживать работу вашей системы в случае сбоя питания.
- Убедитесь, что компоненты остыли перед тем, как касаться дисков и модулей питания.
- Когда работы по обслуживанию не производятся, держите переднюю дверцу стойки и все крышки/панели закрытыми, чтобы поддерживать надлежащее охлаждение.

3.2.4. Требования к монтажу в стойке

3.2.4.1. Рабочая температура окружающей среды

Если серверная платформа установлена в закрытой или многоблочной стойке, температура окружающей среды в стойке может быть выше, чем температура окружающей среды в помещении. Поэтому следует уделить внимание установке оборудования в среде, совместимой с максимальной номинальной температурой окружающей среды производителя (TMRA).

3.2.4.2. Воздушный поток

Общее количество оборудования в стойке должно соответствовать минимальному проходящему воздушному потоку, необходимому для безопасной работы.

3.2.4.3. Механическая нагрузка

Оборудование должно быть установлено в стойку с равномерным распределением механической нагрузки, чтобы не возникало опасных состояний.

3.2.4.4. Перегрузка цепи

Следует рассмотреть вопрос о подключении оборудования к схеме питания и о влиянии любой возможной перегрузки на максимальную токовую защиту и электропитание. При рассмотрении этой проблемы следует использовать данные о номинальной потребляемой мощности оборудования.

3.2.4.5. Надежное заземление

Надежное заземление должно поддерживаться в любое время. Чтобы обеспечить это, сама стойка должна быть заземлена. Особое внимание следует уделять подключениям блоков питания, отличным от прямых подключений к питающей сети.

Во избежание получения травм при установке или обслуживании данного устройства в стойке необходимо принять особые меры предосторожности, чтобы убедиться, что система остается стабильной.

Следующие рекомендации предоставляются для обеспечения вашей безопасности:

- Данное устройство должно быть установлено в нижней части стойки, если оно является единственным устройством в стойке.
- При установке этого устройства в частично заполненную стойку, загружайте стойку снизу-вверх, располагая самые тяжелые компоненты в нижней части стойки.
- Оборудование на скользящих монтажных рельсах не должно использоваться как полка или рабочее пространство.

ПРЕДУПРЕЖДЕНИЕ: **НЕ ПЕРЕМЕЩАЙТЕ СЕРВЕР С ПОМОЩЬЮ ПЕРЕДНИХ РУЧЕК. ОНИ ПРЕДНАЗНАЧЕНЫ ТОЛЬКО ДЛЯ ВЫТЯГИВАНИЯ СЕРВЕРА ИЗ СТОЙКИ.**

3.3. Установка сервера в стойку

В этом разделе содержится информация об установке корпуса в стойку.

ПРИМЕЧАНИЕ: комплектные рельсы предназначены для установки в стойку шириной от 26 до 33,5 дюйма.

На рынке есть множество стоек, что может означать, что процедура сборки будет немного отличаться от описанной в разделе.

Ниже приведено основное руководство по установке корпуса в стойку с установленным оборудованием. Вы также должны обратиться к инструкциям по установке, которые прилагаются к конкретной стойке, которую вы используете.

3.3.1. Установка рельсов в стойку

Телескопические направляющие рельсы поставляются в собранном состоянии и состоят из двух конструктивных частей (Рисунок 3-1):

- внешней рейки, оснащены двумя кронштейнами для крепления к стойке и сепаратором с шариками;
- внутренней рейки для крепления к корпусу оснащены механизмом фиксации.

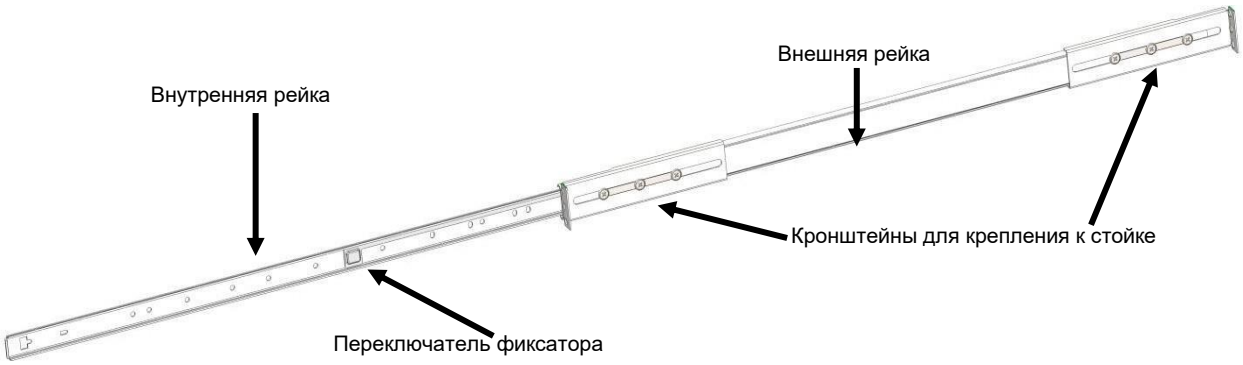


Рисунок 3-1. Телескопические направляющие рельсы (собранное состояние). Внутренняя рейка выдвинута

Перед установкой рельсов в стойку эти части следует разделить. Для этого выдвинуть внутреннюю рейку до щелчка фиксатора, затем при помощи переключателя сдвинуть фиксатор в обратном направлении (от себя) и разъединить части. Для обратной операции, при установке корпуса в стойку, фиксатор следует сдвигать в обратном направлении (к себе).

Оба конца кронштейнов должны быть направлены в одном направлении. Отрегулируйте кронштейны на надлежащее расстояние по глубине стойки и закрепите каждый двумя винтами M5. После закрепления внешней рейки в стойке, сдвиньте свободно перемещающийся сепаратор вплотную к фиксатору, для более раннего контакта с внешней рейкой при будущей установке корпуса. Повторите эти действия для противоположной внешней рейки.

3.3.2. Установка корпуса в стойку

1. Прикрепите внутренние рельсы к шасси винтами M5.
2. Выровняйте рельсы корпуса с внешними рельсами в стойке (Рисунок 3-2).
3. Вдвиньте рельсы шасси в рельсы стойки до замков фиксаторов, прилагая равномерные усилия с обеих сторон. Замки фиксаторов предотвращают

самопроизвольное вдвигание шасси в стойку при проведении работ по обслуживанию шасси.

4. Сдвиньте кнопки левого и правого фиксаторов к себе и продолжите вдвигать шасси по направляющим. Когда сервер полностью вставлен в стойку, вы должны услышать щелчок блокировки.
5. (Дополнительно) Вкрутите винты с насечками на головке для фиксации передней панели сервера к стойке.

Рисунок 3-2. Монтаж шасси в стойку

ПРИМЕЧАНИЕ: рисунок показан только в иллюстративных целях. Всегда устанавливайте серверы в нижней части стойки.

ПРЕДУПРЕЖДЕНИЕ: **ПРЕЖДЕ ЧЕМ ДОСТАВАТЬ УСТРОЙСТВО ДЛЯ ОБСЛУЖИВАНИЯ ПРОВЕРЬТЕ МЕХАНИЗМ ФИКСАЦИИ СТОЙКИ ИЛИ КРЕПЛЕНИЕ СТОЙКИ БОЛТАМИ К ПОЛУ. НЕСТАБИЛЬНОСТЬ СТОЙКИ МОЖЕТ ПРИВЕСТИ К ЕЕ ОПРОКИДЫВАНИЮ.**

4. ОПИСАНИЕ МАТЕРИНСКОЙ ПЛАТЫ

4.1. Описание серверной платы

Серверная материнская плата QTECH 469555.005 представляет собой монолитную сборку печатных плат с функциями, предназначенными для серверов с высокой плотностью монтажа в стойку 1U–4U. На рисунке 4-1 показан общий вид платы с обозначением её основных элементов. На рисунке 4-2 указаны места подключения дополнительных узлов и устройств платы.

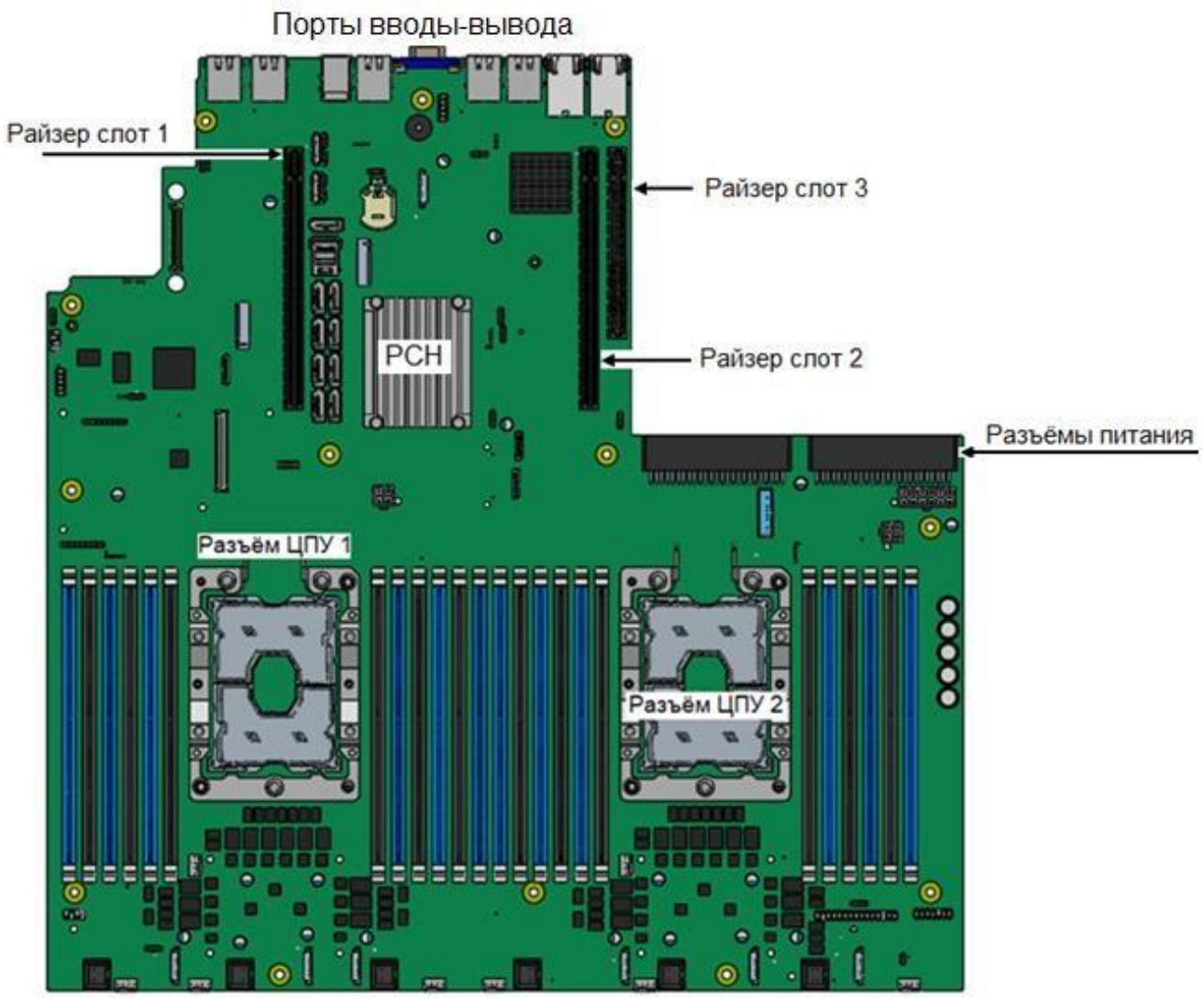


Рисунок 4-1. Серверная плата QTECH 469555.005

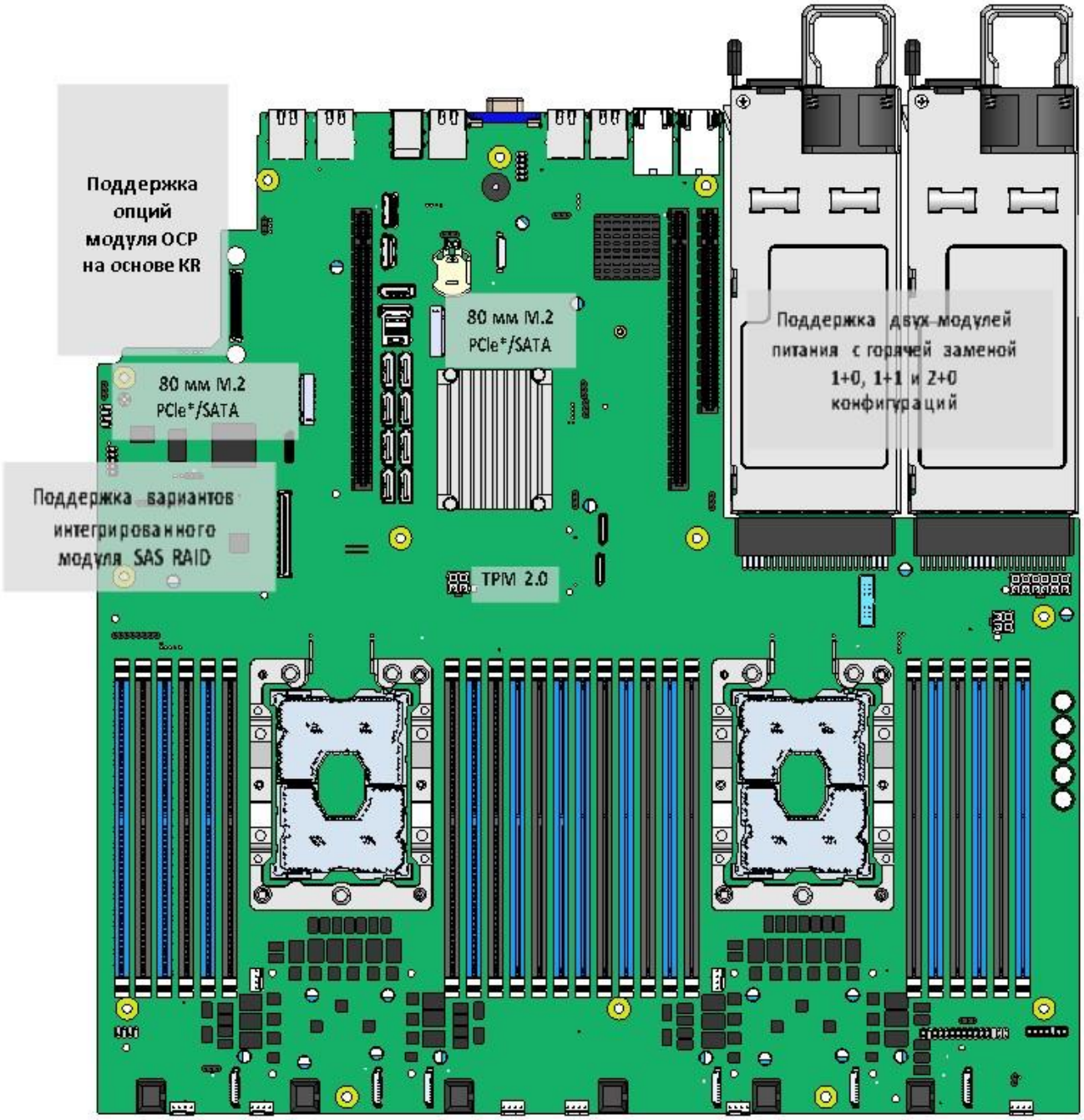


Рисунок 4-2. Серверная плата с доступными встроенными опциями

4.2. Функции серверной платы

В таблице 3 приведен список функций серверной материнской платы.

Таблица 3. Функции серверной платы

Функции	**QTECH 469555.005**
Процессор	2 процессорных разъёма LGA3647-0 (Socket P). Поддержка 1 или 2 процессоров Intel® Xeon® 1 и 2 поколений расширяемого семейства (Platinum, Gold, Silver и Bronze). **ПРИМЕЧАНИЕ:** Процессоры Intel® Xeon® предыдущего поколения не поддерживаются. Максимальная поддерживаемая расчётная тепловая мощность (TDP) до 205 Вт (только плата). Серверные платформы QTECH на базе этой платы могут поддерживать более низкую максимальную расчётную тепловую мощность (TDP)
Объём памяти	24 слота DIMM (по 12 на каждый процессор). DDR4 RDIMM/LRDIMM, до 2933 MT/c, 1,2 В. Совместимый с DDR4 модуль постоянной памяти Intel® Optane™ постоянного тока, до 2666 MT/c, 1,2 В. **ПРИМЕЧАНИЕ:** Максимальная поддерживаемая скорость памяти зависит от SKU установленного процессора и конфигурации набора модулей памяти; Постоянная память Intel® Optane™ DC поддерживается только для процессоров Intel® Xeon® 2 поколения расширяемого семейства (Platinum, Gold, Silver и Bronze)
Набор микросхем Intel® серии C62x	Intel® C621/C624
Локальная сеть (LAN)	×2 порта RJ-45 1 GbE + ×2 порта RJ-45 1 GbE (опция), ×2 RJ-45 10 GbE (только C624) OCP-порт (только C624), IPMI-порт RJ-45 1 GbE
Поддержка модулей OCP	Есть
Поддержка модулей SAS	Есть
Встроенный PCIe* NVMe*	×3 – PCIe* OCuLink Поддержка Intel® VMD Поддержка Intel® VROC (VMD NVMe RAID) (опция)

Функции	QTECH 469555.005
Встроенный SATA	×14 портов SATA 6 Гбит/с (поддерживаются скорости передачи 6 Гбит/с, 3 Гбит/с и 1,5 Гбит/с) ×9 — однопортовых 7-контактных разъемов SATA (8 SATA и 1 sSATA) ×1 — разъёмы M.2/sSATA ×1 — M.2/PCIe ×4 x1 — 4-портовый разъем mini-SAS высокой плотности (HD) (SFF-8643) (4 sSATA). Встроенный программный RAID SATA Intel® VROC (SATA RAID) 6.0 Intel® Embedded Server RAID Technology 2 1.60 с дополнительной поддержкой ключа RAID 5 (подробности см. в пункте 4.16)
Слоты для карт расширения PCIe*	Слот 1: слот PCIe* 3.0 x24 (электрический x8+x16), обрабатываемый ЦПУ1 Слот 2: слот PCIe* 3.0 x24 (электрический x8+x16), обрабатываемый ЦПУ2 Слот 3: слот PCIe* 3.0 x16 (электрический x8+x4), обрабатываемый ЦПУ2
Видео	Видео встроенный 2D-контроллер 16 МБ видеопамяти DDR4 Внешний разъём DB-15
USB	3 — внешние порты USB 3.0 (back panel) 1 — внутренний USB 2.0 типа A разъём 1 — 2×10-контактный разъём с поддержкой передней панели для (2) портов USB 2.0/3.0 1 — 2×5 header 2×USB2.0
Последовательный порт	x1 — разъём внутреннего RS232-порта DH-10 x1 — 3pin header UART
Управление сервером	Встроенный контроллер управления основной платой, совместимый с IPMI 2.0 Поддержка программного обеспечения Intel® Server Management Выделенный встроенный порт управления RJ-45 Расширенное управление сервером с помощью Intel® RMM4 Lite (дополнительная опция)

Функции	QTECH 469555.005
Безопасность	TPM 2.0
Поддержка системных вентиляторов	x2 — 4-контактные разъёмы для вентиляторов процессора x6 — 4–6-контактные разъёмы для передних системных вентиляторов, параллельно 3 типа x1 — вентилятор сзади, система 4-контактный разъём

4.3. Основные элементы серверной платы и их функций

На рисунке 4-3 проиллюстрирован вид всех портов ввода-вывода сверху и со стороны самих разъёмов.

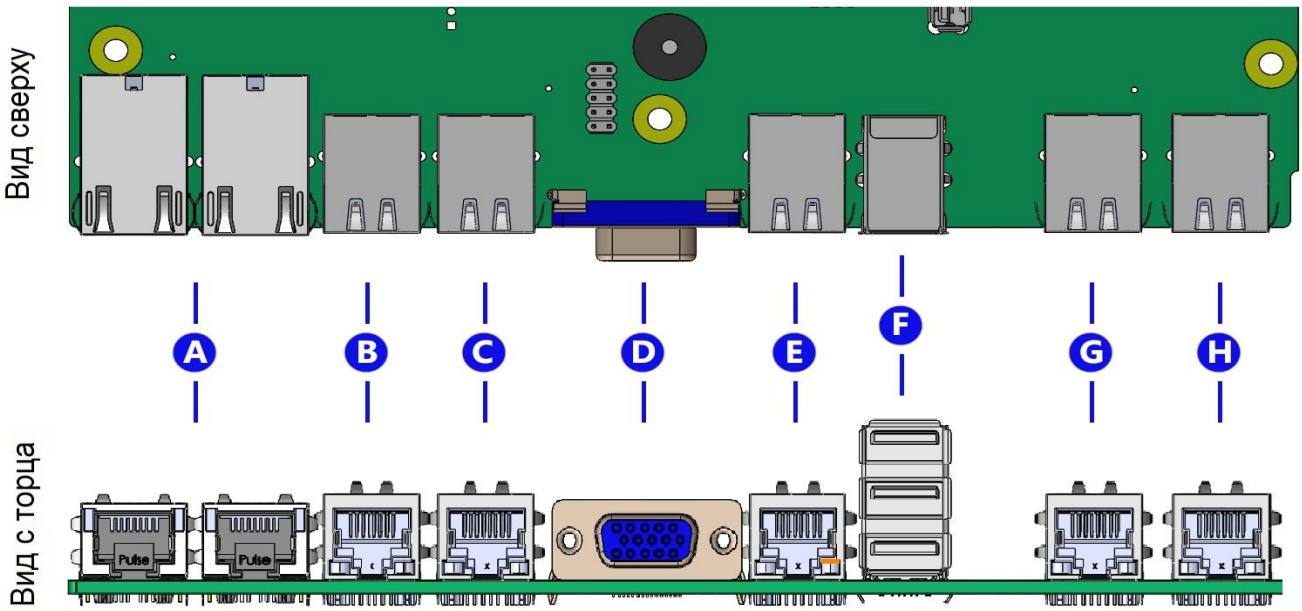


Рисунок 4-3. Разъёмы ввода-вывода

A — Сетевые порты ×2 RJ-45 10 Гбит (опция и только для C624)

B — Сетевой порт RJ-45 1 Гбит i211 (опция)

C — Сетевой порт RJ-45 1 Гбит i211

D — Видеоразъём VGA

E — Сетевой порт RJ-45 1 Гбит i219

F — 3-портовый разъём USB 3.0

G — Сетевой порт RJ-45 1 Гбит i211 (опция)

H — Сетевой порт IPMI RJ-45 1 Гбит

На рисунке 4-4 указаны места расположения светодиодных датчиков состояния и неисправностей процессоров и других рабочих элементов платы. На рисунке 4-5 показаны перемычки для настройки платы.

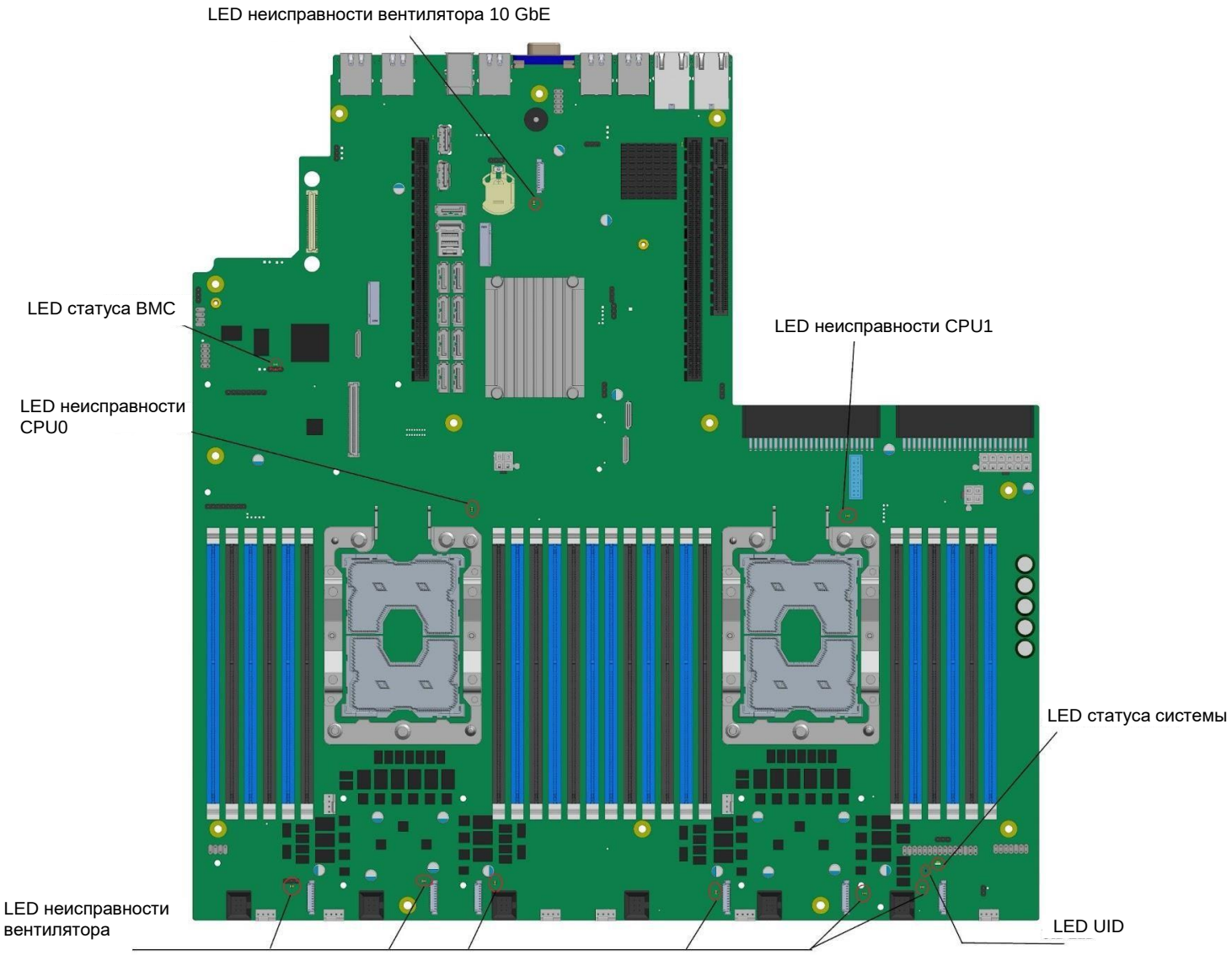


Рисунок 4-4. Датчики состояния платы

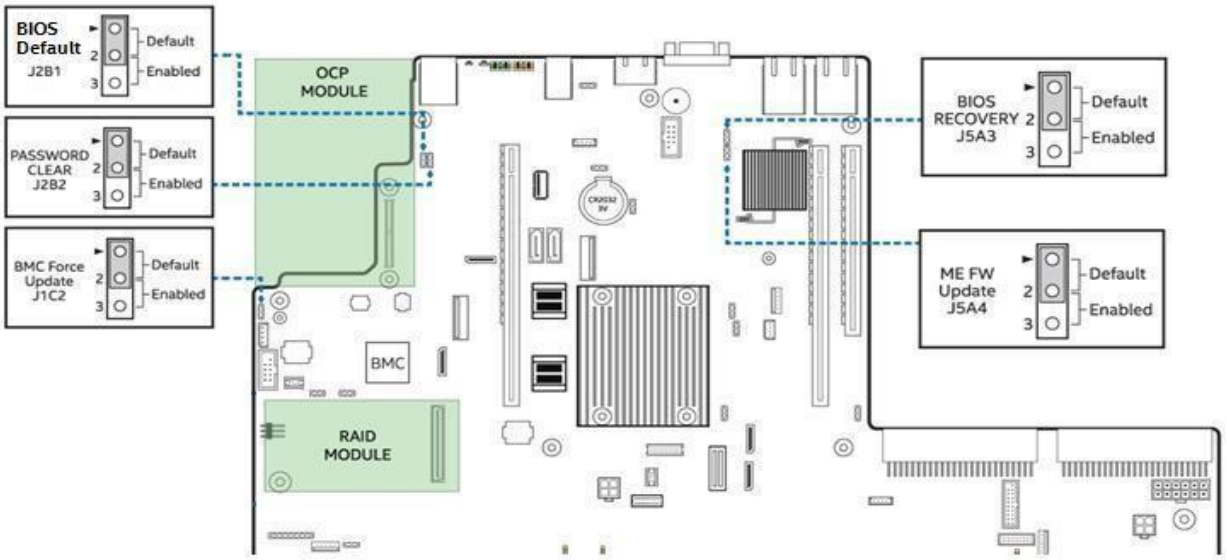


Рисунок 4-5. Перемычки для настройки платы

4.4. Архитектура серверной платы

Архитектура серверной материнской платы QTECH 469555.005 строится на основе масштабируемого семейства процессоров Intel® Xeon® Scalable, чипсета Intel® C621/C624 (PCH), Ethernet-контроллера Intel® X722 (опция), обеспечивающего 10-гигабитный Ethernet на основе физического преобразователя PHY, встроенного в Ethernet-соединение X557-AT2 (опция), а также контроллера, следящего за состоянием серверной платы (BMC) семейства Aspeed AST2500.

Архитектура представлена на рисунке 4-6 в виде блок-схемы, показывающей функции и взаимосвязи каждого из основных компонентов подсистемы.

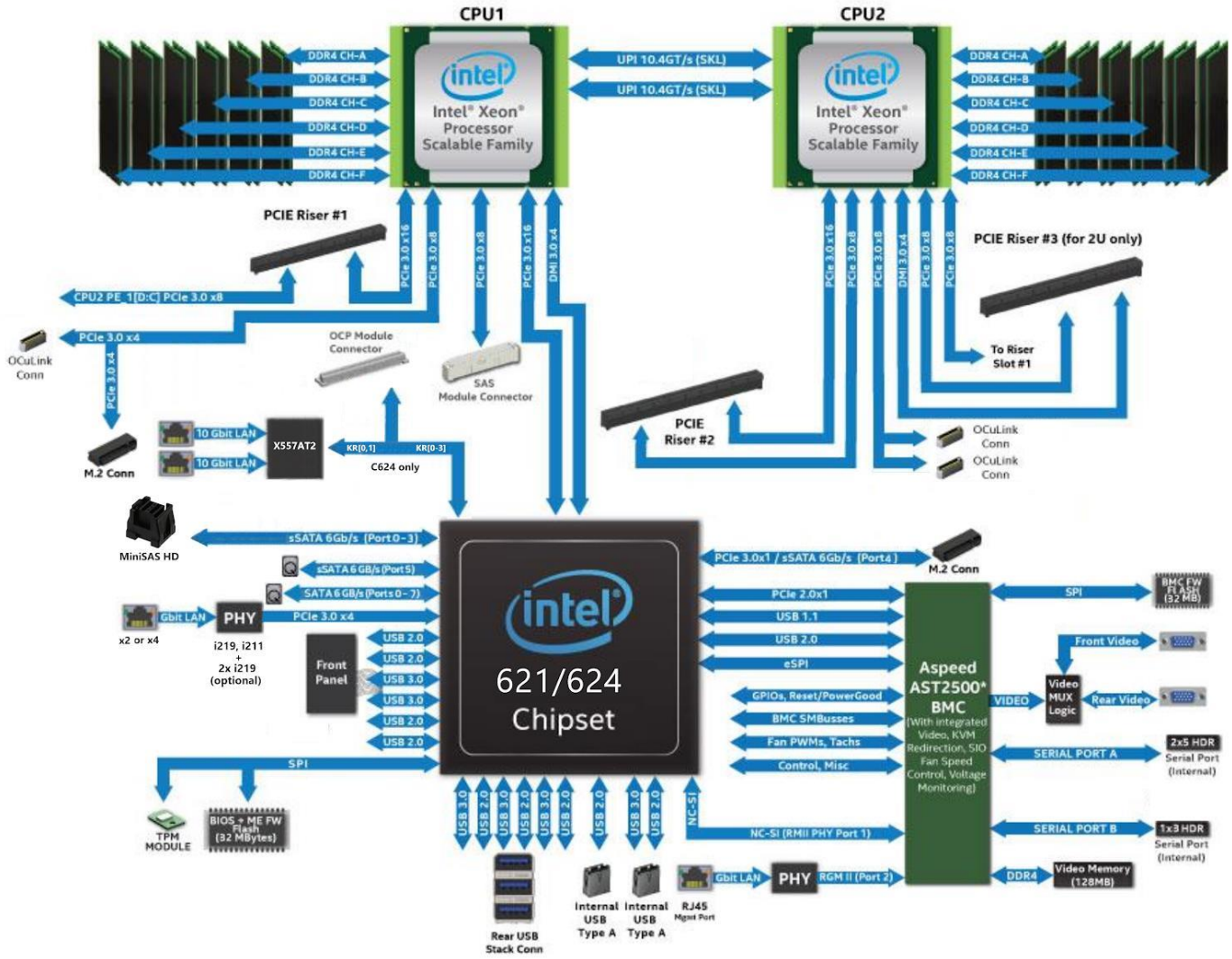


Рисунок 4-6. Блок-схема архитектуры серверной платы QTECH 469555.005

4.5. Стек системного программного обеспечения

Серверная плата включает в себя стек системного программного обеспечения, который состоит из BIOS, BMC, встроенного ПО управления работой системы (Intel® ME), а также сменного в полевых условиях блока FRU и блока записи данных с датчиков (SDR). Многие функции серверной платы выполняются и управляются всеми этими системами в комплексе. В частности, совместно системами BIOS и BMC выполняются следующие функции:

- Сторожевой таймер IPMI.
- Поддержка обмена сообщениями, включая объединение команд и поддержку пользовательских сеансов, поддержка флагов загрузки BIOS.
- Система ведения журнала событий BIOS/BMC.
- Последовательный переход по локальной сети (SOL).
- Синхронизация состояния ACPI BMC, отслеживает изменения состояния ACPI, предоставляемые BIOS.

- Отказоустойчивая загрузка (FRB) и отказоустойчивая загрузка 2-го уровня (FRB2), эти функции поддерживаются функцией сторожевого таймера.
- Управление передней панелью BMC. Функция управляет индикатором состояния системы и индикатором идентификатора шасси. Он поддерживает безопасную блокировку определенных функций передней панели и контролирует нажатие кнопок. Индикатор идентификатора шасси включается с помощью кнопки на передней панели или команды.
- Мониторинг температуры DIMM — новые датчики и улучшенное управление акустикой с использованием алгоритма управления вентилятором с замкнутым контуром, учитывающего показания температуры DIMM.
- Интегрированное KVM.
- Интегрированное перенаправление удалённых носителей.
- Встроенная функция отладки платформы, которая позволяет собирать подробные данные для последующего анализа.

Системное программное обеспечение полностью программируется на серверной плате в процессе сборки. Это необходимо для обеспечения возможности работы с серверной платой при первом включении. Однако, для обеспечения наиболее надёжной работы платы, настоятельно рекомендуется следить за обновлениями ПО и вовремя загружать новое ПО в систему. За обновлениями системного ПО можно следить на данном сайте: https://www.qtech.ru/catalog/servers/.

Обновления системы могут выполняться в ряде операционных сред, включая оболочку UEFI с использованием пакета обновления системы.

В рамках начального процесса интеграции системы, системные интеграторы должны запрограммировать данные конфигурации системы на плате с помощью утилиты FRUSDR, чтобы убедиться, что подсистема управления встроенным ПО способна обеспечить наилучшую производительность и охлаждение для окончательной конфигурации системы. Утилита FRUSDR включена в пакеты SUP и OFU (см. пункт 4.5.2).

4.5.1. Горячие клавиши, поддерживаемые в процессе самотестирования при включении (POST)

Некоторые горячие клавиши распознаются в процессе самотестирования при включении, т.е. в режиме POST. Горячая клавиша — это клавиша или комбинация клавиш, которая распознается оператором системы как ввод команды без подсказки. В большинстве случаев горячие клавиши распознаются даже во время выполнения другой обработки.

Горячие клавиши, поддерживаемые базовой системой ввода/вывода (BIOS), распознаются BIOS только в процессе POST при загрузке системы. Горячие клавиши, поддерживаемые BIOS, больше не распознаются после завершения процесса POST и начала процесса загрузки операционной системы.

В таблице 4 представлен список горячих клавиш, поддерживаемых BIOS.

Таблица 4. Горячие клавиши POST

Клавиша	Функция
<Esc>	Вход в программу настройки BIOS
<F2>	Вход в утилиту настройки BIOS

Клавиша	Функция
<F6>	Всплывающее меню загрузки BIOS
<F12>	Загрузка по сети
<Pause>	Временная остановка POST

4.5.1.1. <Esc>

Если для программы настройки BIOS установлено значение «Тихая загрузка» (по умолчанию), BIOS будет отображать заставку на мониторе в процессе POST. Нажатие клавиши <ESC> закроет экран-заставку и вместо него откроет экран диагностики/информации POST.

Заводской заставкой по умолчанию является логотип QTECH. Пользователь может установить на экран свою заставку, загрузив её с флеш-памяти.

Если экран-заставка отсутствует в области флеш-памяти BIOS или если «Тихая загрузка» отключена в программе настройки BIOS, во время процедуры POST отображается экран диагностики со сводной информацией о конфигурации системы. На экране диагностики всегда представлен только текст, в отличие от экрана с логотипом, на котором представлены только графические объекты.

Если перенаправление консоли включено в программе настройки BIOS, настройка тихой загрузки игнорируется и отображается экран диагностики без каких-либо условий. Это связано с ограничениями перенаправления консоли, которая передает данные в режиме, несовместимом с графикой.

4.5.1.2. <F2> (Вход в настройки BIOS)

Чтобы войти в утилиту настройки BIOS с клавиатуры (или виртуальной клавиатуры), нажмите функциональную клавишу <F2> во время загрузки, когда отображается экран с логотипом OEM или QTECH, или экран диагностики.

На экране диагностики или под экраном с логотипом тихой загрузки отображается следующее сообщение: Press <F2> to enter setup, <F6> Boot Menu, <F12> Network Boot.

ПРИМЕЧАНИЕ: при использовании USB-клавиатуры важно дождаться, пока BIOS обнаружит клавиатуру и подаст звуковой сигнал. До тех пор, пока USB-контроллер не будет инициализирован и клавиатура не активирована, клавиши не реагируют на нажатие.

При входе в утилиту настройки BIOS сначала отображается главный экран. Однако, если в процессе POST возникает серьёзная ошибка, система входит в программу настройки BIOS и отображает экран диспетчера ошибок вместо главного экрана.

4.5.1.3. <F6>

Спецификация загрузки BIOS (BBS) представляет собой всплывающее меню загрузки, которое можно вызвать нажатием клавиши <F6> на экране диагностики. Во всплывающем меню BBS отображаются все доступные загрузочные устройства. Порядок загрузки во всплывающем меню отличается от порядка загрузки в программе настройки BIOS. Всплывающее меню просто перечисляет все доступные устройства, с которых можно загрузить систему, и позволяет вручную выбрать нужное загрузочное устройство.

Если в программе настройки BIOS установлен пароль администратора, то его необходимо ввести для доступа ко всплывающему меню загрузки. Если вводится пароль пользователя,

пользователь попадает непосредственно в диспетчер загрузки в утилите настройки BIOS, позволяя системе загружаться только в порядке, определённом администратором.

4.5.1.4. Возможность обновления BIOS

Чтобы внести в систему исправления BIOS или новые функции, необходимо заменить текущий установленный образ BIOS на обновлённый. Актуальный образ BIOS, а также набор инструментов и инструкций по перепрограммированию доступен на сайте: https://www.qtech.ru/catalog/servers/.

4.5.1.5. Восстановление BIOS

Если система не может успешно загрузиться в ОС, зависает в процессе POST или даже зависает до выполнения POST, то может потребоваться процедура восстановления BIOS для замены дефектной копии основного BIOS.

BIOS предоставляет три механизма для запуска процесса восстановления BIOS, который называется режимом восстановления:

- Перемычка (см. рис. 4-6) режима восстановления заставляет BIOS загружаться в режиме восстановления.
- Если при включении загрузочный блок BIOS обнаруживает, что было выполнено частичное обновление BIOS, BIOS автоматически загружается в режиме восстановления.
- Контроллер BMC устанавливает режим восстановления ввода/вывода общего назначения (GPIO) в случае частичного обновления BIOS и контрольного таймера FRB2.

Восстановление BIOS происходит без каких-либо внешних носителей или запоминающих, так как в режиме восстановления используется резервный образ BIOS внутри флеш-памяти BIOS.

ПРИМЕЧАНИЕ: процедура восстановления приведена здесь для общего ознакомления. Более точной версией, при необходимости, являются инструкции в примечаниях к выпуску BIOS.

Когда перемычка восстановления BIOS установлена, BIOS начинает с записи события запуска восстановления в журнал системных событий (SEL). Затем он загружается и загружает резервный образ BIOS, находящийся во флеш-устройстве BIOS. Этот процесс происходит до того, как станет доступно любое видео или консоль. Система загружается во встроенную оболочку UEFI, и событие завершения восстановления регистрируется в SEL. Затем из оболочки UEFI можно обновить BIOS с помощью стандартной процедуры обновления BIOS, определённой в инструкциях по обновлению, прилагаемых к пакету обновления системы, загруженному с веб-сайта QTECH. После завершения обновления, верните перемычку восстановления в положение по умолчанию, выключите и снова включите систему.

ПРИМЕЧАНИЕ: перед выполнением загрузки для восстановления обязательно ознакомьтесь с примечаниями к выпуску BIOS и проверьте процедуру восстановления, показанную в примечаниях к выпуску. Этот процесс необходимо выполнять шаг за шагом, чтобы обеспечить стабильность системы после его завершения.

4.5.2. Сменный блок FRU и блок записи данных датчика (SDR)

В рамках начального процесса системной интеграции на серверную плату/систему должны быть загружены соответствующие данные FRU и SDR. Это гарантирует, что встроенная система управления платформой сможет отслеживать соответствующие данные датчиков и управлять системой с наилучшим охлаждением и производительностью. Как только

системный интегратор выполняет начальное обновление пакета SDR FRU, последующая автоматическая настройка выполняется без необходимости выполнения дополнительных обновлений SDR или предоставления другого пользовательского ввода в систему при добавлении или удалении любого из следующих компонентов:

- процессор;
- память;
- модуль OCP;
- встроенный модуль SAS RAID;
- источник питания;
- вентилятор;
- процессорная карта PCIe*;
- общая плата с горячей заменой;
- передняя панель.

ПРИМЕЧАНИЕ: если не установлены надлежащие данные FRU и SDR, то система может работать недостаточно эффективно или с неоптимальным охлаждением.

4.6. Центральный процессор

Серверная плата QTECH 469555.005 включает в себя два процессорных разъёма Socket-P LGA3647, совместимых с масштабируемым семейством процессоров Intel®Xeon® 1-го и 2-го поколений C621/C624 (стандартные и промышленные варианты).

ПРИМЕЧАНИЕ: серверная плата способна поддерживать процессоры с максимальной TDP 205 Вт. Однако поддержка TDP может варьироваться в зависимости от возможностей охлаждения выбранного серверного шасси. Проверьте спецификации серверного шасси или серверной системы, чтобы определить максимальный поддерживаемый TDP процессора.

4.6.1. Модуль радиатора процессора и сборка процессорного разъёма

В серверных платах данного поколения реализована следующая идея модуля теплоотвода процессора (PHM): процессор устанавливается на плату в собранном виде со своим радиатором охлаждения, как показано на рисунке 4-7:

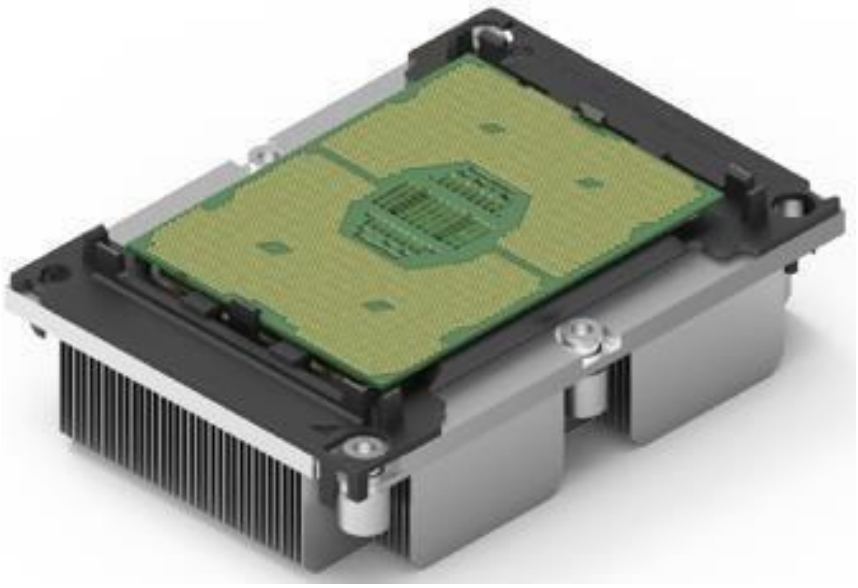


Рисунок 4-7. Процессор в собранном виде со своим радиатором охлаждения

Поэтому перед установкой процессора на плату, его необходимо собрать вместе с радиатором, как показано на рисунке 4-8.

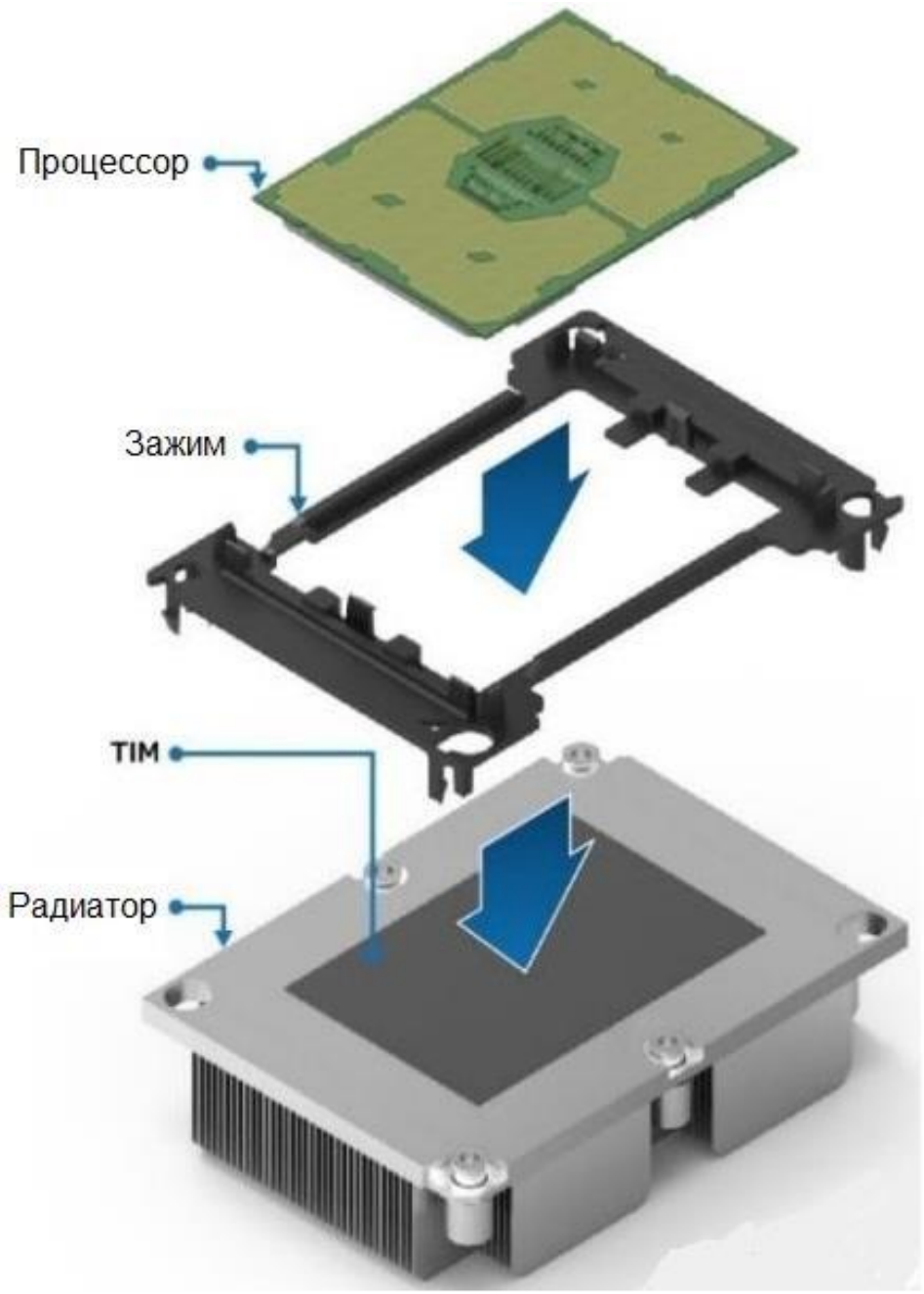


Рисунок 4-8. Сборка процессора и его радиатора

Два направляющих штифта опорной пластины разных размеров позволяют при сборке устанавливать PHM на разъём процессора только одним способом (см. рис. 4-9). PHM правильно установлен, когда он надёжно закреплён на двух направляющих штифтах опорной пластины и равномерно расположен над процессорным разъёмом, как показано на рисунке 4-10. Как только PHM будет правильно установлен на разъёме процессора, необходимо затянуть четыре винта Torx * с радиатором в порядке, указанном на этикетке, прикреплённой к верхней стороне радиатора.

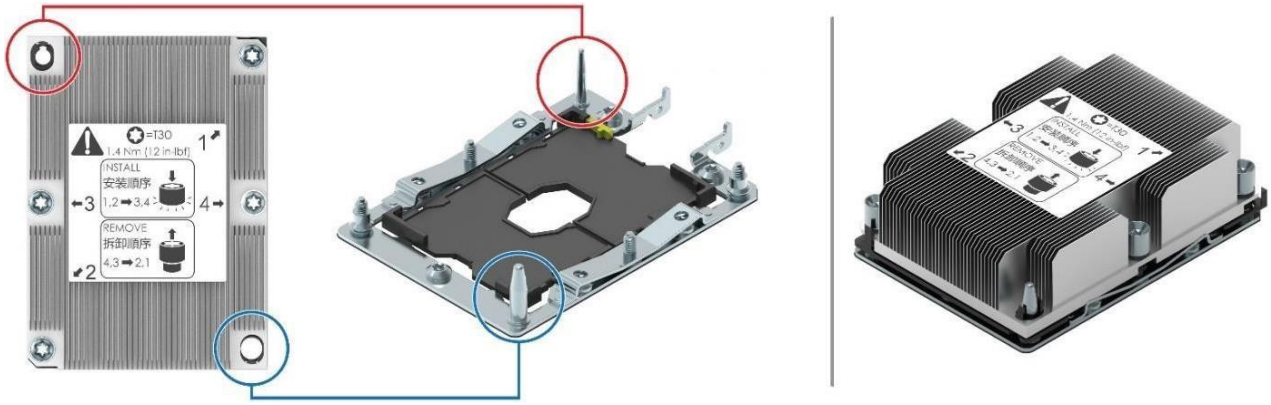


Рисунок 4-9. Направляющие штыри для сборки процессора

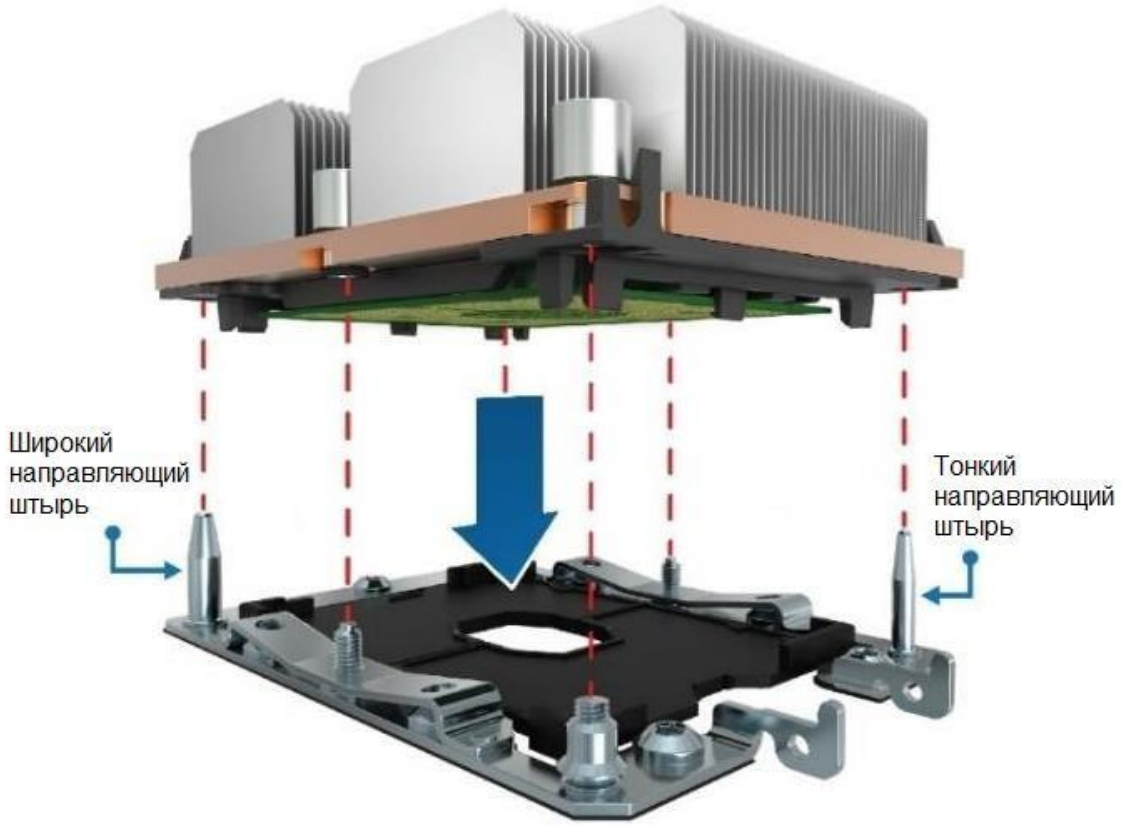


Рисунок 4-10. Монтаж процессора на разъём платы

ВНИМАНИЕ: НЕПРАВИЛЬНОЕ ЗАТЯГИВАНИЕ ВИНТОВ РАДИАТОРА В УКАЗАННОМ ПОРЯДКЕ МОЖЕТ ПРИВЕСТИ К ПОВРЕЖДЕНИЮ УЗЛА РАЗЪЁМА ПРОЦЕССОРА. ВИНТЫ РАДИАТОРА ДОЛЖНЫ БЫТЬ ЗАТЯНУТЫ С МОМЕНТОМ ЗАТЯЖКИ 12 ДЮЙМ-ФУТОВ.

ПРИМЕЧАНИЕ: подробные инструкции по сборке и установке процессора см. в соответствующем руководстве по системной интеграции и обслуживанию семейства продуктов Intel.

Чтобы защитить контакты внутри процессорного разъёма от повреждения, серверные платы, когда на них не установлен процессор, должны иметь защитные пластиковые крышки, установленные над пустым процессорным разъёмом, как показано на рисунке 4-11. Крышки процессорных разъёмов должны быть сняты перед установкой процессора (рис. 4-11 B).

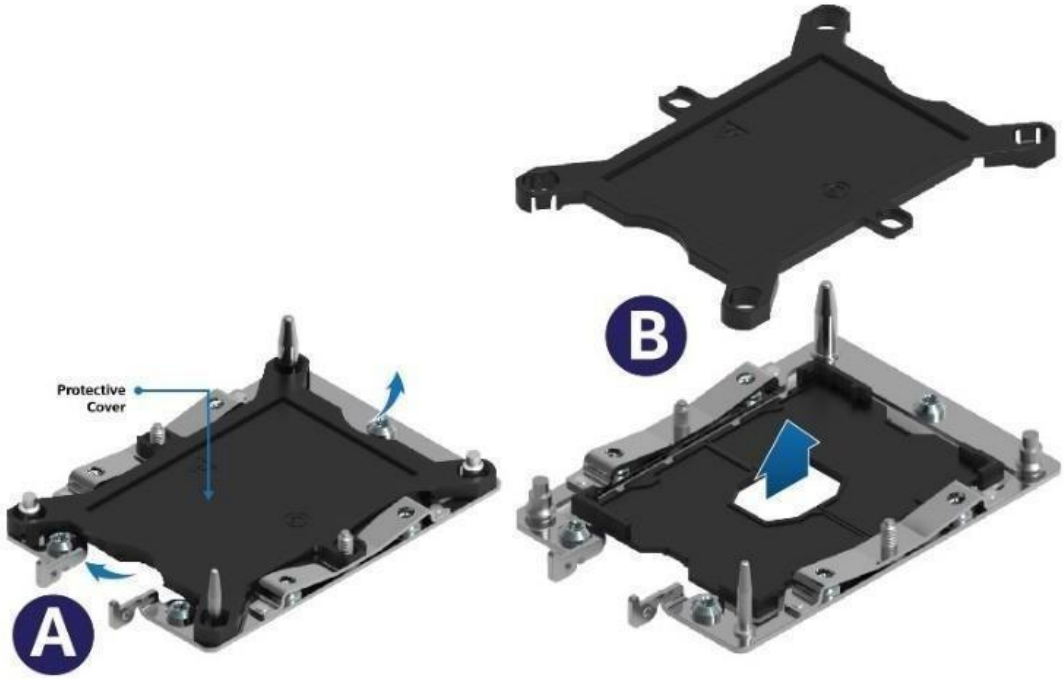


Рисунок 4-11. Защита разъёма для процессора крышкой и её снятие

4.6.2. Поддержка расчётной тепловой мощности процессора (TDP)

Чтобы обеспечить оптимальную работу и длительную надёжность систем на базе процессоров Intel®, процессор должен оставаться в пределах, установленных минимальной и максимальной характеристиками температуры корпуса (TCASE). Серверная плата, описанная в этом документе, предназначена для поддержки семейства процессоров Intel® C621/C624 с TDP до 205 Вт включительно.

ПРИМЕЧАНИЕ ОБ ОТКАЗЕ ОТ ОТВЕТСТВЕННОСТИ: серверные платы QTECH содержат ряд элементов для высокоплотной крупномасштабной интеграции (VLSI) и компонентов питания, требующих достаточно мощного охлаждения. Благодаря собственной разработке и тестированию корпусов QTECH гарантирует, что при использовании в конструкции серверов всех узлов разработки QTECH, изделие удовлетворяет всем параметрам работы. В случае использования в конструкции сервера отдельных узлов других разработчиков, необходимо проконсультироваться со специалистами компании QTECH. В противном случае QTECH не несёт ответственности в случае нештатной работы интегрированной таким образом системы.

4.7. Обзор семейства процессоров Intel® Xeon®

4.7.1. Общие характеристики

Серверная материнская плата QTECH 469555.005 поддерживает масштабируемое семейство процессоров Intel® Xeon® 1-го или 2-го поколения, как показано на схеме ниже:

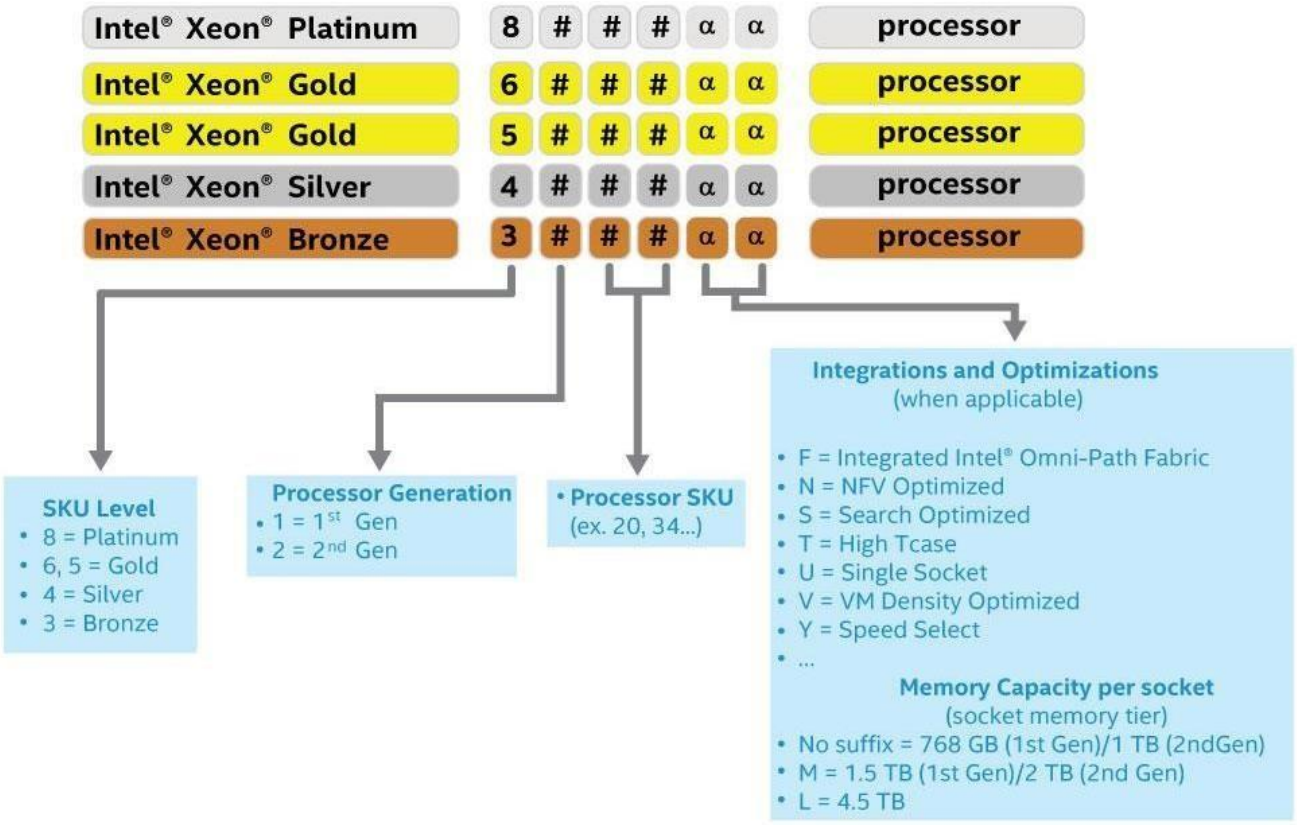


Таблица 5. Сравнение функций семейства процессоров Intel® Xeon® 1-го поколения

Особенность	Platunum 81xx	Gold 61xx	Gold 51xx	Silver 41xx	Bronze 31xx
Количество ссылок Intel® UPI	3	3	2	2	2
Intel UPI Скорость	10,4 ГТ/с	10,4 ГТ/с	10,4 ГТ/с	9,6 ГТ/с	9,6 ГТ/с
Поддерживаемые топологии	2С-2 UPI 2С-3 UPI 4С-2 UPI 4С-3 UPI 8С- 3 UPI	2С-2 UPI 2С-3 UPI 4С-2 UPI 4С-3 UPI	2С-2 UPI 4С-2 UPI	2С-2 UPI	2С-2 UPI
Поддержка контроллера узла	Да	Да	Нет	Нет	Нет
Количество каналов памяти	6	6	6	6	6

Особенность	Platunum 81xx	Gold 61xx	Gold 51xx	Silver 41xx	Bronze 31xx
Макс. скорость DDR4	2666	2666	2400	2400	2133
Емкость памяти	768 ГБ 1,5 ТБ (выбрать SKUs)	768 ГБ 1,5 ТБ (выбрать SKUs)	768 ГБ 1,5 ТБ (выбрать SKUs)	768 ГБ	768 ГБ
Возможности RAS	Продвинутый	Продвинутый	Продвинутый	Стандарт	Стандарт
Технология Intel® Turbo Boost	Да	Да	Да	Да	Нет
Технология Intel® HT	Да	Да	Да	Да	Нет
Поддержка Intel® AVX-512 ISA	Да	Да	Да	Да	Да
Intel® AVX-512 количество модулей FMA 512b	2	2	1	1	1
Количество линий PCIe*	48	48	48	48	48

Таблица 6. Сравнение функций семейства процессоров Intel® Xeon® 2-го поколения

Особенность	82xx Platinum	62xx Gold	52xx Gold	42xx Silver	32xx Bronze
Количество ссылок Intel® UPI	3	3	2	2	2
Скорость UPI	10,4 ГТ/с	10,4 ГТ/с	10,4 ГТ/с	9,6 ГТ/с	9,6 ГТ/с
Поддерживаемые топологии	2C-2 UPI 2C-3 UPI 4C-2 UPI 4C-3 UPI 8C-3 UPI	2C-2 UPI 2C-3 UPI 4C-2 UPI 4C-3 UPI	2C-2 UPI 4C-2 UPI	2C-2 UPI	2C-2 UPI
Поддержка контроллера узла	Да	Да	Нет	Нет	Нет

Особенность	82xx Platinum	62xx Gold	52xx Gold	42xx Silver	32xx Bronze
Количество каналов памяти	6	6	6	6	6
Максимальная скорость DDR4 1DPC	2933	2933	2666	2400	2133
Максимальная скорость DDR4 2DPC	2666	2666	2666	2400	2133
Ёмкость памяти	1 ТБ 2 ТБ (выбрать SKUs) 4,5 ТБ (выбрать SKUs)	1 ТБ 2 ТБ (выбрать SKUs) 4,5 ТБ (выбрать SKUs)	1 ТБ 2 ТБ (выбрать SKUs) 4,5 ТБ (выбрать SKUs)	1 ТБ	1 ТБ
Возможности RAS	Расширенные	Расширен-ные	Расширен-ные	Стандартные	Стандартные
Intel® Turbo Boost Технология	Да	Да	Да	Да	Нет
Intel® Hyper-Threading Технология	Да	Да	Да	Да	Нет
Поддержка Intel® AVX-512 ISA	Да	Да	Да	Да	Да
Intel® AVX-512 количество 512b FMA-юнитов	2	2	1	1	1
VNNI	Да	Да	Да	Да	Да
Количество линий PCIe	48	48	48	48	48

Масштабируемое семейство процессоров Intel® Xeon® 1-го и 2-го поколения объединяет несколько ключевых компонентов системы в один процессорный пакет, включая ядра ЦП, интегрированный контроллер памяти (IMC) и интегрированный модуль ввода-вывода (IIO). Процессор включает в себя множество основных и неосновных функций и технологий, описанных в следующих разделах.

Особенности ядра:

- Intel® Ultra Path Interconnect (Intel® UPI) — до 10,4 ГТ/с;
- технология Intel® Speed Shift — переключение скорости;
- архитектура Intel® x64;
- усовершенствованная технология Intel SpeedStep®;
- технология Intel® Turbo Boost 2.0;
- технология Intel® Hyper-Threading (технология Intel® HT);
- технология виртуализации Intel® (Intel® VT-x);
- технология виртуализации Intel® для прямого ввода-вывода (Intel® VT-d);
- выполнять бит отключения;
- технология Intel® Trusted Execution (Intel® TXT);
- Intel® Advanced Vector Extensions 512 (Intel® AVX-512);
- новые инструкции Intel® Advanced Encryption Standard (Intel® AES-NI).

Дополнительные особенности ядра Intel® Xeon® 2-го поколения:

- Intel® Deep Learning Boost через VNNI;
- технология Intel® Speed Select (выбрать SKUs);
- технология Intel® Resource Director.

Особенности вне ядра:

- до 48 линий PCIe* 3.0 на процессор — двунаправленный конвейер 79 Гбит/с;
- поддерживается 6 каналов памяти DDR4 на процессор;
- интерфейс DMI3/PCIe 3.0 с максимальной скоростью передачи 8,0 ГТ/с;
- усовершенствования непрозрачного моста (Non-Transparent Bridge, NTB) — три полнодуплексных NTBs и 32 MSI-X вектора;
- Intel® Volume Management Device (Intel® VMD) — управляет подключёнными к ЦП NVM Express * (NVMe*) твердотельными дисками (SSD);
- поддержка технологии Intel® Quick Data для Intel® Node Manager 4.0.

Особенности Intel® Xeon® 2-го поколения вне ядра:

- поддержка модуля постоянной памяти постоянного тока Intel® Optane™.

Далее подробнее описываются поддерживаемые технологии.

4.7.2. Архитектура набора команд Intel® 64

Архитектура Intel® x64, это 64-разрядное расширение памяти для архитектуры IA-32. Дополнительные сведения об архитектуре Intel x64 и модели программирования можно найти на http://developer.intel.com/technology/intel64/.

4.7.3. Intel® Hyper-Threading (технология Intel® HT)

Процессор поддерживает технологию Intel® HT, которая позволяет исполнительному ядру функционировать как два логических процессора. Хотя некоторые исполнительные ресурсы, такие, как кеши, единицы исполнения и шины, являются общими, каждый

логический процессор имеет свое собственное архитектурное состояние с его собственным набором регистров общего назначения и контрольными регистрами. Эта функция должна быть включена через BIOS и требует поддержки операционной системы.

4.7.4. Усовершенствованная технология Intel SpeedStep®

Процессоры масштабируемого семейства Intel® Xeon® 1-го и 2-го поколений поддерживают усовершенствованную технологию Intel SpeedStep®. Такие процессоры поддерживают несколько состояний производительности, что позволяет системе динамически регулировать напряжение процессора и частоту ядра по мере необходимости, чтобы обеспечить снижение энергопотребления и тепловыделения. Все элементы управления для перехода между состояниями централизованы внутри процессора, что позволяет увеличить частоту переходов для более эффективной работы.

Расширенная функция технологии Intel SpeedStep может быть включена/отключена с помощью опции на экране «Настройка конфигурации процессора». По умолчанию функция включена. Если этот параметр отключён, то скорость процессора устанавливается равной максимальной частоте ядра процессора TDP (номинальная частота).

4.7.5. Технология Intel® Turbo Boost 2.0

Технология Intel® Turbo Boost используется во всех процессорах масштабируемого семейства Intel® Xeon 1-го и 2-го поколений. Технология Intel Turbo Boost автоматически переводит работу процессора на частоту выше номинальной, если процессор работает ниже предельных значений мощности, температуры и тока. Это приводит к повышению производительности как для многопоточных, так и для однопоточных рабочих нагрузок.

4.7.6. Технология виртуализации Intel® (Intel® VT-x)

Технология виртуализации Intel® для IA-32, Intel® 64 и архитектуры Intel® (Intel® VT-x) обеспечивает аппаратную поддержку в ядре для повышения производительности и надёжности виртуализации.

4.7.7. Технология виртуализации для направленного ввода-вывода (Intel® VT-d)

Технология виртуализации Intel® для направленного ввода-вывода (Intel® VT-d) обеспечивает аппаратную поддержку в реализациях ядра и без ядра для поддержки и повышения производительности и устойчивости виртуализации ввода-вывода.

4.7.8. Бит-отключения

Технология бит-отключения Intel® может помочь предотвратить определённые классы опасностей, связанных с переполнением буфера в сочетании с поддерживающей операционной системой. Это позволяет процессору классифицировать области в памяти по тому, где код приложения может выполняться, а где — нет. Как только в буфер пытается попасть вредоносный код, процессор отключает выполнение кода, предотвращая повреждение и дальнейшее распространение.

4.7.9. Технология надёжного выполнения Intel® (Intel® TXT) для серверов

Технология Intel® надёжного выполнения (Intel® TXT) определяет улучшения на уровне платформы, которые обеспечивают строительные блоки для создания надёжных платформ. Платформа Intel TXT помогает обеспечить аутентичность управляющей среды. Платформа Intel TXT определяет идентичность управляющей среды путём точного измерения и проверки управляющего программного обеспечения.

4.7.10. Улучшенное векторное расширение Intel® 512 (Intel® AVX-512)

Базовые 512-битные расширения инструкций SIMD называются базовыми инструкциями улучшенного векторного расширения Intel® 512 (Intel® AVX-512). Они включают в себя расширения семейства Intel AVX инструкций SIMD, но кодируются с использованием новой схемы кодирования с поддержкой 512-битных векторных регистров, до 32 векторных регистров в 64-битном режиме и условной обработки с использованием защищённых регистров.

4.7.11. Расширенный стандарт шифрования Intel® (Intel® AES-NI)

Новые инструкции Intel® расширенного стандарта шифрования (Intel® AES-NI), это набор инструкций, реализованный во всех процессорах семейства масштабируемых процессоров Intel® Xeon®. Эта функция добавляет инструкции для ускорения операций шифрования и дешифрования, используемых в расширенном стандарте шифрования (AES). Функция Intel AES-NI включает в себя шесть дополнительных инструкций с одной инструкцией и несколькими данными (SIMD) в наборе команд Intel® Streaming SIMD Extensions.

В режиме самотестирования BIOS отвечает за определение наличия у процессора инструкций Intel AES-NI. Некоторые процессоры могут производиться без инструкций Intel AES-NI.

Инструкции Intel AES-NI могут быть включены или отключены BIOS. По умолчанию инструкции Intel AES-NI находятся во включенном состоянии.

4.7.12. Диспетчер узлов питания (Intel® NM) 4.0

Чипсет управления Intel® серии C621/C624 (Intel® ME) поддерживает технологию Intel® «умного» диспетчера узлов питания (Intel® NM). Комбинация Intel ME и Intel NM — это возможность управления питанием и температурой на платформе, которая предоставляет внешние интерфейсы, позволяющие ИТ-специалистам (через внешнее программное обеспечение управления) запрашивать Intel ME о мощности и тепловых параметрах и указывать режимы работы платы (т.е. установить бюджет мощности платформы). Intel® ME обеспечивает выполнение этих режимов, контролируя энергопотребление нижележащих подсистем, используя доступные механизмы управления (например, состояния P/T процессора). Определение параметров режима работы выполняется за пределами Intel ME либо с помощью программного обеспечения интеллектуального управления, либо ИТ-оператором.

Ниже приведены некоторые функции технологии Intel ME/Intel NM:

- **Мониторинг и ограничение мощности платформы**: Intel ME/Intel NM контролирует энергопотребление платформы и удерживает среднюю мощность в течение длительного времени. Его можно запросить, чтобы вернуть фактическую мощность в любом конкретном случае. Возможность ограничения мощности позволяет внешнему программному обеспечению управления решать основные проблемы работоспособности путём установки предела мощности для каждого сервера.
- **Мониторинг температуры воздуха на входе**: Intel ME/Intel NM периодически проверяют в сервере температуру входящего воздуха и сравнивают с её пороговыми значениями. При превышении пороговых значений Intel ME/Intel NM выдает предупреждение. Пороговые значения могут быть заданы пользователем.
- **Ограничение мощности подсистемы памяти**: Intel ME/Intel NM контролирует энергопотребление блока памяти. Потребляемая мощность блока памяти оценивается на основе данных о его среднем быстродействии.

- **Мониторинг и ограничение мощности процессора**: Intel ME/Intel NM контролирует энергопотребление процессора или сокета и сохраняет среднюю мощность в течение длительного времени. Можно запросить возврат фактической мощности в любой момент времени. Процесс мониторинга Intel ME будет использоваться для ограничения энергопотребления процессора с помощью Pсостояний процессора и динамического распределения ядер.
- **Распределение ядер во время загрузки**: позволяет задавать количество используемых во время загрузки ядер для ОС/диспетчер виртуальных машин (VMM), путём указания ограничения на количество активных ядер. Данная функция позволяет менять число активных ядер только во время загрузки/перезагрузки.
- **Распределение ядер во время работы**: данная функция позволяет оператору менять число активных ядер во время работы процессора.

4.7.13. Модуль TPM

TPM — это встроенный в серверную плату аппаратный модуль, сообщающий данные с аппаратной части для создания отчётов о тестировании платы. TPM подключается к PCH через шину LPC или шину SPI.

4.7.14. Технология ускоренного самообучения процессора

В семействе процессоров Intel® Xeon® 2-го поколения реализована технология ускоренного самообучения (накопления в памяти выполненных логических задач с последующим распределением аналогичных задач между ядрами) на базе модуля Intel® AVX-512 с расширенными возможностями. Этот модуль решает задачу более глубокого ускоренного самообучения с помощью специальных алгоритмов векторных нейронных сетей Intel® (VNNI).

4.7.15. Технология выбора скорости

Технология выбора скорости Intel®, доступная для некоторых моделей масштабируемого семейства процессоров Intel® Xeon® 2-го поколения, предлагает три различных точки рабочего напряжения и частоты для гарантированной базовой частоты (P1). Эта частота определяется исходя из количества активных ядер в SKU, при условии соблюдения требований температурного режима. Технология выбора скорости позволяет использовать большее количество активных ядер при более низкой базовой частоте или меньшее количество активных ядер при более высокой базовой частоте, предоставляя несколько характеристик ЦП, в зависимости от рабочей нагрузки/потребностей виртуальной машины.

На рисунке 4-12, для сравнения, представлена в виде графиков функции условная иллюстрация работы процессора без технологии выбора скорости (A) и при её наличии (B):

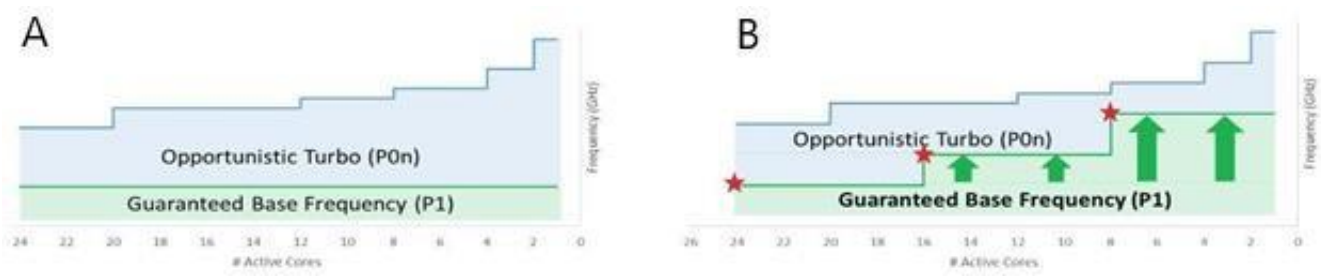


Рисунок 4-12. Работа процессора без технологии выбора скорости (A) и при её наличии (B)

4.7.16. Технология управления ресурсами

Технология Intel® управления ресурсами, доступная в семействе процессоров Intel® Xeon® 2-го поколения, снижает конкуренцию между несколькими приложениями, модулями или автономных ПО, совместно использующих ресурсы платы. Технология позволяет задавать быстродействие памяти для разных операций в соответствии с их приоритетом. Достигается это с помощью следующих функций:

- Технология мониторинга кеша (CMT) — отслеживает использование LLC (кеш L3) каждым программным потоком с помощью идентификатора мониторинга ресурсов (RMID).
- Приоритезация программных данных (CPD) — предоставляет возможность отделять код от данных в LLC с помощью заданной маски.
- Мониторинг быстродействия памяти (МБМ) — предоставляет ОС/VMM возможность назначения RMID для программных потоков и определять быстродействие памяти для данного RMID.
- Распределение быстродействия памяти (MBA) — это новая функция семейства процессоров Intel® Xeon® 2-го поколения, которая позволяет процессору во время работы задавать разное быстродействие для разных ядер или разных задач.

4.7.17. Модуль энергонезависимой памяти Optane™ DC

В процессорах Intel® Xeon® 2-го поколения добавлена поддержка модулей энергонезависимой памяти Intel® Optane™ DC. Модуль энергонезависимой памяти Intel® Optane™ DC обеспечивает более высокую ёмкость (на DIMM) памяти, совместимой с DDR4, с производительностью, близкой к DRAM, и расширенными функциями, которых нет в традиционной SDRAM.

Модуль энергонезависимой памяти Intel® Optane™ DC поддерживает следующие режимы работы:

- Энергозависимая память — режим сохранения данных.
- Постоянная память для некоторых приложений — режим использования данных.
- Оба режима работы одновременно — смешанный режим.

Дополнительную информацию см. в пункте 4.10.1.

4.8. Правила сборки процессора

ПРИМЕЧАНИЕ: серверная плата может поддерживать двухпроцессорные конфигурации, состоящие из разных процессоров, отвечающих определённым критериям; однако QTECH не проводит проверочные испытания таких конфигураций. Кроме того, QTECH не гарантирует надёжную работу серверной системы, в которой установлены не имеющие аналогов процессоры.

Системная BIOS пытается работать с процессорами, которые не соответствуют друг другу, но в целом совместимы. Для оптимальной производительности системы в двухпроцессорных конфигурациях QTECH рекомендует устанавливать идентичные процессоры.

ПРИМЕЧАНИЕ: при использовании однопроцессорной конфигурации процессор должен быть установлен в процессорное гнездо с надписью «CPU_1».

ПРИМЕЧАНИЕ: некоторые функции серверной платы могут быть недоступны, если не установлен второй процессор.

Если установлено два процессора, применяются следующие правила заполнения:

- оба процессора должны иметь одинаковое количество ядер;

- оба процессора должны иметь те же кеш-размеры для всех уровней от процессора кеш-памяти;
- оба процессора должны поддерживать идентичные частоты DDR4;
- оба процессора должны иметь идентичное расширенное семейство, расширенную модель, тип процессора, код семейства и номер модели.

В системе могут использоваться процессоры с разными частотами ядер при соблюдении предшествующих правил. Если это условие обнаруживается, все частоты ядра процессора устанавливаются на наименьший общий знаменатель (наибольшая общая скорость), и выдается сообщение об ошибке.

Степпинг процессора в рамках общего семейства процессоров может быть смешанным, если он указан в обновлениях спецификаций процессора, опубликованных корпорацией Intel. Смешивание процессоров с другой версией степпинга проверяется и поддерживается только между процессорами, которые отличаются друг от друга на плюс или минус один шаг.

4.9. Ошибки инициализации процессора

В таблице 5 описаны условия для разных процессоров и рекомендуемые действия для всех серверных плат Intel® и серверные системы Intel, разработанные на основе 1-го и 2-го поколений масштабируемого семейства процессоров Intel® Xeon® и архитектуры чипсета Intel® C621/C624.

По важности ошибки делятся на следующие категории:

1. Неустранимые. Если система не может загрузиться, POST останавливается и выводит следующее сообщение: **Unrecoverable fatal error found. System will not boot until the error is resolved Press <F2> to enter setup** (Обнаружена неустранимая ошибка. Система не загрузится, пока ошибка не будет устранена. Нажмите <**F2**>, чтобы войти в настройки).

При нажатии клавиши <**F2**> на клавиатуре на экране диспетчера ошибок отображается сообщение об ошибке, и ошибка регистрируется в журнале системных событий (SEL) с кодом ошибки POST.

Параметр «Пауза при ошибке POST» в настройках BIOS не влияет на эту ошибку.

Если система не может загрузиться, система генерирует звуковой код, состоящий из трёх длинных и одного короткого звуковых сигналов. Система не может загрузиться, пока ошибка не будет устранена. Неисправный компонент необходимо заменить.

О неустранимых ошибках сигнализирует непрерывно горящий жёлтый свет индикатора.

2. Крупные. Сообщение об ошибке отображается на экране диспетчера ошибок, и ошибка регистрируется в SEL. Если включён параметр настройки BIOS «Пауза при ошибке POST», для продолжения загрузки системы требуется вмешательство оператора. Если параметр настройки BIOS «Пауза при ошибке POST» отключён, система продолжает загружаться.
3. Незначительные. Сообщение об ошибке может отображаться на экране или в диспетчере ошибок настройки BIOS, код ошибки POST регистрируется в SEL. При таких ошибках система продолжает загружаться, прекращение процедуры по усмотрению пользователя. Параметр «Пауза при ошибке POST» в настройках BIOS не влияет на эту ошибку.

Таблица 7. Свод ошибок смешанных конфигураций процессора

Ошибка	Важность	Действия системы при ошибке
Семейство процессоров не совместимо	Неустранимая	• Останавливается при коде POST 0xE6. • Останавливается тремя длинными и одним коротким звуковыми сигналами. • Выполняет действия при ошибке и не загружается, пока неисправность не будет устранена
Модель процессора не совместима	Неустранимая	• Регистрирует код ошибки POST в SEL. • Предупреждает BMC о том, что индикатор состояния системы должен гореть жёлтым светом. • Дисплеи 0196: выдаёт сообщение о несоответствии модели процессора в диспетчере ошибок. • Выполняет действия при ошибке и не загружается, пока неисправность не будет устранена
Ядра/потоки процессора не совместимы	Неустранимая	• Останавливается при коде POST 0xE5. • Останавливается тремя длинными и одним коротким звуковыми сигналами. • Выполняет действия при ошибке и не загружается, пока неисправность не будет устранена
Кеш процессора или домашний агент не совместимы	Неустранимая	• Останавливается при коде POST 0xE5. • Останавливается тремя длинными и одним коротким звуковыми сигналами. • Выполняет действия при ошибке и не загружается, пока неисправность не будет устранена

Ошибка	Важность	Действия системы при ошибке
Частота процессора (скорость) не совместима	Неустранимая	Если частоты для всех процессоров можно настроить одинаковыми, то: • устанавливает все частоты процессора на самую высокую общую частоту; • не генерирует ошибку — нет ошибки; • продолжает успешно загружать систему. Если нельзя настроить одинаковые частоты для всех процессоров: • регистрирует код ошибки POST в SEL; • предупреждает BMC о том, что индикатор состояния системы должен гореть жёлтым цветом; • не отключает процессор; • дисплеи 0197: скорость процессора не позволяют синхронизировать сообщение в диспетчере ошибок; • выполняет действия при ошибке и не загружается до тех пор, пока неисправность не будет устранена
Частоты канала Intel® UPI Link не совместимы	Неустранимая	Если частоты каналов для всех каналов Intel® Ultra Path Interconnect (Intel® UPI) можно настроить так, чтобы они были одинаковыми: • настраивает все частоты межкомпонентного соединения Intel UPI на самую высокую общую частоту; • не генерирует ошибку — ошибки нет; • продолжает успешно загружать систему. Если частоты каналов для всех каналов Intel UPI нельзя настроить одинаковыми: • регистрирует код ошибки POST в SEL; • предупреждает BMC о том, что индикатор состояния системы должен гореть жёлтым цветом; • не отключает процессор; • дисплеи 0195: частота процессора недостачна для синхронизации сообщения в менеджере ошибок. Выполняет действия при ошибке и не загружается, пока неисправность не будет устранена

Ошибка	Важность	Действия системы при ошибке
Ошибка обновления микрокода процессора	Крупная	• Регистрирует код ошибки POST в SEL. • Отображает 816x: процессор 0x не может создать сообщение об обновлении микрокода в диспетчере ошибок или на экране. Принимает меры по устранению и от «POST Error Pause» в настройке или может остановиться с кодом ошибки POST в диспетчере ошибок, ожидая вмешательства оператора
Отсутствует обновление микрокода процессора	Незначи-тельная	• Регистрирует код ошибки POST в SEL. • Дисплеи 818x: сообщение об обновлении микрокода процессора 0x отсутствует. Система продолжает загружаться, независимо от наличия параметра «Пауза при ошибке POST»

4.10. Поддержка памяти

В этом разделе описывается архитектура, управляющая подсистемой памяти, поддерживаемые типы памяти, правила заполнения памяти и поддерживаемые функции надёжности, доступности и удобства обслуживания памяти (RAS).

4.10.1. Архитектура подсистемы памяти

Архитектура представлена на рисунке 4-13:

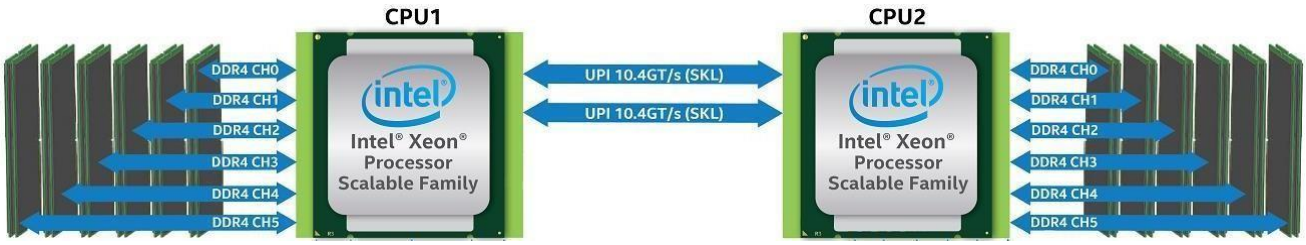


Рисунок 4-13. Архитектура подсистемы памяти

Серверная системная плата QTECH 469555.005 поддерживает до 24 модулей DIMM DDR4, по 12 на каждый процессор. Каждый установленный процессор поддерживает шесть каналов памяти через два встроенных контроллера памяти (IMC). На серверной плате каналам памяти присваиваются идентификационные буквы от A до F, при этом каждый канал памяти поддерживает два слота DIMM.

Серверная плата поддерживает следующее:

- Только совместимые с DDR4 модули DIMM.
- Включён код исправления ошибок (ECC) Поддерживаются зарегистрированные модули DIMM (RDIMM), модули DIMM с уменьшенной нагрузкой (LRDIMM) или энергонезависимые модули памяти с двумя встроенными разъёмами (NVDIMM).
- Только модули RDIMM и LRDIMM со встроенным термодатчиком на кристалле (TSOD).

- Традиционные модули SDRAM DIMM организованы как одноранковые (SR), двухранковые (DR), четырёхранковые (QR) или восьмиранковые (8R):
  - RDIMMS — зарегистрированные модули DIMM — SR/DR/QR/8R, только ECC;
  - LRDIMM — модули DIMM с уменьшенной нагрузкой — только QR/8R, ECC;
  - максимум 8 логических ранков на канал;
  - максимум 10 физических ранков, загруженных на канал.
- Модуль энергонезависимой памяти Intel® Optane™ DC поддерживается семейством Intel® Xeon® 2-го поколения (процессор Platinum, Gold и некоторые модели Silver SKU).

Визуальное отличие традиционных модулей памяти SDRAM DIMM и модуля энергонезависимой памяти Intel® Optane™ DC показано на следующем рисунке 4-14.

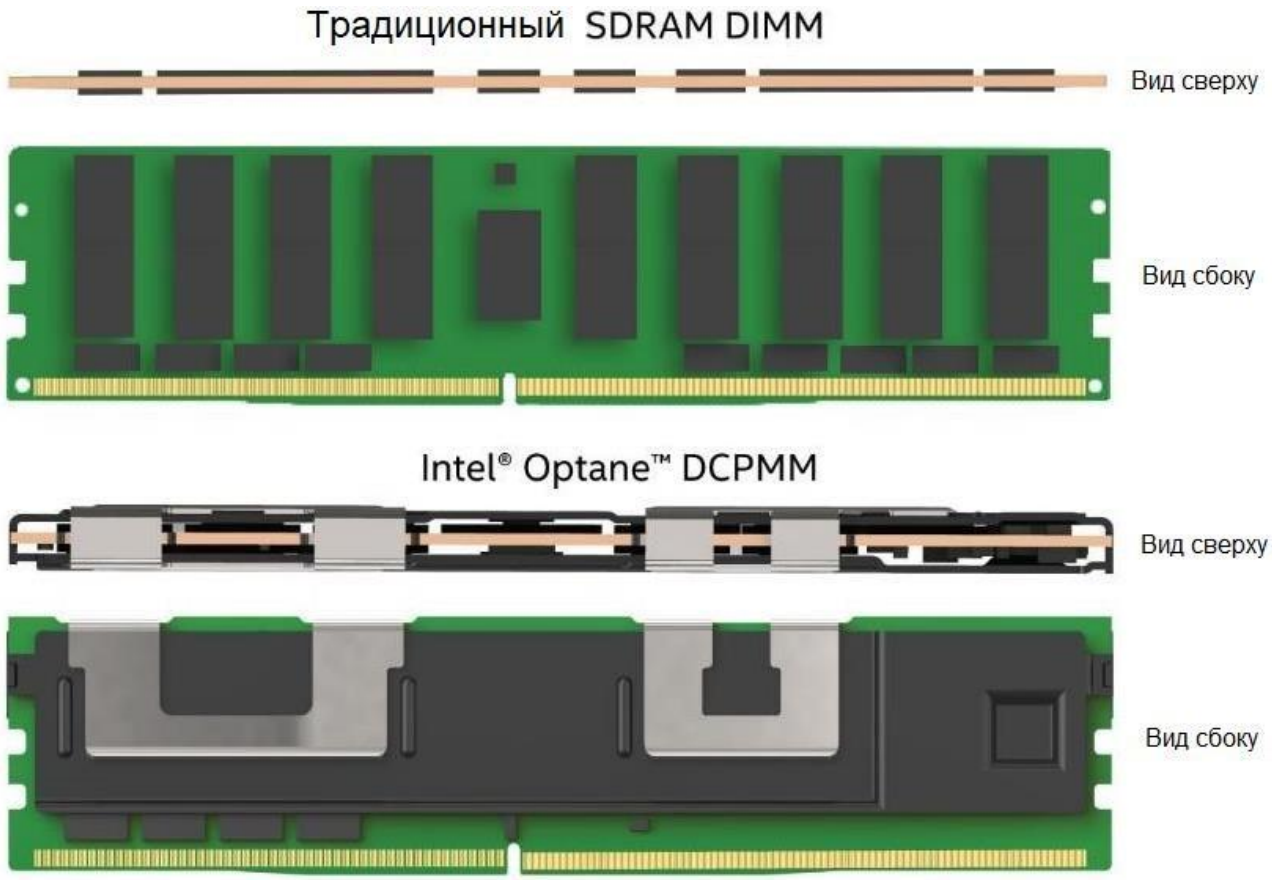


Рисунок 4-14. Модули памяти

4.10.2. Модуль энергонезависимой памяти Intel® Optane™ DC

4.10.3. Общая характеристика

Семейство масштабируемых процессоров Intel® Xeon® 2-го поколения поддерживает модуль энергонезависимой памяти Intel® Optane™ DC-типа памяти. Модуль энергонезависимой памяти Intel® Optane™ DC обеспечивает более высокую плотность (ёмкость на DIMM), совместимые с DDR4 модули памяти с производительностью, близкой к DRAM, и расширенными функциями, которых нет в традиционной SDRAM.

Модуль поддерживает следующие функции:

- всегда включённое шифрование AES-256;
- когерентный кеш: как и DRAM, содержит вытесненную информацию из LLC;
- память с байтовой адресацией;
- более высокая надёжность, чем у твердотельных накопителей корпоративного класса.

Модуль поддерживает следующие режимы работы:

- режим памяти (MM);
- режим прямого приложения (AD);
- смешанный режим.

Режимы прямого приложения и смешанный требуют, как драйвера, так и явной поддержки программного обеспечения. Для получения дополнительной информации о совместимости ОС посетите сайт support.intel.com.

4.10.4. Режим памяти

В режиме памяти энергонезависимая память Intel® Optane™ DC работает, как основная энергозависимая (непостоянная) системная память. В режиме памяти вся доступная традиционная память DRAM в пределах одного контроллера памяти функционирует как кеш-память L4 с обратной записью для модуля энергонезависимой памяти Intel® Optane™ DC. Это снижает стоимость общей ёмкости системной памяти по сравнению только с традиционной DRAM, сохраняя при этом производительность, близкую к DRAM.

4.10.5. Режим прямого приложения

Этот режим (AD) позволяет модулю энергонезависимой памяти работать в качестве энергонезависимой памяти, сохраняя целостность данных при отключении питания для приложений, сохраняя при этом производительность, близкую к DRAM. В режиме AD DRAM работает как обычная системная память, а модуль энергонезависимой памяти работает как хранилище приложений.

4.10.6. Смешанный режим

Смешанный режим позволяет частично использовать ёмкость модуля энергонезависимой памяти для работы в качестве большой части энергозависимой системной памяти, а оставшуюся ёмкость использовать в качестве энергонезависимой памяти для приложений с производительностью, близкой к DRAM. Ёмкость, выделенная для энергозависимой системной памяти, должна соответствовать критериям заполнения режима памяти, а любая оставшаяся ёмкость будет доступна в качестве постоянной памяти для хранения приложений и должна поддерживаться операционной системой, драйвером и приложением.

4.11. Поддерживаемая память

Подробные рекомендации по поддержке модулей DIMM приведены в таблицах 6–9.

Таблица 8. Рекомендации по поддержке традиционных модулей памяти DDR4 SDRAM DIMM семейства процессоров Intel® Xeon®

Тип	**Ранки на DIMM и ширину данных**	**Ёмкость DIMM (ГБ)**		**Максимальная скорость (MT/c); напряжение (В); слоты на канал (SPC) и количество модулей DIMM на канал (DPC)**	
				2 слота на канал	
		Плотность DRAM		1 DPC	2 DPC
		4	8	1,2 В	1,2 В
RDIMM	SRx8	4	8	2666	2666
	SRx4	8	16		
RDIMM	DRx8	8	16		
	DRx4	16	32		
RDIMM 3DS	QRx4	Нет данных	2H-64		
	8Rx4	Нет данных	4H-128		
LRDIMM	QRx4	32	64		
LRDIMM 3DS	QRx4	Нет данных	2H-64		
	8Rx4	Нет данных	4H-128		

Таблица 9. Рекомендации по поддержке традиционных модулей памяти DDR4 SDRAM DIMM семейства процессоров Intel® Xeon® 2-го поколения

Тип	**Ранки на DIMM и ширину данных**	**Ёмкость DIMM (ГБ)**			**Максимальная скорость (MT/c); напряжение (В); слоты на канал (SPC) и количество модулей DIMM на канал (DPC)**	
					2 слота на канал	
		Плотность DRAM			1 DPC	2 DPC
		4[1]	8	16	1,2 В	1,2 В
RDIMM	SRx8	4	8	16	2933	2666
	SRx4	8	16	32		
	DRx8	8	16	32		
RDIMM	DRx4	16	32	64		
RDIMM 3DS	QRx4	Нет данных	2H-64	2H-128		
	8Rx4	Нет данных	4H-128	4H-256		
LRDIMM	QRx4	32	64	128		
LRDIMM 3DS	QRx4	Нет данных	2H-64	2H-128		
	8Rx4	Нет данных	4H-128	4H-256		

[1] Плотность DRAM 4 ГБ поддерживается только на скоростях до 2666 MT/c

Таблица 10. Максимальные поддерживаемые скорости традиционных модулей памяти SDRAM DIMM по уровням SKU в MT/c (мегатранзакций в секунду)

Масштабируемое семейство процессоров Intel® Xeon®	**Platinum 8xxx**	**Gold 6xxx**	**Gold 5xxx**	**Silver 4xxx**	**Bronze 3xxx**
1 поколение	2666	2666	2400	2400	2133
2 поколение	2933[2]	2933[2]	2666	2400	2133

Таблица 11. Поддержка модулей постоянной памяти Intel® Optane™ DC

Семейство процессоров Intel® Xeon®	**Уровень SKU процессора**	**Емкость DIMM (ГБ)**	**Скорость (MT/c)**
1 поколение	Bronze 31xx	Нет данных	Нет данных
	Silver 41xx		
	Gold 51xx		
	Gold 61xx		
	Platinum 81xx		
2 поколение	Bronze 32xx	Нет данных	Нет данных
	Silver 42xx[3]	128 256 512	1866 2133 2400
	Gold 52xx		1866 2133 2400 2666
	Gold 62xx		
	Platinum 82xx		

[2] Максимальная скорость только в конфигурации 1DPC
[3] Поддерживается на некоторых процессорах Silver

4.12. Выбор модулей DIMM

4.12.1. Правила поддержки памяти

ПРИМЕЧАНИЕ: хотя смешанные конфигурации DIMM могут работать, QTECH поддерживает и выполняет проверку платформы только в системах, в которых установлены идентичные модули DIMM.

Каждый установленный процессор имеет шесть каналов памяти. В серверной плате QTECH 469555.005 каналы памяти для каждого процессора обозначены от A до F. Каналы A и D на каждом процессоре поддерживают два слота DIMM. Все остальные каналы памяти имеют один слот DIMM. На серверной материнской плате каждый слот DIMM помечен номером процессора, каналом памяти и номером слота, как показано в следующих примерах: CPU1_DIMM_A2; CPU2_DIMM_A2.

Правила заполнения модулей DIMM требуют, чтобы каналы, поддерживающие более одного модуля DIMM, заполнялись, начиная с синего слота DIMM или слота DIMM, наиболее удалённого от процессора, в подходе «до самого конца». Кроме того, при заполнении четырёхранкового модуля DIMM одноранковым или двухранковым модулем DIMM в том же канале, четырёхранковый модуль DIMM должен располагаться дальше всего от процессора. Слоты памяти, связанные с данным процессором, недоступны, если соответствующий сокет процессора не заполнен.

На серверной плате QTECH 469555.005 предусмотрено 24 слота DIMM: 2 ЦП, 6 каналов памяти на ЦП, 2 модуля DIMM на канал. Все слоты DIMM на серверной плате показаны на рисунке 4-15:

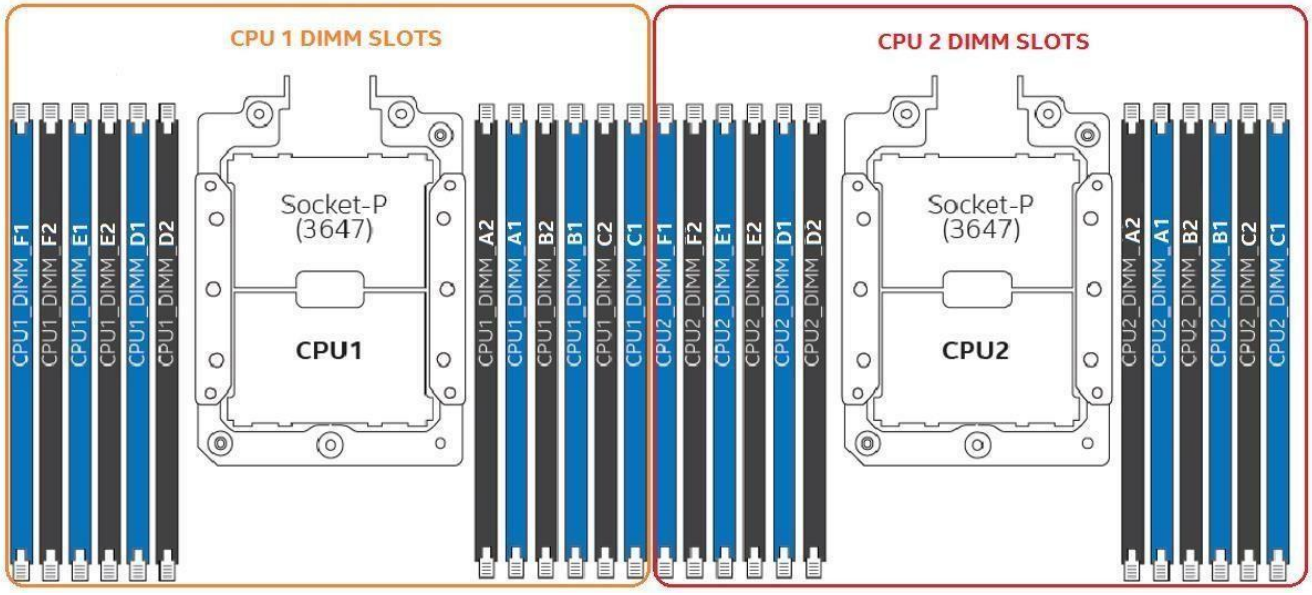


Рисунок 4-15. Слоты DIMM на серверной плате

При установке модулей DIMM применяются следующие правила заполнения памяти:

- Смешивание типов модулей DIMM DDR4 (RDIMM, LRDIMM, 3DS RDIMM, 3DS LRDIMM) внутри процессорных сокетов или между ними приводит к неустранимой ошибке и остановке процесса инициализации памяти.
- Совместное использование модулей DIMM с разными частотами и задержками не поддерживается внутри процессорных сокетов или между ними. Если встречается

смешанная конфигурация, BIOS пытается работать на самой высокой общей частоте и с наименьшей возможной задержкой.

- Каналы, поддерживающие более одного модуля DIMM, должны заполняться, начиная с синего слота DIMM или слота DIMM, наиболее удалённого от процессора, в подходе «до самого конца».
- При заполнении четырёхранкового модуля DIMM одноранковым или двухранковым модулем DIMM в том же канале, четырёхранковый модуль DIMM должен располагаться дальше всего от процессора. Слоты памяти, связанные с данным процессором, недоступны, если соответствующий сокет процессора не заполнен. Неправильное размещение DIMM приводит к появлению кода ошибки MRC. На любом канале можно использовать не более 8 логических ранков, а также не более 10 физических ранков, загруженных на канал.
- Слоты памяти, связанные с данным процессором, недоступны, если соответствующий разъём процессора не занят.
- Процессор может быть установлен без заполнения соответствующих слотов памяти при условии, что установлен второй процессор с соответствующей памятью. В этом случае память совместно используется процессорами. Однако платформа страдает от снижения производительности и задержек из-за удалённой памяти.
- Процессорные сокеты самодостаточны и автономны. Однако вся поддержка подсистемы памяти (например, память RAS и управление ошибками) в настройках BIOS обычно применяется для процессорных сокетов.
- Для нескольких модулей DIMM на один канал (для RDIMM, LRDIMM, 3DS RDIMM, 3DS LRDIMM) всегда устанавливайте модули DIMM с более высокой электрической нагрузкой в слот 1, а затем в слот 2.
- Для обеспечения наилучшей производительности системы в конфигурациях с двумя процессорами, тип и заполнение установленных модулей DIMM, настроенных для ЦПУ2, должны соответствовать типу и заселению DIMM, настроенному для ЦПУ1.

Правила энергонезависимой памяти Intel® Optane™ DC для конкретных модулей для всех режимов работы:

- Поддержка модуля энергонезависимой памяти доступна только при установленном семействе масштабируемых процессоров Intel® Xeon® 2-го поколения.
- Для каждого канала памяти поддерживается только один модуль энергонезависимой памяти Intel® Optane™ DC.
- Модули энергонезависимой памяти Intel® Optane™ DC разной ёмкости нельзя смешивать внутри процессорных сокетов или между ними.
- Слоты памяти, поддерживаемые встроенным контроллером памяти IMC0 (каналы памяти A–C) данного процессора, должны быть заполнены раньше слотов памяти, поддерживаемых встроенным каналом памяти IMC1 (каналы памяти D–F).
- Когда оба слота DIMM внутри канала заполнены, модули энергонезависимой памяти поддерживаются только в чёрных слотах DIMM.
- Поддерживаются конфигурации системы с модулями энергонезависимой памяти, установленными только в каналах памяти A–C данного процессора.
- Традиционные модули памяти SDRAM SRx8 DIMM в сочетании с модулем энергонезависимой памяти Intel® Optane™ DC не поддерживаются ни в каком режиме работы.

Правила для модуля энергонезависимой памяти в режиме памяти:

- На каждый встроенный контроллер памяти (IMC0 и IMC1) процессора, необходим, как минимум, один модуль памяти DRAM DIMM и один модуль энергонезависимой памяти Intel® Optane™ DC.
- Для максимизации быстродействия необходимо заполнить DRAM по всем доступным каналам памяти.

Правила для модуля энергонезависимой памяти в режиме прямого приложения:

- Должен быть, как минимум, один модуль энергонезависимой памяти Intel® Optane™ DC, установленный в любой поддерживаемый слот DIMM.
- На встроенный контроллер памяти (IMC0 и IMC1) для каждого установленного процессора, необходим, как минимум, один модуль DRAM DIMM.

4.12.2. Рекомендации по выбору модулей DIMM

Для обеспечения наилучшей производительности системы в конфигурациях с двумя процессорами тип и заполнение установленных модулей DIMM, настроенных для ЦПУ2, должны соответствовать типу и заполнению DIMM, настроенному для ЦПУ1 (см. таблицы 10–13).

Назначение каналов памяти процессора серверной платы QTECH 469555.005 показано на рисунке 4-16.

Рисунок 4-16. Каналы памяти процессора

Таблица 12. Конфигурации заполнения традиционной памяти DRAM DIMM

# of DIMMs	iMC1						iMC0					
	CH F		CH E		CH D		CH C		CH B		CH A	
	Слот 2	Слот 1	Слот 2	Слот 1	Слот 2	Слот 1	Слот 2	Слот 1	Слот 2	Слот 1	Слот 2	Слот 1
1	–	–	–	–	–	–	–	–	–	–	–	DRAM
2	–	–	–	–	–	–	–	–	–	DRAM	–	DRAM
3	–	–	–	–	–	–	–	DRAM	–	DRAM	–	DRAM
4	–	–	–	DRAM	–	DRAM	–	–	–	DRAM	–	DRAM
5[1]	–	–	–	DRAM	–	DRAM	–	DRAM	–	DRAM	DRAM	DRAM
6	–	DRAM	–	DRAM	–	DRAM	–	DRAM	–	DRAM	–	DRAM
7[1]	–	DRAM	–	DRAM	–	DRAM	–	DRAM	–	DRAM	DRAM	DRAM
8	–	–	DRAM	DRAM	DRAM	DRAM	–	–	DRAM	DRAM	DRAM	DRAM
9[1]	–	DRAM	–	DRAM	–	DRAM	DRAM	DRAM	DRAM	DRAM	DRAM	DRAM
10[1]	–	DRAM	DRAM	DRAM	DRAM	DRAM	–	DRAM	DRAM	DRAM	DRAM	DRAM
11[1]	–	DRAM	DRAM	DRAM	DRAM	DRAM	DRAM	DRAM	DRAM	DRAM	DRAM	DRAM
12	DRAM	DRAM	DRAM	DRAM	DRAM	DRAM	DRAM	DRAM	DRAM	DRAM	DRAM	DRAM

Таблица 13. Конфигурации традиционных модулей памяти DRAM DIMM и модулей энергонезависимой памяти

	Симметричное заполнение памяти по сокетам процессора												
Режи-мы	iMC1						iMC0						
	Канал F		Канал E		Канал D		Канал C		Канал B		Канал A		
	Слот 2	Слот 1	Слот 2	Слот 1	Слот 2	Слот 1	Слот 2	Слот 1	Слот 2	Слот 1	Слот 2	Слот 1	
AD	PMM	DRAM1	PMM	DRAM1	PMM	DRAM1	PMM	DRAM1	PMM	DRAM1	PMM	DRAM1	2-2-2
MM	PMM	DRAM1	PMM	DRAM1	PMM	DRAM1	PMM	DRAM1	PMM	DRAM1	PMM	DRAM1	2-2-2

	Симметричное заполнение памяти по сокетам процессора												
Режи-мы	iMC1						iMC0						
	Канал F		Канал E		Канал D		Канал C		Канал B		Канал A		
	Слот 2	Слот 1	Слот 2	Слот 1	Слот 2	Слот 1	Слот 2	Слот 1	Слот 2	Слот 1	Слот 2	Слот 1	
AD + MM	PMM	DRAM3	PMM	DRAM3	PMM	DRAM3	PMM	DRAM3	PMM	DRAM3	PMM	DRAM3	2-2-2
AD	–	DRAM1	–	DRAM1	PMM	DRAM1	–	DRAM1	–	DRAM1	PMM	DRAM1	2-1-1
MM	–	DRAM2	–	DRAM2	PMM	DRAM2	–	DRAM2	–	DRAM2	PMM	DRAM2	2-1-1
AD + MM	–	DRAM3	–	DRAM3	PMM	DRAM3	–	DRAM3	–	DRAM3	PMM	DRAM3	2-1-1
AD	–	DRAM1	PMM	DRAM1	PMM	DRAM1	–	DRAM1	PMM	DRAM1	PMM	DRAM1	2-2-1
MM	–	DRAM1	PMM	DRAM1	PMM	DRAM1	–	DRAM1	PMM	DRAM1	PMM	DRAM1	2-2-1
AD + MM	–	DRAM3	PMM	DRAM3	PMM	DRAM3	–	DRAM3	PMM	DRAM3	PMM	DRAM3	2-2-1
AD	–	PMM	–	DRAM1	–	DRAM1	–	PMM	–	DRAM1	–	DRAM1	1-1-1
MM	–	PMM	–	DRAM1	–	DRAM1	–	PMM	–	DRAM1	–	DRAM1	1-1-1
AD	–	PMM	DRAM1	DRAM1	DRAM1	DRAM1	–	PMM	DRAM1	DRAM1	DRAM1	DRAM1	2-2-1
	Асимметричное заполнение памяти по сокетам процессора												
Режи-мы	iMC1						iMC0						
	Канал F		Канал E		Канал D		Канал C		Канал B		Канал A		
	Слот 2	Слот 1	Слот 2	Слот 1	Слот 2	Слот 1	Слот 2	Слот 1	Слот 2	Слот 1	Слот 2	Слот 1	
AD	–	DRAM1	–	DRAM1	–	DRAM1	–	DRAM1	–	DRAM1	PMM	DRAM1	2/1-1-1
AD 1	–	DRAM1	–	DRAM1	–	DRAM1	–	DRAM1	–	DRAM1	PMM	DRAM1	2/1-1-1

Таблица 14. Поддерживаемые типы DRAM

		Тип DDR4			Ёмкость, ГБ
DRAM1	RDIMM	3DS RDIMM	LRDIMM	3DS LRDIMM	Любая ёмкость
DRAM2	RDIMM	–	–	–	16 и 32
DRAM3	RDIMM	3DS RDIMM	LRDIMM	–	Любая ёмкость

Типы DRAM1 и DRAM2, указанные в таблице 14 должны соответствовать спецификациям, указанным в таблице 15.

Таблица 15. Традиционные модули DRAM DIMM, совместимые с модулем энергонезависимой памяти Intel® Optane™

Тип DIMM	Ранк	Ширина	Плотность	Высота 3D-стека	Размер
RDIMM	1	4	8	1	16
	1	4	16	1	32
	2	8	8	1	16
	2	8	16	1	32
	2	4	8	1	32
	2	4	16	1	64
	4	4	8	2	64
	4	4	16	2	128
	8	4	8	4	128
	8	4	16	4	256
LRDIMM	4	4	8	1	64
	4	4	16	1	128
	4	4	8	2	64
	4	4	16	2	128

Тип DIMM	Ранк	Ширина	Плотность	Высота 3D-стека	Размер
LRDIMM	8	4	8	4	128
	8	4	16	4	256

- Для MM общее соотношение модулей постоянной памяти DRAM/DC составляет от 1:4 до 1:16. Избыточная ёмкость модуля постоянной памяти DC может быть использована для AD.
- Для каждого отдельного заполнения разрешены перестановки между каналами, если данное заполнение соответствует правилам заполнения данного типа памяти.
- Для каждой отдельной совокупности один и тот же модуль DIMM DDR4 должен использоваться во всех слотах, как указано в правилах заполнения данного типа памяти.
- Для каждого отдельного заполнения сокеты обычно симметричны, за исключением 1 модуля энергонезависимой памяти DC на сокет и 1 модуля энергонезависимой памяти DC на корпус узла.

4.13. Функции RAS-памяти

Поддерживаемые функции памяти RAS зависят от уровня установленного процессора. Каждый уровень процессора в семействе масштабируемых процессоров Intel Xeon поддерживает стандартные или расширенные функции памяти RAS, как указано в таблице 16.

Таблица 16. Функции RAS-памяти

Особенность RAS	Описание	Стандарт	Продви-нутый
Коррекция данных устройства	x8 Single Device Data Correction (SDDC) с помощью статической виртуальной блокировки (применимо к модулям DIMM DRAM x8)	√	√
	ADDDC (SR) (применимо к модулям DIMM DRAM x4)	√	√
	Коррекция данных одного устройства x8 + 1 бит (SDDC + 1) (применимо к модулям DIMM DRAM x8)		√
	SDDC + 1 и ADDDC (MR) + 1 (применимо к модулям DIMM x4 DRAM)		√

Особенность RAS	Описание	Стандарт	Продви-нутый
DDR4 Command/Address (CMD/ADDR) Проверка четности и повторная попытка	Проверка четности CMD/ADDR на основе технологии DDR4 и повторная попытка с регистрацией «адреса» ошибки четности CMD/ADDR и повторной попыткой CMD/ADDR	√	√
Защита данных DDR4 CRC	Обнаруживает сбои шины данных DDR4 во время операции записи	√	√
Требование памяти и очистка патрулей	Очистка по запросу — это возможность записать исправленные данные обратно в память после обнаружения исправляемой ошибки в транзакции чтения. Патрульная очистка проактивно ищет в системной памяти, восстанавливая исправимые ошибки. Предотвращает накопление однобитовых ошибок	√	√
Зеркальное отображение памяти	Полное зеркальное отображение памяти: метод внутри IMC для хранения дублирующей (вторичной или зеркальной) копии содержимого памяти в качестве избыточной резервной копии для использования в случае отказа первичной памяти. Зеркальная копия памяти хранится в памяти IMC того же процессорного разъёма. Dynamic (без перезагрузки) отказоустойчивого для тех зеркальных модулей DIMM прозрачен для ОС и приложений	√	√
Зеркальное отображение памяти	Диапазон адресов/частичное зеркалирование памяти: обеспечивает дополнительную детализацию внутри сокета для зеркалирования памяти, позволяя встроенному ПО или ОС определить диапазон адресов памяти для зеркального отображения, оставив остальную память в сокете в незеркальном режиме		√

Особенность RAS	Описание	Стандарт	Продви-нутый
Резервирование памяти на уровне организации	Динамическое переключение вышедших из строя ранков на резервные ранков, расположенные за теми же ранками контроллера памяти DDR	√	√
Многоранковый экономия памяти	В многоранковом режиме до двух ранков могут быть назначены в качестве запасных	√	√
Сдерживание поврежденных данных iMC	Процесс сообщения об ошибке вместе с обнаруженными данными UC. Патрульный скруббер и резервный двигатель iMC могут отравлять данные UC	√	√
Неудачная изоляция DIMM	Возможность идентифицировать конкретный неисправный DIMM, тем самым позволяя пользователю заменять только вышедший из строя DIMM (ы). В случае неисправленной ошибки и режима блокировки доступна только степень изоляции уровня пары DIMM поддерживается	√	√
Отключение и отображение памяти для отказоустойчивой загрузки (FRB)	Позволяет инициализировать память и загружать ОС даже при сбое памяти	√	√
Почтовый ремонт пакета (PPR)	Начиная с технологии DDR4, доступна дополнительная возможность, известная как Post Package Repair (PPR). PPR предлагает дополнительную свободную ёмкость в DDR4 DRAM, которую можно использовать для замены неисправные области ячеек, обнаруженные во время загрузки системы	√	√

ПРИМЕЧАНИЕ: PAH-функции могут поддерживаться не во всех SKU типа процессора.

Правила заполнения DIMM и настройка BIOS для памяти RAS:

- Параметры резервирования и зеркалирования памяти включены в настройках BIOS.

- Параметры резервирования и зеркалирования памяти являются взаимоисключающими. В настройках BIOS можно выбрать только один режим работы.
- Если режим RAS был включён, а конфигурация памяти не может поддерживать его во время загрузки, система возвращается в режим "независимого канала", регистрирует и отображает ошибки.
- Режим резервирования ранков памяти возможен только в том случае, если все каналы заполнения памяти, удовлетворяют требованию наличия не менее двух одноранковых или двухранковых модулей DIMM или хотя бы одного четырехранкового модуля DIMM, на каждом заполненном канале.
- Режим зеркалирования памяти требует, чтобы для любой пары каналов, использующихся для памяти, объём памяти на обоих каналах был одинаковым.

4.14. Интерфейс PCIe*

4.14.1. Общее описание PCIe*

Интерфейс PCI экспресс* (PCIe*) серверной платы QTECH 469555.005 полностью соответствует базовой спецификации PCIe версии 3.0 и поддерживает значения скорости передачи данных PCIe 3-х версий: 3.0 (8,0 ГТ/с), 2.0 (5,0 ГТ/с) и 1.0 (2,5 ГТ/с). Конкретные характеристики платы и функции, поддерживаемые подсистемой PCIe, см. в разделе 4.21 данного руководства. Информация о маршрутизации портов PCIe от каждого процессора представлена в таблице 17.

Таблица 17. Маршрутизация портов PCIe* от процессоров

	ЦПУ 1		**ЦПУ 2**
PCI-порт	Устройство	PCI-порт	Устройство
DMI 3 – x4	Чипсет	DMI 3 – x4	Слот райзера 3
1A – x4	Слот райзера 1	1A – x4	Слот райзера 2
1B – x4	Слот райзера 1	1B – x4	Слот райзера 2
1C – x4	Слот райзера 1	1C – x4	Слот райзера 1
1D – x4	Слот райзера 1	1D – x4	Слот райзера 1
2A – x4	Чипсет (PCH) – uplink	2A – x4	Слот райзера 2
2B – x4	Чипсет (PCH) – uplink	2B – x4	Слот райзера 2
2C – x4	Чипсет (PCH) – uplink	2C – x4	Слот райзера 2

	ЦПУ 1		ЦПУ 2
2D – x4	Чипсет (PCH) – uplink	2D – x4	Слот райзера 2
3A – x4	Модуль SAS	3A – x4	OCuLink PCIe_SSD2
3B – x4	Модуль SAS	3B – x4	OCulink PCIe_SSD3
3C – x4	OCuLink PCIe_SSD0	3C – x4	Слот райзера 3
3D – x4	M2 PCIe	3D -x4	Слот райзера 3

4.14.2. Перечисление и распределение PCIe*

BIOS присваивает номера шинам, выходящим из PCI, последовательно их сканируя, в соответствии со спецификацией локальной шины PCI 3.0. При обнаружении связи PCI-PCI (шлюз между процессорами), номер шины увеличивается на 1.

Назначение шин PCI может варьироваться от загрузки к загрузке в зависимости от наличия устройств PCI со шлюзами PCI-PCI.

Если у PCI шлюз с одной шиной, то все последующие номера шин PCI меньше номера текущей шины увеличиваются на единицу. Присвоение номера шины происходит один раз в начале процесса загрузки BIOS и не может меняться до следующей перезагрузки системы.

Диспетчер ресурсов BIOS назначает прерывание режима PIC для устройств, к которым обращается устаревший код. BIOS обеспечивает правильную настройку регистров PCI BAR и регистров команд для всех устройств в соответствии с поведением устаревшей BIOS после загрузки устаревшей ОС. Устаревший код не может делать никаких предположений о порядке сканирования устройств или порядке, в котором им выделяются ресурсы. BIOS автоматически назначает IRQ-устройствам в системе для совместимости с устаревшими версиями. Ручная настройка IRQ для устройств не предусмотрена.

4.14.3. Шлюз PCIe между процессорами

Шлюз интерфейса PCIe (NTB) обеспечивает высокопроизводительную связь с малой задержкой между PCIe локальной и удалённых систем. NTB позволяет локальному процессору независимо настраивать и контролировать локальную систему и обеспечивает изоляцию локального домена памяти от удалённого домена памяти, обеспечивая при этом обмен статусом и данными между двумя доменами. NTB обнаруживается локальным процессором как интегрированная конечная точка корневого комплекса (RCiEP).

На рисунке 4-17 показано, как через шлюз подключаются 2 системы с полностью независимыми PCIe. Для системы A количество сетевых портов можно увеличивать от 4 до 16, за счёт других портов.

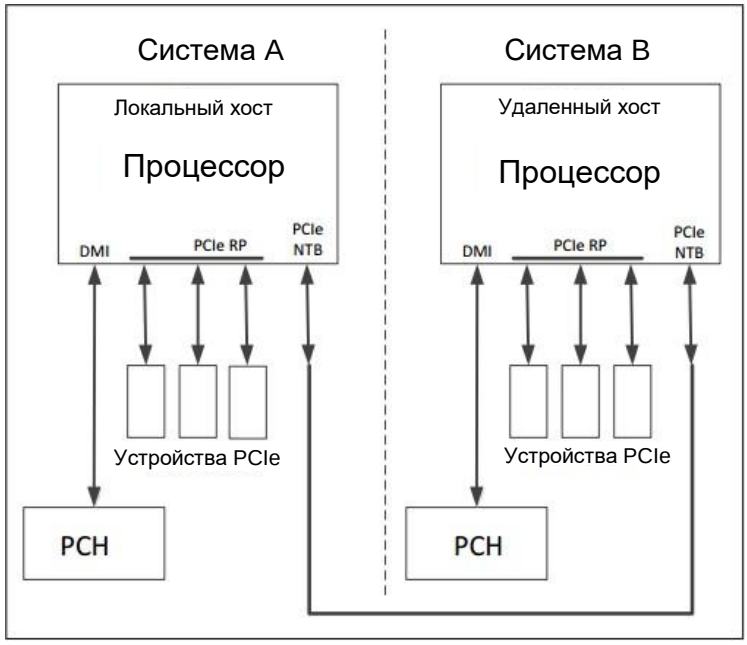


Рисунок 4-17. Две системы, соединенные через шлюз интерфейса PCIe

4.15. Система ввода/вывода

4.15.1. Функции ввода/вывода

Функции ввода/вывода серверной платы реализуются с помощью встроенных функций и функций нескольких встроенных компонентов, включая интегрированный модуль ввода-вывода (IIO) процессора Intel® Xeon®, набор микросхем Intel® серии C621/C624 (PCH) и контроллеры ввода/вывода, встроенные в контроллер управления Aspeed*AST2500. Выше, на рисунке 4-6, представлен обзор функций и взаимосвязей каждого из основных компонентов подсистемы.

Система ввода/вывода серверной платы включает в себя следующие функции:

- поддержка интерфейса PCIe* и карты расширения;
- сетевой адаптер Intel® Ethernet для поддержки OCP*;
- поддержка встроенного RAID-модуля Intel®;
- встроенное хранилище, подсистема;
- поддержка внешнего порта ввода/вывода.

4.15.2. Поддержка переходных плат для PCIe*

Для всех трёх слотов PCIe серверной платы (их расположение на плате см. на рис. 4-1) существуют несколько видов переходных плат. Каждый слот может поддерживать максимальную мощность 75 Вт, соответственно и суммарная мощность портов PCIe на переходной плате не должна превышать потребления мощности в 75 Вт.

В таблицах 16–18 представлены все возможные для обоих процессоров платы QTECH 469555.005 варианты подключения переходных плат по каждому из 3-х её слотов, с соответствующими разрядностями разъёмов.

Суммарная разрядность портов на переходной плате не должна превышать разрядности данного слота PCIe.

На рисунках 18–21 представлены существующие для данной серверной платы варианты переходных плат.

ПРИМЕЧАНИЕ: слоты № 1, № 2 и № 3 предназначены для только переходных плат. Попытка, установить в них другую плату может привести к повреждению одной или обеих плат.

Таблица 18. Конфигурации шин для переходного слота № 1

Слот переходника	2U — 3-слотовый переходник iPC – 469535.083	2U — 2-слотовый переходник iPC – 469535.082
Верхний	ЦПУ 1 — порты 1A и 1B (x8, x16)	ЦПУ 1 — порт 1A через 1D (x16, x16)
Средний	ЦПУ 1 — порты 1C и 1D (x8, x16)	Не поддерживается
Нижний	ЦПУ 2 — порты 1C и 1D (x8, x8)	ЦПУ 2 — порты 1C и 1D (x8, x16)

Таблица 19. Конфигурации шин переходного слота № 2

Слот переходника	2U — 3-слотовый переходник iPC – 469535.083	2U — 2-слотовый переходник iPC – 469535.082
Верхний	ЦПУ 2 — порты 2A и 2B (x8, x16)	ЦПУ 2 — порт 2A через 2D (x16, x16)
Средний	ЦПУ 2 — порты 2C и 2D (x8, x16)	Не поддерживается
Нижний	ЦПУ 2 — порты 1A и 1B (x8, x8)	ЦПУ 2 — порты 1A и 1B (x8, x16)

Таблица 20. Конфигурации шин переходного слота № 3

Слот переходника	2U — низкопрофильный iPC – 469535.081	Примечание
Верхний	ЦПУ 2 — DMI x4 (x4, x8)	Только низкопрофильные переходники
Нижний	ЦПУ 2 — порты 3C и 3D (x8, x8)	

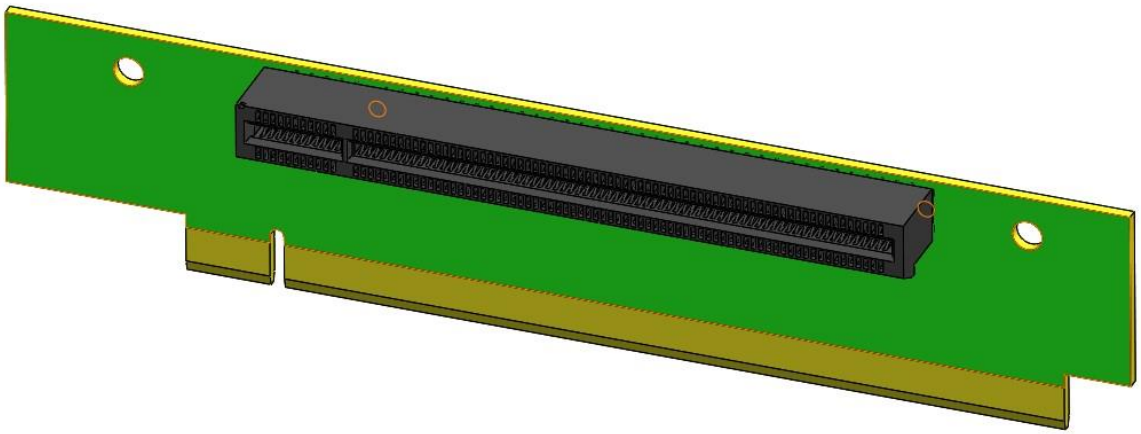


Рисунок 4-18. Однопортовая (x16) 1U переходная плата (469535.084)

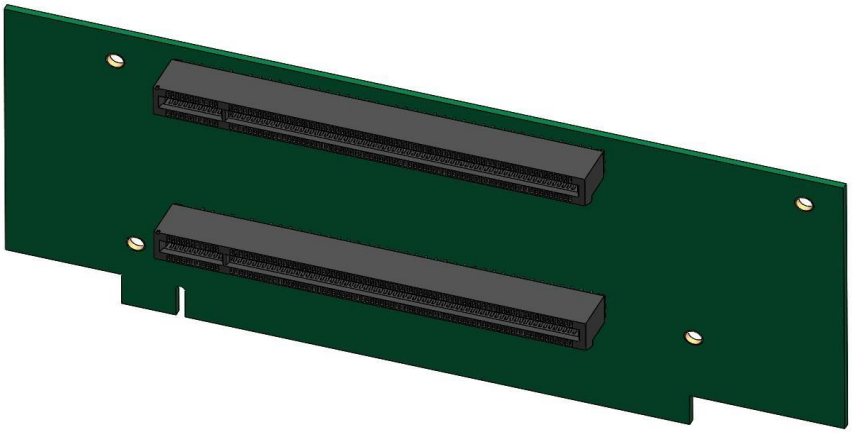


Рисунок 4-19. 2-портовая (x16 и x16) 2U переходная плата (469535.082)

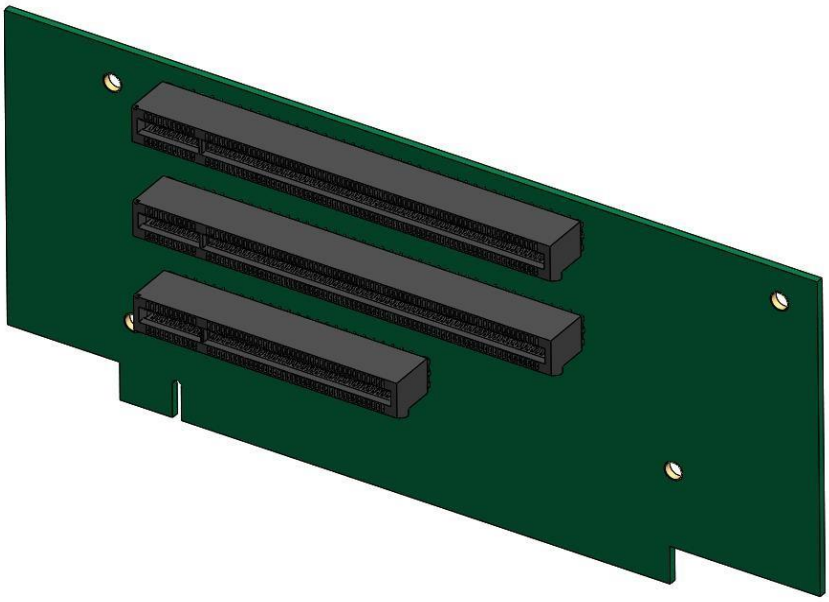


Рисунок 4-20. 3-портовая (x16, x16, x8) 2U переходная плата (469535.083)

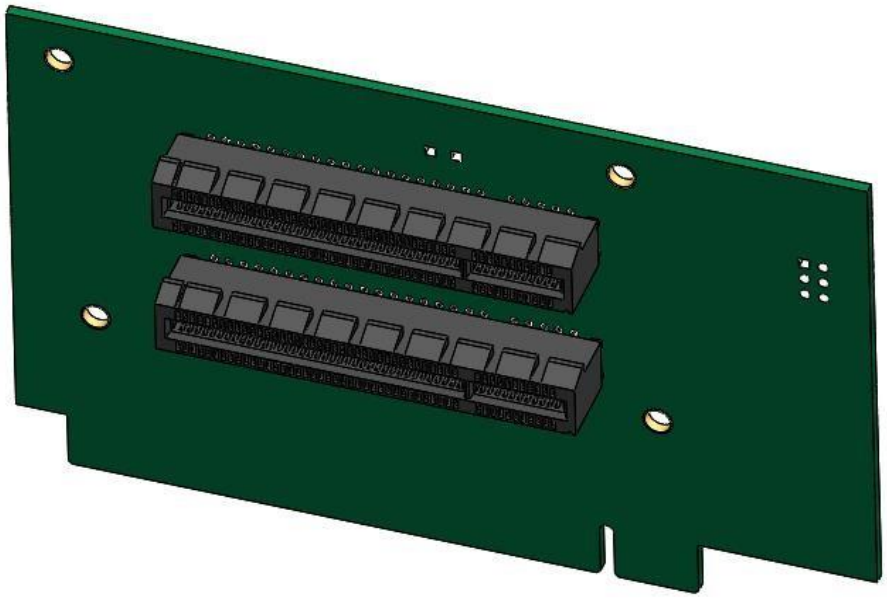


Рисунок 4-21. 2-портовая (x8 и x8) 2U переходная плата (469535.081)

4.15.3. Сетевой адаптер Intel® Ethernet для поддержки OCP*

Серверная плата QTECH 469555.005 (в исполнении с C624) поддерживает линейку мезонинных модулей LAN KR OCP, соответствующих форм-фактору OCP 2.0. Дополнительный мезонинный модуль OCP можно установить в разъём с маркировкой «OCP_IO_Module» на серверной плате, как показано на рисунке:

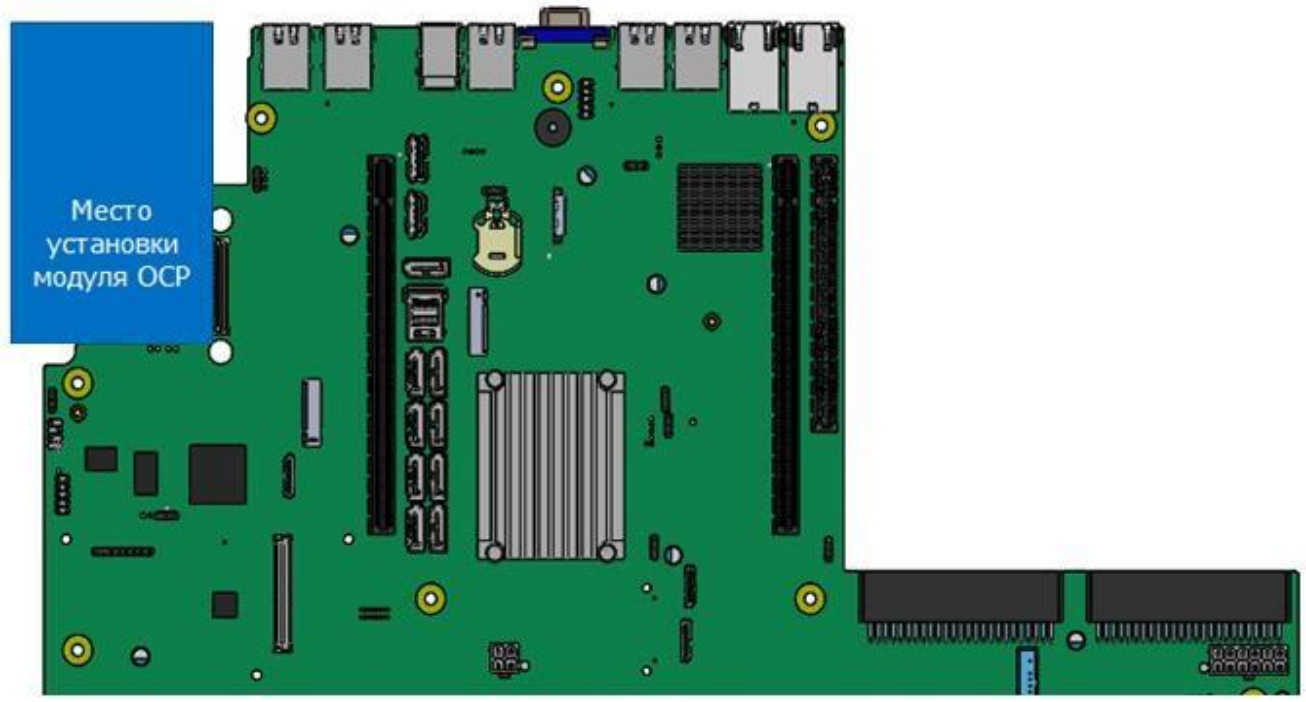


Рисунок 4-22. Список поддерживаемых интерфейсов OCP

Таблица 21. Список поддерживаемых интерфейсов OCP

Описание	iPC
4 порта RJ-45 (1 Гбит)	I357T4OCPG1P5
4 порта SFP+	X527DA4OCPG1P5
2 порта SFP+	X527DA2OCPG1P5
2 порта RJ-45 (10 Гбит)	X557T2OCPG1P5

4.15.4. Поддержка встроенного RAID-модуля

Материнская плата QTECH 469555.005 поддерживает множество PCIe-адаптеров, которые позволяют установить RAID-адаптеры на 12 Гбит. Для системных конфигураций с ограниченным количеством слотов для дополнительных карт дополнительный встроенный модуль RAID от Intel® может быть установлен на 80-контактный разъём высокой плотности с надписью «SAS Module» на плате. Установка на материнскую плату интегрированного RAID-модуля SAS показана на рисунке 4-23.

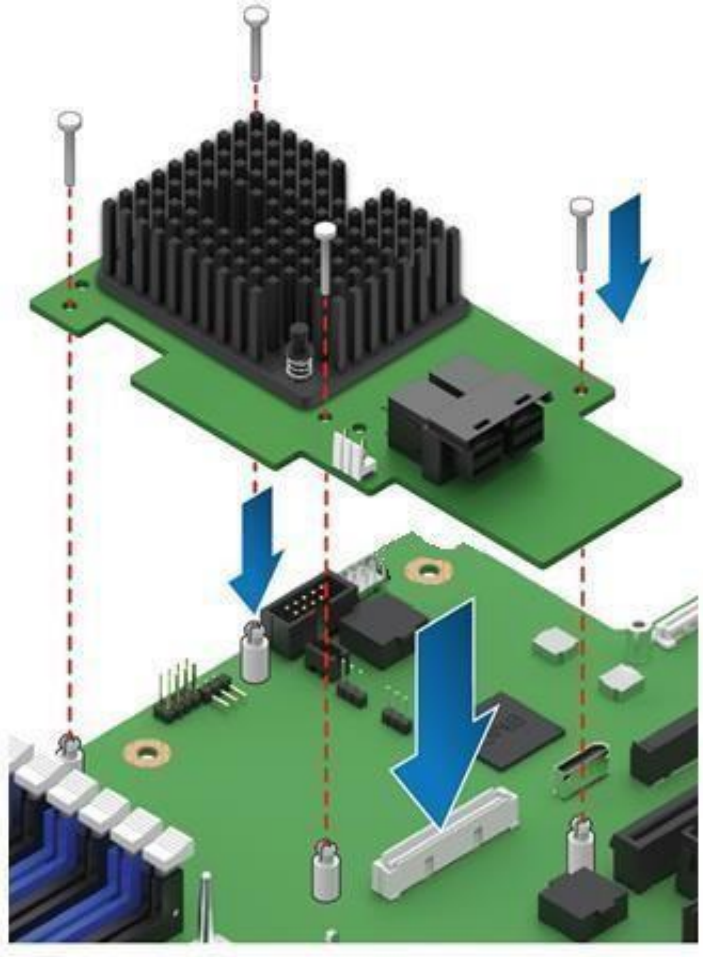


Рисунок 4-23. Монтаж интегрированного RAID-модуля SAS

4.16. Встроенная подсистема хранения данных

Материнская плата QTECH 469555.005 включает поддержку многих технологий, связанных с хранением данных, и встроенные функции для поддержки широкого спектра вариантов хранения данных. К ним относятся:

- x2 — M.2 PCIe*/SATA*;
- x3 — PCIe* OCuLink;
- устройство управления томами Intel® (Intel® VMD) для NVMe*;
- Intel® VROC (VMD NVMe RAID) 6.0;
- x9 — 7-контактный однопортовый SATA;
- x1 — Mini-SAS HD (SFF-8643) 4-портовый SATA;
- встроенные возможности SATA RAID:
    - Intel® VROC (SATA RAID) 6.0,
    - технология Intel® RAID 2 (Intel® ESRT2) v1.60 для SATA.

Далее представлен обзор каждого параметра.

4.16.1. Поддержка твердотельных накопителей M.2

Данная материнская плата имеет два разъёма для M.2 SSD с маркировкой «M2_x4PCIE/sSATA_1» и «M2_x2PCIE/sSATA_2», как показано на рисунке 4-24:

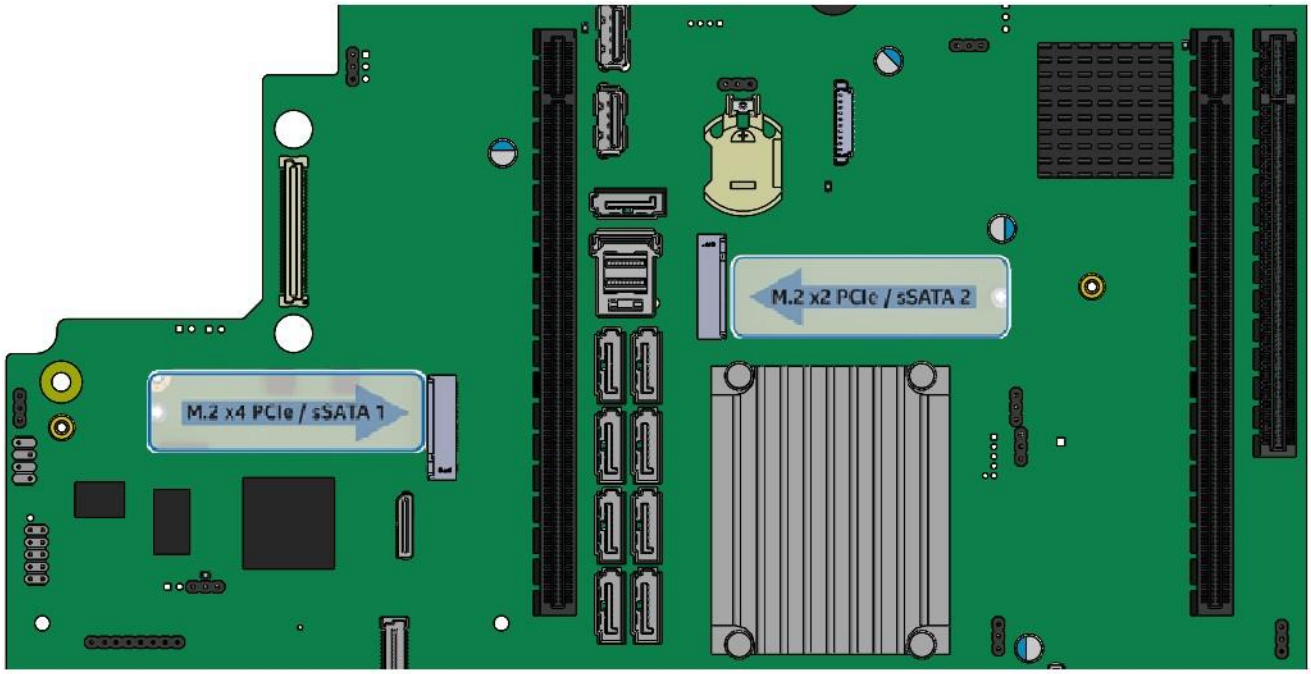


Рисунок 4-24. Два разъёма для M.2 SSD на материнской плате

Разъёмы M.2 могут поддерживать модули 1xPCIe/SATA и 4xPCIe, соответствующие форм-фактору 2280 (80 мм). Линии шины PCIe для каждого разъёма направляются от чипсета Intel и CPU 1 и могут поддерживаться в конфигурациях с одним процессором. Разъём M.2 слева от Riser Slot #1 поддерживается линиями шины PCIe x4. Разъём M.2 справа от Riser Sot #1 поддерживается линиями шины PCIe x1 и sSATA-2 от встроенного в чипсет контроллера sSATA.

Определение контактов разъёма M.2 доступно только после получения схемы платы непосредственно от QTECH (требуется соглашение о неразглашении).

4.16.2. Поддержка встроенного RAID

Поддержка RAID от встроенных опций RAID для твердотельных накопителей M.2, установленных на серверной плате, определяется следующим образом:

- Ни Intel® ESRT2, ни Intel® VROC (SATA RAID) не поддерживают RAID для твердотельных накопителей PCIe M.2 при установке в разъёмы M.2.
- И Intel ESRT2, и Intel® VROC (SATA RAID) обеспечивают поддержку RAID для устройств SATA.
- Ни один из вариантов встроенного RAID не поддерживает совместное использование твердотельных накопителей M.2 SATA и жестких дисков SATA в одном томе RAID.
- Бинарный драйвер включает частичные исходные файлы. Драйвер является полностью открытым исходным кодом с использованием слоя MDRAID в Linux*.

Вариант Intel ESRT2 не поддерживает устройства PCIe.

ПРИМЕЧАНИЕ: поддержка NVMe RAID с использованием Intel® VROC (SATA RAID) и Intel VROC требует, чтобы линии шины PCIe направлялись непосредственно от ЦП. На данной серверной плате линии шины PCIe ко встроенным разъёмам M.2 направляются от чипсета Intel (PCH).

ПРИМЕЧАНИЕ: устройства хранения, используемые для создания единого тома RAID, созданного с использованием Intel® VROC (SATA RAID) или Intel ESRT2, не могут охватывать два встроенных контроллера SATA, а также не поддерживается совместное использование устройств SATA и NVMe в одном томе RAID.

4.16.3. Встроенные разъёмы PCIe* OCuLink

Серверная плата имеет три разъёма PCIe OCuLink для обеспечения интерфейса PCIe для твердотельных накопителей NVMe, установленных на передней объединительной панели с возможностью горячей замены. Сигналы PCIe для разъёмов OCuLink «PCIe_SSD0» и «PCIe_SSD1» направляются непосредственно от ЦПУ1, а сигналы PCIe для разъёмов OCuLink «PCIe_SSD2» и «PCIe_SSD3» направляются напрямую от ЦПУ2. Для определения контактов разъёма OCuLink см. раздел 4.21. Расположение разъёмов OCuLink показано на рисунке 4-25:

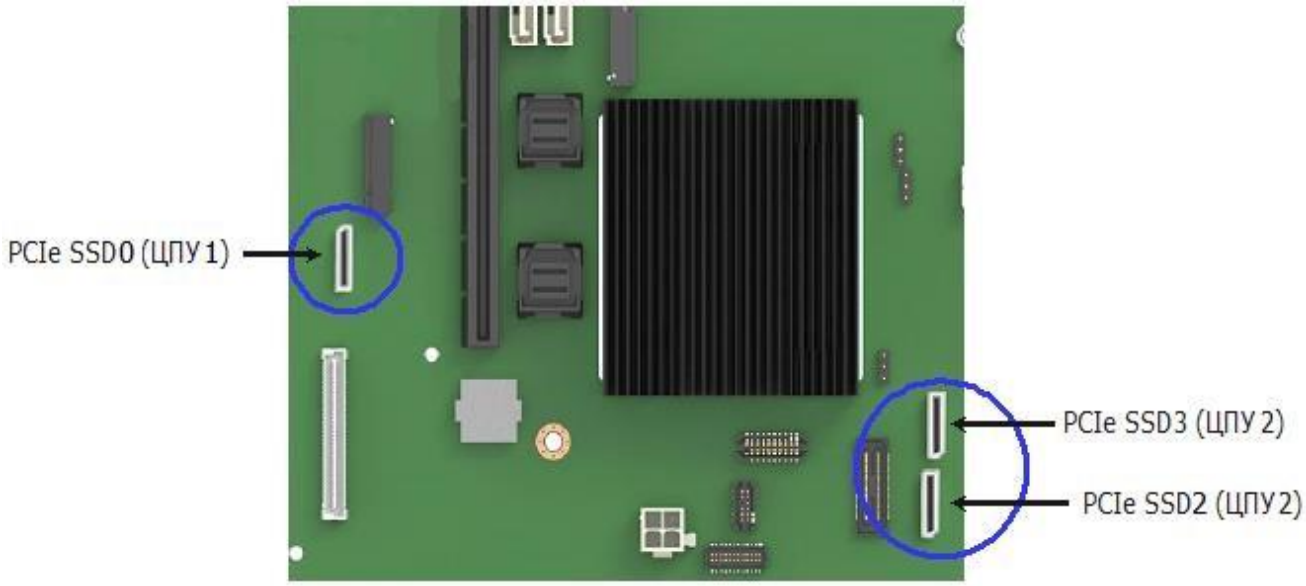


Рисунок 4-25. Разъёмы OCuLink

4.16.4. Функция Intel® VROC (VMD NVMe RAID) 6.0

Ниже на рисунке 4-26 представлен обзор базовой архитектуры Intel® VROC (VMD NVMe RAID):

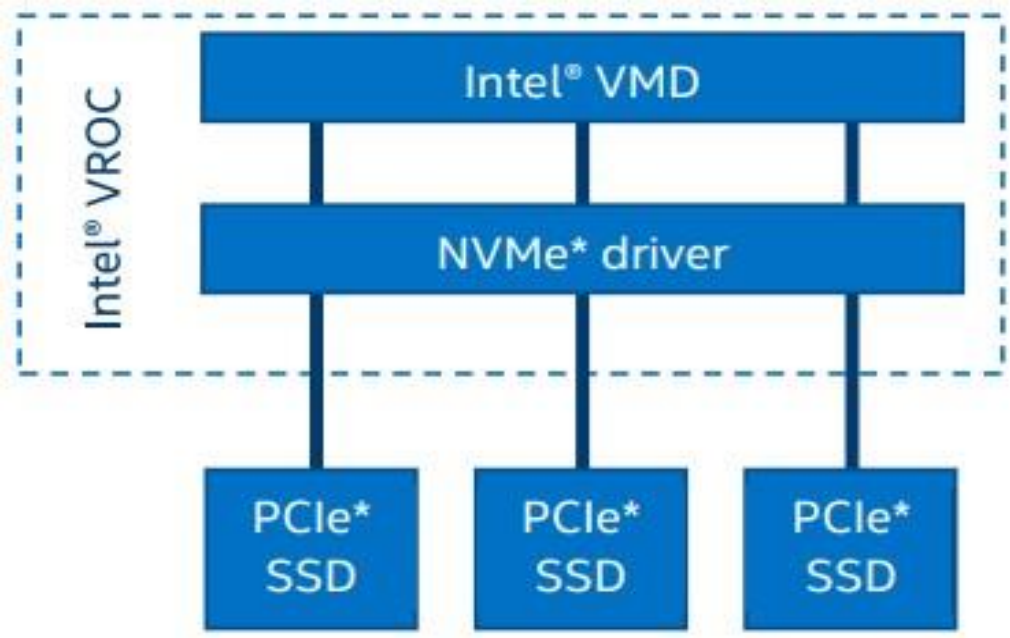


Рисунок 4-26. Базовая архитектура Intel® VROC (VMD NVMe RAID)

Intel® VROC (VMD NVMe RAID) имеет следующие возможности:

- Процессор ввода/вывода с контроллером (ROC) и DRAM.
- Отсутствие необходимости в резервном аккумуляторе или необслуживаемом резервном блоке RAID.
- Защищённый кеш с обратной записью — программное и аппаратное обеспечение, обеспечивающее восстановление после двойной ошибки.
- Изолированные от ОС запоминающие устройства для обработки ошибок.
- Защита данных R5 от сбоя ОС.
- Загрузка с томов RAID на основе твердотельных накопителей NVMe в одном домене VMD.
- Горячее подключение NVMe SSD и неожиданное извлечение на линиях CPU PCIe.
- Управление светодиодами для хранилища, подключенного к процессору PCIe.
- Управление RAID/хранилищем с использованием интерфейсов прикладного программирования (API) с передачей состояния представления (RESTful).
- Графический пользовательский интерфейс (GUI) для Linux.
- Поддержка твердотельных накопителей NVMe с разрешением 4K.

ПРИМЕЧАНИЕ: встроенный разъём, используемый для поддержки вариантов ключа обновления Intel® VROC (VMD NVMe RAID), также используется для поддержки ключа обновления Intel® ESRT2 SATA RAID-5.

В таблице 22 указаны доступные варианты ключей обновления Intel VROC. Включение поддержки Intel® VROC (VMD NVMe RAID) требует установки дополнительного ключа обновления на серверную плату, как показано на рисунке 4-27.

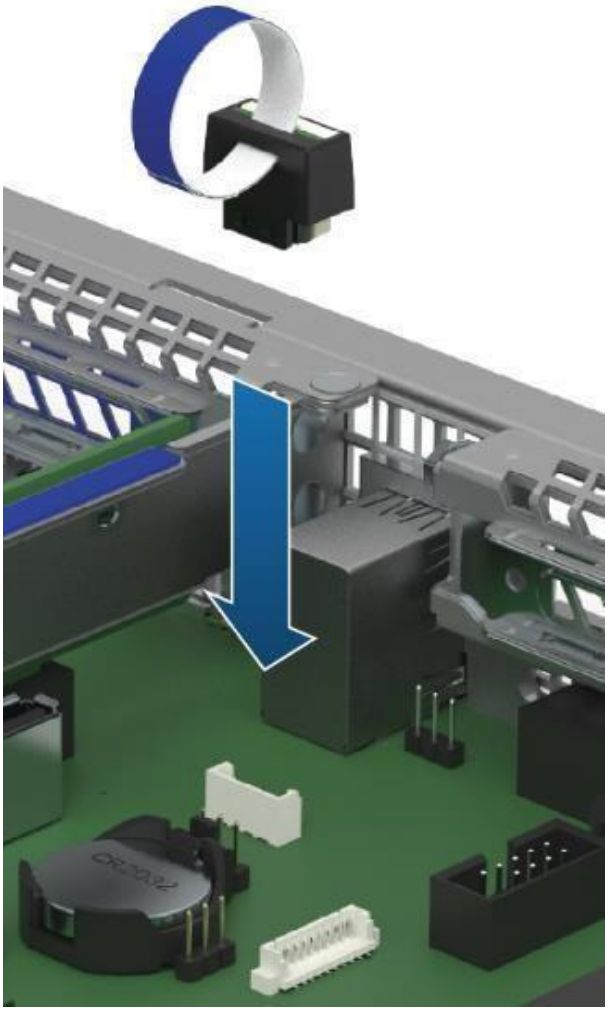


Рисунок 4-27. Установка дополнительного ключа обновления

Таблица 22. Ключевые варианты обновления Intel® VROC (VMD NVMe RAID)

Основные характеристики NVMe* RAID	**Стандартный VROC (iPC VROCSTANMOD)**	**VROC премиум класса (iPC VROCPREMMOD)**
Твердотельный накопитель NVMe с подключением к процессору — высокая производительность	√	√
Загрузка с тома RAID	√	√
Поддержка твердотельных накопителей сторонних производителей	√	√
Отверстие записи RAID закрыто (замена RMFBU)	–	√

Основные характеристики NVMe* RAID	Стандартный VROC (iPC VROCSTANMOD)	VROC премиум класса (iPC VROCPREMMOD)
Поддержка RAID — 0, 1, 10	√	√
Поддержка RAID — 0, 1, 5, 10	–	√
Горячее подключение/неожиданное удаление (только для форм-фактора 2,5-дюймового твердотельного накопителя)	√	√
Управление светодиодами корпуса	√	√

Ключи обновления Intel VROC используется только для твердотельных накопителей PCIe NVMe. Информацию о поддержке SATA RAID см. в пункте 4.16.6.

4.16.5. Поддержка SATA

В серверной плате используются два встроенных в чипсет контроллера AHCI SATA, обозначенные, как «SATA» и «sSATA», обеспечивающие до двенадцати портов SATA с пропускной способностью до 6 Гбит/с.

Контроллер AHCI sSATA поддерживает до 6 портов SATA на серверной плате:

- Один разъём mini-SAS HD (SFF-8643) порты sSATA 0-3.
- Один порт (sSATA 4) через разъём M.2 SSD.
- Однопортовый 7-контактный разъём с маркировкой «sSATA-5» плате.

Контроллер AHCI SATA обеспечивает поддержку до 8 портов SATA на серверной плате:

- 8 однопортовых 7-контактных разъёмов.

ПРИМЕЧАНИЕ: встроенные контроллеры SATA несовместимы и не могут использоваться с картами расширения SAS.

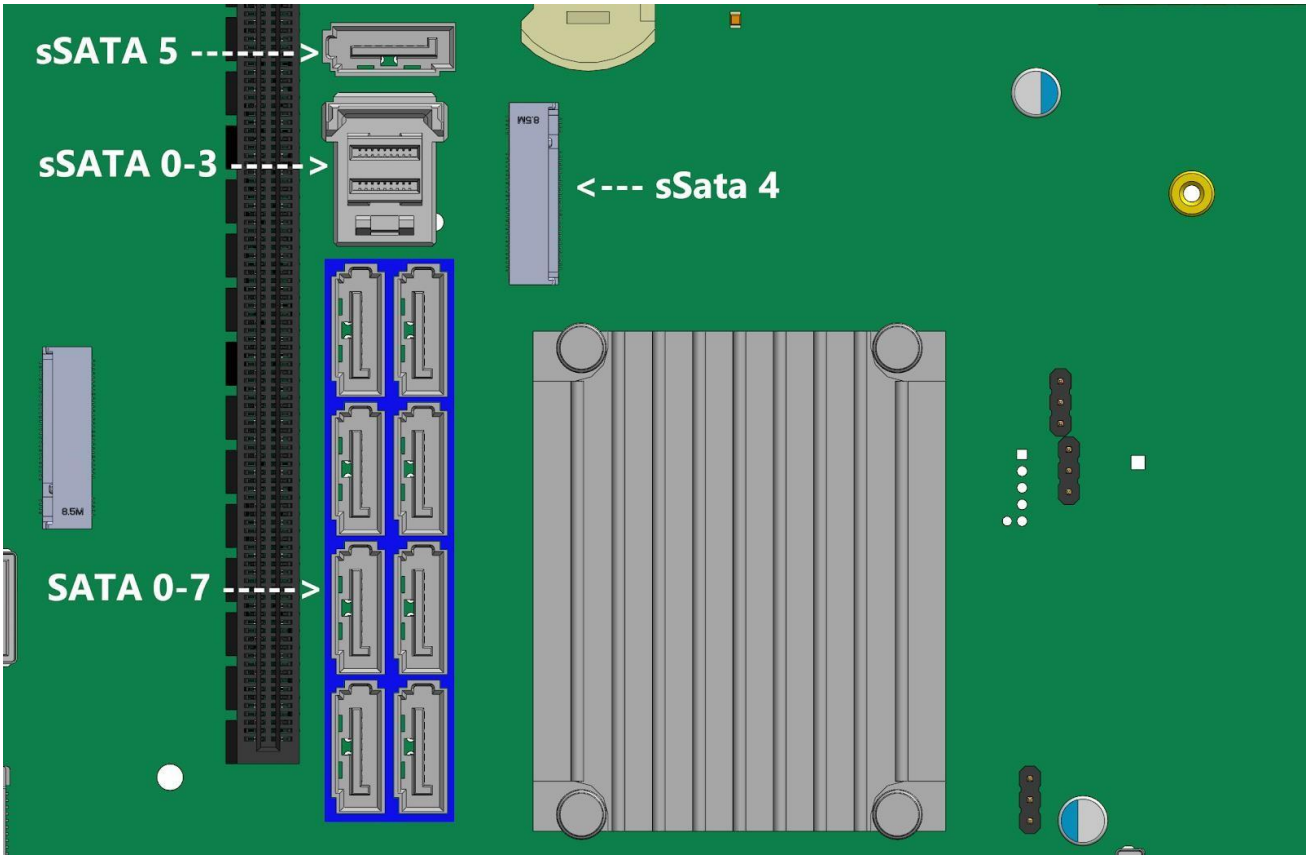


Рисунок 4-28. Идентификация разъёма порта SATA на плате

Контроллер SATA и контроллер sSATA можно независимо включать и отключать, а также настраивать с помощью утилиты настройки BIOS на экране меню Mass Storage Controller Configuration.

В таблице 23 перечислены все поддерживаемые функции контроллеров SATA и sSATA, а в таблице 24 указаны поддерживаемые ими параметры настройки.

Таблица 23. Поддержка функций контроллеров SATA и sSATA

Функции	Описание	Режим AHCI	Режим RAID VROC (SATA RAID)	Режим RAID ESRT2
Встроенная очередь команд (NCQ)	Изменение порядка команд для более эффективной передачи данных	Есть	Есть	
Автоматическая активация для DMA	Сворачивает настройку DMA, а затем активирует последовательность DMA при настройке DMA	Есть	Есть	

Функции	Описание	Режим AHCI	Режим RAID VROC (SATA RAID)	Режим RAID ESRT2
Поддержка горячего подключения	Позволяет обнаруживать устройства без подачи питания и возможность подключать и отключать устройства без предварительного уведомления системы	Есть	Есть	
Асинхронное восстановление сигнала	Обеспечивает восстановление после потери сигнала или установления связи после горячего подключения	Есть	Есть	
Передача данных	Возможность передачи данных до 6 Гбит/с	Есть	Есть	Есть
Асинхронное уведомление ATAPI	Механизм отправки устройством уведомления хосту о том, что устройство требует внимания	Есть	Есть	
Управление питанием, инициированное хостом и каналом	Возможность для хост-контроллера или устройства запрашивать состояния питания интерфейса Partial и Slumber	Есть	Есть	
Ступенчатое раскручивание	Позволяет хосту последовательно запускать жёсткие диски, чтобы предотвратить проблемы с нагрузкой при загрузке	Есть	Есть	Есть
Объединение завершения команд	Снижает накладные расходы на прерывания и завершения, позволяя завершить указанное количество команд, а затем генерируя прерывание для обработки команд	Есть	Нет	

Таблица 24. Параметры настройки контроллеров SATA и sSATA

Контроллер SATA	Контроллер sSATA	Поддержка
AHCI	AHCI	Есть

Контроллер SATA	Контроллер sSATA	Поддержка
AHCI	Не функционирует	Есть
AHCI	VROC (SATA RAID) 6.0	Есть
AHCI	ESRT2	Только для Windows
Не функционирует	AHCI	Есть
Не функционирует	Не функционирует	Есть
Не функционирует	VROC (SATA RAID) 6.0	Есть
Не функционирует	ESRT2	Есть
VROC (SATA RAID) 6.0	AHCI	Есть
VROC (SATA RAID) 6.0	Не функционирует	Есть
VROC (SATA RAID) 6.0	VROC (SATA RAID) 6.0	Есть
VROC (SATA RAID) 6.0	ESRT2	Нет
ESRT2	AHCI	Только для Windows
ESRT2	Не функционирует	Есть
ESRT2	VROC (SATA RAID) 6.0	Нет
ESRT2	ESRT2	Есть

4.16.5.1. Последовательный запуск дисков

Из-за высокой производительности дисков, которые могут быть подключены к встроенному контроллеру Intel® C621/C624 AHCI SATA и контроллеру sSATA, совокупный скачок потребляемой мощности при запуске для всех дисков одновременно может быть намного выше, чем обычные требования к потребляемой мощности, и может потребоваться гораздо больший источник питания для запуска, чем для нормальной работы.

Чтобы смягчить это и уменьшить пиковое энергопотребление во время запуска системы, как контроллер AHCI SATA, так и контроллер sSATA реализуют возможность поэтапного

запуска дисков. Это означает, что диски запускаются отдельно, один за одним с определённой задержкой.

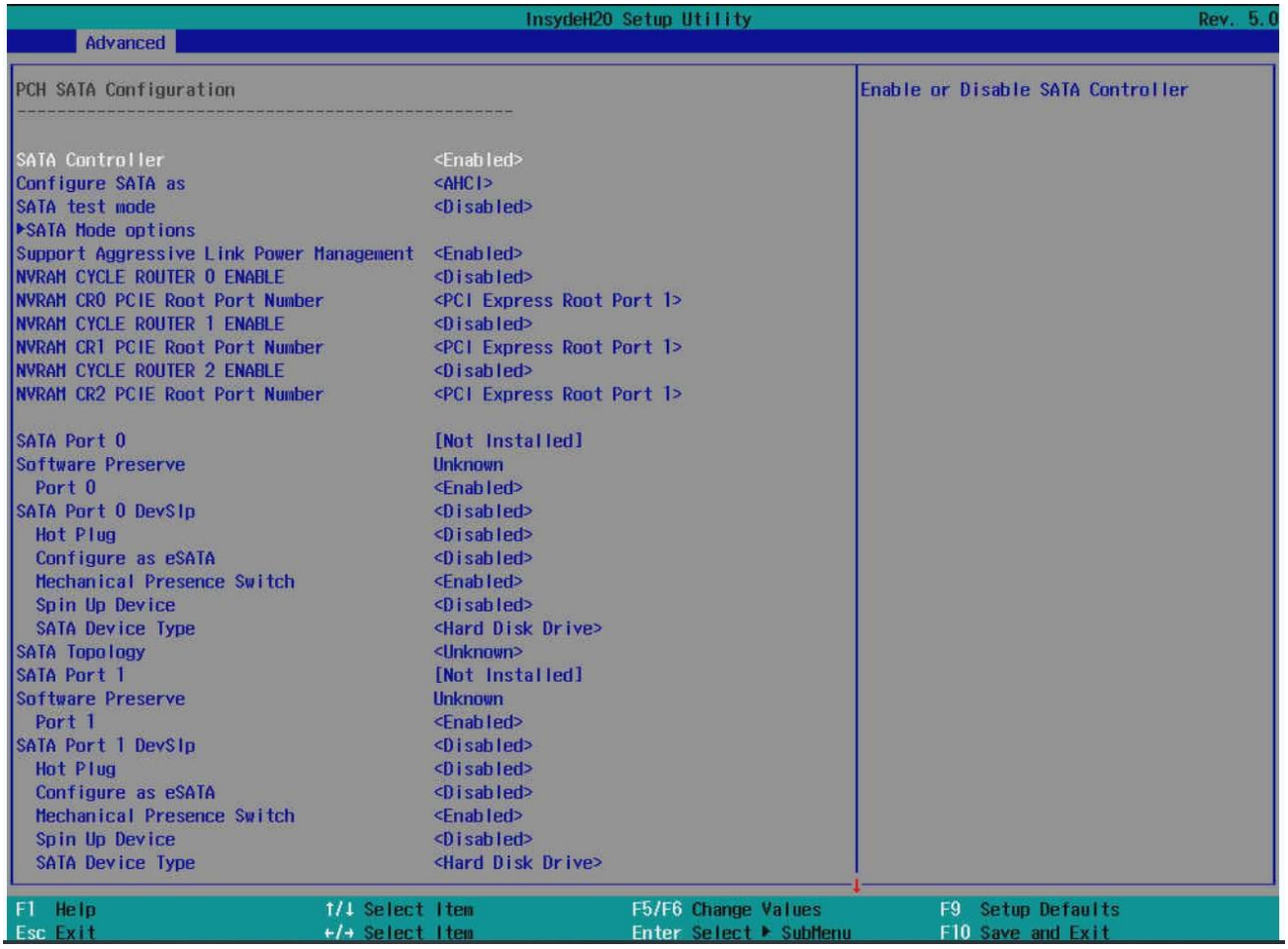
Для встроенного контроллера SATA такой ступенчатый запуск является отдельной опцией (**AHCI HDD Staggered Spin-Up**) в меню конфигурации контроллера запоминающего устройства в утилите настройки BIOS.

4.16.6. Встроенные опции SATA RAID

Серверная плата поддерживает два встроенных варианта SATA RAID:

- VROC (SATA RAID) 6.0;
- технология встроенного в сервер RAID 2 (Intel® ESRT2) 1.60.

По умолчанию параметры встроенного RAID отключены в настройках BIOS. Чтобы включить встроенную поддержку RAID, откройте утилиту настройки BIOS в процессе POST. Параметры встроенного RAID можно найти в разделе меню «**PCH SATA Configuration**» или «**PCH sSATA Configuration**» для первичного и вторичного контроллеров SATA:



4.16.6.1. Intel® VROC (SATA RAID) 6.0

VROC (SATA RAID) предлагает несколько вариантов RAID для удовлетворения потребностей конечного пользователя. Поддержка AHCI обеспечивает более высокую производительность и устраняет узкие места дисков за счёт использования независимых механизмов прямого доступа к памяти, которые предлагает каждый порт SATA в наборе микросхем.

Поддерживаемые уровни RAID включают 0, 1, 5 и 10:

- RAID 0 использует чередование для обеспечения высокой пропускной способности данных, особенно для больших файлов в среде, не требующей отказоустойчивости.
- RAID 1 использует зеркальное отображение, чтобы данные, записываемые на один диск, одновременно записывались на другой диск. Это хорошо для небольших баз данных или других приложений, требующих небольшой ёмкости, но полной избыточности данных.
- RAID 5 использует чередование дисков и данные чётности на всех дисках (распределённая чётность) для обеспечения высокой пропускной способности данных, особенно для небольшого произвольного доступа.
- RAID 10 — комбинация RAID 0 и RAID 1, состоящая из чередующихся данных в зеркальных участках. Он обеспечивает высокую пропускную способность и полную избыточность данных, но использует большее количество диапазонов.

При использовании VROC (SATA RAID) не происходит потери ресурсов PCI (пара запрос/предоставление) или слота для карты расширения. Для работы VROC (SATA RAID) требуется следующее:

- в настройках BIOS должна быть включена опция встроенного RAID;
- в настройках BIOS должна быть установлена опция VROC (SATA RAID);
- должны быть загружены драйверы VROC (SATA RAID) для установленной операционной системы;
- для поддержки уровней RAID 0 или 1 необходимо как минимум два диска SATA;
- для поддержки RAID уровня 5 необходимо как минимум три диска SATA;
- для поддержки уровня RAID 10 необходимо не менее четырех дисков SATA;
- SSD-накопители NVMe и диски SATA нельзя смешивать в одном томе RAID.

С включённым программным RAID-массивом Intel® VROC (SATA RAID) становятся доступными следующие функции.

- Среда загрузки, предшествующая операционной системе, пользовательский интерфейс в текстовом режиме, который позволяет пользователю управлять конфигурацией RAID в системе. Его набор функций остаётся простым, чтобы свести размер к минимуму, но позволяет пользователю создавать и удалять тома RAID и выбирать параметры восстановления при возникновении проблем. Доступ к пользовательскому интерфейсу можно получить, нажав <CTRL-I> в процессе POST-системы.
- Поддержка загрузки при использовании тома RAID в качестве загрузочного диска. Это достигается за счёт предоставления служб Int13, когда приложения MS-DOS должны получить доступ к тому RAID (например, загрузчика NT (NTLDR)) и путём экспорта томов RAID в системный BIOS для выбора в порядке загрузки.
- При каждой загрузке пользователю предоставляется статус томов RAID.

4.16.6.2. Технология Intel® встроенного RAID 2 (Intel® ESRT2) 1.60 для SATA

Intel ESRT2 (на базе LSI*) — это RAID-решение на основе драйверов для SATA, совместимое с серверными RAID-решениями Intel® предыдущего поколения. Intel ESRT2 обеспечивает уровни RAID 0, 1 и 10 с дополнительной возможностью RAID 5 в зависимости от того, установлен ли ключ обновления RAID.

ПРИМЕЧАНИЕ: встроенный вариант Intel ESRT2 не поддерживает RAID для твердотельных накопителей PCIe NVMe.

Intel ESRT2 основан на программном стеке LSI MegaRAID и использует системную память и ЦП. Поддерживаемые уровни RAID включают в себя: RAID 0, RAID 1 и RAID 10. Дополнительную поддержку RAID уровня 5 можно включить, добавив ключ обновления RAID 5 (iPN-RKSATA4R5), как показано на рисунке 4-29:

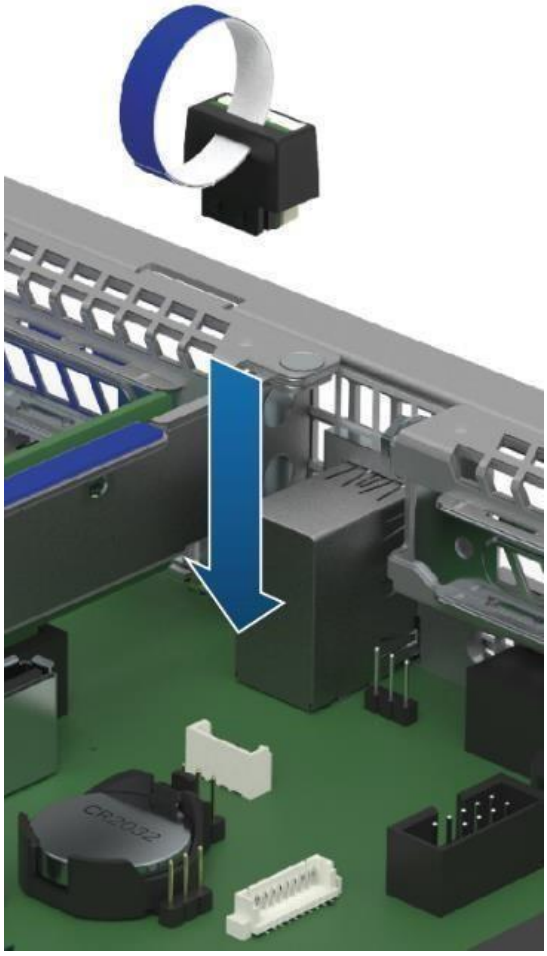


Рисунок 4-29. Ключ обновления RAID 5

ПРИМЕЧАНИЕ: встроенный разъём, используемый для поддержки ключа обновления Intel® ESRT2 SATA RAID-5, также используется для поддержки вариантов ключа обновления Intel® VROC (VMD NVMe RAID).

4.17. Сетевые разъёмы RJ-45

На задней стороне серверной платы имеется несколько разъемов RJ-45, поддерживающих следующие бортовые функции:

- выделенный порт управления сервером;
- разъёмы сетевого интерфейса.

На рисунке 4-30 показаны задние внешние разъёмы серверной платы.

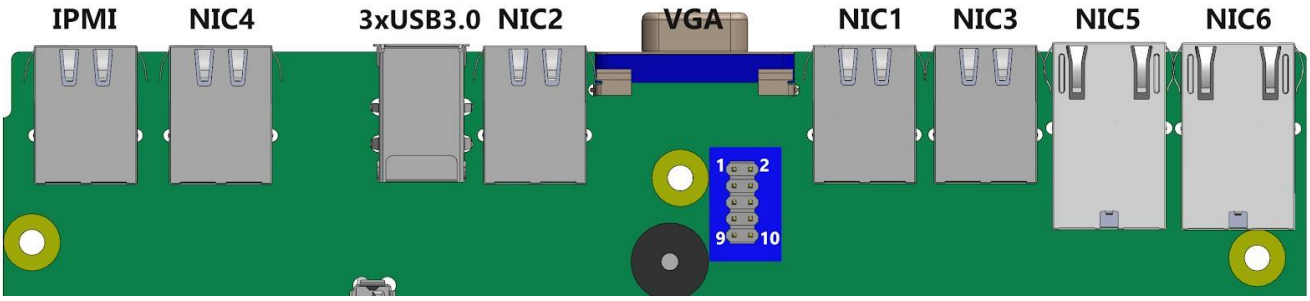


Рисунок 4-30. Разъёмы RJ-45 серверной платы

Разъёмы RJ-45, используемые для выделенного порта управления и разъёмы сетевого интерфейса, имеют два светодиодных индикатора, зелёный и жёлтый:

Зелёный светодиод показывает наличие сетевого подключения и наличие передачи данных, жёлтый светодиод показывает различную скорость передачи данных. Далее в таблице дано описание состояний индикаторов:

Тип портов	Индикатор	Состояние индикатора	Состояние системы
1 Гбит	Зелёный	Непрерывно горит	Установлено соединение с сетью
		Мигает	Передача данных
	Жёлтый	Непрерывно горит	Передача данных со скоростью 1 Гбит
10 Гбит	Зелёный справа	Непрерывно горит	Установлено соединение с сетью
		Мигает	Передача данных
	Зелёный слева	Непрерывно горит	Передача данных со скоростью 1 Гбит
	Жёлтый слева	Непрерывно горит	Передача данных со скоростью 10 Гбит

На серверной плате имеется выделенный порт управления 1 GbE RJ-45. Дополнительную информацию о встроенной поддержке управления сервером см. в разделе 4.25.

Серверная плата QTECH 469555.005 может собираться в различных конфигурациях и иметь до 7 разъёмов типа RJ-45: один выделенный порт управления IPMI и шесть сетевых портов «NIC1» – «NIC6. Плата опционально может быть собрана с контроллером Intel® Ethernet: X557-AT2 10 GbE.

4.18. Поддержка последовательного порта

Серверная плата поддерживает два последовательных порта: A и B.

Последовательный порт A — это внутренний разъём типа header 2x5, расположенный ближе к задней стороне серверной платы (на рисунке 4-30 выделен синим прямоугольником).

В таблице ниже показано распределение контактов:

Назначение контакта	№ контакта	Назначение контакта	№ контакта
DCD	1	DSR	2
SIN	3	RTS	4
SOUT	5	CTS	6
DTR	7	NC	8
GROUND	9	NC	10

Последовательный порт B определяется внутренним разъёмом DH-3, а на серверной плате обозначен маркировкой «J1D4». Распиновка его контактов показана в таблице 23. Данный порт используется для отладки BMC. Разъём устанавливается по требованию заказчика.

Таблица 25. Распределение сигналов по контактам порта B

Вид сигнала	Номер контакта
UART_TXD	1
GND	2
UART_RXD	3

4.19. Поддержка USB-разъёмов

4.19.1. Внешний разъём USB3.0

Серверная плата включает в себя три порта USB 3.0 (1×3, расположенные друг над другом) на её задней стороне (рис. 4-31).

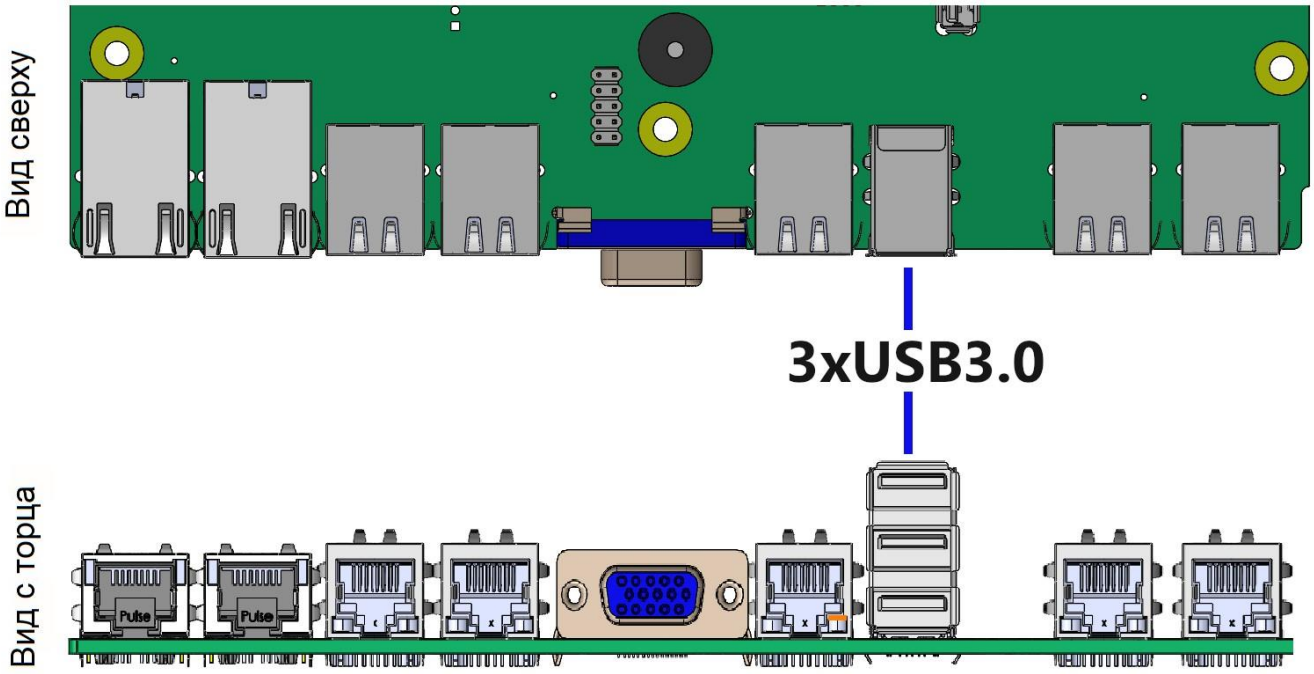


Рисунок 4-31. Расположение портов USB на плате

4.19.2. Внутренний разъём USB 2.0 типа A

Данный разъём расположен на серверной плате, как показано на следующем рисунке (выделено синим овалом):

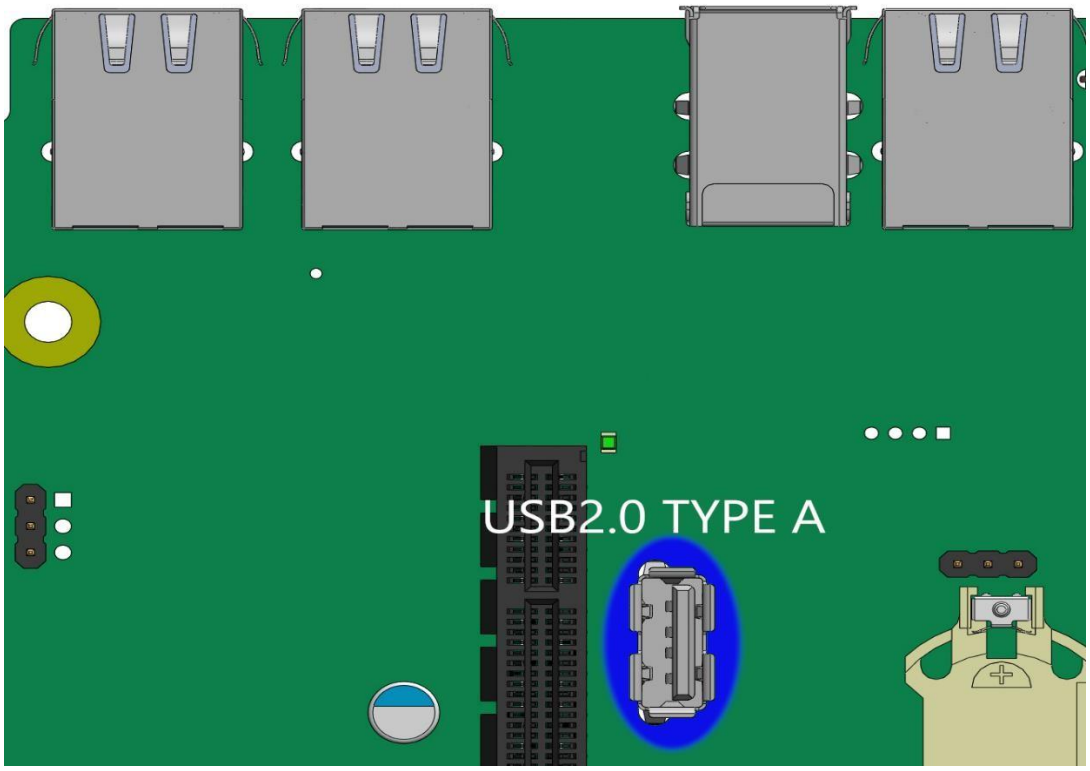


Рисунок 4-32. Внутренний разъём USB 2.0 типа A

4.19.3. Разъём для подключения USB 3.0 front panel

На серверной плате имеется специальный 20-контактный (2×10) закрытый разъём синего цвета (обозначенный «FP_USB_2.0/3.0»), позволяющий установить соединение с двумя портами USB 3.0 на передней панели корпуса сервера.

В таблице 26 показана распиновка данного разъёма, а на рисунке 4-33 показано (выделено жёлтым кругом) его расположение на плате.

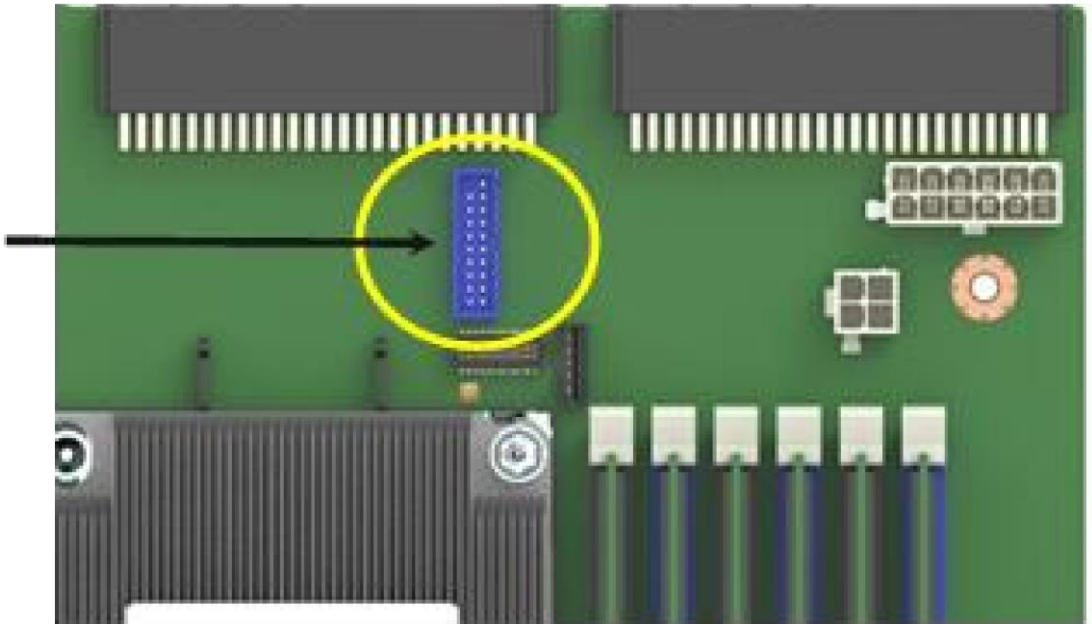


Рисунок 4-33. Расположение разъёма FP_USB_2.0/3.0 на плате

Таблица 26. Распределение сигналов по контактам разъёма FP_USB_2.0/3.0

Вид сигнала	Номер контакта		Вид сигнала
–	–	1	P5V_USB_FP
P5V_USB_FP	19	2	USB3_04_RXN
USB3_01_RXN	18	3	USB3_04_RXP
USB3_01_RXP	17	4	GROUND
GROUND	16	5	USB3_04_TXN
USB3_01_TXN	15	6	USB3_04_TXP
USB3_01_TXP	14	7	GROUND

Вид сигнала	Номер контакта		Вид сигнала
GROUND	13	8	USB2_13_DN
USB2_10_DN	12	9	USB2_13_DP
USB2_10_DP	11	10	USB3_ID

4.19.4. Разъём для подключения USB 2.0 front panel

Серверная плата оснащена также 10-контактным разъёмом, который при подключении кабеля может обеспечить до двух портов USB 2.0 на передней панели сервера. Разъём обозначен «FP_USB_2.0_5-6» и расположен с левой стороны, рядом с разъёмом модуля ввода-вывода.

В таблице 27 показана распиновка данного разъёма, а на рисунке 4-34 показано (выделено жёлтым кругом) его расположение на плате.

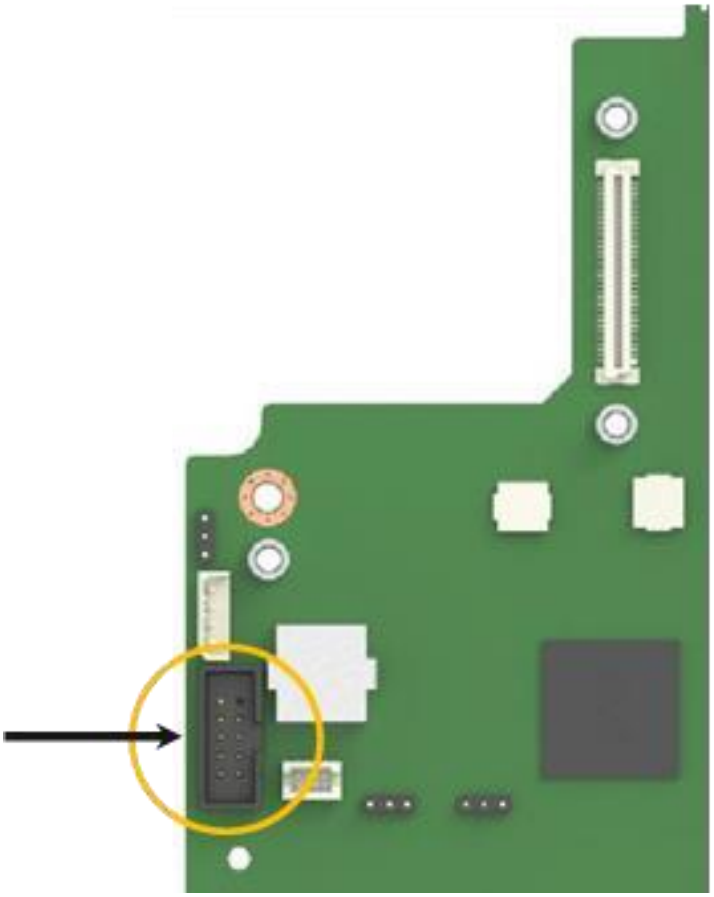


Рисунок 4-34. Расположение разъёма FP_USB_2.0_5-6 на плате

Таблица 27. Распределение сигналов по контактам разъёма FP_USB_2.0_5-6

Вид сигнала	Номер контакта		Вид сигнала
P5V_USB_FP	1	2	P5V_USB_FP
USB2_P11_F_DN	3	4	USB2_P13_F_DN
USB2_P11_F_DP	5	6	USB2_P13_F_DP
GROUND	7	8	GROUND
–	–	10	TP_USB2_FP_10

4.20. Поддержка видео

4.20.1. Разрешение видео

Графический контроллер Aspeed* AST2500 BMC — это VGA-совместимый контроллер с аппаратным ускорением 2D и полной поддержкой мастера шины. При зарезервированных 16 МБ памяти, данный видеоконтроллер может поддерживать разрешения, указанные в таблице 28.

Таблица 28. Поддерживаемые разрешения видео

Разрешение	8 бит/п	16 бит/п	24 бит/п	32 бит/п
640×480	60, 72, 75, 85	60, 72, 75, 85	Не поддерживается	60, 72, 75, 85
800×600	60, 72, 75, 85	60, 72, 75, 85	Не поддерживается	60, 72, 75, 85
1024×768	60, 72, 75, 85	60, 72, 75, 85	Не поддерживается	60, 72, 75, 85
1152×864	75	75	75	75
1280×800	60	60	60	60
1280×1024	60	60	60	60
1440×900	60	60	60	60
1600×1200	60	60	Не поддерживается	Не поддерживается

Разрешение	8 бит/п	16 бит/п	24 бит/п	32 бит/п
1680×1050	60	60	Не поддерживается	Не поддерживается
1920×1080	60	60	Не поддерживается	Не поддерживается
1920×1200	60	60	Не поддерживается	Не поддерживается

4.20.2. Встроенные видеоразъёмы

Серверная плата включает два варианта подключения монитора к серверной системе:

1. Стандартный 15-контактный видеоразъём, расположенный на задней стороне серверной платы (рис. 4-35).
2. На серверной плате рядом с передним правым краем находится разъём A рядом с передним правым краем серверной платы с надписью «FP_VIDEO», который при подключении по кабелю может передавать видео с передней части серверной системы (рис. 4-36).

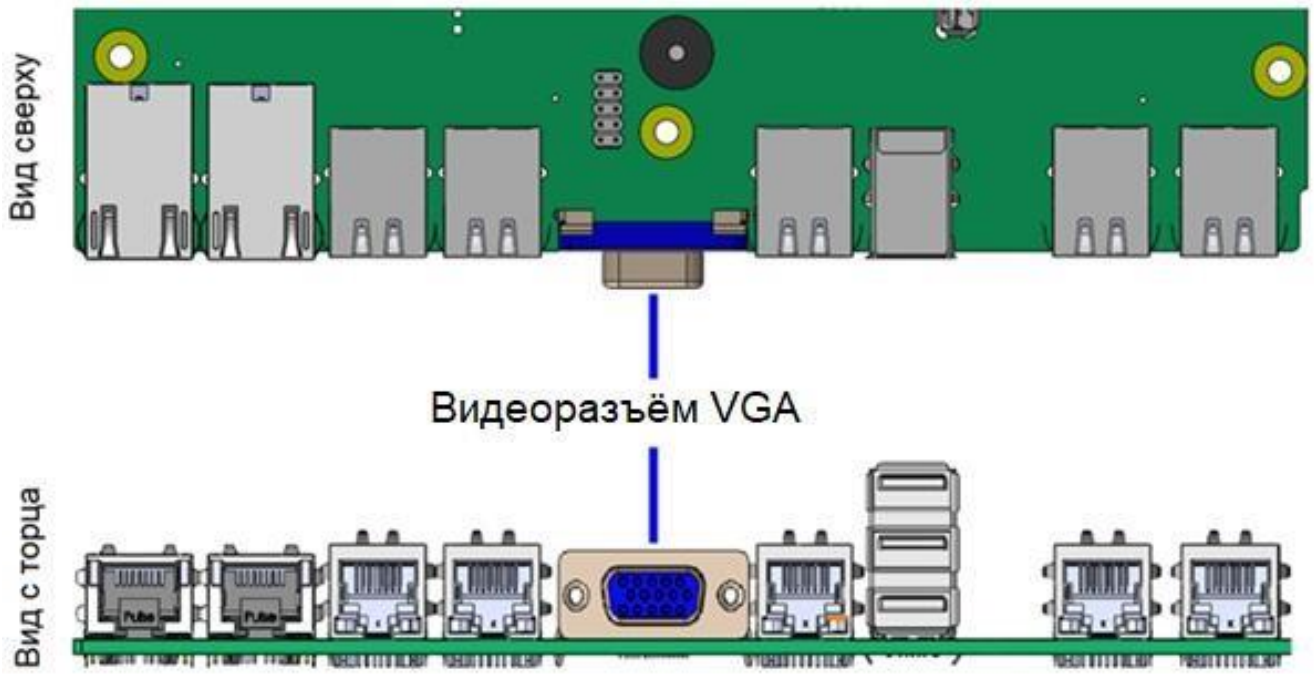


Рисунок 4-35. Стандартный 15-контактный видеоразъём

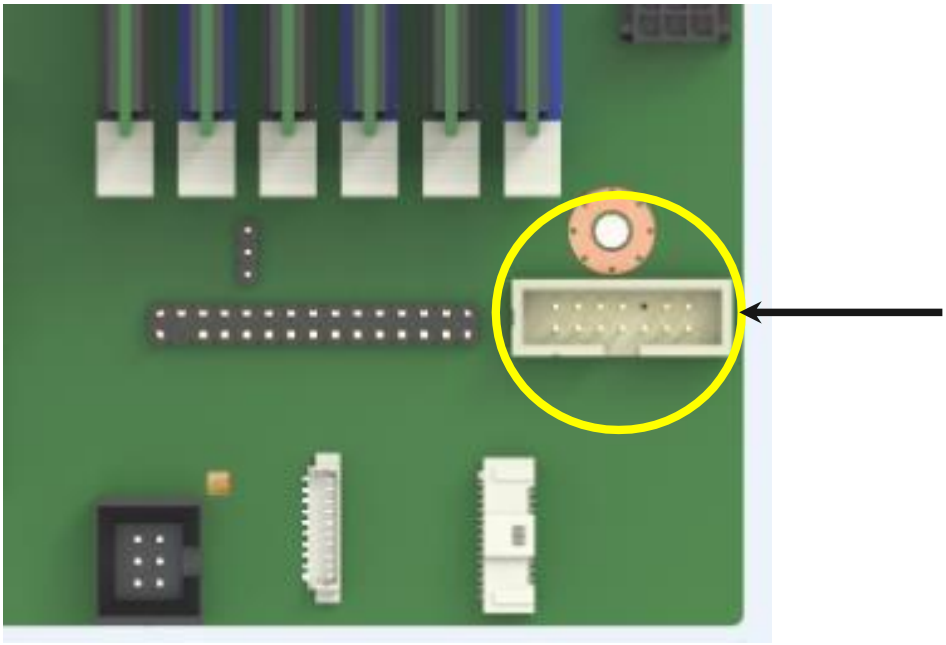


Рисунок 4-36. Расположение разъёма для видео на плате

Когда монитор подключён к передней части системы, видео сзади отключается. В таблице 29 приведена разводка контактов этого разъёма.

Таблица 29. Распиновка видеоразъёма на передней панели ("FP VIDEO")

Вид сигнала	Номер контакта		Вид сигнала
V_IO_FRONT_R_CONN	1	2	GROUND
V_IO_FRONT_G_CONN	3	4	GROUND
V_IO_FRONT_B_CONN	5	6	GROUND
V_BMC_GFX_FRONT_VSYN	7	8	GROUND
V_BMC_GFX_FRONT_HSYN	9	–	KEY
V_BMC_FRONT_DDC_SDA_CONN	11	12	V_FRONT_PRES_N
V_BMC_FRONT_DDC_SCL_CONN	13	14	P5V_VID_CONN_FNT

4.20.3. Поддержка встроенного видео и дополнительного видеоадаптера

Дополнительные видеокарты можно использовать для замены или дополнения встроенной видеоплаты серверной платы. Настройка BIOS включает в себя параметры для поддержки требуемой видеооперации при установке дополнительной видеокарты.

- Если для параметров «Встроенное видео» и «Встроенный видеоадаптер» установлено значение «Включено», оба видеодисплея могут быть активны. Встроенное видео по-прежнему является основной консолью и активно во время прохождения BIOS POST; дополнительный видеоадаптер активен только в среде ОС с поддержкой видеодрайвера.
- Когда встроенное видео включено, а надстройка видеоадаптера отключена, активно только встроенное видео.
- Когда встроенное видео отключено, а дополнительный видеоадаптер включен, активен только дополнительный видеоадаптер.

Конфигурации с дополнительными видеокартами могут быть более сложными с платой с двумя разъёмами ЦП. Некоторые платы с несколькими сокетами имеют слоты PCIe, в которые можно установить дополнительную видеокарту, которая подключена к IIO сокетов ЦП, отличных от сокета ЦП 1. Однако только один сокет ЦП может быть обозначен как устаревший сокет VGA, как это требуется в POST. Для этого существует опция конфигурации PCI Legacy VGA Socket. Правила для этого варианта таковы:

- Параметр «Устаревший разъём VGA» отображается серым цветом и недоступен, если в разъем PCIe, поддерживаемый ЦП 2, не установлена дополнительная видеокарта.
- Поскольку встроенное видео жёстко подключено к разъёму ЦП 1, когда устаревший разъём VGA установлен на разъём ЦП 2, встроенное видео отключается.

4.20.4. Режим двух мониторов

BIOS поддерживает одиночное и двойное видео, если установлены дополнительные видеоадаптеры. Хотя в настройках BIOS нет параметра включения/отключения для двойного видео, он работает, когда включены параметры встроенного видео и дополнительного видеоадаптера.

В режиме одиночного видео в процессе POST определяется встроенный видеоконтроллер или дополнительный видеоадаптер.

В режиме двойного видео встроенный видеоконтроллер включён и является основным видеоустройством, в то время как для дополнительного видеоадаптера выделяются ресурсы, и он рассматривается, как дополнительное видеоустройство в процессе POST. Дополнительный видеоадаптер не будет активен, пока не будет загружена среда операционной системы.

4.21. Контакты встроенных разъёмов

В этом разделе указано расположение и разводка большинства встроенных разъёмов серверной платы:

- все вертикальные слоты;
- разъём модуля OCP*;
- разъём модуля SAS;
- разъёмы твердотельного накопителя M.2;
- слоты DIMM;

- разъёмы процессора.

4.21.1. Разъёмы питания

На серверной плате имеется несколько разъёмов питания, которые используются для подачи питания постоянного тока на различные устройства.

4.21.2. Основное питание

Питание основной серверной платы подается через два разъёма, которые позволяют подключить один или два (один резервный) блока питания непосредственно к серверной плате. Каждый разъём помечен, как «MAIN PWR 1» или «MAIN PWR 2» на серверной плате, как показано на рисунке (выделено жёлтым):

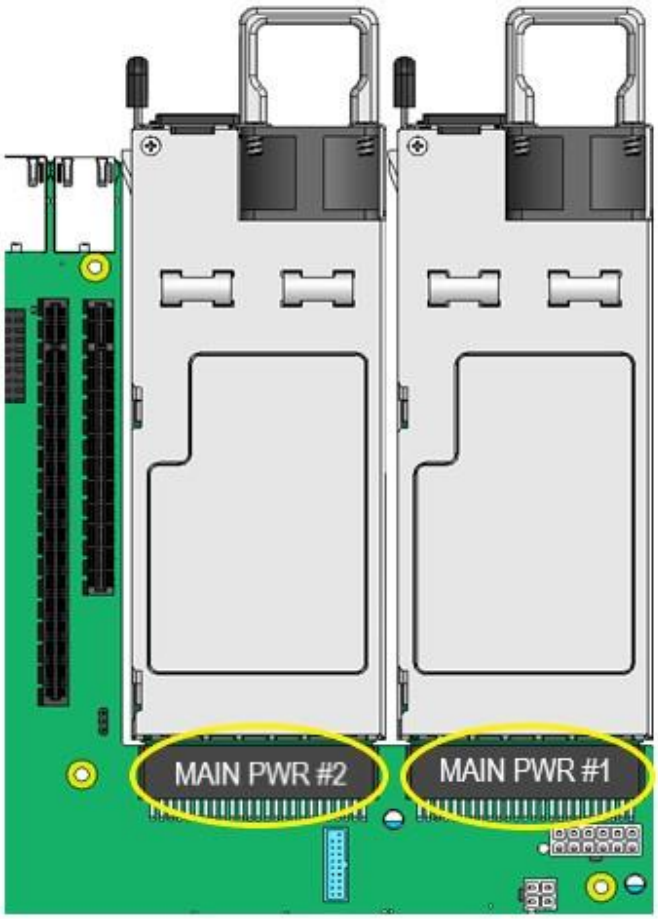


Рисунок 4-37. Разъёмы питания

Серверная плата не поддерживает блоки питания с кабельными жгутами. В конфигурации с резервным блоком питания неисправный модуль блока питания можно заменить в горячем режиме. В таблице 30 приведено расположение выводов разъёма «MAIN PWR 1», а в таблице 31 приведено расположение выводов разъёма «MAIN PWR 2».

Таблица 30. Распиновка разъёма основного питания (слот 1) («MAIN PWR 1»)

Вид сигнала	Номер контакта		Вид сигнала
GROUND	B1	A1	GROUND
GROUND	B2	A2	GROUND
GROUND	B3	A3	GROUND
GROUND	B4	A4	GROUND
GROUND	B5	A5	GROUND
GROUND	B6	A6	GROUND
GROUND	B7	A7	GROUND
GROUND	B8	A8	GROUND
GROUND	B9	A9	GROUND
P12V	B10	A10	P12V
P12V	B11	A11	P12V
P12V	B12	A12	P12V
P12V	B13	A13	P12V
P12V	B14	A14	P12V
P12V	B15	A15	P12V
P12V	B16	A16	P12V
P12V	B17	A17	P12V
P12V	B18	A18	P12V
P3V3_AUX: PD_PS1_FRU_A0	B19	A19	SMB_PMBUS_DATA_R
P3V3_AUX: PD_PS1_FRU_A1	B20	A20	SMB_PMBUS_CLK_R

Вид сигнала	Номер контакта		Вид сигнала
P12V_STBY	B21	A21	FM_PS_EN_PSU_N
FM_PS_CR1	B22	A22	IRQ_SML1_PMBUS_ALERTR2_N
P12V_SHARE	B23	A23	ISENSE_P12V_SENSE_RTN
TP_1_B24	B24	A24	ISENSE_P12V_SENSE
FM_PS_COMPATIBILITY_BUS	B25	A25	PWRGD_PS_PWROK

Таблица 31. Распиновка разъёма основного питания (слот 2) («MAIN PWR 2»)

Вид сигнала	Номер контакта		Вид сигнала
GROUND	B1	A1	GROUND
GROUND	B2	A2	GROUND
GROUND	B3	A3	GROUND
GROUND	B4	A4	GROUND
GROUND	B5	A5	GROUND
GROUND	B6	A6	GROUND
GROUND	B7	A7	GROUND
GROUND	B8	A8	GROUND
GROUND	B9	A9	GROUND
P12V	B10	A10	P12V
P12V	B11	A11	P12V
P12V	B12	A12	P12V
P12V	B13	A13	P12V
P12V	B14	A14	P12V

Вид сигнала	Номер контакта		Вид сигнала
P12V	B15	A15	P12V
P12V	B16	A16	P12V
P12V	B17	A17	P12V
P12V	B18	A18	P12V
P3V3_AUX: PU_PS2FRU_A0	B19	A19	SMB_PMBUS_DATA_R
P3V3_AUX: PD_PS2_FRU_A1	B20	A20	SMB_PMBUS_CLK_R
P12V_STBY	B21	A21	FM_PS_EN_PSU_N
FM_PS_CR1	B22	A22	IRQ_SML1_PMBUS_ALERTR3_N
P12V_SHARE	B23	A23	ISENSE_P12V_SENSE_RTN
TP_2_B24	B24	A24	ISENSE_P12V_SENSE
FM_PS_COMPATIBILITY_BUS	B25	A25	PWRGD_PS_PWROK

4.21.3. Разъём питания объединительной платы с возможностью «горячей» замены

На серверной плате имеется один белый 2×6-контактный разъем питания, который при подключении кабеля обеспечивает питание для объединительных плат с возможностью «горячей» замены. На серверной плате этот разъём обычно помечен как «HSBP PWR». В таблице 32 приведена распиновка данного разъёма, а на рисунке 4-38 указано его месторасположение (выделен красным овалом).

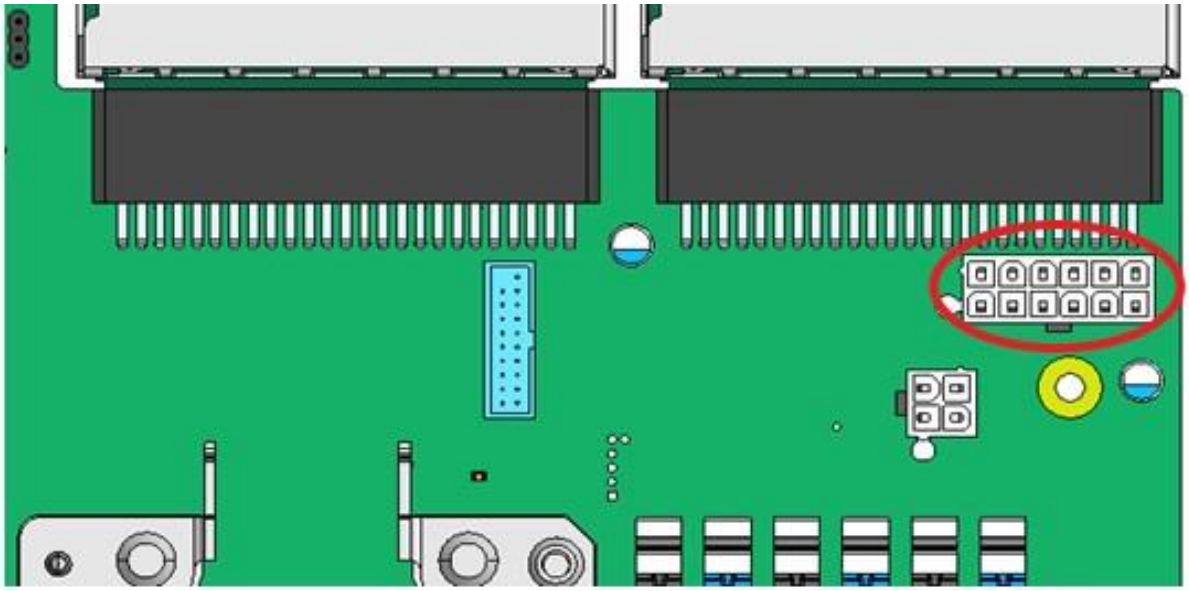


Рисунок 4-38. Расположение разъёма HSBP PWR на плате

Таблица 32. Распиновка разъёма питания объединительной платы «HSBP PWR»

Вид сигнала	Номер контакта		Вид сигнала
GND	1	7	P12V_240VA3
GND	2	8	P12V_240VA3
GND	3	9	P12V_240VA2
GND	4	10	P12V_240VA2
GND	5	11	P12V_240VA1
GND	6	12	P12V_240VA1

4.21.4. Дополнительные разъёмы питания на 12 В для переходной платы

На серверной плате есть два белых 2×2-контактных разъёма питания с маркировкой «OPT_12V_PWR», которые обеспечивают дополнительное питание в 12 В для мощных плат расширения (райзер-карт) PCIe x16 (видео, GPGPU, сопроцессора Intel® Xeon Phi™), требования к питанию которых превышают максимальная мощность 75 Вт, обеспечиваемая разъёмом для райзер-карты. Эти разъёмы выделены жёлтыми кружками на рисунке 4-39, а ниже дана таблица их распиновки.

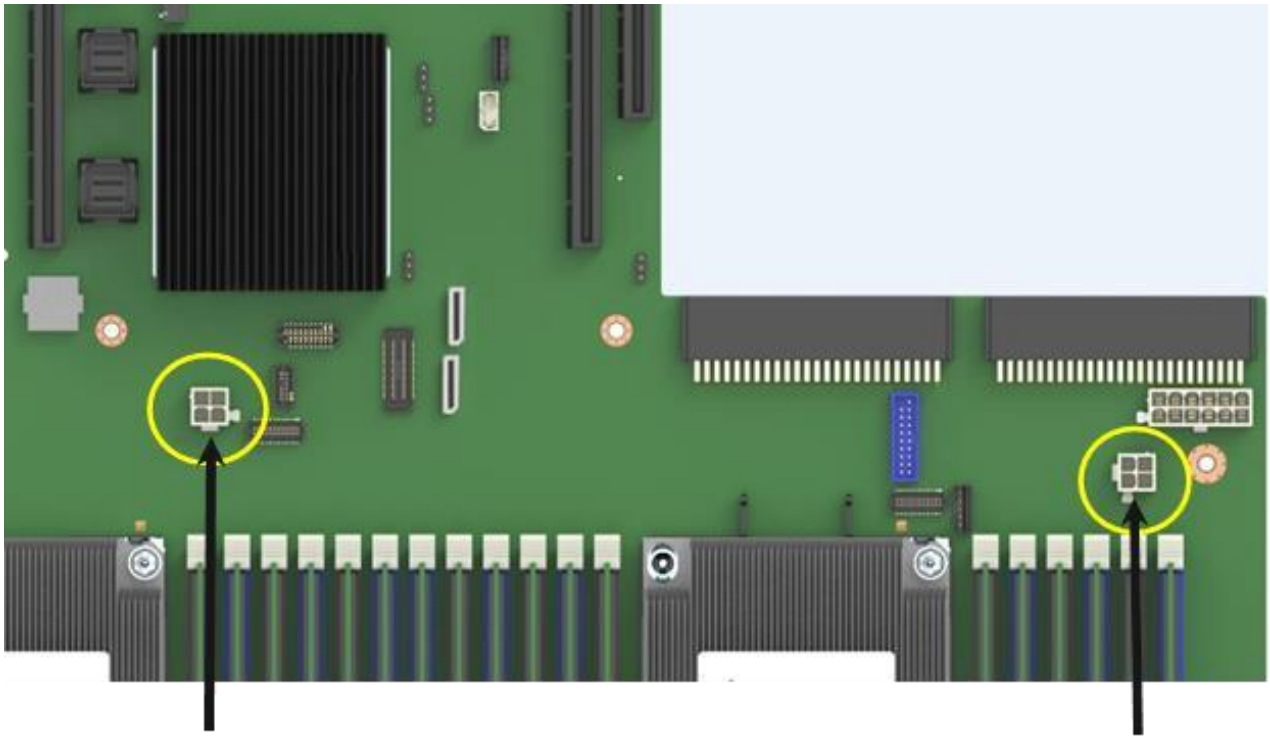


Рисунок 4-39. Расположение разъёмов HSBP PWR на плате

Вид сигнала	Номер контакта		Вид сигнала
P12V	3	1	GROUND
P12V	4	2	GROUND

Кабель от этих разъёмов можно проложить к разъёму питания на данной плате расширения. Максимальная потребляемая мощность для каждого разъёма составляет 225 Вт, но она также ограничена доступной мощностью, обеспечиваемой блоком питания, и общей потребляемой мощностью данной конфигурации системы. Необходимо составить бюджет мощности для всей системы, чтобы определить, какая дополнительная мощность доступна для поддержки любых карт расширения высокой мощности.

В качестве дополнительного оборудования предлагается кабель питания на 12 В (рис. 4-40). Данный кабель может поддерживать как 6-, так и 8-контактные разъёмы питания 12 В AUX, которые можно найти на платах расширения высокой мощности.

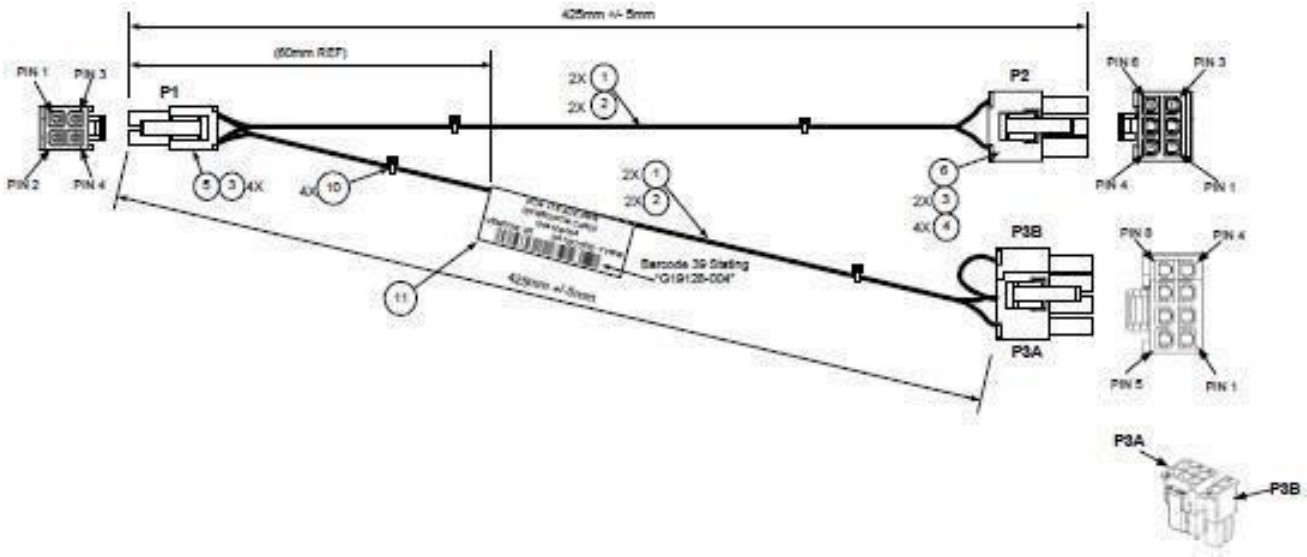


Рисунок 4-40. Дополнительный кабель питания на 12 В

4.22. Маркировка и разъёмы передней панели управления

4.22.1. Обзор светодиодных индикаторов и кнопок управления

Серверная плата включает в себя несколько разъёмов на передней панели управления. В этом разделе представлено функциональное описание и разводка контактов для каждого разъёма.

Для поддержки кнопок управления и светодиодов на передней панели предусмотрено два варианта разъёма: 30-контактный SSI-совместимый разъём с маркировкой «FRONT_PANEL» и специальный 30-контактный разъём высокой плотности с маркировкой «STORAGE_FP», как показано на рисунке 4-41:

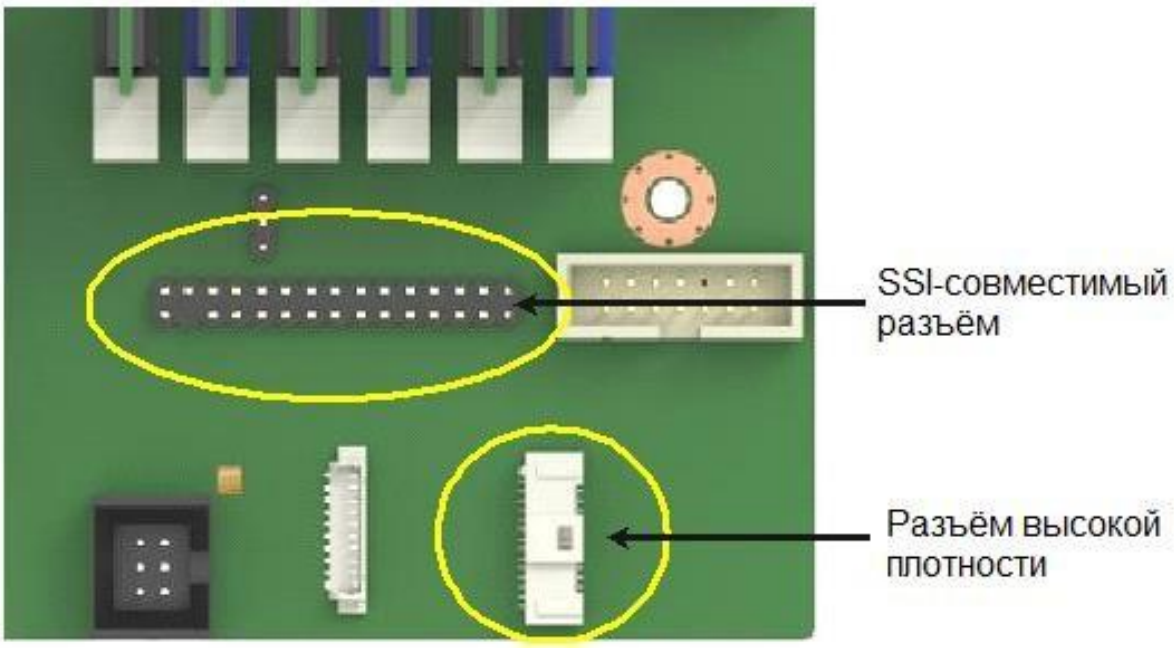


Рисунок 4-41. Варианты разъёмов

На передней панели управления имеются следующие элементы управления:

Рисунок 4-42. Передняя панель управления

1. Кнопка питания.
2. Кнопка идентификации сервера.
3. Кнопка сброса системы (утоплена).
4. Светодиод состояния сервера (зеленый).
5. Светодиод идентификации сервера (синий).
6. Индикатор состояния системы (красный).
7. Индикатор активности устройства хранения (оранжевый).
8. Индикатор сетевой активности системы (2 жёлтых).

Таблица 33. Распиновка обоих типов 30-контактных разъёмов одинакова

Вид сигнала	Номер контакта		Вид сигнала
P3V3_AUX	1	2	P3V3_AUX
KEY	–	4	P5V_STBY
FP_PWR_LED_BUF_R_N	5	6	FP_ID_LED_BUF_R_N
P3V3	7	8	FP_LED_STATUS_GREEN_R_N
LED_HDD_ACTIVITY_R_N	9	10	FP_LED_STATUS_AMBER_R_N
FP_PWR_BTN_N	11	12	LED _NIC_LINK0_ACT_FP_N
GROUND	13	14	LED _NIC_LINK0_LNKUP_FP_N
FP_RST_BTN_R_N	15	16	SMB_SENSOR_3V3STBY_DATA_R0
GROUND	17	18	SMB_SENSOR_3V3STBY_CLK
FP_ID_BTN_R_N	19	20	FP_CHASSIS_INTRUSION
PU_FM_SIO_TEMP_SENSOR	21	22	LED_NIC_LINK1_ACT_FP_N
FP_NMI_BTN_R_N	23	24	LED_NIC_LINK1_LNKUP_FP_N
KEY	–	–	KEY
LED_NIC_LINK2_ACT_FP_N	27	28	LED_NIC_LINK3_ACT_FP_N
LED_NIC_LINK2_LNKUP_FP_N	29	30	LED_NIC_LINK3_LNKUP_FP_N

4.22.2. Функции светодиодных индикаторов и кнопок управления

4.22.2.1. Кнопка и светодиоды питания/спящего режима

Кнопка подачи и выключения питания работает также и как кнопка перехода в спящий режим, если она включена операционной системой, совместимой с ACPI. Нажатие этой кнопки отправляет сигнал на встроенный BMC, который включает или выключает систему. Светодиод питания является одноцветным и может поддерживать различные состояния индикатора (Таблица 34).

Таблица 34. Состояния индикатора

Режим	Индикатор	Питание	Состояние системы
Non-ACPI	Не горит	Нет	Питание системы отключено, а BIOS не инициализировал набор микросхем
	горит	Есть	Система работает
ACPI	Не горит	S5	Прекращена подача питания, операционная система не успела сохранила информации
	горит	S0	Система и операционная система запущены и работают

4.22.2.2. Кнопка идентификатора системы и поддержка светодиодов

Нажатие кнопки системного идентификатора включает светодиодный индикатор идентификации на передней панели и светодиодный индикатор на задней панели серверной платы. Оба светодиода имеют синее свечение. Светодиодная идентификация используется для идентификации системы при эксплуатации сервера в одной стойке с аналогичными серверными системами. Светодиод идентификатора системы также можно включать и выключать удалённо с помощью команды IPMI «Идентификация шасси», которая заставляет светодиод мигать в течение 15 секунд.

4.22.2.3. Кнопка сброса системы

При нажатии на кнопку сброса (**Reset**) происходит перезагрузка и повторная инициализация системы.

4.22.2.4. Поддержка датчика вскрытия NMI

При нажатии кнопки NMI сервер останавливается, а BMC выдает немаскируемое прерывание (NMI) для создания диагностических трассировок и дампов ядра из операционной системы. После того, как BMC сгенерировал NMI, BMC не генерирует другой NMI до тех пор, пока система не будет сброшена или не будет отключено питание. Следующие действия заставляют BMC генерировать импульс NMI:

- Получение команды управления шасси для импульсного диагностического прерывания. Эта команда не приводит к регистрации события в SEL.
- Истечение срока действия сторожевого таймера до истечения времени ожидания с включенным действием NMI/диагностического прерывания до истечения времени ожидания.

Поведение BMC в отношении генерации сигналов NMI и регистрации событий показано в таблице 35:

Таблица 35. Поведение BMC в отношении генерации сигналов NMI и регистрации событий

Причинное событие		**NMI**
	Генерация сигналов	Поддержка регистрации событий датчика прерывания передней панели
Команда управления шасси (импульсное диагностическое прерывание)	X	–
Нажата кнопка диагностического прерывания на передней панели	X	X
Истечение срока действия сторожевого таймера до истечения времени ожидания с действием NMI/диагностического прерывания	X	X

4.22.2.5. Индикатор активности сетевой карты

На передней панели управления имеется светодиодный индикатор активности каждой встроенной сетевой карты. При обнаружении сетевого соединения светодиод горит непрерывно. Светодиод начинает мигать, как только происходит сетевая активность, со скоростью, соответствующей объёму происходящей сетевой активности. Индикаторы в базовой сборке платы выводятся с сетевых портов NIC1 и NIC2.

4.22.2.6. Светодиоды активности устройства хранения

Светодиодный индикатор активности устройства хранения на передней панели указывает на активность накопителя от встроенных контроллеров хранения. На серверной плате также имеется 2-контактный разъём, помеченный как «HDD_Activity», позволяющий подключать дополнительные контроллеры, об активности которых сигнализирует этот же индикатор.

4.22.2.7. Светодиоды состояния системы

Светодиодный индикатор состояния системы — одноцветный (зелёный) светодиод, показывающий текущее состояние серверной системы. У данной серверной платы имеется два таких индикатора: один расположен на передней панели управления, другой расположен на задней кромке серверной платы. Оба светодиода связаны вместе и показывают одинаковое состояние. Состояние индикатора состояния системы управляется встроенной подсистемой управления платформой.

4.23. Разъёмы системного вентилятора

Серверная плата способна поддерживать до шести системных вентиляторов. Каждый системный вентилятор включает пару разъёмов для вентиляторов: 10-контактный разъём для поддержки двухроторного вентилятора с кабелем, обычно используемого в системных конфигурациях 1U; и разъём 2×3-контактный для поддержки одноротороного вентилятора с горячей заменой, обычно используемого в конфигурациях системы 2U. Одновременное

использование обоих типов разъёмов вентиляторов для любой заданной пары системных вентиляторов не поддерживается.

На рисунке 4-43 показана ориентация штырькового 10-ти контактного разъёма двухроторного вентилятора с фиксированным креплением, а в таблице 36 его распиновка:

Рисунок 4-43. Ориентация штырькового 10-ти контактного разъёма двухроторного вентилятора

Таблица 36. Распиновка штырькового 10-ти контактного разъёма двухроторного вентилятора

Вид сигнала	№ контакта
LED_FAN	10
LED_FAN_FAULT	9
SYS FAN PRSNT	8
GROUND	7
GROUND	6
FAN_TACH_#	5
P12V_FAN	4
P12V_FAN	3
FAN PWM	2
FAN_TACH_#+1	1

На следующих рисунке 4-44 и таблице 37 показана ориентация контактов 6-контактного разъёма вентилятора для горячей замены и их распиновка:

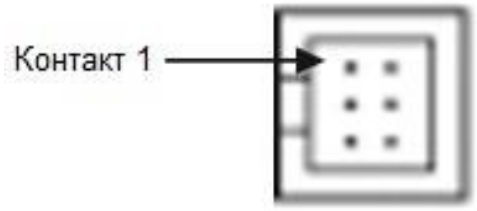


Рисунок 4-44. Ориентация контактов 6-контактного разъёма вентилятора

Таблица 37. Распиновка контактов 6-контактного разъёма вентилятора

Вид сигнала	№ контакта		Вид сигнала
GROUND	1	2	P12V FAN
FAN TACH	3	4	FAN PWM
SYS FAN PRSNT	5	6	LED FAN FAULT

На следующих рисунке 4-45 и таблице 38 показана ориентация контактов 4-контактного разъёма вентилятора для горячей замены и их распиновка:

Таблица 38. Распиновка контактов 4-контактного разъёма вентилятора

Вид сигнала	№ контакта		Вид сигнала
GROUND	1	2	P12V FAN
FAN TACH	3	4	FAN PWM

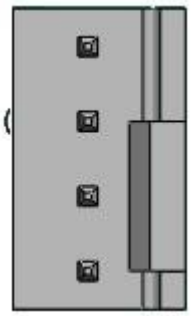


Рисунок 4-45. Ориентация контактов 4-контактного разъёма вентилятора

Каждый разъём контролируется и управляется встроенной системой управления серверной платы. На плате каждая пара разъёмов системного вентилятора помечена «SYS_FAN #», где # принимает значения от 1 до 6.

Расположение каждого разъёма системного вентилятора на серверной плате показано на рисунке 4-46.

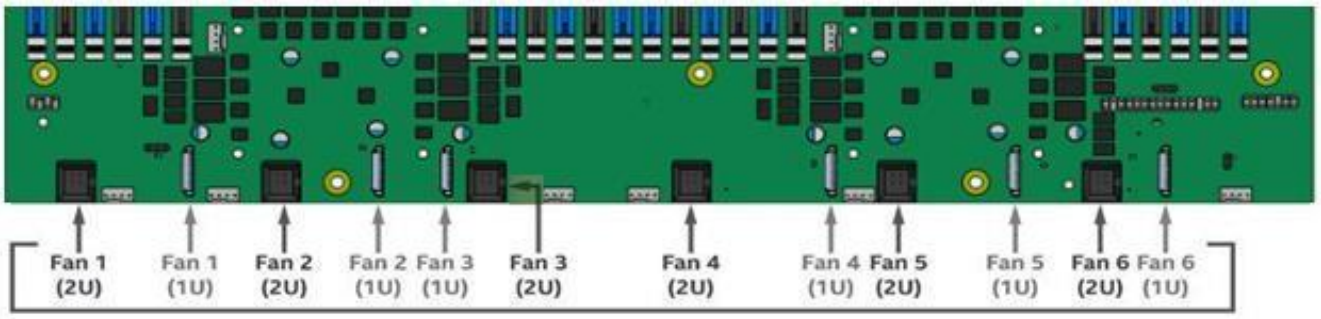


Рисунок 4-46. Расположение каждого разъёма системного вентилятора на серверной плате

4.24. Коннекторы управления

На серверной плате имеется несколько разъёмов интерфейса управления.

Ниже в таблицах 37–39 дана распиновка разъёмов I2C объединительной платы с возможностью горячей замены:

Таблица 39. 3-контактный, SMBUS (J5C3)

№ контакта	Сигнал
1	SDA
2	Ground
3	SCL

Таблица 40. 4-контактный SMBUS (J1K1)

№ контакта	Сигнал
1	SDA
2	Ground
3	SCL
4	RST_PCIE_SSD_PERST

Таблица 41. IPMB – SMBUS 4-контактный (J1C3)

№ контакта	Сигнал
1	CMOS_SDA
2	Ground
3	CMOS_SCL
4	P5V_AUX

На рисунке 4-47 показано их местоположение на плате:

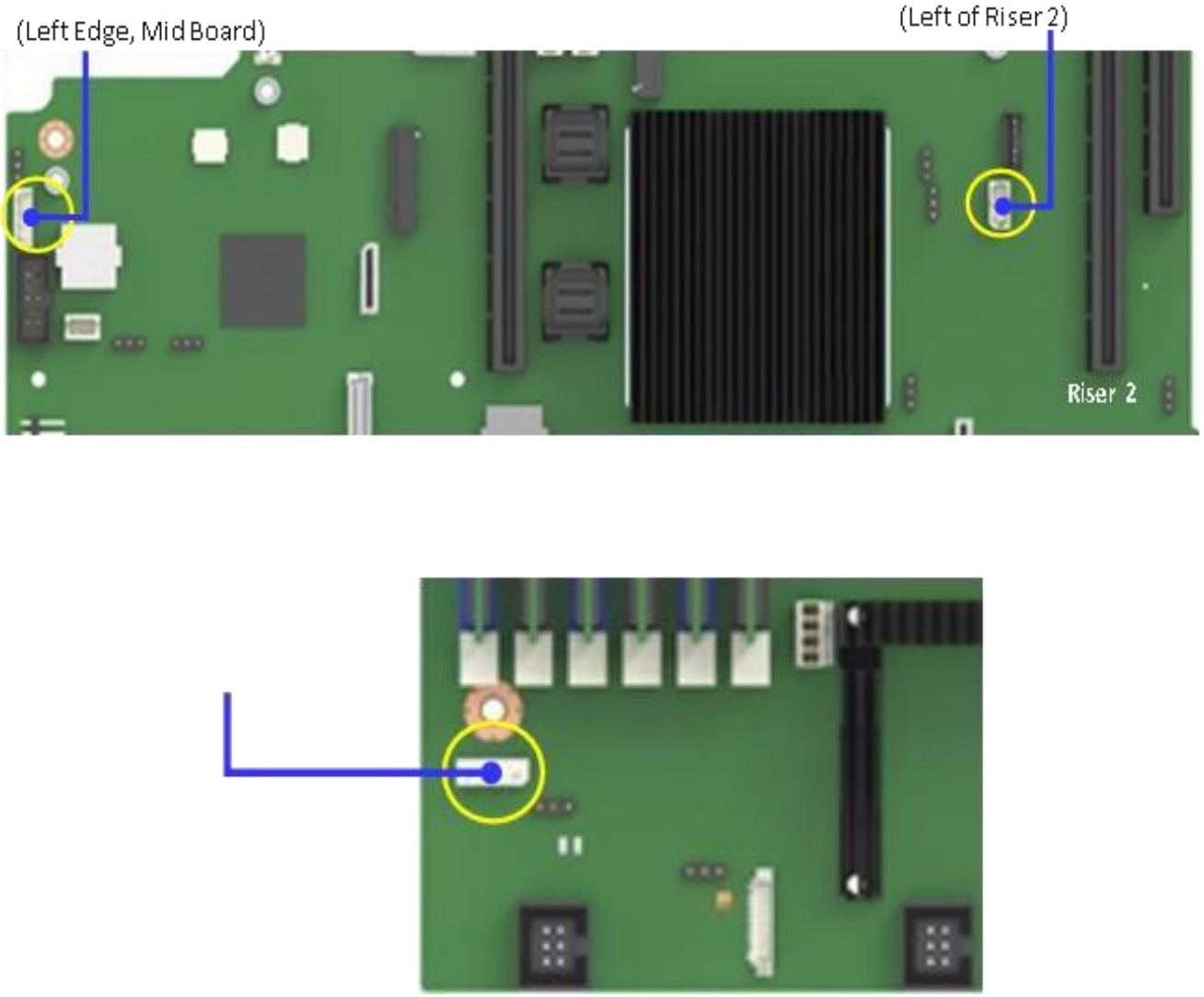


Рисунок 4-47. Местоположение разъёмов I2C объединительной платы

4.25. Базовые и расширенные функции управления

4.25.1. Обзор базовых и расширенных функций

Интегрированный BMC поддерживает базовые и расширенные функции управления сервером. Базовые функции управления доступны по умолчанию. Расширенные функции управления становятся доступными при добавлении дополнительно устанавливаемого ключа. Ключ устанавливается в соединитель, показанный на рисунке ниже (выделено красным):

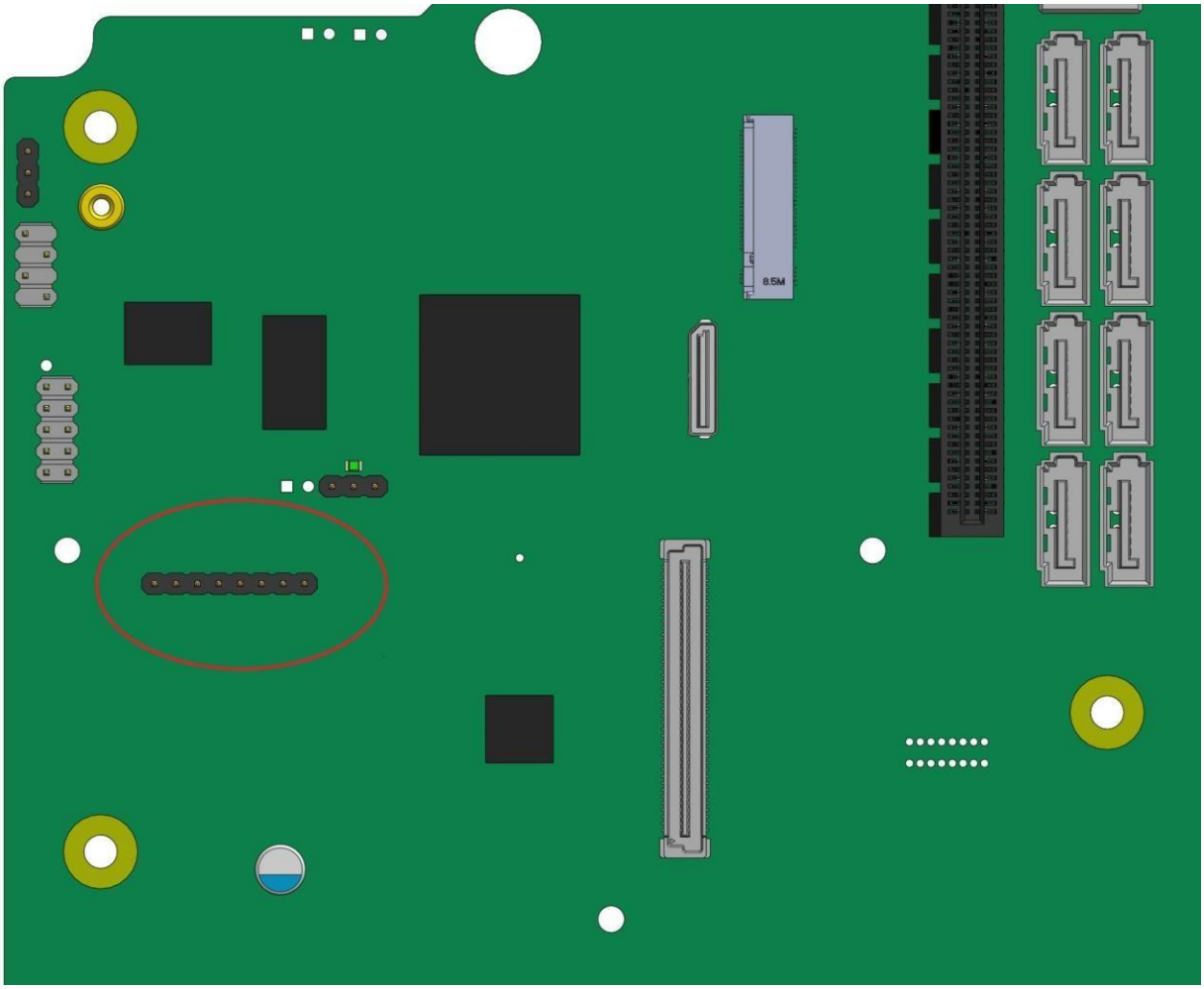


Рисунок 4-48. Соединитель для дополнительно устанавливаемого ключа

По вопросам приобретения ключа обращайтесь к представителю компании QTECH.

Когда прошивка BMC инициализируется, она пытается получить доступ к ключу. Если попытка доступа к ключу успешна, BMC активирует расширенные функции.

В таблице 42 представлен обзор базовых и расширенных функций управления сервером:

Таблица 42. Обзор базовых и расширенных функций управления сервером

Функции	Базовые	Расширенные
Поддержка функций IPMI 2.0	X	X
Внутрисхемное обновление прошивки BMC	X	X
Обнаружение проникновения внутрь корпуса		X
Поддержка бесперебойного питания	X	X
Поддержка ARP/DHCP	X	X
Поддержка терморегулирования PECI	X	X
Оповещение по электронной почте		X
Встроенный веб-сервер	X	X
Поддержка SSH	X	X
Встроенный KVM	X	X
Интегрированное удалённое перенаправление мультимедиа	X	X
Функция удаленного включения/выключения и перезагрузки	X	X
Управление пользователями порта IPMI	X	X
Перенаправление последовательной консоли через LAN (SOL)	X	X

4.26. Выделенный порт управления IPMI

На серверной плате имеется выделенный порт управления 1 GbE RJ-45. Порт управления активен с установленным ключом Intel RMM4 Lite или без него. На рисунке 4-49 ниже показано расположение порта (выделен красным овалом):

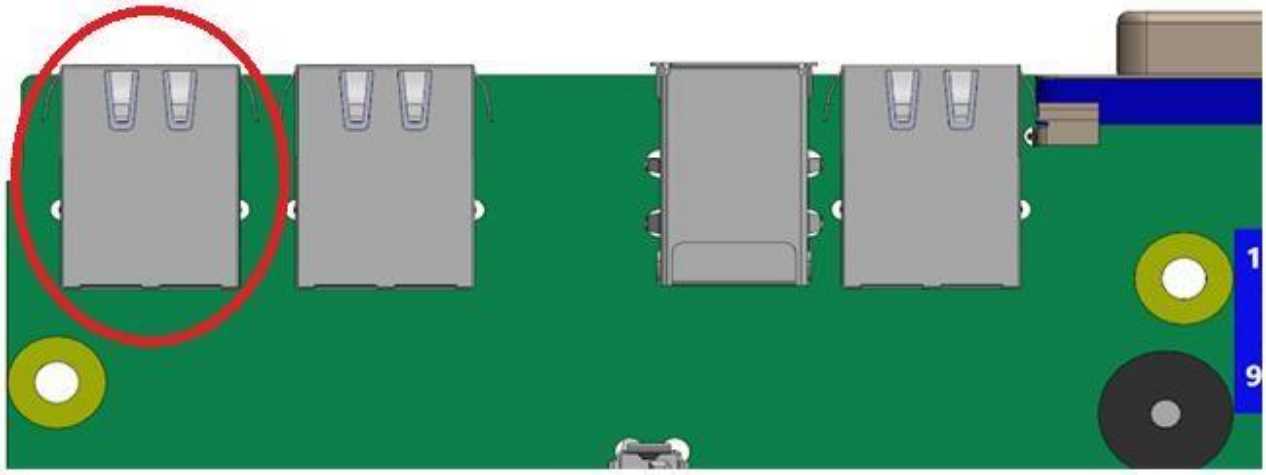


Рисунок 4-49. Выделенный порт управления IPMI

4.27. Встроенный веб-сервер

BMC включают в себя встроенный веб-сервер и настраиваемый веб-интерфейс, который предоставляет возможность управления базовым набором функций BMC. Этот набор поддерживается всеми встроенными сетевыми адаптерами, имеющими подключение управления к BMC, а также дополнительным выделенным сетевым адаптером для управления надстройками. Поддерживается как минимум два одновременных веб-сеанса от двух разных пользователей. Встроенный веб-интерфейс пользователя поддерживает следующие клиентские веб-браузеры:

- Microsoft Internet Explorer*
- Mozilla Firefox*
- Google Chrome*
- Safari*

Встроенный веб-интерфейс пользователя поддерживает надёжную защиту — аутентификацию, шифрование и поддержку брандмауэра – поскольку он позволяет удаленно настраивать сервер и управлять им. Поддерживается шифрование с использованием 128-битного SSL. Аутентификация пользователя основана на идентификаторе пользователя и пароле.

Пользовательский интерфейс, представленный встроенным веб-сервером, аутентифицирует пользователя перед тем, как начать веб-сеанс. В интерфейсе видны все функции для всех пользователей, но те функции, которые запрещены для конкретного пользователя будут неактивны (серого цвета).

веб-интерфейс также предоставляет точку запуска для некоторых расширенных функций, таких как клавиатура, видео, мышь (KVM) и перенаправление мультимедиа. После добавления в меню этих функций, необходимо обновить интерфейс, чтобы данные функции стали активны.

Встроенный веб-сервер отображает выходные данные только на русском или английском языке.

Набор функций веб-интерфейса позволяет выполнять следующее:

- Включить, выключить и перезагрузить сервер, а также просмотреть текущее состояние питания.

- Отображать информацию о версиях BIOS, BMC, ME и SDR.
- Показывать общее состояние системы.
- Отображать конфигурации различных параметров IPMI через LAN как для IPV4, так и для IPV6.
- Отображать конфигурации предупреждений (SNMP и SMTP).
- Отображать информацию об активах системы для продукта, платы и шасси.
- Отображать датчики, принадлежащие BMC (имя, статус, текущее показание, включенные пороговые значения), включая статус датчиков с цветовым кодом.
- Обеспечивать возможность фильтрации датчиков на основе типа датчика (напряжение, температура, вентилятор и источник питания).
- Автоматически обновлять данные датчиков с настраиваемой частотой обновления.
- Предоставлять онлайн-помощь.
- Отображать/очистить SEL (отображение в легком для понимания формате).
- Поддерживать основные стандартные браузеры (Microsoft Internet Explorer* и Mozilla Firefox*).
- Выполнять автоматический тайм-аут сеанса графического интерфейса пользователя после настраиваемого пользователем периода бездействия (по умолчанию этот период составляет 30 минут).
- Обеспечивать встроенную функцию отладки платформы, позволяющую пользователю инициировать «дамп отладки» в файл, который можно отправить в Intel.
- Обеспечить виртуальную лицевую панель с теми же функциями, что и локальная лицевая панель. Отображаемые светодиоды соответствуют текущему состоянию светодиодов на локальной панели. Отображаемые кнопки (например, кнопку питания) можно использовать так же, как и локальные кнопки.
- Отображать данные с датчика Intel ME. Отображаются только датчики, для которых загружены соответствующие SDR.
- Сохранять SEL в файл.
- Принудительно подключать по протоколу HTTPS для большей безопасности. Это обеспечивается параметром конфигурации в пользовательском интерфейсе.
- Отображать информацию о процессоре и памяти, доступную через IPMI, через локальную сеть.
- Устанавливать рациональные режимы питания с помощью Intel® Node Manager (Intel® NM).
- Отображать текущую мощность, потребляемую сервером.
- Просматривать и настраивать параметры VLAN.
- Предупреждать пользователя о том, что изменение конфигурации IP-адреса приводит к отключению.
- Блокировать входы в систему на определенный период времени после нескольких неудачных попыток входа подряд. Период блокировки и количество неудачных входов в систему, которое инициирует период блокировки, настраиваются пользователем.
- Принудительно входить в настройки BIOS при перезагрузке (управление питанием сервера).

- Указывать последовательность самотестирования системы при включении питания (POST) для двух предыдущих циклов загрузки, включая временные метки. Временные метки могут отображаться как время относительно начала POST или предыдущего кода POST.
- Предоставлять возможность настраивать номера портов, используемых для SMASH, HTTP, HTTPS, KVM, защищённого KVM, удалённых носителей и защищённых удалённых носителей.

4.28. Набор функций управления

4.28.1. Клавиатура, видео, мышь (KVM) перенаправление

Встроенная программа BMC поддерживает перенаправление клавиатуры, видео и мыши (KVM) по локальной сети. Эта функция доступна удалённо со встроенного веб-сервера в виде апплета Java*. Эта функция доступна только при наличии Intel® RMM4 Lite. В клиентской системе должна быть установлена среда выполнения Java (JRE) версии 6.0 или более поздней, чтобы запускать KVM или приложения для перенаправления мультимедиа.

BMC поддерживает встроенное приложение KVM (удалённая консоль), которое можно запустить с удалённой консоли с помощью встроенного веб-сервера. Поддерживается перенаправление мыши и клавиатуры на базе USB1.1 или USB2.0. Также можно использовать сеанс перенаправления KVM (KVM-r) одновременно с перенаправлением мультимедиа (media-r). Эта функция позволяет пользователю в интерактивном режиме использовать функции клавиатуры, видео и мыши на удалённом сервере, как если бы пользователь физически находился на управляемом сервере. Консоль перенаправления KVM поддерживает следующие раскладки клавиатуры: английский, голландский, французский, немецкий, итальянский, русский и испанский.

Перенаправление KVM включает в себя функцию программной клавиатуры. Виртуальная клавиатура используется для имитации всей клавиатуры, подключённой к удалённой системе. Программная клавиатура поддерживает следующие раскладки: английская, голландская, французская, немецкая, итальянская, русская и испанская.

Функция перенаправления KVM автоматически определяет разрешение видео для наилучшего захвата экрана и обеспечивает высокопроизводительное отслеживание и синхронизацию мыши. Он позволяет удалённо просматривать и настраивать предзагрузочную процедуру POST и настройку BIOS после того, как BIOS инициализирует видео.

Другие атрибуты этой функции включают в себя:

- шифрование перенаправленного экрана, клавиатуры и мыши;
- сжатие перенаправленного экрана;
- возможность выбора конфигурации мыши в зависимости от типа ОС;
- поддержка определяемых пользователем макросов клавиатуры.

Функция перенаправления KVM поддерживает следующие разрешения и частоты обновления:

- 640×480 при 60 Гц, 72 Гц, 75 Гц, 85 Гц;
- 800×600 при 60 Гц, 72 Гц, 75 Гц, 85 Гц;
- 1024×768 при 60 Гц, 72 Гц, 75 Гц, 85 Гц;
- 1152×864 при 75 Гц;
- 1280×800 при 60 Гц;

- 1280×1024 при 60 Гц;
- 1440×900 при 60 Гц;
- 1600×1200 при 60 Гц.

4.28.1.1. Доступность

Удалённый сеанс KVM доступен, даже когда сервер выключен (в режиме ожидания). Во время перезагрузки сервера или включения/выключения питания не требуется перезапуск удаленного сеанса KVM. Сброс BMC, например, из-за сброса, инициированного сторожевым устройством BMC, или сброса BMC после обновления микропрограммы BMC, требует переустановки сеанса.

Сеансы KVM сохраняются при перезагрузке системы, но не при отключении питания.

4.28.1.2. Применение

При включении сервера удаленный сеанс KVM отображает весь процесс загрузки BIOS. Пользователь может взаимодействовать с настройкой BIOS, изменять и сохранять настройки, а также входить и взаимодействовать с экранами конфигурации дополнительного ПЗУ.

4.28.1.3. Принудительный вход в настройки BIOS

Перенаправление KVM может предоставить возможность принудительного входа в настройку BIOS. Это позволяет системе войти в настройки BIOS во время загрузки, что часто пропускается, когда удаленная консоль перенаправляет видео.

4.28.2. Перенаправление мультимедиа

Встроенный веб-сервер предоставляет приложение на языке Java для включения удалённого перенаправления мультимедиа. Его можно использовать в сочетании с функцией удалённого KVM или как отдельный инструмент.

Функция перенаправления мультимедиа предназначена для того, чтобы позволить системным администраторам или пользователям подключать удалённую среду IDE или USB CD-ROM, дисковод гибких дисков или флеш-диск USB в качестве удаленного устройства к серверу. После подключения удалённое устройство отображается на сервере точно так же, как и локальное устройство, что позволяет системным администраторам или пользователям устанавливать программное обеспечение (включая операционные системы), копировать файлы, обновлять BIOS или загружать сервер с этого устройства.

В следующем списке описаны дополнительные возможности и функции перенаправления мультимедиа:

- Работа удалённо установленных устройств не зависит от локальных устройств на сервере. И удалённые, и локальные устройства можно использовать параллельно.
- В качестве удалённого устройства к серверу можно подключить устройства IDE (CD-ROM, дискеты) или USB.
- Возможна загрузка всех поддерживаемых операционных систем с удалённо подключённого устройства, а также загрузка с ОБРАЗА диска (*.IMG) и ISO-файлов CD-ROM или DVD-ROM.
- Перенаправление мультимедиа поддерживает одновременное перенаправление как для виртуального компакт-диска, так и для виртуального гибкого диска/устройства USB. Устройство компакт-диска может быть либо локальным дисководом компакт-дисков, либо файлом образа ISO; Дискета/USB-устройство может быть либо локальным дисководом, либо локальным USB-устройством, либо файлом образа диска.

- Сеанс удалённого мультимедиа сохраняется, даже когда сервер выключен (в режиме ожидания). Во время перезагрузки сервера или включения/выключения питания перезапуск сеанса удаленного носителя не требуется. Сброс BMC (например, из-за сброса BMC после обновления BMC FW) требует повторного установления сеанса.
- Подключенное устройство видно (и может использоваться) ОС и BIOS управляемой системы как в предзагрузочном, так и в послезагрузочном состоянии.
- Подключенное устройство отображается в порядке загрузки BIOS, и можно изменить порядок загрузки BIOS для загрузки с этого удаленного устройства.
- Можно установить операционную систему на «голый» сервер (без операционной системы) с помощью удаленно подключенного устройства. Это также может потребовать использования KVM-r для настройки ОС во время установки.

USB-накопители отображаются как гибкие диски при перенаправлении мультимедиа. Это позволяет устанавливать драйверы устройств во время установки ОС.

Если во время загрузки системы удалённо подключена виртуальная среда IDE или виртуальная дискета, то они представляются как загрузочные устройства. Невозможно представить в системном BIOS только одиночный тип устройства.

Время бездействия по умолчанию составляет 30 минут и не настраивается пользователем. Сеансы перенаправления мультимедиа сохраняются при сбросе системы, но не при отключении питания переменного тока или сбросе BMC.

4.28.3. Удалённая консоль

Удалённая консоль представляет собой рабочее место оператора: монитор, клавиатуру и мышь, информация с сервера на которое передаётся средствами интернета или по локальной сети. Для того, чтобы установить такую связь с сервером, браузер удалённой консоли должен включить подключаемый модуль Java* Runtime Environment (JRE). Если браузер не поддерживает Java, например, с небольшим карманным устройством, пользователь может поддерживать удалённую хост-систему, используя формы администрирования, отображаемые браузером.

ПО удалённой консоли представляет собой приложение на языке Java, которое устанавливает TCP-соединения с BMC. Для этих подключений используется не стандартный протокол типа HTTP или HTTPS, а уникальный протокол для KVM. Этот протокол использует порты #7578 для KVM, #5120 для перенаправления носителей CDROM и #5123 для перенаправления гибких дисков и USB-носителей.

Когда шифрование включено, протокол использует порты #7582 для KVM, #5124 для перенаправления носителей CD-ROM и #5127 для перенаправления носителей с гибких дисков и USB. Локальная сетевая среда должна разрешать эти подключения; это брандмауэр, и, в случае частной внутренней сети, параметры преобразования сетевых адресов (NAT) должны быть настроены соответствующим образом.

4.28.4. Производительность

Изображение на удалённом экране в точности повторяет изображение на экране сервера. Встроенное ПО экрана адаптируется к изменениям разрешения видео на локальном мониторе и удалённый экран продолжает работать плавно, когда система переходит от графики к тексту или наоборот. Небольшая задержка отклика возможна и зависит от пропускной способности и задержкам в сети.

Включение KVM и/или шифрования мультимедиа снижает производительность. Включение сжатия видео обеспечивает самый быстрый отклик, а отключение сжатия обеспечивает лучшее качество видео. Для наилучшей производительности KVM

рекомендуется канал со скоростью 2 Мбит/с или выше. Перенаправление KVM по IP выполняется параллельно с локальным KVM, не влияя на работу локального KVM.

5. ПОДДЕРЖКА ПРОЦЕССОРА

Материнская плата включает два разъема для процессоров Socket-P0 LGA3647-0, совместимых с семейством процессоров Intel® Xeon® с максимальной расчетной тепловой мощностью (TDP) 205 Вт. Посетите https://ftp.qtech.ru/Servers%20and%20Storage/Server/, чтобы получить полный список поддерживаемых процессоров.

ПРИМЕЧАНИЕ: процессоры Intel® Xeon® предыдущего поколения не поддерживаются серверными платами, описанными в этом документе.

5.1. Модуль радиатора процессора (PHM) и сборка процессорного разъема

Каждый блок процессорного разъема на материнской плате находится в предварительно собранном состоянии и включает в себя заднюю пластину (Backplate), LGA3647-0 процессорный сокет и опорную плату (Bolster plate). Рисунок 5-1 идентифицирует каждый из компонентов суб-сборки.

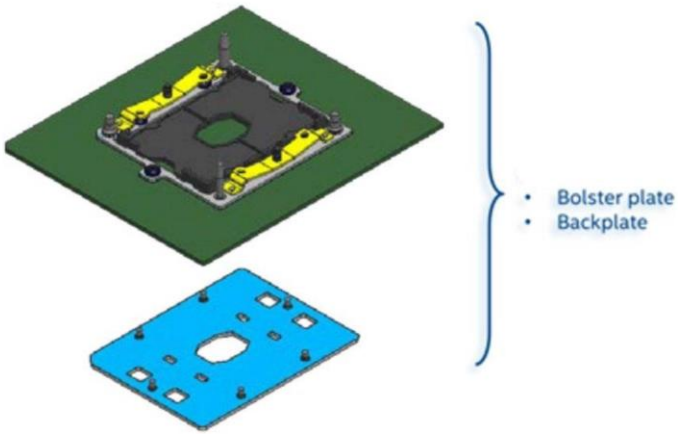


Рисунок 5-1. Сборка процессорного разъема

Серверные платы без установленных процессоров имеют пластиковую защитную крышку от пыли, установленную на каждом блоке процессорного разъема. Перед установкой процессора необходимо осторожно снять защитные крышки (Рисунок 5-2).

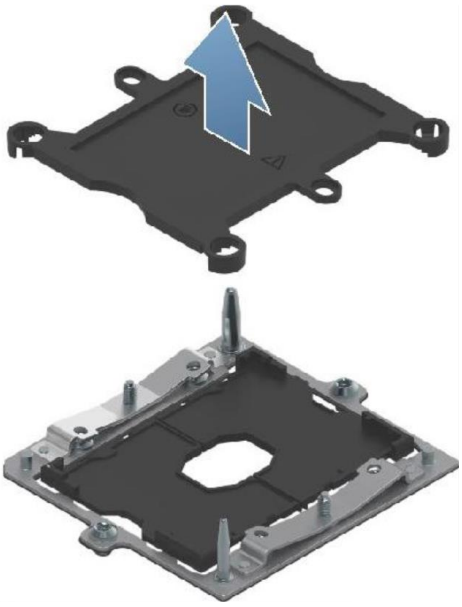


Рисунок 5-2. Узел процессорного гнезда и защитная крышка

Материнская плата этого поколения представляет концепцию модуля теплоотвода процессора (PHM) (Рисунок 5-3, Рисунок 5-4, Рисунок 5-5).

Перед установкой процессора на материнскую плату к нему необходимо прикрепить радиатор.

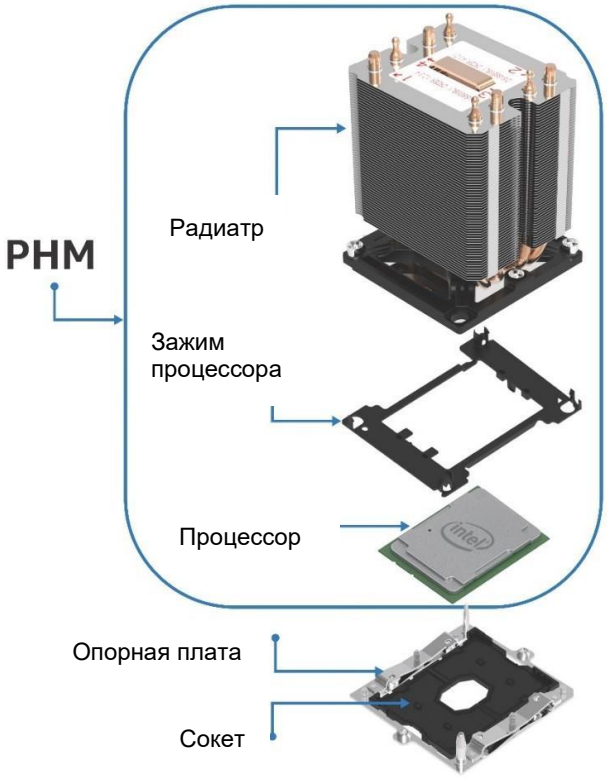


Рисунок 5-3. Компоненты модуля радиатора процессора (PHM) и справочная схема разъема процессора

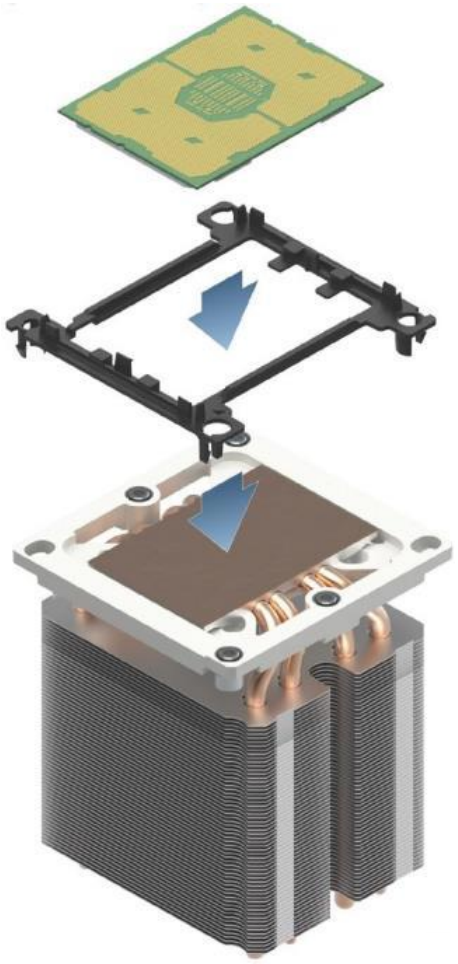


Рисунок 5-4. Сборочный узел модуля радиатора процессора (PHM)

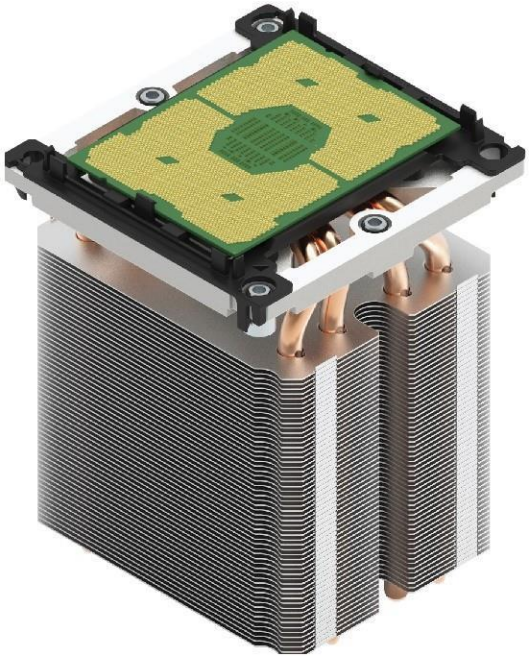


Рисунок 5-5. Полностью собранный модуль радиатора процессора (PHM)

5.2. Поддержка расчетной тепловой мощности процессора (TDP)

Для того, чтобы разрешить оптимальную работу и обеспечить наилучшую долгосрочную надежность в системах на базе процессоров Intel, процессор должен оставаться в пределах определенной спецификацией минимальной и максимальной температуры корпуса (TCASE). Температурные решения, не обеспечивающие достаточный теплоотвод могут повлиять на долгосрочную надежность процессоров и системы в целом. Материнская плата описаная в этом документе разработана для поддержки масштабируемого семейства процессоров Intel® Xeon® мощностью до 205 Вт включительно.

ПРИМЕЧАНИЕ ОБ ОТКАЗЕ ОТ ОТВЕТСТВЕННОСТИ: серверные платы содержат ряд компонентов для высокоплотной очень крупномасштабной интеграции (VLSI) и компонентов питания, для охлаждения которых требуется достаточный воздушный поток. Благодаря собственной разработке и тестированию корпусов QTECH гарантирует, что при совместном использовании серверных блоков QTECH полностью интегрированная система удовлетворяет предполагаемым тепловым требованиям этих компонентов. Системные интеграторы, решившие не использовать серверные блоки, разработанные QTECH, должны проконсультироваться с техническими описаниями поставщиков и рабочими параметрами, чтобы определить объем воздушного потока, необходимый для их конкретных приложений и условий окружающей среды. Компания QTECH не может нести ответственность, если компоненты вышли из строя или материнская плата не работает должным образом при использовании вне каких-либо опубликованных рабочих или нерабочих ограничений.

5.3. Обзор семейства процессоров Intel® Xeon® Scalable

Серверная материнская плата поддерживает семейство процессоров Intel® Xeon® Scalable 1-го и 2-го поколения, как показано ниже:

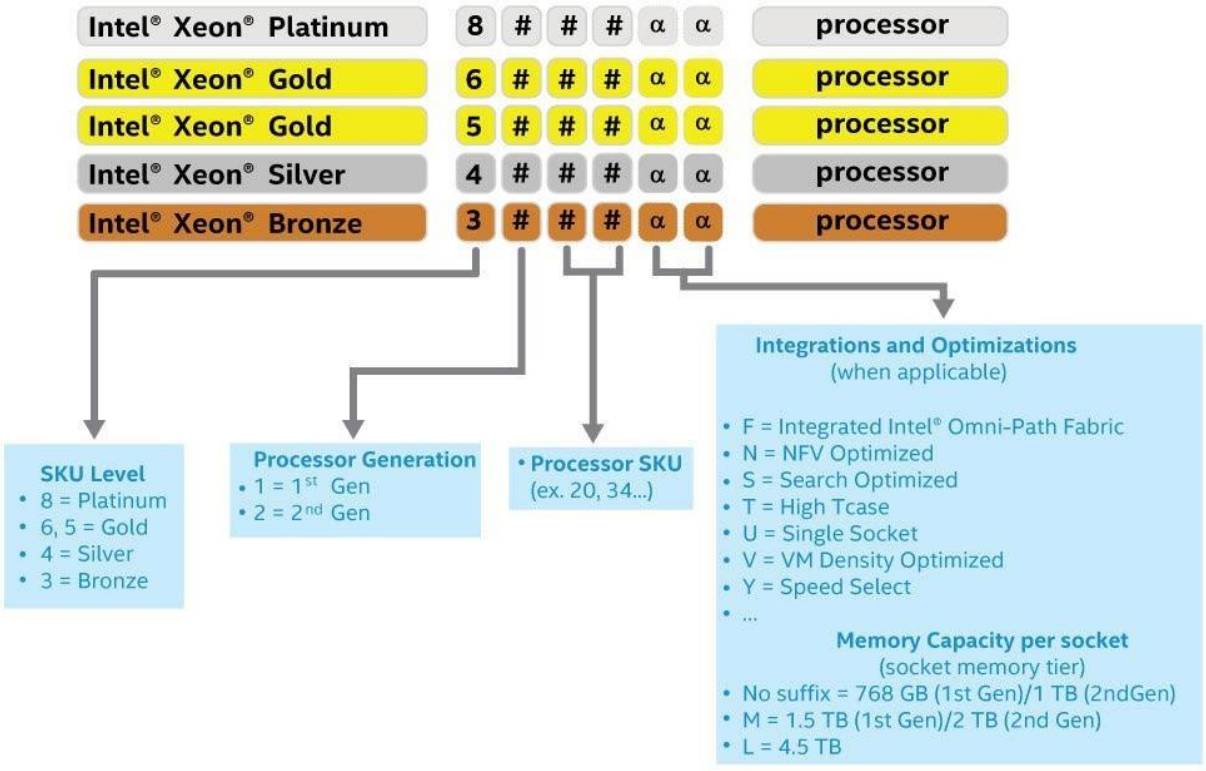


Рисунок 5-6. Идентификация процессора Intel® Xeon®

Таблица 43. Сравнение функций семейства процессоров Intel® Xeon® Scalable 1-го поколения

Особенность	Platunum 81xx	Gold 61xx	Gold 51xx	Silver 41xx	Bronze 31xx
Количество ссылок Intel® UPI	3	3	2	2	2
Intel UPI Скорость	10,4 ГТ/с	10,4 ГТ/с	10,4 ГТ/с	9,6 ГТ/с	9,6 ГТ/с
Поддерживаемые топологии	2C-2 UPI 2C-3 UPI 4C-2 UPI 4C-3 UPI 8C- 3 UPI	2C-2 UPI 2C-3 UPI 4C-2 UPI 4C-3 UPI	2C-2 UPI 4C-2 UPI	2C-2 UPI	2C-2 UPI
Поддержка контроллера узла	Да	Да	Нет	Нет	Нет
Количество каналов памяти	6	6	6	6	6
Макс. скорость DDR4	2666	2666	2400	2400	2133
Емкость памяти	768 ГБ 1,5 ТБ (выбрать SKUs)	768 ГБ 1,5 ТБ (выбрать SKUs)	768 ГБ 1,5 ТБ (выбрать SKUs)	768 ГБ	768 ГБ
Возможности RAS	Продвинутый	Продвинутый	Продвинутый	Стандарт	Стандарт
Технология Intel® Turbo Boost	Да	Да	Да	Да	Нет
Технология Intel® HT	Да	Да	Да	Да	Нет
Поддержка Intel® AVX-512 ISA	Да	Да	Да	Да	Да
Intel® AVX-512 - количество модулей FMA 512b	2	2	1	1	1

Особенность	Platunum 81xx	Gold 61xx	Gold 51xx	Silver 41xx	Bronze 31xx
Количество линий PCIe*	48	48	48	48	48

Таблица 44. Сравнение функций семейства процессоров Intel® Xeon® Scalable 2-го поколения

Особенность	82xx Platinum	62xx Gold	52xx Gold	42xx Silver	32xx Bronze
Количество ссылок Intel® UPI	3	3	2	2	2
Скорость UPI	10,4 ГТ/с	10,4 ГТ/с	10,4 ГТ/с	9,6 ГТ/с	9,6 ГТ/с
Поддержи-ваемые топологии	2C-2 UPI 2C-3 UPI 4C-2 UPI 4C-3 UPI 8C-3 UPI	2C-2 UPI 2C-3 UPI 4C-2 UPI 4C-3 UPI	2C-2 UPI 4C-2 UPI	2C-2 UPI	2C-2 UPI
Поддержка контроллера узла	Да	Да	Нет	Нет	Нет
Количество каналов памяти	6	6	6	6	6
Максимальная скорость DDR4 1DPC	2933	2933	2666	2400	2133
Максимальная скорость DDR4 2DPC	2666	2666	2666	2400	2133
Емкость памяти	1 ТБ 2 ТБ (выбрать SKUs) 4,5 ТБ (выбрать SKUs)	1 ТБ 2 ТБ (выбрать SKUs) 4,5 ТБ (выбрать SKUs)	1 ТБ 2 ТБ (выбрать SKUs) 4,5 ТБ (выбрать SKUs)	1 ТБ	1 ТБ

Особенность	82xx Platinum	62xx Gold	52xx Gold	42xx Silver	32xx Bronze
Возможности RAS	Расширенные	Расширенные	Расширенные	Стандартные	Стандартные
Intel® Turbo Boost Технология	Да	Да	Да	Да	Нет
Intel® Hyper-Threading Технология	Да	Да	Да	Да	Нет
Поддержка Intel® AVX-512 ISA	Да	Да	Да	Да	Да
Intel® AVX-512 – количество 512b FMA юнитов	2	2	1	1	1
VNNI	Да	Да	Да	Да	Да
Количество линий PCIe	48	48	48	48	48

Семейство процессоров Intel® Xeon® Scalable 1-го и 2-го поколения объединяют несколько ключевых компонентов системы в один процессорный пакет, включая ядра ЦП, интегрированный контроллер памяти (IMC) и интегрированный модуль ввода-вывода (IIO). Процессор включает в себя множество основных и неосновных функций и технологий, описанных в следующих разделах.

Особенности ядра:

- Intel® Ultra Path Interconnect (Intel® UPI) — до 10,4 ГТ/с
- Технология Intel® Speed Shift
- Архитектура Intel® x64
- Усовершенствованная технология Intel SpeedStep®
- Технология Intel® Turbo Boost 2.0
- Технология Intel® Hyper-Threading (технология Intel® HT)
- Технология виртуализации Intel® для IA-32, Intel® x64 и архитектуры Intel® (Intel® VT-x)
- Технология виртуализации Intel® для прямого ввода-вывода (Intel® VT-d)
- Выполнять бит отключения
- Технология Intel® Trusted Execution (Intel® TXT)
- Intel® Advanced Vector Extensions 512 (Intel® AVX-512)
- Новые инструкции Intel® Advanced Encryption Standard (Intel® AES-NI)

Дополнительные особенности ядра Intel® Xeon® 2-го поколения:

- Intel® Deep Learning Boost через VNNI
- Технология Intel® Speed Select (выбрать SKUs)
- Технология Intel® Resource Director

Особенности вне ядра:

- До 48 линий PCIe* 3.0 на процессор — двунаправленный конвейер 79 ГБ/с
- Поддерживается 6 каналов памяти DDR4 на процессор
- Интерфейс DMI3/PCIe 3.0 с максимальной скоростью передачи 8,0 ГБ/с
- Усовершенствования непрозрачного моста (Non-Transparent Bridge, NTB) — три полно дуплексных NTBs и 32 MSI-X вектора
- Intel® Volume Management Device (Intel® VMD) — управляет подключенными к ЦП NVM Express * (NVMe*) твердотельными дисками (SSD)
- Технология Intel® Quick Data
- Поддержка Intel® Node Manager 4.0

5.3.1. Архитектура набора команд Intel® x64 (ISA)

Архитектура Intel® x64 — это 64-разрядное расширение памяти для архитектуры IA-32. Дополнительные сведения об архитектуре Intel x64 и модели программирования можно найти на http://developer.intel.com/technology/intel64/.

5.3.2. Технология Intel® Hyper-Threading

Процессор поддерживает технологию Intel® Hyper-Threading (Intel® HT), которая позволяет исполняющему ядру функционировать как два логических процессора. Хотя некоторые исполнительные ресурсы, такие как кеши, единицы исполнения и шины являются общими, каждый логический процессор имеет свое собственное архитектурное состояние с его собственным набором регистров общего назначения и контрольными регистрами. Эта функция должна быть включена через BIOS и требует поддержки операционной системы.

5.3.3. Улучшенная технология Intel SpeedStep®

Процессоры масштабируемого семейства Intel® Xeon® 1-го и 2-го поколения поддерживают улучшенную технологию Intel SpeedStep®. Процессоры поддерживают несколько состояний производительности, что позволяет системе динамически регулировать напряжение процессора и частоту ядра по мере необходимости для снижения энергопотребления и тепловыделения. Все элементы управления для перехода между состояниями централизованы внутри процессора, что позволяет увеличить частоту переходов для более эффективной работы.

Функцию Enhanced Intel SpeedStep Technology можно включать и отключать с помощью параметра на экране настройки конфигурации процессора. По умолчанию технология Enhanced Intel SpeedStep включена. Если этот параметр отключен, скорость процессора устанавливается равной максимальной частоте ядра процессора TDP (номинальная частота).

5.3.4. Технология Intel® Turbo Boost 2.0

Технология Intel® Turbo Boost присутствует во всех процессорах семейства Scalable Intel® Xeon® 1-го и 2-го поколений. Технология Intel Turbo Boost автоматически и автоматически позволяет процессору работать быстрее, чем отмеченная частота, если процессор работает ниже предельных значений мощности, температуры и тока. Это приводит к

повышению производительности как для многопоточных, так и для однопоточных рабочих нагрузок.

5.3.5. Технология виртуализации Intel® для IA-32, Intel® 64 и архитектуры Intel® VT-x

Технология виртуализации Intel® для IA-32, Intel® 64 и архитектуры Intel® (Intel® VT-x) обеспечивает аппаратную поддержку в ядре для повышения производительности и надежности виртуализации. Спецификации Intel VT-x и функциональные описания включены в Руководство разработчика программного обеспечения для архитектур Intel® 64 и IA-32.

5.3.6. Технология виртуализации Intel® для направленного ввода-вывода (Intel® VT-d)

Технология виртуализации Intel® для направленного ввода-вывода (Intel® VT-d) обеспечивает аппаратную поддержку в реализациях ядра и без ядра для поддержки и повышения производительности и устойчивости виртуализации ввода-вывода.

5.3.7. Выполнить бит отключения

Функция Intel Execute Disable Bit может помочь предотвратить определенные классы вредоносных атак переполнения буфера в сочетании с поддерживающей операционной системой. Это позволяет процессору классифицировать области в памяти по тому, где код приложения может выполняться, а где нет. Когда вредоносный код пытается вставить код в буфер, процессор отключает выполнение кода, предотвращая повреждение и дальнейшее распространение.

5.3.8. Технология Intel® Trusted Execution (Intel® TXT) для серверов

Технология Intel® Trusted Execution (Intel® TXT) определяет улучшения на уровне платформы, которые обеспечивают создание надежных платформ. Платформа Intel® TXT помогает обеспечить аутентичность управляющей среды, так что желающие полагаться на платформу могут принять соответствующее решение о доверии. Платформа Intel® TXT определяет идентичность управляющей среды путем точного измерения и проверки управляющего программного обеспечения.

5.3.9. Расширенное векторное расширение Intel® 512 (Intel® AVX-512)

Базовые 512-битные расширения инструкций SIMD называются базовыми инструкциями Intel® Advanced Vector Extension 512 (Intel® AVX-512). Они включают в себя расширения семейства Intel® AVX инструкций SIMD, но кодируются с использованием новой схемы кодирования с поддержкой 512-битных векторных регистров, до 32 векторных регистров в 64-битном режиме и условной обработки с использованием регистров opmask.

5.3.10. Новые команды стандарта Intel® Advanced Encryption Standard (Intel® AES-NI)

Новые инструкции Intel® Advanced Encryption Standard (Intel® AES-NI) — это набор инструкций, реализованный во всех процессорах семейства масштабируемых процессоров Intel® Xeon® 1-го и 2-го поколения. Эта функция добавляет инструкции для ускорения операций шифрования и дешифрования, используемых в Advanced Encryption Standard (AES). Функция Intel® AES-NI включает в себя шесть дополнительных инструкций с одной инструкцией и несколькими данными (SIMD) в наборе команд Intel® Streaming SIMD Extensions.

BIOS отвечает в процессе POST за определение наличия у процессора инструкций Intel® AES-NI. Некоторые процессоры могут производиться без инструкций Intel® AES-NI.

Инструкции Intel® AES-NI могут быть включены или отключены в BIOS. Инструкции Intel® AES-NI находятся во включенном состоянии, если BIOS явно не отключил их.

5.3.11. Intel® Node Manager (Intel® NM) 4.0

Набор микросхем Intel® серии C620 Intel® Management Engine (Intel® ME) поддерживает технологию Intel® Node Manager (Intel® NM). Комбинация Intel® ME и Intel® NM добавляют возможность управления питанием и температурой на платформе, которая предоставляет внешние интерфейсы, которые позволяют ИТ-специалистам (через внешнее программное обеспечение управления) запрашивать Intel® ME о мощности и потреблении мощности платформы, тепловых особенностях и указывать директивы политики. (то есть установить бюджет мощности платформы). Intel® ME обеспечивает выполнение этих директив политики, контролируя энергопотребление нижележащих подсистем, используя доступные механизмы управления (например, состояния P/T процессора). Определение директивы политики выполняется за пределами Intel® ME либо с помощью программного обеспечения интеллектуального управления, либо ИТ-оператором.

Ниже приведены некоторые из приложений технологии Intel® Intelligent Power Node Manager.

- Мониторинг и ограничение мощности платформы: Intel® ME/Intel® NM контролирует энергопотребление платформы и удерживает среднюю мощность в течение длительного времени. Его можно регулировать, чтобы установить фактическую мощность в любом конкретном случае. Возможность ограничения мощности позволяет внешнему программному обеспечению управления решать ключевые ИТ-проблемы путем установки бюджета мощности для каждого сервера.
- Мониторинг температуры воздуха на входе: Intel® ME/Intel® NM периодически контролирует температуру воздуха на входе в сервер. Intel® ME/Intel® NM выдает предупреждение, когда температура входного канала (номер) превышает заданное значение, при включенном предупреждении. Пороговое значение можно установить соответствующей политикой.
- Ограничение мощности подсистемы памяти: Intel® ME/Intel® NM контролирует энергопотребление памяти. Потребляемая мощность памяти оценивается с использованием информации об использовании средней полосы пропускания.
- Мониторинг и ограничение мощности процессора: Intel® ME/Intel® NM контролирует энергопотребление процессора и сокета и сохраняет среднюю мощность в течение длительного времени. Можно запросить возврат фактической мощности в любой момент времени. Процесс мониторинга Intel® ME будет использоваться для ограничения энергопотребления процессора с помощью P-состояний процессора и динамического распределения ядер.
- Распределение ядер при загрузке во времени: Ограничение на количество используемых ядер для OS/Virtual Machine Manager (VMM) путем ограничения числа ядер, являющихся активными при загрузке во времени. После того, как процессы будут выключены, то CPU пределы как многие рабочие ядра являются видимыми для в BIOS и OS/VMM. Эти ядра, которые будут превращены от не могут быть повернуты на динамически после ОС уже начались. Она может быть изменена только в следующей системе перезагрузки.
- Распределение ядер во время выполнения: этот конкретный вариант использования предоставляет пользователю механизм управления мощностью процессора более высокого уровня в период после загрузки. Внешний агент может динамически использовать или не использовать ядра в подсистеме процессора,

запрашивая Intel® ME/Intel® NM для управления ими, указывая количество ядер, которые следует использовать или не использовать.

Дополнительные сведения о поддержке Intel® Intelligent Power Node Manager (см. Раздел 9).

5.3.12. Intel® Deep Learning Boost

Intel® Deep Learning Boost в семействе масштабируемых процессоров Intel® Xeon® 2-го поколения разработано для обеспечения более эффективного ускореного глубокого обучения (вывода) за счет расширения возможностей Intel® AVX-512 с помощью специальных команд Intel® Vector Neural Network (VNNI) для задач глубокого обучения. Дополнительные сведения см. В Руководстве разработчика программного обеспечения для архитектур Intel® 64 и IA-32.

5.3.13. Speed Выбор Intel® Technology

Технология Intel® Speed Select, доступная в некоторых моделях семейства Scalable процессоров Intel® Xeon® 2-го поколения, предлагает три различных точки рабочего напряжения и частоты для установления гарантированной базовой частоты (P1). Эта частота основана на количестве активных ядер в SKU и только при соблюдении требований к температуре. Технология Intel® Speed Select позволяет использовать большее количество активных ядер при более низкой базовой частоте или меньшее количество активных ядер при более высокой базовой частоте, предоставляя несколько характеристик ЦП в зависимости от рабочей нагрузки/потребностей виртуальной машины.

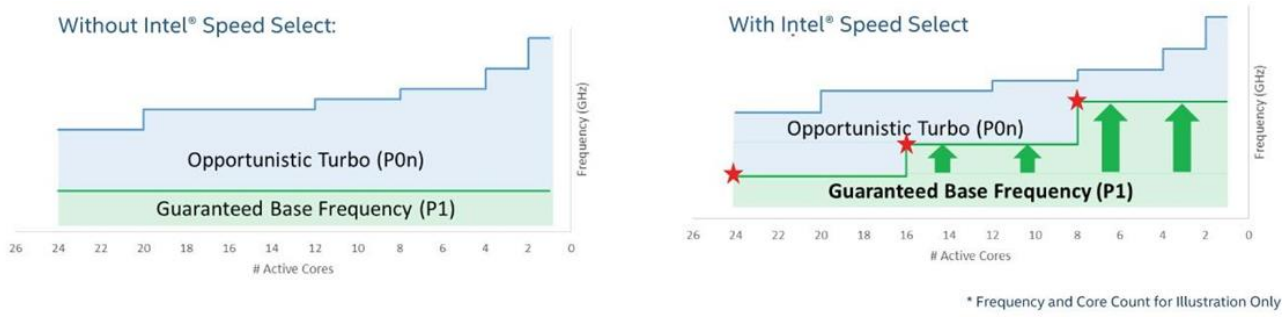


Рисунок 5-7. Сравнение технологии Intel® Speed Select

5.3.14. Технология Intel® Resource Director

Технология Intel® Resource Director, доступная в семействе процессоров Intel® Xeon® 2-го поколения, снижает конкуренцию за ресурсы, когда несколько приложений, контейнеров или виртуальных машин совместно используют ресурсы платформы. Программные потоки могут иметь пропускную способность памяти в соответствии с их приоритетом, а не только с процессором, и это достигается с помощью следующих функций:

- Технология мониторинга кеша (CMT): отслеживает использование LLC (кеш L3) каждым программным потоком с помощью идентификатора мониторинга ресурсов (RMID).
- Приоритезация кода и данных (CDP): обеспечивает контроль размещения кода и данных в кеш-памяти.
- Мониторинг пропускной способности памяти (MBM): дает OS/VMM возможность мониторинга использования пропускной способности памяти для каждого выполняющегося потока.

- Распределение пропускной способности памяти (MBA): MBA — это новая функция, представленная в семействе Scalable процессоров Intel® Xeon® 2-го поколения, которая позволяет программному обеспечению контролировать объем пропускной способности памяти, доступную для рабочих нагрузок, чтобы снизить уровень помех и сформировать требуемую пропускную способность.

5.4. Правила установки процессора

ПРИМЕЧАНИЕ: материнская плата может поддерживать двухпроцессорные конфигурации, состоящие из разных процессоров, отвечающих определенным критериям; однако QTECH не проводит проверочные испытания таких конфигурации. Кроме того, QTECH не гарантирует надежную работу серверной системы, в которой установлены не имеющие аналогов процессоры.

Встроенный BIOS будет пытаться работать с процессорами, которые не соответствуют друг другу, но в целом совместимы. Для оптимальной производительности системы в двухпроцессорных конфигурациях QTECH рекомендует устанавливать идентичные процессоры.

При использовании однопроцессорной конфигурации процессор должен быть установлен в процессорное гнездо с надписью «CPU_1».

ПРИМЕЧАНИЕ: некоторые функции платы могут не работать без установленного второго процессора. См. Рисунок 4-6.

Если установлено два процессора, должны соблюдаться следующие правила:

- оба процессора должны иметь одинаковое количество ядер;
- оба процессора должны иметь одинаковые размеры кеш-памяти для всех уровней процессора;
- оба процессора должны поддерживать идентичные частоты DDR4;
- оба процессора должны иметь идентичное расширенное семейство, расширенную модель, тип процессора, код семейства и номер модели.

В системе могут использоваться процессоры с разными частотами ядер при соблюдении данных правил. Если это условие соблюдается, то все ядра процессора устанавливаются на наименьшую общую частоту (наибольшая общая скорость), и выдается сообщение об ошибке.

Степпинг процессора в рамках общего семейства процессоров может быть смешанным, если он указан в обновлениях спецификаций процессора, опубликованных корпорацией Intel®. Смешивание процессоров с другой версией степпинга проверяется и поддерживается только между процессорами, которые отличаются друг от друга на плюс или минус один шаг.

5.5. Сводка ошибок инициализации процессора

В таблице 8 описаны ошибки смешанных конфигурации процессоров и рекомендуемые действия для материнской платы, созданной на основе семейства масштабируемых процессоров Intel® Xeon® и архитектуры набора микросхем Intel® серии C621. Ошибки могут быть одной из трех степеней серьезности:

- Критическая (Fatal): если система не может загрузиться, POST останавливается и отображается следующее сообщение:
  Unrecoverable fatal error found. System will not boot until the error is resolved
  Press <F2> to enter setup
  (Обнаружена неустранимая фатальная ошибка. Система не загрузится, пока ошибка не будет устранена

Нажмите <F2>, чтобы войти в настройку).
При нажатии клавиши <F2> на клавиатуре сообщение об ошибке отображается на экране диспетчера ошибок, и регистрируется в журнале системных событий (SEL) с кодом ошибки POST.
Параметр «POST Error Pause» в настройках BIOS не влияет на эту ошибку.
Если система не может загрузиться, система генерирует звуковой код, состоящий из трех длинных и одного короткого сигнала. Система не сможет загрузиться, пока ошибка не будет устранена. Неисправный компонент необходимо заменить.
Светодиодный индикатор состояния системы горит желтым цветом для всех фатальных ошибок, обнаруженных во время инициализации процессора.
Постоянно горящий желтый индикатор состояния системы указывает на неисправимый сбой системы.

- Крупная (Major): сообщение об ошибке отображается на экране диспетчера ошибок и регистрируется в журнале событий (SEL). Если в BIOS включена опция «POST Error Pause», для продолжения загрузки системы требуется вмешательство оператора. Если параметр настройки BIOS «POST Error Pause» отключен, система продолжит загрузку.
- Незначительное (Minor): сообщение об ошибке может отображаться на экране или в диспетчере ошибок, а код ошибки POST записывается в журнал SEL. Система продолжит загружаться. Пользователь может отменить вывод сообщения об ошибке. Параметр «POST Error Pause» в настройках BIOS не влияет на эту ошибку.

Таблица 45. Сводка ошибок смешанных конфигураций процессоров

Ошибка	Важность	Действия системы при обнаружении ошибки
Семейство процессоров не идентично	Фатальная	Останавливается с кодом POST 0xE6. Генерирует три длинных и один короткий звуковой сигнал. Выполняет действия при фатальной ошибке (см. Выше) и не загружается, пока неисправность не будет устранена
Модель процессора не идентична	Фатальная	Регистрирует код ошибки POST в SEL. Предупреждает BMC о том, что индикатор состояния системы должен гореть желтым цветом. Отображает ошибку 0196: Обнаружено несоответствие модели процессора. Выполняет действия при фатальной ошибке (см. Выше) и не загружается, пока неисправность не будет устранена
Ядра/потоки процессора не идентичны	Фатальная	Останавливается с кодом POST 0xE5. Воспроизводит три длинных и один короткий звуковой сигнал. Выполняет действия при фатальной ошибке (см. Выше) и не загружается, пока неисправность не будет устранена

Ошибка	Важность	Действия системы при обнаружении ошибки
Кеш процессора или домашний агент не идентичны	Фатальная	Останавливается с кодом POST 0xE5. Воспроизводит три длинных и один короткий звуковой сигнал. Выполняет действия при фатальной ошибке (см. Выше) и не загружается, пока неисправность не будет устранена
Частота процессора (скорость) не идентична	Фатальная	Если частоты для всех процессоров можно настроить одинаковыми: Устанавливает все частоты процессора на самую высокую общую частоту. Не генерирует ошибку, не считается за состояние ошибки.Продолжает успешно загружать систему. Если нельзя настроить одинаковые частоты для всех процессоров: Регистрирует код ошибки POST в SEL
Частота процессора (скорость) не идентична	Фатальная	Предупреждает BMC о том, что индикатор состояния системы должен гореть желтым цветом. Не отключает процессор. Отображает ошибку 0197: Невозможно синхронизировать скорость процессоров. Выполняет действия при фатальной ошибке (см. Выше) и не загружается до тех пор, пока неисправность не будет устранена
Частоты каналов Intel® UPI Link не идентичны	Фатальная	Если частоты всех каналов Intel® Ultra Path Interconnect (Intel® UPI) можно настроить так, чтобы они были одинаковыми: Настраивает все частоты межкомпонентного соединения Intel UPI на самую высокую общую частоту. Не генерирует ошибку, не считается за состояние ошибки. Продолжает успешно загружать систему. Если частоты всех каналов Intel® UPI нельзя настроить одинаковыми: Регистрирует код ошибки POST в SEL. Предупреждает BMC о том, что индикатор состояния системы должен гореть желтым цветом. Не отключает процессор. Отображает ошибку 0195: Intel (R) UPII не может синхронизировать частоты каналов процессоров

Ошибка	Важность	Действия системы при обнаружении ошибки
Частоты каналов Intel® UPI Link не идентичны	Фатальная	Выполняет действия при фатальной ошибке (см. Выше) и не загружается, пока неисправность не будет устранена
Ошибка обновления микрокода процессора	Крупная	Регистрирует код ошибки POST в SEL. Отображает ошибку 816x: процессор 0x выводит сообщение об ошибке обновления микрокода в диспетчере ошибок или на экране. Принимает меры по устранению ошибки. Продолжение загрузки системы зависит от настройки «POST Error Pause». В случае остановки загрузки будет выведен код ошибки POST в диспетчере ошибок, ожидается вмешательство оператора
Отсутствует обновление микрокода процессора	Незначи-тельная	Регистрирует код ошибки POST в SEL. Отображает ошибку 818x: процессор 0x выводит сообщение в диспетчере ошибок или на экране, что микрокод обновление не найдено. Система продолжает загружаться независимо от параметра «POST Error Pause»

6. ПОДДЕРЖКА PCI EXPRESS* (PCIE*)

Интерфейс PCI Express* (PCIe*) полностью совместим с базовой спецификацией PCI Express версии 3.0 и поддерживает следующие скорости передачи данных PCIe: Gen 3.0 (8.0 ГТ/с), Gen 2.0 (5.0 ГТ/с) и Gen 1.0 (2,5 ГТ/с).

Конкретные функции по маршрутизации информации от каждого процессора поддерживаемые PCIe портами см Таблица 46.

Таблица 46. Маршрутизация портов CPU - PCIe*

CPU 1		**CPU 2**	
Порты PCI	Бортовое устройство	Порты PCI	Бортовое устройство
Порт DMI 3 - x4	Чипсет	Порт DMI 3 - x4	Не используемый
Порт 1A - x4	Канал восходящей связи с технологией Intel® QuickAssist	Порт 1A - x4	Слот #2
Порт 1B - x4	Канал восходящей связи с технологией Intel® QuickAssist	порт 1B - x4	Слот #2
Порт 1C - x4	Slot M.4 / PCIe x4	Порт 1C - x4	Слот #2
Порт 1D - x4	Не используется	Порт 1D - x4	Слот #2
Порт 2A - x4	Слот #6	Порт 2A - x4	Слот #4
Порт 2B - x4	Слот #6	Порт 2B - x4	Слот #4
Порт 2C - x4	Слот #6	Порт 2C - x4	Слот #4
Порт 2D - x4	Слот #6	Порт 2D - x4	Слот #4
Порт 3A - x4	Слот #5	Порт 3A - x4	Слот #1
Порт 3B - x4	Слот #5	Порт 3B - x4	Слот #1
Порт 3C - x4	Не используется	Порт 3C - x4	Слот #3
Порт 3D -x4	Не используется	Порт 3D -x4	Слот #3

6.1. Перечисление и распределение PCIe*

BIOS назначает номера шины PCI в соответствии со спецификацией локальной шины PCI версии 3.0. Номер шины увеличивается, когда BIOS обнаруживает устройство моста PCI-PCI.

Сканирование продолжается на вторичной стороне моста, пока всем подчиненным шинам не будут присвоены номера. Назначение номеров шины PCI может варьироваться от загрузки к загрузке в зависимости от наличия устройств PCI с мостами PCI-PCI.

Если мостовое устройство с единственной шиной позади него вставляется в шину PCI, все последующие номера шины PCI ниже текущей шины увеличиваются на единицу. Назначение шины происходит один раз, в начале процесса загрузки BIOS, и никогда не изменяется на этапе предварительной загрузки.

7. ПОДДЕРЖКА ПАМЯТИ

В этой главе описывается архитектура, управляющая подсистемой памяти, поддерживаемые типы памяти, правила установки памяти и поддерживаемые функции надежности, доступности и удобства обслуживания (RAS) памяти.

7.1. Архитектура подсистемы памяти

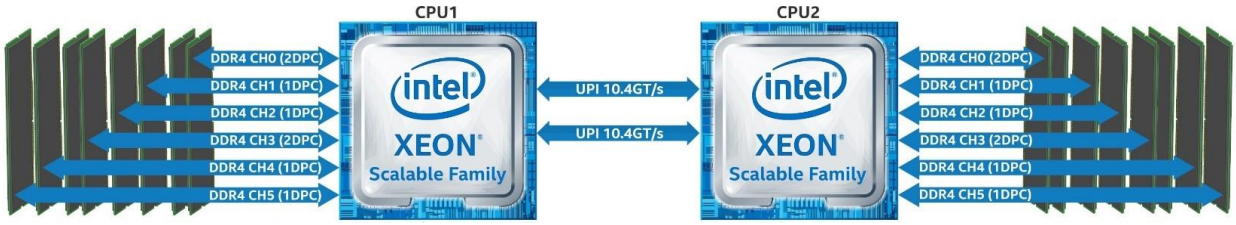


Рисунок 7-1. Архитектура подсистемы памяти

ПРИМЕЧАНИЕ: материнская плата поддерживает только память DDR4.

Каждый установленный процессор включает в себя интегрированный контроллер памяти (IMC), способный поддерживать до шести каналов памяти DDR4, в которых можно разместить до двух слотов DIMM на канал. В материнской плате предусмотрено всего 16 разъемов DIMM (восемь модулей DIMM на процессор) — 1 разъем DDR4 DIMM на канал памяти на четырех каналах и 2 разъема DDR4 DIMM на двух каналах (топология 2-1-1).

Материнская плата поддерживает следующее:

- Поддерживаются только модули DIMM DDR4.
- Поддерживаются только модули RDIMM и LRDIMM с термодатчиком на DIMM (TSOD).
- Поддерживаются только модули RDIMM и LRDIMM с включенным кодом исправления ошибок (ECC).
- Традиционные модули DIMM SDRAM организованы как одноранговые (SR), двухранговые (DR) или четырехранговые (QR).

7.2. Поддерживаемая память

В следующих таблицах перечислены подробные инструкции по поддержке DIMM:

Таблица 47. Рекомендации по поддержке традиционных модулей памяти DIMM DDR4 SDRAM для масштабируемого семейства процессоров Intel® Xeon® 1-го поколения

Тип	**Ранги на DIMM и ширину данных**	**Емкость DIMM (ГБ)**		**Максимальная скорость (MT/c); Напряжение (В); Слотов на канал (SPC) и модулей DIMM на канал (DPC)**		
				1 слот на канал	2 слота на канал	
		Плотность DRAM		1DPC	1DPC	2DPC
		4 ГБ	8 ГБ	1,2 В	1,2 В	1,2 В
RDIMM	SRx8	4 ГБ	8 ГБ	2666 MT/c	2666 MT/c	2666 MT/c
	SRx4	8 ГБ	16 ГБ			
	DRx8	8 ГБ	16 ГБ			
	DRx4	16 ГБ	32 ГБ			
RDIMM 3DS	QRx4	Нет данных	2H-64 ГБ			
	8Rx4	Нет данных	4H-128 ГБ			
LRDIMM	QRx4	32 ГБ	64 ГБ			
LRDIMM 3DS	QRx4	Нет данных	2H-64 ГБ			
	8Rx4	Нет данных	4H-128 ГБ			

Таблица 48. Рекомендации по поддержке традиционных модулей памяти DIMM DDR4 SDRAM для масштабируемого семейства процессоров Intel® Xeon® 2-го поколения

Тип	**Ранги на DIMM и ширину данных**	**Емкость DIMM (ГБ)**			**Максимальная скорость (MT/c); Напряжение (В); Слотов на Канал (SPC) и количество модулей DIMM на канал (DPC)**		
					1 слот на Канал	2 слота на канал	
		Плотность DRAM			1DPC	1DPC	2DPC
		4 ГБ	8 ГБ	16 ГБ	1,2 В	1,2 В	1,2 В
RDIMM	SRx8	4 ГБ	8 ГБ	16 ГБ	2933 MT/c	2933 MT/c	2666 MT/c
	SRx4	8 ГБ	16 ГБ	32 ГБ			
	DRx8	8 ГБ	16 ГБ	32 ГБ			
	DRx4	16 ГБ	32 ГБ	64 ГБ			
RDIMM 3DS	QRx4	Нет данных	2H-64 ГБ	2H-128 ГБ			
	8Rx4	Нет данных	4H-128 ГБ	4H-56 ГБ			
LRDIMM	QRx4	32 ГБ	64 ГБ	128 ГБ			
LRDIMM 3DS	QRx4	Нет данных	2H-64 ГБ	2H-128 ГБ			
	8Rx4	Нет данных	4H-128 ГБ	4H-256 ГБ			

Таблица 49. Максимальные поддерживаемые скорости традиционных модулей памяти SDRAM DIMM по уровням SKU в MT/c (мегатранзакций в секунду)

	Platinum 8xxx	Gold 6xxx	Gold 5xxx	Silver 4xxx	Bronze 3xxx
Масштабируемое семейство процессоров Intel® Xeon® 1-го поколения	2666	2666	2400	2400	2133
Масштабируемое семейство процессоров Intel® Xeon® 2-го поколения	29332	29332	2666	2400	2133

Пояснения:

1. Плотность DRAM 4 ГБ поддерживается только на скоростях до 2666 MT/c.
2. Макс. скорость только в конфигурации 1DPC.

7.3. Общие правила поддержки памяти

ПРИМЕЧАНИЕ: хотя смешанные конфигурации DIMM могут работать, QTECH поддерживает и выполняет проверку платформы только в системах, в которых установлены идентичные модули DIMM.

Каждый установленный процессор имеет шесть каналов памяти. На материнской плате каналы памяти для каждого процессора обозначены от A до F. Каналы A и D на каждом процессоре поддерживают два слота DIMM. Все остальные каналы памяти имеют один слот DIMM. На материнской плате каждый слот DIMM помечен номером процессора, каналом памяти и номером слота, как показано в следующих примерах: CPU1_DIMM_A2; CPU2_DIMM_A2.

Правила установки модулей DIMM требуют, чтобы каналы, поддерживающие более одного модуля DIMM, заполнялись, начиная с синего слота DIMM или слота DIMM, наиболее удаленного от процессора, в подходе «до самого конца». Кроме того, при использовании четырехрангового модуля DIMM и однорангового или двухрангового модуля DIMM в том же канале, четырехранговый модуль DIMM должен располагаться дальше всего от процессора. Слоты памяти, связанные с данным процессором, недоступны, если соответствующий сокет процессора не заполнен.

Процессор может быть установлен без заполнения связанных слотов памяти, при условии, что второй процессор установлен со связанной памятью. В этом случае память используется совместно; однако платформа страдает от снижения производительности и задержек.

Разъемы для процессоров являются автономными и независимыми. Тем не менее, все подсистемы поддержки памяти (например, памяти RAS или ошибки управления) в настройках BIOS будут применены через процессорные сокеты.

В материнской плате предусмотрено всего 16 разъемов DIMM. Один разъем DDR4 DIMM на канал памяти на четырех каналах и два разъема на двух каналах (топология 2-1-1). Номенклатура слотов памяти подробно см. Рисунок 7-2.

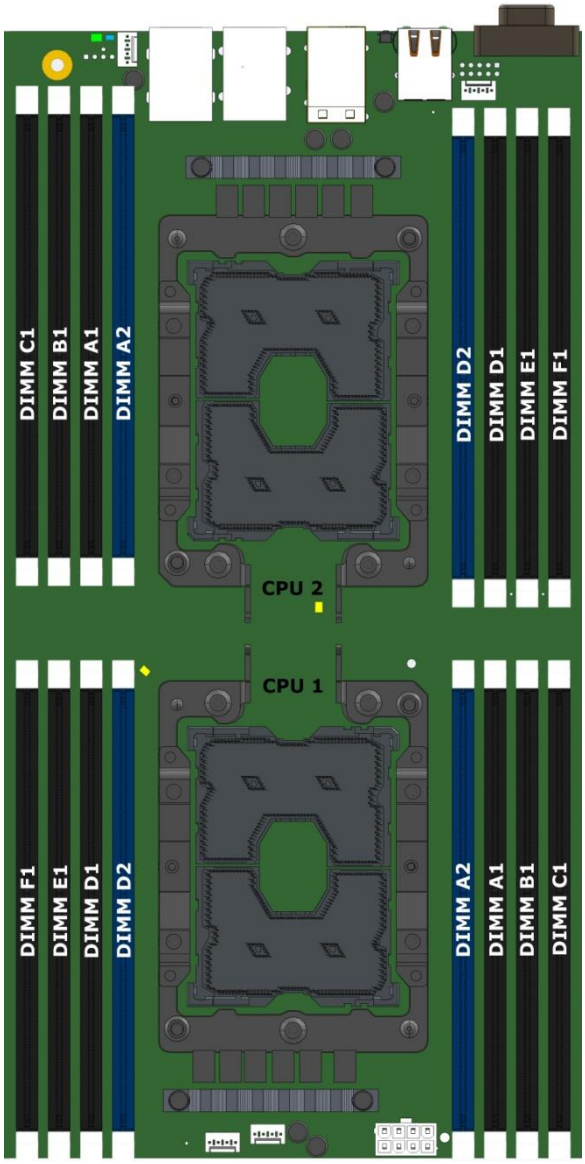


Рисунок 7-2. Расположение разъемов памяти на материнской плате

Требования к расположению модулей DIMM перечислены ниже.

- Для нескольких модулей DIMM на канал:
  - Для RDIMM, LRDIMM, 3DS RDIMM, или 3DS LRDIMM, всегда устанавливать DIMMs с более высокой электрической нагрузкой в первом слоте канала (синий слот), а затем второй слот.
- Когда только один модуль DIMM будет использоваться в каналах A или D, он должен быть установлен в синий DIMM-слот.
- На любом канале можно использовать максимум 8 логических рангов, а также максимум 10 физических рангов, загруженных на канал.
- Смешивание типов DDR4 DIMM (RDIMM, LRDIMM, 3DS-RDIMM, 3DS-LRDIMM, NVDIMM) в пределах канала сокета или через сокеты не поддерживается. Это критическая ошибка при инициализации памяти.

- Совместное использование модулей DIMM с разными частотами и задержками не поддерживается внутри процессорных сокетов и между ними. Если встречается смешанная конфигурация, BIOS пытается работать с максимальной общей частотой и минимально возможной задержкой.
- LRDIMM Rank Multiplication Mode и Direct Map Mode не должны быть смешанными внутри канала или через процессорные разъемы. Это критическая ошибка при инициализации памяти.
- Для того, чтобы установить 3 QR LRDIMM на том же канале, они должны работать с Rank Multiplication Mode в PM = 2.
- Режимы RAS Rank Sparing и Mirroring в BIOS являются взаимоисключающими. Можно выбрать только один режим работы, и он будет применяться ко всей системе.
- Если был настроен режим RAS, но конфигурация памяти не может поддерживать его во время загрузки, система вернется в режим "независимого канала", и будет регистрировать и отображать ошибки.
- Режим резервирования возможно только тогда, когда все каналы, которые оборудуются памятью, отвечают требования по наличию по меньшей мере 2 SR- или DR-модуля DIMM, или по крайней мере один QR DIMM-модуль установлен, на каждом заполняемом канале.
- Зеркальный режим требует, чтобы для любого канала, пары модулей должны быть одинакового размера. См. Подробные сведения о номенклатуре сопряжения в BIOS EPS для масштабируемого семейства процессоров Intel Xeon Scalable.

7.3.1. Рекомендации по заполнению модулей DIMM для обеспечения максимальной производительности

Процессоры семейства Intel® Xeon® Scalable включают два встроенных контроллера памяти (IMC), каждый из которых поддерживает три 6 каналов памяти.

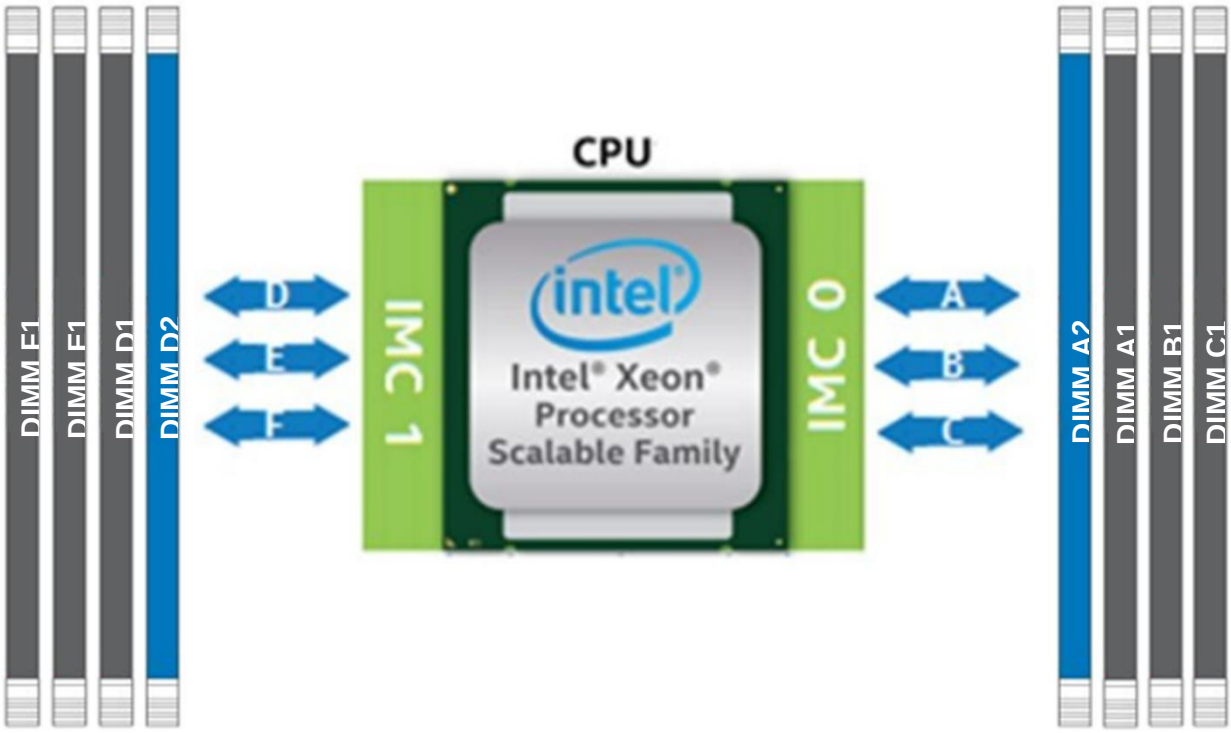


Рисунок 7-3. Расположение разъемов памяти для серверной платы

Для наилучшей производительности модули DIMM следует заполнять в соответствии со следующими рекомендациями:

- Каждый установленный процессор должен иметь соответствующие конфигурации DIMM.
- Следующие рекомендации по заполнению модулей DIMM необходимо соблюдать для каждого установленного процессора.
    - Конфигурации от 1 DIMM до 3 DIMM — модули DIMM должны быть установлены в DIMM Slot1 (черные слоты) каналов с A по C
    - Конфигурации от 4 DIMM — модули DIMM должны быть установлены в DIMM Slot1 (черные слоты) каналов A, B, D и E
    - Конфигурации от 5 DIMM — НЕ рекомендуются. Это несбалансированная конфигурация, которая будет давать производительность меньше оптимальной
    - Конфигурации от 6 DIMM — модули DIMM должны быть установлены в DIMM Slot1 (черные слоты) всех каналов
    - Конфигурации от 7 DIMM — НЕ рекомендуются. Это несбалансированная конфигурация, которая будет давать производительность меньше оптимальной
    - Конфигурации от 8 DIMM — модули DIMM должны быть установлены во все DIMM-слоты

7.4. Особенности RAS-памяти

Поддерживаемые функции RAS-памяти зависят от уровня установленного процессора. Каждый уровень процессора в семействе масштабируемых процессоров Intel® Xeon® поддерживает стандартные или расширенные функции RAS-памяти (Таблица 50).

Таблица 50. Особенности RAS-памяти

Особенность RASM	Описание	Стан-дарт	Продви-нутый
Коррекция данных устройства	x8 Single Device Data Correction (SDDC) с помощью статической виртуальной блокировки (применимо к модулям DIMM DRAM x8)	√	√
	ADDDC (SR) (применимо к модулям DIMM DRAM x4)	√	√
	Коррекция данных одного устройства x8 + 1 бит (SDDC + 1) (применимо к модулям DIMM DRAM x8)		√
Коррекция данных устройства	SDDC + 1 и ADDDC (MR) + 1 (применимо к модулям DIMM x4 DRAM)		√

Особенность RASM	Описание	Стан-дарт	Продви-нутый
DDR4 Command/Address (CMD/ADDR) Проверка четности и повторная попытка	Проверка четности CMD/ADDR на основе технологии DDR4 и повторная попытка с регистрацией «адреса» ошибки четности CMD/ADDR и повторной попыткой CMD/ADDR	√	√
Защита данных DDR4 CRC	Обнаруживает сбои шины данных DDR4 во время операции записи	√	√
Требование памяти и очистка	Очистка по запросу — это возможность записать исправленные данные обратно в память после обнаружения исправляемой ошибки в транзакции чтения. Очистка проактивно ищет в системной памяти, восстанавливая исправимые ошибки. Предотвращает накопление однобитовых ошибок	√	√
Зеркальное отображение памяти	Полное зеркальное отображение памяти: метод внутри IMC для хранения дублирующей (вторичной или зеркальной) копии содержимого памяти в качестве избыточной резервной копии для использования в случае отказа первичной памяти. Зеркальная копия памяти хранится в памяти-IMC того же процессорного разъема. Dynamic (без перезагрузки) отказоустойчивого для тех зеркальных модулей-DIMM прозрачен для ОС и приложений	√	√
Зеркальное отображение памяти	Диапазон адресов/частичное зеркалирование памяти: обеспечивает дополнительную детализацию внутри сокета для зеркалирования памяти, позволяя встроенному ПО или ОС определить диапазон адресов памяти для зеркального отображения, оставив остальную память в сокете в незеркальном режиме		√

Особенность RASM	Описание	Стан-дарт	Продви-нутый
Режим экономии резервной памяти	Динамическое переключение вышедшей из строя памяти в резерв, расположенный за тем же контроллером памяти DDR	√	√
Многоранговый режим экономии памяти	В многоранговом режиме до двух рангов из восьми могут быть назначены в качестве запасных	√	√
Обнаружение поврежденных данных iMC	Процесс сообщения об ошибке вместе с обнаруженными данными UC. Патрульный скруббер и резервный двигатель iMC могут отравлять данные UC	√	√
Идентификация неисправных DIMM	Возможность идентифицировать конкретный неисправный DIMM, тем самым позволяя пользователю заменять только вышедший из строя DIMM (ы). В случае критической ошибки и режима блокировки доступна только идентификация уровня пары DIMM поддерживается	√	√
Отключение и отображение памяти для отказоустойчивой загрузки (FRB)	Позволяет инициализировать память и загружать ОС даже при сбое памяти	√	√
Самовосстановление памяти (PPR)	Начиная с технологии DDR4, доступна дополнительная возможность, известная как Post Package Repair (PPR). PPR предлагает дополнительную свободную емкость в DDR4 DRAM, которую можно использовать для замены неисправных ячеек, обнаруженные во время загрузки системы	√	√

ПРИМЕЧАНИЕ: функции RAS-памяти могут поддерживаться не на всех SKU-типах процессоров.

7.4.1. Правила и настройка BIOS для RAS-памяти

При включении функций-RAS применяются следующие правила:

- Параметры резервирования памяти или зеркалирования памяти включены в настройках BIOS. Опции резервирования памяти и зеркального отображения памяти исключают друг друга; в настройках BIOS можно выбрать только один режим работы.
- Если режим удаленного доступа был включен, но конфигурация памяти не может поддерживать его во время загрузки, система возвращается в режим "независимого канала", а также регистрирует и отображает соответствующую ошибку.
- Режим Rank Sparing возможен только тогда, когда все каналы заполнены памятью и удовлетворяют требованию — наличие по меньшей мере двух SR или DR DIMM или одного QR DIMM, установленного в каждом заполненном канале.
- Режим зеркалирования памяти требует, чтобы для любой пары объём памяти на обоих концах канала был одинаковым.

8. СИСТЕМНЫЙ ВВОД/ВЫВОД

8.1. Поддержка дополнительных карт PCIe*

Материнская плата включает функции для одновременной поддержки нескольких типов карт расширения, включая карты расширения PCIe* в слотах с 1 по 6 и выделенную переходную плату LAN, совмещенную со слотом 5. Кроме того, слоты 2 и 6 поддерживают переходную плату. Слоты для карт расширения PCIe* и их свойства описаны ниже.

- Слот 1: PCIe* 3.0 x8 (x8, электрический), обрабатываемый CPU2
- Слот 2: PCIe* 3.0 x16 (x16, электрический), обрабатываемый ЦП2 (с возможностью переходной платы)
- Слот 3: PCIe* 3.0 x8 (x8, электрический), обрабатываемый CPU2
- Слот 4: PCIe* 3.0 x16 (x16, электрический), обрабатываемый CPU2
- Слот 5: PCIe* 3.0 x8 (x8, электрический), обрабатываемый CPU1
- Слот 6: PCIe* 3.0 x16 (x16, электрический), обрабатываемый ЦП1 (с возможностью переходной платы)

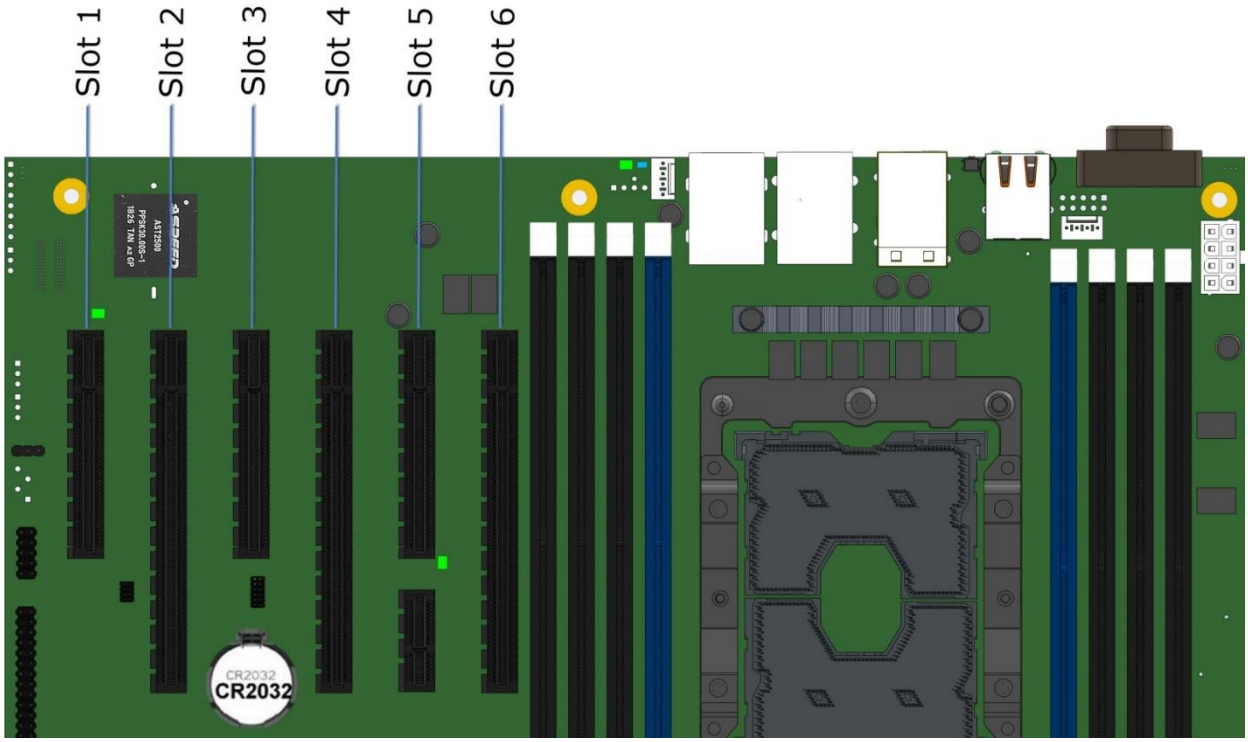


Рисунок 8-1. Слоты PCIe*

Такая конфигурация слотов позволяет устанавливать до 3 дополнительных карт двойной ширины и полной длины. Для этого случая также предоставляется дополнительное питание.

8.1.1. Поддержка Riser Card

Слоты PCIe* 2 и 6 могут поддерживать переходные платы. Каждый слот переходной платы x16 поддерживает стандартные выводы разъема x16 PCIe*, а также включает в себя две тактовые частоты 100 МГц и бит Riser_ID (для предоставления информации о ширине

канала в BIOS-системы). Каждый из разъемов переходной платы может поддерживать переходные платы со следующими конфигурациями разъемов для плат расширения PCIe*:

- переходная плата x16 с двумя слотами x4 PCIe*
- x16 стойка с одним x4 PCIe* слот и один x8 PCIe* слот
- переходная плата x16 с двумя слотами x8 PCIe*
- переходная плата x16 с одним слотом x16 PCIe*

8.2. Встроенная подсистема хранения данных

Материнская плата включает поддержку многих технологий хранения и встроенных функций для поддержки широкого спектра вариантов хранения. Это включает:

- (2) — M.2 PCIe*/последовательный ATA (SATA)
- (4) — PCIe* OCuLink *
- Устройство управления томами Intel® (Intel® VMD) для твердотельных накопителей NVMe*
- Intel® VROC (VMD NVMe RAID)
- (2) — 7-контактный однопортовый SATA
- (2) — Mini-SAS HD (SFF-8643), 4 порта SATA
- Встроенный SATA избыточный массив независимых дисков (RAID) (опционально)
    - Intel® VROC (SATA RAID) 6.0
    - Intel® Embedded Сервер RAID технология 2 v1.60 для SATA

В следующих секциях дается обзор по каждой опции.

8.2.1. Поддержка устройств хранения M.2

Материнская плата поддерживает два устройства PCIe*/SATA 2280 M.2 в стековой конфигурации. Каждый разъем M.2 может поддерживать модули PCIe или SATA, соответствующие форм-фактору 2280 (ширина 22 мм, длина 80 мм). Дорожки шины PCIe для каждого разъема направляются от набора микросхем и могут поддерживаться как в однопроцессорной, так и в двухпроцессорной конфигурации.

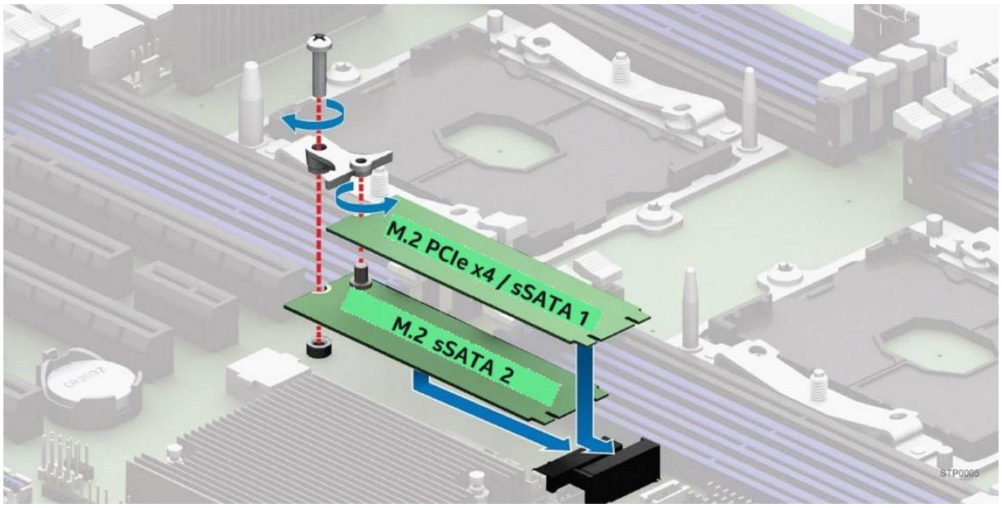


Рисунок 8-2. Разъемы M.2

PCH обеспечивает следующую поддержку для каждого разъема M.2:

- Верхний разъем — PCIe x4/sSATA-порт 1
- Нижний разъем — порт PCIe x2/sSATA 2

Где sSATA — это конкретный встроенный контроллер SATA PCH, от которого маршрутизируются порты SATA. См. Раздел 12.3.2 для получения подробной информации о распиновке разъема M.2.

ПРИМЕЧАНИЕ: устройства PCIe* M.2 будут обнаружены и видны в BIOS только в случае, когда установлен режим загрузки uEFI. Устройства SATA M.2 обнаруживаются и видны в BIOS как в режиме загрузки legacy, так и в uEFI.

8.2.2. Поддержка встроенного RAID

Поддержка встроенных на материнской плате вариантов RAID для твердотельных накопителей M.2 определяется следующим образом:

- Ни Intel® Embedded Server RAID Technology 2 (Intel® ESRT2), ни Intel® VROC (SATA RAID) не имеют поддержки RAID для твердотельных накопителей PCIe M.2 при установке на разъемы M.2 на материнской плате.

ПРИМЕЧАНИЕ: поддержка RAID для твердотельных накопителей NVMe* с использованием Intel® VROC (VMD NVMe RAID) требует, чтобы полосы шины PCIe маршрутизировались непосредственно от CPU. На материнской плате линии шины PCIe, подключенные к встроенным разъемам M.2, направляются от набора микросхем Intel (PCH). Встроенный RAID-массив Intel® ESRT2 не поддерживает устройства PCIe.

- Intel® ESRT2 и Intel® VROC (SATA RAID) обеспечивают поддержку RAID для устройств SATA.
- Ни один из вариантов встроенного RAID не поддерживает смешивание SATA SSD и SATA HDD в одном томе RAID.
- Использование твердотельных накопителей SATA SSD и PCIe NVMe в одном томе RAID не поддерживается.
- Совместимость с открытым исходным кодом — бинарный драйвер (включает частичные исходные файлы) или открытый исходный код с использованием MDRAID в Linux.

8.2.3. Intel® Volume Management Device (Intel® VMD) для NVMe* SSDs

Intel® Volume Management Device (Intel® VMD) — это аппаратная логика внутри корневого комплекса процессора, помогающая управлять твердотельными накопителями PCIe* NVMe*. Он обеспечивает надежную поддержку горячей замены и управление светодиодными индикаторами состояния. Это позволяет обслуживать твердотельные накопители NVMe* SSD-системы хранения, не опасаясь сбоев системы или зависаний при извлечении или установке NVMe SSD на шину PCIe*.

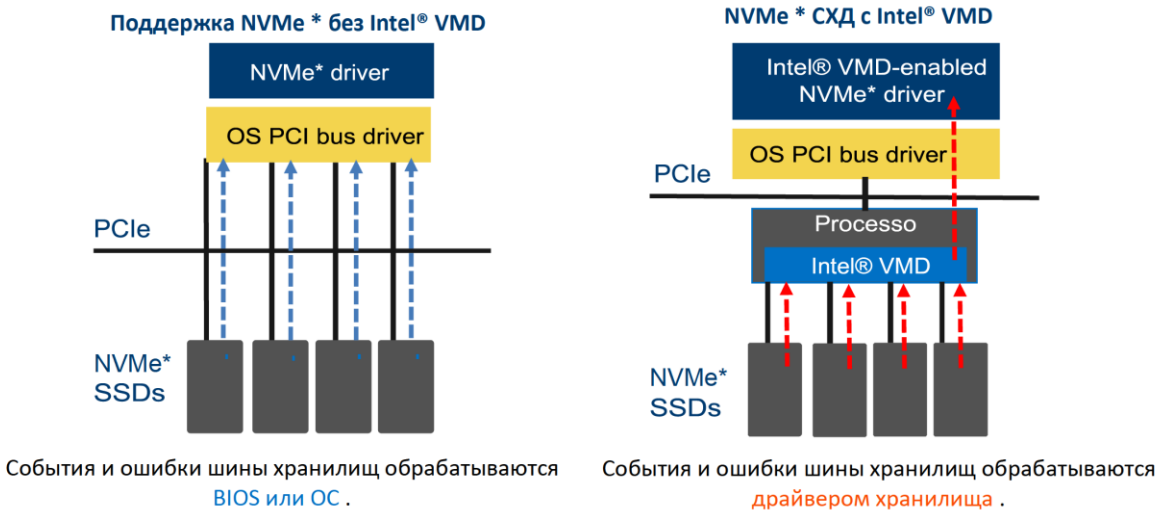


Рисунок 8-3. Устройство управления томами Intel® (Intel® VMD) для твердотельных накопителей NVMe*

Intel® VMD обрабатывает физическое управление твердотельными накопителями NVMe как отдельную задачу, которая может быть расширена, если включена опция поддержки Intel® VROC для реализации систем хранения на основе RAID. См. Раздел 8.2.4 для получения дополнительной информации.

Ниже приведен список функций технологии Intel® VMD:

- Аппаратное обеспечение интегрировано в корневой комплекс процессора PCIe*.
- Деревья PCIe* отображаются в своих собственных адресных пространствах (доменах).
- Каждый домен управляет линиями x16 PCIe*.
- Может быть включен/отключен в настройках BIOS с уровнем детализации x4.
- Драйвер настраивает домен и управляет им, выполняя перечисление устройств и обработку событий/ошибок с помощью быстрого ввода-вывода.
- Могут загружаться дополнительные драйвера для дочерних устройств, поддерживающих Intel VMD.
- Поддержка горячей замены — массив твердотельных накопителей PCIe* с возможностью горячей замены.
- Поддержка для PCIe* SSD — накопителей (без сетевого интерфейса контроллеров (NIC)), графические карты и т.д.
- Максимум 128 номеров шины PCIe* на домен.
- Поддержка MCTP через SMBus.
- Поддержка MMIO (без ввода-вывода с отображением портов).
- Не поддерживает NTB, Quick Data Tech, Intel® Omni-Path Architecture и SR-IOV.
- Исправимые ошибки не приводят к выходу системы из строя.
- Intel® VMD управляет устройствами только на линиях PCIe*, маршрутизируемых непосредственно от процессора. Intel® VMD не может обеспечить управление устройствами на линиях PCI, маршрутизируемых от набора микросхем (PCH) (см. Рисунок 4-6).

- Когда Intel® VMD включен, BIOS не регистрирует устройства, находящиеся за Intel® VMD. Драйвер Intel с поддержкой VMD отвечает за регистрирование этих устройств и предоставление их хосту.
- Intel® VMD поддерживает твердотельные накопители PCIe* с возможностью горячей замены, подключенные к нисходящим портам коммутатора. Intel® VMD не поддерживает горячее подключение самого коммутатора.

8.2.4. Intel® VROC (VMD NVMe RAID) 6.0

Intel® VROC (VMD NVMe RAID) обеспечивает использование NVMe в RAID и управление томами.

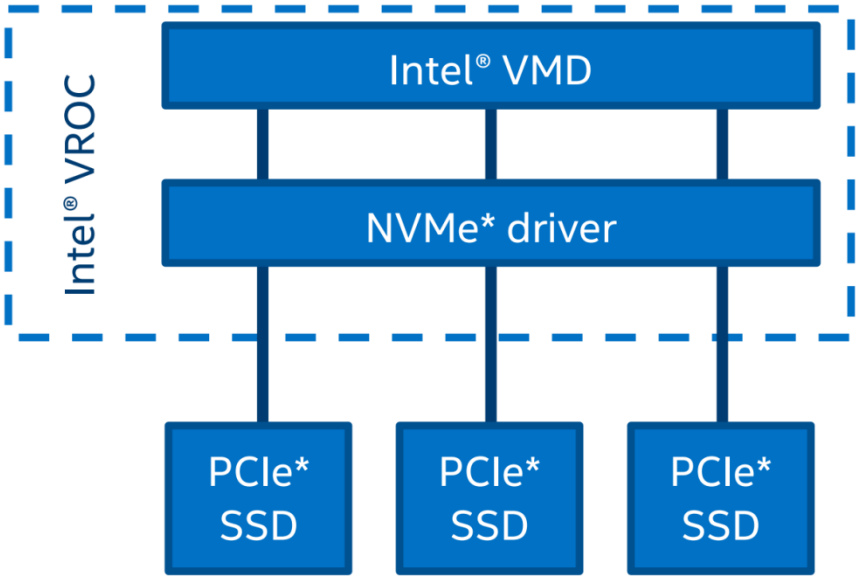


Рисунок 8-4. Обзор базовой архитектуры Intel® VROC

Intel® VROC (VMD NVMe RAID) поддерживает следующее:

- Процессор ввода-вывода с контроллером (ROC) и DRAM.
- Нет необходимости в резервном устройстве RAID, не требует дополнительного обслуживания.
- Защищенный кеш с обратной записью — программное и аппаратное обеспечение, позволяющее восстановить данные после двойной ошибки.
- Изолированные от ОС устройства хранения для обработки ошибок.
- Защищены от сбоя ОС данные R5.
- Загрузка с RAID-томов, основанных на NVMe твердотельных накопителях в виде единого Intel® VMD-домена.
- Горячее подключение NVMe SSD и защита от неожиданного удаление на линиях процессора PCIe*.
- Светодиодное оповещение о подключении накопителей к CPU PCIe.
- Управление RAID/накопителями с использованием интерфейсов прикладного программирования (API) с репрезентативной передачей состояния (RESTful).
- Графический пользовательский интерфейс (GUI) для Linux*.
- Встроенная поддержка NVme SSD 4K.

Включение поддержки Intel VROC требует установки на материнской плате «Raid Key», дополнительного ключа обновления (см. Рисунок 8-5). См. Таблица 51, где указаны доступные варианты ключа обновления Intel VROC.

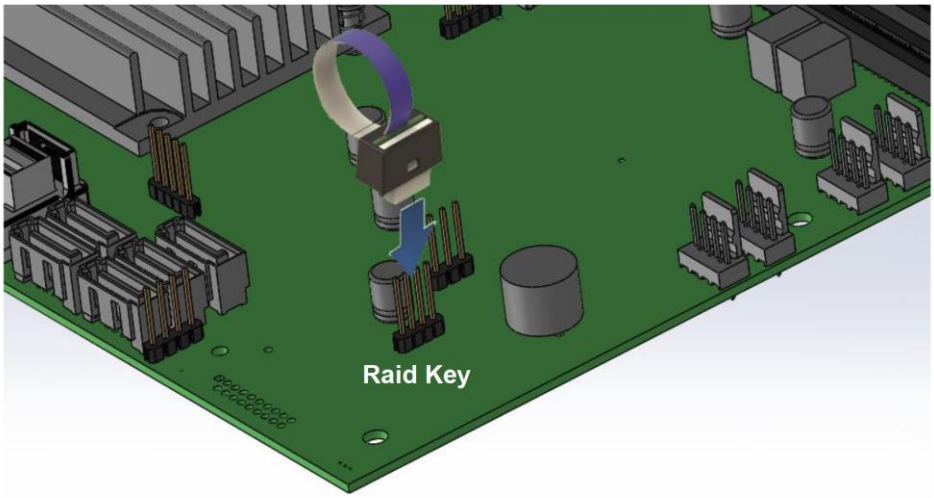


Рисунок 8-5. Ключ обновления Intel® VROC

ПРИМЕЧАНИЕ: встроенный разъем, используемый для поддержки ключей обновления Intel® VROC (VMD NVMe RAID), также используется для поддержки ключа обновления Intel® ESRT2 SATA RAID-5.

Таблица 51. Параметры ключа обновления Intel® VROC (VMD NVMe RAID)

Основные характеристики NVMe* RAID	Стандартный Intel® VROC (iPC VROCSTANMOD)	Премиум Intel® VROC (iPC VROCPREMMOD)
К процессору подключен твердотельный накопитель NVMe — обеспечение высокой производительности	√	√
Загрузка с тома RAID	√	√
Поддержка SSD сторонних производителей	√	√
RAID 0/1/10	√	√
RAID 0/1/5/10	-	√
Запись RAID невозможна (замена BBU)	-	√
Горячая замена/неожиданное удаление	√	√

Основные характеристики NVMe* RAID	Стандартный Intel® VROC (iPC VROCSTANMOD)	Премиум Intel® VROC (iPC VROCPREMMOD)
(Только форм-фактор твердотельного накопителя 2,5 дюйма; форм-фактор карты расширения не поддерживается)		
Управление светодиодами корпуса	√	√

ПРИМЕЧАНИЕ: ключи обновления Intel® VROC (Таблица 51), используются только для твердотельных накопителей PCIe* NVMe*. Информацию о поддержке SATA RAID см. В разделе 8.2.6.

8.2.5. Встроенная поддержка SATA

Материнская плата использует два «Расширенный хост-контроллер интерфейса» (AHCI) SATA, встроенные в PCH, идентифицированные как SATA и sSATA, обеспечивая до 12 SATA-портов со скоростью передачи данных до 6 Гбит/с.

Контроллер AHCI SATA обеспечивает поддержку восьми портов SATA:

- Четыре порта из в мини-SAS HD (SFF-8643) разъема помечены «SATA-порты 0-3»
- Четыре порта из в мини-SAS HD (SFF-8643) разъем с маркировкой «SATA-порты 4-7»

Контроллер AHCI sSATA обеспечивает поддержку до четырех sSATA-портов:

- Два порта, подключенных к разъемам SSD M.2, помеченным как «M2_2X_PCIE_SSATA_1» и "M2_4X_PCIE_SSATA_2"
- Доступ к двум другим портам осуществляется через два белых однопортовых 7-контактных разъема с маркировкой "sSATA-3" и "sSATA-4"

См. раздел 12.3.2 для получения подробной информации о поддержке и функциях M.2 SSD.

ПРИМЕЧАНИЕ: встроенные контроллеры SATA несовместимы и не могут использоваться с картами расширения SAS.

Таблица 52. Поддержка функций контроллера SATA и sSATA

Особенность	Описание	AHCI/RAID Отключено	AHCI/RAID Включено
Собственная очередь команд (NCQ)	Позволяет устройству переупорядочивать команды для более эффективной передачи данных	N/A	Поддерживается
Автоматическая активация для DMA	Сворачивает установку DMA, а затем последовательность активации DMA только в установку DMA	N/A	Поддерживается

Особенность	Описание	AHCI/RAID Отключено	AHCI/RAID Включено
Поддержка горячей замены*	Позволяет обнаруживать устройства без подачи питания, а также подключать и отключать устройства без предварительного уведомления системы	N/A	Поддерживается
* Существует риск потери данных при удалении диска, не входящего в отказоустойчивый RAID			
Асинхронное восстановление сигнала	Обеспечивает восстановление после потери сигнала или установление связи после горячего подключения	N/A	Поддерживается
Скорость передачи 6 Гбит/с	Возможность передачи данных до 6 Гбит/с	Поддержи-вается	Поддерживается
Расширенное технологическое присоединение с асинхронным уведомлением о пакетном интерфейсе (ATAPI)	Механизм отправки устройством уведомления хосту о том, что устройство требует внимания	N/A	Поддерживается
Управление питанием, инициированное хостом или каналом	Возможность хост-контроллера или устройства запрашивать состояния питания интерфейса	N/A	Поддерживается
Поэтапное вращение	Позволяет хосту последовательно раскручивать жесткие диски, чтобы предотвратить проблемы с питанием при загрузке	Поддержи-вается	Поддерживается
Объединение завершения команд	Уменьшает накладные расходы на завершение, позволяя выполнить указанное количество команд и затем генерируя завершение для обработки команд	N/A	N/A

Контроллер SATA и контроллер sSATA можно независимо включать, отключать и настраивать с помощью утилиты настройки BIOS в меню «Storage Controller Configuration». В следующей таблице указаны поддерживаемые параметры настройки.

Таблица 53. Параметры настройки утилиты BIOS контроллера SATA и sSATA

Состояние контроллера SATA	Состояние контроллера sSATA	Поддерживается
AHCI	AHCI	Да
AHCI	Повышенная	Да
AHCI	Отключено	Да
AHCI	Intel® VROC (SATA RAID)	Да
AHCI	Технология Intel Embedded Server RAID 2	Нет
Повышенная	AHCI	Да
Повышенная	Повышенная	Да
Повышенная	Отключено	Да
Повышенная	Intel® VROC (SATA RAID)	Да
Повышенная	Технология Intel Embedded Server RAID 2	Нет
Отключено	AHCI	Да
Отключено	Повышенная	Да
Отключено	Отключено	Да
Отключено	Intel® VROC (SATA RAID)	Да
Отключено	Технология Intel Embedded Server RAID 2	Нет
Intel® VROC (SATA RAID)	AHCI	Да
Intel® VROC (SATA RAID)	Повышенная	Да

Состояние контроллера SATA	Состояние контроллера sSATA	Поддерживается
Intel® VROC (SATA RAID)	Отключено	Да
Intel® VROC (SATA RAID)	Intel® VROC (SATA RAID)	Да
Intel® VROC (SATA RAID)	Технология Intel Embedded Server RAID 2	Нет
Технология Intel Embedded Server RAID 2	AHCI	Только Microsoft Windows*
Технология Intel Embedded Server RAID 2	Повышенная	Да
Технология Intel Embedded Server RAID 2	Отключено	Да
Технология Intel Embedded Server RAID 2	Intel® VROC (SATA RAID)	Нет
Технология Intel Embedded Server RAID 2	Технология Intel Embedded Server RAID 2	Нет

ПРИМЕЧАНИЕ: встроенные контроллеры SATA несовместимы и не могут использоваться с картами расширения SAS.

8.2.5.1. Поэтапное вращение диска

Из-за большого количества дисков, которые могут быть подключены к встроенным контроллерам AHCI SATA, совокупный скачок энергопотребления при запуске для всех дисков может быть намного выше, чем нормальные требования к питанию, и может потребоваться гораздо больший блок питания для запуска, чем для обычного функционирования.

Чтобы смягчить это и уменьшить пиковую потребляемую мощность во время запуска системы, как контроллер AHCI SATA, так и контроллер sSATA реализуют возможность поэтапного раскрутки подключенных дисков. Это позволяет приводам подключаться независимо друг от друга с задержкой между ними.

Параметр встроенного SATA Staggered Disk Spin-up настраивается с помощью программы настройки BIOS <F2>. Параметр настройки обозначен как «AHCI HDD Staggered Spin-Up» и находится на экране «Storage Controller Configuration».

8.2.6. Встроенная программная поддержка RAID

В серверную плату встроена поддержка двух вариантов программного RAID:

- Intel® VROC (SATA RAID) 6.0
- Intel® Embedded Server, RAID Technology 2 (Intel® ESRT2) основана на LSI* MegaRAID программной технологии

С помощью утилиты настройки BIOS Setup Utility **<F2>**, доступ к которой осуществляется во время POST-системы, доступны параметры для включения или отключения программного RAID, а также для выбора используемого встроенного программного обеспечения RAID.

ПРИМЕЧАНИЕ: материнская плата включает в себя два встроенных контроллера интерфейса SATA и sSATA. Технология Intel® Embedded Server RAID поддерживается только встроенным контроллером SATA.

8.2.6.1. Intel® VROC (SATA RAID) 6.0

Intel® VROC (SATA RAID) 6.0 предлагает несколько вариантов RAID для удовлетворения потребностей операционной среды. Поддержка AHCI обеспечивает более высокую производительность и устраняет узкие места при работе с диском, используя преимущества независимых механизмов DMA, которые предлагается в наборе микросхем каждого порта SATA.

- **RAID уровня 0** обеспечивает разделение томов дисков без избыточности с масштабированием производительности до шести дисков, что обеспечивает более высокую пропускную способность для приложений с интенсивным использованием данных, таких как редактирование видео.
- **RAID уровня 1** выполняет зеркалирование с использованием двух дисков одинаковой емкости и формата, что обеспечивает безопасность данных. При использовании жестких дисков с разной скоростью вращения диска в минуту (RPM) функциональность не изменяется.
- **RAID уровня 5** обеспечивает высокоэффективное хранение при сохранении отказоустойчивости трех и более дисков. Благодаря чередованию четности и ее чередованию по всем дискам отказоустойчивость любого отдельного диска достигается при использовании только емкости одного диска. То есть трехдисковый RAID 5 имеет емкость двух дисков, а четырехдисковый RAID 5 имеет емкость трех дисков. RAID 5 имеет высокую скорость чтения и среднюю скорость записи. RAID 5 хорошо подходит для приложений, которым требуется большой объем хранилища при сохранении отказоустойчивости.
- **RAID уровня 10** обеспечивает высокий уровень производительности хранилища с защитой данных, сочетая в себе отказоустойчивость уровня RAID 1 с производительностью уровня RAID 0. Благодаря чередованию сегментов RAID уровня 1 высокая скорость ввода-вывода может быть достигнута в системах, требующих как производительности, так и отказоустойчивости. RAID уровня 10 требует четыре жестких диска и обеспечивает емкость двух дисков.

ПРИМЕЧАНИЕ: конфигурации RAID не могут охватывать оба встроенных контроллера AHCI SATA.

При использовании Intel® VROC (SATA RAID) нет потери ресурсов PCI (пара запрос/предоставление) или слота для карты расширения. Функциональность Intel® VROC (SATA RAID) должна соответствовать следующим требованиям.

- Опция программного RAID должна быть включена в настройках BIOS.
- Intel® VROC (SATA RAID) должен быть выбран в настройке BIOS.
- Должны быть загружены драйверы Intel® VROC (SATA RAID) для установленной операционной системы.
- Для поддержки уровней RAID 0 или 1 необходимо как минимум два диска SATA.
- Для поддержки уровня RAID 5 необходимо как минимум три диска SATA.
- По крайней мере, четыре SATA-дисков будут необходимы для поддержки RAID уровня 10.

При включенном программном RAID Intel® VROC (SATA RAID) становятся доступными следующие функции:

- Пользовательский интерфейс в текстовом режиме во время загрузки. Предоперационная среда, которая позволяет пользователю управлять конфигурацией RAID в системе. Простой набор функций, чтобы уменьшить размер до минимума, позволяет пользователю создавать и удалять тома RAID и выбирать параметры восстановления при возникновении проблем. Пользовательский интерфейс может быть доступен при нажатии **<Ctrl-I>** во время системы POST.
- Поддержка загрузки при использовании тома RAID в качестве загрузочного диска. Для этого он предоставляет службы Int13, когда к этому RAID необходимо получить доступ приложениям MS-DOS (например, загрузчик NT (NTLDR)), и экспортирует тома RAID в системную BIOS для выбора в порядке загрузки.
- При каждой загрузке пользователю демонстрируется статус томов RAID.

8.2.6.2. Intel® Embedded Сервер RAID технология 2 (Intel® ESRT2) 1,60

Intel® Embedded Server, RAID Technology 2 основана на LSI * MegaRAID программном стеке и использует системную память и процессор.

Intel® ESRT2 поддерживает следующие уровни RAID.

- **RAID уровня 0** обеспечивает разделение томов дисков без резервирования с возможностью увеличения производительности до шести дисков, что обеспечивает более высокую пропускную способность для приложений, интенсивно использующих данные, таких как редактирование видео.
- **RAID уровня 1** выполняет зеркалирование с использованием двух дисков одинаковой емкости и формата, что обеспечивает безопасность данных. При использовании жестких дисков с разной скоростью вращения диска в минуту (RPM) функциональность не изменяется.
- **RAID уровня 10** обеспечивает высокий уровень производительности хранилища с защитой данных, сочетая отказоустойчивость RAID уровня 1 с производительностью RAID уровня 0. Благодаря чередованию сегментов RAID уровня 1 высокая скорость ввода-вывода может быть достигнута в системах, требующих и производительность, и отказоустойчивость. RAID уровня 10 требует четыре жестких диска и обеспечивает емкость двух дисков.

Дополнительная поддержка RAID уровня 5 может быть включена с помощью Raid Key, ключа обновления RAID 5 (IPN - RKSATA4R5).

- **RAID уровня 5** обеспечивает высокоэффективное хранение при сохранении отказоустойчивости трех и более дисков. Благодаря чередованию четности и ее чередованию по всем дискам отказоустойчивость любого отдельного диска достигается при использовании только емкости одного диска. То есть трехдисковый RAID 5 имеет емкость двух дисков, а четырехдисковый RAID 5 имеет емкость трех дисков. RAID 5 имеет высокую скорость транзакций чтения и среднюю скорость записи. RAID 5 хорошо подходит для приложений, которым требуется большой объем хранилища при сохранении отказоустойчивости.

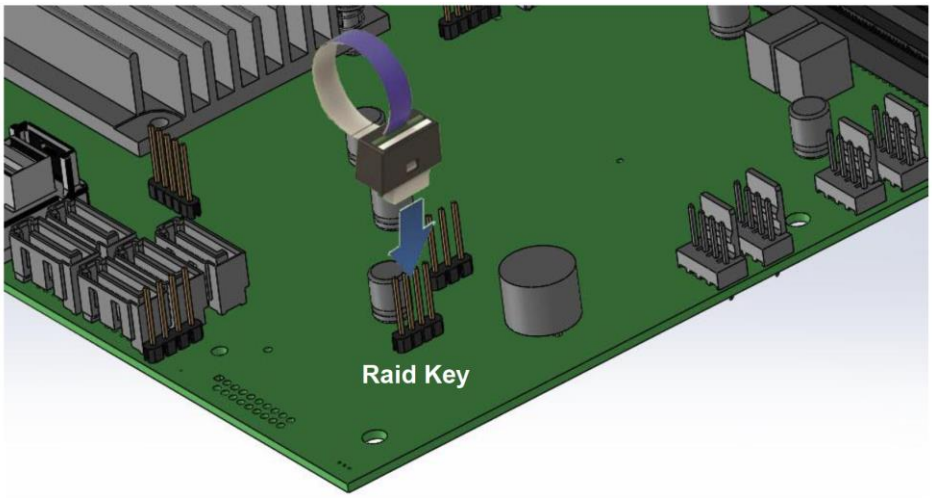


Рисунок 8-6. Ключ обновления SATA RAID 5

Встроенный разъем, используемый для обеспечения поддержки ключа обновления Intel® ESRT2 SATA RAID 5, также используется для поддержки параметров ключа обновления Intel® VROC (VMD NVMe RAID).

ПРИМЕЧАНИЕ: конфигурации RAID не могут охватывать оба встроенных контроллера AHCI SATA.

Intel® Embedded Сервер RAID Technology 2 на материнскойплате поддерживается максимум из шести дисков.

Бинарный драйвер включает частичные исходные файлы. Драйвер является полностью открытым исходным кодом с использованием уровня MDRAID в Linux*.

8.3. Сетевой интерфейс

Материнская плата оснащена четырьмя встроенными портами Ethernet. Кроме того, может быть установлена дополнительная переходная LAN-плата. Все встроенные порты Ethernet управляются контроллером Intel® Ethernet Connection 722. В этом разделе описаны оба интерфейса.

8.3.1. Встроенные порты Ethernet

На задней стороне серверной материнской платы расположены четыре порта Ethernet 1 Гбит. В программе настройки BIOS они обозначены как порты 1, 2, 3, 4.

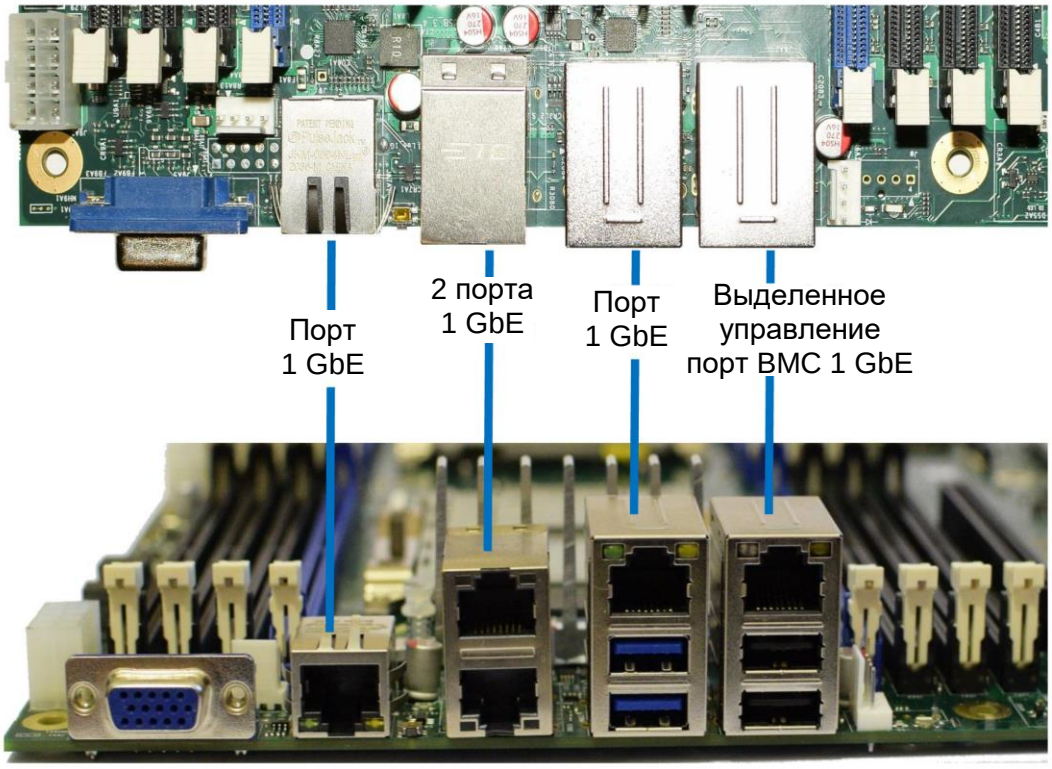


Рисунок 8-7. Разъемы сетевого интерфейса

Каждый порт Ethernet имеет два светодиода (см. Рисунок 8-8). Светодиод слева от разъема является светодиодом «Соединения/Активности (Link/Activity)» и указывает на сетевое соединение, когда он горит, и активность передачи/приема, когда мигает. Светодиод справа показывает скорость соединения (см. Таблица 54).

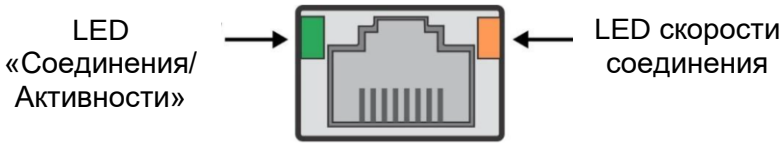


Рисунок 8-8. Внешний RJ45 сетевой интерфейс контроллера (NIC), определение LED

Таблица 54. Внешний сетевой интерфейс контроллера (NIC), Определение LED

Светодиод	Состояние светодиода	Состояние сетевой карты
Соединения/Активность (слева)	Выключено	Канал LAN не установлен
	Горит зеленым	Соединение LAN установлено
	Мигает зеленым	Передача или получение активности
Скорость соединения (справа)	Горит оранжевым	Поддерживаемая средняя скорость передачи данных (1 Гбит/с)
	Горит зеленым	Самая высокая поддерживаемая скорость передачи данных (10 Гбит/с)

8.3.2. Подключение переходной платы SFP + LAN

Материнская плата предлагает возможность подключения SFP + 10 Гбит/с через дополнительную переходную плату LAN. Сетевой контроллер интегрирован в концентратор контроллера платформы (PCH), а дополнительная переходная плата обеспечивает физический интерфейс.

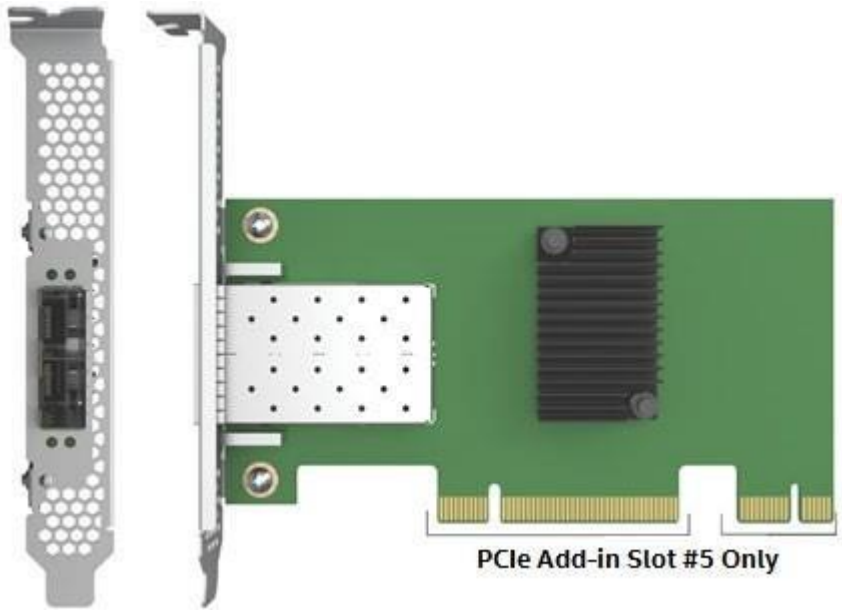


Рисунок 8-9. Переходная плата SFP + LAN

Подключение SFP + LAN Riser поддерживается только при установке в слот расширения PCIe №5 на материнской плате, который включает в себя разъем расширения, обеспечивающий связь со встроенными PCH и BMC.

Подключение SFP + LAN Riser можно использовать в однопроцессорных и двухпроцессорных конфигурациях.

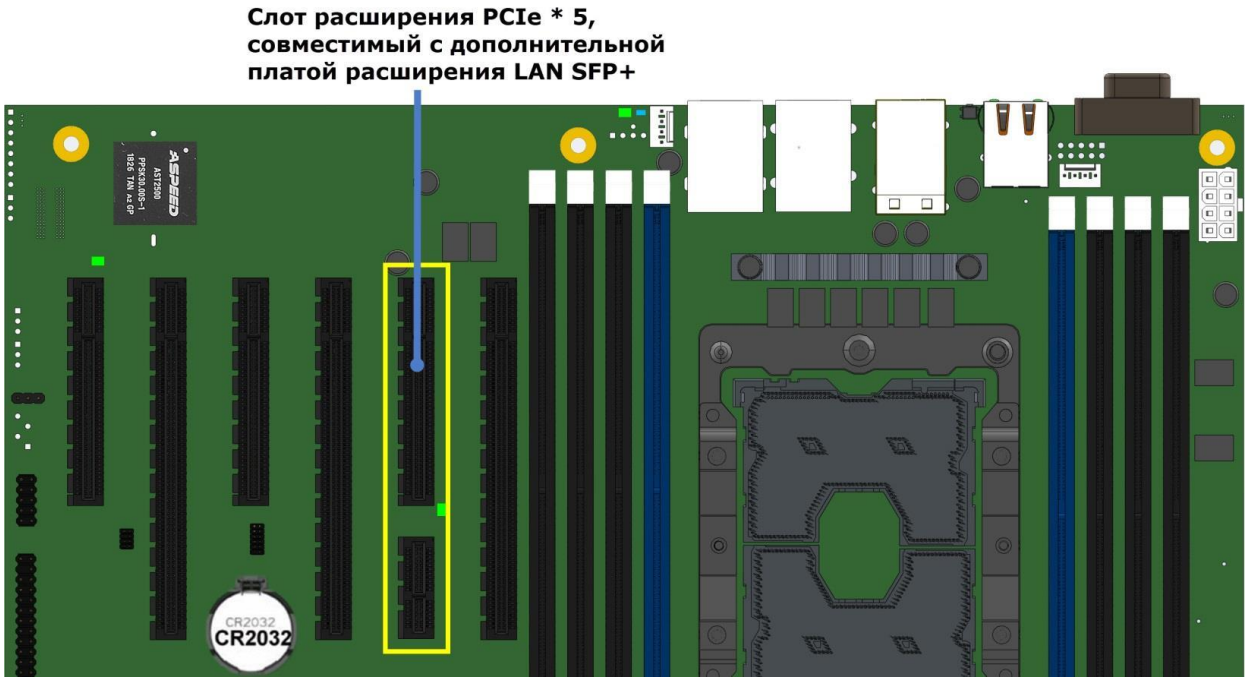


Рисунок 8-10. Поддержка дополнительной платы расширения LAN SFP+

Когда система включена, BIOS определяет наличие переходной платы SFP + LAN, включает сетевой контроллер в PCH и назначает порты LAN 5 и 6 разъемам переходной платы SFP+.

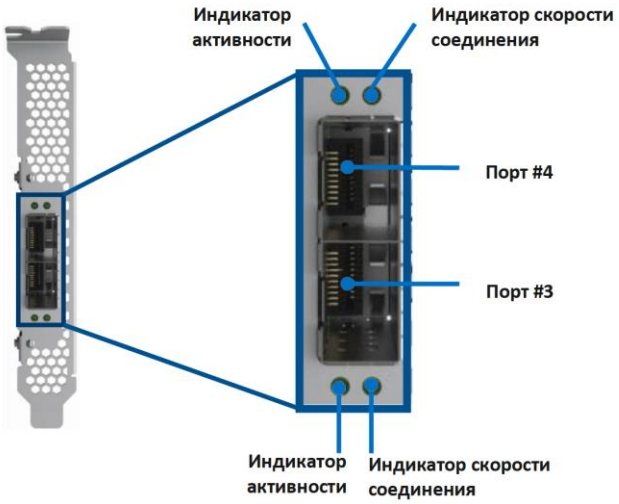


Рисунок 8-11. Индикация дополнительной платы расширения

Таблица 55. Описание индикаторов переходной платы SFP + LAN

Светодиод	Состояние светодиода	Состояние сетевой карты
Ссылка/действие (слева)	Выключено	Канал LAN не установлен
	Горит зеленым	Соединение LAN установлено
	Мигает зеленым	Передача или получение активности
Скорость соединения (справа)	Горит оранжевым	Низкая поддерживаемая скорость передачи данных (1 Гбит/с)
	Горит зеленым	Высокая поддерживаемая скорость передачи данных (10 Гбит/с)

Важно: в настройках BIOS всегда отображается 6 портов Ethernet. Для включения портов 5 и 6 требуется установить переходную плату LAN.

9. БЕЗОПАСНОСТЬ СИСТЕМЫ

Материнская плата поддерживает различные параметры безопасности системы, предназначенные для предотвращения несанкционированного доступа к системе или изменения настроек сервера. Поддерживаемые параметры безопасности системы включают:

- Защита паролем
- Блокировка передней панели
- Поддержка доверенного платформенного модуля (TPM)
- Технология Intel® Trusted Execution (Intel® TXT)

9.1. Настройка параметров безопасности в программе настройки BIOS

Утилита настройки BIOS Setup Utility <F2>, доступная во время POST, включает вкладку «Security» для настройки паролей, блокировки передней панели и настроек TPM. Меню «Security» предоставляет конфигурацию для настройки параметров безопасности системы:

Рисунок 9-1. Параметры безопасности настройки BIOS

Настройка BIOS	Опции	Описание
TPM Status (Статус TPM)	Нет	Описание статуса TPM

Настройка BIOS	Опции	Описание
TPM Operation (Работа TPM)	[Нет операции] [Отключить и деактивировать] [Включено и активно]	Включение/выключение функции TPM. Эта опция автоматически вернется в режим No-Operation
Supervisor Password (Пароль администратора)	Не установлен Введите пароль	Когда пароль не установлен, вам будет предложено ввести любой пароль Администратора
Clear PltKey On Reset (Очистить PltKey при перезагрузке)	Отключить/Включить	Включить/Выключить очистку ключа безопасности платформы при перезагрузке

9.2. Защита BIOS паролем

BIOS использует пароли для предотвращения несанкционированного доступа к настройке сервера. Пароли могут ограничивать доступ к настройке BIOS, ограничивать использование всплывающего меню загрузки и подавлять автоматическое изменение порядка устройств USB. Также есть возможность настроить требование пароля для загрузки системы. Если в настройке BIOS включена функция «Power-on password», BIOS останавливается в процессе POST, чтобы запросить пароль для продолжения.

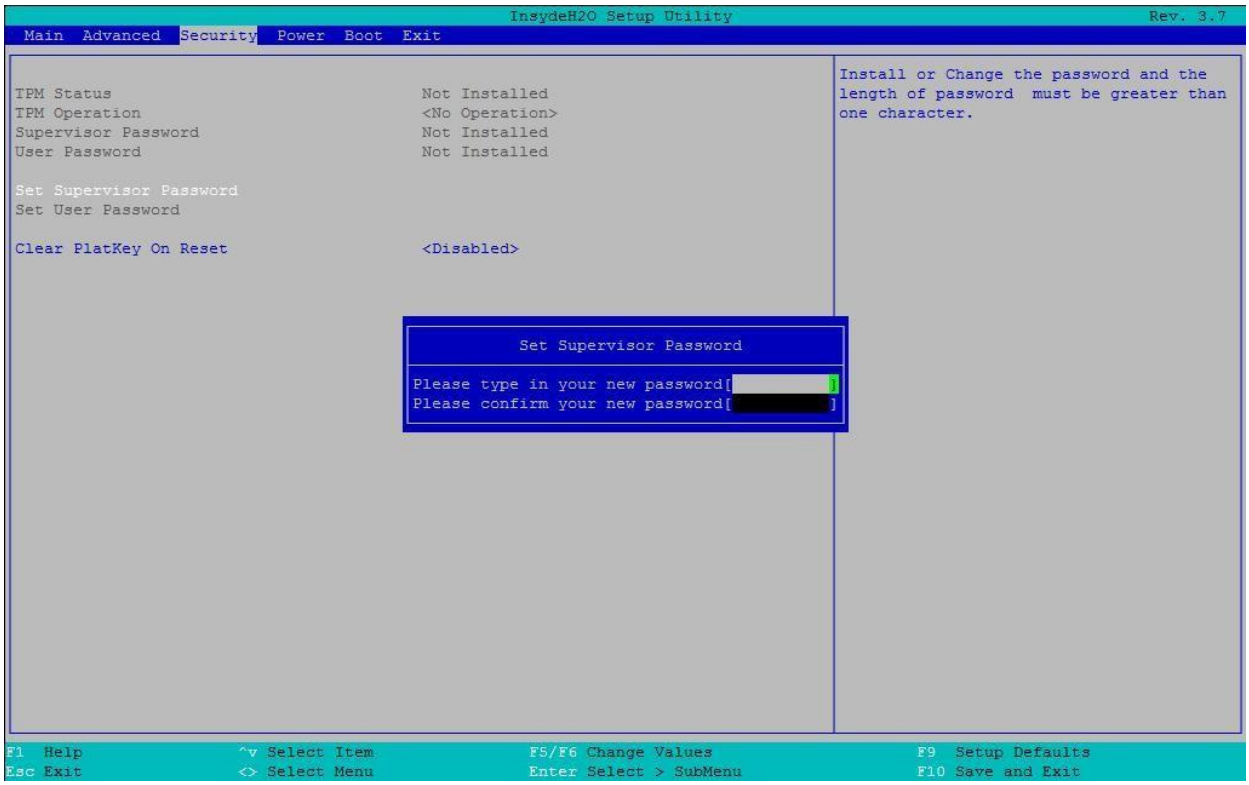


Рисунок 9-2. Установление пароля администратора

Пароли администратора (Supervisor) и пользователя (User) поддерживаются BIOS. Перед установкой пароля пользователя необходимо установить пароль администратора. Максимальная длина пароля — 14 символов. Пароль может состоять из буквенно-цифровых символов (az, AZ, 0–9) и чувствителен к регистру. Также разрешены некоторые специальные символы из следующего набора:

! @ # $% ^ & * () - _ + =?

Пароли администратора и пользователя должны отличаться друг от друга. При попытке ввести одинаковые пароли, выводится сообщение об ошибке. Приветствуется использование надежных паролей, но не обязательно. Надежный пароль состоит не менее чем из восьми символов и должен включать хотя бы по одному буквенному, числовому и специальному символу. Если вводится ненадежный пароль, перед его принятием отображается предупреждающее сообщение.

После установки пароль пользователя можно удалить, заменив его пустой строкой. Для этого требуется пароль администратора, и это должно быть сделано с помощью настройки BIOS или других явных средств изменения паролей. Удаление пароля администратора также удаляет пароль пользователя.

При необходимости пароли можно сбросить с помощью перемычки сброса пароля (см. Раздел 13). Сброс настроек конфигурации BIOS до значений по умолчанию (любым способом) не влияет на пароли администратора и пользователя.

Ввод пароля пользователя позволяет изменять только системное время и дату на главном экране настройки BIOS. Остальные поля можно изменить, только если был введен пароль администратора. Также может потребоваться пароль для входа в программу настройки BIOS, если он установлен.

Администратор имеет контроль над всеми полями настройки BIOS, включая возможность очистки пароля пользователя и пароля администратора.

Настоятельно рекомендуется установить, как минимум пароль администратора, чтобы каждый, кто загружает систему, не мог получить административный доступ. Если не установлен пароль администратора, любой пользователь может войти в программу настройки BIOS и изменить настройки BIOS по своему желанию.

Помимо ограничения доступа к большинству полей, при вводе пароля пользователя, накладывается ограничения на загрузку системы. Для простой загрузки в ранее определенном порядке пароль не требуется. Однако всплывающее меню загрузки, доступ к которому осуществляется путем ввода **<Esc>** во время POST, требует пароля администратора. См. Раздел 4.5.1 для получения дополнительной информации о всплывающем меню загрузки.

Кроме того, пароль пользователя не позволяет переупорядочивать USB, когда к системе подключено новое загрузочное устройство USB. Пользователю запрещена загрузка в любом другом порядке, кроме порядка загрузки, определенного администратором в настройках BIOS.

В качестве меры безопасности, во время загрузки, если пользователь или администратор вводит неправильный пароль три раза подряд, система переводится в состояние остановки. Для выхода из состояния остановки требуется сброс системы. Эта функция затрудняет угадывание или взлом пароля.

Кроме того, при следующей успешной перезагрузке диспетчер ошибок отображает код основной ошибки 0048 и регистрирует событие в SEL, чтобы предупредить авторизованного пользователя или администратора о том, что произошла ошибка доступа по паролю.

9.3. Поддержка доверенного платформенного модуля (TPM) (Опционально)

Опция Trusted Platform Module (TPM) — это аппаратное устройство безопасности, которое решает растущую проблему целостности процесса загрузки и предлагает лучшую защиту данных. TPM обеспечивает защиту от несанкционированного доступа, перед передачей управления операционной системе. Устройство TPM обеспечивает защищенное хранилище для хранения данных, например, ключей безопасности и паролей. Кроме того, TPM-устройство имеет функции шифрования и хеширования. В серверной материнской плате реализован TPM в соответствии с основной спецификацией TPM, уровень 2, версии 1.2, разработанной Trusted Computing Group (TCG).

Устройство TPM дополнительно устанавливается на 12-контактный разъем высокой плотности с надписью «TPM» на материнской плате. Устройство защищено от атак внешнего программного обеспечения и физической кражи.

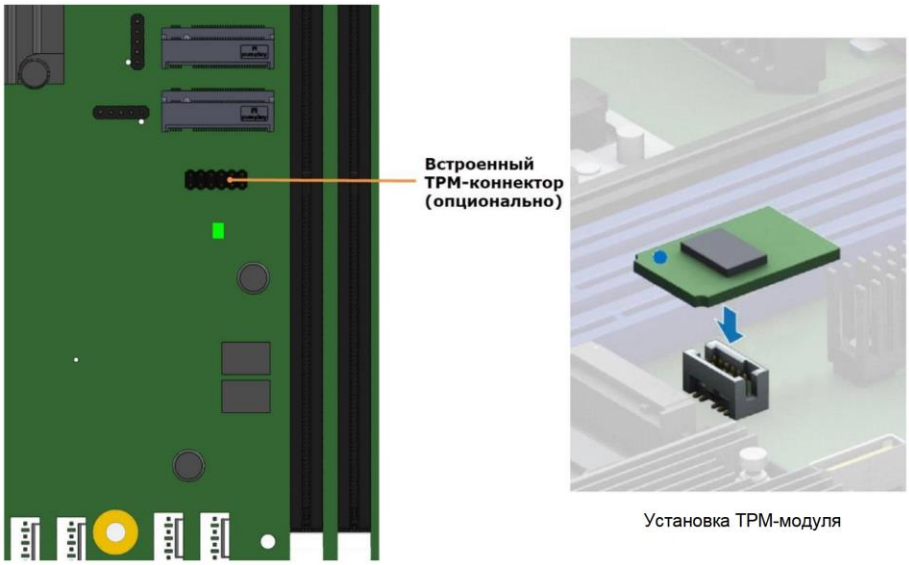


Рисунок 9-3. Встроенный разъем TPM

В предзагрузочной среде, такой как BIOS и загрузчик операционной системы, TPM используется для сбора и хранения уникальных измерений нескольких факторов в процессе загрузки для создания отпечатка системы. Этот уникальный отпечаток остается неизменным, если только в предзагрузочную среду не вмешиваются. Следовательно, он используется для сравнения с будущими измерениями для проверки целостности процесса загрузки.

После того, как BIOS завершит измерение процесса загрузки, он передает управление загрузчику операционной системы и, в свою очередь, операционной системе. Если операционная система поддерживает TPM, она сравнивает измерения TPM BIOS с показателями предыдущей загрузки, чтобы убедиться, что система не была изменена, прежде чем продолжить процесс загрузки операционной системы. После того, как операционная система запущена, она необязательно использует TPM для обеспечения дополнительной безопасности системы и данных. (Например, корпоративные версии Windows Vista * и более поздних версий поддерживают шифрование диска Windows * BitLocker *).

9.3.1. Безопасность BIOS TPM

Поддержка BIOS TPM удовлетворяет Спецификации реализации TCG PC Client для обычного BIOS, Спецификацию интерфейса физического присутствия TCG PC Client Platform и документы Microsoft Windows * BitLocker * Requirements. Роль BIOS для безопасности TPM включает в себя следующие функции.

- Измеряет и сохраняет процесс загрузки в микроконтроллере TPM, чтобы операционная система с поддержкой TPM могла проверить целостность загрузки системы.
- Обеспечивает расширяемый интерфейс встроенного ПО (EFI) и унаследованные интерфейсы для операционной системы с поддержкой TPM.
- Устройство TPM использует расширенный интерфейс конфигурации и питания (ACPI), что позволяет операционной системе с поддержкой TPM отправлять запросы административных команд TPM в BIOS.
- Проверяет физическое присутствие оператора. Подтверждает и выполняет запросы административных команд TPM операционной системы.
- Предоставляет параметры настройки BIOS для изменения состояний безопасности TPM и отмены контроля TPM.

Для получения дополнительных сведений см. Спецификацию реализации TCG PC Client для обычного BIOS, Спецификацию интерфейса физического присутствия TCG PC Client Platform и документы Microsoft Windows * BitLocker * Requirements.

9.3.2. Физическое присутствие

Для административных операций с TPM требуется, чтобы оператор указывал данные функции в контроле TPM или подтверждал физическое присутствие, чтобы подтвердить выполнение административных операций. В BIOS реализована индикация присутствия оператора путем проверки пароля администратора настройки BIOS.

Административная последовательность TPM, вызываемая из операционной системы, выполняется следующим образом:

1. Пользователь отправляет административный запрос TPM через программное обеспечение безопасности операционной системы.
2. Операционная система запрашивает у BIOS выполнение административной команды TPM с помощью методов ACPI TPM, а затем перезагружает систему.
3. BIOS проверяет физическое присутствие оператора и подтверждает команду.
4. BIOS выполняет административную команду TPM, запрещает вход в программу настройки BIOS и загружается непосредственно в операционную систему, которая запросила команду TPM.

9.3.3. Параметры настройки безопасности TPM

Настройка BIOS TPM позволяет оператору просматривать текущее состояние TPM и выполнять административные операции TPM. Для выполнения параметров администрирования TPM через настройку BIOS требуется проверка физического присутствия TPM.

Настройка BIOS TPM отображает текущее состояние TPM, см. Таблицу 56. Обратите внимание, что при использовании TPM операционная система или приложение с поддержкой TPM может изменить состояние TPM независимо от настройки BIOS. Когда операционная система изменяет состояние TPM, программа настройки BIOS отображает обновленное состояние TPM.

Таблица 56. Состояния TPM конфигурации безопасности BIOS

Состояние TPM	Описание
Включено и активировано	Включенное и активированное устройство TPM выполняет все команды, использующие функции TPM. Доступны операции безопасности TPM
Включено и деактивированно	Включенное и деактивированное устройство TPM не выполняет команды, использующие функции TPM. Операции безопасности TPM недоступны, за исключением настройки контроля TPM, которая разрешена, если еще не установлена
Отключено и активировано	Отключенное устройство TPM не выполняет команды, использующие функции TPM. Операции безопасности TPM недоступны
Отключено и деактивировано	Отключенное устройство TPM не выполняет команды, использующие функции TPM. Операции безопасности TPM недоступны

Используя настройку BIOS TPM, оператор может включать и выключать функции TPM и очищать содержимое контроля TPM. После того, как запрошенная операция настройки BIOS TPM будет выполнена, параметр вернется в состояние «**No operation**». Параметр «**Clear Ownership**» TPM в настройке BIOS позволяет оператору очистить ключ контроля TPM и позволяет оператору взять на себя управление системой с помощью TPM. Используйте этот параметр, чтобы очистить настройки безопасности для вновь инициализированной системы или очистить систему, для которой был утерян ключ безопасности контроля TPM.

Параметры административного управления TPM см. Таблицу 57.

Таблица 57. Административные элементы управления TPM конфигурации безопасности BIOS

Административный контроль TPM	Описание
Нет операции	Никаких изменений в текущем состоянии. Обратите внимание, что настройка BIOS по умолчанию возвращается к «Нет операции» при каждом цикле загрузки
Включить	Включает и активирует TPM
Выключить	Отключает и деактивирует TPM
Clear Ownership	Совершает проверку подлинности и возвращает TPM к заводскому состоянию по умолчанию

9.4. Технология Intel® Trusted Execution

Семейство процессоров Intel® Xeon® поддерживает технологию Intel® Trusted Execution (Intel® TXT), которая представляет собой надежную среду безопасности. Разработанный для защиты от программных атак, Intel® TXT интегрирует новые функции и возможности безопасности в процессор, набор микросхем и другие компоненты платформы. При использовании в сочетании с технологией виртуализации Intel®, Intel® TXT обеспечивает доверие на основе аппаратного обеспечения для ваших виртуальных приложений.

Эта аппаратная безопасность обеспечивает более безопасную вычислительную среду общего назначения, способную работать с широким спектром операционных систем и приложений, чтобы повысить безопасность и целостность конфиденциальной информации без ущерба для удобства использования платформы.

Для Intel® TXT требуется компьютерная система с включенной технологией виртуализации Intel® (как Intel® VT-x, так и Intel® VT-d), процессор с поддержкой Intel® TXT, набор микросхем и BIOS, модули аутентифицированного кода и совместимая с Intel® TXT среда измеряемого запуска (MLE). MLE может состоять из монитора виртуальной машины, ОС или приложения. Кроме того, Intel® TXT требует, чтобы система включала TPM v1.2, как определено *в основной спецификации TPM Trusted Computing Group, уровень 2, версия 1.2*.

Если данные условия обеспечиваются, то Intel® TXT можно включить или отключить в процессоре с помощью параметра настройки BIOS. Для получения общей информации о Intel® TXT посетите http://www.intel.com/technology/security/.

10. УПРАВЛЕНИЕ ПЛАТФОРМОЙ

Управление платформой поддерживается несколькими аппаратными и программными компонентами, интегрированными в материнскую плату, которые работают совместно для обеспечения:

- Функции системы управления: система питания, ACPI, управление сбросом системы, инициализация системы, интерфейс передней панели, журнал системных событий.
- Контроля различных датчиков платы и системы, регулирование температурных характеристик и производительности платформы для поддержания (по возможности) функциональности сервера в случае отказа компонентов и/или неблагоприятных условий окружающей среды.
- Отслеживание и уведомление о состоянии системы.
- Обеспечивает интерфейс для приложений программного обеспечения Intel® Server Management.

В этой главе представлен общий обзор функций управления платформой и функций, реализованных на материнской плате.

10.1. Обзор набора функций управления

В следующих разделах описаны функции, которые поддерживает встроенное микропрограммное обеспечение BMC. Поддержка и использование некоторых функций зависит от дополнительных компонентов и опций системного уровня, которые могут быть установлены.

10.1.1. Обзор функций IPMI 2.0

Контроллер управления основной платой (BMC) поддерживает следующие функции IPMI 2.0:

- Сторожевой таймер IPMI.
- Поддержка обмена сообщениями, включая передачу команд и поддержку пользователей/сеансов.
- Восстанавливать работоспособность сервера в автоматическом или ручном режиме, удаленная перезагрузка системы, включение/выключение питания, загрузка ISO-образов и обновление программного обеспечения.
- Прием и обработка событий от других подсистем платформы.
- Доступ к системным устройствам, заменяемым на месте (FRU), с помощью команд IPMI FRU.
- Ведение журнала системных событий (SEL), включая отслеживание серьезности события.
- Хранение и доступ к системным записям данных датчиков (SDR).
- Управление сенсорным устройством, мониторинг состояния системы и создание отчетности.
- IPMI-интерфейсы:
    - Хост-интерфейсы, включая программное обеспечение для управления системой (SMS) с поддержкой очереди приема сообщений и режимом управления сервером (SMM).
    - Интерфейс интеллектуальной шины управления платформой (IPMB).

- Интерфейс LAN, поддерживающий протокол IPMI-over-LAN (RMCP, RMCP +).

- Последовательный по LAN (SOL).
- Синхронизация состояния ACPI с изменениями состояния, предоставляемыми BIOS.
- Инициализация и самотестирование во время выполнения, включая предоставление результатов внешним объектам. См. Также Спецификацию интерфейса интеллектуального управления платформой второго поколения v2.0.

10.1.2. Обзор функций, не относящихся к IPMI

BMC поддерживает следующие функции, не связанные с IPMI.

- Обновление прошивки BMC.
- Отказоустойчивая загрузка (FRB), включая FRB2, поддерживаемую функцией сторожевого таймера.
- Обнаружение вторжения в корпус (в зависимости от поддержки платформы).
- Управление скоростью вентиляторов с SDR, мониторинг и поддержка резервирования вентиляторов.
- Мониторинг и поддержка резервирования источников питания.
- Поддержка вентиляторов с возможностью горячей замены.
- Тестовые команды для установки и диагностики сигналов состояния платформы.
- Коды диагностических звуковых сигналов для состояния неисправности.
- Хранение и извлечение глобального уникального идентификатора системы (GUID).
- Управление на передней панели, включая светодиодный индикатор состояния системы и светодиодный индикатор идентификатора корпуса (включается с помощью кнопки или команды на передней панели), безопасная блокировка определенных функций передней панели и мониторинг нажатия кнопок.
- Сохранение состояния питания.
- Анализ сбоев питания.
- Управление блоком питания, включая поддержку датчика блока питания и обработку условий отключения питания.
- Контроль за температурой DIMM с использованием алгоритма управления вентиляторами с обратной связью с мониторингом показаний температуры DIMM.
- Отправка и ответ на протоколы разрешения адресов (ARP) (поддерживаются встроенными сетевыми адаптерами).
- Протокол динамической конфигурации хоста (DHCP) (поддерживается встроенными сетевыми адаптерами).
- Поддержка управления температурным режимом интерфейса и управления окружающей средой платформы (PECI).
- Уведомление по электронной почте.
- Поддержка встроенного пользовательского интерфейса веб-сервера в наборе функций Basic Manageability.
- Улучшения встроенного веб-сервера.
  - Удобочитаемый SEL.
  - Дополнительная возможность настройки системы.

- Дополнительная возможность мониторинга системы.
- Встроенная клавиатура, видео и мышь (KVM).
- Улучшения перенаправления KVM.
  - Поддержка более высокого разрешения.
- Интегрированное перенаправление удаленного носителя.
- Поддержка облегченного протокола доступа к каталогам (LDAP).
- Улучшения в обеспечении и инвентаризации.
  - Экспорт данных инвентаризации/системной информации (частичная таблица SMBIOS).
- Поддержка управления для блоков питания, совместимых с шиной управления питанием (PMBus *) 1.2.
- Репозиторий данных BMC (функция области управляемых данных).
- Система контроля воздушного потока.
- Датчик общей совокупной температуры.
- Управление температурой памяти.
- Датчики вентилятора блока питания.
- Интеллектуальная перегрузка (SmaRT)/регулирование замкнутой системы (CLST).
- Холодное резервирование блоков питания.
- Обновление прошивки блока питания.
- Проверка совместимости блока питания.
- Улучшения надежности прошивки BMC.
- Мониторинг состояния системы управления BMC.

10.2. Возможности и функции управления платформой

10.2.1. Подсистема питания

Серверная плата поддерживает несколько источников управления питанием, которые могут инициировать включение или выключение питания, см. Таблица 58.

Таблица 58. Источники управления питанием

Источник	Имя внешнего сигнала или внутренняя подсистема	Возможность
Кнопка питания	Кнопка питания на передней панели	Включает или выключает питание
Сторожевой таймер BMC	Внутренний BMC-таймер	Выключает питание или цикл питания
Команды управления шасси BMC	Направлено через командный процессор	Включает или выключает питание или цикл питания

Источник	Имя внешнего сигнала или внутренняя подсистема	Возможность
Сохранение состояния питания	Реализуется посредством внутренней логики BMC	Включает питание при возобновлении подачи переменного тока
Чипсет	Спящий сигнал S4/S5 (такой же, как POWER_ON)	Включает или выключает питание
CPU Thermal	CPU-Thermtrip	Отключает питание
PCH Thermal	PCH Thermtrip	Отключает питание
WOL (пробуждение по локальной сети) LAN		Включает питание

10.2.2. Расширенный интерфейс настройки и питания (ACPI)

Материнская плата поддерживает состояния Advanced Configuration and Power Interface (ACPI), см. Таблица 59.

Таблица 59. Состояния питания ACPI

Состояние	Поддерживается	Описание
S0	Да	Работает. Индикатор питания на передней панели горит (не контролируется BMC). Вентиляторы вращаются с нормальной скоростью, определяемой сигналами датчиков. Кнопки на передней панели работают нормально
S1	Нет	Не поддерживается
S2	Нет	Не поддерживается
S3	Нет	Не поддерживается
S4	Нет	Не поддерживается

Состояние	Поддерживается	Описание
S5	Да	Мягкое отключение. Кнопки на передней панели не заблокированы. Вентиляторы остановлены. Процесс включения происходит в обычном режиме загрузки. Кнопки питания, сброса, немаскируемого прерывания (NMI) на передней панели и кнопки ID разблокированы

Во время инициализации системы и BIOS, и BMC инициализируют функции, подробно описанные в следующих разделах.

10.2.2.1. Процессор Tcontrol

Процессоры, используемые с этим набором микросхем, могут реализовать функцию под названием Tcontrol, которая обеспечивает регулировку в поведении вентиляторов, чтобы достичь оптимального охлаждения и шума. BMC считывает температуру CPU через PECI прокси — механизм, предусмотренный в Intel® Management Engine (Intel® ME). BMC использует эти значения в алгоритме контроля скорости вентилятора.

10.2.2.2. 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. Серверная платформа поддерживают только FRB-2 с использованием команд сторожевого таймера.

FRB-2 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 FRB-2 процесса загрузки.

После того, как BIOS идентифицировал и сохранил информацию BSP, он устанавливает бит использования таймера FRB-2 и загружает сторожевой таймер с новым интервалом тайм-аута.

Если сторожевой таймер истекает, когда на FRB бит использования сторожевого таймера ещё установлен, BMC (если он соответствующе настроен) регистрирует событие обнуления сторожевого таймера, устанавливая значение тайм-аут FRB-2 в байтах данных события. Затем BMC выполняет аппаратный сброс системы, если в качестве реакции на тайм-аут сторожевого таймера в BIOS установлена перезагрузка.

BIOS отвечает за отключение тайм-аута FRB-2 перед запуском сканирования дополнительного ПЗУ и перед отображением запроса пароля для загрузки. Если процессор выходит из строя и вызывает тайм-аут FRB-2, BMC перезагружает систему.

BIOS получает от BMC статус сторожевого таймера. Если в статусе отображается истекший таймер FRB-2, BIOS регистрирует сбой в журнале системных событий (SEL). В записи байтов OEM в SEL записывается последний код POST, сгенерированный во время предыдущей попытки загрузки. Отказ FRB-2 не отражается на показании датчика состояния процессора.

Отказ FRB2 не влияет на светодиоды на передней панели.

10.2.2.3. Отображение почтового индекса

BMC, получив резервное питание, инициализирует внутреннее оборудование для отслеживания записей через порт 80 (код POST). Данные, записанные в порт 80, выводятся на системные светодиоды POST.

BMC отключит светодиоды POST после завершения POST.

10.2.3. Контрольный счетчик

BMC реализует сторожевой таймер, полностью совместимый с IPMI 2.0. Дополнительные сведения см. В спецификации интерфейса интеллектуального управления платформой второго поколения v2.0. Немаскируемое/диагностическое прерывание, определенное для сторожевого таймера IPMI 2.0 связано с NMI. Прерывание SMI перед тайм-аутом сторожевого таймера или генерация аналогичного сигнала не поддерживается.

10.2.4. Журнал системных событий (SEL)

BMC реализует журнал системных событий, как указано в спецификации интерфейса интеллектуального управления платформой версии 2.0. Доступ к SEL производится независимо от состояния питания системы, через внутренние или внеполосные интерфейсы BMC, доступ к информации системного журнала можно получить даже если сервер выключен.

BMC выделяет 95 231 байт (примерно 93 кБ) энергонезависимой памяти для хранения системных событий. Одновременно можно сохранить до 3639 записей SEL. Поскольку SEL является циклическим, любая команда, которая приводит к переполнению SEL за пределами выделенного пространства, перезаписывает самые старые записи в SEL, при установленном флаге переполнения.

10.3. Мониторинг датчиков

BMC контролирует оборудование системы и сообщает о состоянии датчиков. Информация, собранная с физических датчиков, транслируется в датчики IPMI. BMC также сообщает о различных изменениях в состоянии системы, поддерживая виртуальные датчики, которые специально не привязаны к физическому оборудованию. В этом разделе описываются общие аспекты управления датчиками BMC, а также описывается, как моделируются определенные типы датчиков. Если не указано иное, термин датчик относится к определению датчика модели IPMI.

- Сенсорное сканирование.
- Датчики BIOS только для событий.
- Датчики.
- Сторожевой датчик IPMI.
- Сторожевой датчик BMC.
- Мониторинг работоспособности управления системой BMC.
- Сторожевой таймер VR.
- Система воздушного потока.
- Датчики контроля вентилятора.
- Датчики теплового контроля.
- Датчики контроля напряжения.
- Датчик CATERR.

- Мониторинг событий привязки LAN.
- CMOS-мониторинг батареи.
- Датчик NMI (диагностическое прерывание).

10.3.1. Поведение при повторном включении датчика

Датчики могут быть ручными или автоматическими. Датчик автоматического повторного включения сбрасывает состояние события для порога или смещения, если этот порог или смещение изменяются после подтверждения. Это позволяет генерировать новое событие и связанный побочный эффект. Примером побочного эффекта является увеличение скорости вентиляторов из-за превышения верхнего критического порога датчика температуры. Состояние события и состояние входа (значение) датчика отслеживают друг друга. Большинство датчиков повторно активируются автоматически.

Датчик ручного повторного включения не сбрасывает состояние подтверждения, даже когда порог или смещение сбрасываются. В этом случае состояние события и состояние входа (значение) датчика не отслеживают друг друга. Состояние утверждения события стабильное. Для повторного включения датчика можно использовать следующие методы:

- Автоматическое повторное включение — применяется только к датчикам, которые обозначены как автоматическое повторное включение.
- Команда IPMI — событие повторного включения датчика.
- Внутренний метод BMC — BMC может повторно активировать определенные датчики из состояния триггера. Например, некоторые датчики могут быть повторно активированы сбросом системы. Сброс BMC повторно активирует все датчики.
- Сброс системы или цикла питания постоянного тока повторно активирует все датчики вентиляторной системы.

10.3.2. Температурный мониторинг

BMC обеспечивает мониторинг устройств измерения температуры компонентов и платы. Эта возможность мониторинга реализуется в виде аналоговых/пороговых или дискретных датчиков IPMI, в зависимости от характера измерения.

Для аналоговых/пороговых датчиков, за исключением датчиков температуры процессора, критические и некритические пороги (верхний и нижний) устанавливаются с помощью SDR, а генерация событий включена как для событий подтверждения, так и для событий отмены.

Для дискретных датчиков разрешена генерация как подтверждения, так и отмены подтверждения.

Обязательный мониторинг термодатчиков платформы включает:

- Температура на входе (физический датчик обычно находится на передней панели системы или объединительной панели жесткого диска (HDD)).
- Датчики температуры окружающей среды.
- Температура процессора.
- Температура памяти (DIMM).
- Горячий мониторинг CPU Voltage Regulator-Down (VRD).
- Температура на входе блока питания (БП) (поддерживается только для блоков питания, совместимых с PMBus*).

Кроме того, микропрограммное обеспечение BMC может создавать виртуальные датчики, основанные на комбинации или агрегировании нескольких физических тепловых датчиков

и приложений математической формулы к показаниям теплового датчика или датчика мощности.

10.4. Стандартное управление вентиляторами

BMC контролирует системные вентиляторы. Каждый вентилятор связан с датчиком скорости вентилятора, который определяет отказ вентилятора, а также может быть связан с датчиком присутствия вентилятора для поддержки горячей замены. Для конфигураций с резервированием вентилятора отказ вентилятора и его состояние определяет состояние датчика резервирования вентилятора.

Системные вентиляторы разделены на домены, каждый из которых имеет отдельный сигнал управления скоростью вентиляторов и отдельную настраиваемую политику управления вентиляторами. Домен вентиляторов может иметь набор связанных с ним датчиков температуры и вентиляторов. Они используются для определения текущего состояния домена вентилятора.

Домен имеет три состояния: спящий, ускоренный и номинальный. Состояния сна и ускорения имеют фиксированные (но настраиваемые с помощью OEM SDR) скорости вращения вентилятора, связанные с ними. Номинальное состояние имеет переменную скорость, определяемую политикой вентиляторной области. Запись OEM SDR используется для настройки политики вентиляторного-домена.

Состояние вентиляторного-домена контролируется несколькими факторами. Факторы для изменения состояния перечислены ниже в порядке приоритета, от высокого к низкому.

- Связанный вентилятор находится в критическом состоянии или отсутствует. SDR описывает, какие домены вентиляторов увеличиваются в ответ на отказ вентиляторов или их удаление в каждом домене. Если вентилятор снимается, когда система находится в режиме отключения вентиляторов, он не обнаруживается, и не происходит никаких изменений, пока система не выйдет из режима отключения вентиляторов.
- Любой связанный датчик температуры находится в критическом состоянии. SDR описывает, какие нарушения температурного порога вызывают ускорение вентилятора для каждой области вентилятора.
- BMC находится в режиме обновления микропрограммы или работающая микропрограмма повреждена.

Если применяется какое-либо из вышеперечисленных условий, вентиляторы устанавливаются на фиксированную скорость ускоренного режима.

Номинальная скорость вентилятора в области вентилятора может быть сконфигурирована как статическая (фиксированное значение) или контролироваться состоянием одного или нескольких связанных датчиков температуры.

10.4.1. Вентиляторы с горячей заменой

Поддерживаются вентиляторы с горячей заменой, которые можно снимать и заменять, пока система включена и работает. BMC реализует датчики присутствия вентилятора для каждого вентилятора с возможностью горячей замены.

Когда вентилятор отсутствует, соответствующий датчик скорости вентилятора переводится в состояние чтения/недоступности, а любые связанные области вентиляторов переводятся в состояние ускорения. Вентиляторы могут уже быть увеличены из-за предыдущего отказа вентилятора или его снятия.

При замене снятого вентилятора соответствующий датчик скорости вентилятора повторно активируется. Если нет других критических условий, вызывающих условие ускорения вентиляторов, скорость вентиляторов возвращается к номинальному состоянию.

Выключение и включение питания или сброс системы повторно активирует датчики скорости вращения вентилятора, если состояние отказа все еще присутствует, режим ускорение возвращается после повторной инициализации датчика и обнаружения нарушения порога.

10.4.1.1. Мониторинг резервных вентиляторов

BMC поддерживает резервный мониторинг вентиляторов и реализует датчик резервирования вентиляторов. Датчик резервирования вентиляторов генерирует события, когда связанный с ним набор вентиляторов переходит из состояния резервирования в состояние без резервирования, что определяется количеством и состоянием вентиляторов. Определение резервирования вентиляторов зависит от конфигурации. BMC позволяет настраивать избыточность для каждого датчика вентилятора с помощью записей OEM SDR.

Число отказов вентиляторов или удаление вентиляторов с горячей заменой не превышающее количество резервных вентиляторов, указанного в SDR в конфигурации вентиляторов, является некритичным отказом и отражается на состоянии передней панели. Отказ вентиляторов или их удаление, превышающее количество резервных вентиляторов, является нефатальным состоянием при недостаточных ресурсах и отражается в состоянии передней панели как нефатальная ошибка.

Резервирование проверяется только тогда, когда система находится во включенном состоянии с питанием от постоянного тока. Изменения резервирования вентиляторов, которые происходят, когда система отключена от постоянного тока или, когда отключается переменный ток, не регистрируются, пока система не будет включена.

10.4.2. Области вентиляторов

Скорость вращения системных вентиляторов регулируется с помощью сигналов широтно-импульсной модуляции (ШИМ), которые управляются отдельно для каждой области с помощью встроенного оборудования ШИМ. Скорость вентилятора изменяется путем регулировки рабочего цикла, который представляет собой процент времени, в течение которого сигнал достигает высокого уровня в каждом импульсе.

BMC контролирует средний рабочий цикл каждого сигнала ШИМ путем непосредственного управления встроенными регистрами управления ШИМ. Одно и то же устройство может управлять несколькими сигналами ШИМ.

10.4.3. Температурный и акустический менеджмент

Эта функция относится к усовершенствованному управлению вентиляторами для оптимального охлаждения системы при одновременном снижении уровня шума, создаваемого вентиляторами системы. Стандарты агрессивной акустики могут потребовать компромисса между скоростью вращения вентиляторов и параметрами производительности системы, которые влияют на требования к охлаждению, в первую очередь пропускной способности памяти. BIOS, BMC и SDR работают вместе, чтобы обеспечить контроль над определением этого компромисса.

Эта возможность требует от BMC доступа к датчикам температуры на отдельных модулях памяти DIMM. Кроме того, регулирование температуры с обратной связью поддерживается только для модулей DIMM с датчиками температуры.

10.4.4. Вход термодатчика для управления скоростью вентилятора

BMC использует различные датчики IPMI для управления скоростью вращения вентилятора. Некоторые из датчиков являются IPMI-моделями реальных физических датчиков, тогда как некоторые являются виртуальными датчиками, значения которых

получаются из физических датчиков с использованием расчетов и/или табличной информации.

Следующие термодатчики IPMI используются для контроля скорости вентилятора:

- Датчики температуры воздуха на входе.
- Цифровой термодатчик процессора (DTS) — датчики запаса прочности.
- Датчики теплового запаса DIMM.
- Датчик температуры воздуха на выходе.
- Датчик температуры PCH.
- Датчики общего теплового запаса.
- Датчик температуры SSB (набор микросхем Intel® C620).
- Встроенные датчики температуры контроллера Ethernet (поддержка этого зависит от используемого контроллера Ethernet).
- Встроенные датчики температуры контроллера SAS (при наличии).
- Датчик температуры CPU VR.
- Датчик температуры DIMM VR.
- Датчик температуры BMC.
- Датчик температуры DIMM VRM.

Рисунок 10-1 показывает высокоуровневое представление структуры управления скоростью вентилятора, которая определяет скорость вентилятора.

Рисунок 10-1. Процесс управления скоростью вентилятора высокого уровня

10.4.4.1. Повышение скорости вентилятора из-за отказа вентилятора

Каждый сбой вентилятора может определять уникальный ответ от всех других вентиляторных доменов. Таблица OEM SDR определяет реакцию каждого домена вентиляторов на основании отказа любого вентилятора, включая вентиляторы системы и

блока питания (только для блоков питания, совместимых с PMBus *). Это означает, что, если в системе шесть вентиляторов, существует шесть различных реакций вентилятора на отказ.

10.5. Управление температурой памяти

Системная память является наиболее сложной подсистемой для термического управления, поскольку она требует существенного взаимодействия между BMC, BIOS и аппаратным обеспечением контроллера встроенной памяти. В этом разделе представлен обзор возможности управления с точки зрения BMC.

10.5.1. Регулирование температуры памяти

Система поддерживает управление температурой за счет Closed Loop Thermal Throttling (CLTT). Уровни смещения изменяются динамически в зависимости от теплового режима памяти и системы, определяемого системой, мощностью и тепловыми параметрами DIMM. Функция управления скоростью вентилятора BMC связана с используемым механизмом регулирования памяти.

Для различных параметров регулирования памяти используется следующая терминология:

- Статический Closed-Loop Thermal Throttling (Static-CLTT): CLTT-регистры будут сконфигурированы с помощью BIOS Memory Reference Code (MRC) во время процедуры POST. Смещение уровней CLTT будет работать, в замкнутом контуре системы с температурным датчиком DIMM в качестве управлющего входа. Во время работы системы регулирование смещения не будет производиться.
- Динамический Closed-Loop Thermal Throttling (Dynamic-CLTT): CLTT-регистры будут сконфигурированы с помощью BIOS MRC во время процедуры POST. Дросселирование памяти будет работать, в замкнутом контуре системы с температурным датчиком DIMM в качестве управлющего входа. Регулировка смещения выполняется во время работы в зависимости от изменений в охлаждении системы (скорости вращения вентиляторов).

Серверная система QTECH серии QSRV E-R/P-R, имеющая модули DIMM с термодатчиками и использующая семейство масштабируемых процессоров Intel® Xeon®, поддерживает тип CLTT, называемый Hybrid-CLTT. При режиме Hybrid-CLTT встроенный контроллер памяти оценивает температуру DRAM между фактическими считываниями TSOD. Таким образом, термины Dynamic-CLTT и Static-CLTT относятся к этому «гибридному» режиму. Обратите внимание, что, если опрос TSOD, выполняемый IMC, прерывается, показания температуры, которые BMC получает от IMC, будут являться оценочными значениями.

10.5.2. Динамический (гибридный) CLTT

Система будет поддерживать динамический CLTT, для которого микропрограмма BMC динамически изменяет регистры теплового смещения в IMC во время работы на основе изменений в охлаждении системы (скорости вращения вентиляторов). Для статического CLTT к показанию TSOD применяется фиксированное значение смещения; однако это не дает таких точных результатов, как если бы смещение учитывало текущий воздушный поток через модуль DIMM, как это делается с динамическим CLTT.

Для поддержки этой функции BMC определяет скорость воздуха для каждой области вентиляторов на основе значения ШИМ, установленного для области. Поскольку эта связь зависит от конфигурации шасси, необходимо использовать метод, поддерживающий эту зависимость (например, через OEM SDR), который устанавливает таблицу поиска, обеспечивающую эту связь.

В BIOS имеется встроенная справочная таблица, которая предоставляет значения теплового смещения для каждого типа DIMM и настройки диапазона скорости воздуха (поддерживаются три диапазона скорости воздуха). Во время загрузки системы BIOS предоставит BMC три значения смещения (соответствующие трем диапазонам скорости воздуха) для каждого включенного модуля DIMM. Используя эти данные, микропрограммное обеспечение BMC составляет таблицу, в которой отображается значение смещения, соответствующее заданному диапазону скорости воздуха для каждого модуля DIMM. Во время работы BMC применяет алгоритм усреднения для определения целевого значения смещения, соответствующего текущей скорости воздуха, а затем BMC записывает это новое значение смещения в регистр теплового смещения IMC для DIMM.

10.6. Шина управления питанием (PMBus *)

Шина управления питанием (PMBus *) — это открытый стандартный протокол, основанный на SMBus * 2.0. Он определяет средства связи с преобразователями мощности и другими устройствами электропитания с помощью команд на основе SMBus *. В системе должны быть установлены блоки питания, соответствующие PMBus *, чтобы контролировать их состояние и/или измерения мощности.

Для получения дополнительной информации о PMBus * посетите веб-сайт форума по интерфейсу системного управления http://www.powersig.org/.

10.6.1. Управление светодиодом неисправности компонента

Серверная плата поддерживает несколько наборов светодиодных индикаторов неисправности компонентов. Для облегченной диагностики см. Рисунок 4-4. Некоторые светодиоды принадлежат BMC, а некоторые — BIOS.

- Индикаторы неисправности DIMM — BMC управляет аппаратным обеспечением индикаторов неисправности DIMM. Эти светодиоды отражают состояние датчиков событий, принадлежащих BIOS. Когда BIOS обнаруживает неисправное состояние модуля DIMM, он посылает IPMI OEM-команды (набор индикации о неисправности) к BMC, чтобы инструктировать BMC на включение соответствующей DIMM LED неисправности. Эти светодиоды активны только тогда, когда система находится во включенном состоянии. BMC не активирует и не изменяет состояние светодиодов, если это не указано в BIOS.
- Индикаторы состояния жесткого диска — HSBP PSoC * управление этими светодиодами, если они есть, и определение состояния неисправности/исправности дисков, которое отражают светодиоды, производится шасси QTECH или оборудованием стороннего производителя.
- Индикаторы неисправности CPU — на материнской плате имеется индикатор неисправности для каждого сокета процессора, управляемый BMC. Светодиод горит, если есть несоответствие MSID, когда номинальная мощность процессора несовместима с платой.

Таблица 60. Светодиоды неисправности компонентов

Составная часть	Владелец	Состояние	Описание
Светодиод неисправности DIMM	BMC	Горит желтым	Сбой памяти — обнаружен BIOS
		Выключено	DIMM работает правильно
Светодиод неисправности HDD	HSBP PSoC*	Горит желтым	Неисправность жесткого диска
		Мигающий желтый	Прогнозирование сбоев, восстановление, выявление
		Выключено	Хорошо (ошибок нет)
Светодиоды неисправности CPU	BMC	Горит желтым	Несоответствие MSID
		Выключено	Хорошо (ошибок нет)

11. СТАНДАРТНЫЕ ФУНКЦИИ УПРАВЛЕНИЯ СЕРВЕРОМ

Встроенный BMC поддерживает стандартные функции управления сервером, доступные по умолчанию (см. Таблица 61).

Таблица 61. Стандартные функции управления сервером

Особенность	Стандарт
Поддержка функций IPMI 2.0	✓
Внутрисхемное обновление прошивки BMC	✓
FRB2	✓
Обнаружение вторжения в корпус	✓
Контроль резервирования вентиляторов	✓
Поддержка вентилятора с горячей заменой	✓
Акустический менеджмент	✓
Поддержка диагностического звукового кода	✓
Сохранение состояния питания	✓
Поддержка протокола разрешения адресов (ARP)/протокола динамической конфигурации хоста (DHCP)	✓
Поддержка терморегулирования PECI	✓
Уведомление по электронной почте	✓
Встроенный веб-сервер	✓
Поддержка безопасной оболочки (SSH)	✓
Встроенная клавиатура, видео и мышь (KVM)	✓
Интегрированное перенаправление удаленного мультимедиа	✓
Облегченный протокол доступа к каталогам (LDAP)	✓

Особенность	Стандарт
Поддержка Intel® Intelligent Power Node Manager	✓

11.1. Выделенный порт управления

Материнская плата содержит выделенный порт управления RJ45 1 ГБ (см. Рисунок 8-7).

11.2. Встроенный веб-сервер

Стандартную управляемость BMC обеспечивает встроенный веб-сервер и настраиваемый OEM-интерфейс, которые предоставляют возможности управления базовым набором функций BMC. веб-интерфейс поддерживается всеми встроенными сетевыми адаптерами, которые имеют возможность управления BMC, а также выделенным порт управления. Поддерживаются как минимум два одновременных веб-сеанса от двух разных пользователей. Встроенный пользовательский веб-интерфейс поддерживается следующими клиентскими веб-браузерами:

- Microsoft Edge *
- Microsoft Internet Explorer *
- Mozilla Firefox *
- Mozilla Firefox *
- Google Chrome *
- Safari *

Встроенный пользовательский веб-интерфейс поддерживает строгую безопасность — аутентификацию, шифрование и поддержку брандмауэра, поскольку он позволяет удаленно настраивать сервер и управлять им. Поддерживается шифрование с использованием до 256-битного уровня защищенных сокетов (SSL). Аутентификация пользователя основана на идентификаторе пользователя и пароле.

Интерфейс, предоставляемый встроенным веб-сервером, аутентифицирует пользователя перед тем, как разрешить инициировать веб-сеанс. Веб-интерфейс также предоставляет точку запуска для таких функция, как клавиатура, видео и мышь (KVM) и перенаправление мультимедиа.

Функции веб-интерфейса:

- Включение, выключение и перезагрузка сервера, а также отображение текущего состояния питания.
- Отображение информации о версии BIOS, BMC, ME и SDR.
- Отображение общего состояния системы.
- Настройка различных параметров IPMI через LAN для IPV4 и IPV6.
- Настройка оповещения по (SNMP и SMTP).
- Отображение информации об активах системы для продукта, платы и шасси.
- Отображение датчиков, принадлежащих BMC (имя, состояние, текущие показания, включенные пороги), включая состояние датчиков с цветовым кодом.
- Предоставляет возможность фильтровать датчики в зависимости от типа датчика (напряжение, температура, вентилятор и источник питания).
- Автоматическое обновление данных датчика.

- Поддержка основных стандартных браузеров (Microsoft Internet Explorer * и Mozilla Firefox *).
- Предоставляет встроенную функцию отладки платформы, позволяющую пользователю инициировать «отладочный дамп» в файл.
- Эмулирует виртуальную переднюю панель с той же функциональностью, что и локальная передняя панель. Отображаемые светодиоды соответствуют текущему состоянию светодиодов локальной панели. Отображаемые кнопки (например, кнопка питания) можно использовать так же, как и локальные кнопки.
- Отображение данных датчика ME. Отображаются только датчики, для которых загружена связанность с SDR.
- Принудительное подключение HTTPS для большей безопасности.
- Отображение информации о процессоре и памяти, доступной в IPMI через LAN.
- Отображение мощности, потребляемой сервером.
- Просмотр и настройка параметров VLAN.
- Предупреждение пользователя, что изменение конфигурации IP-адреса вызовет отключение.
- Принудительный вход в настройки BIOS при сбросе (управление питанием сервера).

11.3. Поддержка функций управления

Встроенный контроллер управления материнской платой (BMC) поддерживает функции управления, удобный удаленный доступ с клавиатуры, видео и мыши (KVM) и управление через локальную сеть и Интернет. Он захватывает, оцифровывает и сжимает видео, а также передает с его помощью сигналы клавиатуры и мыши на удаленный компьютер и обратно. Программное обеспечение для удаленного доступа и управления работает во встроенном контроллере управления материнской платой.

Ключевые особенности:

- **Перенаправление KVM** либо с выделенной управляющей сетевой карты, либо с сетевых карт серверной материнской платы, используемых для управления трафиком до двух сеансов KVM. KVM автоматически определяет разрешение видео для получения наилучшего снимка экрана, высокопроизводительного отслеживания мыши и синхронизации. Он позволяет удаленно просматривать и настраивать параметры POST и BIOS перед загрузкой.
- **Перенаправление носителей**, позволяющее системным администраторам или пользователям подключать удаленную среду IDE или USB CDROM, дисковод гибких дисков или флеш-накопитель USB в качестве удаленного устройства на сервере. После подключения удаленное устройство представляется серверу как локальное устройство, позволяя системным администраторам или пользователям устанавливать программное обеспечение (включая операционные системы), копировать файлы, обновлять BIOS или загружать сервер с этого устройства.

11.3.1. Перенаправление клавиатуры, видео и мыши (KVM)

Прошивка BMC поддерживает перенаправление клавиатуры, видео и мыши (KVM) по локальной сети. Клиентская система должна иметь Java Runtime Environment (JRE) версии 6.0 или более поздней для запуска KVM или апплетов перенаправления мультимедиа.

BMC поддерживает встроенное приложение KVM (удаленная консоль), которое можно запускать со встроенного веб-сервера. Поддерживается перенаправление мыши и клавиатуры на базе USB 1.1, USB 2.0. Также можно использовать сеанс перенаправления

KVM одновременно с перенаправлением мультимедиа. Эта функция позволяет пользователю интерактивно использовать функции клавиатуры, видео и мыши удаленного сервера, как если бы пользователь физически находился у управляемого сервера.

Перенаправление KVM включает функцию программной клавиатуры, используемую для имитации клавиатуры, подключенной к удаленной системе. Функциональная клавиатура поддерживает следующие раскладки: английский, голландский, французский, немецкий, итальянский, русский и испанский.

Функция перенаправления KVM автоматически определяет разрешение видео для наилучшего захвата экрана и обеспечивает высокопроизводительное отслеживание и синхронизацию мыши. KVM позволяет удаленно просматривать и настраивать параметры POST, перед загрузкой, и производить настройку BIOS после инициализации.

Другие атрибуты перенаправления KVM включают:

- Шифрование перенаправленного экрана, клавиатуры и мыши.
- Сжатие перенаправленного экрана.
- Возможность выбора конфигурации мыши в зависимости от типа ОС.
- Поддержка макросов клавиатуры, определяемых пользователем.

Функция перенаправления KVM поддерживает следующие разрешения и частоты обновления:

- 640×480 при 60 Гц, 72 Гц, 75 Гц, 85 Гц, 100 Гц
- 800×600 при 60 Гц, 72 Гц, 75 Гц, 85 Гц
- 1024×768 при 60 Гц, 72 Гц, 75 Гц, 85 Гц
- 1280×960 при 60 Гц
- 1280×1024 при 60 Гц
- 1600×1200 при 60 Гц
- 1650×1080 (WSXGA +) при 60 Гц
- 1920×1080 (1080 п) при 60 Гц
- 1920×1200 (WUXGA) при 60 Гц

11.3.1.1. Доступность

Удаленный сеанс KVM доступен, даже если сервер выключен (в режиме ожидания). Во время перезагрузки сервера или включения/выключения питания перезапуск удаленного сеанса KVM не требуется. Сброс BMC, например, из-за инициированного сторожевым таймером BMC сброса или сброса BMC после обновления прошивки BMC — требует восстановления сеанса. Сеансы KVM сохраняются при сбросе системы, но не при потере питания переменного тока.

11.3.1.2. Безопасность

Функция перенаправления KVM поддерживает несколько алгоритмов шифрования, включая RC4 и AES. Фактический используемый алгоритм согласовывается с клиентом в зависимости от его возможностей.

11.3.1.3. Использование

Когда сервер включен, удаленный сеанс KVM отображает полный процесс загрузки BIOS. Пользователь может взаимодействовать с настройкой BIOS, изменять и сохранять настройки, а также взаимодействовать с экранами конфигурации дополнительного ПЗУ.

11.3.1.4. Принудительный вход в BIOS Setup

Перенаправление KVM может предоставить возможность принудительного входа в BIOS Setup. Это позволяет системе войти в программу настройки BIOS во время загрузки, которая часто пропускается, когда удаленная консоль перенаправляет видео.

11.3.2. Перенаправление медиа

Встроенный веб-сервер предоставляет Java-апплет для включения удаленного перенаправления мультимедиа. Его можно использовать вместе с функцией удаленного KVM или как отдельный апплет.

Функция перенаправления носителя предназначена для того, чтобы позволить системным администраторам или пользователям подключать удаленную среду IDE или USB CD-ROM, дисковод гибких дисков или флеш-диск USB в качестве удаленного устройства к серверу. После подключения удаленное устройство выглядит для сервера как локальное устройство, позволяя системным администраторам или пользователям устанавливать программное обеспечение (включая операционные системы), копировать файлы, обновлять BIOS или загружать сервер с этого устройства.

В следующем списке описаны дополнительные возможности и функции перенаправления мультимедиа.

- Работа удаленно установленных устройств не зависит от локальных устройств на сервере. И удаленные, и локальные устройства можно использовать параллельно.
- Устройства IDE (CD-ROM, Floppy) или USB-устройства могут быть подключены к серверу как удаленное устройство.
- С удаленного устройства можно загрузить все поддерживаемые операционные системы и выполнить загрузку с диска IMAGE (* .IMG) и файлов ISO CD-ROM или DVD-ROM.
- Перенаправление мультимедиа поддерживает перенаправление, как для виртуального компакт-диска, так и для виртуального гибкого диска/USB-устройства одновременно. Устройство CD-ROM, Floppy и USB может быть либо локальным устройством, либо файлом образа диска (ISO).
- Функция перенаправления мультимедиа поддерживает несколько алгоритмов шифрования, включая RC4 и AES. Фактический используемый алгоритм согласовывается с клиентом в зависимости от его возможностей.
- Сеанс удаленного мультимедиа сохраняется, даже когда сервер выключен (в режиме ожидания).
- Смонтированное устройство является видимым для BIOS и установленной ОС.
- Подключенное устройство отображается в порядке загрузки BIOS, и можно изменить порядок загрузки BIOS для загрузки с этого удаленного устройства.
- Можно установить операционную систему на сервер без ОС с помощью удаленного устройства. Это также может потребовать использования KVM для настройки ОС во время установки.

USB-накопители отображаются в виде гибких дисков при перенаправлении носителя. Это позволяет устанавливать драйверы устройств во время установки ОС. Невозможно использование системы с только удаленными устройствами.

11.3.2.1. Доступность

Таймаут бездействия по умолчанию составляет 30 минут и не настраивается пользователем. Сеансы перенаправления носителей сохраняются при сбросе системы, но не при потере питания переменного тока или сбросе BMC.

11.3.3. Удаленная консоль

Удаленная консоль — это перенаправленный экран, клавиатура и мышь удаленной хост-системы (KVM). Для использования окна удаленной консоли в веб-интерфейсе предусмотрена соответствующая страница и клавиша вызова. Окно удаленной консоли открывается в браузере по протоколу HTTPS.

11.3.4. Производительность

Удаленная консоль точно демонстрирует локальный дисплей. Эта функция адаптируется к изменениям разрешения видео на локальном дисплее и продолжает работать плавно, когда система переходит от графики к тексту или наоборот. Время отклика может немного задерживаться в зависимости от пропускной способности и задержки сети.

Включение шифрования мультимедиа снижает производительность. Включение сжатия видео обеспечивает самый быстрый отклик, а отключение сжатия обеспечивает лучшее качество видео. Для наилучшей производительности KVM рекомендуется канал со скоростью 2 Мбит/с или выше. Перенаправление KVM через IP выполняется параллельно с локальным KVM, не влияя на его работу.

12. ОБЗОР ВСТРОЕННЫХ РАЗЪЕМОВ/ ОБОЗНАЧЕНИЙ

В этом разделе указаны местоположения и выводы для встроенных разъемов и обозначений материнской платы, которые обеспечивают интерфейс управления встроенной платформой или других доступных пользователю опций и функций. См. Рисунок 4-3 для получения подробной информации о расположении разъемов в этом разделе.

12.1. Разъемы питания

Серверная плата включает несколько разъемов питания, которые используются для подачи постоянного тока на различные устройства.

12.1.1. Основное питание

Питание материнской платы осуществляется через один 24-контактный разъем питания. Разъем помечен как «MAIN_PWR_CONN» в левой нижней части материнской платы. Таблица 62 представляет схему расположения контактов главного разъема питания.

Таблица 62. Распиновка главного разъема питания («MAIN_PWR_CONN»)

Контакт	Имя сигнала	Контакт	Имя сигнала
1	P3V3	13	P3V3
2	P3V3	14	N12V
3	GND	15	GND
4	P5V	16	FM_PS_EN_PSU_ON
5	GND	17	GND
6	P5V	18	GND
7	GND	19	GND
8	PWRGD_PS_PWROK_PSU_R1	20	NC_PS_RES_TP
9	P5V_STBY_PSU	21 год	P5V
10	P12V	22	P5V
11	P12V	23	P5V
12	P3V3	24	GND

12.1.2. Разъемы питания ЦП

ПРИМЕЧАНИЕ: поскольку BMC отслеживает наличие сигналов питания в материнской плате, питание должно подаваться как на CPU1, так и на CPU2, даже если CPU2 не установлен. Если сигналы питания не обнаружены, серверная плата не загрузится.

На серверной материнской плате есть два белых 8-контактных разъема питания CPU с маркировкой «CPU_1_PWR» и «CPU_2_PWR». В следующих таблицах показано расположение выводов для каждого разъема.

Таблица 63. Распиновка разъема питания CPU1 («CPU_1_PWR»)

Контакт	Имя сигнала	Контакт	Имя сигнала
1	GND	5	P12V1
2	GND	6	P12V1
3	GND	7	P12V3A
4	GND	8	P12V3A

Таблица 64. Распиновка разъема питания CPU2 («CPU_2_PWR»)

Контакт	Имя сигнала	Контакт	Имя сигнала
1	GND	5	P12V2
2	GND	6	P12V2
3	GND	7	P12V3B
4	GND	8	P12V3B

12.1.3. Дополнительный разъем питания 12V

По умолчанию серверная плата может обеспечить до 180 Вт общей мощности шести разъемам для карт расширения PCIe *. Для поддержки требований к питанию, превышающих этот предел, серверная плата включает один белый 2×2-контактный разъем питания, который можно использовать для подачи до 216 Вт дополнительной мощности на серверную плату. В корпусе QTECH этот разъем подключен к соответствующему разъему 2×2 на плате распределения питания. Бюджет мощности для всей системы должен быть рассчитан, чтобы определить, сколько дополнительной мощности доступно для поддержки любых дополнительных карт.

Таблица 65. Распиновка разъема дополнительного питания («AUX_PWR_IN»)

Контакт	Имя сигнала	Контакт	Имя сигнала
1	GND	3	P12V
2	GND	4	P12V

ПРИМЕЧАНИЕ: в соответствии со спецификацией PCIe * максимальная мощность, поддерживаемая непосредственно от слота для карты расширения x8 PCIe *, = 25 Вт. Максимальная мощность, поддерживаемая непосредственно от слота для карты расширения x16 PCIe *, = 75 Вт.

12.2. Разъемы передней панели

Серверная плата включает в себя несколько разъемов, обеспечивающих различные варианты передней панели. В этом разделе представлено функциональное описание и разводка контактов каждого разъема.

12.2.1. Разъем передней панели

На левом краю материнской платы находится 30-контактный разъем передней панели, совместимый с SSI, который обеспечивает различные функции передней панели, включая кнопки: кнопку питания/сна, кнопку идентификатора системы и кнопку NMI; светодиоды — активность сетевой карты, индикаторы активности жесткого диска, индикатор состояния системы и индикатор идентификатора системы.

Таблица 66. Распиновка разъема передней панели

Контакт	Имя сигнала	Контакт	Имя сигнала
1	P3V3_AUX	2	P3V3_AUX
3	Ключ	4	P5V_STBY
5	FP_PWR_LED BUF_N	6	FP_ID_LED BUF_N
7	P3V3	8	FP_LED STATUS_GREEN BUF_N
9	LED_HDD_ACTIVITY_N	10	FP_LED_STATUS_AMBER_BUF_N
11	FP_PWR_BTN_N	12	LED_NIC_LINK1_ACT_BUF_N
13	GND	14	LED_NIC_LINK1_LNKUP_BUF_N
15	FP_RST_BTN_N	16	SMB_SENSOR_3V3STBY_DATA
17	GND	18	SMB_SENSOR_3V3STBY_CLK

Контакт	Имя сигнала	Контакт	Имя сигнала
19	FP_ID_BTN_N	20	FP_CHASSIS_INTRUSION
21	PU_FM_SIO_TEMP_SENSOR	22	LED_NIC_LINK2_ACT_BUF_N
23	FP_NMI_BTN_N	24	LED_NIC_LINK2_LNKUP_BUF_N
25	Не используется	26	Не используется
27	PU_NIC3_LED_N	28	PU_NIC4_LED_N
29	FP_LNK_ACT_NIC3_LED_B_N	30	FP_LNK_ACT_NIC4_LED_B_N

12.2.2. USB-разъем на передней панели

Материнская плата включает 20-контактный разъем, который при подключении кабеля может обеспечить до двух портов USB 3.0 на передней панели. В следующей таблице представлена распиновка разъема.

Таблица 67. Распиновка разъема USB 3.0 на передней панели

Контакт	Имя сигнала	Контакт	Имя сигнала
1	P5V_AUX_USB_FP_USB3		
2	USB3_01_FB_RX_DN	19	P5V_AUX_USB_FP_USB3
3	USB3_01_FB_RX_DP	18	USB3_00_FB_RX_DN
4	GND	17	USB3_00_FB_RX_DP
5	USB3_01_FB_TX_DN	16	GND
6	USB3_01_FB_TX_DP	15	USB3_00_FB_TX_DN
7	GND	14	USB3_00_FB_TX_DP
8	USB2_13_FB_DN	13	GND
9	USB2_13_FB_DP	12	USB2_8_FB_DN
10	TP_FM_OC5_FP_R_N	11	USB2_8_FB_DP

12.3. Разъемы для встроенного хранилища

На материнской плате есть разъемы для поддержки нескольких вариантов запоминающих устройств. В этом разделе представлен функциональный обзор и разводка контактов каждого разъема.

12.3.1. Разъемы SATA 6 Гбит/с

Материнская плата включает два 7-контактных разъема SATA, обеспечивающих скорость передачи данных до 6 Гбит/с. Таблица 68 показывает расположение контактов обоих разъемов.

Таблица 68. Распиновка разъема SATA 6 Гбит/с

Контакт	Имя сигнала	Контакт	Имя сигнала
1	GND	5	SATA_RX_N
2	SATA_TX_P	6	SATA_RX_P
3	SATA_TX_N	7	GND
4	GND	-	-

Материнская плата также включает два порта mini-SAS HD, которые поддерживают до восьми дисков SATA 6 Гбит/с. Таблица 69 показывает расположение выводов обоих разъемов.

Таблица 69. Разъемы Mini-SAS HD для контактов SATA 6 Гбит/с

КОНТАКТ	Имя сигнала	КОНТАКТ	Имя сигнала
1A1	FM_QAT_ENABLE_N	2A1	FM_QAT_ENABLE_N
1B1	GND	2B1	GND
1C1	SGPIO_SATA_DATA0_R	2C1	SGPIO_SATA_DATA1_R
1D1	PU_DATAIN1_SATA_0	2D1	PU_DATAIN1_SATA_1
1A2	SGPIO_SATA_CLOCK_R	2A2	SGPIO_SATA_CLOCK_R
1B2	SGPIO_SATA_LOAD_R	2B2	SGPIO_SATA_LOAD_R
1C2	GND	2C2	GND
1D2	PD_SATA0_CONTROLLER_TYPE	2D2	PD_SATA1_CONTROLLER_TYPE
1A3	GND	2A3	GND

КОНТАКТ	Имя сигнала	КОНТАКТ	Имя сигнала
1B3	GND	2B3	GND
1C3	GND	2C3	GND
1D3	GND	2D3	GND
1A4	SATA6G_P1_RX_C_DP	2A4	SATA6G_P5_RX_C_DP
1B4	SATA6G_P0_RX_C_DP	2B4	SATA6G_P4_RX_C_DP
1C4	SATA6G_P1_TX_C_DP	2C4	SATA6G_P5_TX_C_DP
1D4	SATA6G_P0_TX_C_DP	2D4	SATA6G_P4_TX_C_DP
1A5	SATA6G_P1_RX_C_DN	2A5	SATA6G_P5_RX_C_DN
1B5	SATA6G_P0_RX_C_DN	2B5	SATA6G_P4_RX_C_DN
1C5	SATA6G_P1_TX_C_DN	2C5	SATA6G_P5_TX_C_DN
1D5	SATA6G_P0_TX_C_DN	2D5	SATA6G_P4_TX_C_DN
1A6	GND	2A6	GND
1B6	GND	2B6	GND
1C6	GND	2C6	GND
1D6	GND	2D6	GND
1A7	SATA6G_P3_RX_C_DP	2A7	SATA6G_P7_RX_C_DP
1B7	SATA6G_P2_RX_C_DP	2B7	SATA6G_P6_RX_C_DP
1C7	SATA6G_P3_TX_C_DP	2C7	SATA6G_P7_TX_C_DP
1D7	SATA6G_P2_TX_C_DP	2D7	SATA6G_P6_TX_C_DP
1A8	SATA6G_P3_RX_C_DN	2A8	SATA6G_P7_RX_C_DN
1B8	SATA6G_P2_RX_C_DN	2B8	SATA6G_P6_RX_C_DN

КОНТАКТ	Имя сигнала	КОНТАКТ	Имя сигнала
1C8	SATA6G_P3_TX_C_DN	2C8	SATA6G_P7_TX_C_DN
1D8	SATA6G_P2_TX_C_DN	2D8	SATA6G_P6_TX_C_DN
1A9	GND	2A9	GND
1B9	GND	2B9	GND
1C9	GND	2C9	GND
1D9	GND	2D9	GND

12.3.2. Разъемы M.2

В таблице 30 показаны выводы разъемов M.2 на плате. 4 столбца слева показывают сигналы при наличии устройства SATA, а 4 столбца справа показывают сигналы при наличии устройства PCIe *.

Таблица 70. Распиновка разъема M.2 (для модулей SATA и PCIe *)

Контакт	Сигнал	Контакт	Сигнал	Контакт	Сигнал	Контакт	Сигнал
1	CONFIG_3 =GND	2	3.3V	1	CONFIG_3 =GND	2	3.3V
3	GND	4	3.3V	3	GND	4	3.3V
5	N/C	6	N/C	5	N/C	6	N/C
7	N/C	8	N/C	7	N/C	8	N/C
9	N/C	10	DAS/DSS (I/O)	9	N/C	10	LED1#
11	N/C	12	Module Key	11	N/C	12	Module Key
13	Module Key	14	Module Key	13	Module Key	14	Module Key
15	Module Key	16	Module Key	15	Module Key	16	Module Key
17	Module Key	18	Module Key	17	Module Key	18	Module Key
19	Module Key	20	N/C	19	Module Key	20	N/C

Контакт	Сигнал	Контакт	Сигнал	Контакт	Сигнал	Контакт	Сигнал
21	CONFIG_0 =GND	22	N/C	21	CONFIG_0 =GND	22	N/C
23	N/C	24	N/C	23	N/C	24	N/C
25	N/C	26	N/C	25	N/C	26	N/C
27	GND	28	N/C	27	GND	28	N/C
29	N/C	30	N/C	29	PETn1	30	N/C
31	N/C	32	N/C	31	PETp1	32	N/C
33	GND	34	N/C	33	GND	34	N/C
35	N/C	36	N/C	35	PERn1	36	N/C
37	N/C	38	DEVSLP(I)80 /3.3V)	37	PERp1	38	N/C
39	GND	40	SMB_CLK (I/O)	39	GND	40	SMB_CLK (I/O)
41	SATA-B+	42	SMB_DATA	41	PETn0	42	SMB_DATA
43	SATA-B-	44	ALERT#(0)	43	PETp0	44	ALERT#(0)
45	GND	46	N/C	45	GND	46	N/C
47	SATA-A+	48	N/C	47	PERn0	48	N/C
49	SATA-A-	50	N/C	49	PERp0	50	PERST# (I)(0/3.3V)
51	GND	52	N/C	51	GND	52	CLKREQ# (I/O) (0/3.3V)
53	N/C	54	N/C	53	REFCLKn	54	PEWAKE# (I/O) (0/3.3V)

Контакт	Сигнал	Контакт	Сигнал	Контакт	Сигнал	Контакт	Сигнал
55	N/C	56	Reserved for MFG_DATA	55	REFCLKp	56	Reserved for MFG_DATA
57	GND	58	Reserved for MFG_CLOCK	57	GND	58	Reserved for MFG_CLOCK
59	Module Key	60	Module Key	59	Module Key	60	Module Key
61	Module Key	62	Module Key	61	Module Key	62	Module Key
63	Module Key	64	Module Key	63	Module Key	64	Module Key
65	Module Key	66	Module Key	65	Module Key	66	Module Key
67	N/C	68	SUSCLK(32 KHz) (I)(0/3.3V)	67	N/C	68	SUSCLK(32KHz) (I)(0/3.3V)
69	CONFIG_1 =GND	70	3.3V	69	CONFIG_1 =NC	70	3.3V
71	GND	72	3.3V	71	GND	72	3.3V
73	GND	74	3.3V	73	GND	74	3.3V
75	CONFIG_2 =GND			75	CONFIG_2 =GND		

12.4. Разъемы вентилятора

Материнская плата поддерживает девять вентиляторов. Семь предназначены для поддержки вентиляторов системы охлаждения, а два — для вентиляторов процессора.

12.4.1. Разъемы системного вентилятора

Серверная плата включает шесть 6-контактных разъемов системного вентилятора на переднем крае платы, помеченные SYS_FAN_ # (1-6), и один 4-контактный разъем вентилятора, расположенный рядом с задним краем платы, помеченный SYS_FAN_7. В следующих таблицах приведены выводы для каждого типа разъема.

Таблица 71. 6-контактный разъем системы вентилятора Разъем Pin-аут

Контакт	Имя сигнала	Контакт	Имя сигнала
1	GND	4	PWM
2	12V	5	PRSNT
3	TACH	6	FAULT

Таблица 72. 4-контактный разъем системы вентилятора Разъем Pin-аут

Контакт	Имя сигнала
1	GND
2	12V
3	TACH
4	PWM

12.4.2. Разъемы вентилятора ЦП

Материнская плата включает два 4-контактных разъема вентилятора CPU, помеченных как CPU_1_Fan и CPU_2_Fan. В следующей таблице приведены выводы для каждого.

Таблица 73. Распиновка разъема вентилятора CPU

Контакт	Имя сигнала
1	GND
2	12V
3	TACH
4	PWM

12.5. Другие разъемы

На материнской плате имеется несколько разъемов ввода-вывода для различных интерфейсов, используемых для связи между BMC и периферийными устройствами, для мониторинга и для взаимодействия с пользователем.

12.5.1. HSBP Inter-Integrated Circuit (I2C) разъемы

Материнская плата включает разъём для межинтегральной схемы (I2C), помеченный «HSBP_I2C», для связи с объединительными платами с возможностью «горячей» замены. В следующей таблице показано расположение выводов.

Таблица 74. Распиновка I2C разъема («HSBP_I2C_B»)

Контакт	Имя сигнала
1	SMB HSBP 3V3STBY DATA
2	GND
3	SMB HSBP 3V3STBY CLK
4	RST PCIE SSD PERST N

12.5.2. Разъем последовательного порта

Материнская плата включает один внутренний разъем последовательного порта DH-10.

Таблица 75. Распиновка разъема последовательного порта

Контакт	Имя сигнала	Контакт	Имя сигнала
1	SPA_DCD	2	SPA_DSR
3	SPA_SIN	4	SPA_RTS
5	SPA_SOUT_N	6	SPA_CTS
7	SPA_DTR	8	SPA_RI
9	GND		

12.5.3. Разъем PMBus

Материнская плата обеспечивает шину управления питанием, чтобы BMC мог контролировать установленные источники питания и связываться с ними. Распиновка этого разъема показана в следующей таблице.

Таблица 76. Распиновка разъема PMBus

Контакт	Имя сигнала
1	SMB_PMB1_SML1_STBY_LVC3_SCL
2	SMB_PMB1_SML1_STBY_LVC3_SDA

Контакт	Имя сигнала
3	IRQ_SML1_PMBUS_ALERT_RC_N
4	GND
5	P3V3

12.5.4. Разъем контроля вторжения в корпус

Материнская плата включает 2-контактный разъем вскрытия корпуса, который можно использовать, когда шасси сконфигурировано с переключателем вскрытия корпуса. Разъем имеет следующую распиновку.

Таблица 77. Распиновка заголовка вскрытия корпуса

Состояние заголовка	Сигнал	Описание
Контакты 1 и 2 закрыты	FM INTRUDER HDR N is pulled HIGH	Крышка корпуса закрыта
Контакты 1 и 2 открыты	FM INTRUDER HDR N is pulled LOW	Крышка корпуса снята

13. ПЕРЕМЫЧКИ СБРОСА И ВОССТАНОВЛЕНИЯ

Материнская плата имеет несколько блоков трехконтактных перемычек, которые можно использовать для настройки, защиты или восстановления определенных функций материнской платы.

Символ ▼ обозначает контакт 1 на каждой колодке перемычек.

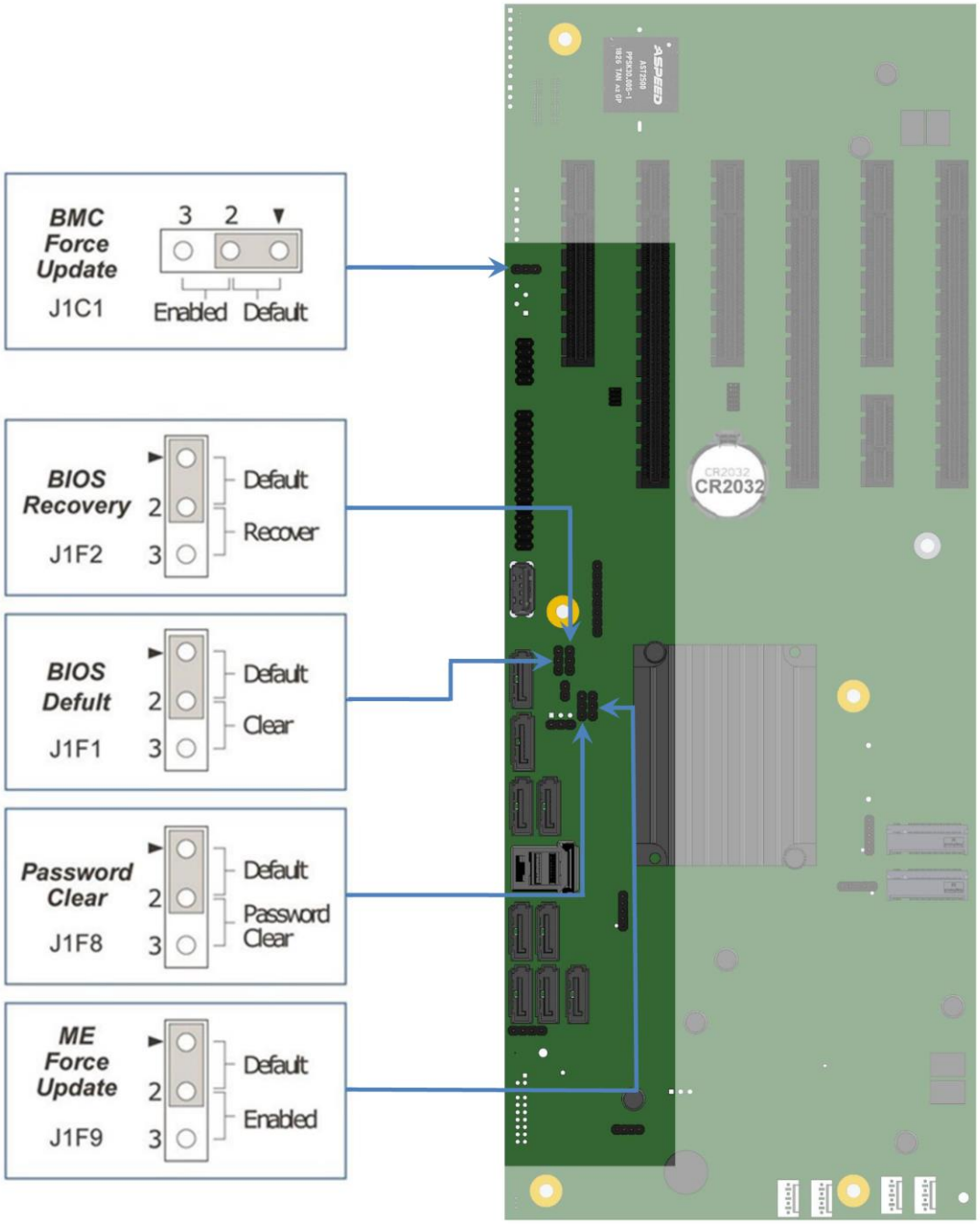


Рисунок 13-1. Расположение перемычек и контакты

13.1. Блок перемычек сброса BIOS к настройкам по умолчанию

Эта перемычка сбрасывает параметры BIOS, настроенные с помощью <F2> BIOS Setup Utility, обратно к исходным заводским настройкам по умолчанию.

ПРИМЕЧАНИЕ: эта перемычка не сбрасывает пароли администратора или пользователя. Для сброса паролей необходимо использовать перемычку для сброса пароля.

1. Выключите сервер и отсоедините шнур (-ы) питания.
2. Снимите с системы верхнюю крышку и переместите в «BIOS DFLT» перемычку из контактов 1–2 (по умолчанию) в контакты 2–3 (положение для сброса BIOS к настройкам по умолчанию).
3. Подождите 5 секунд, а затем переключите перемычку обратно в контакты 1–2.
4. Установите на место верхнюю крышку.
5. Установите шнур (-ы) питания системы.
6. Во время процедуры POST откройте служебную программу настройки BIOS Setup Utility <F2>, чтобы настроить и сохранить необходимые параметры BIOS.

ПРИМЕЧАНИЯ:

- Система автоматически включится после подачи переменного тока в систему.
- Возможно, потребуется сбросить системное время и дату.
- После сброса параметров BIOS с помощью перемычки BIOS по умолчанию на экране диспетчера ошибок в программе настройки BIOS Setup Utility <F2> отобразятся две ошибки:
    - 0012 Дата/время системы RTC не установлены.
    - 5220 Настройки BIOS сброшены до настроек по умолчанию.

13.2. Блок перемычек для сброса пароля

Эта перемычка сбрасывает пароль пользователя и пароль администратора, если они были установлены. Оператор должен знать, что это создает брешь в безопасности до тех пор, пока пароли не будут снова установлены с помощью утилиты <F2> BIOS Setup Utility. Это единственный метод, с помощью которого можно безоговорочно очистить пароли администратора и пользователя. Кроме этой перемычки, пароли можно установить или сбросить только путем их явного изменения в BIOS Setup или аналогичными способами. Никакой метод сброса настроек конфигурации BIOS до значений по умолчанию не повлияет ни на пароль администратора, ни на пароль пользователя.

1. Выключите сервер. В целях безопасности отключите шнур (-ы) питания.
2. Снимите верхнюю крышку системы.
3. Переместить в «Password Clear» перемычку из контактов 1–2 (по умолчанию) в контакты 2–3 (положение для сброса пароля).
4. Установите на место верхнюю крышку системы и снова подсоедините шнур (-ы) питания.
5. Включите сервер и во время процедуры POST откройте служебную программу настройки BIOS Setup Utility <F2>.
6. Убедитесь, что операция очистки пароля прошла успешно, просмотрев экран диспетчера ошибок. Должны быть зарегистрированы две ошибки:
    - 5221 Пароли сброшены перемычкой;

- 5224 Перемычка сброса пароля установлена.

7. Выйдите из программы настройки BIOS и выключите сервер. В целях безопасности отсоедините шнур (-ы) питания переменного тока.
8. Снимите верхнюю крышку и переместите перемычку «Сброс пароля» обратно на контакты 1–2 (по умолчанию).
9. Установите на место верхнюю крышку и подсоедините шнур (-ы) питания переменного тока.
10. Включите сервер.
11. Настоятельно рекомендуется: немедленно загрузиться в BIOS Setup Utility <F2>, перейти на вкладку «Security» и установить пароли администратора и пользователя.

13.3. Блок перемычек принудительного обновления микропрограммы Management Engine (ME)

Когда перемычка принудительного обновления микропрограммы ME перемещается из положения по умолчанию, ME вынужден работать с уменьшенной минимальной рабочей мощностью. Эту перемычку следует использовать только в том случае, если прошивка ME была повреждена и требует переустановки. Используйте следующую процедуру.

ПРИМЕЧАНИЕ: файлы обновления микропрограммы включены в пакеты обновления системы (SUP), размещенные на в центре загрузкок QTECH https://ftp.qtech.ru/Servers%20and%20Storage/Server/

1. Выключите систему.
2. Отсоедините шнур (-ы) питания переменного тока.

ПРИМЕЧАНИЕ: если переместить перемычку ME FRC UPD при подаче питания переменного тока на систему, ME не будет работать должным образом.

1. Снимите верхнюю крышку.
2. Переместить в «ME FRC UPD» перемычку из контактов 1–2 (по умолчанию) в контакты 2–3 (положение для принудительного обновления микропрограммы ME.
3. Установите на место верхнюю крышкуи снова подсоедините шнур (-ы) питания переменного тока.
4. Включите систему.
5. Загрузитесь в оболочку EFI.
6. Измените каталоги на папку, содержащую файлы обновлений.
7. Обновите прошивку ME с помощью следующей команды:

```
iflash32/u/ni <номер версии> _ ME.cap
```

8. После успешного завершения обновления выключите систему.
9. Отсоедините шнур (-ы) питания переменного тока.
10. Снимите верхнюю крышку.
11. Верните перемычку «ME FRC UPD» в контакты 1–2 (по умолчанию).
12. Снова подсоедините шнур (-ы) питания переменного тока.
13. Включите систему.

13.4. Блок перемычек принудительного обновления BMC

Перемычка «BMC Force Update» используется для перевода BMC в режим загрузки низкоуровневого обновления. Это заставляет BMC прерывать свой обычный процесс загрузки и оставаться в загрузчике без выполнения какого-либо кода Linux.

Эту перемычку следует использовать только в том случае, если микропрограмма BMC была повреждена и требует переустановки. Сделайте следующее:

ПРИМЕЧАНИЕ: файлы обновления включены в пакеты обновления системы (SUP), размещенные в центре загрузки QTECH https://ftp.qtech.ru/Servers%20and%20Storage/Server/

1. Выключите систему.
2. Отсоедините шнур (-ы) питания переменного тока.

ПРИМЕЧАНИЕ: если переместить перемычку BMC FRC UPD при подаче питания переменного тока на систему, BMC не будет работать должным образом.

3. Снимите верхнюю крышку.
4. Переместить в «BMC FRC UPD» Перемычку из контактов 1–2 (по умолчанию), в контакты 2–3 (положение для принудительного обновления BMC).
5. Установите на место верхнюю крышку и снова подсоедините шнур (-ы) питания переменного тока.
6. Включите систему.
7. Загрузитесь в оболочку EFI.
8. Измените каталоги на папку, содержащую файлы обновлений.
9. Обновите прошивку BMC с помощью следующей команды:

   FWPIAUPD -u -bin -ni -b -o -pia -if = USB <имя файла.BIN>

10. После успешного завершения обновления выключите систему.
11. Отсоедините шнур (-ы) питания переменного тока.
12. Снимите верхнюю крышку.
13. Верните перемычку «BMC FRC UPD» в контакты 1–2 (по умолчанию).
14. Снова подсоедините шнур (-ы) питания переменного тока.
15. Включите систему.
16. Загрузитесь в оболочку EFI.
17. Измените каталоги на папку, содержащую файлы обновлений.
18. Переустановите данные SDR-платы/системы, запустив утилиту FRUSDR.
19. После загрузки SDR перезагрузите сервер.

13.5. Блок перемычек восстановления BIOS

Когда блок перемычки восстановления BIOS перемещается из контактов по умолчанию (контакты 1–2), система загружается с использованием резервного образа BIOS в оболочку uEFI, где может быть выполнено стандартное обновление BIOS (см. Инструкции по обновлению BIOS, которые включены в пакеты обновления системы (SUP), загруженные с центра загрузки QTECH). Эта перемычка используется, когда системная BIOS повреждена и не работает, что требует загрузки нового образа BIOS на материнскую плату.

ПРИМЕЧАНИЕ: перемычка восстановления BIOS используется ТОЛЬКО для переустановки образа BIOS в случае повреждения BIOS. Эта перемычка НЕ используется, когда BIOS работает нормально и вам необходимо обновить BIOS с одной версии до другой.

Следует соблюдать следующую процедуру.

ПРИМЕЧАНИЕ: пакеты обновления системы (SUP) можно загрузить в центре загрузок QTECH https://ftp.qtech.ru/Servers%20and%20Storage/Server/

1. Выключите систему.
2. В целях безопасности отсоедините шнур (-ы) питания переменного тока.
3. Снимите верхнюю крышку.
4. Переместите перемычку «*BIOS Recovery*» с контактов 1–2 (по умолчанию) в контакты 2–3 (положение для восстановления BIOS).
5. Установите на место верхнюю крышку и снова подсоедините шнур (-ы) питания переменного тока.
6. Включите систему.
7. Система автоматически загрузится с оболочкой EFI. Обновите BIOS, используя стандартные инструкции по обновлению BIOS, прилагаемую к пакету обновления.
8. После успешного завершения обновления BIOS выключите систему. В целях безопасности отсоедините шнур (-ы) питания переменного тока от системы.
9. Снимите верхнюю крышку.
10. Верните перемычку восстановления BIOS в контакты 1–2 (по умолчанию).
11. Установите на место верхнюю крышку и снова подсоедините шнур (-ы) питания переменного тока.
12. Загрузитесь в настройки BIOS Setup Utility **<F2>.**
13. Настройте желаемые параметры BIOS.
14. Нажмите кнопку **<F10>** для сохранения и выхода из утилиты.

14. СВЕТОВАЯ ДИАГНОСТИКА

Материнская плата включает несколько встроенных светодиодных индикаторов, помогающих в поиске и устранении неисправностей на различных уровнях.

14.1. Системные светодиоды

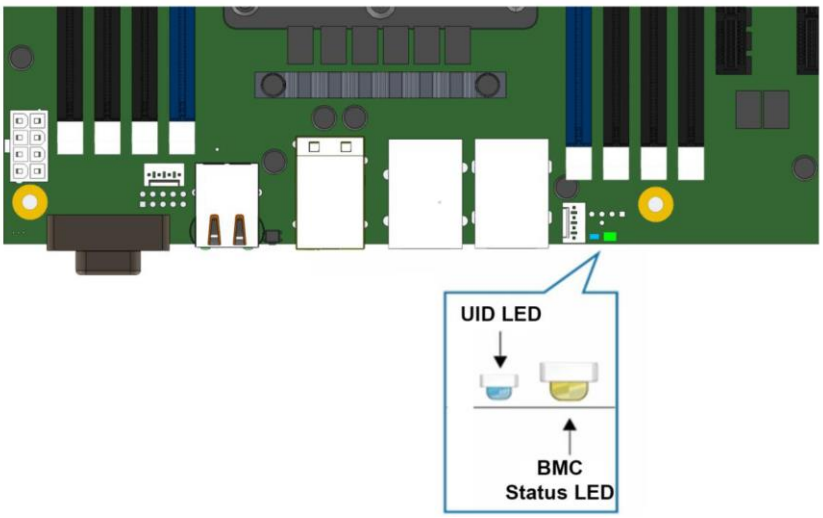


Рисунок 14-1. Светодиодный индикатор состояния системы и идентификационный светодиодный индикатор

14.1.1. Светодиод идентификатора системы

На материнской плате имеется синий светодиодный индикатор системного идентификатора, который используется для визуальной идентификации определенного сервера, установленного среди множества других подобных серверов. Есть два варианта включения светодиода идентификатора системы.

- Нажмите кнопку светодиода идентификации на передней панели, при этом светодиод будет гореть постоянно, пока кнопка не будет нажата снова.
- Удаленно введите команду идентификации шасси IPMI, в результате чего светодиодный индикатор начнет мигать.

Светодиодный индикатор идентификатора системы на материнской плате напрямую связан со светодиодным индикатором идентификатора системы на передней панели системы, если он имеется.

14.1.2. Светодиод состояния системы

Материнская плата оснащена двухцветным светодиодным индикатором состояния системы. Светодиод состояния системы на материнской плате напрямую связан со светодиодом состояния системы на передней панели, если он есть. Этот светодиод показывает текущее состояние сервера. Возможные состояния светодиода: непрерывный зеленый, мигающий зеленый, непрерывный желтый и мигающий желтый.

Когда сервер выключен (переходит в состояние выключения постоянного тока), BMC все еще находится в режиме ожидания и сохраняет состояние датчика и светодиодного индикатора состояния на передней панели, установленное до отключения питания.

Когда к системе в первый раз подается питание переменного тока, индикатор состояния горит желтым, а затем сразу же начинает мигать зеленым, показывая, что BMC загружается. Если процесс загрузки BMC завершился без ошибок, индикатор состояния загорится зеленым. Все состояния светодиодных индикаторов состояния системы см. Таблица 78.

Таблица 78. Сведения о состоянии светодиода состояния системы

Цвет	Состояние	Состояние системы	Описание
Зеленый	Горит постоянно	Хорошо	Указывает, что состояние системы — «Исправно». Система не выдает ошибок. Электропитание переменного тока присутствует, BMC загружен, функция управления запущена и работает. 1. После сброса BMC загружается Linux *. Управление будет передано от BMC uBoot к BMC Linux *. Это состояние продлится от 10 до 20 секунд
Зеленый	~ 1 Гц мигает	Некритическая Ошибка	Система обнаружила некритическую ошибку: 1. Потеря избыточности, например, источника питания или вентилятора. Применяется, только если связанная подсистема платформы имеет возможности резервирования. 2. Предупреждение или отказ вентилятора, когда количество полностью работающих вентиляторов достигает минимального количествв, необходимого для охлаждения системы. 3. Пересечение датчиком критического порога — температуры (в том числе температуры в HSBP), напряжения, входной мощности к источнику питания, выходного тока для главной шины питания, от источника питания, и процессора. 4. Датчики (Therm Ctrl). 5. Произошел сбой блока питания при наличии резервного блока питания

Цвет	Состояние	Состояние системы	Описание
Зеленый	~ 1 Гц мигает	Некритическая Ошибка	6. Невозможно использовать всю установленную память (установлено более 1 модуля DIMM). 7. Превышение порогового значение числа исправимых ошибок и переход на запасной модуль DIMM (резервирование памяти). Это указывает на то, что у пользователя больше нет модулей DIMM для обеспечения избыточности. Соответствующий индикатор DIMM горит. 8. В зеркальной конфигурации, когда происходит нарушение зеркального отображения памяти, и система теряет избыточность памяти. 9. Выход из строя аккумуляторной батареи. 10. Запуск BMC в uBoot. (Обозначается светодиодом шасси, мигающим с частотой 3 Гц). 11. Система в состоянии ошибки (нет управляемости). BMC uBoot запущен, но не передал управление BMC Linux *. Плата будет в этом состоянии 6 – 8 секунд после сброса BMC, пока идет загрузка образа Linux * во флеш-память. 12. BMC Watchdog сбросил BMC. 13. Обнаружен сигнал датчика блока питания для ошибки конфигурации. 14. HDD HSC отключен или неисправен. 15. Неисправность жесткого диска

Цвет	Состояние	Состояние системы	Описание
Желтый	~ 1 Гц мигает	Предупреждение	Предупреждающая сигнализация - система может выйти из строя: 1. Превышен критический порог — напряжение, температура (включая температуру HSBP), входное питание для источника питания, выходной ток для главной шины питания от источника питания и датчиков PROCHOT (Therm Ctrl). 2. Сигнал от VRD. 3. Минимальное количество вентиляторов для охлаждения системы отсутствует или вышло из строя. 4. Датчик резервирования блока питания — Недостаточная компенсация ресурсов (указывает на недостаточное количество блоков питания)

14.2. Диагностические светодиоды POST-кода

Два набора из четырех диагностических светодиодов POST-кода (один набор зеленых светодиодов и один набор желтых светодиодов) расположены на задней стороне платы рядом со встроенными разъемами Ethernet. В процессе загрузки системы BIOS выполняет ряд процессов конфигурации платформы, каждому из которых назначается определенный шестнадцатеричный номер POST-кода. При запуске каждой процедуры настройки BIOS отображает данный POST-код на диагностических индикаторах POST-кода. Эти светодиоды предназначены для помощи в поиске и устранении неисправностей в зависании системы во время процесса POST. Диагностические светодиоды могут использоваться для определения последнего выполненного процесса POST. См. Раздел 18 для полного описания работы светодиодов и списка всех поддерживаемых кодов POST.

14.3. Светодиоды сбоя CPU

На серверной материнской плате имеется светодиод сбоя CPU для каждого разъема CPU. Светодиод сбоя CPU горит, если обнаружена ошибка несоответствия MSID (т. е. номинальная мощность CPU несовместима с платой).

14.4. Светодиодные индикаторы состояния загрузки/сброса BMC

Во время загрузки BMC или процесса сброса BMC индикатор состояния системы и индикатор идентификатора системы используются для индикации переходов и состояний процесса загрузки BMC. Загрузка BMC произойдет при первом включении питания переменного тока. (Включение/выключение источника питания постоянного тока не будет вызывать сброс BMC.) Сброс BMC будет происходить после обновления встроенного программного обеспечение, прием команды сброса BMC и сброса инициированного BMC

Watchdog. В следующей таблице определены состояния светодиодных индикаторов во время процесса загрузки/сброса BMC.

Таблица 79. Светодиодные индикаторы состояния загрузки/сброса BMC

Состояние загрузки/сброса BMC	**UID LED**	**BMC Status LED**	**Комментарий**
BMC/тест видеопамяти не пройден	Горит синим	Горит желтым	Неустранимое состояние. Свяжитесь с вашим представителем QTECH для получения информации по замене этой материнской платы
Ошибка обоих универсальных загрузчика (u-Boot)	Мигает синим 6 Гц	Горит желтым	Неустранимое состояние. Свяжитесь с вашим представителем QTECH для получения информации по замене этой материнской платы
BMC в u-Boot	Мигает синим 3 Гц	Мигает зеленым 1 Гц	Мигающий зеленый светодиод показывает проблемное состояние (отсутствие управляемости), мигание синего цвета означает, что u-Boot запущен, но не передал управление BMC Linux. Плата будет в этом состоянии 6 – 8 секунд после сброса BMC, пока идет загрузка образа Linux во флеш-память
BMC Загрузка Linux	Горит синим	Горит зеленым	Стабильный зеленый и синий светодиод указывает, что управление было передано от u-Boot к BMC Linux, после сброса цикла переменного тока/BMC. Состояние продлится от 10 до 20 секунд
Конец процесса загрузки/сброса BMC. Нормальная работа системы	Выключен	Горит зеленым	Указывает, что BMC Linux загружен и работает, обеспечены функции управляемости. Светодиоды неисправности/состояния работают как обычно

15. ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ МАТЕРИНСКОЙ ПЛАТЫ

В следующей таблице приведены операционные и внереализационные экологические ограничения материнской платы. Работа при условиях, несоблюдающих приведенные в таблице ниже пределы, может привести к необратимому повреждению системы. Воздействие предельных значений в течение длительного времени может повлиять на надежность системы.

Таблица 80. Ограничения материнской платы по окружающей среде

Параметр	**Пределы**	
Рабочая температура	От 0 °C до +55 °C (от +32 °F до +131 °F)	
Нерабочая температура	От −40 °C до +70 °C (от −40 °F до +158 °F)	
Напряжение	Напряжение постоянного тока: ± 5 % от всех номинальных напряжений	
Ударная, без упаковки	Трапециевидный, 25 г, 40–79 фунтов. 205 дюймов/с	
Ударная, упакованная	Вес продукта	Высота свободного падения
	< 20 фунтов	36 дюймов
	≥ 20 фунтов. до < 40 фунтов	30 дюймов
	≥ 40 фунтов. до < 80 фунтов	24 дюйма
	≥ 80 фунтов. до < 100 фунтов	18 дюймов
	≥ 100 фунтов. до < 120 фунтов	12 дюйма
	≥ 120 фунтов	9 дюймов
Вибрация, без упаковки	От 5 Гц до 500 Гц, 3,13g RMS случайное	

ПРИМЕЧАНИЕ:

Указанные выше значения ударов без упаковки представляют собой проходные значения перегрузки, и они меньше, чем Стандарты окружающей среды для материнских плат (50 г, 170 дюймов/с).

Примечание об отказе от ответственности: системный интегратор несет ответственность за определение надлежащих ограничений платы и системы, если системный интегратор выбирает другую конфигурацию системы или другое шасси. QTECH не может нести ответственность, если компоненты вышли из строя или серверная плата не работает должным образом при использовании вне каких-либо опубликованных рабочих или нерабочих ограничений.

16. ОБЗОР BIOS

16.1. Меню POST

В данном документе объясняется функционал меню BIOS, который отображает настройки конфигурации системы и позволяет изменять эти настройки.

Чтобы войти в меню BIOS, нажмите **<Esc>** на клавиатуре во время процедуры самотестирования при включении питания. Появится POST-меню BIOS (см. Рисунок 16-1):

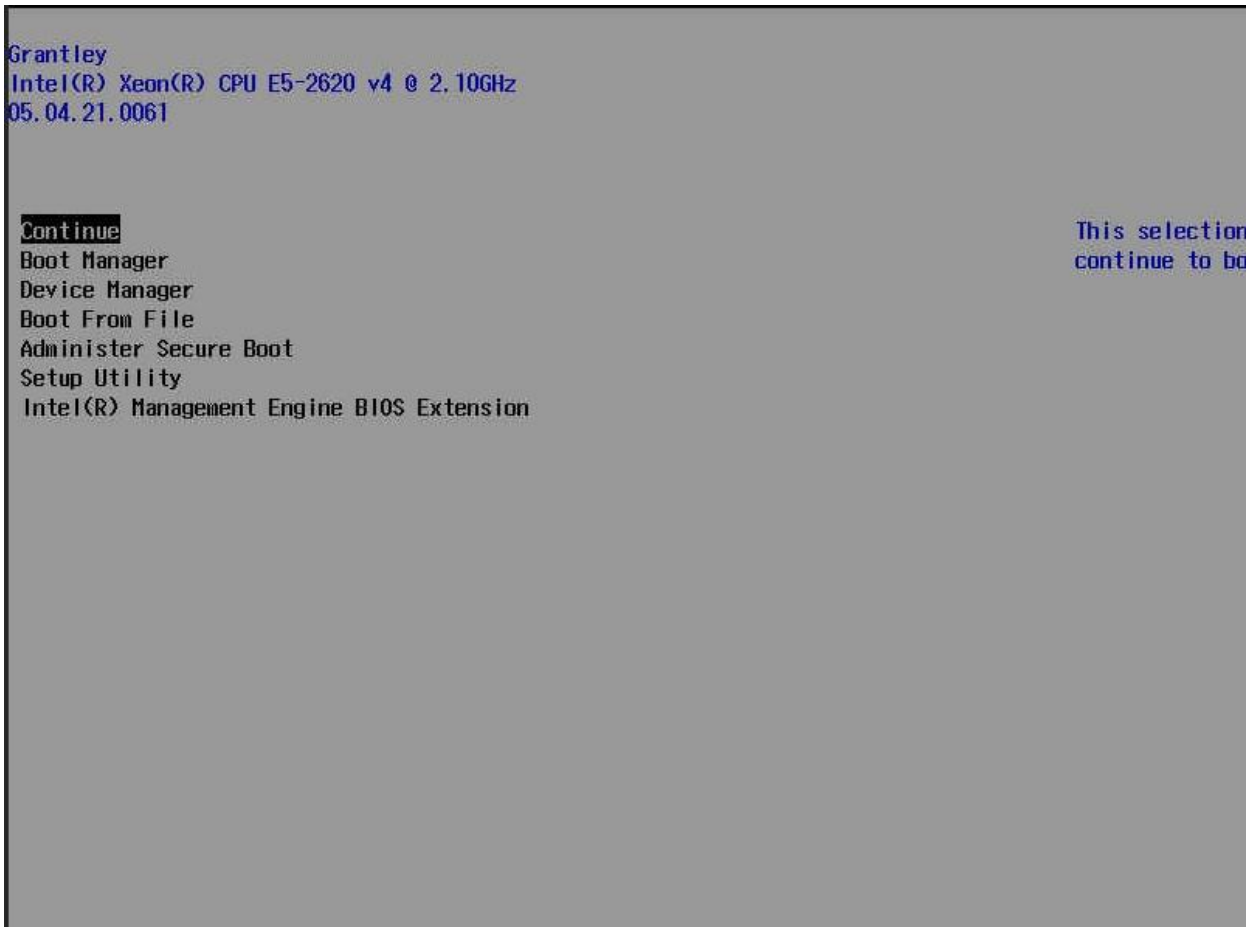


Рисунок 16-1. POST-меню BIOS

Для доступа к меню настройки BIOS, вы можете выбрать **'Setup Utility'** и нажать клавишу **‘Enter’**.

16.2. Меню настройки BIOS

Зайдя в меню настройки BIOS Setup Utility, вы увидите следующие пункты меню:

Рисунок 16-2. Разделы меню настройки BIOS

Разделы меню	Описание
Main (Главный)	Отображает системную информацию, такую как тип процессора и его скорость, скорость системной шины, скорость системной памяти, общую установленная память, текущий язык EFI, а также системную дату и время
Advanced (Расширенный)	Позволяет настраивать дополнительные системные настройки, такие как конфигурация загрузки, функции ACPI и конфигурация наборов микросхем
Security (Безопасность)	Устанавливает пароли и защитные функции
Power (Питание)	Настраивает функции управления питанием
Boot (Загрузка)	Устанавливает настройки загрузки, такие как быстрая загрузка или загрузка с USB-устройств
Exit (Выход)	Позволяет пользователю сохранять или отменять изменения BIOS и загружать оптимальные или пользовательские настройки по умолчанию

Если изменения, внесённые в BIOS, приводят к сбоям в работе системы или нежелательной производительности системы, снова войдите в BIOS и нажмите F9 для загрузки Setup Defaults, а затем F10 для сохранения и выхода из BIOS.

Для навигации по каждому разделу меню используйте стрелки влево и вправо на клавиатуре. Стрелки вверх и вниз позволяют осуществлять навигацию по пунктам каждого меню. Нажмите клавишу Enter, чтобы выбрать элемент и перейти в подменю (если доступно). Используйте клавишу Esc в любое время для возврата к предыдущему соответствующему подменю или меню. Инструкции по быстрой навигации см. также в нижней части экрана меню BIOS.

Если после изменения каких-либо настроек BIOS система перешла в состояние, не позволяющее запустить меню BIOS и вернуться к настройкам по умолчанию осуществите следующие действия:

- обесточьте систему;
- откройте крышку корпуса;
- деинсталируйте батарейку;
- подождите 15 – 30 секунд;
- установите батарейку в гнездо;
- закройте крышку;
- произведите попытку запуска системы согласно инструкциям.

Опции BIOS, приведенные в разделах ниже, могут быть доступны в актуальной версии BIOS для рассматриваемой платформы не в полном объеме.

16.2.1. Main — главное меню

Раздел "Main" BIOS содержит краткий обзор основной информации о системе и возможность изменения языка отображения BIOS и системного времени.

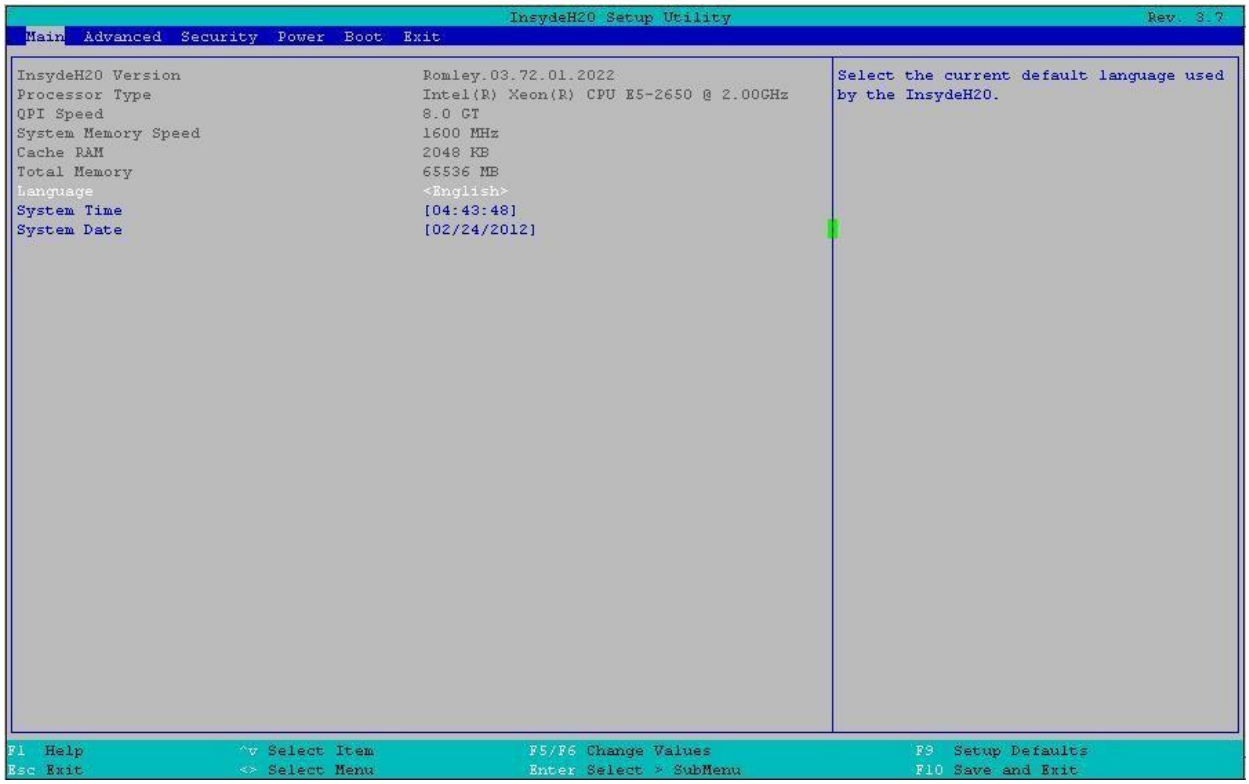


Рисунок 16-3. Меню Main

Настройка BIOS	Опции	Описание
InsydeH2O Version (Версия BIOS)	Нет вариантов	Отображает версию программного обеспечения, установленного BIOS
Processor Type (Тип процессора)	Нет вариантов	Отображает марку, модель и скорость установленного процессора
QPI Speed (скорость QPI)	Нет вариантов	Отображает автоматически определяемую скорость QPI системы
System Memory Speed (Скорость системной памяти)	Нет вариантов	Отображает автоматически определяемую скорость системной памяти
Cache RAM (Кеш ОЗУ)	Нет вариантов	Отображает текущий объем кеша оперативной памяти в системе

Настройка BIOS	Опции	Описание
Total Memory (Общая память)	Нет вариантов	Отображает общий объем обнаруженной системной памяти, установленной в системе
Language (Язык)	английский	Выбор языка, который будет отображаться в программе установки. (В текущей версии только один язык)
System Time (Системное время)	Установить время	Позволяет пользователю изменять время, распознаваемое системой
System Date (Системная дата)	Дата корректировки	Позволяет пользователю изменить дату, распознанную системой

16.2.2. Advanced — расширенное меню

Раздел "Advanced" меню BIOS позволяет настраивать расширенные системные настройки.

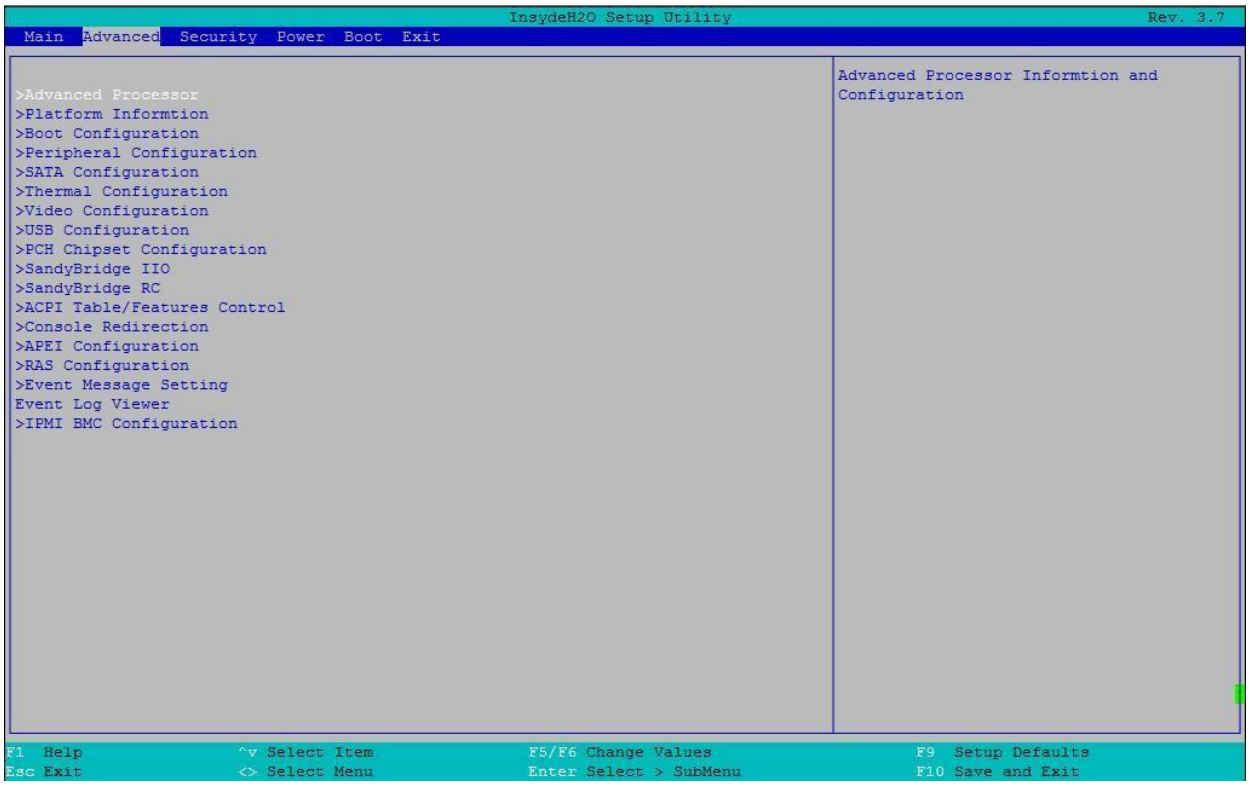


Рисунок 16-4. Меню Advanced

Настройка BIOS	Опции	Описание
Advanced Processor (Расширенные настройки Процессора)	См. раздел 16.2.2.1	Расширенные настройки Процессора
Platform Information (Информация о платформе)	См. раздел 16.2.2.1.3	Информация о платформе
Boot Configuration (Конфигурация загрузки)	См. раздел 16.2.2.2	Конфигурация загрузки
Peripheral Configuration (Периферийная конфигурация)	См. раздел 16.2.2.3	Конфигурация периферийных устройств
SATA Configuration (Конфигурация SATA)	См. раздел 16.2.2.4	Позволяет выбирать контроллер SATA и тип драйвера жесткого диска, установленного в вашем сервере
Termal Configuration (Тепловая конфигурация)	См. раздел 16.2.2.5	Настройки тепловой конфигурации
Video Configuration (Видео конфигурация)	См. раздел 16.2.2.6	Настройка параметров видео
USB Configuration (Конфигурация USB)	См. раздел 16.2.2.7	Настраивает поддержку USB-порта
PCH Chipset Configuration (Конфигурация набора микросхем PCH)	См. раздел 16.2.2.8	Расширенная конфигурация набора микросхем
SandyBridge IIO (Мост интерфейса ввода/вывода)	См. раздел 16.2.2.9	Выбор, компонентов SandyBridge IIO для настройки
SandyBridge RC (Мост RC)	См. раздел 16.2.2.10	Настройка SandyBridge RC

Настройка BIOS	Опции	Описание
ACPI Table/Features Control (ACPI-таблица/настройка характеристик)	См. раздел 16.2.2.11	Настройка ACPI-таблиц/установка характеристик
Console Redirection (Переадресация консоли)	См. раздел 16.2.2.12	Настройки перенаправления консоли
APEI Configuration	См. раздел 16.2.2.13	APEI-конфигурация
RAS Configuration	См. раздел 16.2.2.14	RAS-конфигурация
Event Message Setting	См. раздел 16.2.2.15	Настройка сообщений о событиях
Event Log Viewer	См. раздел 16.2.2.16	Утилита предназначеная для просмотра журнала событий
IPMI BMC Configuration (Конфигурация IPMI BMC)	См. раздел 16.2.2.17	Конфигурация IPMI BMC

16.2.2.1. Advanced/Advanced Processor

Расширенные настройки/Расширенные настройки Процессора

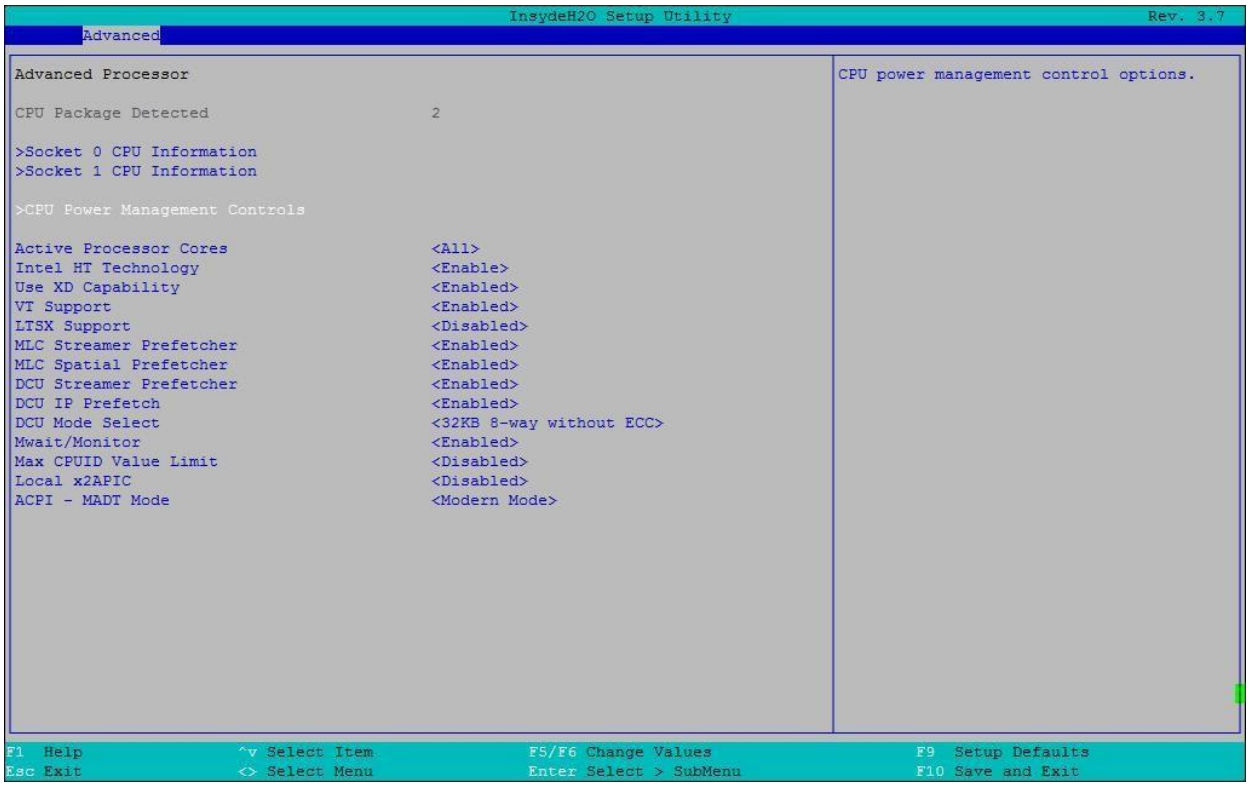


Рисунок 16-5. Меню Advanced Processor

Настройка BIOS	Опции	Описание
CPU Package Detected (Обнаружен процессорный пакет)	Нет вариантов	Количество заполненных пакетов CPU
Socket 0/1 CPU Information (Сокет 0/1 Информация о процессоре)	См. раздел 16.2.2.1.1	Подробная информация для сокета процессора 0 или 1
CPU Power Management Controls (Управление питанием процессора)	См. раздел 16.2.2.1.2	Возможности управления питанием процессора

Настройка BIOS	Опции	Описание
Active Processor Cores (Активные процессорные ядра)	Все 1 2 3 4 5 6 7	Количество ядер, которые можно включить в каждом пакете процессора
Intel HT Technology (Технология Intel HT)	Отключено Включено	Когда 'Выключено' разрешено только по одному потоку на каждое ядро
Use XD Capability (Использовать возможности XD)	Отключено Включено	Включение или отключение возможности XD процессора
VT Support (Поддержка VT)	Отключено Включено	Включение/выключение технологии Virtualization Technology
LTSX Support (Поддержка LTSX)	Отключено Включено	Технология LaGrande Включение/выключение
MLC Streamer Prefetcher	Отключено Включено	Позволяет включать и отключать аппаратную предварительную выборку стримера данных и инструкций из оперативной памяти в кеш L2 (MLC, Mid-Level Cache) для настройки производительности процессора. По умолчанию — Enabled (Включено)
MLC Spatial Prefetcher	Отключено Включено	Позволяет включать и отключать предвыборку смежной линии кеша L2 (MLC) для сокращения времени задержки кеша и настройки производительности для конкретного использования. По умолчанию — Enabled (Включено)
DCU Streamer Prefetcher	Отключено Включено	Позволяет включать и отключать предвыборку стримера блока кеша данных (L1 Data Cache Unit). По умолчанию — Enabled (Включено)

Настройка BIOS	Опции	Описание
DCU IP Prefetch	Отключено Включено	Позволяет включать и отключать, основанную на адресах инструкцию (IP — Instruction Pointer-Based) предвыборку блока кеша данных (DCU) для настройки производительности процессора. По умолчанию — Enabled (Включено)
DCU Mode Select (Выбор режима DCU)	32KB 8-полосный без ECC	Выбор режима работы DCU (L1 Data Cache Unit). Выбор размера блока данных и тип памяти (с ECC или без ECC)
	16KB 4-полосный без ECC	
	16KB с ECC	
Mwait/Monitor	Отключено Включено	Включение/отключение инструкций Monitor и поддержки MWAIT
Max CPUID Value Limit (Ограничение максимального значения CPUID)	Отключено Включено	Ограничение максимального значения CPUID. Максимальное значение CPUID не должно превышать 3 (если максимальное значение CPUID > 3). Эта настройка бесполезна для ОС Windows
Local x2APIC	Отключено Включено	Включить/выключить локальный x2APIC. Некоторые операционные системы не поддерживают эту функцию. Для этой функции необходима поддержка ACPI 4.0 и прерывание перенаправления
ACPI – MADT Mode	Legacy Mode Modern Mode	Позволяет выбрать режимы Legacy или Modern для ACPI MADT (Multiple APIC Description Table) нумерации процессоров, Legacy: для Win2000 или более ранних операционных систем, Modern: WinXP или более поздних ОС

16.2.2.1.1. Advanced/Advanced Processor/Socket 0 CPU Information

Расширенные настройки/Расширенные настройки Процессора/Сокет 0, информация о процессоре

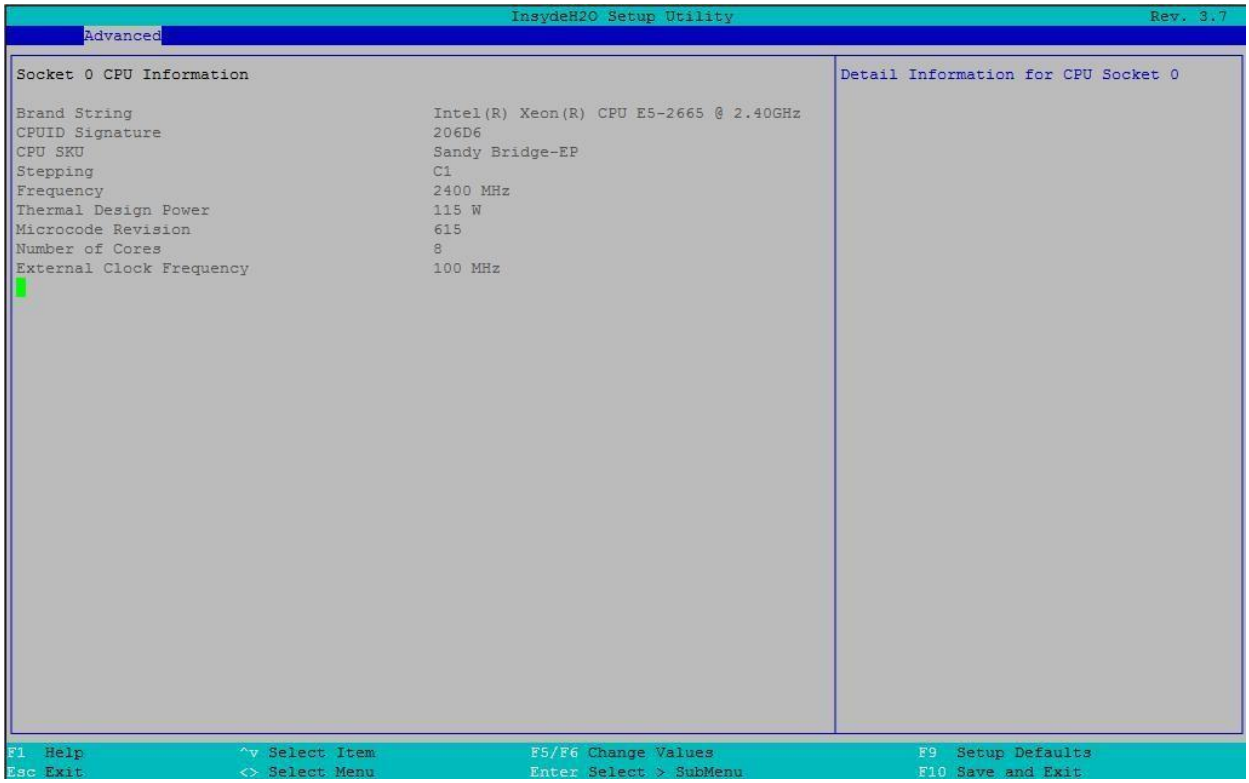


Рисунок 16-6. Меню Socket 0 CPU Information

Настройка BIOS	Опции	Описание
Brand String	Нет опций	Строка марки процессора на основе CPUID (80000002h, 80000003h, 80000004h)
CPUID Signature	Нет опций	Подпись процессора CPUID 01h
CPU SKU	Нет опций	Тип SKU процессора. Возможные значения: Sandy Bridge-EP4S, Sandy Bridge-EP или Sandy Bridge-EN
Stepping	Нет опций	Процессорный шаг
Frequency	Нет опций	Текущая частота процессора в МГц
Thermal Design Power	Нет опций	Тепловая схема питания процессора
Microcode Revision	Нет опций	Ревизия версии микрокода
Number of Cores	Нет опций	Количество ядер в данном процессоре

Настройка BIOS	Опции	Описание
External Clock Frequency	Нет опций	Внешняя тактовая частота

16.2.2.1.2. Advanced/Advanced Processor/CPU Power Management Controls

Расширенные настройки/Расширенные настройки Процессора/Управление питанием процессора

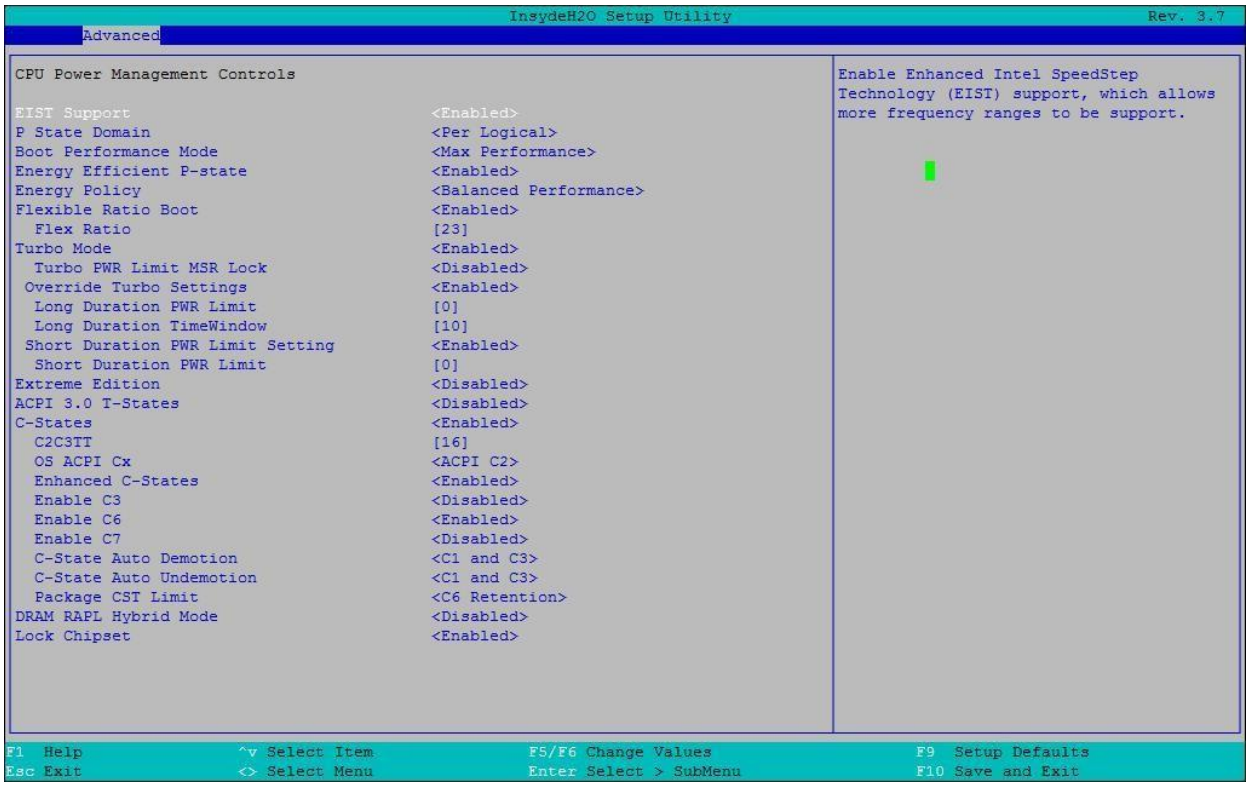


Рисунок 16-7. Меню CPU Power Management Controls

Настройка BIOS	Опции	Описание
EIST Support	Отключено/ Включено	Включите поддержку расширенной технологии Intel SpeedStep (EIST), которая позволяет поддерживать большее количество частотных диапазонов
P State Domain	Per Logical/Per Package	Выберите, какой домен — P-state — логический или пакетный
Boot Performance Mode	Максимальная производительность Максимальная эффективность	Выберите состояние производительности, которое BIOS установит перед выключением ОС

Настройка BIOS	Опции	Описание
Energy Efficient P-State	Отключено/ Включено	Включение/выключение функции энергосберегающего состояния
Energy Policy	Производительность Баланс производительности и энергоэффективности Энергоэффективность	Энергоэффективность используется процессором для внутреннего контроля параметров соотношения мощности и производительности
Flexible Ratio Boot	Отключено/ Включено	Включение/выключение гибкой загрузки с заданным соотношением сторон
Flex Ratio	Значение регулировки [Максимальное эффективное соотношение — Максимальное не турбо соотношение]	Настройте коэффициент гибкости между максимальным нетурбо-коэффициентом и максимальным коэффициентом полезного действия
Turbo Mode	Отключено/ Включено	Включить режим турборежима процессора (требуется также включение EMTTM)
Turbo PWR Limit MSR Lock	Отключено/ Включено	Для блокировки настроек турборежима. Рекомендуется оставить MSR разблокированным для OS/SW модификации
Override Turbo Settings	Отключено/ Включено	Включение/выключение различных настроек турборежима
Long Duration PWR Limit	Значение настройки [0 – 150]	Предел мощности турборежима (1) в Ваттах. Значение может варьироваться от 0 до Fused Value. Значение 0 будет запрограммировано на значение предохранителя. Значение TDP, превышающее значение плавления, не будет запрограммировано

Настройка BIOS	Опции	Описание
Long Duration TimeWindow	Значение настройки [0 – 128]	Временное окно, в секундах, предела мощности. Указывает на временное окно, в течение которого должно поддерживаться значение TDP. Значение 0 будет запрограммировано на значение предохранителя
Short Duration PWR Limit Setting	Отключено/ Включено	Включить/выключить. Ограничение мощности (Ограничение мощности 2)
Short Duration PWR Limit	Значение настройки [0 – 180]	Ограничение мощности турборежима (2) в ваттах. Значение 0 будет запрограммировано на 1.2*TDP
Extreme Edition	Отключено/ Включено	Включение или отключение поддержки Extreme Edition
ACPI 3.0 T-state	Отключено/ Включено	Включение/выключение T-состояний ACPI 3.0
C-States	Отключено/ Включено	Включение состояний энергосбережения процессора в режиме ожидания (C-состояния)
C2C3TT	Значение настройки [1 – 255]	Таймер перехода от C2 к C3
OS ACPI Cx	ACPI C2 ACPI C3	Отчет CC3/CC6 для ОС ACPI C2 или ACPI C3
Enhanced C-states	Отключено/ Включено	Обеспечивает возможность перехода от одного P-State к другому в сочетании с C-States
Enable C3	Отключено/ Включено	Включить/выключить Core C3
Enable C6	Отключено/ Включено	Включить/выключить Core C6
Enable C7	Отключено/ Включено	Включить/выключить Core C7

Настройка BIOS	Опции	Описание
C-State Auto Demotion	Отключен Только C1 Только C3 C1 и C3	Разрешить/Отключить автоматическое понижение C-State
C-State Auto Undemotion	Отключен Только C1 Только C3 C1 и C3	Разрешить/Отключить Автоматическую отмену удаления в C-State
Package CST Limit	C0/C1 C2 C6 Неудержание C6 Удержание	Указание наименьшего значения C для данного пакета
DRAM RAPL Hybrid Mode	Отключено/ Включено	Включить/выключить гибридный режим DRAM RAPL
Lock Chipset	Отключено/ Включено	Решите, нужно ли устанавливать безопасную блокировку SMBus или нет

16.2.2.1.3. Advanced/Advanced Processor/Platform Information

Расширенные настройки/Расширенные настройки Процессора/Информация о платформе

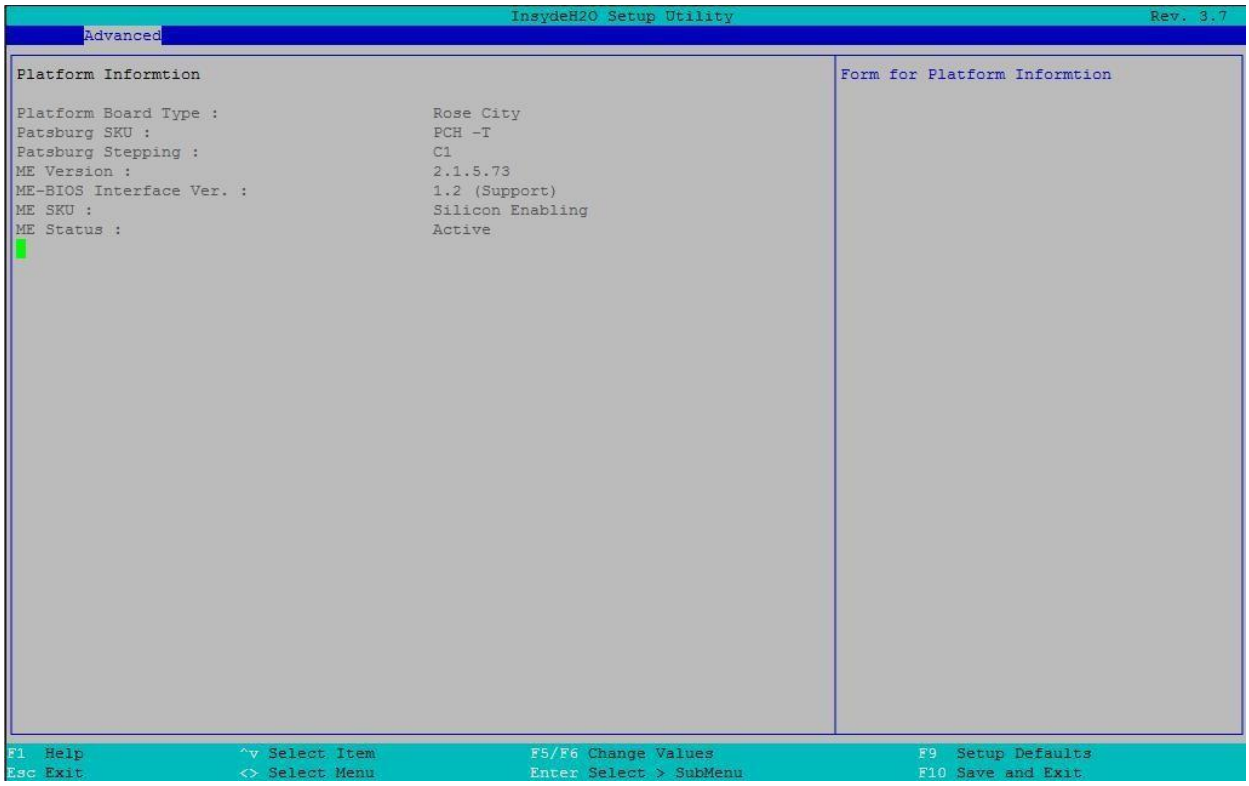


Рисунок 16-8. Меню Platform Information

Настройка BIOS	Опции	Описание
Platform Board Type	Нет	Описание типа платформы CRB. Rose City/Harbor City/River City/Potter City
Patsburg SKU	Нет	Описание PCH SKU. A/B/D/T SKU
Patsburg Stepping	Нет	Описание того, какой PCH Stepping. Бывший A2, B0, B1, C0, C1, C1
ME Version	Нет	Версия ME F/W
ME-BIOS Interface Ver	Нет	Описание версии интерфейса ME-BIOS. Это команда ME HECI для получения версии интерфейса (спецификация версии)
ME SKU	Нет	Описание ME SKU. Silicon Enabling/Node Manager/DNM/DM
ME Status	Нет	Статус включения/выключения ME

16.2.2.2. Advanced/Boot Configuration

Расширенные настройки/Конфигурация загрузки

Рисунок 16-9. Меню Boot Configuration

Настройка BIOS	Опции	Описание
SCU Resolution	640×480 800×600 1024×768	Изменение разрешения программы настройки
Numlock	Вкл./Выкл.	Выбор состояние включения для Numlock

16.2.2.3. Advanced/Peripheral Configuration

Расширенные настройки/Периферийная конфигурация

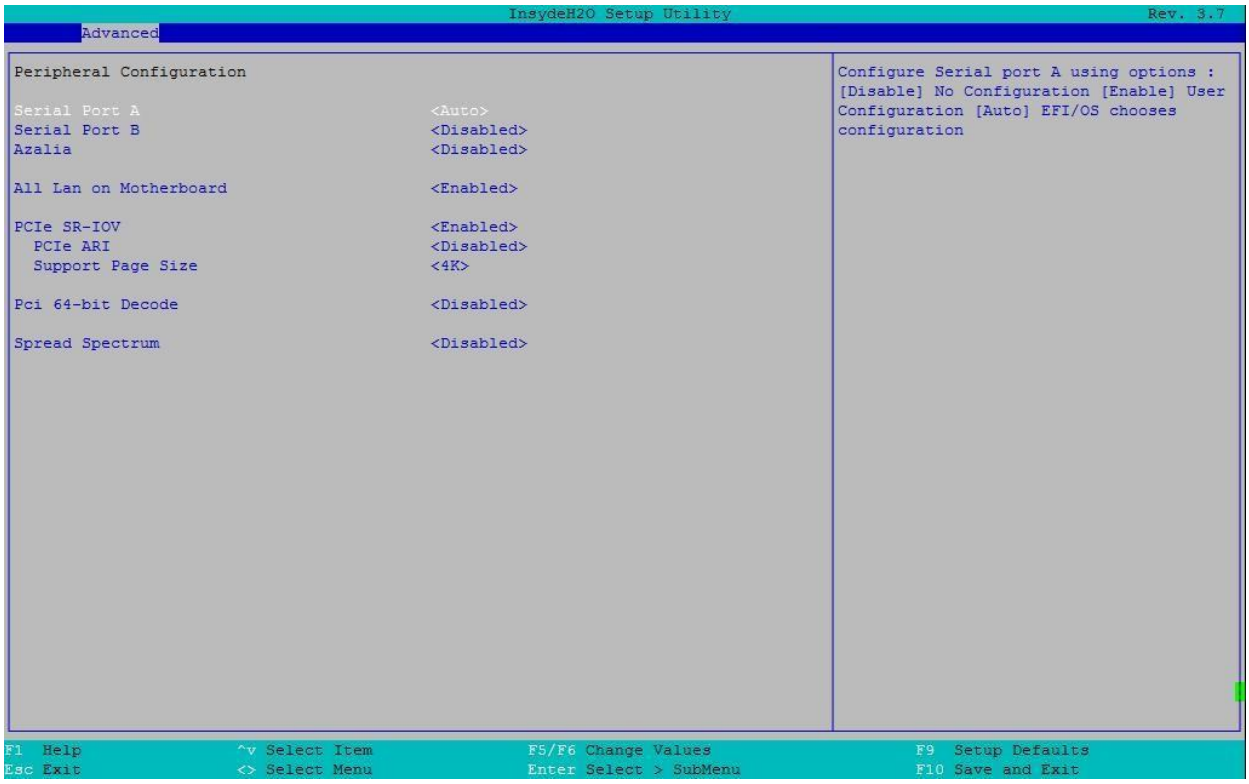


Рисунок 16-10. Меню Peripheral Configuration

Настройка BIOS	Опции	Описание
Serial Port A	Disabled Auto Enabled	Настройка параметров для последовательного порта A. [Disabled] отключит порт от использования. [Авто] позволит ОС выбрать конфигурацию последовательного порта. [Включено] позволит пользователю определить адрес ввода/вывода и настройки IRQ
Serial Port B	Disabled Auto Enabled	Настройка параметров для последовательного порта B. [Disabled] отключит порт от использования. [Авто] позволит ОС выбрать конфигурацию последовательного порта. [Включено] позволит пользователю определить адрес ввода/вывода и настройки IRQ
Azalia	Disable Enable	Включение/выключение кодека Azalia: отключить кодек Azalia: включить
All Lan on Motherboard	Disable Enable	Все контроллеры Lan на материнской плате включаются или выключаются

Настройка BIOS	Опции	Описание
PCIe SR-IOV	Disable Enable	Отключите функцию SR-IOV, если не используется карта PCIe Add-in. Включите функцию SR-IOV, если используется карта PCIe Add-in
PCIe ARI	Disable Enable	Включить/выключить ARI
Support Page Size	4K 8K 16K 64K 256K 1M 4M	Для настройки формата страницы при включении SR-IOV
PCIe 64-bits Decode	Disable Enable	Разрешить системе поддерживать 64-битный BAR для устройств PCIe
Spread Spectrum	Disable Enable	Включить/выключить настройку Spread Spectrum для уменьшения EMI

16.2.2.4. Advanced/SATA Configuration

Расширенные настройки/Конфигурация SATA

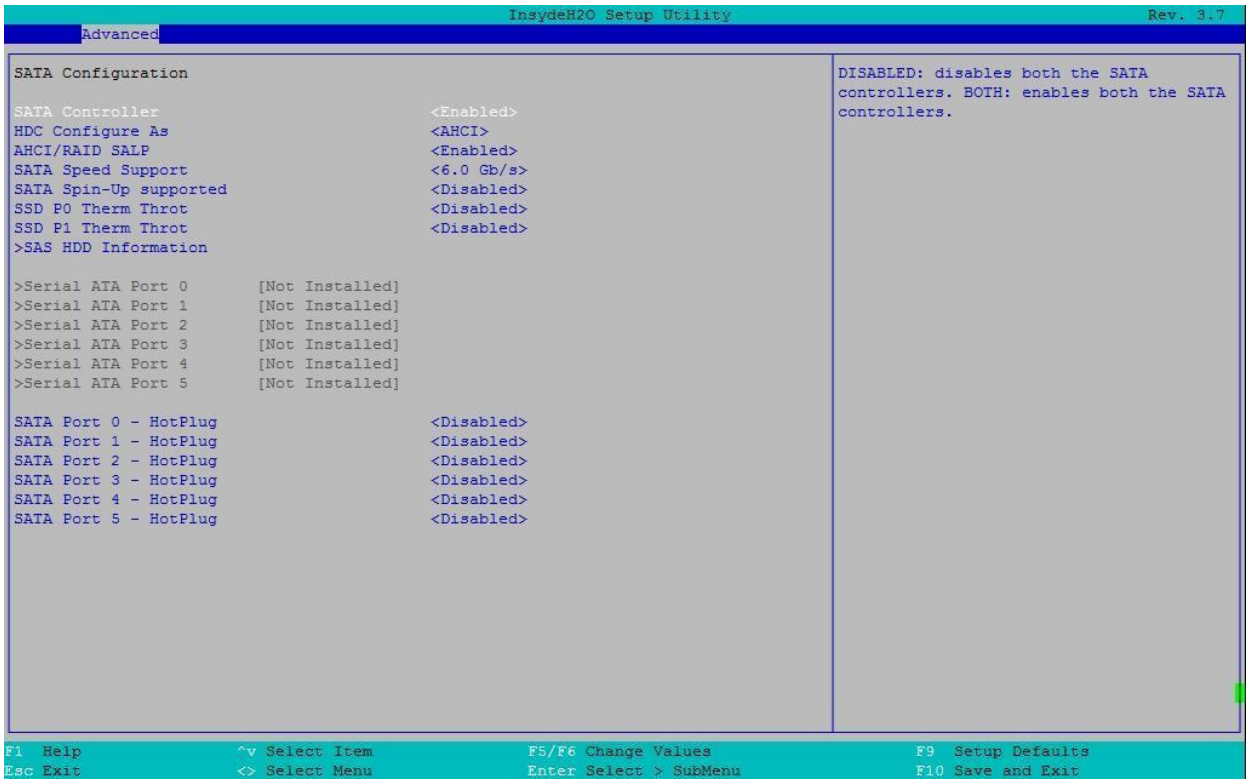


Рисунок 16-11. Меню SATA Configuration

Настройка BIOS	Опции	Описание
SATA Controller	Включено Отключено	Включение/выключение драйверов, связанных с SATA
HDC Configure As	IDE AHCI RAID	Установите контроллер SATA в режим IDE/AHCI/RAID
AHCI/RAID SALP	Включено Отключено	Включение/выключение поддержки AHCI/RAID
SATA Speed Support	1,5 Гбит/с 3,0 Гбит/с 6,0 Гбит/с	Указание максимальной скорости, которую контроллер SATA может поддерживать на своих портах. (Используется только в режиме AHCI/RAID)
SATA Spin-Up Support	Включено Отключено	При обнаружении от 0 до 1 PCH, запускает последовательность инициализации COMRESET для устройства

Настройка BIOS	Опции	Описание
SSD P0 Therm Throt	Включено Отключено	Включить параметр Thermal Throttling, если на порту 0/1 есть SSD. Отключить для HDD
SSD P1 Therm Throt	Включено Отключено	Включить параметр Thermal Throttling, если на порту 0/1 есть SSD. Отключить для HDD
SAS HDD Information	См. раздел 16.2.2.4.1	
SATA Port 0 – HotPlug	Включено Отключено	Включение/выключение SATA-порт 0 HotPlug
SATA Port 1 – HotPlug	Включено Отключено	Включение/выключение SATA-порт 1 HotPlug
SATA Port 2 – HotPlug	Включено Отключено	Включение/выключение SATA-порт 2 HotPlug
SATA Port 3 – HotPlug	Включено Отключено	Включение/выключение SATA-порт 3 HotPlug
SATA Port 4 – HotPlug	Включено Отключено	Включение/выключение SATA-порт 4 HotPlug
SATA Port 5 – HotPlug	Включено Отключено	Включение/выключение SATA-порт 5 HotPlug

16.2.2.4.1. Advanced/SATA Configuration/SAS HDD Information

Расширенные настройки/Конфигурация SATA/Информация о жестких дисках SAS

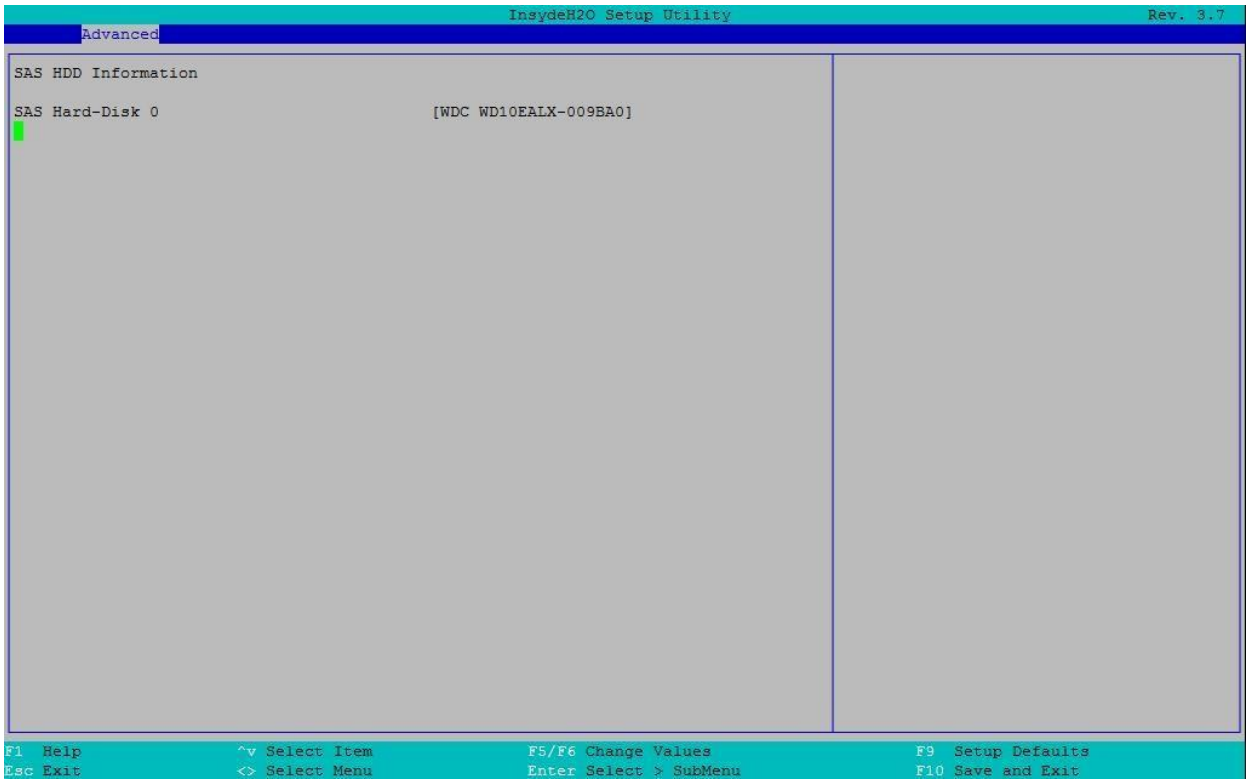


Рисунок 16-12. Меню SAS HDD Information

Настройка BIOS	Опции	Описание
SATA HDD-Disk X	Нет	Информация о жестких дисках на портах контроллера SCU

16.2.2.5. Advanced/Thermal Configuration

Расширенные настройки/Тепловая Конфигурация

Рисунок 16-13. Меню Thermal Configuration

Настройка BIOS	Опции	Описание
Platform Thermal Configuration	См. раздел 16.2.2.5.1	Тепловая конфигурация платформы
CPU Thermal Configuration	См. раздел 16.2.2.5.2	Тепловая конфигурация процессора

16.2.2.5.1. Advanced/Thermal Configuration/Platform Thermal Configuration

Расширенные настройки/Тепловая Конфигурация/Тепловая конфигурация платформы

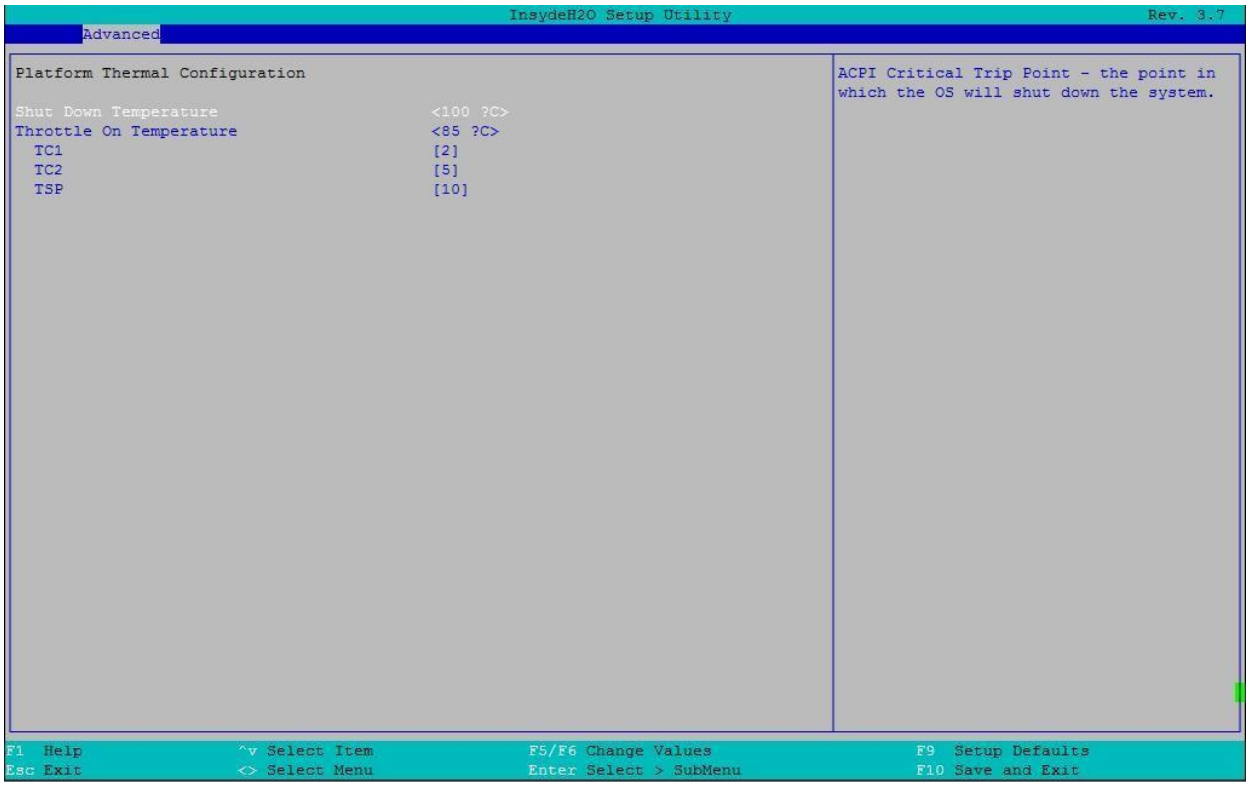


Рисунок 16-14. Меню Platform Thermal Configuration

Настройка BIOS	Опции	Описание
Shut Down Temperature	70 °C 75 °C 80 °C 85 °C 90 °C 100 °C 110 °C 120 °C	ACPI Критическая точка отключения — в критической точке операционная система отключит систему

Настройка BIOS	Опции	Описание
Throttle On Temperature	40 °C 45 °C 50 °C 55 °C 60 °C 65 °C 70 °C 75 °C 80 °C 85 °C 90 °C	Установите точку температуры процессора при включении
TC1	Значение настройки [1 – 16]	Температурная константа TC1 для формулы ACPI Passive Cooling (CPU Throttle On)
TC2	Значение настройки [1 – 16]	Температурная константа TC2 для формулы ACPI Passive Cooling (CPU Throttle On)
TSP	Значение регулировки [2 – 32]	В десятых долях секунды отображается, как часто ОС будет считывать температуру, когда включено пассивное охлаждение

16.2.2.5.2. Advanced/Thermal Configuration/Cpu Thermal Configuration

Расширенные настройки/Тепловая Конфигурация/Тепловая конфигурация процессора

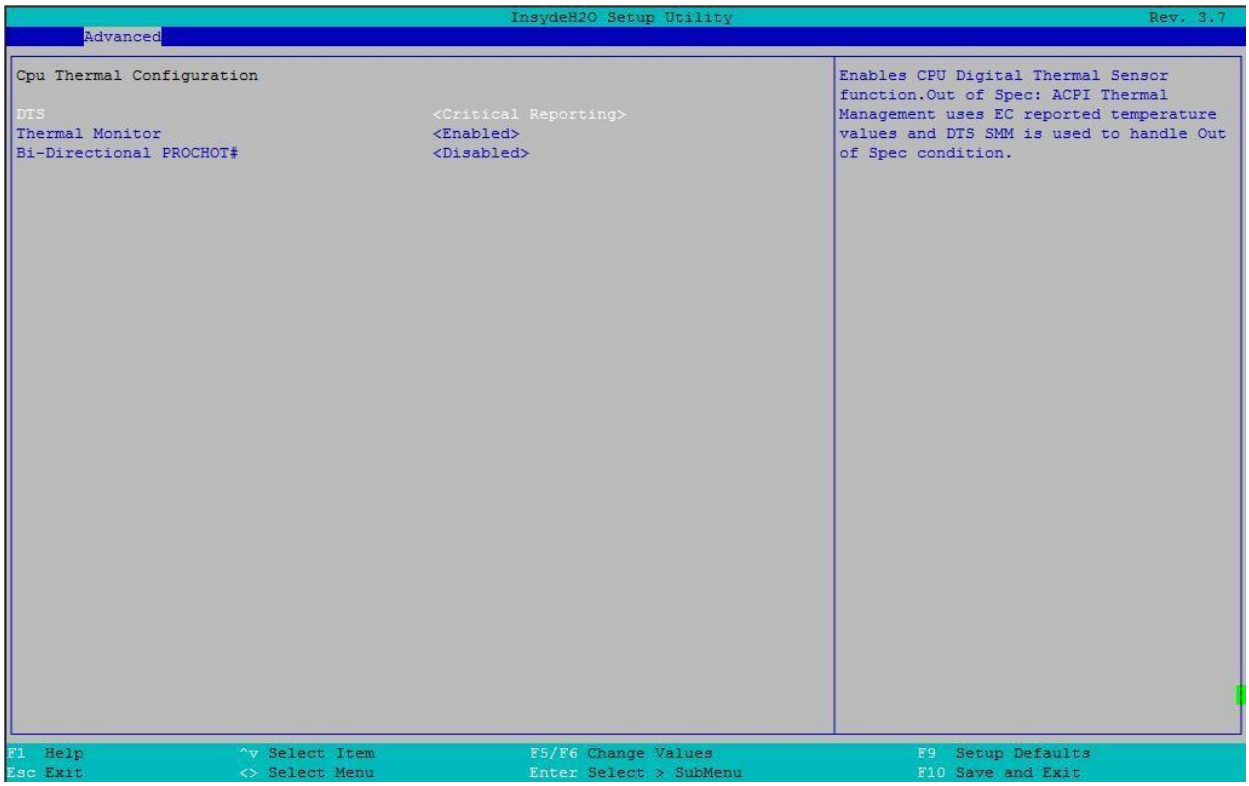


Рисунок 16-15. Меню Cpu Thermal Configuration

Настройка BIOS	Опции	Описание
DTS	Отключено Включено Critical Reporting	Включает функцию цифрового термодатчика CPU. Выход из спецификации: ACPI Thermal Management использует значения температуры, о которых сообщалось в EC, а DTS SMM используется для обработки состояния вне спецификации
Thermal Monitor	Отключено Включено	Включение/выключение теплового монитора
Bi-Directional PROCHOT#	Отключено Включено	Когда срабатывает термодатчик процессора (любого из ядер), будет активирован PROCHOT#

16.2.2.6. Advanced/Video Configuration

Расширенные настройки/Конфигурация Видео

Рисунок 16-16. Меню Video Configuration

Настройка BIOS	Опции	Описание
Display Mode	On Board First Plug In First	Установка типа настройки режима отображения

16.2.2.7. Advanced/USB Configuration

Расширенные настройки/Конфигурация USB

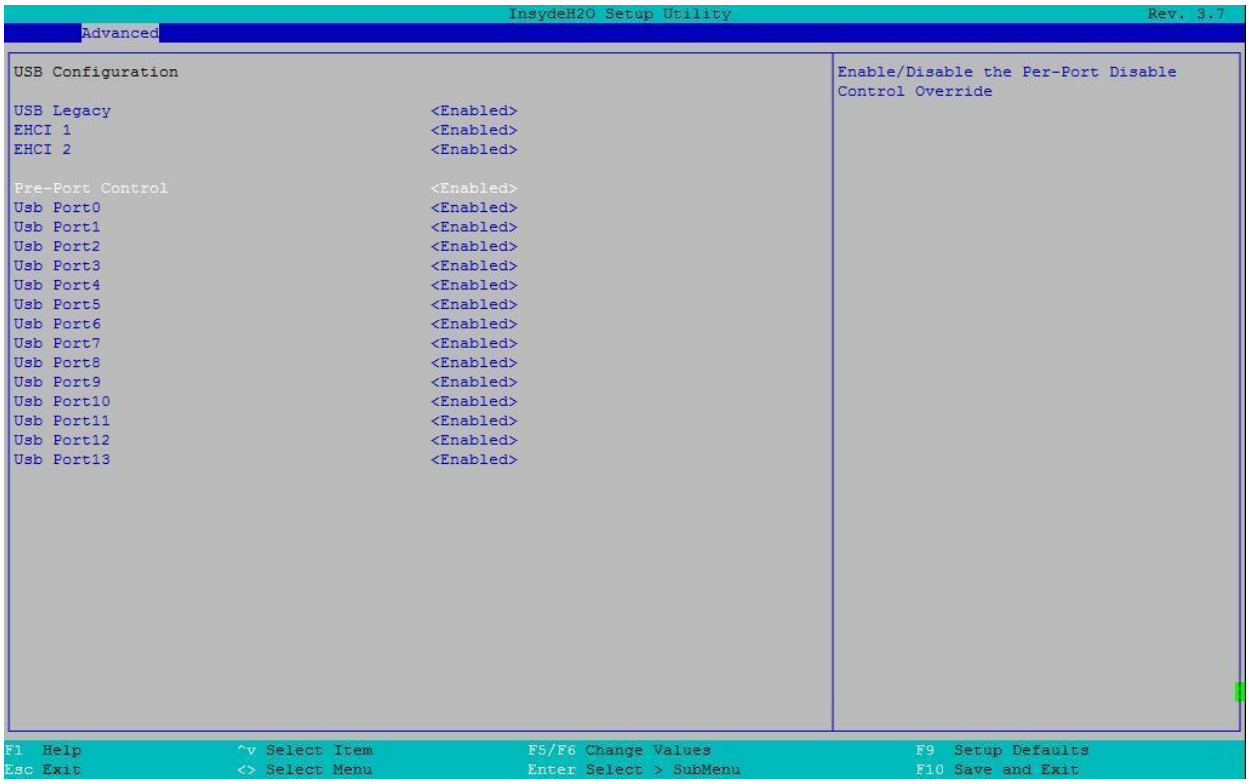


Рисунок 16-17. Меню USB Configuration

Настройка BIOS	Опции	Описание
USB Legacy	Отключить Включить	Загрузка USB-устройства и доступ к нему в устаревшей среде (например, DOS)
EHCI 1	Отключить Включить	Включение/выключение контроллера PCH EHCI 1
EHCI 2	Отключить Включить	Включение/выключение контроллера PCH EHCI 2
Per-Port Control	Отключить Включить	Позволяет пользователю управлять включением и выключением каждого USB-порта
Порт USB 0-13	Отключить Включить	Выключить/Включить порт USB

16.2.2.8. Advanced/PCH Chipset Configuration

Расширенные настройки/Конфигурация PCH-чипсета

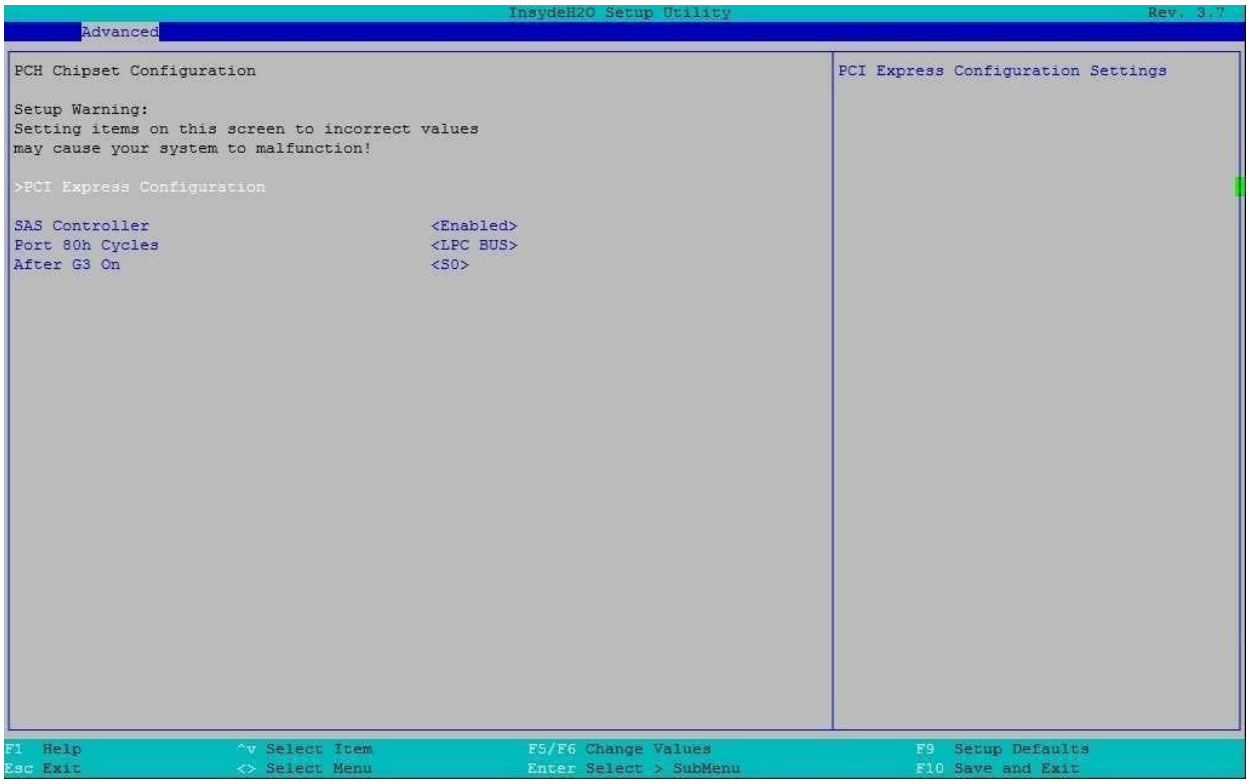


Рисунок 16-18. Меню PCH Chipset Configuration

Настройка BIOS	Опции	Описание
PCI Express Configuration	См. раздел 16.2.2.8.1	PCH Конфигурации корневого порта PCH PCIe
SAS Controller	Отключить Включить	Включение/выключение контроллера PCH SAS
Port 80h Cycles	LPC Bus PCI Bus	Установка режима работы порта 80h — LPC или PCI Bus
After G3 On	S0 S5 Last State	Установка режима платформенной ACPI после G3 (механическое выключение) в ACPI S0/S5/Last State

16.2.2.8.1. Advanced/PCH Chipset Configuration/PCI Express Configuration

Расширенные настройки/Конфигурация PCH-чипсета/Конфигурация PCI Express

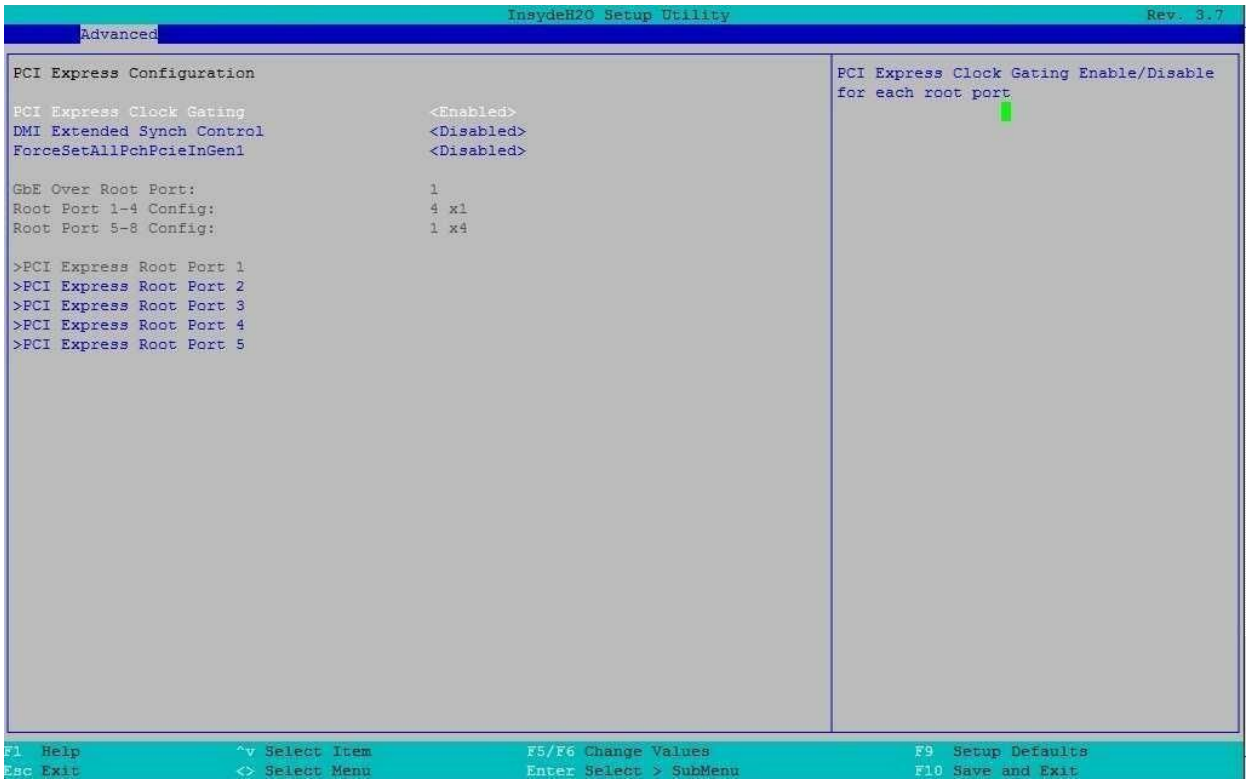


Рисунок 16-19. Меню PCI Express Configuration

Настройка BIOS	Опции	Описание
PCI Express Clock Gating	Отключить Включить	Включение/выключение синхронизации PCIe Clock Gating (энергосбережение)
DMI Extended Synch Control	Отключить Включить	Включение/выключение расширенного управления синхронизацией PCH DMI
ForceSetAllPchPci eInGen1	Отключить Включить	Установите все PCIe корневой порт PCH на 1-е поколение
After G3 On	S0 S5 Last state	Установите состояние платформы ACPI после G3 (механическое выключение) на ACPI S0/S5/Last state
PCI Express Root Port 1	См. раздел 16.2.2.8.2	Настройки корневого Порта 1 PCH PCI Express
PCI Express Root Port 2	См. раздел 16.2.2.8.2	Настройки корневого Порта 2 PCH PCI Express

Настройка BIOS	Опции	Описание
PCI Express Root Port 3	См. раздел 16.2.2.8.2	Настройки корневого Порта 3 PCH PCI Express
PCI Express Root Port 4	См. раздел 16.2.2.8.2	Настройки корневого Порта 4 PCH PCI Express
PCI Express Root Port 5	См. раздел 16.2.2.8.2	Настройки корневого Порта 5 PCH PCI Express
PCI Express Root Port 6	См. раздел 16.2.2.8.2	Настройки корневого Порта 6 PCH PCI Express
PCI Express Root Port 7	См. раздел 16.2.2.8.2	Настройки корневого Порта 7 PCH PCI Express
PCI Express Root Port 8	См. раздел 16.2.2.8.2	Настройки корневого Порта 8 PCH PCI Express

16.2.2.8.2. Advanced/PCH Chipset Configuration/PCI Express Configuration/PCI Express Root Port

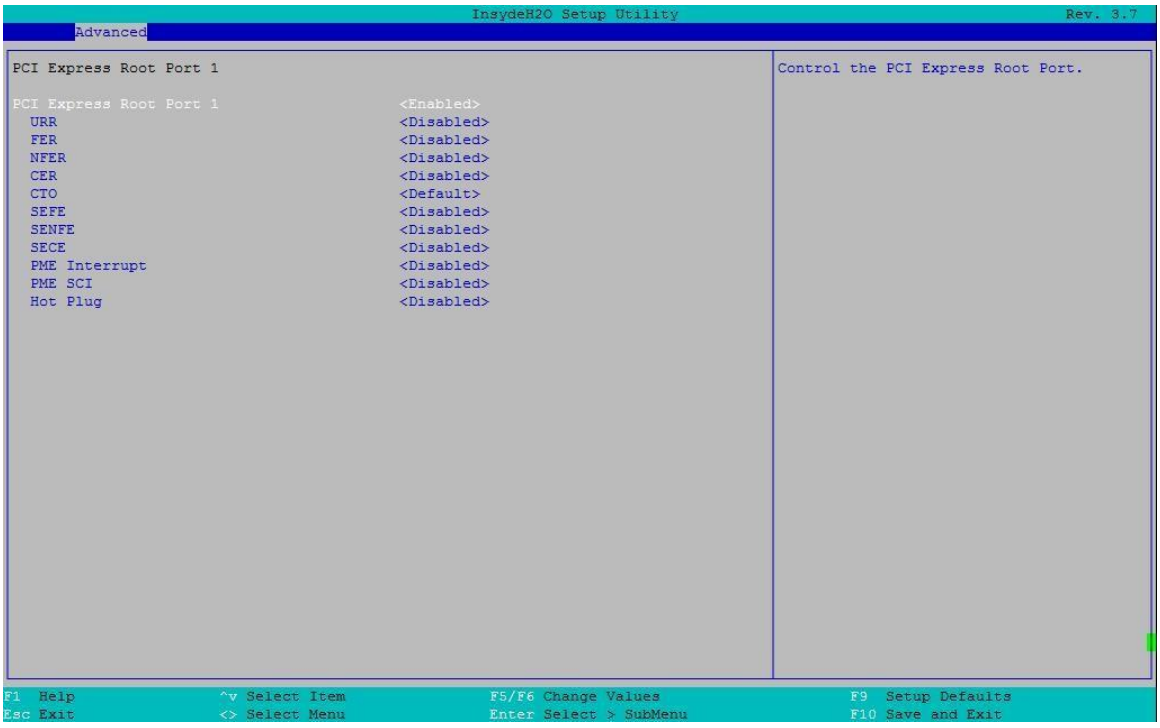


Рисунок 16-20. Меню PCI Express Root Port

Настройка BIOS	Опции	Описание
PCI Express Root Port 1	Отключено Включено	Управление корневым портом PCI Express Root Port
URR	Отключено Включено	Отчет о неподдерживаемых запросах PCI Express
FER	Отключено Включено	Отчет о фатальных ошибках устройства PCI Express
NFER	Отключено Включено	Сообщения о нефатальных ошибках устройства PCI Express
CER	Отключено Включено	Сообщение об исправляемых ошибках устройства PCI Express
CTO	По умолчанию 16 – 55 мс 65 – 210 мс 260 – 900 мс 1,0 – 3,5 мс Отключено	Тайм-аут завершения работы устройства PCI Express
SEFE	Отключено Включено	Ошибка корневой системы PCI Express при фатальной ошибке
SENFE	Отключено Включено	Ошибка корневой системы PCI Express при не фатальной ошибке
SECE	Отключено Включено	Корневая ошибка системы PCI Express при исправлении
PME interrupt	Отключено Включено	Корневое прерывание PCI Express PME
PME SCI	Отключено Включено	PCI Express PME SCI Включение/выключение
Hot Plug SCI	Отключено Включено	PCI Express Hot Plug SCI Включение/выключение

16.2.2.9. Advanced/SandyBridge IIO Configuration

Расширенные настройки/Конфигурация SandyBridge IIO

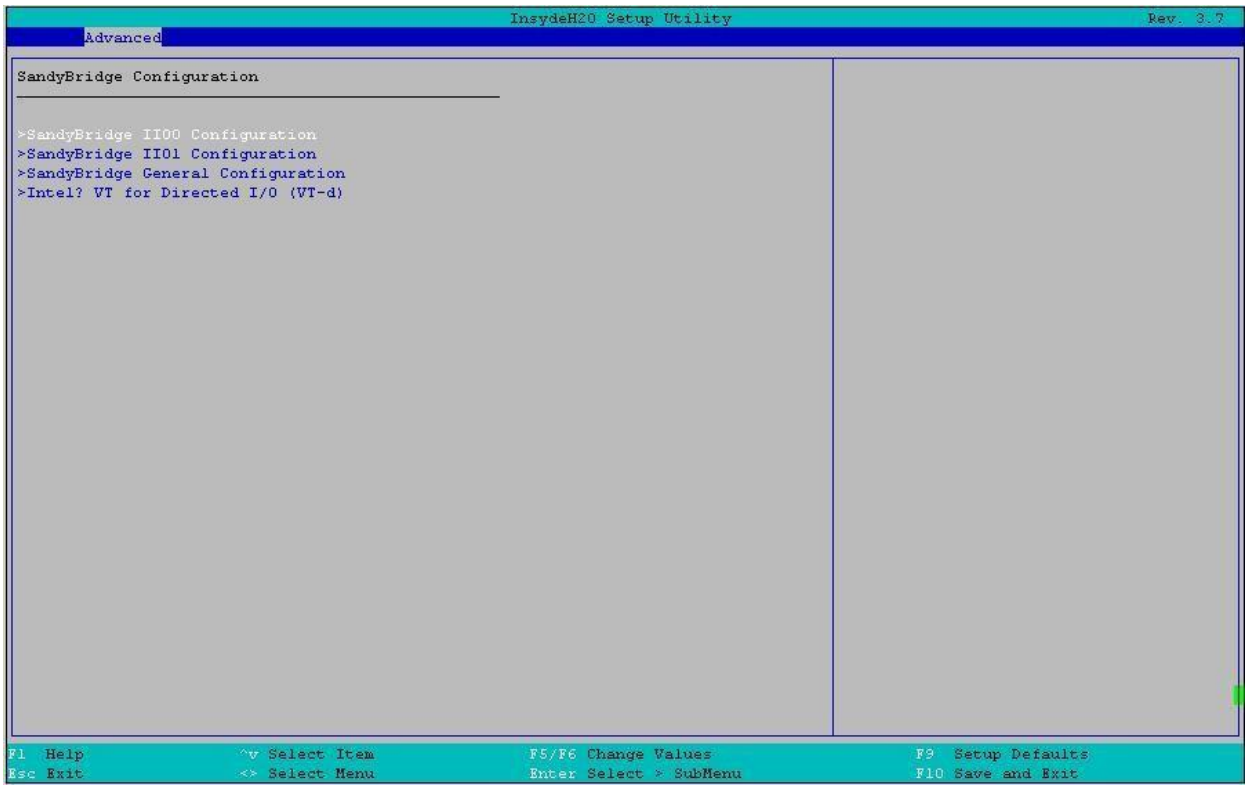


Рисунок 16-21. Меню SandyBridge IIO Configuration

Настройка BIOS	Опции	Описание
SandyBridge IIO0 Configuration	См. раздел 16.2.2.9.2	Конфигурирование IIO 0 PCIe
SandyBridge IIO1Configuration	См. раздел 16.2.2.9.2	Конфигурирование IIO 1 PCIe
SandyBridge General Configuration	См. раздел 16.2.2.9.3	Общая конфигурация для всех интерфейсов ввода/вывода
Intel VT for Directed I/O (VT-d)	См. раздел 16.2.2.9.4	Настройка VT-d

16.2.2.9.1. Advanced/SandyBridge IIO/ SandyBrideg IIO 0, 1

Расширенные настройки/Конфигурация SandyBridge IIO/SandyBrideg IIO 0, 1

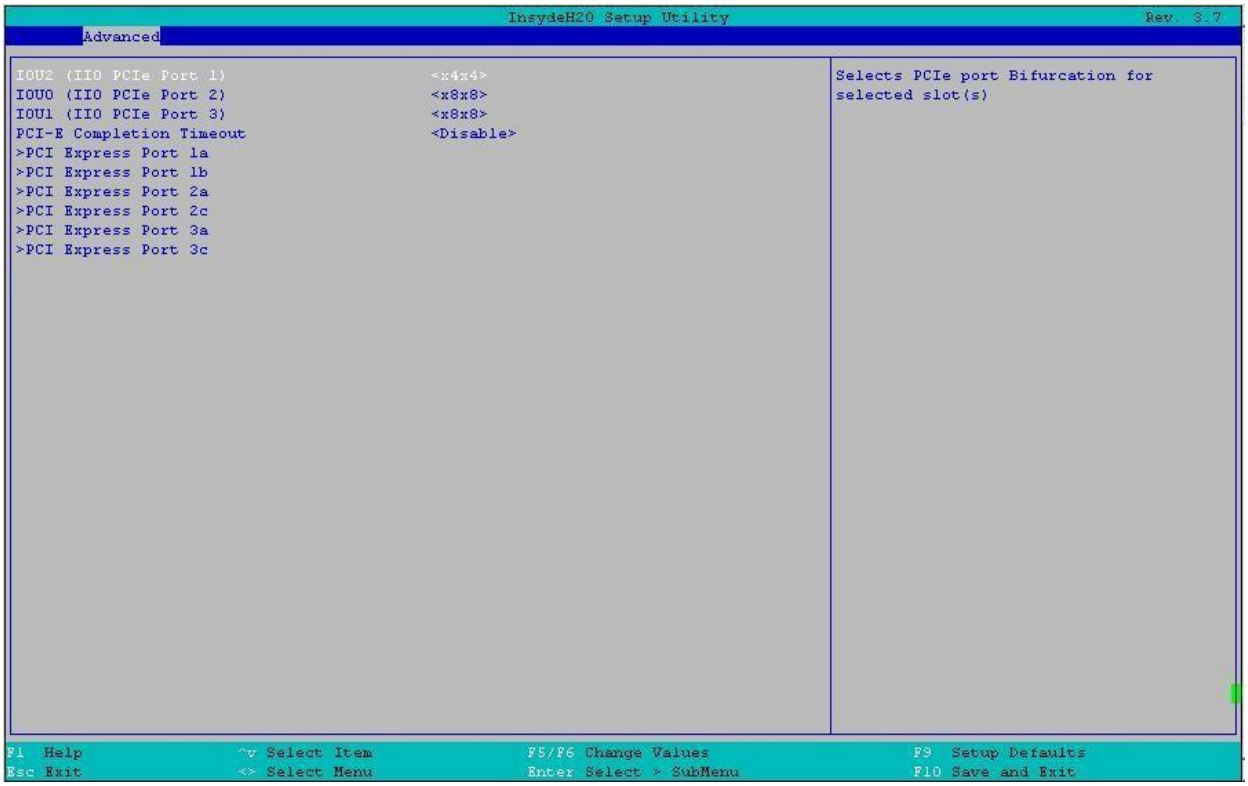


Рисунок 16-22. Меню SandyBrideg IIO 0, 1

Настройка BIOS	Опции	Описание
IOU2 (IIO PCIe Port 1)	x4x4 x8	Разделение PCIe для выбранного разъема(ов)
IOU0 (IIO PCIe Port 2)	x4x4x4x4 x4x4x8 x8x4x4 x16	Разделения PCIe для выбранного разъема(ов)
IOU1 (IIO PCIe Port 3)	x4x4x4x4 x4x4x8 x8x4x4 x16	Разделения PCIe для выбранного разъема(ов)
PCI-E Completion Timeout	Включить Отключить	Время завершения (D:x F:0 O:94h B:4) где x 0-9
Порт PCI Express 1a	См. раздел 16.2.2.9.2	Настройки, связанные с портом PCI Express 0-10
Порт PCI Express 1b	См. раздел 16.2.2.9.2	Настройки, связанные с портом PCI Express 0-10

Настройка BIOS	Опции	Описание
Порт PCI Express 2a	См. раздел 16.2.2.9.2	Настройки, связанные с портом PCI Express 0-10
PCI Express Port 2c	См. раздел 16.2.2.9.2	Настройки, связанные с портом PCI Express 0-10
Порт PCI Express 3a	См. раздел 16.2.2.9.2	Настройки, связанные с портом PCI Express 0-10
Порт PCI Express 3c	См. раздел 16.2.2.9.2	Настройки, связанные с портом PCI Express 0-10

16.2.2.9.2. Advanced/SandyBridge IIO/ SandyBridge IIO0, 1/PCI-E Port 0-3c

Расширенные настройки/Конфигурация SandyBridge IIO/SandyBrideg IIO 0, 1/PCI-E Port 0-3c

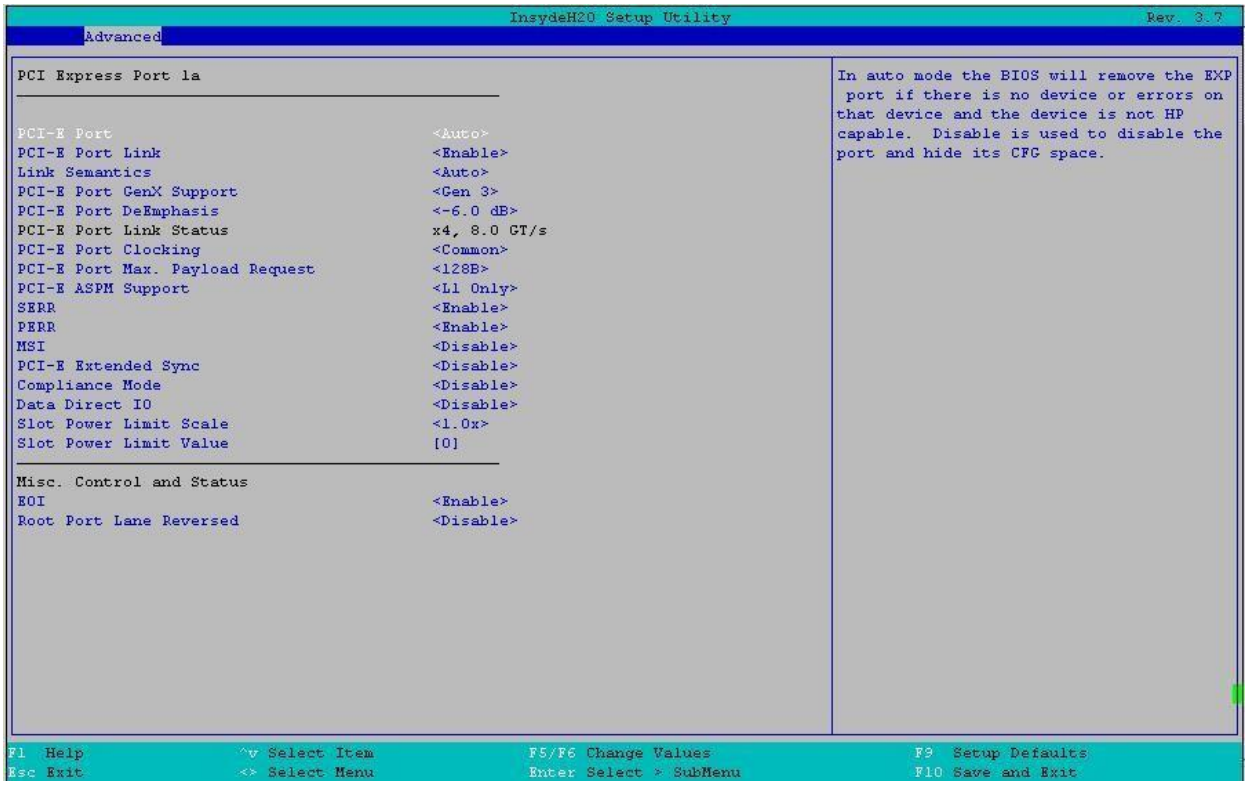


Рисунок 16-23. Меню PCI-E Port 0-3c

Настройка BIOS	Опции	Описание
PCI-E Port	Авто Включить Отключить	В автоматическом режиме BIOS удалит порт EXP

Настройка BIOS	Опции	Описание
PCI-E Port Link	Включить Отключить	Эта опция отключает ссылку, так что обучение не происходит, но пространство CFG все еще активно
Link Semantics	Авто Strict Gen1	Опция устанавливает режим ссылки на Gen 1
PCI-E Port GenX support	Gen 1 Gen 2 Gen 3	Выберите поддержку генерации PCIe для порта PCI Express. Для Gen1, пожалуйста, также установите De-Emphais = −6dB
PCI-E Port DeEmphasis	−6,0 дБ −3,5 дБ	Управление De-Emphais для данного порта PCIe
PCI-E Port Link Status	Нет	Показать состояние соединения с портом
PCI-E Port Clocking	Distinct Common	Это относится к этим компонентам и компоненту нисходящего потока
PCI-E Port Max. Payload Request	128 B 256 B Авто	Установите размер Max payload равным 256 B, если это возможно
PCI-E ASPM Support	Отключить Только L1	Эта опция включает/выключает поддержку ASPM (только L0s/L0s & L1) для последующих устройств
SERR	Отключить Включить	BUS0 DevX FUN0 Выкл 0x04 бит 8, где X равен 0 – 9
PERR	Отключить Включить	BUS0 DevX FUN0 Выкл 0x04 бит 6, где X равен 0 – 9
MSI	Отключить Включить	BUS0 DEVx FUN0 OFF 0x5A бит 0, где X равен 0 – 9
PCI-E Extended Sync	Отключить Включить	Включение/выключение расширенного режима синхронизации (D:x F:0 O:7Ch B:7), где x равен 0 – 9
Compliance Mode	Отключить Включить	Отключение/включение режима соответствия для данного порта PCIe

Настройка BIOS	Опции	Описание
Data Direct IO	Отключить Включить	Включает Data Direct IO
Slot Power Limit scale	1.0x 0.1x 0.01x 0.001x	Максимальная потребляемая мощность карты адаптера не более 255
Предельное значение слота	Значение настройки [0 – 255]	Предельное потребление энергии картой адаптера, макс. 255
EOI	Отключить Включить	Отключение/включение устройства 1 – 10 MISCCTRLSTS (Reg 0x188) Bit 26
Root Port Lane Reversed	Отключить Включить	Отключение/включение функции корневого порта изменять полосу движения

16.2.2.9.3. Advanced/SandyBridge IIO/ SandyBridge General Configuration

Расширенные настройки/SandyBridge IIO/SandyBridge общая конфигурация

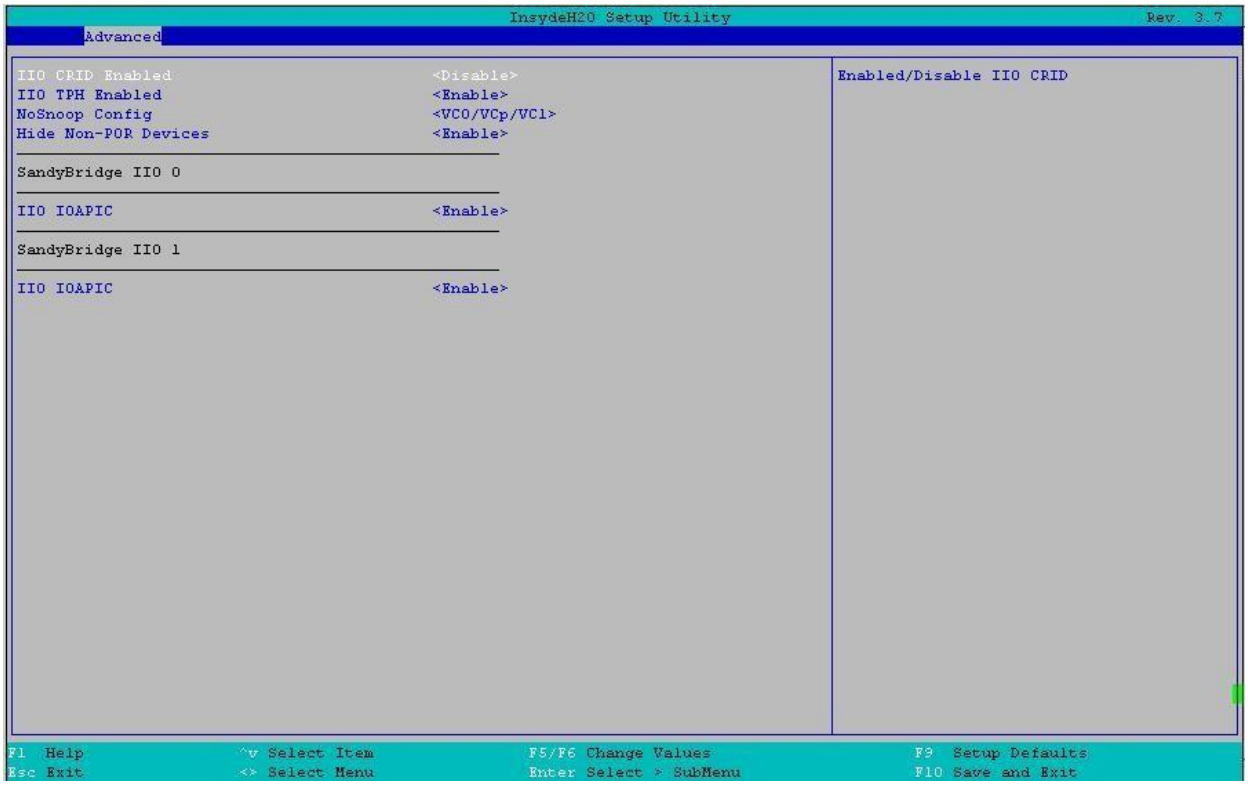


Рисунок 16-24. Меню SandyBridge General Configuration

Настройка BIOS	Опции	Описание
IIO CRID Enabled	Отключить Включить	Включение/выключение IIO CRID
IIO TPH Enabled	Отключить Включить	Включение/выключение IIO TPH
NoSnoop Config	VC0/VCp/VC1 VC0/VCp/VC1 VC1 VC1	NoSnoop конфигурация для VC0, VCp, VC1
Hide Non-POR Devices	Отключить Включить	Скрыть не POR-устройства
IIO IOAPIC	Отключить Включить	Разрешить/Отключить IIO IOAPIC

16.2.2.9.4. Advanced/SandyBridge IIO/ Intel VT for Directed I/O (VT-d)

Расширенные настройки/SandyBridge IIO/Intel VT для прямого ввода/вывода (VT-d)

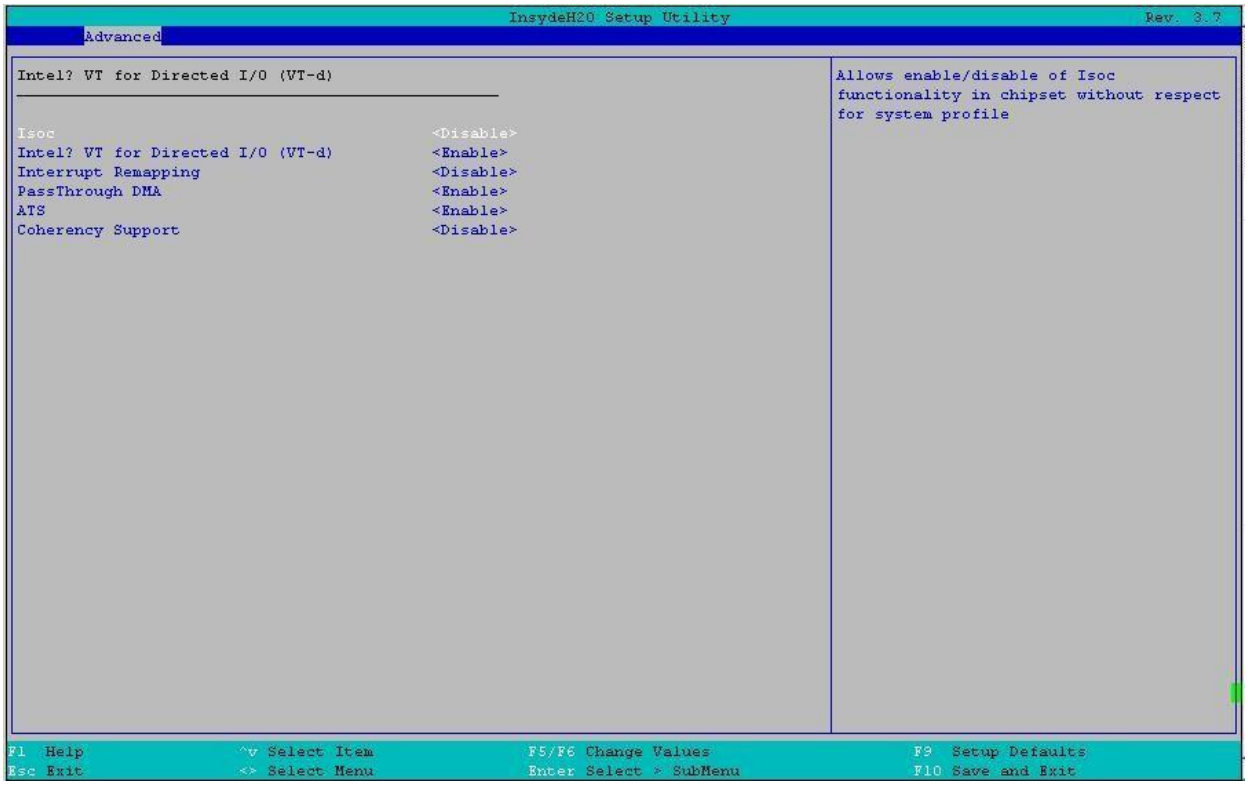


Рисунок 16-25. Меню Intel VT for Directed I/O (VT-d)

Настройка BIOS	Опции	Описание
Isoc	Включить Отключить АВТО	Позволяет включать/выключать функциональность Isoc в чипсете без учета профиля системы

Настройка BIOS	Опции	Описание
Intel VT for Directed I/O (VT-d)	Включить Отключить	Включите/отключите Intel Virtualization для I/O (VT-d)
Interrupt Remapping	Включить Отключить	Включение/выключение поддержки переопределения прерываний VT_D
PassThrough DMA	Включить Отключить	Включение/выключение Non-Iscoh VT_D, Engine PassThrough DMA
ATS	Включить Отключить	Включение/выключение поддержки Non-Iscoh VT_D Engine ATS
Coherency Support	Включить Отключить	Включение/выключение Non-Iscoh VT_D Engine Coherency support

16.2.2.10. Advanced/SandyBridge RC

Расширенные настройки/SandyBridge RC

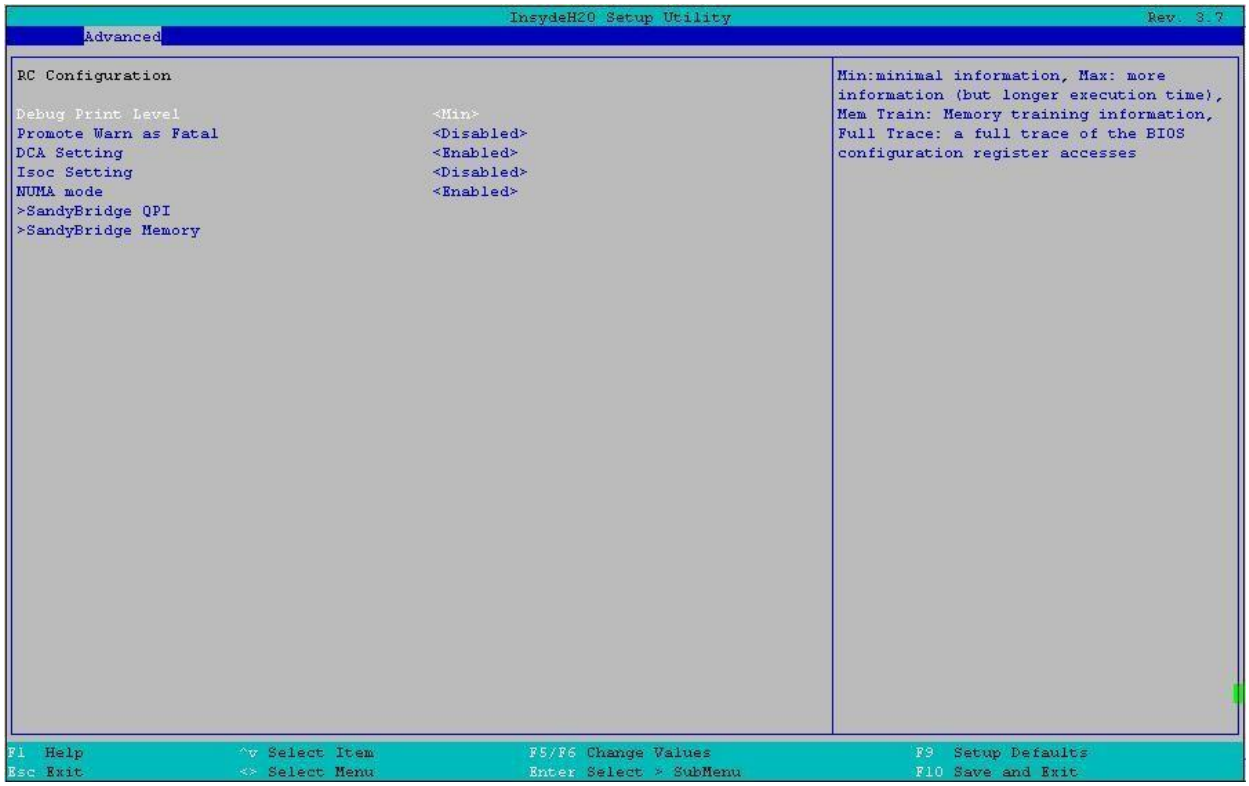


Рисунок 16-26. Меню SandyBridge RC

Настройка BIOS	Опции	Описание
Debug Print Level	Отключить Min Max Full trace Mem Train	Min: минимальная информация, Max: больше информации (но более длительное время выполнения), Mem Train: информация о трассировке памяти, Full Trace: полная трассировка обращений к регистру конфигурации BIOS
Promote Warn as Fatal	Включить Отключить	Включить/выключить предупреждение о фатальной ошибке
DCA Setting	Включить Отключить	Включить/выключить DCA
Isoc Setting	Включить Отключить	Включить/выключить Isoc
NUMA mode	Включить Отключить	Включить/выключить режим NUMA
>SandyBridge QPI	См. раздел 16.2.2.10.1	Относительная настройка QPI
>SandyBridge Memory	См. раздел 16.2.2.10.2	Относительная настройка памяти

16.2.2.10.1. Advanced/SandyBridge RC/SandyBridge QPI

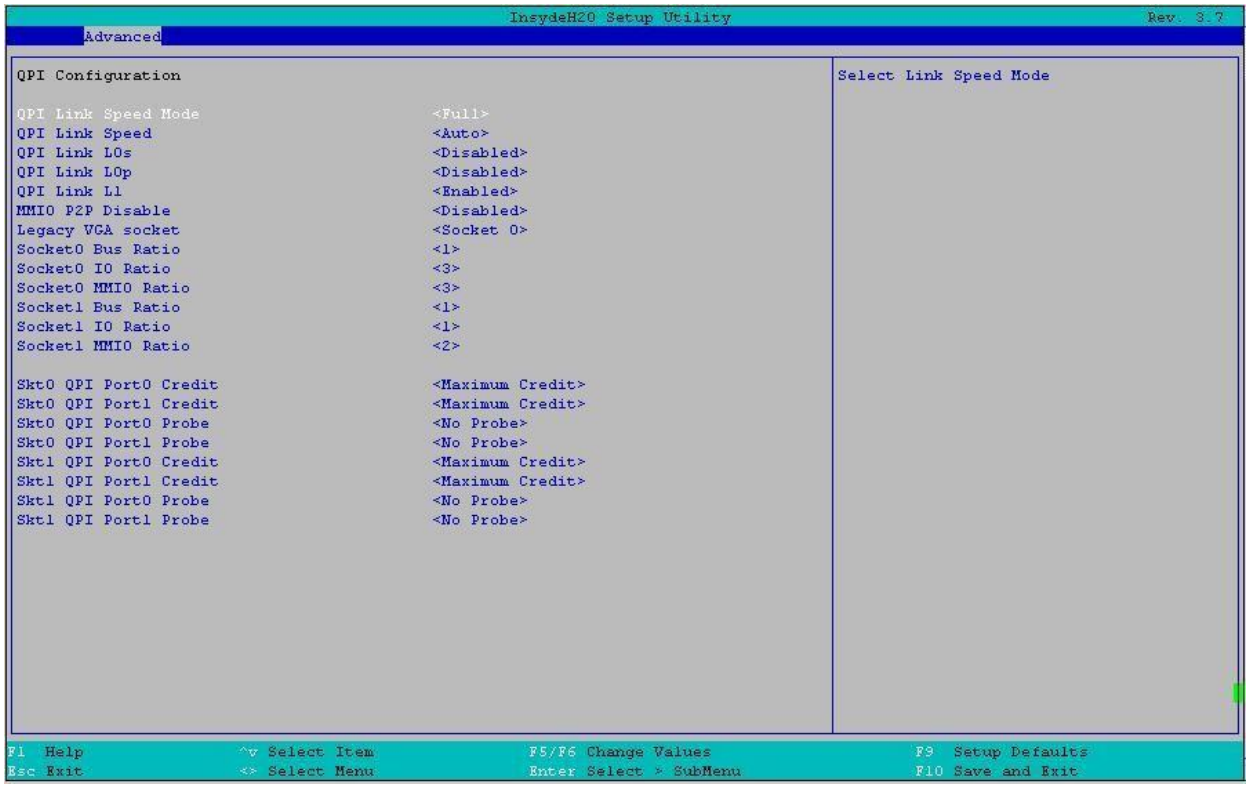


Рисунок 16-27. Меню SandyBridge QPI

Настройка BIOS	Опции	Описание
QPI Link Speed Mode	Медленный/ Быстрый	Выбор режима скорости соединения
QPI Link Speed	Авто 6,4 ГТ/с 7,2 ГТ/с 8,0 ГТ/с	Выберите скорость соединения: 6,2 ГТ/с, 7,2 ГТ/с, 8,0 ГТ/с
QPI Link L0s	Отключено/ Включено	Включить/отключить связь QPI L0s
QPI Link L0p	Отключено/ Включено	Включить/отключить связь QPI L0p
QPI Link L1	Отключено/ Включено	Включить/отключить связь QPI L1

Настройка BIOS	Опции	Описание
MMIO P2P Disable	Отключено/ Включено	Эта опция контролирует P2P-трафик через сокеты. Это не влияет на P2P-трафик
Legacy VGA socket	Socket 0 Socket 1 Socket 2 Socket 3	Выбор legacy VGA socket
Socket0/1 Bus Ratio	1 2 3 4	Настроить коэффициент шины Socket 0/1
Socket0/1 IO Ratio	1 2 3 4	Настройка соотношения входных и выходных разъемов 0/1
Socket0/1 MMIO Ratio	1 2 3 4	Настройка соотношения розеток 0/1 MMIO
Skt0/1 QPI Port 0/1 Credit	Maximum Credit/Force Reduce	Настройка операция с уменьшенным количеством ссылок
Skt0/1 QPI Port 0/1 Probe	No Probe/COHASSET VSR	Указание типа средней шины

16.2.2.10.2. Advanced/SandyBridge RC/SandyBridge Memory

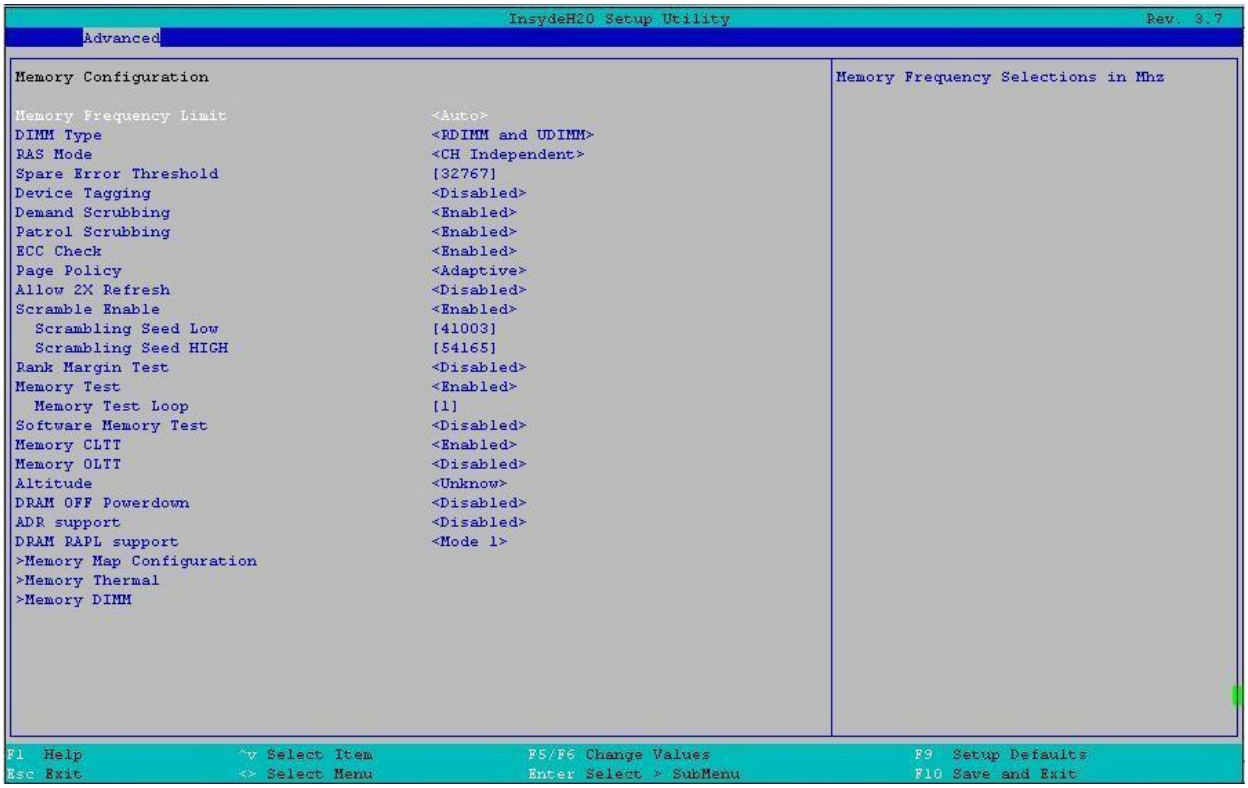


Рисунок 16-28. Меню SandyBridge Memory

Настройка BIOS	Опции	Описание
Memory Frequency Limit	Авто 800 1066 1333 1600 1867	Выбор частоты памяти в МГц
DIMM Type	RDIMM только UDIMM только RDIMM и DIMM	Выбор типа DIMM
RAS Mode	CH Independent CH Mirroring CH LockStep Rank Spare Rank Spare/CH Lock	Выбор режима RAS

Настройка BIOS	Опции	Описание
Spare Error Threshold	Регулируемое значение [1 – 32 767]	Порог ошибки. Содержит количество исправляемых ошибок ECC, требуемых до запуска события SMI. Это значение будет запрограммировано в полях cor_err_th_0 и cor_err_th_1 регистров CORRERRTHRSHLD для всех каналов и всех сокетов. Значение по умолчанию 0x7FFF (32 767). Максимальное значение 0x7FFF (32 767)
Device Tagging	Включено Отключено	Включение/выключение метки устройства
Demand Scrubbing	Включено Отключено	Включить/выключить очистку по требованию
Patrol Scrubbing	Включено Отключено	Включить/выключить очистку
ECC Check	Включено Отключено	Включить/выключить проверку ECC
Page Policy	Закрыть Открыть Адаптивный	Выбор политики страницы
Allow 2X Refresh	Включено Отключено	Включить/выключить 2X-обновление
Scramble Enable	Включено Отключено	Включить/выключить Scramble
Scrambling Seed Low	Отрегулируйте значение [1 – 65 535]	Установите значение Scramble для шифрования данных низкого уровня
Scrambling Seed HIGH	Отрегулируйте значение [1 – 65 535]	Установите значение Scramble для шифрования данных высокого уровня
Rank Margin Test	Включено Отключено	Включить/выключить тест на разницу в уровне памяти, длина по умолчанию 1000

Настройка BIOS	Опции	Описание
Memory Test	Включено Отключено	Включить тест памяти
Memory Test Loop	Отрегулируйте значение [1 – 65 535]	Установить значение цикла тестирования памяти, минимум 1, максимум 65 535
Software Memory Test	Включено Отключено	Включить тест памяти программного обеспечения
Memory CLTT	Включено Отключено	Включить/выключить память CLTT
Memory OLTT	Включено Отключено	Включить/выключить память OLTT
Altitude	Неизвестно 300 м или менее 301 м – 900 м 901 – 1500 м Выше 1500 м	Выбор Altitude для расчетов теплового регулирования памяти
DRAM OFF Powerdown	Включено Отключено	Если установлено, включает режим медленного отключения DRAM OFF в DIMM при выполнении самообновления
ADR support	Включено Отключено	Позволяет обнаруживать и активировать ADR
DRAM RAPL support	Отключен режим 0 Режим 1	Выбор того, будет ли код ссылки инициализироваться и активировать DRAM RAPL
>Memory Map Configuration	См. раздел 16.2.2.10.3	Относительная настройка карты памяти
>Memory Thermal	См. раздел 16.2.2.10.4	Тепловая относительная настройка памяти
>Memory DIMM	См. раздел 16.2.2.10.5	Показывать/настраить информацию о DIMM-памяти

16.2.2.10.3. Advanced/SandyBridge RC/.../Memory Map Configuration

Конфигурация карты памяти

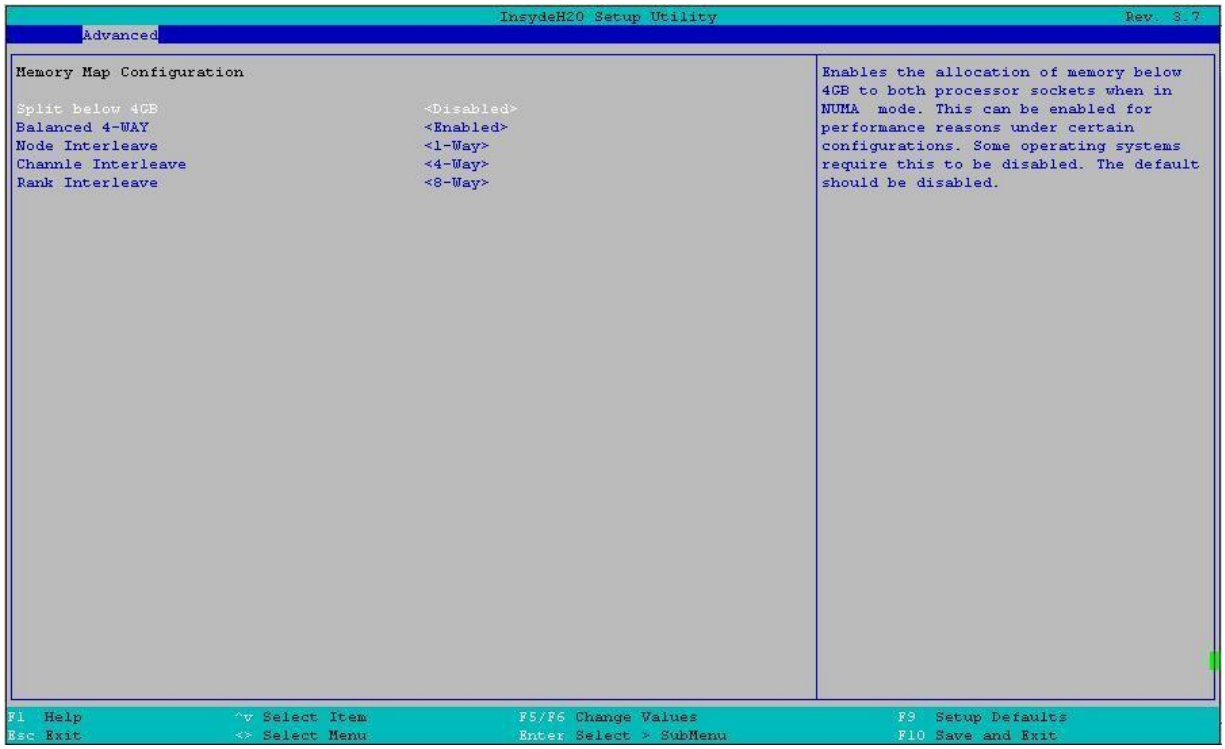


Рисунок 16-29. Меню Memory Map Configuration

Настройка BIOS	Опции	Описание
Split below 4 ГБ	Отключено Включено	Позволяет распределить память емкостью менее 4 ГБ между обоими сокетами процессора в NUMA режиме. Это может использоваться по причинам низкой производительности при определенных конфигурациях. Некоторые операционные системы требуют, чтобы эта функция была отключена. Значение по умолчанию — отключено
Balanced 4-WAY	Включено Отключено	Включает более оптимальный способ объединения Non-NUMA DP платформ, имеющих конфигурацию каналов 2-1-1 (2 DIMM на один канал и 1 DIMM на два других канала)
Node Interleave	Авто 1-Way 2-Way 4-Way	Настройка чередования узлов

Настройка BIOS	Опции	Описание
Channle Interleave	Авто 1-Way 2-Way 3-Way 4-Way	Настройка чередования каналов
Rank interleave	Авто 1-Way 2-Way 4-Way 8-Way	Настройка чередования рангов

16.2.2.10.4. Advanced/SandyBridge RC/.../Memory Thermal

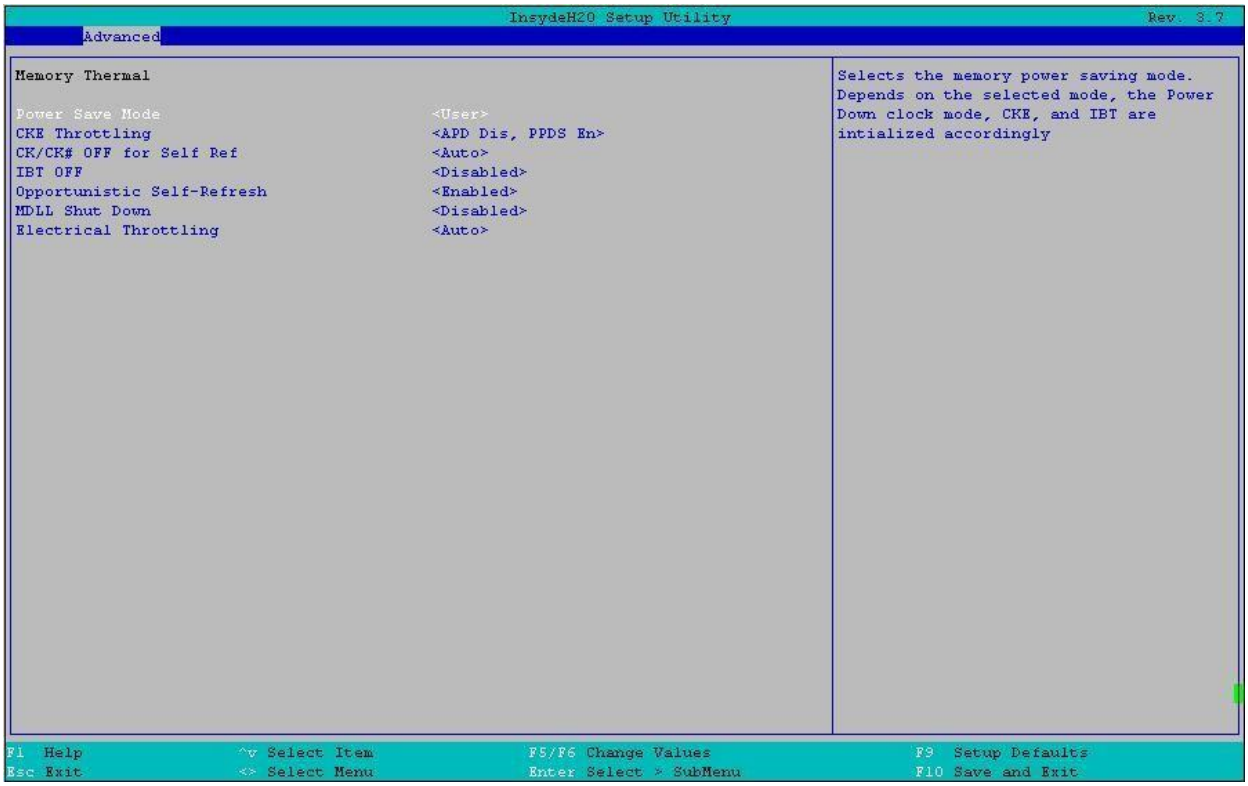


Рисунок 16-30. Меню Memory Thermal

Настройка BIOS	Опции	Описание
Power Save Mode	Откл Медленный Быстрый Собственные настройки	Выбор режима энергосбережения памяти

Настройка BIOS	Опции	Описание
CKE Throttling	Откл. APD En, PPD Dis APD Dis, PPDF En APD Dis, PPDS En APD En, PPDF En APD En, PPDS En	Настройка регулирования CKE
CK/CK# OFF for Self Ref	CK driven CK tri-stated CK pulled low CK pulled high Auto	Настройка CK/CK# для самообновления
IBT OFF	Включено Отключено	Настройка IBT OFF
Opportunistic Self-Refresh	Включено Отключено	Включение/отключение согласованного самообновления
MDLL Shut Down	Включено Отключено	Включение/отключение функции выключение во время самообновления MDLL
Electrical Throttling	Включено Отключено Авто	Настройка электрического регулирования памяти

16.2.2.10.5. Advanced/SandyBridge RC/.../Memory DIMM

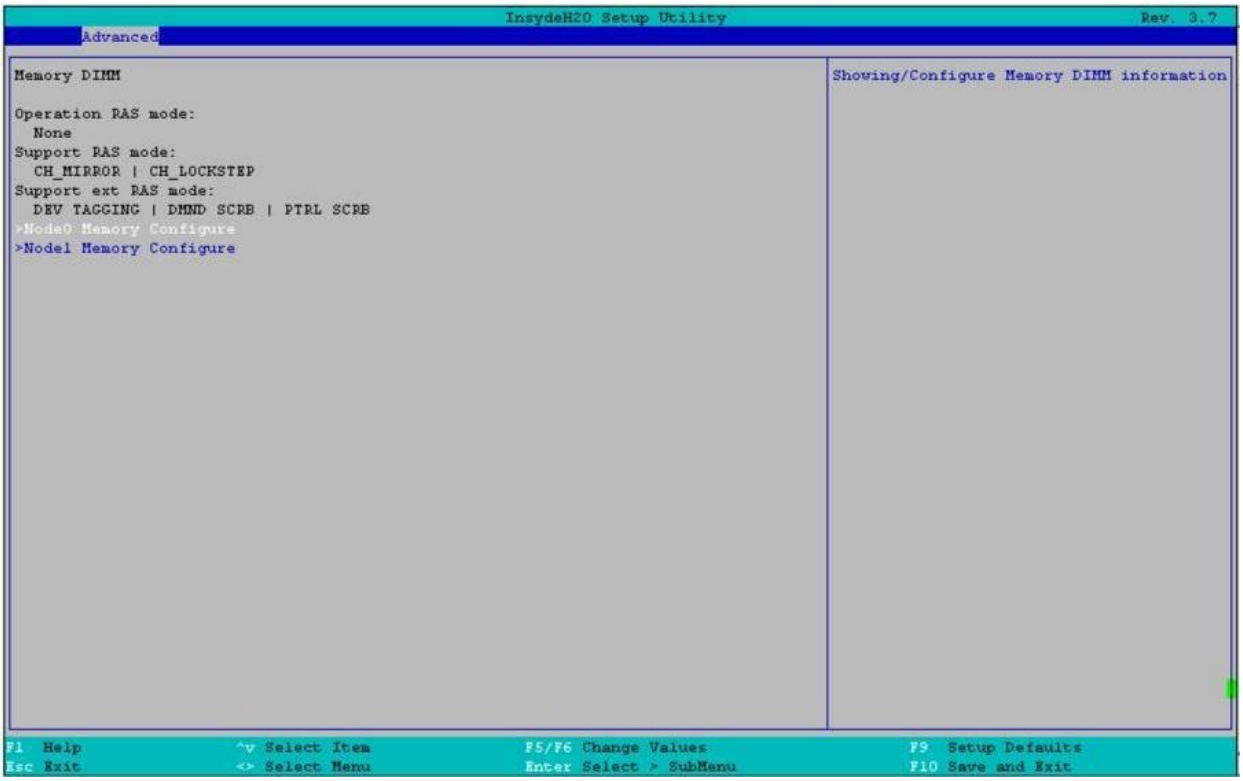


Рисунок 16-31. Меню Memory DIMM

Настройка BIOS	Опции	Описание
>Node0 Memory Configure	См. раздел 16.2.2.10.6	Показывать/настраивать информацию о DIMM-памяти
>Node1 Memory Configure	См. раздел 16.2.2.10.6	Показывать/настраивать информацию о DIMM-памяти

16.2.2.10.6. Advanced/SandyBridge RC/.../Memory DIMM/Node0, 1 MEM CFG

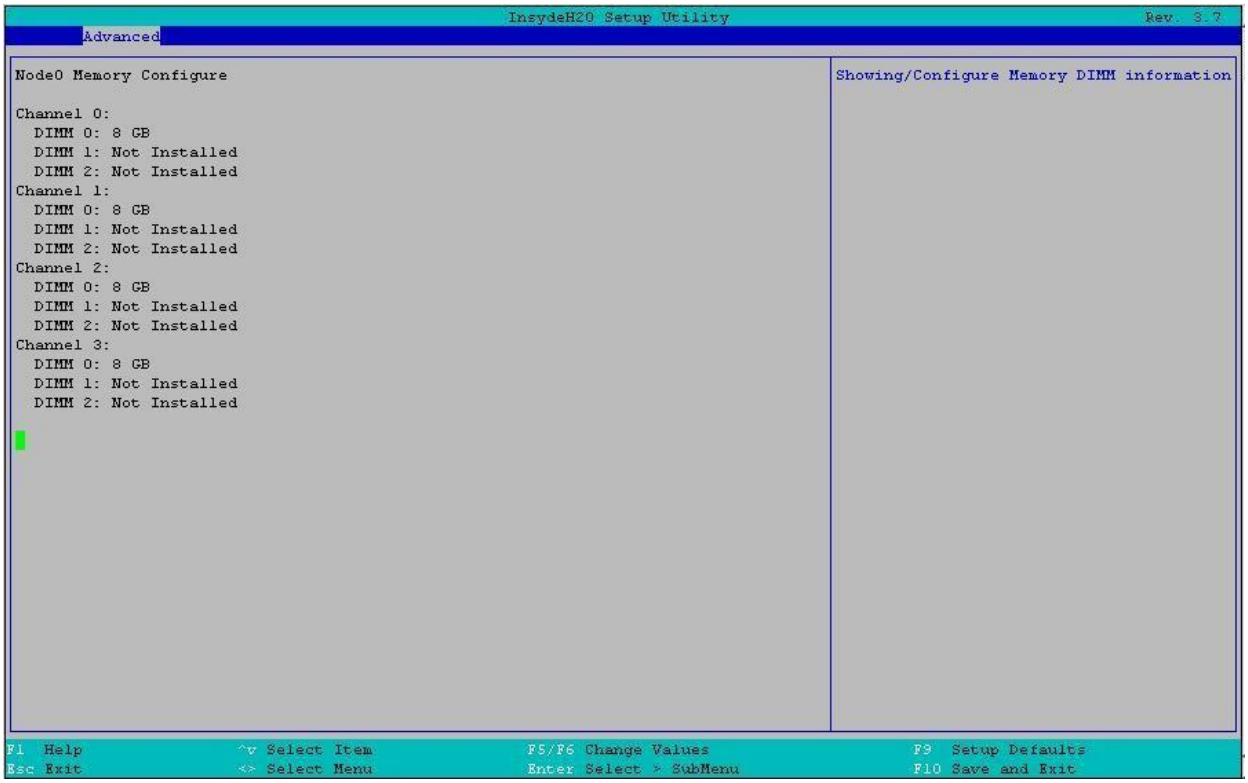


Рисунок 16-32. Меню Node0, 1 MEM CFG

Настройка BIOS	Опции	Описание
Node0 Memory Configure	Нет вариантов	Показывает информацию о DIMM-памяти

16.2.2.11. AdvancedACPI Table/Features Control

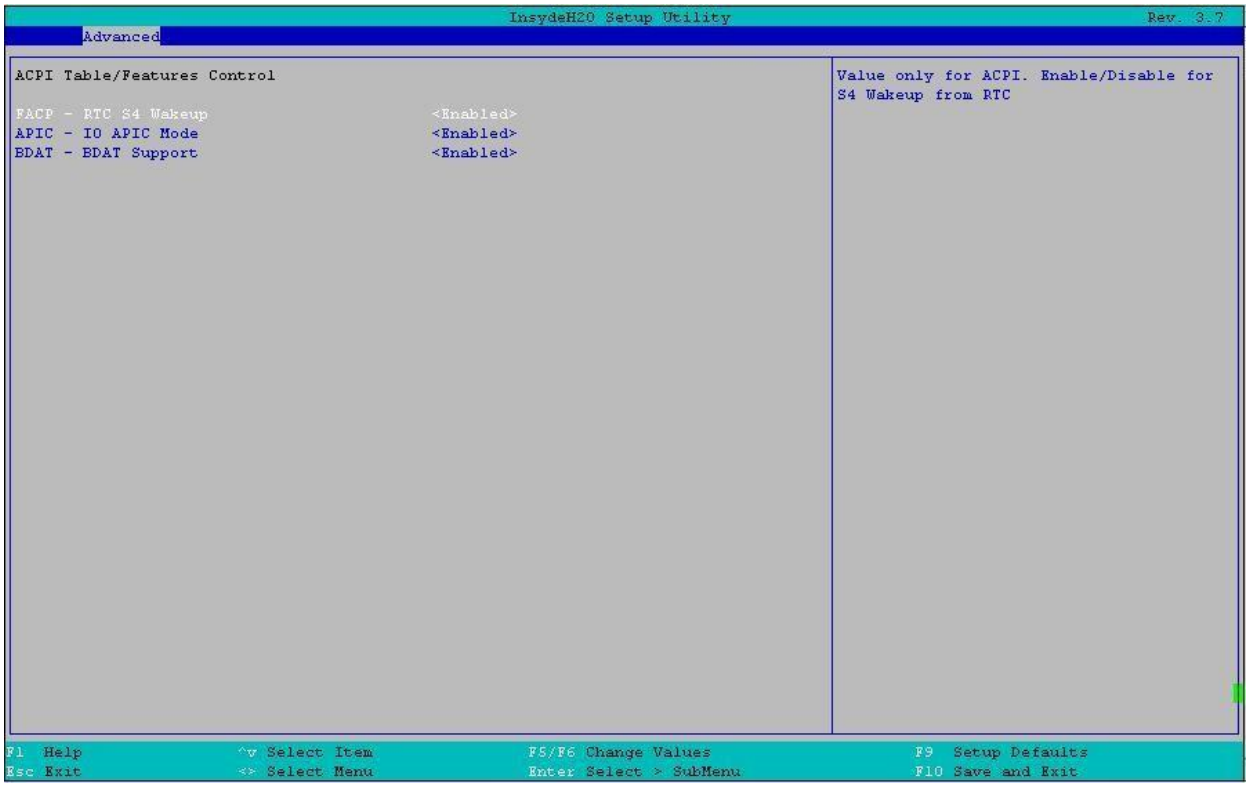


Рисунок 16-33. Меню Features Control

Настройка BIOS	Опции	Описание
FACP – RTC S4 Wakeup	Отключено Включено	Значение только для ACPI. Разрешить/запретить S4 Wakeup от RTC
APIC – IO APIC Mode	Отключено Включено	Этот элемент действителен только для WIN2K и WINXP. Включите этот режим, когда APIC-режим необходим. Протестируйте IO ACPI, установив параметр Enable. Будет инициализирован локальный APIC и соответствующие биты разрешения будут установлены в ICH4M
BDAT – BDAT Support	Отключено Включено	Включение/Отключить публикацию таблицы ACPI BDAT

16.2.2.12. Advanced/Console Redirection

Расширенные настройки/Переадресация консоли

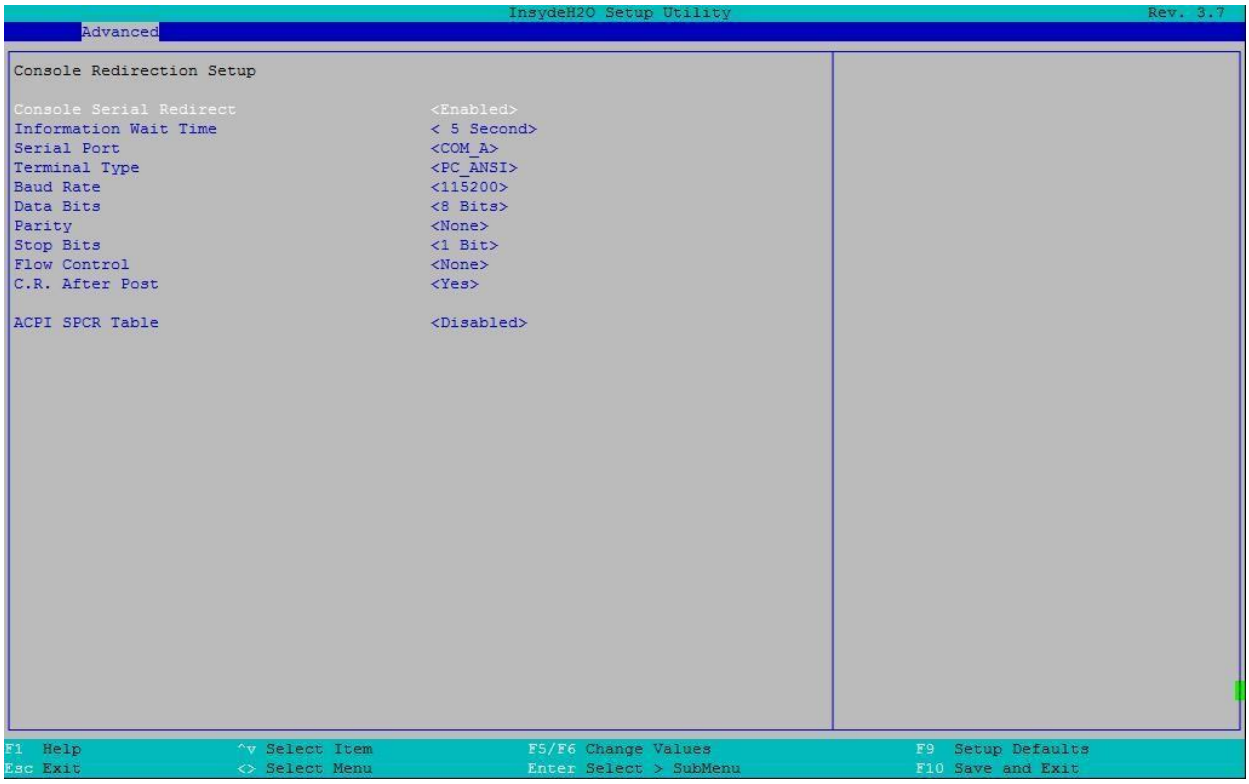


Рисунок 16-34. Меню Console Redirection

Настройка BIOS	Опции	Описание
Console Serial Redirect (Переадресация консоли)	Отключено Включено	Отключить/Включить переадресацию последовательного порта консоли
Information Wait Time (Время ожидания информации)	0 Секунд 2 секунды 5 Секунд 10 Секунд 30 Секунд	Установите время ожидание, пока загрузится OPROM, для перенаправления консоли
Serial Port (Последовательный порт)	COM_A COM_B COM_B COM_C COM_D Все порты	Решите, для какго последовательного порта будет применяться перенаправление консоли. Только COM A/B/C/D или все последовательные порты (включая последовательный порт PCI)

Настройка BIOS	Опции	Описание
Terminal Type (Тип терминала)	VT_100 VT_100+ VT_UTF8 PC_ANSI	Установите тип терминала VT100/VT100+/UTF8/PC_ANSI
Baud Rate (Скорость передачи данных)	115200 57600 38400 19200 9600 4800 2400 1200	Установите скорость передачи данных последовательного порта при перенаправлении консоли
Data Bits (Число битов в байте данных)	7 бит 8 бит	Установите число битов в байте данных
Parity (Паритет)	None Even Odd	Установите параметр паритета
Stop Bits (Количество стоп-битов)	1 Bit 2 Bits	Установите Stop Bits на последовательном порту для функции перенаправления консоли
Flow Control (Управление потоком)	None RTS/CTS Xon/Xoff	Установите управление потоком на последовательный порт для функции перенаправления консоли
C.R After POST	Да Нет	Установка того, будет ли переадресация консоли работать до завершения POST или устаревшей ОС (например, DOS)
ACPI SPCR Table	Отключено Включено	Включить/выключить отчетную таблицу SPCR для ОС (например, Windows 2008)

16.2.2.13. Advanced/APEI Configuration

Расширенные настройки/Конфигурация APEI

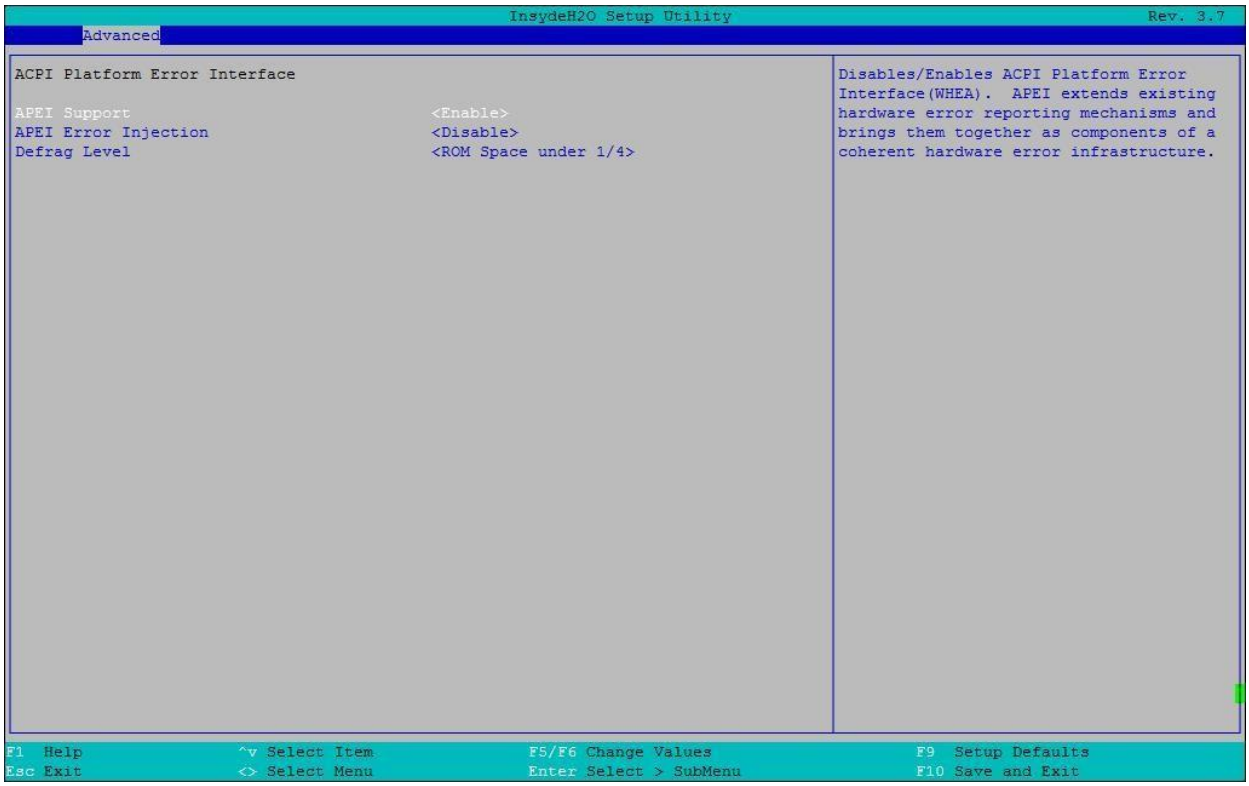


Рисунок 16-35. Меню Конфигурация APEI

Настройка BIOS	Опции	Описание
APEI Support (Поддержка APEI)	Отключить Включить	Отключает/включает интерфейс ошибок платформы ACPI (WHEA)
APEI Error Injection	Disable MEMORY_ CE MEMORY_UE_NON_FATAL MEMORY_ UE_FATAL PCIE_CE PCIE_UE_NON_FATAL PCIE_UE_FATAL	Введите ошибку, чтобы проверить функцию APEI

Настройка BIOS	Опции	Описание
Defrag Level (Уровень дефрагментации)	ROM Space under 1/4 ROM Space under 1/3 ROM Space under 1/2 Every time when error occur	Уровень дефрагментации ROM

16.2.2.14. Advanced/RAS Configuration

Расширенные настройки/Конфигурация RAS

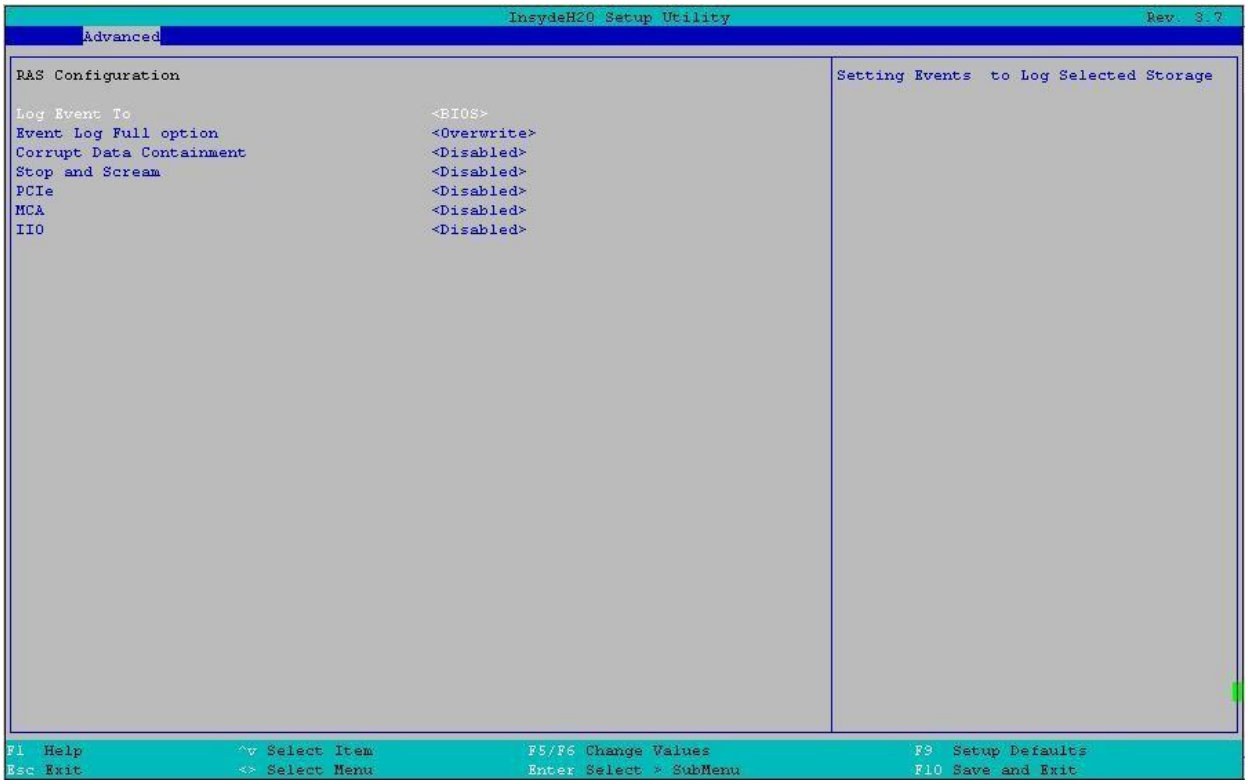


Рисунок 16-36. Меню RAS Configuration

Настройка BIOS	Опции	Описание
Log Event To (Войти в журнал)	ALL BIOS BMC SEL DCMI SEL MEMORY	Настройка журнала событий на выбранное хранилище

Настройка BIOS	Опции	Описание
Event Log Full option (Настройка переполнения журнала)	Overwrite Clear All Stop Logging	Задать действие при переполнении журнала
Corrupt Data Containment (Повреждение данных)	Отключить Включить	Включить/выключить защиту данных от повреждения
Stop and Scream (защита от кражи)	Отключить Включить	Включить/выключить функцию защиты от кражи
PCIe	Отключить Включить	Включение/выключение PCIe RAS
MCA	Отключить Включить	Включение/выключение MCA RAS
IIO	Отключить Включить	Включение/выключение IIO RAS

16.2.2.15. Advanced/Event Message Setting

Расширенные настройки/Настройка сообщений о событии

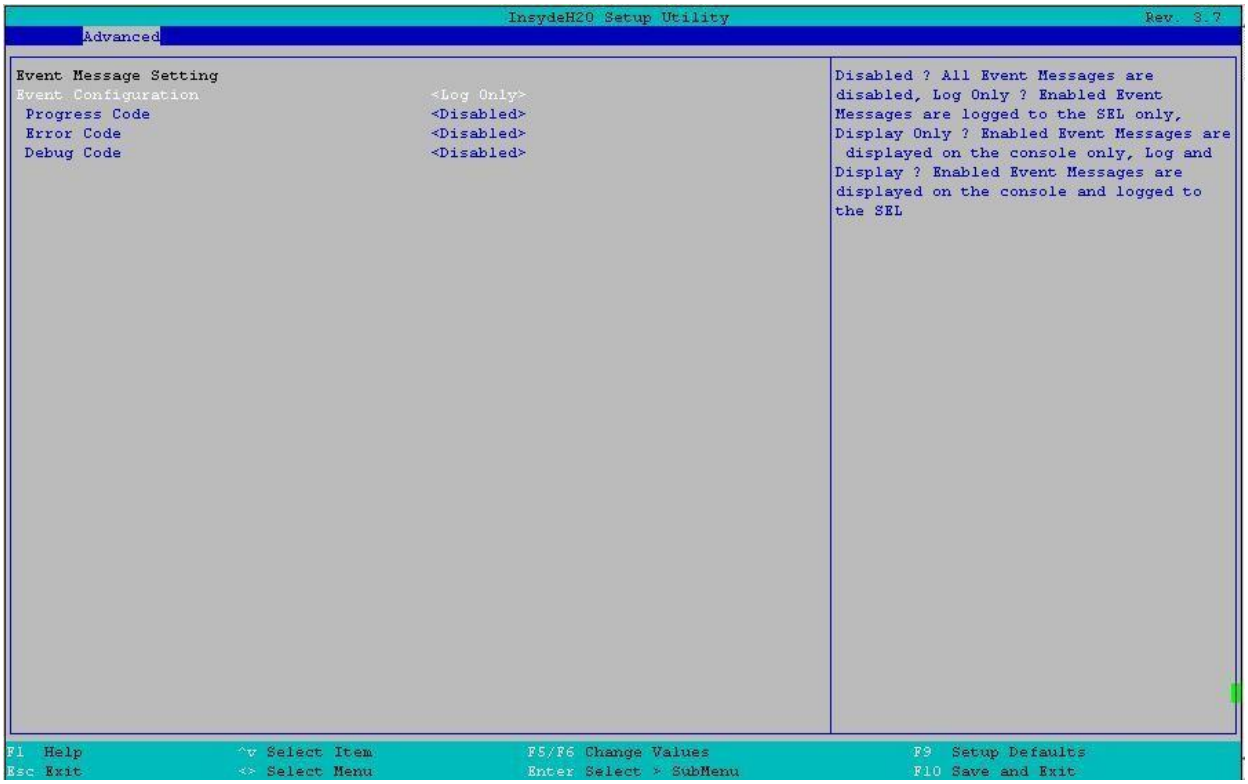


Рисунок 16-37. Меню Event Message Setting

Настройка BIOS	Опции	Описание
Event Configuration (Конфигурация события)	Disabled Log only Display only Log and Display	Отключено: все сообщения о событиях отключены Только журнал: включенные сообщения о событиях регистрируются только в SEL Только дисплей: включенные сообщения о событиях отображаются только на консоли Журнал и дисплей: включенные сообщения о событиях отображаются на консоли и регистрируются в SEL
Progress Code (Прогресс-код)	Отключено Включено	Сообщения с кодами прогресса отключены/включены в BIOS
Error Code (Код ошибки)	Отключено Включено	Сообщения с кодами ошибок отключены/включены в BIOS
Debug Code (Отладочный код)	Отключено Включено	Сообщения об отладке кода отключены/включены в BIOS

16.2.2.16. Advanced/Event Log Viewer

Расширенные настройки/Просмотр журнала событий

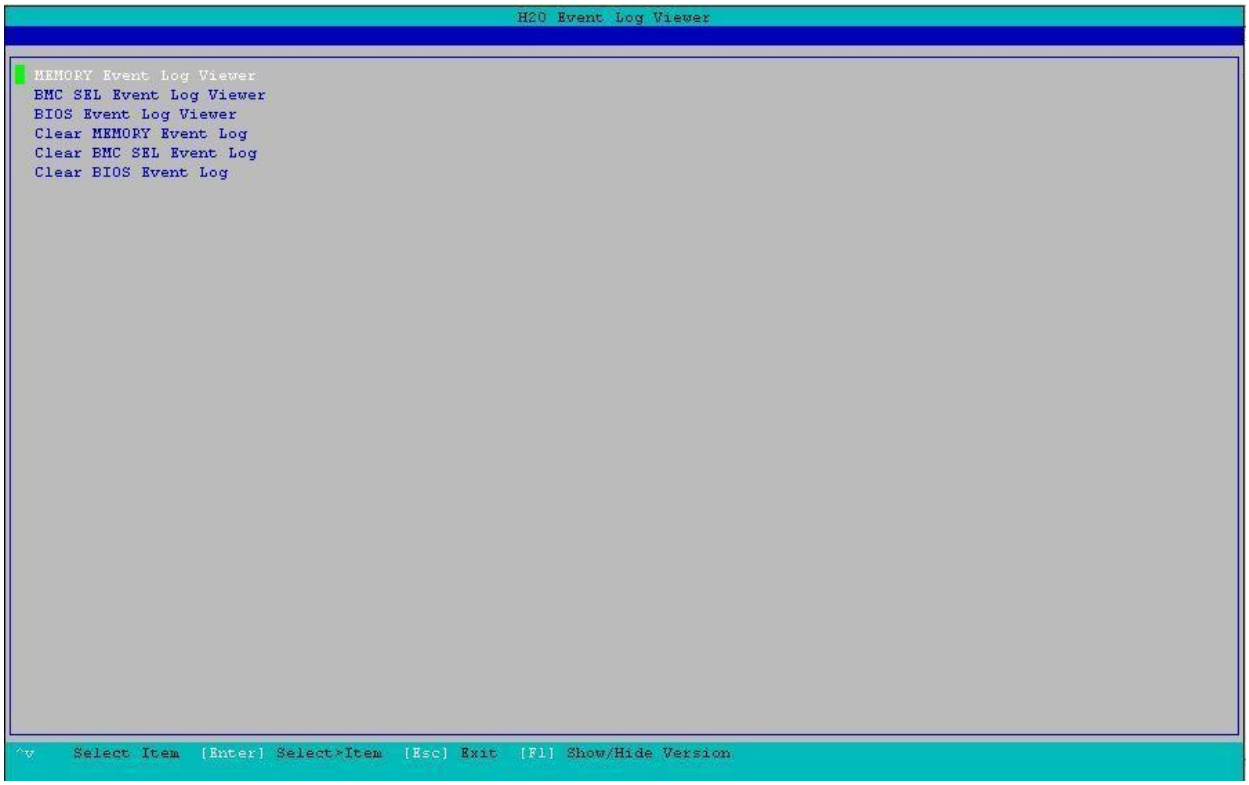


Рисунок 16-38. Меню Event Log Viewer

Настройка BIOS	Опции	Описание
MEMORY Event Log Viewer (Просмотр журнала событий MEMORY)	Нет	Просмотр журнала событий MEMORY
BMC SEL Event Log Viewer (Просмотр журнала событий BMC SEL)	Нет	Просмотр журнала событий BMC SEL
BIOS Event Log Viewer (Просмотр журнала событий BIOS)	Нет	Просмотр журнала событий BIOS
Clear MEMORY Event Log (Очистить журнал событий MEMORY)	Нет	Очистить журнал событий MEMORY

Настройка BIOS	Опции	Описание
Clear BMC SEL Event Log (Очистить журнал событий BMC SEL)	Нет	Очистить журнал событий BMC SEL
Clear BIOS Event Log (Очистить журнал событий BIOS)	Нет	Очистить журнал событий BIOS

16.2.2.17. Advanced/IPMI BMC Configuration

Расширенная конфигурация BMC IPMI

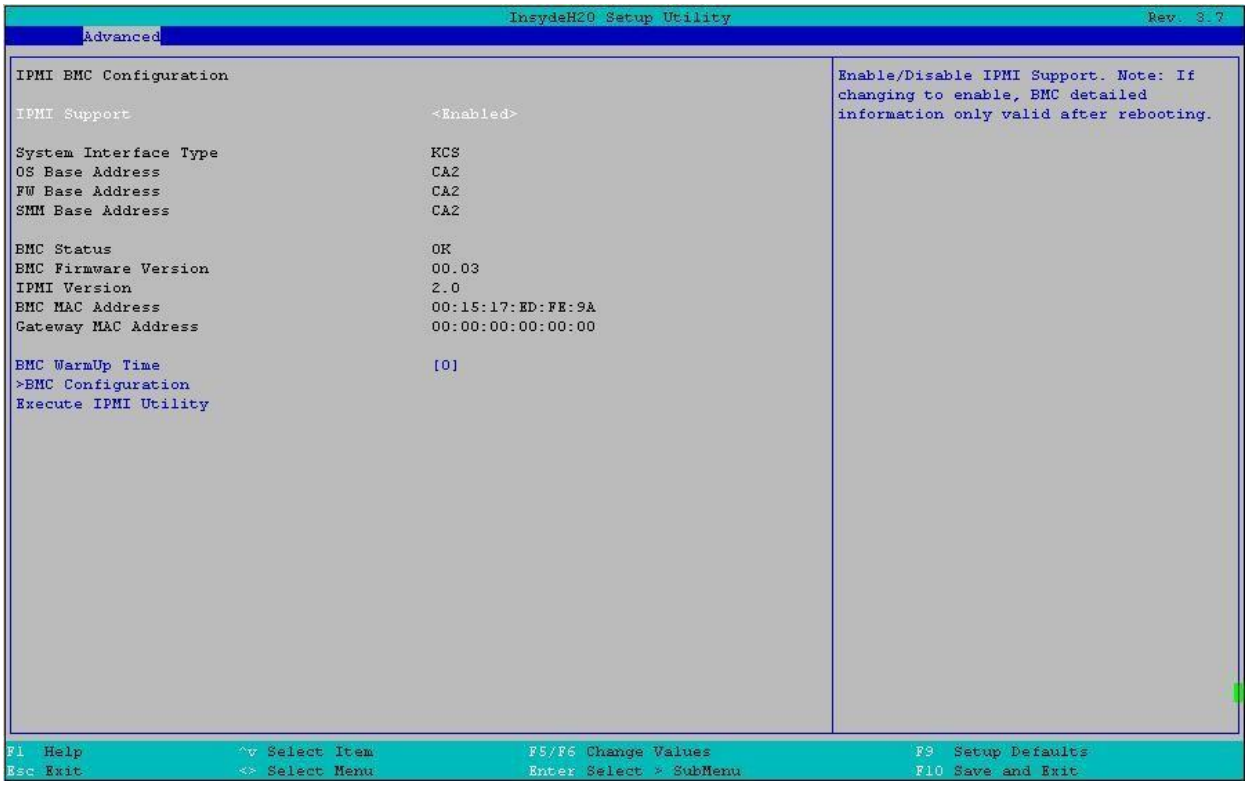


Рисунок 16-39. Меню IPMI BMC Configuration

Настройка BIOS	Опции	Описание
IPMI Support (Поддержка IPMI)	Включить Отключить	Включение/выключение поддержки IPMI. Примечание: при включении данной функции подробная информация BMC действительна только после перезагрузки

Настройка BIOS	Опции	Описание
System Interface Type (Тип системного интерфейса)	Нет	Показать тип системного интерфейса IPMI
OS Base Addrese (Базовый адрес ОС)	Нет	Показать, как ОС использует IO-порт для IPMI
FW Base Addrese (Базовый адрес FW)	Нет	Показать FW использует IO-порт для IPMI
SMM Base Addrese (Базовый адрес SMM)	Нет	Показать использование SMM-порта ввода-вывода для IPMI
BMC Status (Статус BMC)	Нет	Показать статус BMC
BMC Firmware Version (Версия прошивки BMC)	Нет	Показать версию прошивки BMC
IPMI Version (Версия IPMI)	Нет	Показать версию IPMI
BMC MAC Address (BMC MAC адрес)	Нет	Показать MAC-адрес в BMC
Gateway MAC Address (MAC-адрес шлюза)	Нет	Показать MAC-адрес шлюза
BMC WarmUp Time (Время прогрева BMC)	Установите значение [0 – 240]	Максимальное время ожидания от POST до BMC в секундах
BMC Configuration (BMC конфигурация)	См. раздел 16.2.2.17.1	Меню конфигурации BMC. Все пункты этого меню — это настройки, которые BIOS будет посылать на BMC
Execute IPMI Utility (Выполнить утилиту IPMI)	Нет	Подробное содержание смотрите в IPMI

16.2.2.17.1. Advanced/IPMI BMC Configuration/BMC Configuration

Расширенные настройки/Конфигурация IPMI BMC/Конфигурация BMC

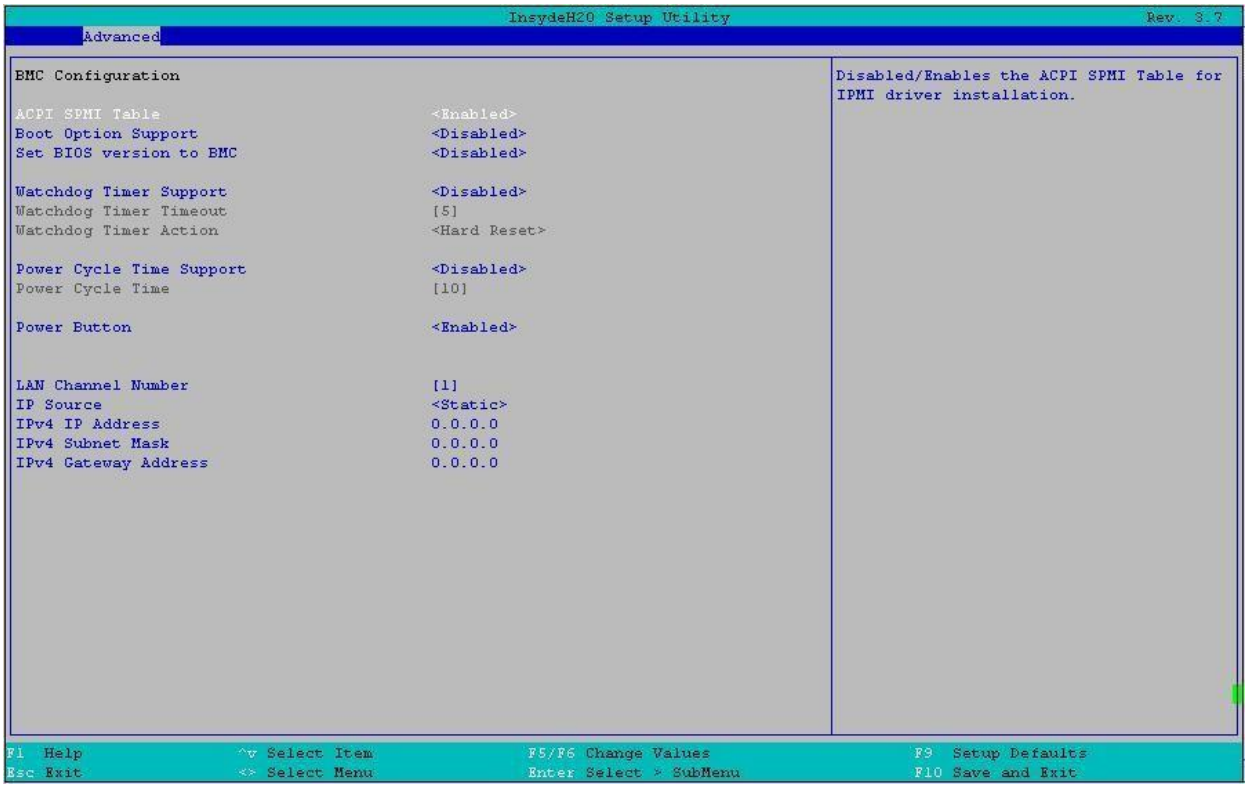


Рисунок 16-40. Меню BMC Configuration

Настройка BIOS	Опции	Описание
ACPI SPMI Table (Таблица ACPI SPMI)	Отключить Включить	Отключить/Включить ACPI SPMI-таблицу для установки драйвера IPMI
Boot Option Support (Поддержка опций загрузки)	Отключить Включить	Включение/выключение загрузки через опцию “Boot Option” в BMC
Set BIOS version to BMC (Установить версию BIOS на BMC)	Отключить Включить	Включение/выключение установки версии BIOS на BMC. Если опция включена, BMC сохранит версию BIOS
Watchdog Timer Support	Отключить Включить	Включение/выключение Watchdog таймера при загрузке

Настройка BIOS	Опции	Описание
Watchdog Timer Timeout	Установите значение [2 – 8]	Введите количество минут, в течение которых система должна загрузить ОС, прежде чем произойдет действие Timeout. Допустимые значения: от 2 до 8 минут
Watchdog Timer Action	Hard reset Power off Restart	Выбор действия: Жесткий сброс, отключение питания или перезагрузка
Power Cycle Time Support	Отключить Включить	Включение/выключение функции отправки команды времени цикла питания в BMC во время POST
Power Cycle Time	Отрегули-руйте значение [0 – 255]	Время, в течение которого питание системы будет отключаться во время цикла питания, инициированного командой Chassis Control или временем сторожевого таймера. Действительные значения составляют от 0 до 255 секунд
Power Button (Кнопка питания)	Включить Отключить	Включение/выключение данной функции путем нажатия кнопки питания
LAN Channel Number (Номер канала LAN)	Установите значение [0 – 15]	Выберите номер канала LAN для BMC
IP Source (Источник IP)	DHCP Статический	DHCP: настройки BMC IPv4 будут автоматически сконфигурированы с помощью DHCP. Статический: настройки BMC IPv4 будут сконфигурированы вручную
IPv4 IP Address (IPv4-адрес)	Valid IPv4 IP Address type	Настройка IP-адреса BMC IPv4. После сохранения изменений конфигурация будет установлена на BMC
IP4 Subset Mask (IPv4-маска подсети)	Valid IPv4 Mask type	Настройка маски подсети BMC IPv4. После сохранения изменений конфигурация будет установлена на BMC
IPv4 Gateway Address (IPv4-адрес шлюза)	Valid IPv4 Geteway Address type	Настройка адреса шлюза по умолчанию BMC IPv4. После сохранения изменений конфигурация будет установлена на

16.2.3. Security Menu

Меню безопасности

Меню Security предоставляет конфигурацию для настройки параметров безопасности системы:

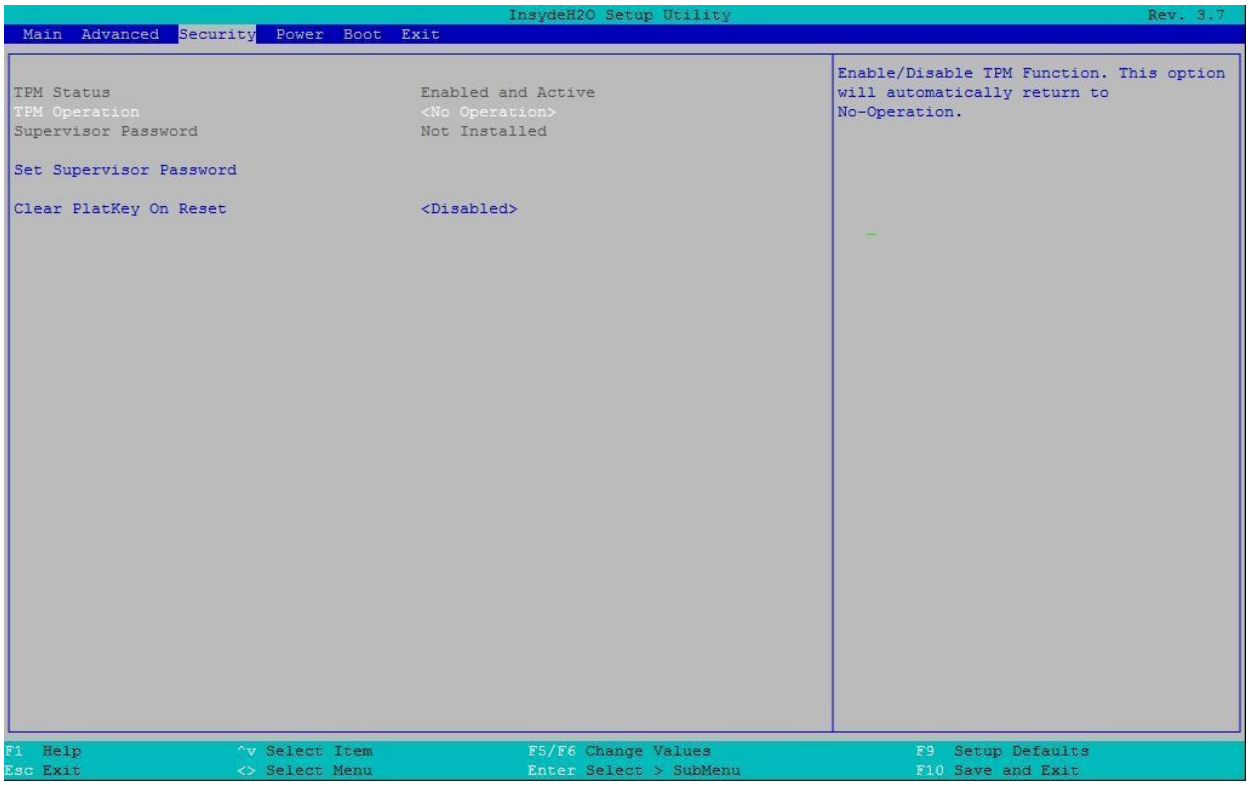


Рисунок 16-41. Меню безопасности

Настройка BIOS	Опции	Описание
TPM Status (Статус TPM)	Нет	Описание статуса TPM
TPM Operation (Работа TPM)	[Нет операции] [Отключить и деактивировать] [Включено и активно]	Включение/выключение функции TPM. Эта опция автоматически вернется в режим No-Operation
Supervisor Password (Пароль администратора)	Не установлен Введите пароль	Когда установлен пароль, вам будет предложено ввести любой понравившийся вам пароль Администратора
Clear PltKey On Reset (Очистить PltKey при перезагрузке)	Отключить Включить	Включить/Выключить очистку ключа безопасности платформы при перезагрузке

Установка пароля администратора

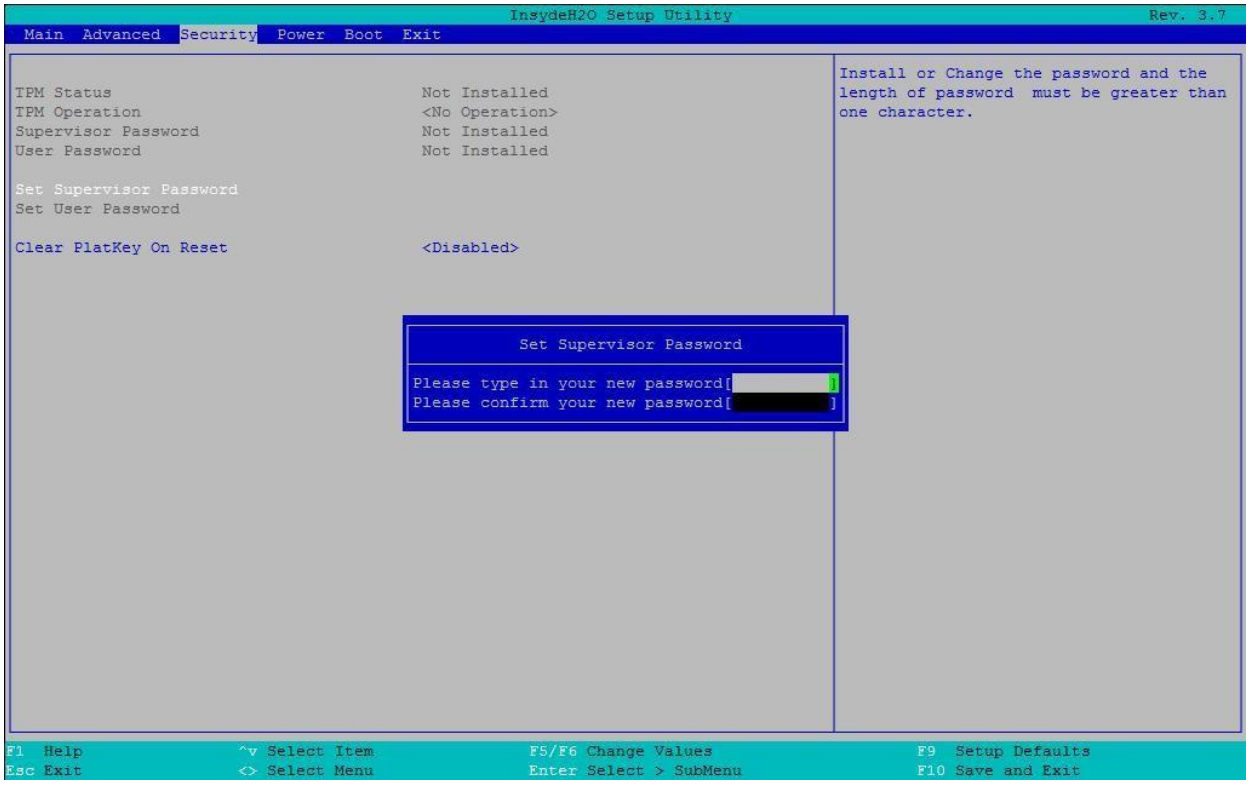


Рисунок 16-42. Установка пароля администратора

16.2.4. Power Menu

Меню электропитания

Меню «Power» (Рисунок 16-43) позволяет пользователям задавать или контролировать различные режимы управления электропитанием, температурой и спящим режимом.

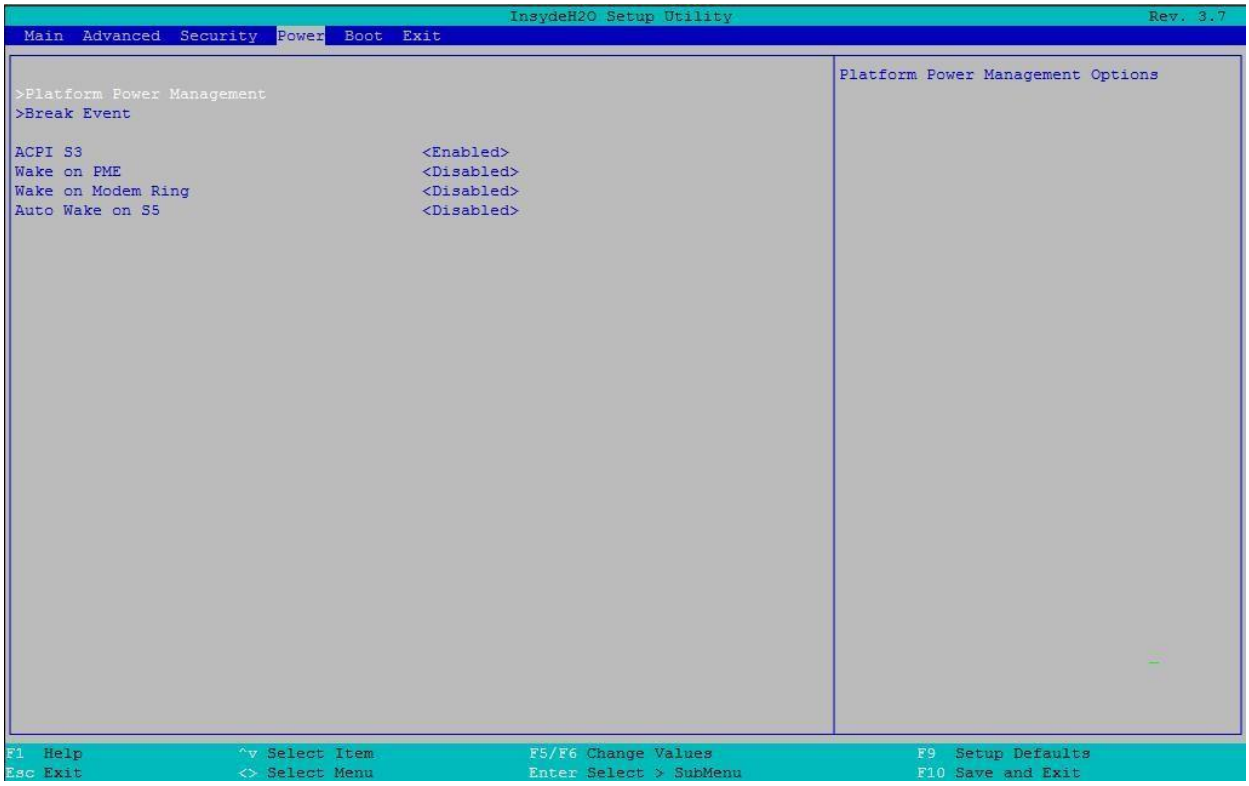


Рисунок 16-43. Меню электропитания

Настройка BIOS	Опции	Описание
Platform Power Management	См. раздел 16.2.4.1	Управления электропитанием платформы
Break Event	См. раздел 16.2.4.2	Перейти к параметрам управления событиями аварии элементов
ACPI S3	Отключено Включено	Включение/выключение спящего режима ACPI S3
Wake on PME	Отключено Включено	Определяет действие, предпринимаемое при отключении питания системы
Wake on Modem Ring	Отключено Включено	Определяет действие, выполняемое при выключении питания системы и звонке модема, подключенного к последовательному порту
Auto Wake on S5	Отключить Включить	Автоматическое пробуждение на S5, по дням месяца или в определенное время суток

16.2.4.1. Power/Platform Power Management

Электропитание/Управление электропитанием платформы

Рисунок 16-44. Меню Platform Power Management

Настройка BIOS	Опции	Описание
PCI Clock Run (Запуск часов PCI)	Отключено Включено	Если включено, логика CLKRUN # остановит тактовый генератор PCI

16.2.4.2. Power/Break Event

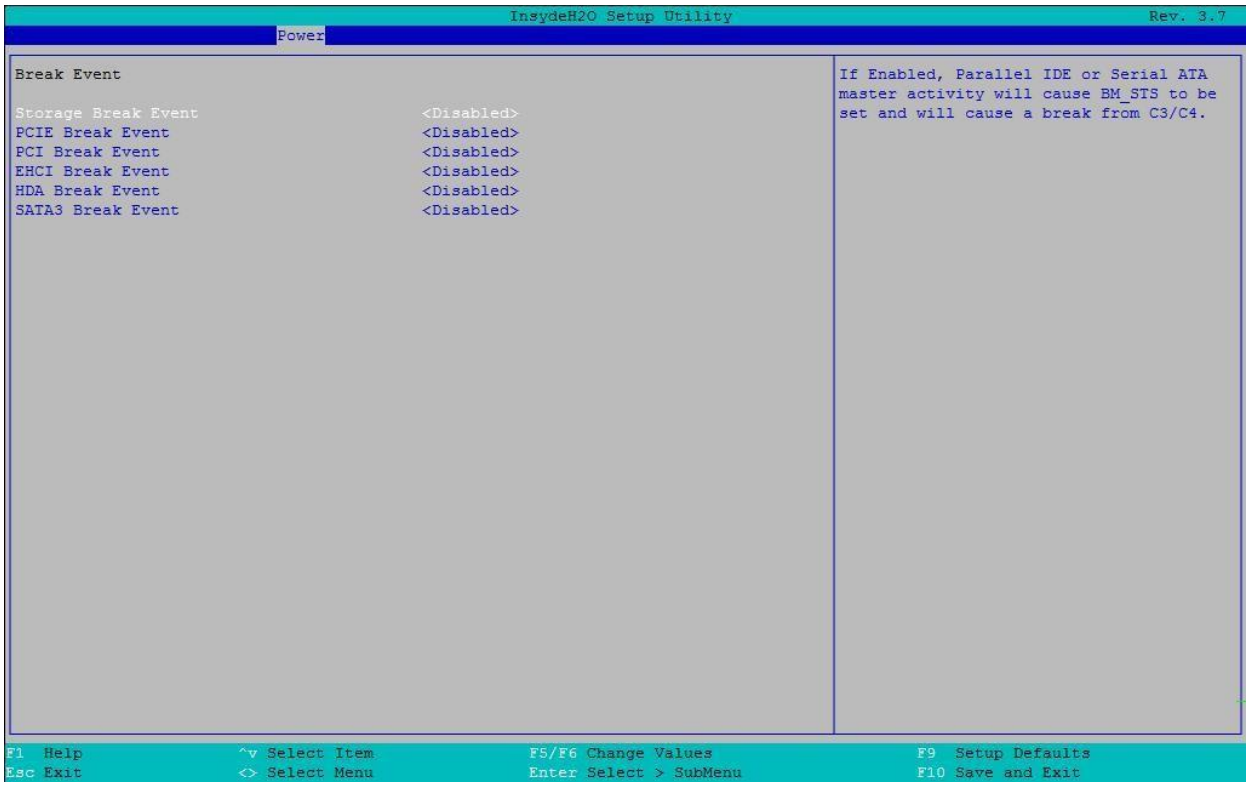


Рисунок 16-45. Меню Break Event

Настройка BIOS	Опции	Описание
Storage Break Event	Отключить Включить	Если этот параметр включен, работа параллельной IDE или ведущего устройства Serial ATA приведет к установке BM_STS и отказу от C3/C4
PCIe Break Event	Отключить Включить	Если Включено, активность PCI Express Master приведет к установке BM_STS и отказу от C3/C4
PCI Break Event	Отключить Включить	Если Включено, активность ведущего устройства PCI приведет к установке BM_STS и отказу от C3/C4
EHCI Break Event	Отключить Включить	Если Включено, активность ведущего устройства EHCI приведет к установке BM_STS и прерыванию работы C3/C4
HDA Break Event	Отключить Включить	Если этот параметр включен, ведущее устройство HDA приведет к установке BM_STS и отказу от C3/C4

Настройка BIOS	Опции	Описание
SATA 3 Break Event	Отключить Включить	Если Включено, активность ведущего устройства SATA3 Master приведет к установке BM_STS и отказу от C3/C4

16.2.5. Boot Menu

Загрузочное меню

Меню загрузки позволяет настроить последовательность загрузки загрузочных устройства. Оно включает следующее:

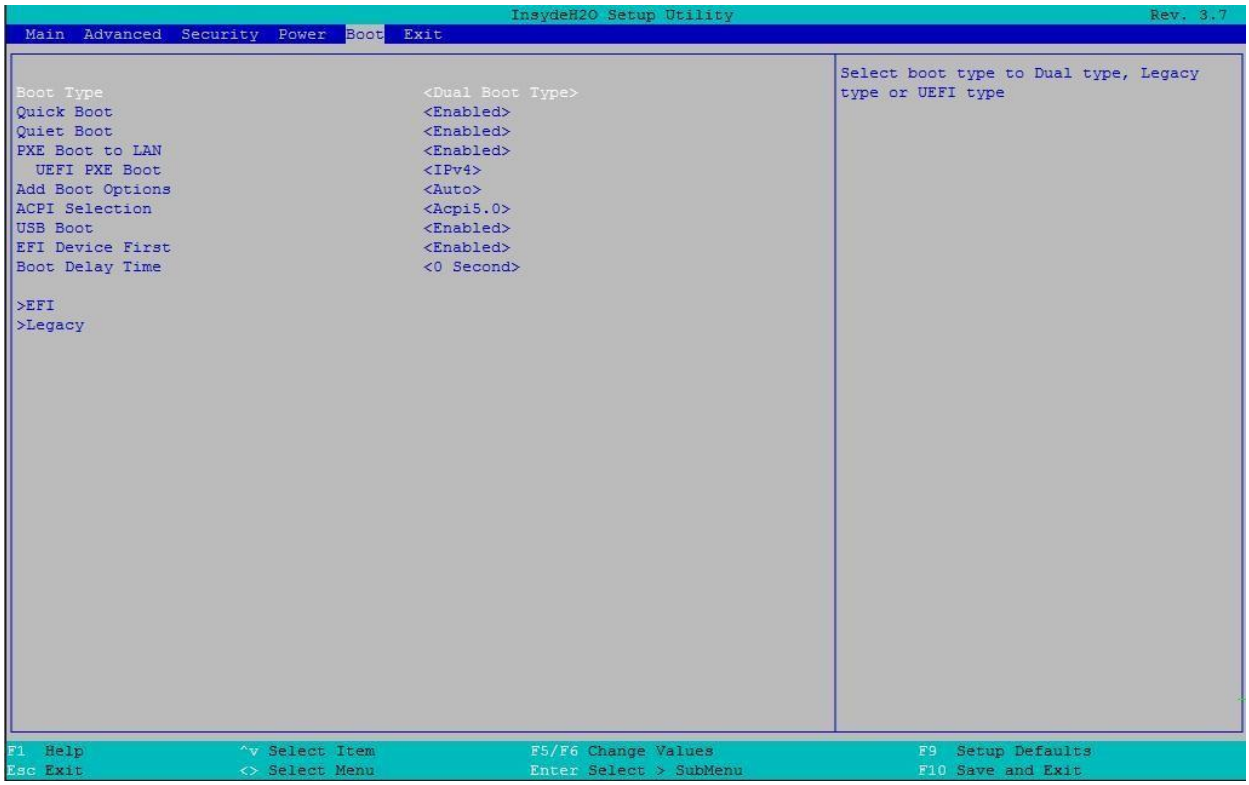


Рисунок 16-46. Загрузочное меню

Настройка BIOS	Опции	Описание
Boot Type (Тип загрузки)	Dual Boot Type Legacy Boot Type UEFI Boot Type	Выберите тип загрузки: Dual Boot type, Legacy type или UEFI type
Quick Boot (Быстрая загрузка)	Отключено Включено	Позволяет BIOS пропускать определенные тесты при загрузке. Это уменьшит время, необходимое для загрузки системы

Настройка BIOS	Опции	Описание
Quiet Boot (Тихая загрузка)	Отключено Включено	Отключить или включить загрузку в текстовом режиме
PXE Boot to LAN (PXE-Загрузка по локальной сети)	Отключено Включено	Отключить или включить PXE-загрузку по локальной сети
UEFI PXE Boot (Загрузка UEFI PXE)	IPv4 IPv6 IPv4/IPv6 Отключено	Настройка протокола IPv4 или IPv6 для загрузки UEFI PXE
Add Boot Options (Добавить настройки загрузки)	First Last Auto	Добавить порядок загрузки для оболочки
ACPI Selection (Выбор ACPI)	Acpi1.0B Acpi3.0 Acpi4.0 Acpi5.0	Выберите загрузку Acpi
USB Boot (Загрузка по USB)	Отключено Включено	Отключение или включение загрузки с загрузочных устройств USB
EFI Device First	Отключено Включено	Определяет первое загрузочное устройство — “EFI” или “legacy”. Если включено, то в первую очередь это устройство “EFI”. Если отключено, первым будет устройство “legacy”
Boot Delay Time (Время задержки загрузки)	0 Секунда 3 секунды 5 секунд 10 секунд	Выберите значение времени задержки. Позволяет пользователю нажать горячие клавиши перед загрузкой
EFI	См. раздел 16.2.5.1	Настройка порядка загрузочных EFI-устройств
Legacy	См. раздел 16.2.5.2	Настройка порядка загрузочных Legacy-устройств

16.2.5.1. Boot/EFI

Рисунок 16-47. Меню EFI

Настройка BIOS	Опции	Описание
Internal EFI Shell (Внутренняя оболочка EFI)	Нет опций	Настройки загрузки EFI

16.2.5.2. Boot/Legacy

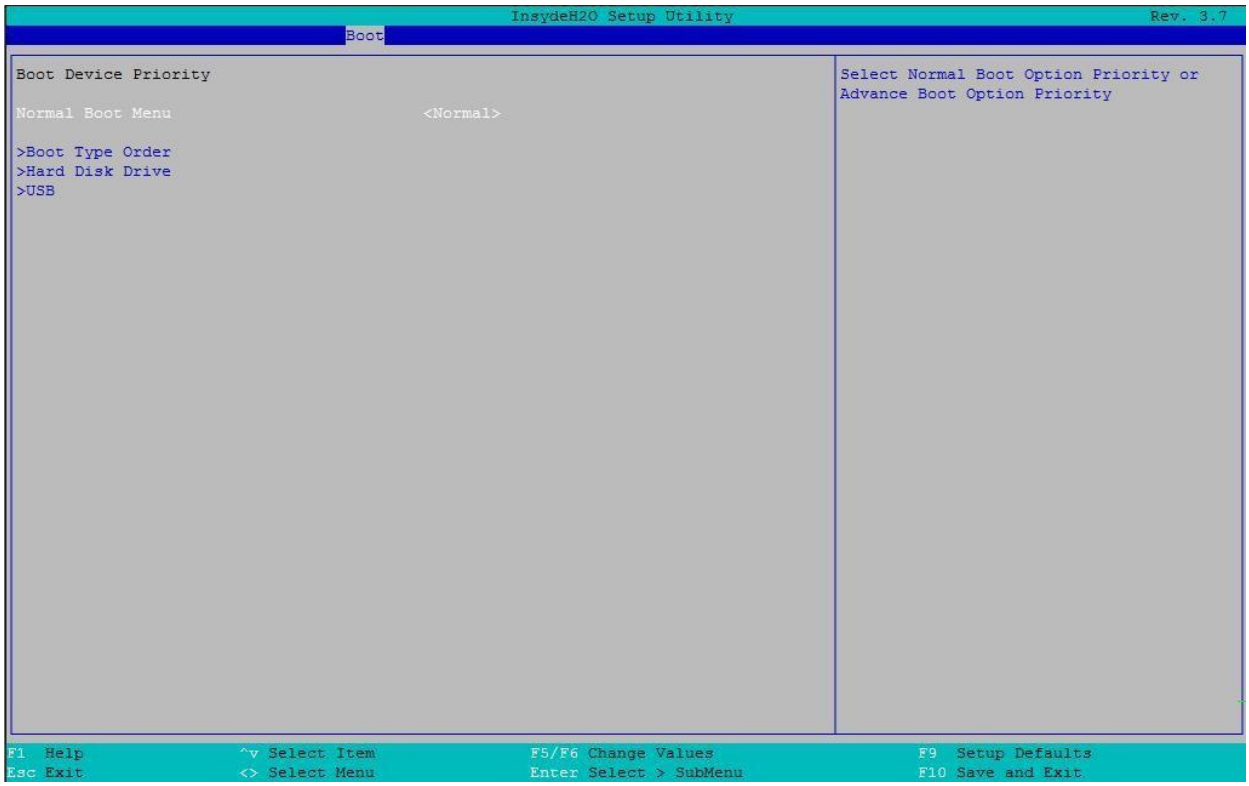


Рисунок 16-48. Меню Legacy

Настройка BIOS	Опции	Описание
Normal Boot Menu (Обычное меню загрузки)	Normal Extended	Выберите Приоритет Обычной загрузки или Приоритет расширенной загрузки
Boot Type Order (Порядок типов загрузки)	См. раздел 16.2.5.2.1	Изменить порядок типов загрузки
Hard Disk Driver (Драйвер жесткого диска)	См. раздел 16.2.5.2.2	Изменить порядок загрузки CD/DVD-ROM драйвера загрузочного устройства
USB	См. раздел 16.2.5.2.3	Отключение или включение загрузки на загрузочные устройства USB

16.2.5.2.1. Boot/Legacy/Boot Type Order

Порядок типов загрузки

Рисунок 16-49. Порядок типов загрузки

Настройка BIOS	Опции	Описание
Floppy Driver (Драйвер гибкого диска)	Нет опций	Legacy Boot Type 1
Hard Disk Driver (Драйвер жесткого диска)	Нет опций	Legacy Boot Type 1
CD/DVD-ROM Driver (Драйвер CD/DVD-ROM)	Нет опций	Legacy Boot Type 3
USB (Драйвер USB)	Нет опций	Legacy Boot Type 4
Others (Другие)	Нет опций	Другие типы загрузки с Legacy-устройств

16.2.5.2.2. Boot/Legacy/Hard Disk Drive

Выбор жесткого диска для загрузки

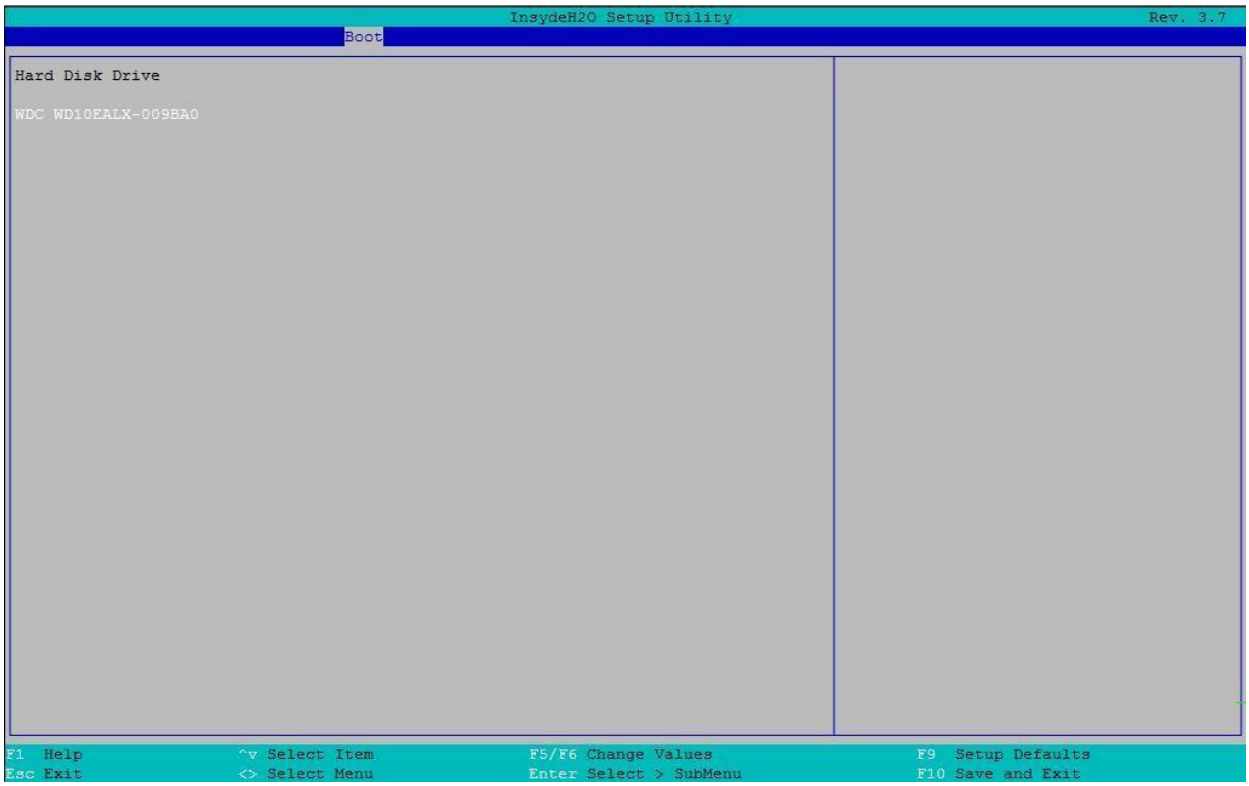


Рисунок 16-50. Выбор жесткого диска для загрузки

Настройка BIOS	Опции	Описание
Hard Disk Driver (Драйвер жесткого диска)	Нет опций	Модель драйвера жесткого диска, подключенного к этой платформе

16.2.5.2.3. Boot/Legacy/USB

Загрузка с USB

Рисунок 16-51. Загрузка с USB

Настройка BIOS	Опции	Описание
USB Flash Driver (Длайвер USB Flash)	Нет опций	Модель загрузочного флеш-накопителя USB, подключенного к этой платформе

16.2.6. Exit menu

Выход из меню. Меню выхода предоставляет следующие опции:

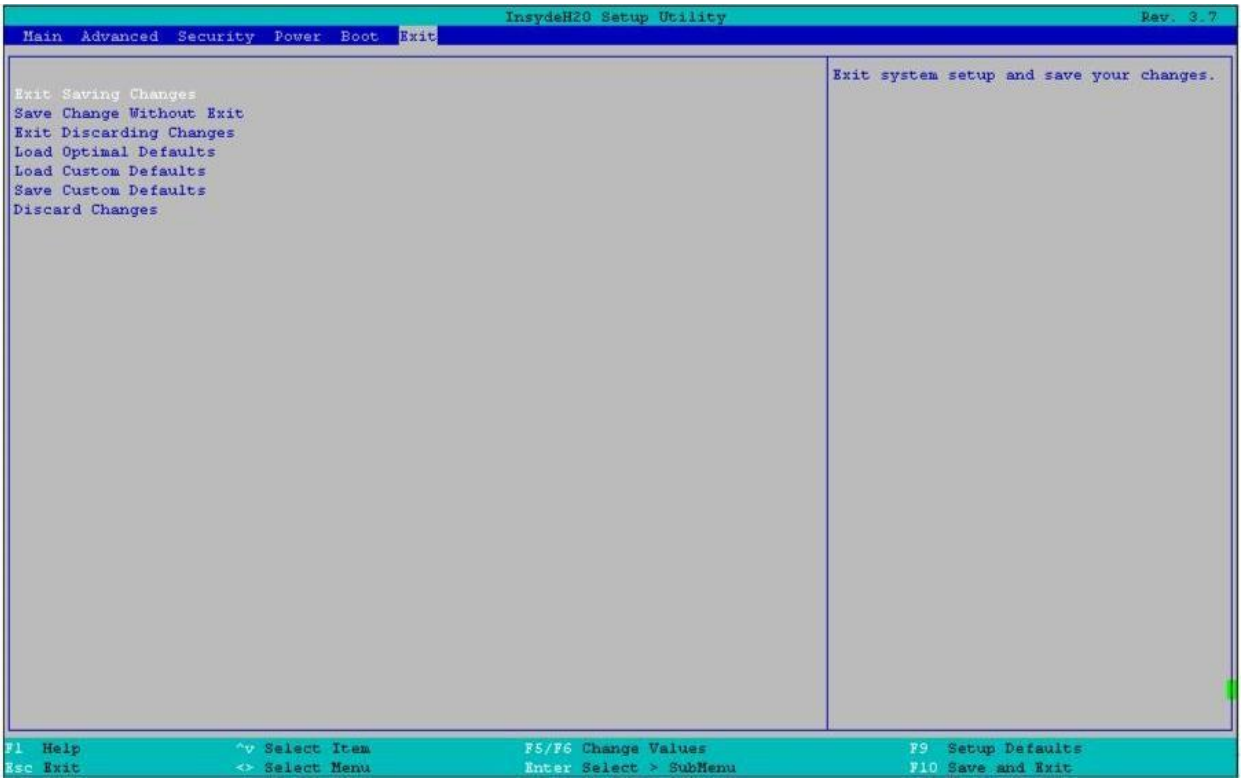


Рисунок 16-52. Меню выхода

Настройка BIOS	Опции	Описание
Exit Saving Changes (Выйти, сохранив изменения)	Да/Нет	Выход из меню и сохранение всех изменений настроек в BIOS
Save Change Without Exit (Сохранить изменения без выхода)	Да/Нет	Сохранить изменения, не выходя из меню
Exit Discarding Changes (Выйти отменив изменения)	Да/Нет	Выход из меню и сброс всех изменений настроек
Load Optimal Defaults (Загрузить Оптимальные настройки по умолчанию)	Да/Нет	Загрузить оптимальные настройки BIOS по умолчанию

Настройка BIOS	Опции	Описание
Load Custom Default (Загрузить пользовательские настройки по умолчанию)	Да/Нет	Загрузить сохраненные пользовательские настройки BIOS по умолчанию
Save Custom Default (Сохранить пользовательские настройки по умолчанию)	Да/Нет	Сохранить пользовательские настройки BIOS, в качестве профиля по умолчанию
Discard Changes (Отменить настройки)	Да/Нет	Сбрасить все изменения настроек и восстановить предыдущее состояние конфигурации

16.2.7. General Help

Общая помощь

Вы можете нажать клавишу "F1" в любом месте меню и получить страницу общей справки, как показано ниже.

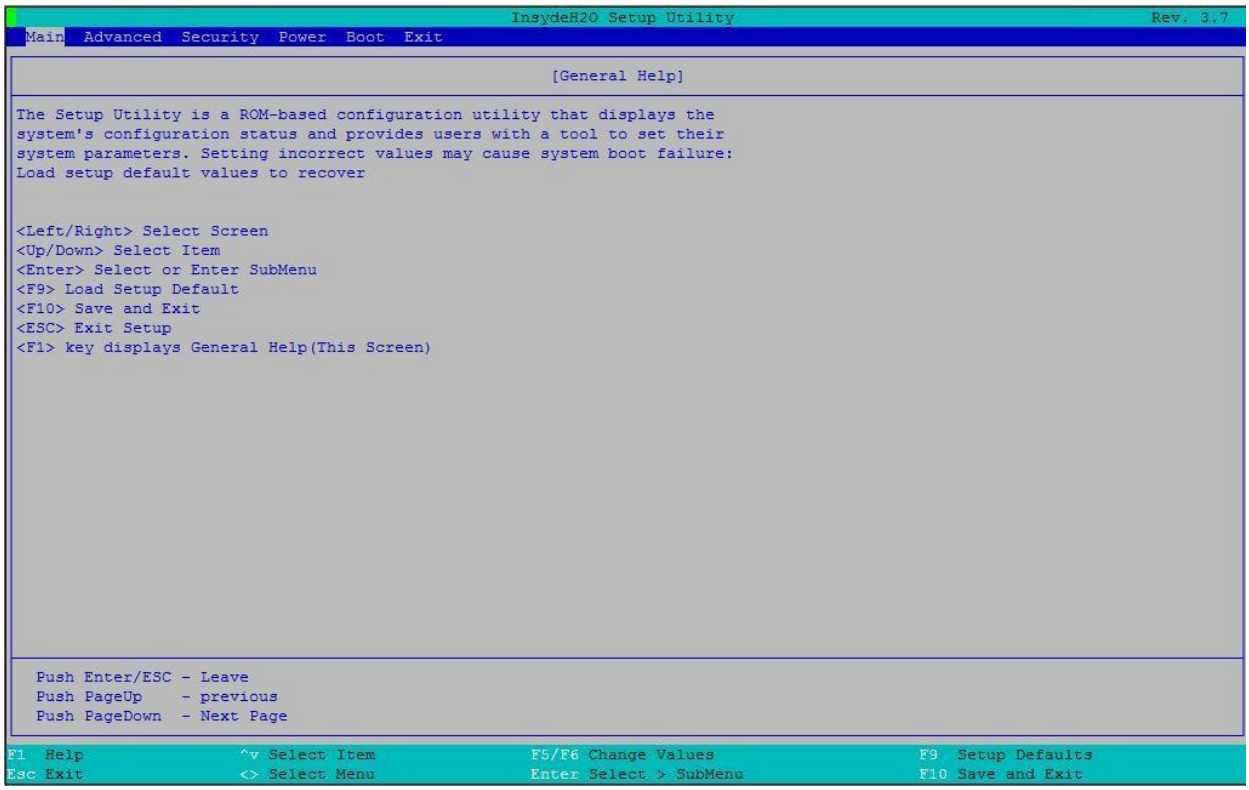


Рисунок 16-53. Меню общей помощи

16.3. Экран менеджера загрузки

Экран менеджера загрузки появляется при нажатии клавиши <ESC> и выборе "Boot Manager" из состояния POST-меню.

На экране отобразятся все загрузочные устройства в меню параметров загрузки. Пользователь может использовать клавиши «вверх»/«вниз» для выбора загрузочного устройства и нажать [ENTER] для подтверждения, или нажать [ESC] для выхода.

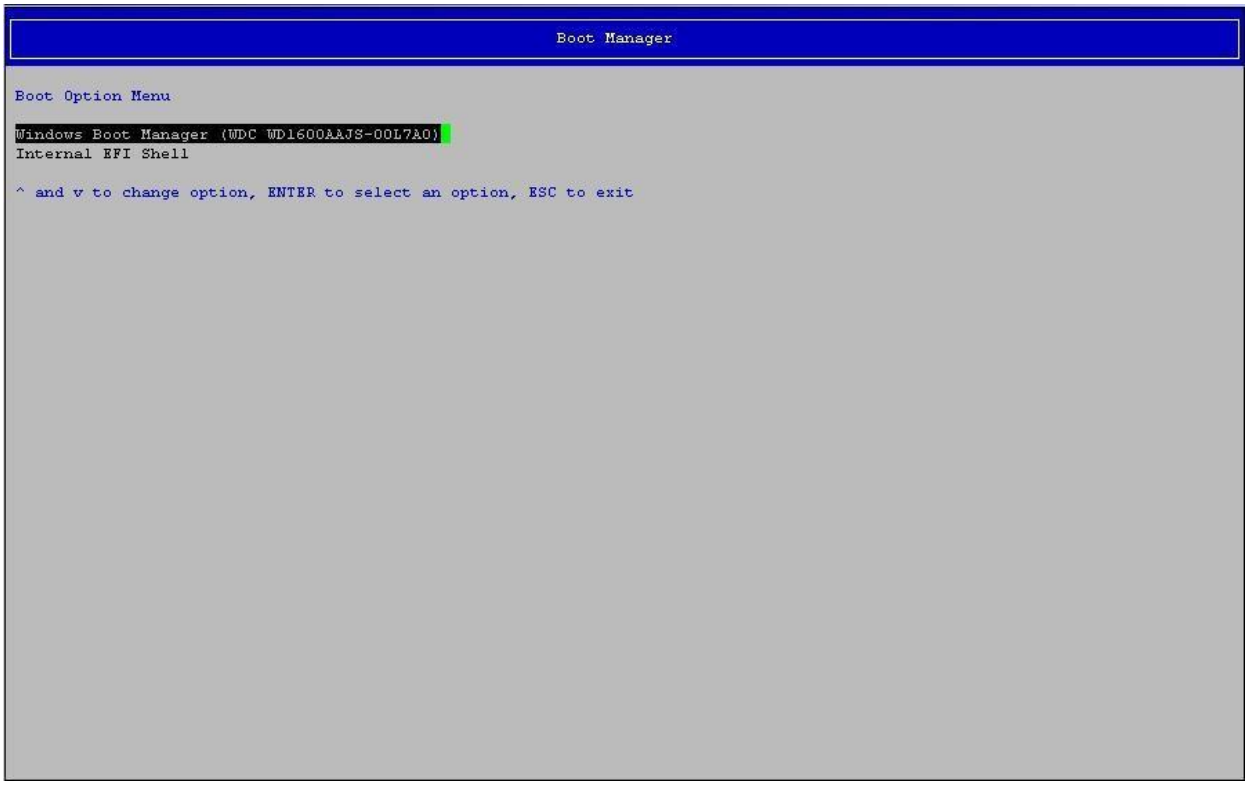


Рисунок 16-54. Экран менеджера загрузки

16.4. Экран ввода пароля во время загрузки

Экран ввода системного пароля во время загрузки показан ниже. Этот экран появляется в следующей ситуации.

1. Перед входом в BIOS Setup меню, если установлен пароль администратора.

«введите текущий пароль».

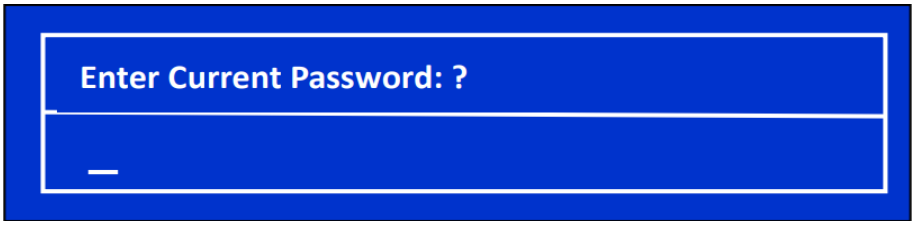


Рисунок 16-55. Экран ввода пароля во время загрузки

2. Любые введенные символы не отображаются, но отображаются символы "*".

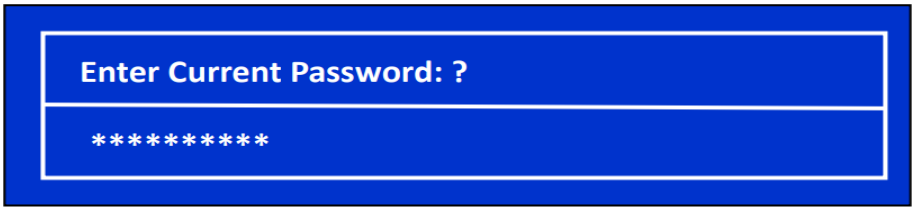


Рисунок 16-56. Отображение введенного пароля во время загрузки

3. При вводе неверного пароля отображается следующее сообщение *«Неправильный пароль»*.

Рисунок 16-57. Сообщение о неправильном пароле

4. При трехкратном вводе неправильного пароля отображается следующее сообщение *(«Состояние ошибки. Введен неправильный пароль 3 раза. Пожалуйста, перезапустите систему»*), после чего система останавливается.

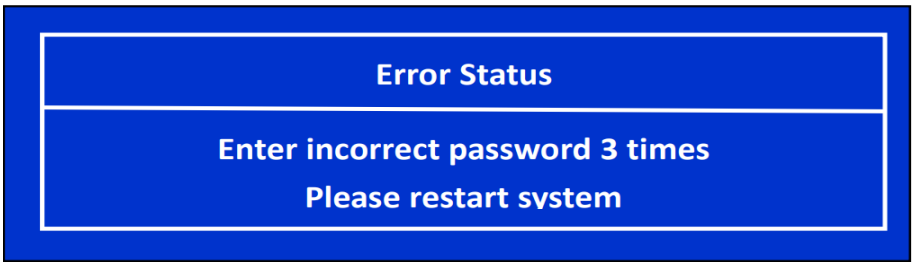


Рисунок 16-58. Сообщение о трехкратной ошибке ввода пароля

17. ПРИЛОЖЕНИЕ А. СОВЕТЫ ПО ИНТЕГРАЦИИ И ИСПОЛЬЗОВАНИЮ

- При добавлении или удалении компонентов, или периферийных устройств с материнской платы шнур (-ы) питания должны быть отсоединены от сервера. Когда к серверу подано питание, резервное напряжение все еще присутствует, даже если плата выключена.
- Материнская плата поддерживает семейство масштабируемых процессоров Intel® Xeon® с расчетной тепловой мощностью (TDP) до 205 Вт включительно. Предыдущие поколения процессоров Intel® Xeon® не поддерживаются. Серверные системы, использующие эту материнскую плату, могут не соответствовать расчетным ограничениям TDP. Перед выбором процессора проверьте пределы TDP-серверной системы.
- Процессоры должны устанавливаться в следующем порядке: CPU 1, CPU 2.
- Для достижения наилучшей производительности количество установленных модулей DDR4 DIMM должно быть сбалансировано как для процессорных сокетов, так и для каналов памяти.
- При обнаружении, во время инициализации процессора, любой критической ошибки светодиодный индикатор состояния системы будет гореть желтым цветом. Желтый светодиод указывает на то, что обнаружена неустранимая ошибка и произошел отказ системы.
- Разделы RAID, созданные с помощью Intel® VROC (SATA RAID), не могут охватывать два встроенных контроллера SATA. В раздел RAID можно включить только диски, подключенные к общему контроллеру SATA.

18. ПРИЛОЖЕНИЕ B. ОШИБКИ КОДА POST

18.1. B.1 Коды ошибок POST

Большинство ошибок, возникающих во время POST, сообщаются с использованием кодов ошибок POST. Эти коды представляют собой конкретные сбои, предупреждения или информацию. Коды ошибок POST могут отображаться на экране диспетчера ошибок и всегда записываются в журнал системных событий (SEL). Регистрируемые события доступны для приложений управления системой, включая удаленное и внеполосное управление.

Существуют исключительные случаи на этапе ранней инициализации, когда системные ресурсы не инициализированы должным образом для обработки сообщений с кодами ошибок POST. Эти случаи в основном представляют собой состояния фатальной ошибки, возникающие в результате инициализации процессоров и памяти, и передающиеся диагностическими светодиодами с остановкой системы.

В следующей таблице перечислены поддерживаемые коды ошибок POST. Каждому коду ошибки присваивается тип ошибки, который определяет действие, которое BIOS выполняет при обнаружении ошибки. Типы ошибок подразделяются на незначительные, серьезные и критические. Действия BIOS для каждого из них определяются следующим образом:

- **Фатальные (Fatal):** Если система не может загрузиться, POST останавливается и отображает следующее сообщение:
  Unrecoverable fatal error found. System will not boot until the error is resolved
  Press <F2> to enter setup
  (Обнаружена неустранимая фатальная ошибка. Система не загрузится, пока ошибка не будет устранена
  Нажмите <F2>, чтобы войти в настройку.)
  При нажатии клавиши <F2> на клавиатуре сообщение об ошибке отображается на экране диспетчера ошибок и регистрируется в журнале системных событий (SEL) с кодом ошибки POST.
  Параметр «**Пауза при ошибке POST**» в настройках BIOS не влияет на эту ошибку.
  Если система не может загрузиться, система генерирует звуковой код, состоящий из трех длинных сигналов и одного короткого сигнала. Система не может загрузиться, пока ошибка не будет устранена. Неисправный компонент необходимо заменить.
  Светодиодный индикатор состояния системы горит желтым цветом для всех фатальных ошибок, обнаруженных во время инициализации процессора. Постоянно горящий желтый индикатор состояния системы указывает на неисправимый сбой системы.
- **Серьезные (Major):** сообщение об ошибке отображается на экране диспетчера ошибок и регистрируется в журнале событий. Если в BIOS включена опция «**POST Error Pause**», для продолжения загрузки системы требуется вмешательство оператора. Если параметр настройки BIOS «**POST Error Pause**» отключен, система продолжит загрузку.

ПРИМЕЧАНИЕ: для ошибки 0048 «**Password check failed**» система останавливается, а затем после сброса/перезагрузки отображает код ошибки на экране диспетчера ошибок.

- **Незначительные (Minor):** сообщение об ошибке может отображаться на экране или в диспетчере ошибок настройки BIOS, а код ошибки POST записывается в журнал SEL. Система продолжает загружаться в проблемном состоянии.

Пользователь может захотеть заменить ошибочный блок. Параметр «**POST Error Pause**» в настройках BIOS не влияет на эту ошибку.

ПРИМЕЧАНИЕ: коды ошибок POST (Таблица 81) являются общими для всех серверных платформ QTECH серии QSRV E-R/P-R текущего поколения. Функции, присутствующие на данной материнской плате/системе, определяют, какие из перечисленных кодов ошибок поддерживаются.

Таблица 81. Коды ошибок и сообщения POST

Код ошибки	Сообщение об ошибке	Сообщение о действиях	Тип ошибки
0012	System RTC date/time not set		Major
0048	Password check failed	Please put right password	Major
0140	PCI component encountered a PERR error		Major
0141	PCI resource conflict		Major
0146	PCI out of resources error	Please enable Memory Mapped I/O above 4 GB item at SETUP to use 64bit MMIO	Major
0191	Processor core/thread count mismatch detected	Please use identical CPU type	Fatal
0192	Processor cache size mismatch detected	Please use identical CPU type	Fatal
0194	Processor family mismatch detected	Please use identical CPU type	Fatal
0195	Processor Intel(R) UPI link frequencies unable to synchronize		Fatal
0196	Processor model mismatch detected	Please use identical CPU type	Fatal
0197	Processor frequencies unable to synchronize	Please use identical CPU type	Fatal
5220	BIOS Settings reset to default settings		Major

Код ошибки	Сообщение об ошибке	Сообщение о действиях	Тип ошибки
5221	Passwords cleared by jumper		Major
5224	Password clear jumper is Set	Recommend to remind user to install BIOS password as BIOS admin password is the master keys for several BIOS security features	Major
8130	Processor 01 disabled		Major
8131	Processor 02 disabled		Major
8160	Processor 01 unable to apply microcode update		Major
8161	Processor 02 unable to apply microcode update		Major
8170	Processor 01 failed self-test (BIST)		Major
8171	Processor 02 failed self-test (BIST)		Major
8180	Processor 01 microcode update not found		Minor
8181	Processor 02 microcode update not found		Minor
8190	Watchdog timer failed on last boot		Major
8198	OS boot watchdog timer failure		Major
8300	Baseboard management controller failed self-test		Major
8305	Hot Swap Controller failure		Major
83A0	Intel ME failed self-test		Major

Код ошибки	Сообщение об ошибке	Сообщение о действиях	Тип ошибки
83A1	Intel ME failed to respond		Major
84F2	Baseboard management controller failed to respond		Major
84F3	Baseboard management controller in update mode		Major
84F4	Sensor data record empty	Please update right SDR	Major
84FF	System event log full	Please clear SEL through EWS or SELVIEW utility	Minor
8500	Memory component could not be configured in the selected RAS mode		Major
8501	DIMM population error	Please plug DIMM at right population	Major
8520	CPU1_DIMM_A1 failed test/initialization	Please remove the disabled DIMM	Major
8521	CPU1_DIMM_A2 failed test/initialization	Please remove the disabled DIMM	Major
8522	CPU1_DIMM_A3 failed test/initialization	Please remove the disabled DIMM	Major
8523	CPU1_DIMM_B1 failed test/initialization	Please remove the disabled DIMM	Major
8524	CPU1_DIMM_B2 failed test/initialization	Please remove the disabled DIMM	Major
8525	CPU1_DIMM_B3 failed test/initialization	Please remove the disabled DIMM	Major
8526	CPU1_DIMM_C1 failed test/initialization	Please remove the disabled DIMM	Major
8527	CPU1_DIMM_C2 failed test/initialization	Please remove the disabled DIMM	Major

Код ошибки	Сообщение об ошибке	Сообщение о действиях	Тип ошибки
8528	CPU1_DIMM_C3 failed test/initialization	Please remove the disabled DIMM	Major
8529	CPU1_DIMM_D1 failed test/initialization	Please remove the disabled DIMM	Major
852A	CPU1_DIMM_D2 failed test/initialization	Please remove the disabled DIMM	Major
852B	CPU1_DIMM_D3 failed test/initialization	Please remove the disabled DIMM	Major
852C	CPU1_DIMM_E1 failed test/initialization	Please remove the disabled DIMM	Major
852D	CPU1_DIMM_E2 failed test/initialization	Please remove the disabled DIMM	Major
852E	CPU1_DIMM_E3 failed test/initialization	Please remove the disabled DIMM	Major
852F	CPU1_DIMM_F1 failed test/initialization	Please remove the disabled DIMM	Major
8530	CPU1_DIMM_F2 failed test/initialization	Please remove the disabled DIMM	Major
8531	CPU1_DIMM_F3 failed test/initialization	Please remove the disabled DIMM	Major
8532	CPU1_DIMM_G1 failed test/initialization	Please remove the disabled DIMM	Major
8533	CPU1_DIMM_G2 failed test/initialization	Please remove the disabled DIMM	Major
8534	CPU1_DIMM_G3 failed test/initialization	Please remove the disabled DIMM	Major
8535	CPU1_DIMM_H1 failed test/initialization	Please remove the disabled DIMM	Major

Код ошибки	Сообщение об ошибке	Сообщение о действиях	Тип ошибки
8536	CPU1_DIMM_H2 failed test/initialization	Please remove the disabled DIMM	Major
8537	CPU1_DIMM_H3 failed test/initialization	Please remove the disabled DIMM	Major
8538	CPU2_DIMM_A1 failed test/initialization	Please remove the disabled DIMM	Major
8539	CPU2_DIMM_A2 failed test/initialization	Please remove the disabled DIMM	Major
853A	CPU2_DIMM_A3 failed test/initialization	Please remove the disabled DIMM	Major
853B	CPU2_DIMM_B1 failed test/initialization	Please remove the disabled DIMM	Major
853C	CPU2_DIMM_B2 failed test/initialization	Please remove the disabled DIMM	Major
853D	CPU2_DIMM_B3 failed test/initialization	Please remove the disabled DIMM	Major
853E	CPU2_DIMM_C1 failed test/initialization	Please remove the disabled DIMM	Major
853F (Go to 85C0)	CPU2_DIMM_C2 failed test/initialization	Please remove the disabled DIMM	Major
8540	CPU1_DIMM_A1 disabled	Please remove the disabled DIMM	Major
8541	CPU1_DIMM_A2 disabled	Please remove the disabled DIMM	Major
8542	CPU1_DIMM_A3 disabled	Please remove the disabled DIMM	Major
8543	CPU1_DIMM_B1 disabled	Please remove the disabled DIMM	Major
8544	CPU1_DIMM_B2 disabled	Please remove the disabled DIMM	Major
8545	CPU1_DIMM_B3 disabled	Please remove the disabled DIMM	Major

Код ошибки	Сообщение об ошибке	Сообщение о действиях	Тип ошибки
8546	CPU1_DIMM_C1 disabled	Please remove the disabled DIMM	Major
8547	CPU1_DIMM_C2 disabled	Please remove the disabled DIMM	Major
8548	CPU1_DIMM_C3 disabled	Please remove the disabled DIMM	Major
8549	CPU1_DIMM_D1 disabled	Please remove the disabled DIMM	Major
854A	CPU1_DIMM_D2 disabled	Please remove the disabled DIMM	Major
854B	CPU1_DIMM_D3 disabled	Please remove the disabled DIMM	Major
854C	CPU1_DIMM_E1 disabled	Please remove the disabled DIMM	Major
854D	CPU1_DIMM_E2 disabled	Please remove the disabled DIMM	Major
854E	CPU1_DIMM_E3 disabled	Please remove the disabled DIMM	Major
854F	CPU1_DIMM_F1 disabled	Please remove the disabled DIMM	Major
8550	CPU1_DIMM_F2 disabled	Please remove the disabled DIMM	Major
8551	CPU1_DIMM_F3 disabled	Please remove the disabled DIMM	Major
8552	CPU1_DIMM_G1 disabled	Please remove the disabled DIMM	Major
8553	CPU1_DIMM_G2 disabled	Please remove the disabled DIMM	Major
8554	CPU1_DIMM_G3 disabled	Please remove the disabled DIMM	Major
8555	CPU1_DIMM_H1 disabled	Please remove the disabled DIMM	Major
8556	CPU1_DIMM_H2 disabled	Please remove the disabled DIMM	Major
8557	CPU1_DIMM_H3 disabled	Please remove the disabled DIMM	Major
8558	CPU2_DIMM_A1 disabled	Please remove the disabled DIMM	Major
8559	CPU2_DIMM_A2 disabled	Please remove the disabled DIMM	Major
855A	CPU2_DIMM_A3 disabled	Please remove the disabled DIMM	Major

Код ошибки	Сообщение об ошибке	Сообщение о действиях	Тип ошибки
855B	CPU2_DIMM_B1 disabled	Please remove the disabled DIMM	Major
855C	CPU2_DIMM_B2 disabled	Please remove the disabled DIMM	Major
855D	CPU2_DIMM_B3 disabled	Please remove the disabled DIMM	Major
855E	CPU2_DIMM_C1 disabled	Please remove the disabled DIMM	Major
855F (Go to 85D0)	CPU2_DIMM_C2 disabled	Please remove the disabled DIMM	Major
8560	CPU1_DIMM_A1 encountered a Serial Presence Detection (SPD) failure		Major
8561	CPU1_DIMM_A2 encountered a Serial Presence Detection (SPD) failure		Major
8562	CPU1_DIMM_A3 encountered a Serial Presence Detection (SPD) failure		Major
8563	CPU1_DIMM_B1 encountered a Serial Presence Detection (SPD) failure		Major
8564	CPU1_DIMM_B2 encountered a Serial Presence Detection (SPD) failure		Major
8565	CPU1_DIMM_B3 encountered a Serial Presence Detection (SPD) failure		Major

Код ошибки	Сообщение об ошибке	Сообщение о действиях	Тип ошибки
8566	CPU1_DIMM_C1 encountered a Serial Presence Detection (SPD) failure		Major
8567	CPU1_DIMM_C2 encountered a Serial Presence Detection (SPD) failure		Major
8568	CPU1_DIMM_C3 encountered a Serial Presence Detection (SPD) failure		Major
8569	CPU1_DIMM_D1 encountered a Serial Presence Detection (SPD) failure		Major
856A	CPU1_DIMM_D2 encountered a Serial Presence Detection (SPD) failure		Major
856B	CPU1_DIMM_D3 encountered a Serial Presence Detection (SPD) failure		Major
856C	CPU1_DIMM_E1 encountered a Serial Presence Detection (SPD) failure		Major
856D	CPU1_DIMM_E2 encountered a Serial Presence Detection (SPD) failure		Major
856E	CPU1_DIMM_E3 encountered a Serial Presence Detection (SPD) failure		Major

Код ошибки	Сообщение об ошибке	Сообщение о действиях	Тип ошибки
856F	CPU1_DIMM_F1 encountered a Serial Presence Detection (SPD) failure		Major
8570	CPU1_DIMM_F2 encountered a Serial Presence Detection (SPD) failure		Major
8571	CPU1_DIMM_F3 encountered a Serial Presence Detection (SPD) failure		Major
8572	CPU1_DIMM_G1 encountered a Serial Presence Detection (SPD) failure		Major
8573	CPU1_DIMM_G2 encountered a Serial Presence Detection (SPD) failure		Major
8574	CPU1_DIMM_G3 encountered a Serial Presence Detection (SPD) failure		Major
8575	CPU1_DIMM_H1 encountered a Serial Presence Detection (SPD) failure		Major
8576	CPU1_DIMM_H2 encountered a Serial Presence Detection (SPD) failure		Major
8577	CPU1_DIMM_H3 encountered a Serial Presence Detection (SPD) failure		Major

Код ошибки	Сообщение об ошибке	Сообщение о действиях	Тип ошибки
8578	CPU2_DIMM_A1 encountered a Serial Presence Detection (SPD) failure		Major
8579	CPU2_DIMM_A2 encountered a Serial Presence Detection (SPD) failure		Major
857A	CPU2_DIMM_A3 encountered a Serial Presence Detection (SPD) failure		Major
857B	CPU2_DIMM_B1 encountered a Serial Presence Detection (SPD) failure		Major
857C	CPU2_DIMM_B2 encountered a Serial Presence Detection (SPD) failure		Major
857D	CPU2_DIMM_B3 encountered a Serial Presence Detection (SPD) failure		Major
857E	CPU2_DIMM_C1 encountered a Serial Presence Detection (SPD) failure		Major
857F (Go to 85E0)	CPU2_DIMM_C2 encountered a Serial Presence Detection (SPD) failure		Major
85C0	CPU2_DIMM_C3 failed test/initialization	Please remove the disabled DIMM	Major
85C1	CPU2_DIMM_D1 failed test/initialization	Please remove the disabled DIMM	Major

Код ошибки	Сообщение об ошибке	Сообщение о действиях	Тип ошибки
85C2	CPU2_DIMM_D2 failed test/initialization	Please remove the disabled DIMM	Major
85C3	CPU2_DIMM_D3 failed test/initialization	Please remove the disabled DIMM	Major
85C4	CPU2_DIMM_E1 failed test/initialization	Please remove the disabled DIMM	Major
85C5	CPU2_DIMM_E2 failed test/initialization	Please remove the disabled DIMM	Major
85C6	CPU2_DIMM_E3 failed test/initialization	Please remove the disabled DIMM	Major
85C7	CPU2_DIMM_F1 failed test/initialization	Please remove the disabled DIMM	Major
85C8	CPU2_DIMM_F2 failed test/initialization	Please remove the disabled DIMM	Major
85C9	CPU2_DIMM_F3 failed test/initialization	Please remove the disabled DIMM	Major
85CA	CPU2_DIMM_G1 failed test/initialization	Please remove the disabled DIMM	Major
85CB	CPU2_DIMM_G2 failed test/initialization	Please remove the disabled DIMM	Major
85CC	CPU2_DIMM_G3 failed test/initialization	Please remove the disabled DIMM	Major
85CD	CPU2_DIMM_H1 failed test/initialization	Please remove the disabled DIMM	Major
85CE	CPU2_DIMM_H2 failed test/initialization	Please remove the disabled DIMM	Major
85CF	CPU2_DIMM_H3 failed test/initialization	Please remove the disabled DIMM	Major
85D0	CPU2_DIMM_C3 disabled	Please remove the disabled DIMM	Major

Код ошибки	Сообщение об ошибке	Сообщение о действиях	Тип ошибки
85D1	CPU2_DIMM_D1 disabled	Please remove the disabled DIMM	Major
85D2	CPU2_DIMM_D2 disabled	Please remove the disabled DIMM	Major
85D3	CPU2_DIMM_D3 disabled	Please remove the disabled DIMM	Major
85D4	CPU2_DIMM_E1 disabled	Please remove the disabled DIMM	Major
85D5	CPU2_DIMM_E2 disabled	Please remove the disabled DIMM	Major
85D6	CPU2_DIMM_E3 disabled	Please remove the disabled DIMM	Major
85D7	CPU2_DIMM_F1 disabled	Please remove the disabled DIMM	Major
85D8	CPU2_DIMM_F2 disabled	Please remove the disabled DIMM	Major
85D9	CPU2_DIMM_F3 disabled	Please remove the disabled DIMM	Major
85DA	CPU2_DIMM_G1 disabled	Please remove the disabled DIMM	Major
85DB	CPU2_DIMM_G2 disabled	Please remove the disabled DIMM	Major
85DC	CPU2_DIMM_G3 disabled	Please remove the disabled DIMM	Major
85DD	CPU2_DIMM_H1 disabled	Please remove the disabled DIMM	Major
85DE	CPU2_DIMM_H2 disabled	Please remove the disabled DIMM	Major
85DF	CPU2_DIMM_H3 disabled	Please remove the disabled DIMM	Major
85E0	CPU2_DIMM_C3 encountered a Serial Presence Detection (SPD) failure		Major
85E1	CPU2_DIMM_D1 encountered a Serial Presence Detection (SPD) failure		Major

Код ошибки	Сообщение об ошибке	Сообщение о действиях	Тип ошибки
85E2	CPU2_DIMM_D2 encountered a Serial Presence Detection (SPD) failure		Major
85E3	CPU2_DIMM_D3 encountered a Serial Presence Detection (SPD) failure		Major
85E4	CPU2_DIMM_E1 encountered a Serial Presence Detection (SPD) failure		Major
85E5	CPU2_DIMM_E2 encountered a Serial Presence Detection (SPD) failure		Major
85E6	CPU2_DIMM_E3 encountered a Serial Presence Detection (SPD) failure		Major
85E7	CPU2_DIMM_F1 encountered a Serial Presence Detection (SPD) failure		Major
85E8	CPU2_DIMM_F2 encountered a Serial Presence Detection (SPD) failure		Major
85E9	CPU2_DIMM_F3 encountered a Serial Presence Detection (SPD) failure		Major
85EA	CPU2_DIMM_G1 encountered a Serial Presence Detection (SPD) failure		Major

Код ошибки	Сообщение об ошибке	Сообщение о действиях	Тип ошибки
85EB	CPU2_DIMM_G2 encountered a Serial Presence Detection (SPD) failure		Major
85EC	CPU2_DIMM_G3 encountered a Serial Presence Detection (SPD) failure		Major
85ED	CPU2_DIMM_H1 encountered a Serial Presence Detection (SPD) failure		Major
85EE	CPU2_DIMM_H2 encountered a Serial Presence Detection (SPD) failure		Major
85EF	CPU2_DIMM_H3 encountered a Serial Presence Detection (SPD) failure		Major
8604	POST Reclaim of non-critical NVRAM variables		Minor
8605	BIOS Settings are corrupted		Major
8606	NVRAM variable space was corrupted and has been reinitialized		Major
8607	Recovery boot has been initiated	Note: The Primary BIOS image may be corrupted or the system may hang during POST. A BIOS update is required	Fatal
92A3	Serial port component was not detected		Major
92A9	Serial port component encountered a resource conflict error		Major

Код ошибки	Сообщение об ошибке	Сообщение о действиях	Тип ошибки
A000	TPM device not detected		Minor
A001	TPM device missing or not responding		Minor
A002	TPM device failure		Minor
A003	TPM device failed self-test		Minor
A100	BIOS ACM Error		Major
A421	PCI component encountered a SERR error		Fatal
A5A0	PCI Express component encountered a PERR error		Minor
A5A1	PCI Express component encountered an SERR error		Fatal
A6A0	DXE Boot Services driver: Not enough memory available to shadow a Legacy Option ROM	Please disable OpRom at SETUP to save runtime memory	Minor

18.2. B.2 Звуковые коды ошибок POST

Звуковые коды ошибок POST (см. Таблица 82). Перед инициализацией системного видео BIOS использует эти звуковые коды, чтобы сообщить пользователю об ошибках. За звуковым сигналом следует код, видимый пользователем, на светодиодах выполнения POST.

Таблица 82. Звуковые коды ошибок POST

Гудки	Сообщение об ошибке	Код выполнения POST	Описание
1 короткий	USB device action	N/A	Короткий звуковой сигнал раздается всякий раз, когда USB-устройство обнаруживается в процессе POST и вставляется или извлекается во время выполнения

Гудки	Сообщение об ошибке	Код выполнения POST	Описание
1 длинный	Intel® TXT security violation	AE, AF	Система остановлена, так как технология Intel® Trusted Execution обнаружила потенциальное нарушение безопасности системы
3 коротких	Memory error	Multiple	Система остановлена из-за обнаружения фатальной ошибки, связанной с памятью
3 длинных и 1 короткий	CPU mismatch error	E5, E6	Система остановлена из-за обнаружения фатальной ошибки, связанной с несоответствием семейства CPU/ядер/кеша
2 коротких	BIOS recovery started	N/A	Начата загрузка для восстановления
4 коротких	BIOS recovery failed	N/A	Восстановление не удалось. Обычно это происходит сразу после начала восстановления, так что звучит как 2 – 4 звуковых сигнала

Встроенный BMC может генерировать звуковые коды при обнаружении отказов. Звуковые коды звучат каждый раз, когда обнаруживается проблема, например, при каждой попытке включения питания, но не звучат постоянно. Коды перечислены см. Таблицу 83. Каждая цифра в коде представлена последовательностью звуковых сигналов, количество которых равно цифре.

Таблица 83. Встроенные звуковые коды BMC

Код	Связанные датчики	Причина звукового сигнала
1-5-2-1	CPUs не установлены или первый разъем CPU пуст	Сокет CPU1 пуст или сокеты установлены неправильно. CPU1 должен быть установлен перед CPU2
1-5-2-2	Сообщение об ошибке CPU CAT (IERR)	CPU обнаружил ошибку при инициализации
1-5-2-3	Ошибка тайм-аута CPU ERR2	CPU не удалось инициализировать систему за указанное время

Код	Связанные датчики	Причина звукового сигнала
1-5-2-4	Несоответствие MSID	Несоответствие MSID возникает, если процессор установлен в системную плату с несовместимыми возможностями питания
1-5-2-5	Ошибка заполнения CPU	Сокет CPU1 пуст или сокеты заполнены неправильно. CPU1 должен быть установлен перед CPU2
1-5-4-2	Неисправность питания	Неожиданное отключение питания постоянного тока (обрыв питания) — датчики блока питания сообщают об отказе блока питания
1-5-4-4	Ошибка управления питанием (тайм-аут подтверждения питания)	Тайм-аут подтверждения питания — датчики блока питания сообщают о сбое программного управления мощностью
1-5-1-2	Сообщение датчика сторожевого таймера VR	Последовательность включения постоянного тока контроллера VR не была выполнена вовремя
1-5-1-4	Состояние источника питания	Присутствует блок питания (PSU), который является несовместимым с одним или несколькими другими блоками питания в системе, что приводит к неожиданному отключению или к невозможности включения системы

19. ПРИЛОЖЕНИЕ C. ЗАЯВЛЕНИЕ ОБ ЭНЕРГОЗАВИСИМОСТИ

В этом приложении описаны энергозависимые и энергонезависимые компоненты (Таблица 84, Таблица 85). Описание столбцов приводится ниже таблиц.

ПРИМЕЧАНИЕ: в этот раздел не входят какие-либо компоненты, не входящие непосредственно в материнскую плату, такие как компоненты корпуса, процессоры, память, жесткие диски или дополнительные карты.

Таблица 84. Энергозависимые и энергонезависимые компоненты материнской платы

Тип компонента	Размер	Расположение компонента	Данные пользо-вателя	Название
Энергонезависимый	32 МБ/ 64 МБ для безопасности SKU	U1D2	Нет	ПЗУ BMC FW
Энергонезависимый	32 МБ/ 64 МБ для безопасности SKU	U3E1	Нет	ПЗУ BIOS
Энергонезависимый	4 Мбит	U8L1	Нет	X557-AT2 EEROM
Энергозависимый	512 МБ	U1A2	Нет	BMC FW SDRAM

Таблица 85. Энергозависимые и энергонезависимые компоненты на плате расширения LAN

Тип компонента	Размер	Расположение компонента	Данные пользователя	Название
Энергонезависимый	512 кБ	EU2A1	Нет	Inphi® PHY EEPROM
Энергонезависимый	2 кбит	EU3A1	Нет	LAN Riser FRU

- **Тип компонентов:** Материнская плата состоит из трех типов компонентов:
  - **Энергонезависимая:** энергонезависимая память является постоянной и не очищается при отключении питания от системы. Чтобы удалить данные, необходимо стереть энергонезависимую память. Точный метод очистки этих областей зависит от конкретного компонента. Некоторые области

необходимы для нормальной работы платы, и очистка этих областей может вывести материнскую плату из строя.

  - **Энергозависимая:** энергозависимая память очищается автоматически при отключении питания от системы.
  - **Батарея питание RAM:** используется питание от батареи на плате. Данные в оперативной памяти с питанием от батареи сохраняются до тех пор, пока батарея не будет снята с материнской платы.

- **Размер:** размер каждого компонента в битах, кбитах, мегабитах, байтах, килобайтах (кБ) или мегабайтах (МБ).
- **Расположение компонента:** расположение компонента — это физическое расположение каждого компонента, соответствующее информации о схеме материнской платы.
- **Данные пользователя:** компоненты флеш-памяти, на плате, не хранят пользовательские данные из операционной системы. Никакие данные уровня операционной системы не сохраняются ни в одном из перечисленных компонентов после отключения питания переменного тока. Сохранность информации, записанной в каждый компонент, определяется его типом (см. Таблица 84).

Каждый компонент хранит данные, относящиеся к его функции. Некоторые компоненты могут содержать пароли, обеспечивающие доступ к конфигурации или функциям этого устройства. Эти пароли специфичны для устройства и уникальны, они не связаны с паролями операционной системы. Конкретные компоненты, которые могут содержать данные пароля:

- **BIOS:** BIOS материнской платы обеспечивает возможность предотвращения неавторизованных пользователей к настройке параметров BIOS, когда установлен пароль BIOS. Этот пароль хранится во флеш-памяти BIOS и используется только для установки ограничений доступа к конфигурации BIOS.
- **BMC:** материнская плата поддерживает контроллер управления платой (BMC), соответствующий интерфейсу интеллектуального управления платформой (IPMI) 2.0. BMC обеспечивает возможности мониторинга состояния, оповещения и удаленного управления питанием для материнской платы. BMC не имеет доступа к данным уровня операционной системы.

BMC поддерживает возможность удаленного программного обеспечения для подключения по сети и выполнения мониторинга состояния и управления питанием. Этот доступ можно настроить так, чтобы он требовал аутентификации по паролю. Если он настроен, то BMC поддерживает пароли пользователей для управления этим доступом. Эти пароли хранятся во флеш-памяти BMC.

20. ПРИЛОЖЕНИЕ D. НОРМАТИВНАЯ ИНФОРМАЦИЯ И СЕРТИФИКАЦИЯ

20.1. D.1 Нормативная информация о продукте

Этот продукт был оценен и сертифицирован как оборудование информационных технологий (ITE), которое может быть установлено в офисах, школах, компьютерных классах и подобных местах коммерческого типа. Пригодность этого продукта для других категорий сертификации продукции и/или сред (таких как: медицина, промышленность, телекоммуникации, NEBS, жилые помещения, системы сигнализации, испытательное оборудование и т. д.).

Компания QTECH подтвердила, что все продукты, **сконфигурированные и проданные QTECH своим клиентам**, соответствуют требованиям для всех нормативных сертификатов, определенных в следующей таблице. Заказчик QTECH несет ответственность за то, чтобы его окончательные конфигурации серверной системы были протестированы и сертифицированы на соответствие нормативным требованиям стран, в которые они планируют поставлять или развертывать серверные платформы.

Таблица 86. Нормативная сертификация

	Серверная платформа QTECH серии QSRV E-R/P-R		**Комментарии**
	Материнская плата	Серверный корпус	Уровень интеграции продукта
Нормативная сертификация			
Сертификация CU (Россия/Беларусь/Казахстан)	✓	✓	Серверная платформа
Европейская декларация соответствия CE	✓	✓	Серверная платформа
Проверка выбросов FCC, часть 15 (США и Канада)	○	○	
Сертификация GS в Германии	○	○	
Сертификация BIS в Индии	○	○	
Соответствие международным стандартам — CISPR32 и CISPR24	○	○	
Сертификация VCCI для Японии	○	○	

	Серверная платформа QTECH серии QSRV E-R/P-R		Комментарии
	Материнская плата	Серверный корпус	Уровень интеграции продукта
Сертификация KC в Корее	○	○	
Сертификация в Мексики	○	○	
Сертификация NRTL (США и Канада)	○	○	
Сертификация в Южной Африке	○	○	
Сертификация BSMI Тайваня	○	○	
Сертификация в Украине	○	○	

Таблица Ключ	
Не протестировано/не сертифицировано	○
Испытано/Заверенная — только Limited OEM SKUs	●
Тестирование/Сертификация (Планируется)	(Дата)
Протестировано/сертифицировано	✓

20.2. D.2 EU Директива EC 2019/424 (Lot 9)

С 1 марта 2020 года вступит в силу дополнительный компонент нормативной схемы маркировки CE Европейского Союза (EC), обозначенный как EU Директива EC 2019/424 (Lot 9). После этой даты все новые серверные системы, поставленные или развернутые на территории EC, должны соответствовать всем требованиям маркировки CE, включая те, которые определены дополнительными правилами EU Lot 9.

QTECH подтвердила, что все серверные продукты для своих клиентов соответствуют нормативным требованиям CE, необходимым для данного вида продукции, в том числе тех, которые определены EC Lot 9.

Посетите следующий веб-сайт для получения дополнительной информации о EU Директиве EC 2019/424 (Lot 9):
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0424

В соответствии с требованиями к эффективности материалов, указанными в EU Директиве EC 2019/424 (Lot 9), компания QTECH предоставляет все необходимые сопутствующие товары, указанные ниже:

- Технические характеристики продукта
  - Продукция – Серверные платформы – Серверные платформы GPU – Серия QSRV E-R/P-R – Техническое описание
    https://www.qtech.ru/catalog/servers/servernye_platformy_gpu/
- Система BIOS/Firmware и обновление безопасности
  - Пакет обновления системы (SUP) — только uEFI
  - Intel® One Boot Flash Update (OFU) — поддержка различных ОС
    https://ftp.qtech.ru/Servers%20and%20Storage/Server/
- Intel Solid State Drive (SSD) Secure Data Deletion и микропрограммное обновление
  - Примечание: для конфигураций системы, которые могут быть настроены с твердотельным накопителем Intel
  - Набор инструментов для твердотельных накопителей Intel®
  - https://downloadcenter.intel.com/download/29205?v=t
- Intel® RAID Controller Firmware Updates и другие вспомогательные программы
  - Примечание: для конфигураций систем, которые могут быть настроены с помощью RAID-контроллера QTECH
    https://ftp.qtech.ru/Servers%20and%20Storage/Server/

Продукт L9 — это серверная система, готовая к включению, без установленной операционной системы. Продукт L6 требует установки дополнительных компонентов, чтобы он был готов к включению. Продукты L3 — это варианты компонентов, которые требуют интеграции в шасси для создания функциональной серверной системы.

20.3. D.3 EU Директива EC 2019/424 (Lot 9) — Сводка поддержки

Шаблон для отчета об информации, необходимой для оценки соответствия сервера (EC) 2019/424 (Lot 9). Приведенная здесь информация не представляет собой окончательных результатов тестирования системы сервера. Фактические результаты тестирования заказчиком конфигураций сервера могут отличаться от этого списка. Пользователь использует эту информацию исключительно на свой страх и риск, и QTECH не несет ответственности за соответствие нормативных требований на уровне серверной системы требованиям EC 2019/424 (лот 9).

Таблица 87. Информация о продукте

Информация о продукте	
Тип продукта	Сервер
Название производителя	QTECH
Зарегистрированное торговое наименование и адрес	ООО "КЬЮТЭК"; Юридический адрес: 115230, МОСКВА ГОРОД, ПРОЕЗД ХЛЕБОЗАВОДСКИЙ, ДОМ 7, СТРОЕНИЕ 9, Э 1 П VIII КОМ 12 ОФ
Номер модели продукта и номера моделей для младшего сегмента настройка производительности и высокой производительности, если применимо	
Год выпуска продукта	2021 г.
КПД блока питания при 10 %, 20 %, 50 % и 100 % номинальной выходной мощности	См. следующие таблицы
Коэффициент БП при 50 % от номинального уровня нагрузки	См. следующие таблицы
Номинальная выходная мощность блока питания (Только сервер)	См. следующие таблицы
Мощность в состоянии простоя (Вт) — только сервер	См. следующие таблицы
Список всех компонентов для дополнительных значений мощности на холостом ходу (только сервер)	См. следующие таблицы
Максимальная мощность (только сервер)	См. следующие таблицы

Информация о продукте	
Заявленный класс условий эксплуатации	См. следующие таблицы
Мощность в состоянии простоя (Вт) при более высокой граничной температуре (Только сервер)	См. следующие таблицы
Эффективность активного состояния и производительность в активном состояние сервера (только сервер)	См. следующие таблицы
Информация о функции безопасного удаления данных	См. следующие таблицы
Список рекомендуемых комбинаций для блейд-сервера с совместимым шасси (только сервер)	См. следующие таблицы
Если модель продукта является частью семейства продуктов QTECH, список всех конфигураций модели, представленных моделью должнен быть поставлен (только Сервер)	См. следующие таблицы

Таблица 88. Данные об энергоэффективности — 1 установленная конфигурация (один) CPU

Конфигурация				
			1-CPU Low-End Config	1-CPU High-End Config
Подробности	Узел/ Материнская плата (МБ)	Количество узлов или МБ, установленных в системе	1	1
	Процессор	Количество процессоров на узел/МБ	1	1

Конфигурация				
	Процессор	Модель процессора	Intel® Xeon® Scalable Gold 5122	Intel® Xeon® Scalable Platinum 8280
	Объем памяти	Количество установленных модулей DIMM на узел/МБ	6 (1 DIMM/ канал памяти)	6 (1 DIMM/ канал памяти)
		Емкость на DIMM (ГБ)	32 ГБ	64 ГБ
		Общий объем памяти (ГБ) на узел/МБ	192 ГБ	384 ГБ
	SSD	Общее количество установленных SSD	2	2
	Блок питания (БП)	Общее количество установленных блоков питания	2	2
	Версии системного программного обеспечения, установленные для каждого узла		BIOS R1009 BMC 2.22 FRUSDR 1.76	BIOS R1009 BMC 2.22 FRUSDR 1.76
Сводка данных				
Измеренное и рассчитанное количество серверов	P База		25	25
	Дополнительный процессор		17,22	84,95
	Дополнительный источник питания		10	10
	Устройства хранения данных		10	10
	Дополнительная память		33,84	68,40

Конфигурация			
Измеренное и рассчитанное количество серверов	Дополнительное устройство ввода-вывода (10 Гбит/с, 15 Вт/2 порта на МБ)	30	30
	Perf cpu	1,722	8,495
Пределы/ Результаты	Допустимая мощность холостого хода (Вт)	126,06	228,35
	Проверенная мощность холостого хода (Вт) на узел	84,2	88,7
	Минимально эффективная мощность (Вт)	9	9
	Проверенная эффективная мощность (Вт) на узел	12,4	31,0
Другой результат теста	Мощность холостого хода при более высокой температуре. (на узел) при 35 градусах Цельсия	92,6	93,2
	Максимальная мощность (на узел)	245,0	386,7

Таблица 89. Данные об энергоэффективности — 2 установленных конфигурации (сдвоенных) ЦП

Конфигурация				
			2-CPU Low-End Config	2-CPU High-End Config
Подробности	Узел/ Материнская плата (МБ)	Количество узлов или МБ, установленных в системе	1	1
	Процессор	Количество процессоров на узел/МБ	2	2

Конфигурация				
Подробности	Процессор	Модель процессора	Intel® Xeon® Scalable Gold 5122	Intel® Xeon® Scalable Platinum 8280
	Объем памяти	Количество установленных модулей DIMM на узел/МБ	12 = 6 на процессор (1 DIMM/канал памяти)	12 = 6 на процессор (1 DIMM/ канал памяти)
		Емкость на DIMM (ГБ)	32 ГБ	64 ГБ
		Общий объем памяти (ГБ) на узел/МБ	384 ГБ	768 ГБ
	SSD	Общее количество установленных SSD	2	2
	Блок питания (БП)	Общее количество установленных блоков питания	2	2
	Версии системного программного обеспечения, установленные для каждого узла или МБ		BIOS R1009 BMC 2.22 FRUSDR 1.76	BIOS R1009 BMC 2.22 FRUSDR 1.76
Сводка данных				
Измеренное и рассчитанное количество серверов	P База		38	38
	Дополнительный процессор		23,41	119,91
	Дополнительный источник питания		10	10
	Устройства хранения данных		10	10
	Дополнительная память		68,40	137,52

Конфигурация			
Измеренное и рассчитанное количество серверов	Дополнительное устройство ввода-вывода (10 Гбит/с, 15 Вт/2 порта на МБ)	30	30
	Perf cpu	1,722	8,495
Пределы/ Результаты	Допустимая мощность холостого хода (Вт)	179,81	345,43
	Проверенная мощность холостого хода (Вт) на узел	104,4	111,4
	Минимально эффективная мощность (Вт)	9,5	9,5
	Проверенная эффективная мощность (Вт) на узел	14,1	33,6
Другой результат теста	Мощность холостого хода при более высокой температуре. (на узел) при 35 градусах Цельсия	109,2	118,1
	Максимальная мощность (на узел)	397,2	762,2

Дополнительная информация:

Химическая декларация
Неодим не применяется. (жесткий диск не поставляется QTECH)
Кобальт не применяется. (нет BBU. Монетная батарея не поставляется QTECH)

21. ПРИЛОЖЕНИЕ Е. ГЛОССАРИЙ

Таблица 90. Глоссарий

Термин	Definition	Определение
Intel® AES-NI	Intel® Advanced Encryption Standard New Instructions	Новые инструкции Intel® Advanced Encryption Standard
ACPI	Advanced Configuration and Power Interface	Расширенная конфигурация и интерфейс питания
ADDDC	Adaptive Data Correction	Адаптивная коррекция данных
AHCI	Advanced Host Controller Interface	Расширенный интерфейс хост-контроллера
AIC	Add-in Card	Дополнительная карта
API	Application Programming Interface	Интерфейс прикладного программирования
ARP	Address Resolution Protocol	Протокол разрешения адресов
ATAPI	Advanced Technology Attachment with Packet Interface	Вложение передовых технологий с пакетным интерфейсом
Intel® AVX-512	Intel® Advanced Vector Extension 512	Intel® Advanced Vector Extension 512
Intel® AVX2	Intel® Advanced Vector Extensions 2	Intel® Advanced Vector Extensions 2
BBS	BIOS Boot Specification	Спецификация загрузки BIOS
BBU	Battery Backup Unit	Блок резервного аккумулятора
BIOS	Basic Input Output System	Базовая система ввода вывода
BMC	Baseboard Management Controller	Контроллер управления основной платой
BSP	Bootstrap Processor	Процессор начальной загрузки
CATERR	Catastrophical Error	Катастрофическая ошибка
CFM	cubic feet per minute	Кубических футов в минуту

Термин	Definition	Определение
CLST	Closed-Loop System Throttling	Дросселирование замкнутой системы
CLTT	Closed-Loop Thermal Throttling	Термодросселирование с замкнутым контуром
CMD/ADR	Command/address	Команда/адрес
DDR4	Double Data Rate Type 4	Двойная скорость передачи данных, тип 4
DHCP	Dynamic Host Configuration Protocol	Протокол динамического конфигурирования сервера
DIMM	Dual In-line Memory Module	Двухрядный модуль памяти
DMA	Direct Memory Access	Прямой доступ к памяти
DMI	Direct Media Interface. When accompanied by a number, it refers to the revision (DMI3: DMI revision 3.0)	Прямой медиаинтерфейс. Если сопровождается номером, это означает версию (DMI3: DMI revision 3.0)
DR	Dual Rank	Двойной ранг
DRAM	Dynamic Random Access Memory	Динамическая память с произвольным доступом
DTS	Digital Thermal Sensor	Цифровой термодатчик
ECC	Error Correction Code	Код исправления ошибок
EDS	External Design Specification	Спецификация внешнего дизайна
EFI	Extensible Firmware Interface	Расширяемый интерфейс прошивки
EPS	External Product Specification	Спецификация внешнего продукта
ESRT2	Intel® Embedded Server RAID Technology 2	Технология Intel® Embedded Server RAID 2
FLOPs	Floating-point Operations Per Second	Операций с плавающей точкой в секунду

Термин	Definition	Определение
FMA	Fused Multiply Add	Fused Multiply Add
FRB	Fault Resilient Boot	Отказоустойчивая загрузка
FRU	Field Replaceable Unit	Сменный блок
Gb	Giga bit	Бит гига
GbE	Giga bit Ethernet	Гигабитный Ethernet
Gbps	Giga bits per second	Гигабит в секунду
GPGPU	General Purpose/ Graphics Processing Unit	Универсальный/Графический процессор
GPIO	General Purpose Input-Output	Ввод-вывод общего назначения
GPU	Graphics Processing Unit (graphics card)	Графический процессор (видеокарта)
GT/s	Giga Transfers per second	Гига переводов в секунду
GUI	Graphical User Interface	Графический интерфейс пользователя
GUID	Globally Unique Identifier	Глобальный уникальный идентификатор
HDD	Hard Disk Drive	Накопитель на жестком диске
I2C	Inter-Integrated Circuit	Межинтегральная схема
IDE	Integrated Drive Electronics	Интегрированная приводная электроника
IIO	Integrated IO Module	Интегрированный модуль ввода-вывода
IMC	Integrated Memory Controller	Встроенный контроллер памяти
iPC	Intel Product Code	Код продукции Intel

Термин	Definition	Определение
IPMB	Intelligent Platform Management Bus	Интеллектуальная шина управления платформой
IPMI	Intelligent Platform Management Interface	Интеллектуальный интерфейс управления платформой
JRE	Java* Runtime Environment	Java * Среда выполнения
KVM	Keyboard, Video and Mouse	Клавиатура, видео и мышь
LAN	Local Area Network	Локальная сеть
LDAP	Lightweight Directory Access Protocol	Облегченный протокол доступа к каталогам
LRDIMM	Load Reduced DIMM	DIMM с пониженной нагрузкой
LSB	Least Significant Bit	Наименьший значащий бит
MDRAID	Linux Software Raid	Программное обеспечение Linux Raid
Intel® ME	Intel® Management Engine	Intel® Management Engine
MLE	Measured Launched Environment	Измеренная запускаемая среда
MRC	Memory Reference Code	Справочный код памяти
MSB	Most Significant Bit	Самый важный бит
NDA	Non-Disclosure Agreement	Соглашение о неразглашении
Intel® NM	Intel® Node Manager	Intel® Node Manager
NMI	Non-Maskable Interrupt	Немаскируемое прерывание
NTB	PCI Express Non-Transparent Bridge	Непрозрачный мост PCI Express
NTLDR	NT loader	Загрузчик NT
NVDIMM	Non-Volatile Dual Inline Memory Module	Энергонезависимый двухрядный модуль памяти

Термин	Definition	Определение
OCuLink	Optical Copper Link	Оптическая медная связь
OEM	Original Equipment Manufacturer	Производитель оригинального оборудования
Intel® OFU	Intel® One Boot Flash Update Utility	Утилита обновления Intel® One Boot Flash
OLTT	Open-Loop Thermal Throttling	Тепловое дросселирование с открытым контуром
OS	Operating System	Операционная система
PCH	Platform Controller Hub (chipset)	Концентратор контроллера платформы (набор микросхем)
PCI	Peripheral Component Interconnect	Подключение периферийных компонентов
PCIe*	PCI Express*	PCI Express *
PECI	Platform Environmental Control Interface	Интерфейс управления окружающей средой платформы
PHM	Processor Heat Sink Module	Модуль радиатора процессора
PMBus*	Power Management Bus	Шина управления питанием
POST	Power-On Self-Test	Самотестирование при включении
PPR	Post Package Repair	Почтовый ремонт посылки
PSU	Power Supply Unit	Блок питания
PWM	Pulse Width Modulation	Широтно-импульсная модуляция
QR	Quad Rank	Quad Rank
RAID	Redundant Array of Independent Disks	Избыточный массив независимых дисков
RAS	Reliability, availability, and serviceability	Надежность, доступность и удобство обслуживания

Термин	Definition	Определение
RESTful	Representational State Transfer	Изобразительное State Transfer
RCiEP	Root Complex Integrated Endpoint	Интегрированная конечная точка корневого комплекса
RDIMM	Registered DIMM	Зарегистрированный DIMM
Intel® RMM4 Lite	Intel® Remote Management Module 4 Lite	Модуль удаленного управления Intel® 4 Lite
ROC	Raid-on-Chip	Raid-on-Chip
SAS	Serial Attached SCSI	Последовательный SCSI
SATA	Serial ATA	Последовательный ATA
SCSI	Small Computer System Interface	Интерфейс малой компьютерной системы
SDDC	Single Device Data Correction	Коррекция данных одного устройства
SDR	Sensor Data Record	Запись данных датчика
SEL	System Event Log	Журнал системных событий
SFP+	Small Form Pluggable Plus	Подключаемый модуль Small Form Plus
SIMD	Single Instruction Multiple Data	Одна инструкция, несколько данных
SKU	Stock Keeping Unit	Подразделение складского учета
SmaRT	Smart Ride Through	Умная поездка
SMM	Server Management Mode	Режим управления сервером
SMS	System Management Software	Программное обеспечение для управления системой
SOL	Serial Over LAN	Последовательный через LAN

Термин	Definition	Определение
SPD	Serial Presence Detection	Обнаружение последовательного присутствия
SR	Single Rank	Одиночный ранг
sSATA	Secondary SATA	Вторичный SATA
SSB	Server South Bridge	Южный мост сервера
SSD	Solid State Drive	Твердотельный накопитель
Intel® SSE	Intel® Streaming SIMD Extensions	Расширения Intel® Streaming SIMD
SSH	Secure Shell	Безопасная оболочка
SSL	Secure Sockets Layer	Уровень защищенных гнезд
SUP	System Update Package	Пакет обновления системы
TCG	Trusted Computing Group	Группа доверенных вычислений
TDP	Thermal Design Power	Тепловая схема питания
TPM	Trusted Platform Module	Модуль доверенной платформы
TPS	Technical Product Specification	Технические характеристики продукта
Intel® TXT	Intel® Trusted Execution Technology for servers	Технология Intel® Trusted Execution для серверов
UEFI	Unified Extensible Firmware Interface	Унифицированный расширяемый интерфейс встроенных микропрограмм
Intel® UPI	Intel® Ultra Path Interconnect	Intel® Ultra Path Interconnect
USB	Universal Serial Bus	Универсальная последовательная шина
VGA	Video Graphics Array	Видеографическая матрица

Термин	Definition	Определение
VLSI	Very Large Scale Integration	Очень крупномасштабная интеграция
Intel® VMD	Intel® Volume Management Device	Устройство управления томами Intel®
VMM	Virtual Machine Manager	Диспетчер виртуальных машин
VR	Voltage Regulator	Регулятор напряжения
Intel® VROC	Intel® Virtual RAID on CPU	Intel® Virtual RAID на CPU
VRD	Voltage Regulator-Down	Регулятор понижения напряжения
Intel® VT	Intel® Virtualization Technology	Технология виртуализации Intel

Комплектация

Материнская плата устанавливается в стандартный серверный корпус. Пожалуйста, проверьте наличие в комплекте стандартных деталей, перечисленных ниже:

Таблица 91. Комплектация материнской платы

Объект		Стандартная упаковка	Стандартная заводская упаковка	Примечание
Материнская плата		1	1	Установлена в корпус
Дата-кабель	Кабель питания SATA DOM	Нет	Нет	
	Дата-кабель SATA 6G	4 – 10	Нет	
	Дата-кабель порта COM	Нет	Нет	Нет
Компакт-диск с приложениями	CD-диск с приложениями и драйверами	Нет	Нет	Драйверы доступны для скачивания на официальном сайте

Объект		Стандартная упаковка	Стандартная заводская упаковка	Примечание
Компакт-диск с приложениями	CD-диск с программами удалённого управления BMC	Нет	Нет	Пользователи могут непосредственно через IP получать удалённый доступ, не требуется установка ПО
Документация	Руководство по эксплуатации Список совместимости	Нет	Нет	Руководство по эксплуатации и список совместимости доступны для скачивания на официальном сайте

Если какие-либо части из вышеперечисленных пунктов повреждены или отсутствуют, как можно скорее свяжитесь с официальным дилером или напрямую с компанией QTECH.

22. ОБЩАЯ ИНФОРМАЦИЯ

22.1. Гарантия и сервис

Процедура и необходимые действия по вопросам гарантии описаны на сайте QTECH в разделе «Поддержка» −> «Гарантийное обслуживание».

Ознакомиться с информацией по вопросам тестирования оборудования можно на сайте QTECH в разделе «Поддержка» −> «Взять оборудование на тест».

Вы можете написать напрямую в службу сервиса по электронной почте sc@qtech.ru.

22.2. Техническая поддержка

Если вам необходимо содействие в вопросах, касающихся нашего оборудования, то можете воспользоваться разделом технической поддержки пользователей QTECH на нашем сайте www.qtech.ru/support/.

Телефон Технической поддержки +7 (495) 269-08-81

Центральный офис +7 (495) 477-81-18

22.3. Электронная версия документа

Дата публикации 23.07.2025

https://files.qtech.ru/upload/servers/QSRV_E-R_P-R/QSRV_E-R_P-R_user_manual.pdf