Серверная

материнская плата

Rikor® КДБА.469555.003

R-BD-SXRM-XS16.EA.V6.0

Руководство пользователя

Ред. 1.1 16.04.2021

АЙТИЭНТИ
системный интегратор
По вопросам приобретения:
ООО "АЙТИЭНТИ"
тел: +7 (495) 128-04-63
e-mail: zakaz@itint.ru
сайт: www.itint.ru

<Эта страница намеренно оставлена пустой>

История редакций документа

Дата	Редакция	Изменения
сентябрь 2020 г.	1.0	Выпуск опытного образца. (Документ в разработке)
апрель 2021 г.	1.1	Выпуск серийной продукции

Отказ от ответственности

Информация, содержащаяся в данном руководстве пользователя, тщательно проверена и считается достоверной. Поставщик не несет ответственности за любые неточности, которые могут содержаться в этом документе, и не берет на себя обязательства по обновлению или сохранению информации в этом руководстве или уведомлению какого-либо лица или организации об обновлениях. Информация и технические характеристики, указанные в данном руководстве предназначены только для ознакомления, содержание может обновляться в любое время без уведомления. Обратите внимание: для самой последней версии этого руководства, пожалуйста, посетите наш веб-сайт по адресу **www.rikor.com**.

ООО Рикор-ИМТ («Rikor-IMT») оставляет за собой право вносить изменения в продукт, описанный в этом руководстве, в любое время и без уведомления. Этот продукт, включая программное обеспечение и документацию, является собственностью Rikor-IMT и/или его лицензиаров и предоставляется только по лицензии. Любое использование или воспроизведение данного продукта, не допускается, за исключением случаев, явно разрешенных условиями указанной лицензии. Другие продукты и компании, упомянутые здесь, являются товарными знаками или зарегистрированными товарными знаками соответствующих компаний или владельцев знаков.

НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ RIKOR-IMT НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА ПРЯМЫЕ, НЕПРЯМЫЕ, СПЕЦИАЛЬНЫЕ, СЛУЧАЙНЫЕ, СПЕКУЛЯТИВНЫЕ ИЛИ КОСВЕННЫЕ УБЫТКИ, ВОЗНИКАЮЩИЕ ИЗ ИСПОЛЬЗОВАНИЯ ИЛИ НЕВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ЭТОГО ПРОДУКТА ИЛИ ДОКУМЕНТАЦИИ, ДАЖЕ ЕСЛИ ВЫ ОСВЕДОМЛЕНЫ О ВОЗМОЖНОСТИ ТАКИХ УБЫТКОВ. RIKOR-IMT НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА ЛЮБОЕ ОБОРУДОВАНИЕ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ИЛИ ДАННЫЕ, ЗАПОМНЕННЫЕ ИЛИ ИСПОЛЬЗУЕМЫЕ В ПРОДУКТЕ, ВКЛЮЧАЯ ЗАТРАТЫ НА РЕМОНТ, ЗАМЕНУ, ИНТЕГРАЦИЮ, УСТАНОВКУ ИЛИ ВОССТАНОВЛЕНИЯ ТАКОГО ОБОРУДОВАНИЯ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ИЛИ ДАННЫХ.

Эксплуатация этого оборудования в жилом районе может вызвать вредные помехи, и в этом случае вам придется исправлять помехи за свой счет.

Следующие причины, приведшие к неисправности или повреждению, не являются гарантийным случаем:

A. Стихийное бедствие (наводнение, пожар, удар молнии, тайфун и прочее), непреодолимая сила или действия человека, приведшие к повреждению.

B. Самостоятельный разбор, ремонт изделия или техническое обслуживание изделия в не аккредитованных сервисных центрах Rikor.

C. Самовольное или с привлечением третьих лиц внесение изменений, восстановление, изменение стандартов, а также установка, добавление, расширение комплектующими, приобретёнными не у данной компании или официальных дилеров.

D. Проблемы и неисправности, возникшие вследствие самостоятельной установки ПО или ненадлежащей настройки.

E. Проблемы и неполадки, вызванные компьютерными вирусами.

F. Гарантийная этикетка нарушена или не читается, гарантийный талон стёрт или не соответствует изделию.

G. Требование к Rikor предоставить услуги по установке ПО (пользователи должны предоставить своё собственное лицензионное ПО), устранения неполадок ПО, удаление пароля и прочее.

H. Проблемы и неисправности, возникшие в результате другого неправильного использования.

Любые споры, возникающие между производителем и клиентом, регулируются законами Российской Федерации. Общая ответственность Rikor-IMT по всем претензиям не будет превышать цену, уплаченную за аппаратный продукт.

Редакция 1.1

Подготовлено: 30 апреля 2021

ОГЛАВЛЕНИЕ

Предисловие

Об этом руководстве

Данный документ является руководством по эксплуатации для пользователей серверной материнской платы **Rikor® КДБА.469555.003**, описывающим настройки, характеристики и структуру материнской платы. В дополнение к материнской плате перечислены несколько важных конструктивных частей, входящих в систему.

Данное руководство служит ознакомительным материалом для технического персонала, обслуживающего профессиональные системные интеграторы и персональные компьютеры. Установка и обслуживание данного продукта должны проводиться только опытными техническими сотрудниками.

Это руководство может периодически обновляться без предварительного уведомления. Проверьте веб-сайт Rikor® на предмет возможных обновлений.

Примечания

Чтобы ваша операционная система работала правильно, следуйте приведенным ниже ссылкам, чтобы загрузить все необходимые драйверы/утилиты и руководство пользователя для вашего сервера. Все перечисленные файлы поставляются в комплекте с данным оборудованием на CD/DVD-диске.

- Руководство пользователя и список совместимости:

  http://www.rikor.com/support/UserManual_Rikor_KDBA.469555.003.pdf

- Список совместимости:

  http://www.rikor.com/support/CompatibleList_Rikor_KDBA.469555.003.pdf

- Драйверы и утилиты:

  ftp://ftp.rikor.com/support/drivers/KDBA.469555.003/

- Информация о безопасности продукта:

  http://www.rikor.com/support/ safety_information.pdf

- Если у вас есть какие-либо вопросы, обратитесь в нашу службу поддержки:

  support@rikor.com

Распаковка системы

Осмотрите коробку, в которой была доставлена материнская плата, и обратите внимание, была ли повреждена упаковка, каким-либо образом. Если какое-либо оборудование окажется повреждённым, подайте заявление о возмещении ущерба перевозчику, который его доставил.

Предупреждения

Особое внимание следует обратить на следующие символы, используемые в этом руководстве.

Предупреждение! Обозначает важную информацию, предоставляемую для предотвращения повреждения оборудования/имущества или телесных повреждений.

Предупреждение! Указывает, что выполняемые процедуры производятся с опасностью наличия высокого напряжения.

1. Описание серверной материнской платы

Серверная материнская плата Rikor® КДВА.469555.003 представляет собой монолитную печатную плату в сборе с функциями, которые предназначены для обеспечения гибкости в средах с масштабируемой производительностью.

Эта материнская плата предназначена для поддержки семейства Scalable процессоров Intel® Xeon® 1-го или 2-го поколения. Процессоры Intel® Xeon® предыдущего поколения не поддерживаются. Справочную информацию по совместимому периферийному оборудованию смотрите в файле CompatibleList_Rikor_KDBA.469555.003.pdf.

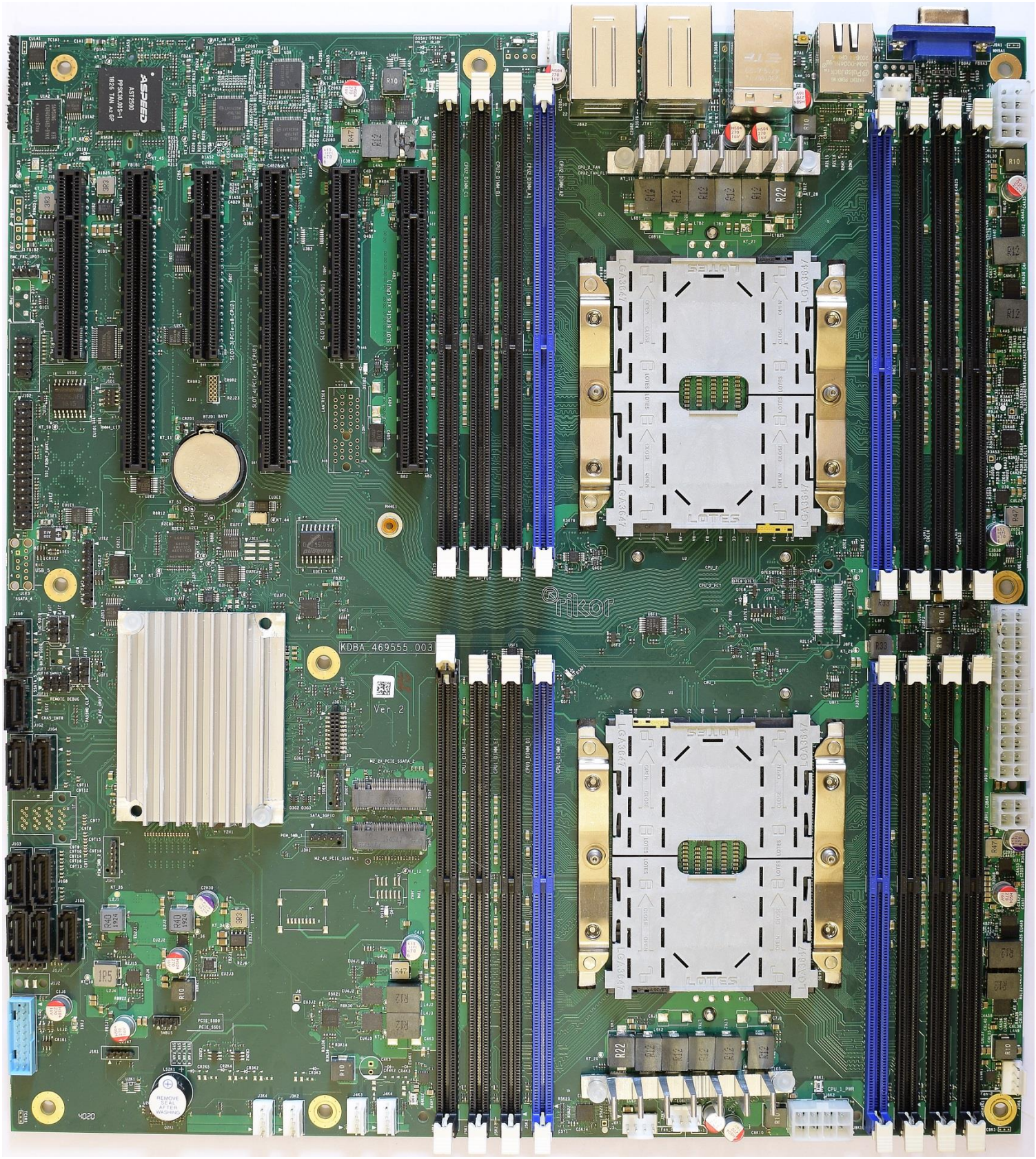


Рисунок 1. Серверная материнская плата Rikor® КДБА.469555.003

1.1 Набор функций серверной материнской платы

Таблица 1. Набор функций серверной материнской платы Rikor® КДБА.469555.003

Функция серверной материнской платы	Rikor® КДБА.469555.003
Процессор	• 2 - процессорных разъема LGA3647-0 (Socket P) • Поддержка (1) или (2) процессоров 1 -го и 2 -го поколения процессоров Intel® Xeon® линейки (Platinum, Gold, Silver и Bronze) **Примечание.** Процессоры Intel® Xeon® предыдущего поколения не поддерживаются. • Максимальная поддерживаемая расчетная тепловая мощность (TDP) до 205 Вт (только плата) **Примечание.** Серверные системы Rikor® на базе этой платы могут поддерживать более низкую максимальную расчетную тепловую мощность (TDP).
объем памяти	• 16 слотов DIMM (по 8 на каждый процессор) • DDR4 RDIMM/LRDIMM, до 2933 MT/c, 1.2 В **Примечание**. Максимальная поддерживаемая скорость памяти зависит от SKU установленного процессора и конфигурации набора модулей памяти.
Набор микросхем Intel® серии C62x	Набор микросхем Intel® C621
Технология Intel® QuickAssist	Нет
Локальная сеть (LAN)	1 Двухпортовый RJ45 1 GbE на борту, 2 однопортовых RJ45 1 GbE на борту (совмещенных с USB),1 однопортовый RJ45 1 GbE на борту Дополнительная переходная плата, совместимая со слотом 5, с двумя разъемами SFP+ 1 Гбит/с
Встроенный PCIe* NVMe *	• Поддержка Intel® VMD • Поддержка Intel® VROC (VMD NVMe RAID) (опция)
Встроенный SATA	12 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) • (2) - Разъемы M.2/sSATA и M.2/PCIe* • (2) - 4-портовые разъемы 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 разделе 5.2)
Слоты для карт расширения PCIe*	• Слот 1: слот PCIe* 3.0 x8 (электрический x8), обрабатываемый CPU2 • Слот 2: слот PCIe* 3.0 x16 (электрический x16), обрабатываемый CPU2 (с возможностью расширения) • Слот 3: слот PCIe* 3.0 x8 (электрический x8), обрабатываемый CPU2 • Слот 4: слот PCIe* 3.0 x16 (электрический x16), обрабатываемый CPU2 • Слот 5: слот PCIe* 3.0 x8 (электрический x8), обрабатываемый CPU1 • Слот 6: слот PCIe* 3.0 x16 (электрический x16) обрабатываемый CPU1 (с возможностью расширения)
видео	• Видео Встроенный 2D контроллер • 16 МБ видеопамяти DDR4 • (1) - Внешний разъем DB-15
USB	• (2) - внешние порты USB 2.0 • (2) - внешние порты USB 3.0 • (1) - внутренний USB 3.0 типа A разъем • (1) - 2x10-контактный разъем с поддержкой передней панели для (2) портов USB 2.0/3.0
Серийный порт	(1) - разъем внутреннего последовательного порта DH-10
Управление сервером	• Встроенный контроллер управления основной платой, совместимый с IPMI 2.0 • Поддержка программного обеспечения Intel® Server Management • Выделенный встроенный порт управления RJ45 • Расширенное управление сервером с помощью Intel® RMM4 Lite (дополнительная опция)
Поддержка системных вентиляторов	• (2) - 4-контактные разъемы для вентиляторов процессора • (6) - 6-контактные разъемы для передних системных вентиляторов • (1) - вентилятор сзади система 4-контактный заголовок

1.2 Идентификация компонентов/функций серверной материнской платы

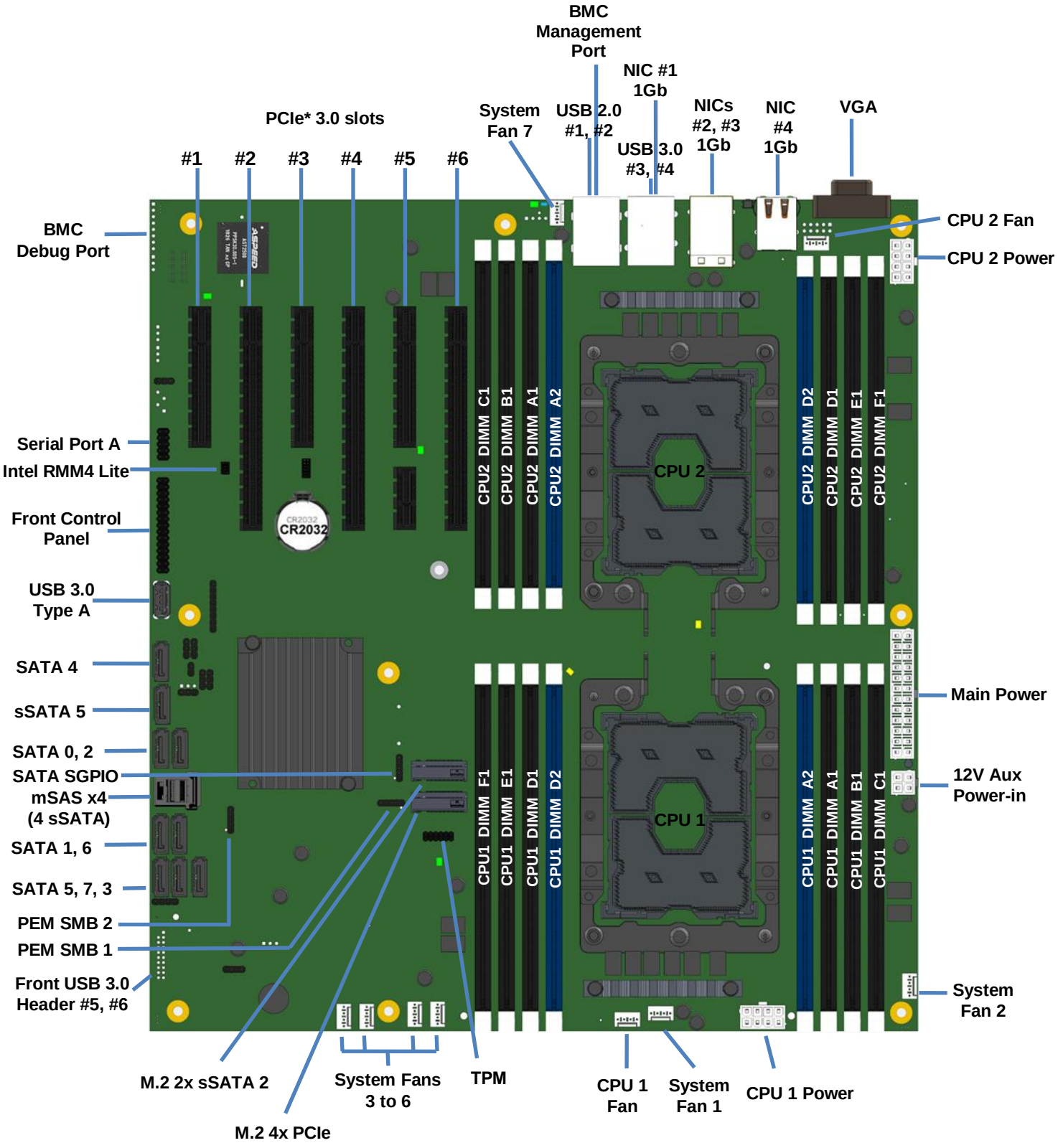


Рисунок 2. Идентификация компонентов/функций серверной материнской платы Rikor® КДБА.469555.003

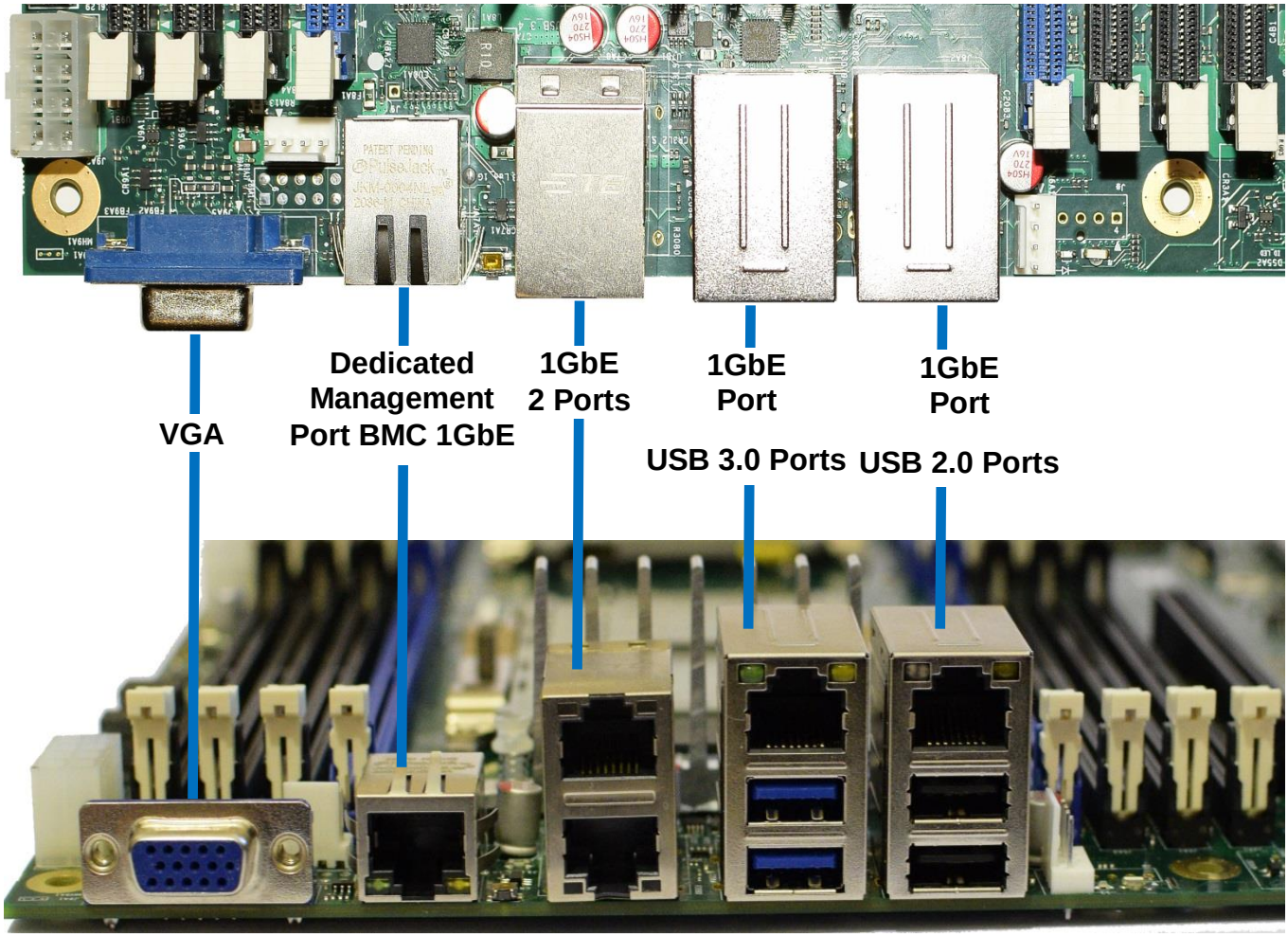


Рисунок 3. Внешние разъемы ввода/вывода серверной материнской платы Rikor® КДБА.469555.003

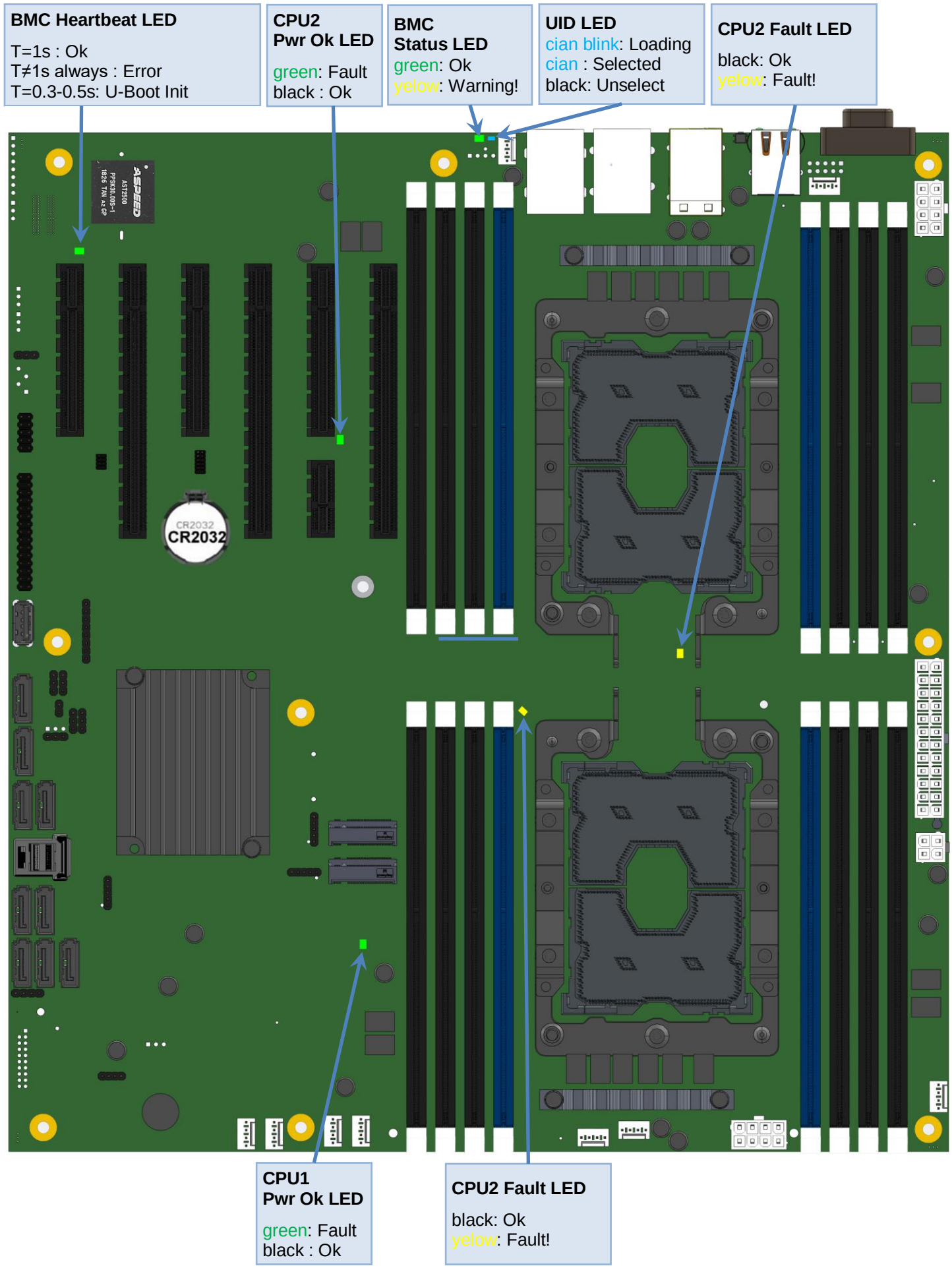


Рисунок 4. Световая диагностика - идентификация светодиода

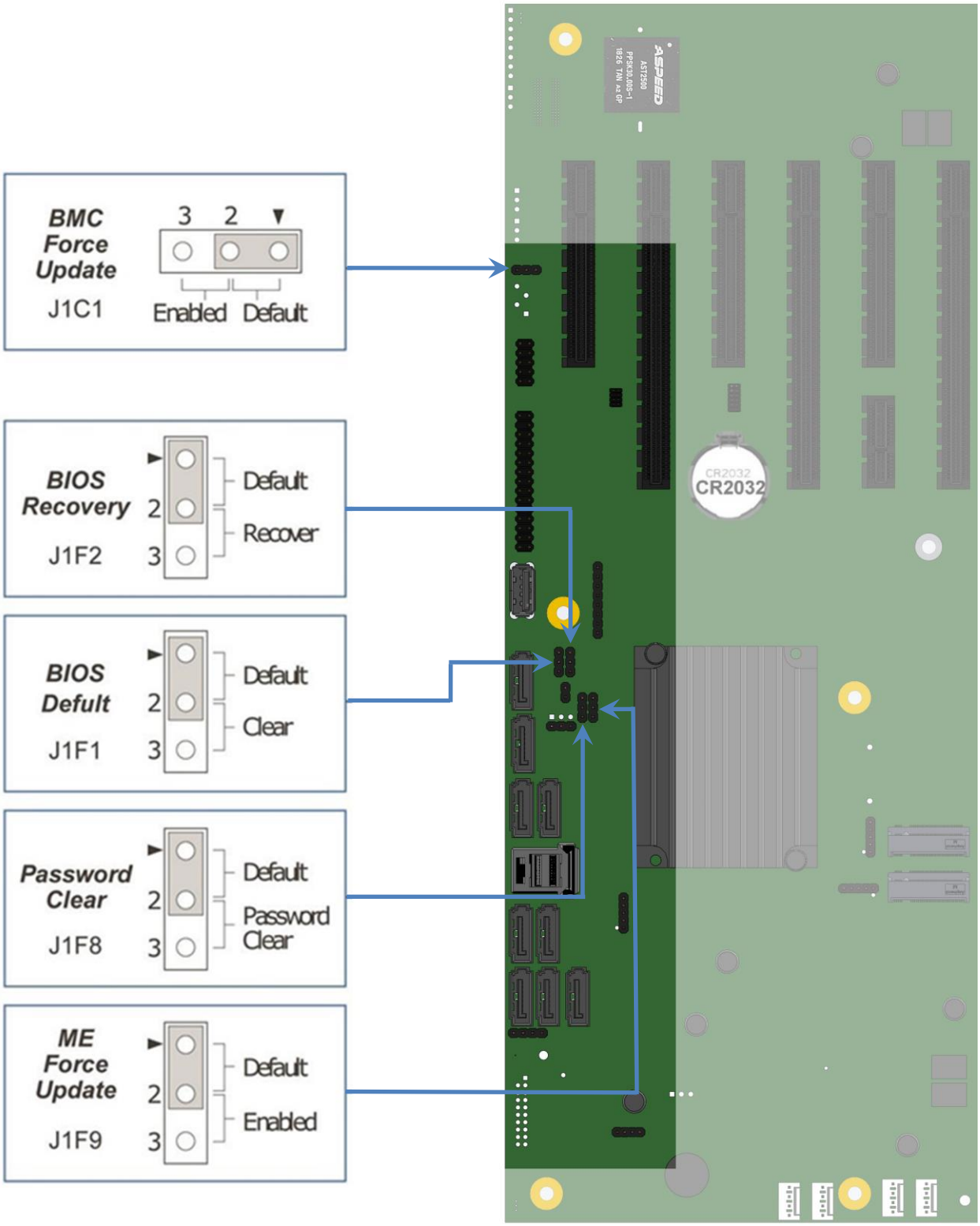


Рисунок 5. Идентификация блока перемычек

См. раздел 10 для получения дополнительных сведений о перемычках сброса и восстановления.

1.3 Механические чертежи серверной материнской платы

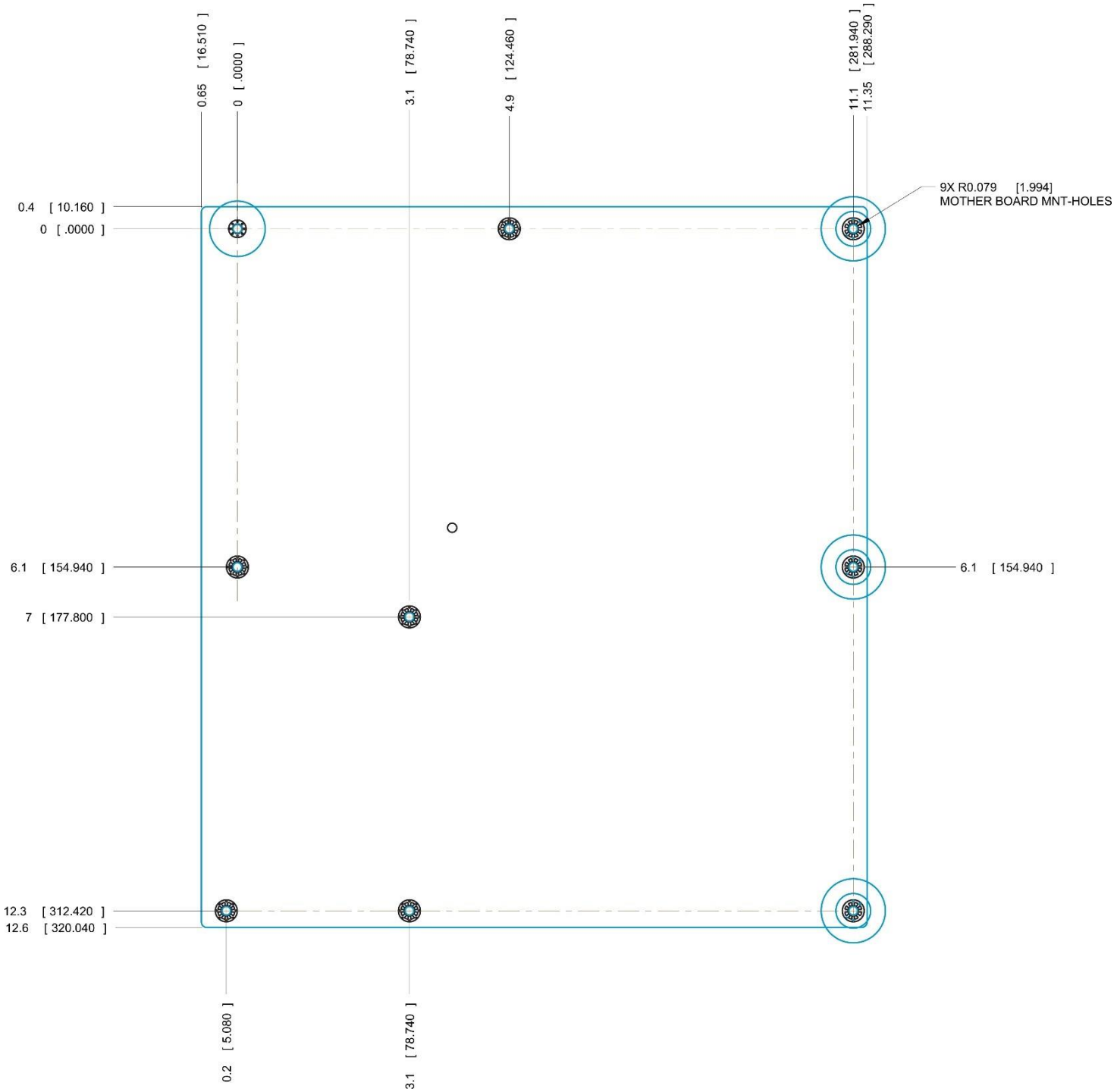


Рисунок 6. Монтажные отверстия

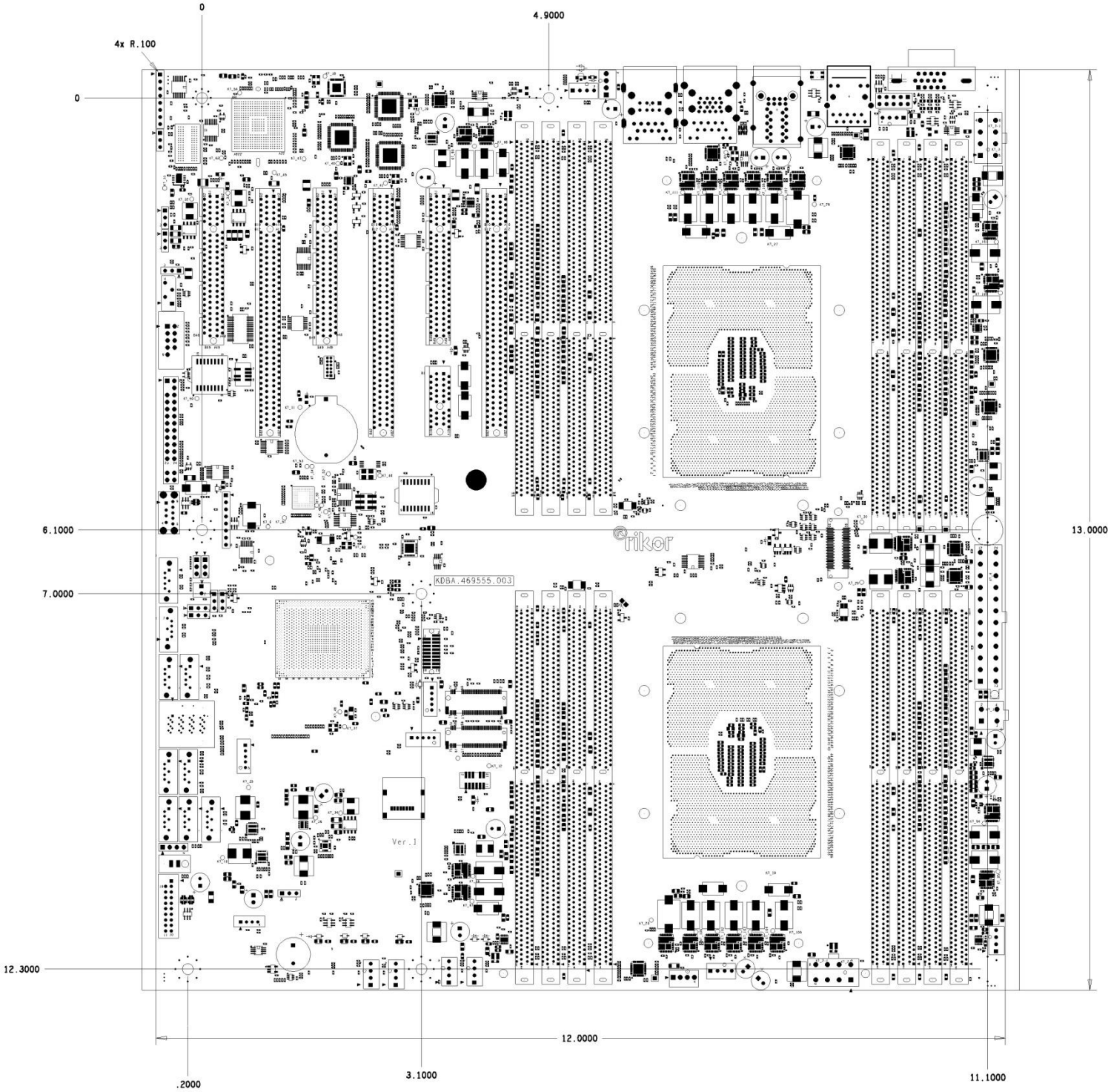


Рисунок 7. Основные компоненты и разъемы

1.4 Обзор архитектуры продукта

Архитектура семейства серверных материнских плат **Rikor® КДБА.469555.003** разработана на основе интегрированных функций и функций семейства процессоров Intel® Xeon® Scalable, набора микросхем Intel® C621, а также контроллера управления платой Aspeed * AST2500 (BMC).

На следующей диаграмме представлен обзор архитектуры серверной материнской платы, показывающий функции и взаимосвязи каждого из основных компонентов подсистемы.

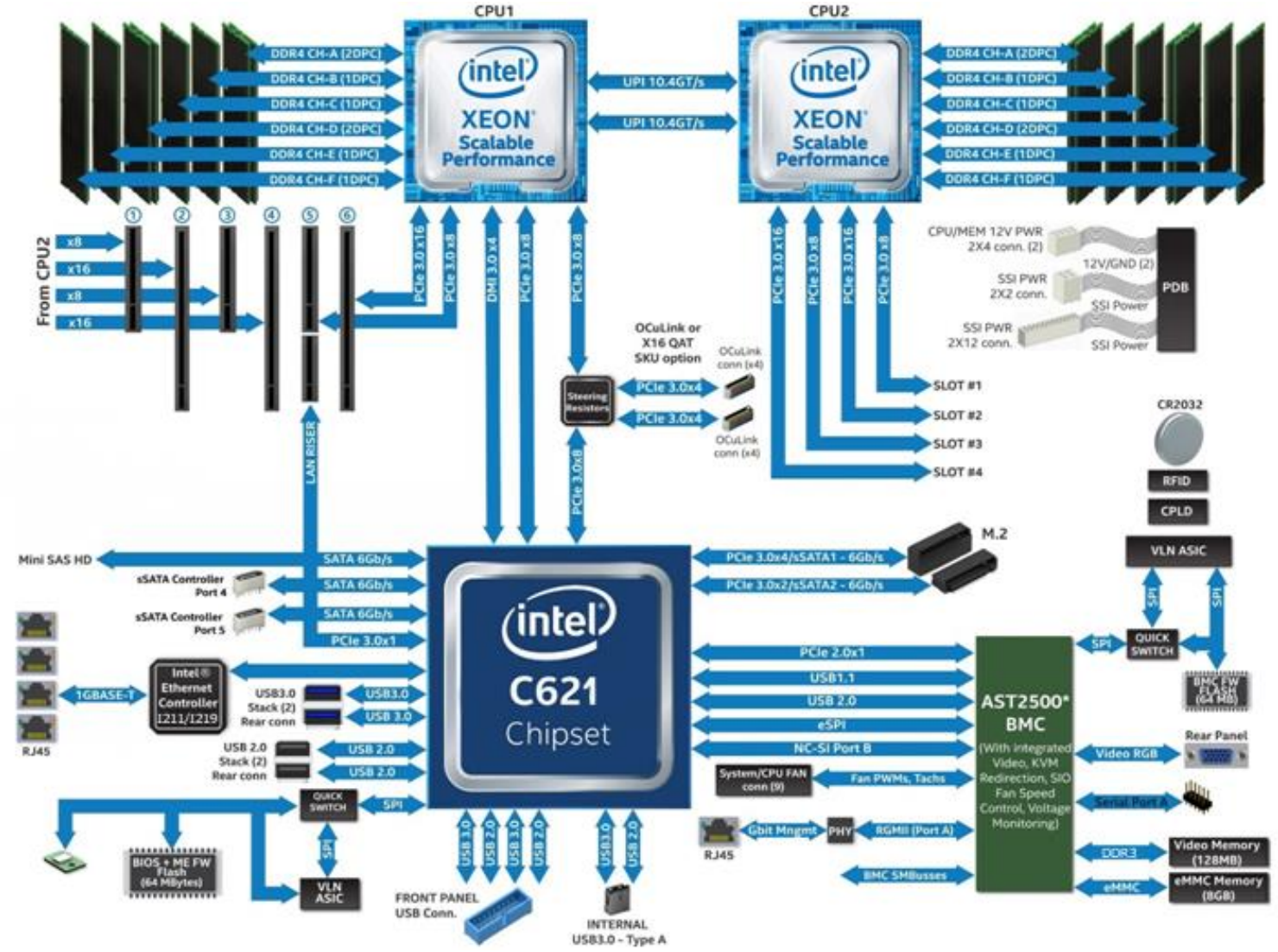


Рисунок 8. Блок-схема серверной материнской платы Rikor® КДБА.469555.003

1.5 Стек системного программного обеспечения

Системное программное обеспечение предварительно программируется компанией Rikor® на серверной плате в процессе сборки платы, что позволяет серверной плате работать при первом включении после интеграции системы.

Актуальные версии встроенного программного обеспечения доступны на сайте https://rikor.com.

Обновления системы могут выполняться в нескольких операционных средах, включая встроенную оболочку Unified Extensible Firmware Interface (UEFI).

В данном разделе особенности и функции BIOS приведены в краткой форме. Для более подробной информации обо всех настройках BIOS смотрите Раздел 13.

1.5.1 Горячие клавиши, поддерживаемые во время самотестирования при включении (POST)

Некоторые горячие клавиши распознаются во время самотестирования при включении (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 во время процесса POST при загрузке системы. Горячие клавиши, поддерживаемые BIOS, больше не распознаются после завершения процесса POST и начала процесса загрузки операционной системы.

В Таблице 2 представлен список горячих клавиш, поддерживаемых BIOS.

Таблица 2. Горячие клавиши POST

Горячая клавиша	Функция
<Esc>	Войти в программу настройки BIOS
<Pause>	Временно остановить POST

1.5.1.1 Логотип POST и диагностические экраны

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

Заводской заставкой по умолчанию является логотип Rikor. Пользовательский экран-заставка OEM может быть установлен в назначенное место флэш-памяти, чтобы заменить заводские настройки по умолчанию.

Если экран-заставка отсутствует в области флэш-памяти BIOS или если тихая загрузка отключена в программе настройки BIOS, во время процедуры POST отображается экран диагностики POST со сводной информацией о конфигурации системы. Экран диагностики POST представляет собой чисто текстовый экран в отличие от экрана с логотипом графического режима.

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

1.5.1.2 Всплывающее меню загрузки BIOS

Спецификация загрузки BIOS (BIOS Boot Specification - BBS) предоставляет всплывающее меню загрузки, которое можно вызвать, нажав клавишу **<Esc>** во время POST. 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 желаемое загрузочное устройство.

Если в программе настройки BIOS установлен пароль администратора, пароль администратора требуется для доступа к всплывающему меню загрузки. Если вводится пароль пользователя, пользователь попадает непосредственно в диспетчер загрузки в утилите настройки BIOS, позволяя системе загружаться только в порядке, предварительно определенном администратором.

1.5.1.3 Вход в программу настройки BIOS

Чтобы войти в программу настройки BIOS с помощью клавиатуры (или эмулированной клавиатуры), нажмите функциональную клавишу **<Esc>** во время загрузки, когда отображается экран с логотипом Rikor или экран диагностики POST.

Примечание. При использовании USB-клавиатуры важно подождать, пока BIOS обнаружит клавиатуру и подаст звуковой сигнал; Пока USB-контроллер не будет инициализирован и клавиатура не будет активирована, нажатия клавиш не будут считываться системой.

При входе в утилиту настройки BIOS сначала отображается главный экран. Однако если во время POST возникает серьезная ошибка, система входит в программу настройки BIOS и отображает экран диспетчера ошибок вместо основного экрана.

1.5.2 Возможность обновления BIOS

Чтобы внести в систему исправления BIOS или новые функции, необходимо заменить текущий установленный образ BIOS на обновленный. Актуальный образ BIOS, а также набор инструментов и инструкций по перепрограммированию доступен на сайте https://rikor.com.

1.5.3 Восстановление BIOS

Если система не может успешно загрузиться в ОС, зависает во время POST или даже зависает и не может начать выполнение POST, может потребоваться выполнить процедуру восстановления BIOS для замены дефектной копии основного BIOS.

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

- Перемычка режима восстановления заставляет BIOS загружаться в режиме восстановления. Расположение перемычки см. на Рисунке 5.
- Если при включении загрузочный блок BIOS обнаруживает, что было выполнено частичное обновление BIOS, BIOS автоматически загружается в режиме восстановления.
- Контроллер управления основной платой (BMC) устанавливает режим восстановления ввода/вывода общего назначения (GPIO) в случае частичного обновления BIOS и тайм-аута FRB2.

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

Примечание: Процедура восстановления приведена здесь для общего ознакомления. Однако в случае противоречия окончательной версией 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 загружается с резервным образом BIOS, находящимся во флэш-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, определенной в инструкциях по обновлению, прилагаемых к пакету обновления системы, загруженному с веб-сайта Rikor. После завершения обновления верните перемычку восстановления в положение по умолчанию и выключите и снова включите систему.

Если BIOS обнаруживает частичное обновление BIOS или BMC устанавливает режим восстановления GPIO, BIOS загружается в режиме восстановления. Разница в том, что BIOS загружается со страницы диспетчера ошибок в программе настройки BIOS. В программе настройки BIOS можно выбрать загрузочное устройство, оболочку или Linux, например, для выполнения процедуры обновления BIOS в среде оболочки или ОС.

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.

2. Поддержка процессора

Серверная материнская плата **Rikor® КДБА.469555.003** включает два разъема для процессоров Socket-P0 LGA3647-0, совместимых с семейством процессоров Intel® Xeon® с максимальной расчетной тепловой мощностью (TDP) 205 Вт. Посетите http://rikor.com/, чтобы получить полный список поддерживаемых процессоров.

Примечание. Процессоры Intel® Xeon® предыдущего поколения не поддерживаются серверными платами Rikor®, описанными в этом документе.

2.1 Модуль радиатора процессора (PHM) и сборка процессорного разъема

Каждый блок процессорного разъема на серверной материнской плате находится в предварительно собранном состоянии и включает в себя заднюю пластину(Backplate), LGA3647-0 процессорный сокет и опорную плату (Bolster plate) в сборе. Иллюстрация на Рисунке 9 идентифицирует каждый из компонентов суб-сборки.

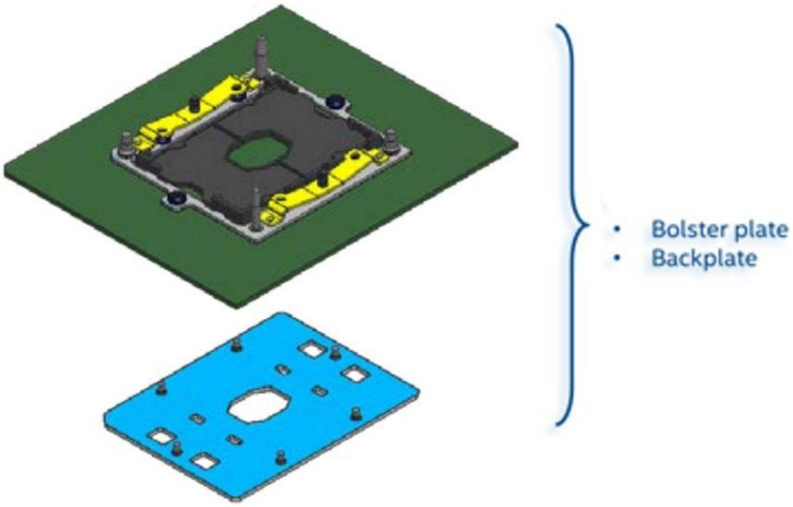


Рисунок 9. Сборка процессорного разъема

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, как показано на Рисунке 10.

Рисунок 10. Узел процессорного гнезда и защитная крышка от пыли

Серверная плата этого поколения представляет концепцию модуля теплоотвода процессора (PHM), показанную на Рисунках 11, 12 и 13.

Для установки процессора необходимо, чтобы процессор был прикреплен к радиатору процессора перед установкой на серверную плату.

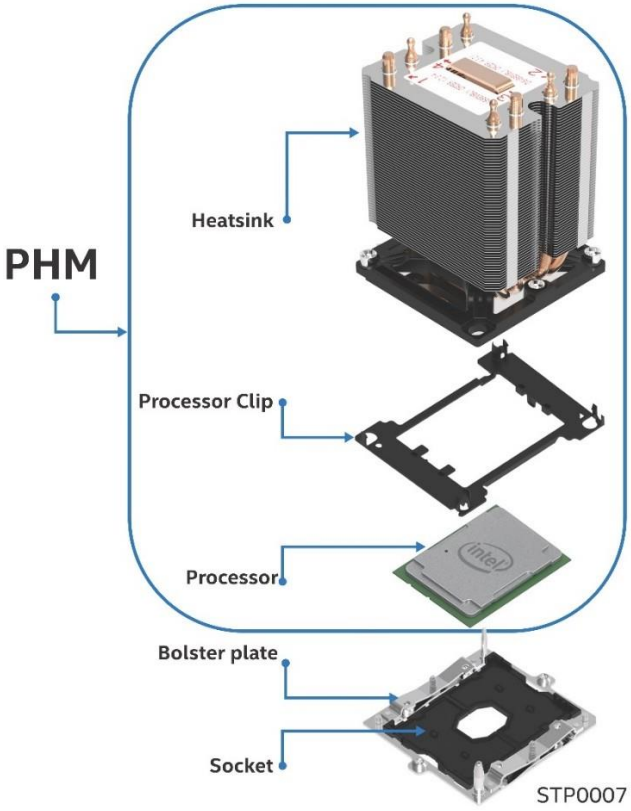


Рисунок 11. Компоненты модуля радиатора процессора (PHM) и справочная схема разъема процессора

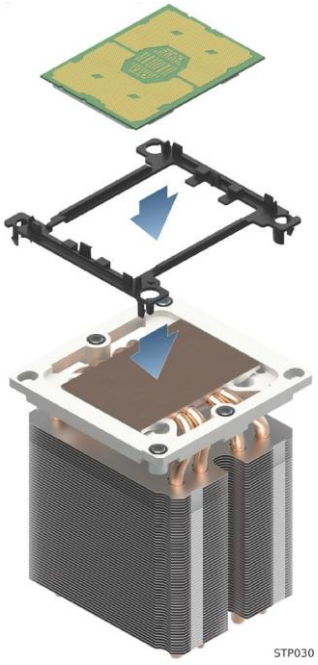


Рисунок 12. Сборочный узел модуля радиатора процессора (PHM)

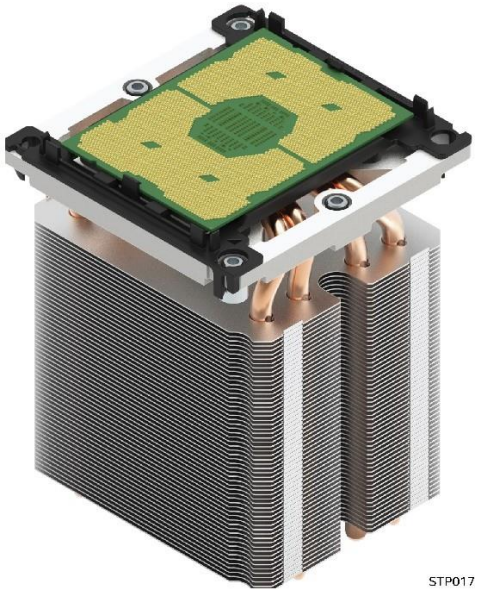


Рисунок 13. Полностью собранный модуль радиатора процессора (PHM)

2.2 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. Серверная плата, описаная в этом документе, разработана для поддержки масштабируемого семейства процессоров Intel® Xeon® мощностью до 205 W включительно.

Примечание об отказе от ответственности: серверные платы Rikor® 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 Rikor® гарантирует, что при совместном использовании серверных строительных блоков Rikor® полностью интегрированная система удовлетворяет предполагаемым тепловым требованиям этих компонентов. Системные интеграторы, решившие не использовать серверные строительные блоки, разработанные Rikor, должны проконсультироваться с техническими описаниями поставщиков и рабочими параметрами, чтобы определить объем воздушного потока, необходимый для их конкретных приложений и условий окружающей среды. Компания Rikor® 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.

2.3 Обзор семейства процессоров Intel® Xeon® Scalable

Серверная материнская плата Rikor® КДБА.469555.003 поддерживает семейство процессоров Intel® Xeon® Scalable 1-го или 2-го поколения, как показано ниже:

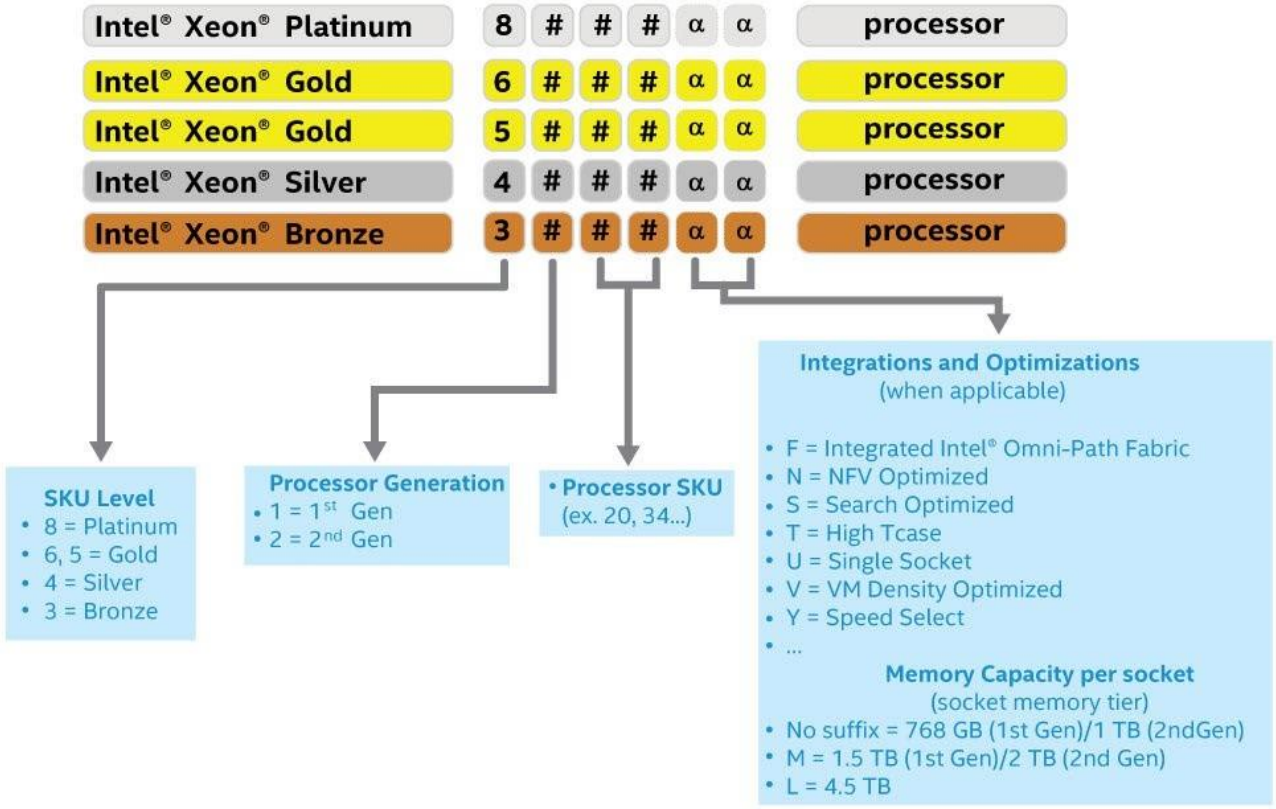


Рисунок 14. Идентификация процессора Intel® Xeon®

Таблица 3. 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 GT/s	10,4 GT/s	10,4 GT/s	9,6 GT/s	9,6 GT/s
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 GB 1,5 ТБ (выбрать SKUs)	768 GB 1,5 ТБ (выбрать SKUs)	768 GB 1,5 ТБ (выбрать SKUs)	768 GB	768 GB
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 4. 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 GT/s	10,4 GT/s	10,4 GT/s	9,6 GT/s	9,6 GT/s
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
Максимальная скорость DDR4 1DPC	2933	2933	2666	2400	2133
Максимальная скорость DDR4 2DPC	2666	2666	2666	2400	2133
Емкость памяти	1 TB 2 TB(выбрать SKUs) 4,5 TB (выбрать SKUs)	1 TB 2 TB(выбрать SKUs) 4,5 TB (выбрать SKUs)	1 TB 2 TB(выбрать SKUs) 4,5 TB (выбрать SKUs)	1 TB	1 TB
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 GT/s
- 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 GB/s
- Поддерживается 6 каналов памяти DDR4 на процессор
- Интерфейс DMI3/PCIe 3.0 с максимальной скоростью передачи 8,0 GT/s

- 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

2.3.1 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/ .

2.3.2 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 кэши, 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.

2.3.3 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).

2.3.4 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.

2.3.5 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*.

2.3.6 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.

2.3.7 Бит отключения выполнения

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.

2.3.8 Технология Intel® Trusted Execution (Intel® TXT) для серверов

Технология Intel® Trusted Execution (Intel® TXT) определяет улучшения на уровне платформы, которые обеспечивают строительные блоки для создания 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.

2.3.9 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.

2.3.10 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 BIOS. Инструкции Intel AES-NI находятся во включенном состоянии, если BIOS явно не отключил их.

2.3.11 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 - это 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 Особенностьх 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 запросить, чтобы вернуть 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. Если есть это предупреждение порог в силе, то Intel ME/Intel NM выдает в предупреждение, когда впускной канал (номер) температура превышает заданное значение. Пороговое значение может быть установлено 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 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 P-состояний процессора и динамического распределения ядер.

- **Основные распределения при загрузке времени**: Ограничение на количество из ядер для OS/Virtual Machine менеджер (VMM) использование путем ограничения как многие ядер являются активными при загрузке времени. После того, как сердечники будут превращены 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 в следующей системе перезагрузки.
- **Распределение ядер во время выполнения**: этот конкретный вариант использования предоставляет пользователю механизм управления мощностью процессора более высокого уровня во время выполнения 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 8.

2.3.12 Intel® Deep Learning Boost

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

2.3.13 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 гарантированной базовой частоты (P1). Эта частота основана на количестве активных ядер в SKU 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.

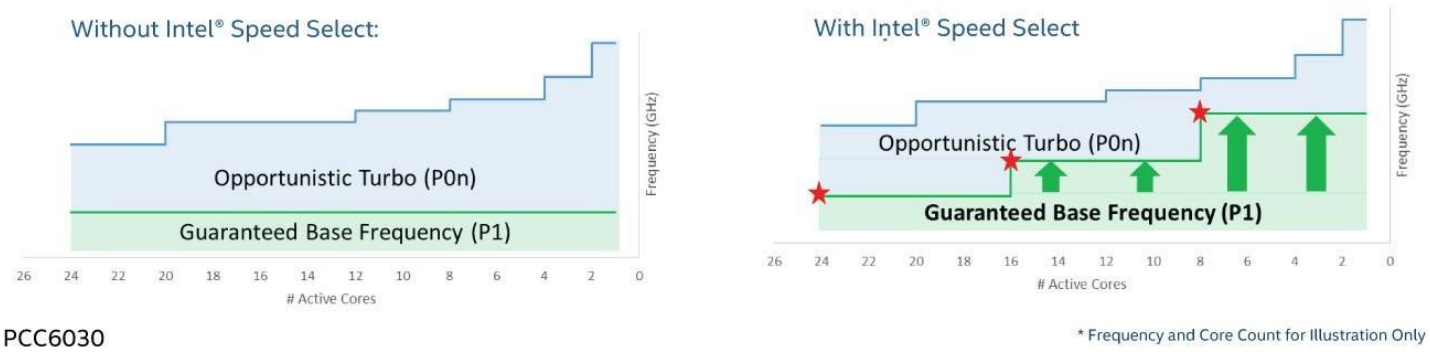


Рисунок 15. Сравнение технологии Intel® Speed Select

2.3.14 Технология Intel® Resource Director

Технология Intel® Resource Director, доступная в семействе процессоров Intel® Xeon® 2-го поколения, снижает конкуренцию за выполнение, 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 кэша (CMT):** отслеживает использование LLC (кэш L3) каждым программным потоком с помощью идентификатора мониторинга ресурсов (RMID).
- **Код данные приоритезация (CPD):** обеспечивает в возможность для отдельного кода из данных в ООО с использованием масок.
- **Память Пропускная способность мониторинга (МБМ):** дает OS/VMM в способности от назначения RMID для программных потоков и читать использование пропускной способности памяти для данного RMID.

- **Распределение пропускной способности памяти (MAD):** MBA - это новая функция, представленная в семействе Scalable процессоров Intel® Xeon® 2-го поколения, которая позволяет программному обеспечению контролировать объем пропускной способности памяти, который поток или ядро может использовать в зависимости от кредитов.

2.4 Правила установки процессора

Примечание. Серверная плата может поддерживать двухпроцессорные конфигурации, состоящие из разных процессоров, отвечающих определенным критериям; однако Rikor® не проводит проверочные испытания этой конфигурации. Кроме того, Rikor® не гарантирует надежную 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 Rikor® 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 8. Блок-схема семейства серверных плат Rikor® КДБА.469555.003.

Если установлено два процессора, применяются следующие правила заполнения:

- Оба процессора должны иметь одинаковое количество ядер.
- Оба процессора должны иметь одинаковые размеры кэша всех уровней кэш-памяти 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 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.

2.5 Сводка ошибок инициализации процессора

В Таблице 5 описаны условия смешанного процессора и рекомендуемые действия для всех серверных плат Intel® и серверных систем Intel®, созданных 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 загрузки, POST останавливается и отображения на 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 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 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.

- **Крупная (Major)**: сообщение об ошибке отображается на экране диспетчера ошибки, и ошибка регистрируется в журнале событий. Если в BIOS включена опция «Пауза после ошибки», для продолжения загрузки системы требуется вмешательство оператора. Если параметр настройки BIOS «Пауза при ошибке POST» отключен, система продолжит загрузку.
- **Незначительная (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 ухудшенном состоянии. Пользователь может захотеть заменить ошибочный блок. Параметр «Пауза при ошибке POST» в настройках BIOS не влияет на эту ошибку.

Таблица 5. Сводка ошибок смешанных конфигураций процессоров

Ошибка	Важность	Действия системы при обнаружении BIOS состояния ошибки
Семейство процессоров не идентично	Фатальная	• Останавливается при коде POST 0xE6. • Останавливается тремя длинными и одним коротким звуковыми сигналами. • 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. • Дисплеи 0196: Процессор модель несоответствие обнаружено сообщения в к ошибке менеджера. • Выполняет действия при фатальной ошибке (см. выше) и не загружается, пока неисправность не будет устранена.
Ядра/потоки процессора не идентичны	Фатальная	• Останавливается при коде POST 0xE5. • Останавливается тремя длинными и одним коротким звуковыми сигналами. • Выполняет действия при фатальной ошибке (см. выше) и не загружается, пока неисправность не будет устранена.
Кэш процессора или домашний агент не идентичны	Фатальная	• Останавливается при коде POST 0xE5. • Останавливается тремя длинными и одним коротким звуковыми сигналами. • 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 - это не состояние 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 желтым цветом. • Не отключает процессор. • Дисплеи 0197: процессор скорость неспособная к синхронизировать сообщения в с менеджером ошибок. • Выполняет действия при фатальной ошибке (см. выше) и не загружается до тех пор, пока неисправность не будет устранена.
Частоты канала Intel® UPI Link не идентичны	Фатальная	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 - это не состояние ошибки. • 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 желтым цветом. • Не отключает процессор. • Дисплеи 0195: Процессор Intel (R) UPII ссылка частота неспособная для синхронизации сообщения в менеджере ошибок.

		• 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 816x: Процессор 0x не может применить сообщение об обновлении микрокода в диспетчере ошибок или на экране. • Принимает меры по устранению серьезной ошибки. Система может продолжать загружаться в ухудшенном состоянии, в зависимости от настройки «POST Error Pause» или может остановиться с кодом ошибки POST в диспетчере ошибок, ожидая вмешательства оператора.
Отсутствует обновление микрокода процессора	Незначительная	• Регистрирует код ошибки POST в SEL. • Дисплеи 818x: процессор 0x микрокод обновление не найдено сообщение в с менеджером ошибки или на экране. • Система продолжает загружаться в ухудшенном состоянии независимо от параметра «Пауза при ошибке POST» в настройке.

3. Поддержка PCI Express * (PCIe *)

Интерфейс PCI Express * (PCIe *) семейства продуктов серверной материнской платы Rikor® КДБА.469555.003 полностью совместим с *базовой спецификацией PCI Express* версии *3.0 и* поддерживает следующие скорости передачи данных PCIe: Gen 3.0 (8.0 GT/s), Gen 2.0 (5.0 GT/c) и Gen 1.0 (2,5 GT/s).

Для конкретных функций платы и функций, поддерживаемых с помощью в PCIe подсистемы, см. Раздел 5.1.

Таблица 6 показывает маршрутизацию информации PCIe портов от каждого процессора.

Таблица 6. маршрутизация портов CPU - PCIe *

ЦП 1		**ЦП 2**	
Порты PCI	Бортовое устройство	**Порты PCI**	Бортовое устройство
Порт DMI 3 - x4	Чипсет	**Порт DMI 3 - x4**	Не используемый
Порт 1A - x4	Не используется	**Порт 1A - x4**	Слот #2
Порт 1B - x4	Не используется	**порта 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

3.1 Перечисление и распределение PCIe *

BIOS назначает номера шины PCI в иерархии «сначала в глубину» 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.

4. Поддержка памяти

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

4.1 Архитектура подсистемы памяти

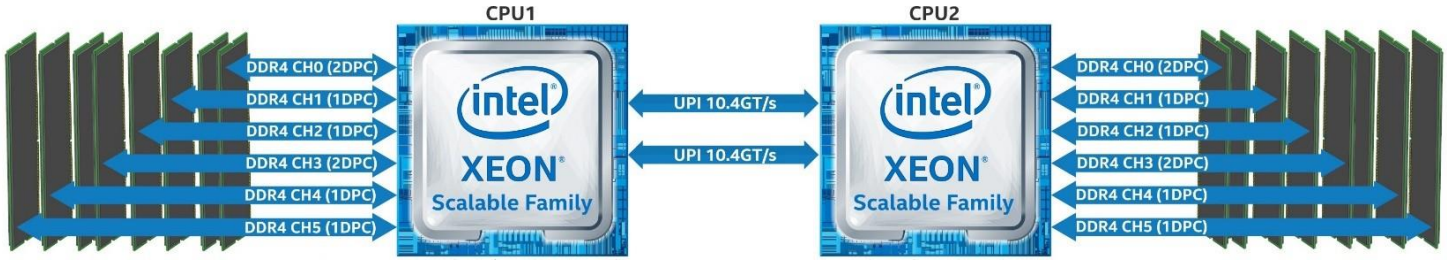


Рисунок 16. Архитектура подсистемы памяти

Примечание. Семейство серверных плат Rikor® КДБА.469555.003 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 семействе серверных плат Rikor® КДБА.469555.003 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 (2-1-1 топология).

Серверная 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).

4.2 Поддерживаемая память

В следующих таблицах перечислены подробные инструкции по поддержке DIMM:

Таблица 7. Рекомендации по поддержке традиционных модулей памяти DIMM DDR4 SDRAM масштабируемого семейства процессоров Intel® Xeon® 1-го поколения

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

Таблица 8. Рекомендации по поддержке традиционных модулей памяти DIMM DDR4 SDRAM масштабируемого семейства процессоров Intel® Xeon® 2-го поколения

Тип	Ранги на DIMM и ширину данных	Емкость DIMM (GB)			Максимальная скорость (MT/s); Напряжение (V); 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 GB [1]	8 GB	16 GB	1,2 V	1,2 V	1,2 V
RDIMM	SRx8	4GB	8 GB	16 GB	2933	2933	2666
	SRx4	8 GB	16 GB	32 GB			
	DRx8	8 GB	16 GB	32 GB			
	DRx4	16 GB	32 GB	64 GB			
RDIMM 3DS	QRx4	Нет данных	2H-64 GB	2H-128 GB			
	8Rx4	Нет данных	4H-128 GB	4H-256 GB			
LRDIMM	QRx4	32 GB	64 GB	128 GB			
LRDIMM 3DS	QRx4	Нет данных	2H-64 GB	2H-128 GB			
	8Rx4	Нет данных	4H-128 GB	4H-256 GB			

Таблица 9. Максимальные поддерживаемые скорости традиционных модулей памяти SDRAM DIMM по уровням SKU в MT/s (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	2933 [2]	2933 [2]	2666	2400	2133

Пояснения:

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

4.3 Общие правила поддержки памяти

Примечание. Хотя смешанные конфигурации DIMM могут работать, Rikor поддерживает и выполняет проверку платформы только в системах, в которых установлены идентичные модули DIMM.

Каждый установленный процессор имеет шесть каналов памяти. В семействе серверных плат Rikor® КДБА.469555.003 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 удаленного от процессора, в подходе «до самого конца». Кроме того, при заполнении четырехрангового модуля DIMM одноранговым или двухранговым модулем 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 процессорами; однако платформа страдает от снижения производительности и задержек.

Разъемы для процессоров являются автономными и автономными. Тем не менее, все подсистемы памяти поддержки (например, памяти RAS или ошибки управления) в в BIOS настройки утилиты будут применены обычно через процессорных сокетов.

В семействе серверных плат Rikor® КДБА.469555.003 предусмотрено всего 16 разъемов DIMM - 1 разъем DDR4 DIMM на канал памяти на четырех каналах и 2 разъема на двух каналах (топология 2-1-1). Номенклатура слотов памяти подробно представлена на Рисунке 17.

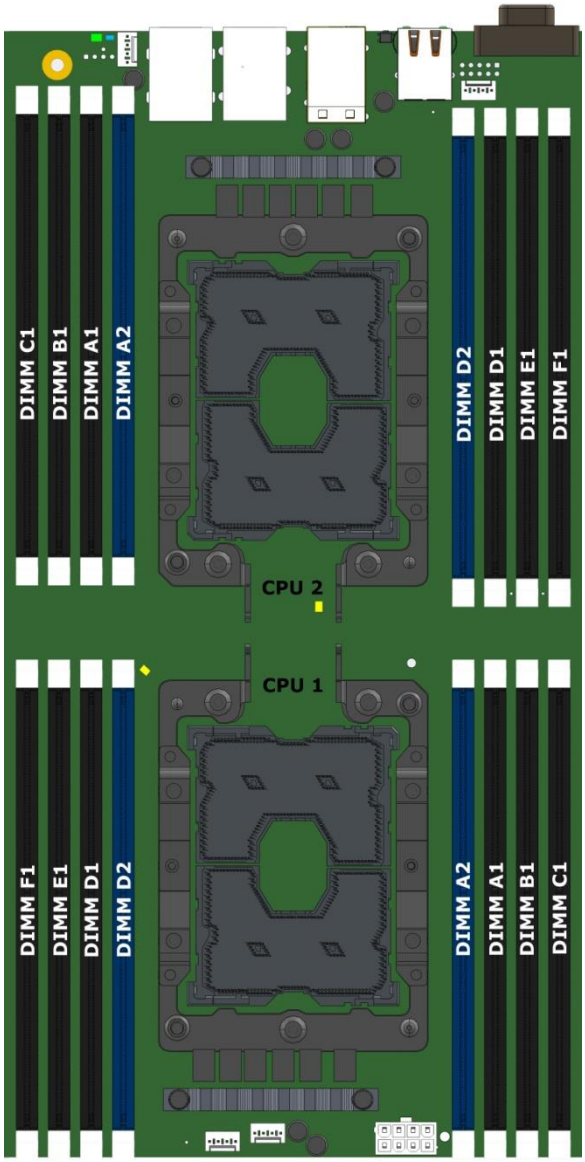


Рисунок 17. Расположение разъемов памяти для серверных плат Rikor® КДБА.469555.003

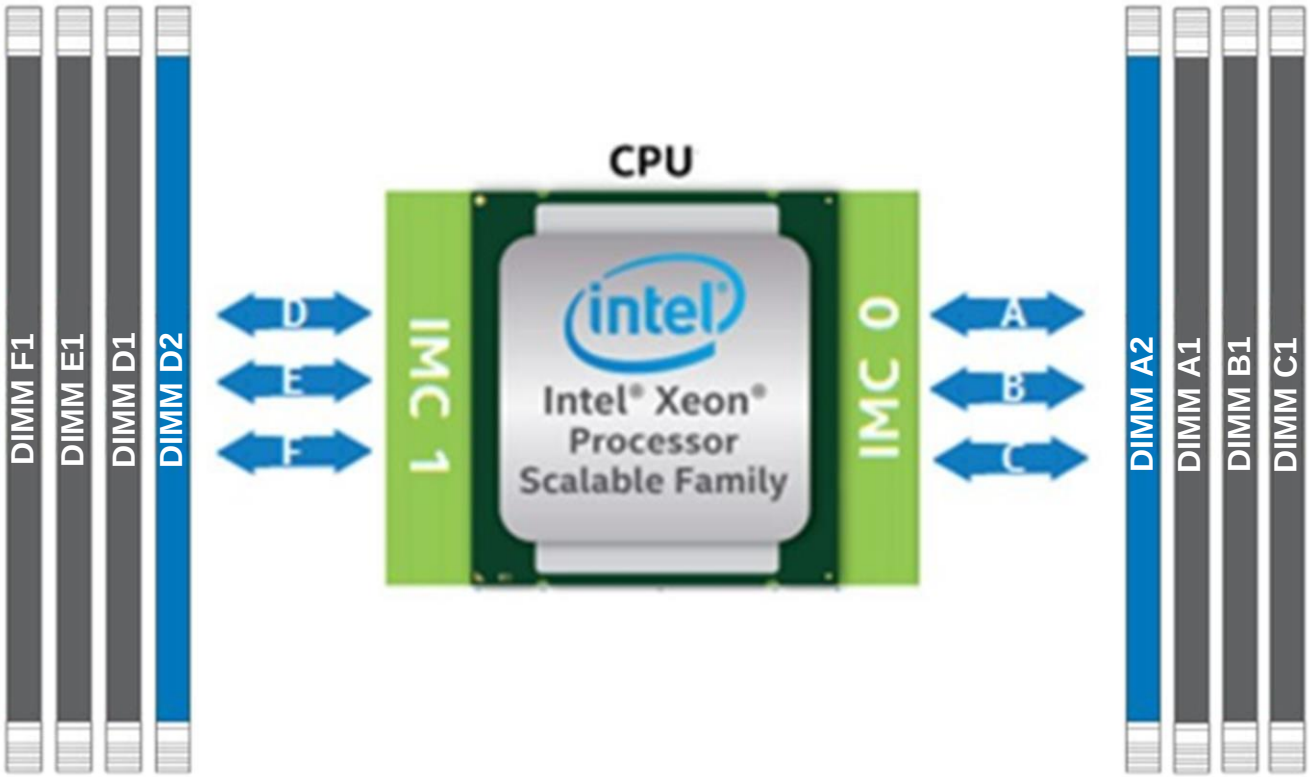
Требования к заполнению модулей DIMM перечислены ниже.

- Для нескольких модулей DIMM на канал:
  - Для RDIMM, LRDIMM, 3DS RDIMM, или 3DS LRDIMM, всегда заселить DIMMs с более высокой электрической нагрузки в первом слоте канала (синий слот), а затем второй слот.
- Когда только один модуль DIMM будет использоваться в в каналах A или D, она должна быть заселена в с СИНИЙ DIMM слот.
- На любом канале можно использовать максимум 8 логических рангов, а также максимум 10 физических рангов, загруженных на канал.
- Смешивание из DDR4 DIMM Типы (RDIMM, LRDIMM, 3DS-RDIMM, 3DS-LRDIMM, NVDIMM) в пределах канала или 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 Ранг Умножение Режим и Direct Map Mode должен не быть смешанными внутри или через процессорные разъемы. Это критическая ошибка при инициализации памяти.
- Для того чтобы установить 3 QR LRDIMMs на том же канале, то они должны работать с Rank Умножение в PM = 2. Это будет делать каждый LRDIMM появляются в виде DR DIMM с рангах дважды в целом.
- Режимы RAS Rank Sparing и Mirroring в этой BIOS являются взаимоисключающими. Можно выбрать только один режим работы, и он будет применяться ко всей системе.

- Если был настроен режим RAS, и объем памяти не поддерживает 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 заполняются памятью отвечают требования по имеющим по меньшей мере 2 SR или DR модуль DIMM установлен, или по крайней мере один QR - DIMM установлен, на каждый заполненном канале.
- Зеркальные режимы требуют, что для любого канала пары, которая является заселенной с памятью, память население на обоих каналах паров должно быть одинакового размером. См. подробные сведения о номенклатуре сопряжения в BIOS EPS для масштабируемого семейства процессоров Intel Xeon Scalable.

4.3.1 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 канала памяти.



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.
  - **От 1 DIMM до 3 DIMM конфигурации** - модули DIMM должны быть установлены в DIMM Slot1 (черные **слоты**) каналов с **A** по **C**
  - **4 DIMM конфигурации** - модули DIMM должны быть установлены в DIMM Slot1 (**черные слоты**) каналов **A, B, D** и **E**
  - **5 DIMM конфигурации** - **НЕ рекомендуются**. Это несбалансированная конфигурация, которая будет давать производительность меньше оптимальной
  - **6 DIMM конфигурации** - модули DIMM должны быть установлены в DIMM Slot1 (**черные слоты**) всех каналов
  - **7 DIMM конфигурации** - **НЕ рекомендуются**. Это несбалансированная конфигурация, которая будет давать производительность меньше оптимальной
  - **8 DIMM конфигурации** - модули DIMM должны быть установлены во все DIMM слоты

4.4 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, как указано в Таблице 10.

Таблица 10. Особенности RAS памяти

Особенность RASM	Описание	Стандарт	Продвинутый
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).		√
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 разъема. Dynamic (без перезагрузки) отказоустойчивого для тех зеркальных модулей DIMM прозрачен для ОС и приложений.	√	√
	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.		√
Щадящий Ранг Уровня экономии Памяти	Динамическое переключение вышедших из строя рядов в резервные ряды, расположенные за теми же рядами контроллера памяти DDR.	√	√
Многоранговый Уровень экономии памяти	В многоранговом режиме до двух рангов из восьми 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 емкость в DDR4 DRAM, которую можно использовать для замены неисправные области ячеек, обнаруженные во время загрузки системы.	√	√

Примечание. Функции RAS памяти могут поддерживаться не на всех SKU типах процессоров.

4.4.1 Правила для наборов DIMM и настройки BIOS для RAS памяти

При включении функций RAS применяются следующие правила:

- Параметры резервирования памяти и 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 и конфигурация памяти не может поддерживать его во время загрузки, система возвращается в режим "независимого канала", а также регистрирует и отображает ошибки.
- Режим Rank Sparing возможен только тогда, когда все каналы, заполненные памятью удовлетворяют требованию, иметь по меньшей мере два SR или DR DIMMs установленными или по крайней мере один QR - DIMM установленный в каждом заполненном канале.
- Режим зеркалирования памяти требует, чтобы для любого канала пары, в которой установлена память, объем памяти на обоих каналах пары был одинаковым.

5. Системный ввод/вывод

5.1 Поддержка дополнительных карт PCIe *

Серверная 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)

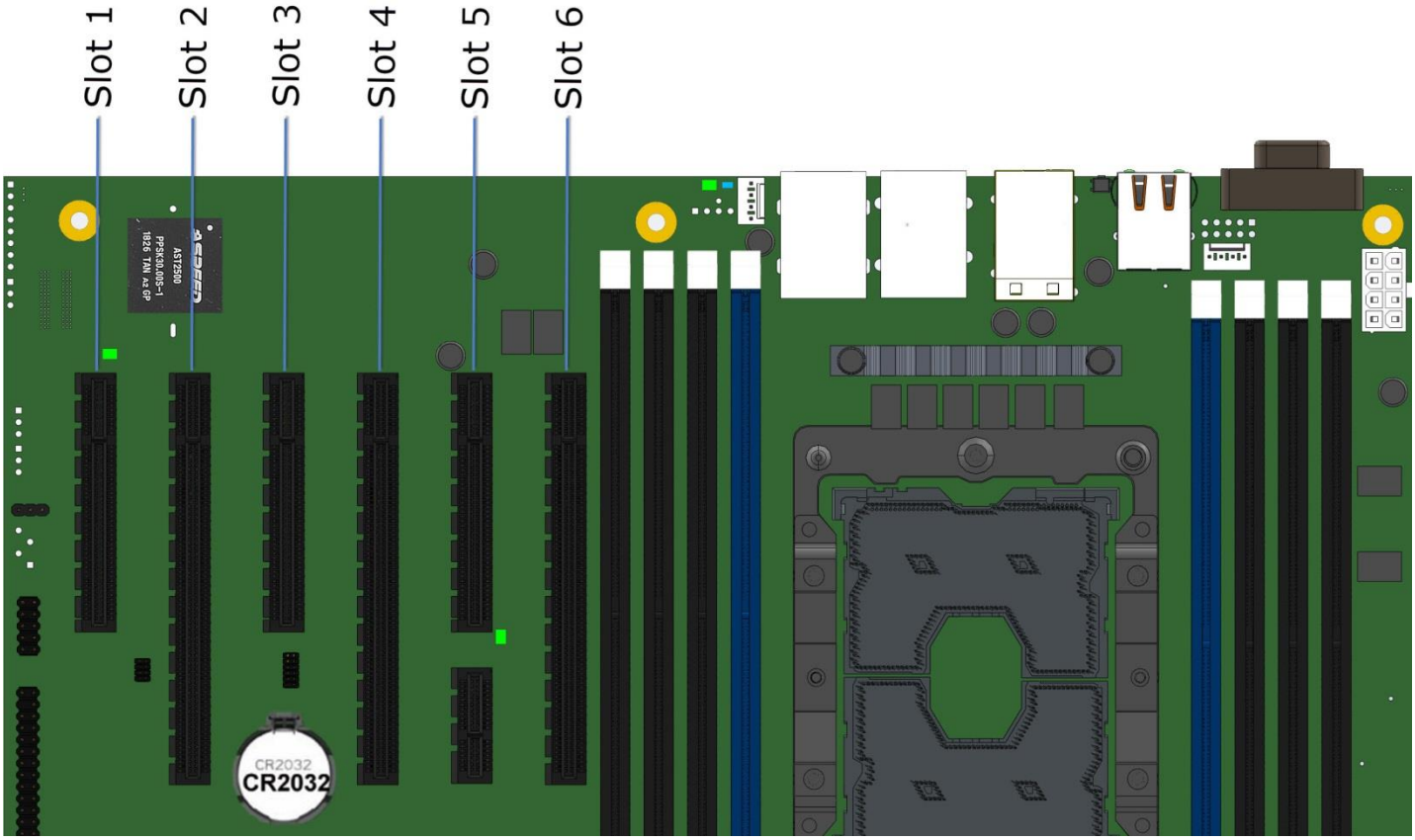


Рисунок 18. Слоты PCIe *

Такая конфигурация слотов позволяет устанавливать до 3 дополнительных карт двойной ширины и полной длины. Для этого случая также предоставляется дополнительное дополнительное питание. См. Раздел 10 для получения подробной информации о дополнительных вариантах питания.

5.1.1 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 назначенных разъемов переходной платы может поддерживать переходные платы со следующими конфигурациями разъемов для плат расширения PCIe *:

- переходная плата x16 с двумя слотами x4 PCIe *
- x16 стояка 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 *

5.2 Встроенная подсистема хранения данных

Семейство серверных плат Rikor® КДБА.469555.003 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) опционы
  - Intel® VROC (SATA RAID) 6.0
  - Intel® Embedded Сервер RAID технология 2 v1.60 для SATA

The следующих секциях дается обзор по каждой опции.

5.2.1 Поддержка устройств хранения M.2

Серверная 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 конфигурациях.

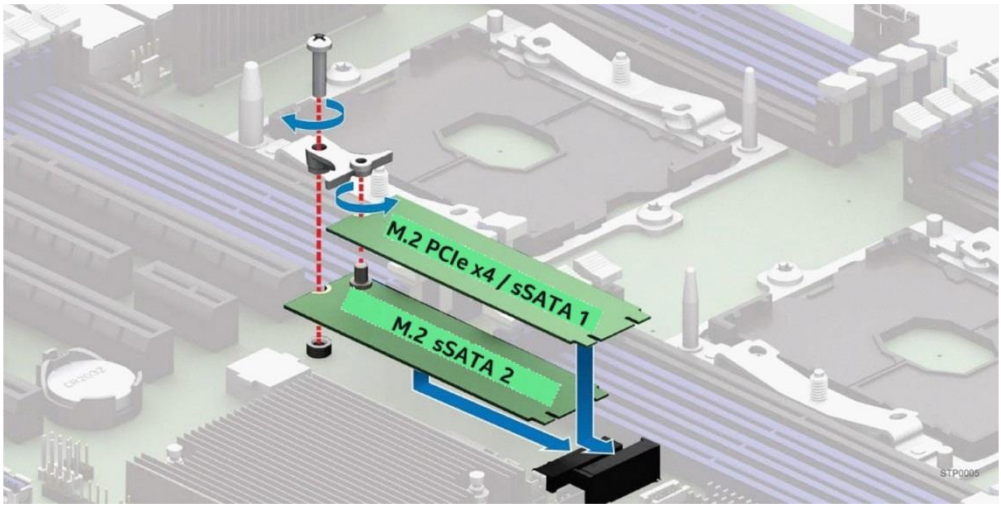


Рисунок 19. Разъемы M.2

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 9.3.2 для получения подробной информации о распиновке разъема M.2.

Примечание. Устройства PCIe* M.2 будут обнаружены и видны BIOS только когда для режима загрузки установлено значение uEFI. Устройства SATA M.2 обнаруживаются и видны BIOS как в режиме загрузки legacy, так и в uEFI.

5.2.1.1 Поддержка встроенного RAID

Поддержка RAID из встроенных вариантов RAID для установленных на серверной материнской плате 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 серверной материнской плате.

Примечание. Поддержка RAID для твердотельных накопителей NVMe * с использованием Intel® VROC (VMD NVMe RAID) требует, чтобы полосы шины PCIe маршрутизировались непосредственно от ЦП. На этой серверной 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.

- И 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.

Примечание. 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 уровня MDRAID в Linux *.

5.2.3 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 *.

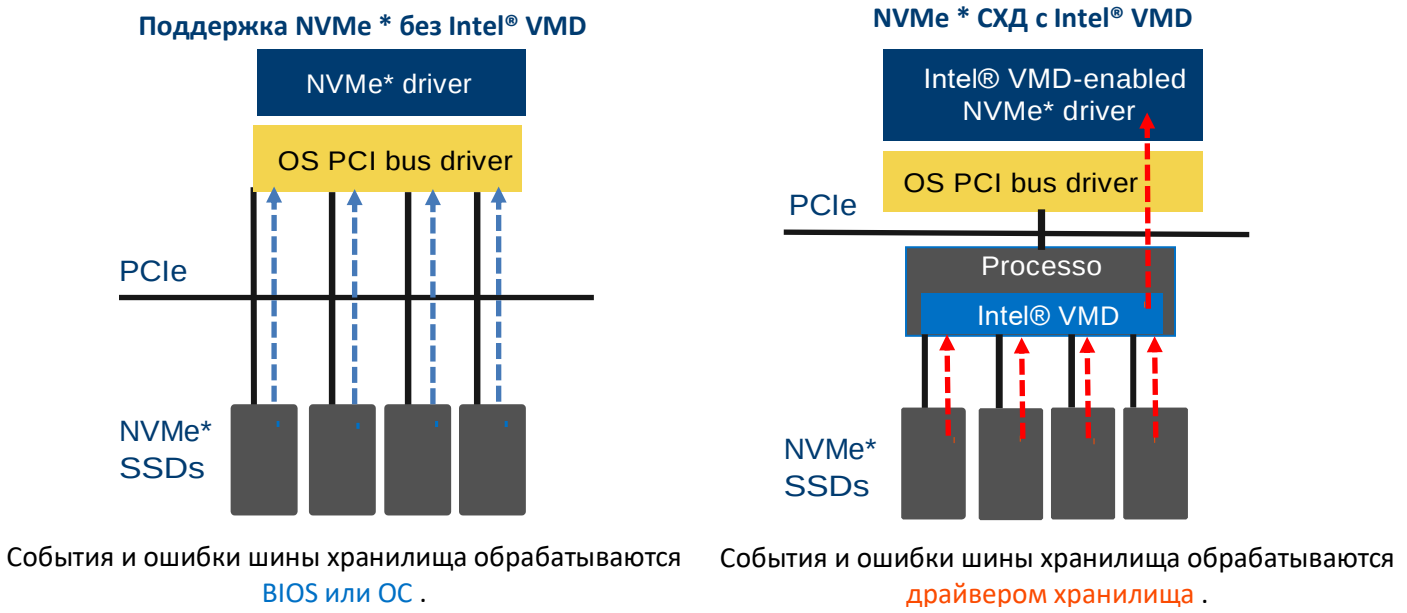


Рисунок 20. Устройство управления томами Intel® (Intel® VMD) для твердотельных накопителей NVMe *

Intel® VMD обрабатывает физическое управление твердотельными накопителями NVMe как отдельную функцию, но может быть расширена, если включены опции поддержки Intel® VROC для реализации систем хранения на основе RAID. См. Раздел 5.2.4 для получения дополнительной информации.

Ниже приведен список функций технологии Intel® VMD:

- Аппаратное обеспечение интегрировано в корневой комплекс процессора PCIe * .
- Целые деревья PCIe * отображаются в свои собственные адресные пространства (домены).
- 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 пути ввода-вывода.
- Может загружать дополнительный драйвер дочернего устройства, поддерживающий Intel VMD.
- Поддержка горячей замены - массив твердотельных накопителей PCIe * с возможностью горячей замены.
- Поддержка для PCIe * SSD - накопителей и переключает только (без сетевого интерфейса контроллеров (NIC), графические карты и т.д.)
- Максимум 128 номеров шины PCIe * на домен.
- Поддержка только MCTP через SMBus.
- Поддержка только MMIO (без ввода-вывода с отображением портов).
- Не поддерживает NTB, Quick Data Tech, Intel® Omni-Path Architecture или 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) (Рисунок 20).
- Когда Intel VMD включен, BIOS не перечисляет устройства, находящиеся за Intel VMD. Драйвер Intel с поддержкой VMD отвечает за перечисление 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.

5.2.4 Intel® VROC (VMD NVMe RAID) 6.0

Intel® VROC (VMD NVMe RAID) обеспечивает загрузку NVMe на RAID и управление томами.

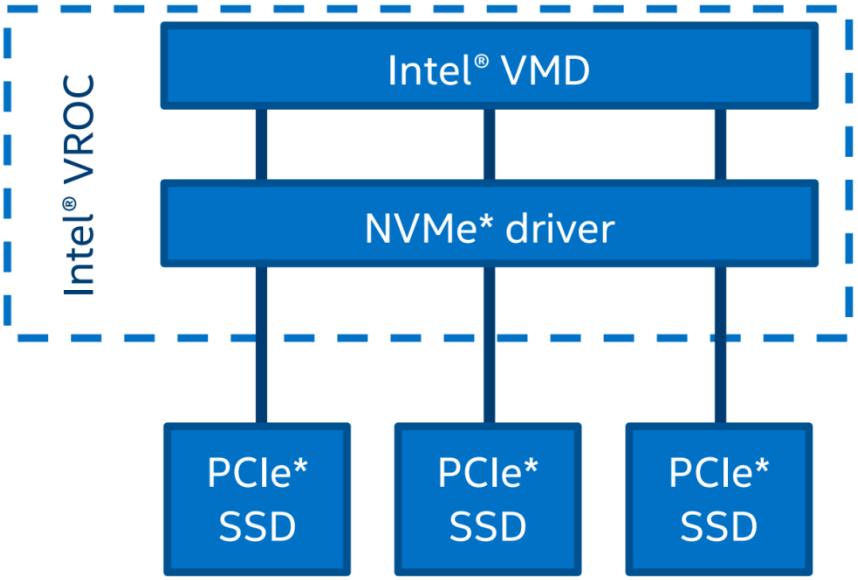


Рисунок 21. Обзор базовой архитектуры Intel® VROC

Intel® VROC (VMD NVMe RAID) поддерживает следующее:

- Процессор ввода-вывода с контроллером (ROC) и DRAM.
- Нет необходимости в резервном аккумуляторе/резервном устройстве RAID, не требующем обслуживания

- Защищенный кеш с обратной записью - программное и аппаратное обеспечение, позволяющее восстановить после двойной ошибки.
- Изолированные устройства хранения от ОС для обработки ошибок.
- Защищены данные R5 от сбоя ОС.
- Загрузка с RAID - томов, основанных на NVMe твердотельных накопителей в виде единого Intel VMD домена.
- Горячее подключение NVMe SSD и неожиданное удаление на линиях процессора PCIe*.
- Светодиодное управление подключенным хранилищем CPU PCIe.
- Управление RAID/хранилищем 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 дополнительного ключа обновления на серверной материнской плате, как показано на Рисунке 22. В Таблице 11 указаны доступные варианты ключа обновления Intel VROC.

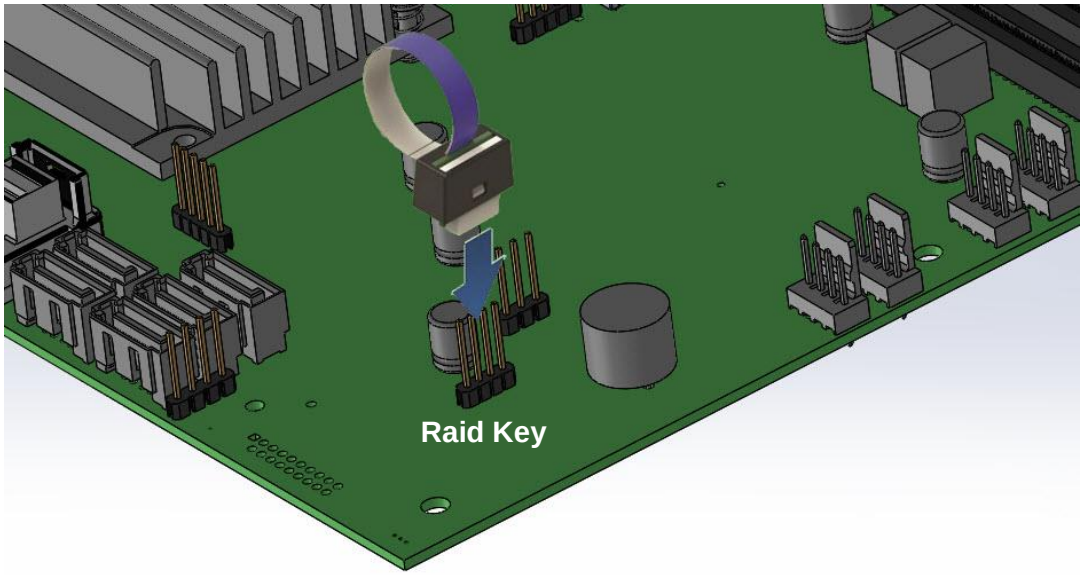


Рисунок 22. Ключ обновления Intel® VROC

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 11. 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 - высокая производительность.	√	√
Загрузка с тома RAID	√	√
Поддержка SSD сторонних производителей	√	√
RAID 0/1/10	√	√
RAID 0/1/5/10	-	√
Отверстие для записи RAID закрыто (замена BBU)	-	√
Горячая замена/неожиданное удаление (Только форм-фактор твердотельного накопителя 2,5 дюйма; форм-фактор карты расширения не поддерживается)	√	√
Управление светодиодами корпуса	√	√

Примечание. Ключи обновления Intel® VROC, указанные в Таблице 11, используются только для твердотельных накопителей PCIe * NVMe *. Информацию о поддержке SATA RAID см. в разделе 5.2.6.

5.2.5 Встроенная поддержка SATA

Серверная плата использует два (AHCI) SATA контроллера, встроенные в PCH, идентифицированные, как SATA и sSATA, обеспечивающие для 12 SATA портов скорость 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 для деятельности до четырех SATA 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 портам осуществляется через два белых однопортовых 7-контактных разъема с маркировкой "sSATA-4" и "sSATA-5"

См. раздел 5.2.1 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 12. 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
Поддержка горячей замены [1]	Позволяет обнаруживать устройства без подачи питания, а также подключать и отключать устройства без предварительного уведомления системы.	N/A	Поддерживается
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.	Поддерживается	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 и каналом	Возможность хост-контроллера или устройства запрашивать частичные и спящие состояния питания интерфейса.	N/A	Поддерживается
Поэтапное вращение	Позволяет хосту последовательно раскручивать жесткие диски, чтобы предотвратить проблемы с питанием при загрузке.	Поддерживается	Поддерживается
Объединение завершения команд	Уменьшает накладные расходы на прерывание и завершение, позволяя выполнить указанное количество команд и затем генерируя прерывание для обработки команд.	N/A	N/A

[1] Существует риск потери данных при удалении диска, не входящего в отказоустойчивый RAID.

Контроллер SATA и контроллер sSATA можно независимо включать, отключать и настраивать с помощью утилиты настройки BIOS в экране меню «Конфигурация контроллера запоминающего устройства». В следующей таблице указаны поддерживаемые параметры настройки.

Таблица 13. 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

Состояние контроллера SATA	Состояние контроллера sSATA	Поддерживается
Intel® VROC (SATA RAID)	Повышенная	Да
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.

5.2.5.1 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 операции.

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 «Настройка конфигурации контроллера запоминающего устройства».

5.2.6 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) 1,60 основе на LSI * MegaRAID программное обеспечение RAID технологии

С помощью утилиты настройки BIOS <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. Семейство серверных плат Rikor® КДБА.469555.003 включает в себя встроенное хранилище SATA и sSATA. Технология Intel Embedded Server RAID поддерживается только встроенным контроллером SATA.

5.2.6.1 Intel® VROC (SATA RAID) 6.0

Intel® VROC (SATA RAID) 6.0 предлагает несколько вариантов RAID для удовлетворения потребностей данной операционной среды. Поддержка AHCI обеспечивает более высокую производительность и устраняет узкие места на диске, используя преимущества независимых механизмов DMA, которые каждый порт SATA предлагает в наборе микросхем.

- **RAID Level 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 транзакций 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 отказ - устойчивость уровня RAID 1 с производительностью уровня RAID 0. Распределение сегментов RAID уровня 1 позволяет достичь высоких скоростей ввода-вывода 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 два 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.
- Параметр Intel® VROC (SATA RAID) должен быть выбран в настройке BIOS.
- Драйверы Intel® VROC (SATA RAID) должны быть загружены 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, который позволяет пользователю управлять конфигурацией RAID в системе. Его набор функций остается простым, чтобы уменьшить размер до минимума, но 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 тому 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 предоставляется статус томов RAID.

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

Intel® Embedded Server, RAID Technology 2 будет основана на в LSI * MegaRAID программного стека 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 различными дисками оборотов в минуту (RPM), функциональность не влияет.
- **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 обоих производительность и отказоустойчивость. RAID уровня 10 требует четыре жестких диска и обеспечивает емкость двух дисков.

Дополнительно поддержка для RAID уровня 5 может быть включен с в дополнение в виде RAID 5 обновления ключа (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.

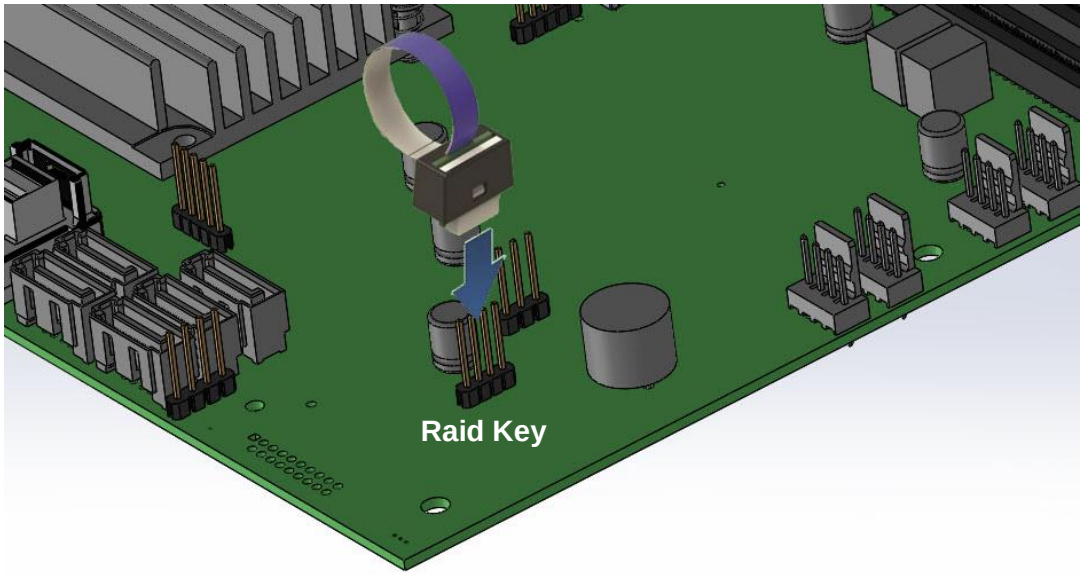


Рисунок 23. Ключ обновления SATA RAID 5

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 два встроенных контроллера AHCI SATA.

Intel Embedded Сервер RAID Technology 2 на этом сервере плате поддерживает более максимум из шести дисков, который является максимальным на борту SATA порт поддержки.

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

5.3 Сетевой интерфейс

Серверная плата Rikor® КДБА.469555.003 оснащена четыремя встроенными портами Ethernet (и 1 порт BMC Ethernet). Кроме того, может быть установлена дополнительная переходная плата LAN для поддержки двух портов SFP +. Все встроенные порты Ethernet управляются контроллером Intel® Ethernet Connection 722. В этом разделе описаны оба интерфейса.

5.3.1 Встроенные порты Ethernet

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

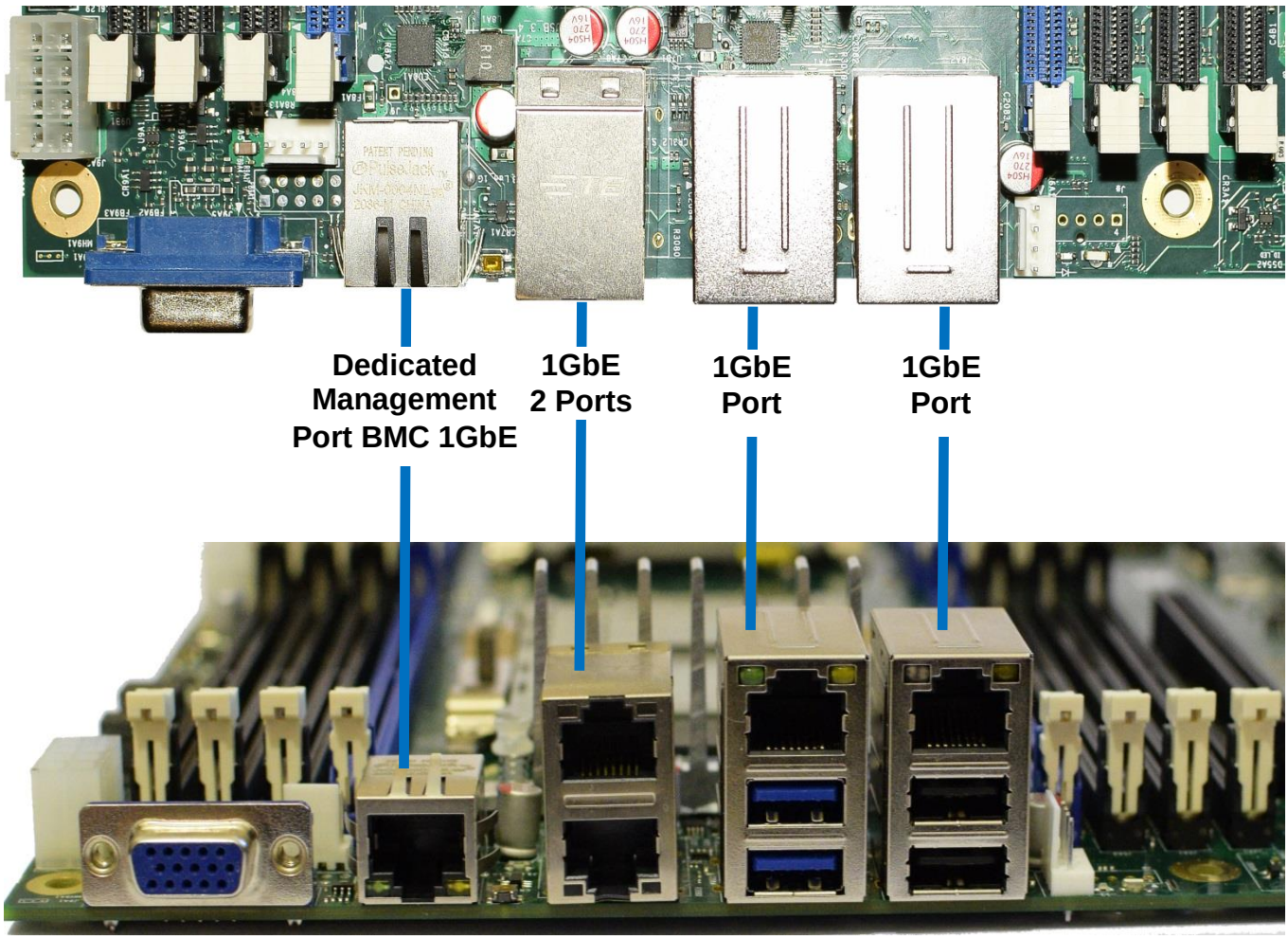


Рисунок 24. Разъемы сетевого интерфейса

Каждый порт Ethernet имеет два светодиода, как показано на Рисунке 25. Светодиод слева от разъема является светодиодом Соединения/Активности(Link/Activity) и указывает на сетевое соединение, когда он включен, и активность передачи/приема, когда мигает. Светодиод справа от разъема показывает скорость соединения, как описано в Таблице 14.

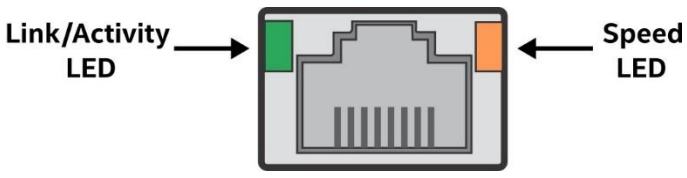


Рисунок 25. Внешний RJ45 сетевой интерфейс контроллера (NIC) порт LED определение

Таблица 14. Бортовое Сетевой интерфейс контроллера (NIC) LED Определение

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)	Твердый янтарь	Поддерживаемая средняя скорость передачи данных (1 Гбит/с).
	Горит зеленым	Самая высокая поддерживаемая скорость передачи данных (10 Гбит/с).

6. Безопасность системы

Серверная 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)

6.1 Настройка параметров безопасности в программе настройки BIOS

Утилита настройки BIOS <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:

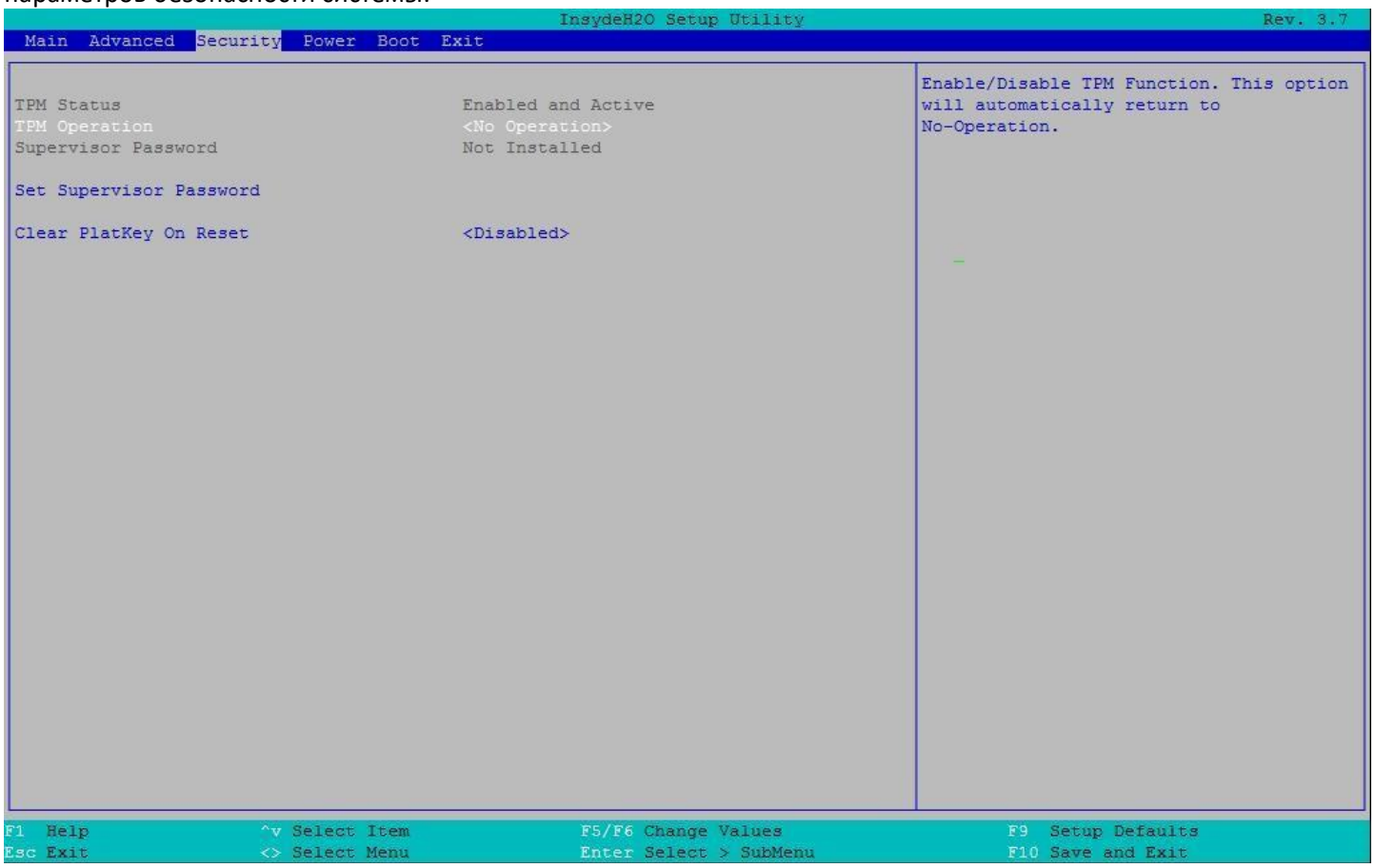


Рисунок 26. Параметры безопасности настройки BIOS

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 Админа
Clear PltKey On Reset *(Очистить PltKey при перезагрузке)*	Отключить / Включить	Включить/Выключить очистку ключа безопасности платформы при перезагрузке

6.2 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 потребовать пароль при включении для загрузки системы. Если в настройке BIOS включена функция «Пароль при включении», BIOS преждевременно останавливается в процессе POST, чтобы запросить пароль перед продолжением.

Установить пароль администратора

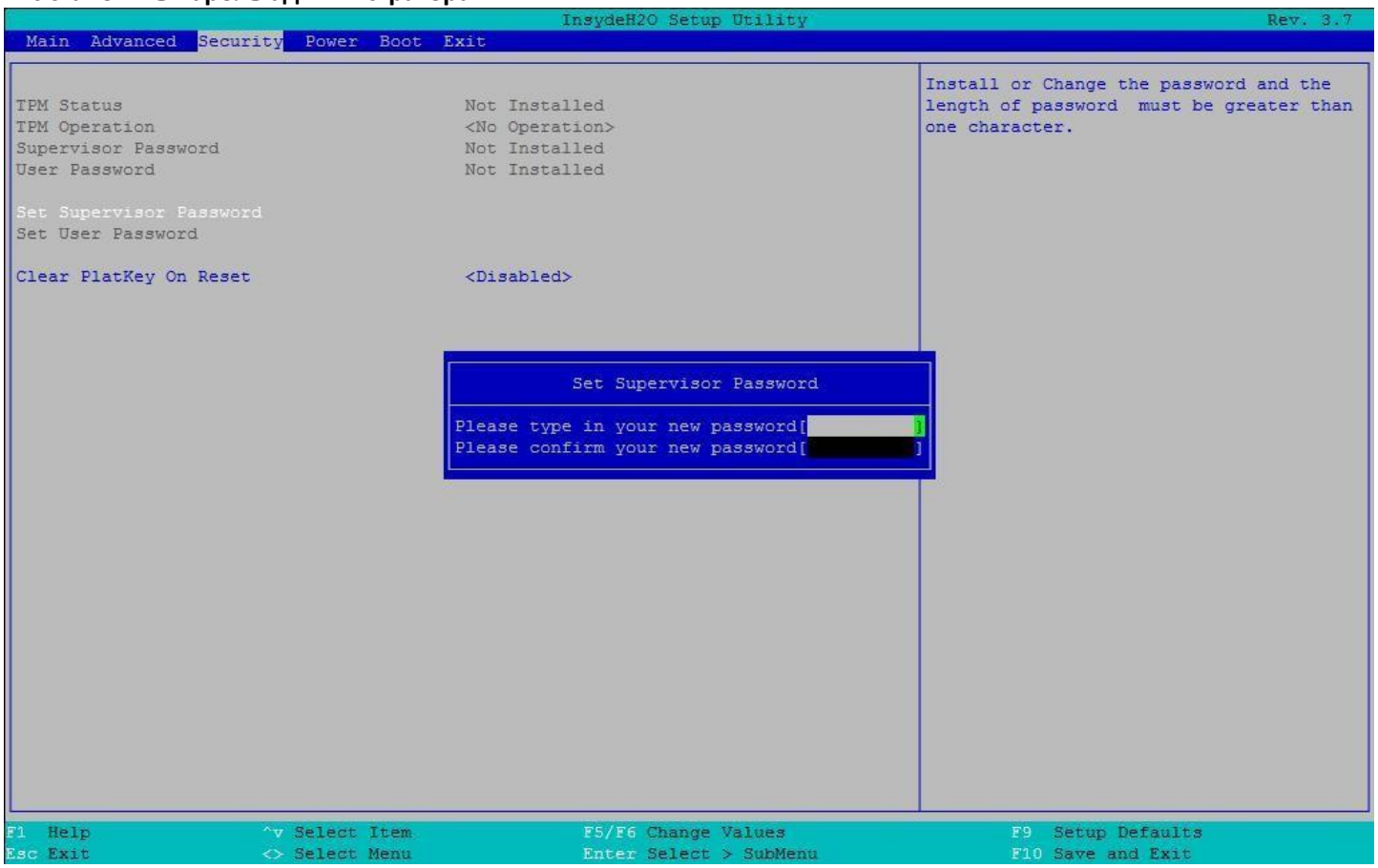


Рисунок 27

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. Сообщение об ошибке отображается, если есть попытка ввести тот же пароль для одного, что и для другого. 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 всплывающее предупреждающее сообщение.

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

При необходимости пароли можно сбросить с помощью перемычки сброса пароля (см. раздел 10.2). Сброс настроек конфигурации BIOS до значений по умолчанию (любым способом) не влияет на пароли администратора или пользователя.

Ввод пароля пользователя позволяет пользователю изменять только системное время и системную дату на главном экране настройки BIOS. Остальные поля можно изменить, только если был введен пароль администратора. Если установлен какой-либо пароль, для входа в программу настройки BIOS требуется пароль.

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 для просмотра только при вводе пароля пользователя, определение пароля пользователя накладывает ограничения на загрузку системы. Для простой загрузки в определенном порядке загрузка пароля не требуется. Однако всплывающее меню загрузки, доступ к которому осуществляется путем ввода **<F6>** во время POST, требует пароль администратора. См. Раздел 1.5.1.2 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, если пользователь или администратор вводит неправильный пароль три раза подряд во время загрузки, 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 SEL, чтобы предупредить авторизованного пользователя или администратора о том, что произошла ошибка доступа по паролю.

6.3 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 защищает процесс запуска системы, обеспечивая защиту от несанкционированного доступа, прежде чем передать управление системой 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 серверной материнской плате и защищено от атак внешнего программного обеспечения и физического кражи.

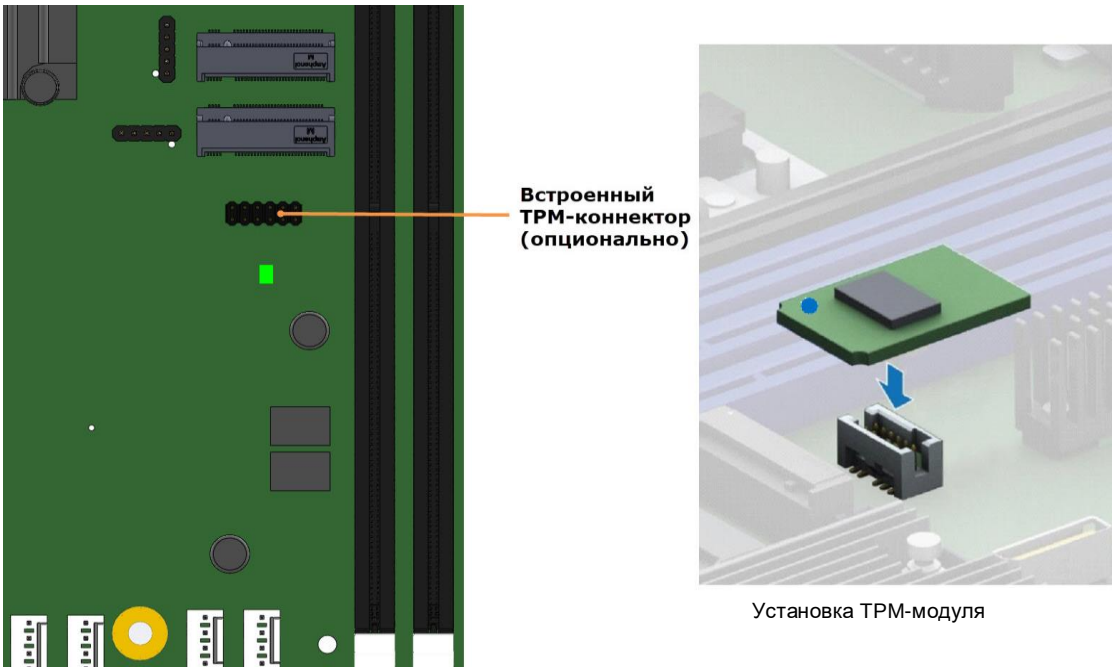


Рисунок 28. Встроенный разъем TPM

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 системы 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 *.)

6.3.1 Безопасность BIOS TPM

В Удовлетворяет поддержка BIOS TPM к *спецификации конкретной реализации TPM PC Client для обычного BIOS,* на *PC Client Конкретные спецификации TPM интерфейса,* и *Microsoft Windows * BitLocker * Требования*. 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 для использования TPM.
- Создает устройство TPM с расширенным интерфейсом конфигурации и питания (ACPI) и методы, позволяющие 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 владения 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*.

6.3.2 Физическое присутствие

Для административных операций с TPM требуется, чтобы оператор указывал владение TPM или 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 и подтверждает команду оператору.
4. BIOS выполняет административную команду TPM, запрещает вход в программу настройки BIOS и загружается непосредственно в операционную систему, которая запросила команду TPM.

6.3.3 Параметры настройки безопасности TPM

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

Настройка BIOS TPM отображает текущее состояние TPM, как описано в Таблице 15. 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 15. 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 отключено	Включенное и деактивированное устройство TPM не выполняет команды, использующие функции TPM. Операции безопасности TPM недоступны, за исключением настройки владения 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 владения TPM. После того, как запрошенная операция настройки BIOS TPM будет выполнена, параметр вернется в состояние **Нет операции**. Параметр **Clear Ownership** TPM в настройке BIOS позволяет оператору очистить ключ владения 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 владения TPM.

Параметры административного управления TPM описаны в Таблице 16.

Таблица 16. 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.
Включи	Включает и активирует TPM.
Выключить	Отключает и деактивирует TPM.
Clear Ownership удаляет TPM	проверка подлинности владения и возвращает TPM к заводским состояниям по умолчанию.

6.4 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 конфиденциальность 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 доступно, 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/ .

7. Управление платформой

Управление платформой поддерживается несколькими аппаратными и программными компонентами, интегрированными в серверную плату, которые работают вместе для:

- Функции системы управления - система питания, ACPI, управление сбросом системы, инициализация системы, интерфейс передней панели, журнал системных событий.
- Контролируйте различные датчики платы и системы и регулируйте термические характеристики и производительность платформы для поддержания (по возможности) функциональности сервера в случае отказа компонентов и/или неблагоприятных условий окружающей среды.
- Отслеживайте и сообщайте о состоянии системы.
- Обеспечивает интерфейс для приложений программного обеспечения Intel® Server Management.

В этом разделе представлен общий обзор функций управления платформой и функций, реализованных на серверной материнской плате.

Серверная система Intel® *Спецификация BMC Firmware Внешнего продукта (EPS)* и Серверная система Intel® *Спецификация BIOS Внешнего продукта (EPS)* для серверной продукции Intel® на базе процессора Intel® Xeon® Scalable семья должна быть ссылкой для получения дополнительного углубленного и дизайна -уровневая информация управления платформой.

7.1 Обзор набора функций управления

В следующих разделах описаны функции, которые поддерживает встроенное микропрограммное обеспечение BMC. Поддержка и использование некоторых функций зависит от серверной платформы, в которую интегрирована серверная плата, и любых дополнительных компонентов и опций системного уровня, которые могут быть установлены.

7.1.1 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.
- Функциональность устройства корпуса, включая управление питанием/сбросом и поддержку флагов загрузки BIOS.
- Устройство приемника событий для приема и обработки событий от других подсистем платформы.
- Доступ к системным устройствам, заменяемым на месте (FRU), с помощью команд IPMI FRU.
- Функциональность устройства журнала системных событий (SEL), включая отслеживание серьезности SEL и расширенный SEL.
- Хранение и доступ к системным записям данных датчиков (SDR).
- Управление сенсорным устройством и опрос для мониторинга и отчетности о состоянии системы.
- 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 через 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*.

7.1.2 Обзор функций, не относящихся к IPMI

BMC поддерживает следующие функции, не связанные с IPMI.

- Внутрисхемное обновление прошивки BMC.
- Отказоустойчивая загрузка (FRB), включая FRB2, поддерживаемую функцией сторожевого таймера.
- Обнаружение вторжения в корпус (в зависимости от поддержки платформы).
- Управление скоростью вентилятора с SDR, мониторинг и поддержка резервирования вентиляторов.
- Улучшения в управлении скоростью вентилятора.
- Мониторинг и поддержка резервирования источников питания.
- Поддержка вентилятора с возможностью горячей замены.
- Тестовые команды для установки и получения состояний сигналов платформы.
- Коды диагностических звуковых сигналов для состояний 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.
- Мониторинг температуры DIMM с использованием алгоритма управления вентилятором с обратной связью с учетом 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 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.

7.2 Возможности и функции управления платформой

7.2.1 Подсистема питания

Серверная плата поддерживает несколько источников управления питанием, которые могут инициировать включение или выключение питания, как описано в Таблице 17.

Таблица 17. Источники регулирования мощности

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
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

7.2.2 Расширенный интерфейс настройки и питания (ACPI)

Серверная плата поддерживает состояния Advanced Configuration and Power Interface (ACPI), как подробно описано в Таблице 18.

Таблица 18. 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	Поддерживается только на платформах рабочих станций. См. соответствующую информацию для конкретной платформы для получения дополнительной информации.
S4	Нет	Не поддерживается.
S5	Да	Мягкое отключение. • Кнопки на передней панели не заблокированы. • Поклонники 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.

7.2.2.1 Процессор Tcontrol Настройка

Процессоры, используемые с этой набором микросхем реализовать в функцию под названием Tcontrol, который обеспечивает на значение конкретного процессора, который может быть использован для регулировки в веерном управлении поведением, чтобы достичь оптимального охлаждения и акустику. BMC считывает их из CPU через в PECI прокси – механизм, предусмотренный в Intel® Management Engine (Intel® ME). BMC использует эти значения в качестве части из-за скорости вентилятора контроля алгоритма.

7.2.2.2 Отказоустойчивая загрузка (FRB)

Отказоустойчивая загрузка (FRB) это набор алгоритмов BIOS и BMC и аппаратной поддержки, которые позволяют многопроцессорной системе загружаться, даже если процессор начальной загрузки (BSP) выходит из строя. Только FRB2 поддерживается с помощью команд сторожевого таймера.
FRB2 относится к алгоритму FRB, который обнаруживает сбои системы во время POST. BIOS использует сторожевой таймер BMC для резервного копирования своей работы во время POST. BIOS настраивает сторожевой таймер, чтобы указать, что BIOS использует таймер для фазы FRB2 операции загрузки.
После того, как BIOS идентифицировал и сохранил информацию BSP, он устанавливает бит использования таймера FRB2 и загружает сторожевой таймер с новым интервалом тайм-аута.
Если сторожевой таймер истекает, когда бит использования сторожевого таймера установлен на FRB2, BMC (если так настроен) регистрирует событие истечения сторожевого таймера, показывая тайм-аут FRB2 в байтах данных события. Затем BMC выполняет аппаратный сброс системы, предполагая, что сброс, выбранный BIOS, является действием тайм-аута сторожевого таймера.
BIOS отвечает за отключение тайм-аута FRB2 перед запуском сканирования дополнительного ПЗУ и перед отображением запроса пароля загрузки. Если процессор выходит из строя и вызывает тайм-аут FRB2, BMC перезагружает систему.
BIOS получает от BMC статус сторожевого таймера. Если в статусе отображается истекший таймер FRB2, 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 FRB2 не отражается на показании датчика состояния процессора.
Отказ FRB2 не влияет на светодиоды на передней панели.

7.2.3 Сторожевой таймер

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

7.2.4 Журнал системных событий (SEL)

BMC реализует журнал системных событий, как указано в *спецификации интерфейса интеллектуального управления платформой версии 2.0*. Доступ к SEL доступен независимо от состояния питания системы через внутренние и внеполосные интерфейсы BMC.
BMC выделяет 95 231 байт (примерно 93 КБ) энергонезависимой памяти для хранения системных событий. Метки времени SEL могут быть не в порядке. 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 установке флага переполнения.

7.3 Мониторинг датчиков

BMC контролирует оборудование системы и сообщает о состоянии системы. Информация, собранная с физических датчиков, транслируется в датчики IPMI как часть модели датчика IPMI. BMC также сообщает о различных изменениях состояния 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 маржи
- Сторожевой датчик IPMI
- Сторожевой датчик BMC
- Мониторинг работоспособности управления системой BMC
- Сторожевой таймер VR
- Система воздушного потока Датчики контроля - действительны для Серверный корпус Intel® только
- Датчики контроля вентилятора
- Датчики теплового контроля
- Датчики контроля напряжения
- Датчик CATERR
- Мониторинг событий привязки LAN
- CMOS мониторинг батареи
- Датчик NMI (диагностическое прерывание)

7.3.1 Поведение при повторном включении датчика

Датчики могут быть ручными или автоматическими. Датчик автоматического повторного включения повторно активирует (сбрасывает) состояние события утверждения для порога или смещения, если этот порог или смещение отменяются после подтверждения. Это позволяет последующее утверждение порога или смещения для генерации нового события и связанного побочного эффекта. Примером побочного эффекта является усиление 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 липкое. 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-за состояния триггера. Например, некоторые датчики могут быть повторно активированы из-за сброса системы. Сброс BMC повторно активирует все датчики.
- Сброс системы или цикл питания постоянного тока повторно активирует все датчики вентилятора системы.

7.3.2 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))
- Плата датчиков 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.

7.4 Стандартное управление вентиляторами

BMC контролирует и 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 вентиляторы отказ вентилятора и его состояние определяют состояние датчика резервирования вентилятора.

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

Домен вентилятора 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 фан-домена.

Состояние фан-домена контролируется несколькими факторами. Факторы для состояния повышения 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 никакого повышения вентилятора, 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.

7.4.1 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 вентилятора, скорость вентилятора возвращается к номинальному состоянию. Выключение и включение и выключение питания или сброс системы повторно

активирует датчики скорости вращения вентилятора и устраняет условия отказа вентилятора. Если состояние отказа все еще присутствует, состояние наддува возвращается после повторной инициализации датчика и снова обнаруживается нарушение порога.

7.4.1.1 Обнаружение резервирования 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 избыточности вентилятора с помощью записей OEM SDR.

Отказ вентилятора или удаление вентиляторов с горячей заменой до количества резервных вентиляторов, указанного в SDR в конфигурации вентилятора, является некритичным отказом и отражается на состоянии передней панели. Отказ вентилятора или его 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 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.

7.4.2 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.

7.4.3 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 вентилятора 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.

7.4.4 Вход термодатчика для управления скоростью вентилятора

BMC использует различные датчики IPMI в качестве входа 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 в качестве входа для контроля скорости вентилятора:

- Датчики температуры плинтуса,
- 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, и
- Датчик температуры DIMM VRM.

На Рисунке 29 показано высокоуровневое представление структуры управления скоростью вентилятора, которая определяет скорость вентилятора.

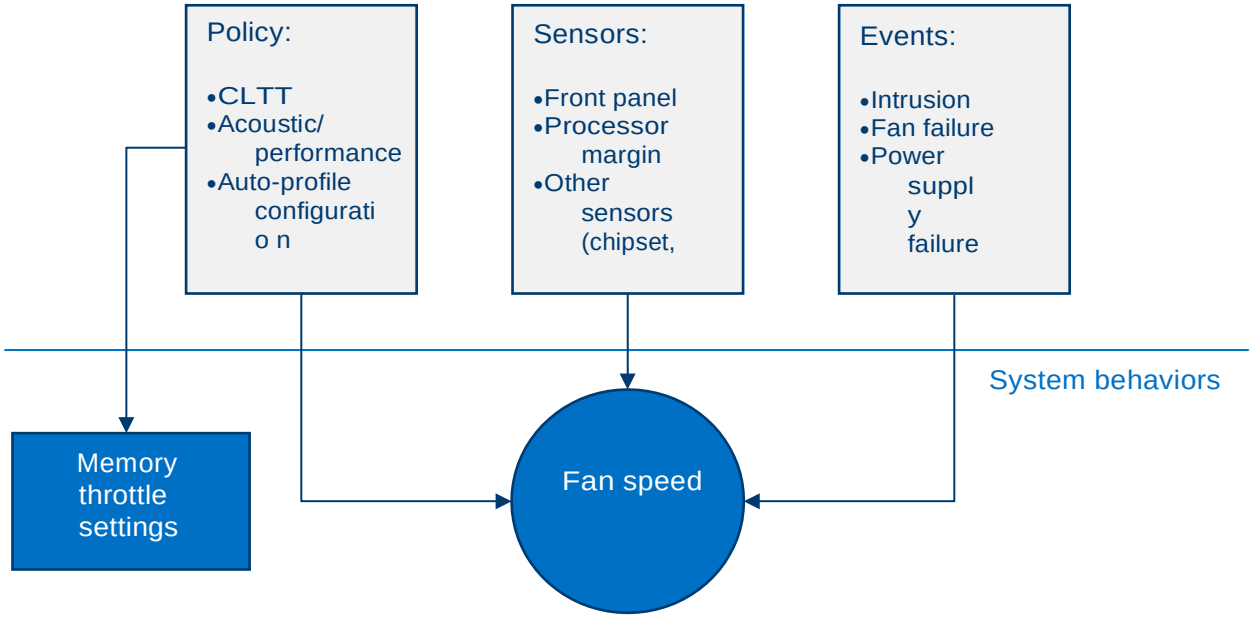


Рисунок 29. Процесс управления скоростью вентилятора высокого уровня

7.4.4.1 Повышение скорости вентилятора из-за отказа вентилятора

Каждый сбой вентилятора может определять уникальный ответ от всех других областей вентилятора. 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.

7.5 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 этой возможности управления с точки зрения BMC.

7.5.1.1 Регулирование температуры памяти

Система поддерживает управление температурой только за счет регулирования температуры с обратной связью (CLTT). Уровни дросселирования изменяются динамически до ограничения ограничения 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 управления регистры будут сконфигурированы с помощью в BIOS Memory Reference кодекса (MRC) во время процедуры POST. Памяти дросселирование будет работать, как в замкнутом контуре системы с DIMM температурных датчиков, как в контрольной ввода. В противном случае, система никак не изменить любой из дроссельного управления регистров в на встроенной памяти контроллера во время выполнения.
- **Динамический Closed-Loop Thermal Throttling (Dynamic-CLTT)**: CLTT управления регистры будут сконфигурированы с помощью BIOS MRC во время процедуры POST. Памяти дросселирование будет работать, как

в замкнутом контуре системы с в DIMM датчики температуры в качестве управляющего входа. Регулировка дросселирования выполняется во время работы в зависимости от изменений в охлаждении системы (скорости вращения вентилятора).

Серверные системы Intel®, поддерживающие семейство масштабируемых процессоров Intel® Xeon®, поддерживают тип CLTT, называемый Hybrid-CLTT, для которого встроенный контроллер памяти оценивает температуру DRAM между фактическими считываниями TSOD. Hybrid-CLTT используется во всех серверных системах Intel®, поддерживающих семейство масштабируемых процессоров Intel® Xeon®, которые имеют модули DIMM с термодатчиками. Таким образом, термины Dynamic-CLTT и Static-CLTT действительно относятся к этому «гибридному» режиму. Обратите внимание, что если опрос TSOD, выполняемый IMC, прерывается, показания температуры, которые BMC получает от IMC, являются этими оценочными значениями.

7.5.1.2 Динамический (гибридный) CLTT

Система будет поддерживать динамический CLTT (память), для которого микропрограмма BMC динамически изменяет регистры теплового смещения в IMC во время выполнения на основе изменений в охлаждении системы (скорости вращения вентилятора). Для статического CLTT к показанию TSOD применяется фиксированное значение смещения, чтобы получить температуру кристалла; 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 компания BMC определяет скорость воздуха для каждой области вентилятора 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 будет встроенная справочная таблица, которая предоставляет значения теплового смещения для каждого типа DIMM, настройки высоты и 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.

7.6 Шина управления питанием (PMBus *)

Шина управления питанием (PMBus *) - это открытый стандартный протокол, основанный на транспорте SMBus * 2.0. Он определяет средства связи с преобразователями мощности и другими устройствами с помощью команд на основе SMBus *. В системе должны быть установлены блоки питания, соответствующие PMBus *, для BMC или Intel® ME, 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/ .

7.6.1 Управление светодиодом неисправности компонента

Индикаторы **неисправности ЦП** - на серверной материнской плате имеется индикатор неисправности, управляемый BMC, для каждого сокета процессора. Светодиод горит, если есть несоответствие MSID, когда номинальная мощность процессора несовместима с платой (см. Рисунок 4).

Таблица 19. Светодиоды неисправности компонентов

Составная часть	Состояние	Описание
Светодиоды неисправности CPU	Горит желтым	Несоответствие MSID
	Выключено	Хорошо (ошибок нет)

8. Стандартные функции управления сервером

Встроенный BMC поддерживает стандартные функции управления сервером, доступные по умолчанию (Таблица 20).

Таблица 20. Стандартные функции управления сервером

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

8.1 Выделенный порт управления

Серверная плата включает выделенный порт управления (BMC) RJ45 1 Гб (Рисунки 3 и 24). Порт управления активен с установленным ключом Intel® RMM4 Lite или без него.

8.2 Встроенный веб-сервер

Стандартная управляемость BMC обеспечивает встроенный веб-сервер и настраиваемый OEM-интерфейс веб-интерфейс, который предоставляет возможности управления базовым набором функций BMC. Он поддерживается всеми встроенными сетевыми адаптерами, которые имеют возможность управления для BMC, а также встроенный выделенный порт управления. Поддерживаются как минимум два одновременных веб-сеанса от двух разных пользователей. Встроенный пользовательский веб-интерфейс поддерживает следующие клиентские веб-браузеры:

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

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, представленный 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, который может быть отправлен в Intel® для отладки.
- Обеспечьте 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 загружены связанные SDR.
- Принудительное подключение HTTPS для большей безопасности.
- Отображение информации о процессоре и памяти, доступной через IPMI через LAN.
- Отображение мощности, потребляемой сервером.
- Просмотр и настройка параметров VLAN.
- Предупредить пользователя, что изменение конфигурации IP-адреса вызывает отключение.
- Принудительно войти в настройки BIOS при сбросе (управление питанием сервера).

8.3 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 и 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 флэш-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.

8.3.1 Перенаправление клавиатуры, видео и мыши (KVM)

Прошивка BMC поддерживает перенаправление клавиатуры, видео и мыши (KVM) по локальной сети. BMC поддерживает встроенное приложение KVM (удаленная консоль), которое можно запускать со встроенного веб-сервера с удаленной консоли. Поддерживается перенаправление мыши и клавиатуры на базе USB1.1 или 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 на управляемом сервере.

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

Другие атрибуты перенаправления KVM включают:

- Шифрование перенаправленного экрана, клавиатуры и мыши,
- Сжатие перенаправленного экрана,

Функция перенаправления KVM поддерживает следующие разрешения и частоты обновления:

- 640x480 при 60 Гц, 72 Гц, 75 Гц, 85 Гц, 100 Гц
- 800x600 при 60 Гц, 72 Гц, 75 Гц, 85 Гц
- 1024x768 при 60 Гц, 72 Гц, 75 Гц, 85 Гц
- 1280x960 при 60 Гц
- 1280x1024 при 60 Гц
- 1600x1200 при 60 Гц
- 1650x1080 (WSXGA +) при 60 Гц
- 1920x1080 (1080p) при 60 Гц
- 1920x1200 (WUXGA) при 60 Гц

8.3.1.1 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 - действительно требует восстановления сеанса. Сеансы KVM сохраняются при сбросе системы, но не при потере питания переменного тока.

8.3.1.2 Безопасность

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

8.3.1.3 Использование

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

8.3.1.4 Принудительный вход в BIOS Setup

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

8.3.2 Перенаправление медиа

Функция перенаправления носителя предназначена для того, чтобы позволить системным администраторам или пользователям подключать удаленную среду IDE или USB-CD-ROM, дисковод гибких дисков или флэш-диск USB в качестве удаленного устройства к серверу. После установки пульт

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, гибкий диск) 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. См. Список протестированных/поддерживаемых операционных систем для получения дополнительной информации.
- Перенаправление мультимедиа поддерживает перенаправление, как для виртуального компакт-диска, так и для виртуального гибкого диска/USB-устройства одновременно. Устройство компакт-дисков может быть либо локальным дисководом компакт-дисков, либо файлом образа ISO; устройство Floppy/USB может быть либо локальным дисководом, либо локальным устройством USB, либо файлом образа диска.
- 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 установленой 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-r 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.

Если утройство IDE или виртуальная дискета подключены удаленно во время загрузки системы, и устройство IDE, и виртуальная дискета представлены как загрузочные устройства. Невозможно представить в BIOS системы только один тип устройства.

8.3.2.1 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.

8.3.3 Удаленная консоль

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

8.3.4 Производительность

Удаленный дисплей точно представляет местный 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 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 через IP выполняется параллельно с локальным KVM, не влияя на работу локальной KVM.

9. Обзор встроенных разъемов/обозначений

В этом разделе указаны местоположения и выводы для встроенных разъемов и обозначений серверной материнской платы, которые обеспечивают интерфейс для системных опций и функций, для управления встроенной платформой или других доступных пользователю опций и функций (Рисунок 2).

9.1 Разъемы питания

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

9.1.1 Основное питание

Питание основной серверной материнской платы осуществляется через один 24-контактный разъем питания. Разъем помечен как «MAIN_PWR_CONN» в левой нижней части серверной материнской платы. В Таблице 21 представлена схема расположения контактов главного разъема питания.

Таблица 21. 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

9.1.2 Разъемы питания ЦП

Примечание. Поскольку BMC отслеживает наличие сигналов питания в серверной материнской плате, питание должно подаваться как на ЦП1, так и на ЦП2, даже если ЦП2 не установлен. Если сигналы присутствия не обнаружены, серверная плата не загрузится.

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

Таблица 22. 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 23. Распиновка разъема питания CPU2 («CPU_2_PWR»)

Контакт	Имя сигнала	Контакт	Имя сигнала
1	GND	5	P12V2
2	GND	6	P12V2

Контакт	Имя сигнала	Контакт	Имя сигнала
3	GND	7	P12V3B
4	GND	8	P12V3B

9.1.3 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 2x2-контактный разъем питания, который можно использовать для подачи до 216 Вт дополнительной мощности на серверную плату. В корпусе Intel этот разъем подключен к соответствующему разъему 2x2 на плате распределения питания. Бюджет мощности для всей системы должен быть выполнен, чтобы определить, сколько дополнительной мощности доступно для поддержки любых мощных дополнительных карт.

Таблица 24. 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.

9.2 Заголовки и 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.

9.2.1 Заголовок передней панели

На левом краю серверной 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 - и светодиоды - активность сетевой карты. Индикаторы, индикаторы активности жесткого диска, индикатор состояния системы и индикатор идентификатора системы.

Таблица 25. Распиновка заголовка 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
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

9.2.2 USB- разъем на передней панели

Серверная 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 26. Распиновка разъема USB 3.0 на передней панели

Контакт	Имя сигнала	Контакт	Имя сигнала
1	P5V_AUX_USB_FP_USB3	ключ	КЛЮЧ
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

9.3 Разъемы для встроенного хранилища

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

9.3.1 Разъемы SATA 6 Гбит/с

Серверная плата включает два 7-контактных разъема SATA, обеспечивающих скорость передачи данных до 6 Гбит/с. В Таблице 27 показано расположение контактов обоих разъемов.

Таблица 27. 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	-	-

Серверная плата Rikor® КДБА.469555.003 также включает два порта mini-SAS HD, которые поддерживают до восьми дисков SATA 6 Гбит/с. В Таблице 28 показано расположение выводов обоих разъемов.

Таблица 28. 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
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

9.3.2 Разъемы M.2

В Таблице 29 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 29. 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
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)
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(32KHz) (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		

9.4 Разъемы вентилятора

Серверная плата поддерживает девять вентиляторов. Семь предназначены для поддержки вентиляторов системы охлаждения, а два - для вентиляторов процессора.

9.4.1 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 30. 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 31. 4-контактный разъем системы вентилятора Разъем Pin-аут

Контакт	Имя сигнала
1	GND
2	12V
3	TACH
4	PWM

9.4.2 Разъемы вентилятора ЦП

Серверная плата включает два 4-контактных разъема вентилятора ЦП, помеченных как CPU_1_Fan и CPU_2_Fan. В следующей таблице приведены выводы для каждого.

Таблица 32. Распиновка разъема вентилятора ЦП

Контакт	Имя сигнала
1	GND
2	12V
3	TACH
4	PWM

9.5 Другие заголовки и разъемы

На серверной материнской плате имеется несколько разъемов ввода-вывода для различных интерфейсов, используемых для связи между BMC и периферийными устройствами для мониторинга, а также для взаимодействия с пользователем.

9.5.1 HSBP Inter-Integrated Circuit (I ² C) Заголовки

Семейство серверных плат Rikor® КДБА.469555.003 включает заголовок межинтегральной схемы (I ² C), помеченный «HSBP_I2C», для связи с объединительными платами с возможностью «горячей» замены. В следующей таблице показано расположение выводов.

Таблица 33. Распиновка I 2 C заголовка B («HSBP_I2C_B»)

Контакт	Имя сигнала
1	SMB HSBP 3V3STBY DATA
2	GND
3	SMB HSBP 3V3STBY CLK
4	RST PCIE SSD PERST N

9.5.2 Разъем последовательного порта

Серверная плата включает один внутренний разъем последовательного порта DH-10.

Таблица 34. Распиновка разъема последовательного порта A

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		

9.5.3 Разъем PMBUS

Серверная плата обеспечивает шину управления питанием, чтобы BMC мог контролировать установленные источники питания и связываться с ними. Распиновка этого разъема показана в следующей таблице.

Таблица 35. Распиновка разъема PMBUS

Контакт	Имя сигнала
1	SMB_PMB1_SML1_STBY_LVC3_SCL
2	SMB_PMB1_SML1_STBY_LVC3_SDA
3	IRQ_SML1_PMBUS_ALERT_RC_N
4	GND
5	P3V3

9.5.4 Заголовок вторжения в корпус

Серверная плата включает 2-контактный заголовок вскрытия корпуса, который можно использовать, когда шасси сконфигурировано с переключателем вскрытия корпуса. Заголовок имеет следующую распиновку.

Таблица 36. 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 шасси снята

10. Перемычки сброса и восстановления

Семейство серверных плат Rikor® КДБА.469555.003 имеет несколько блоков трехконтактных перемычек, которые можно использовать для настройки, защиты или восстановления определенных функций серверной материнской платы.

Символ ▼ обозначает контакт 1 на каждой колодке перемычек.

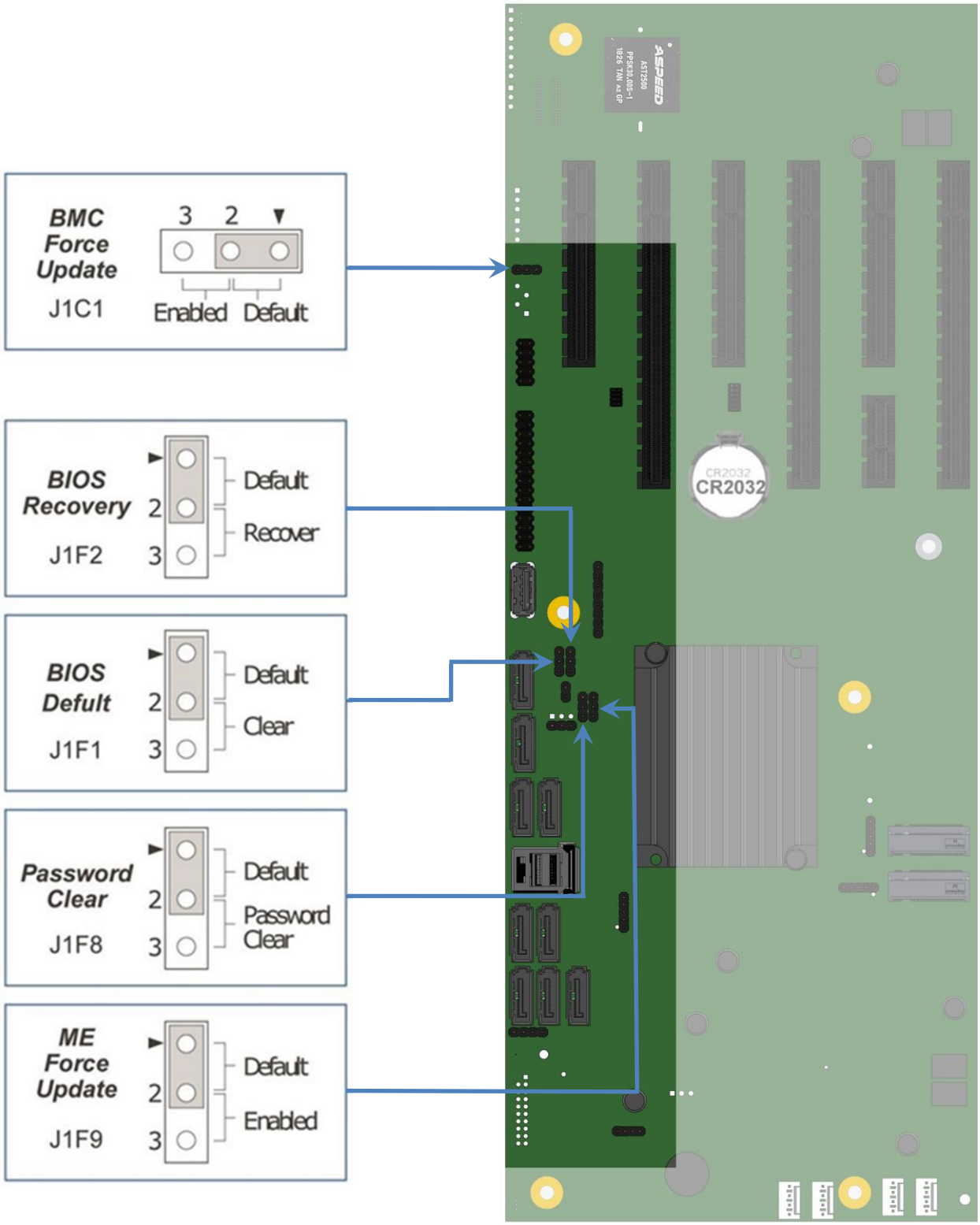


Рисунок 30. Расположение перемычек и контакты

10.1 Блок перемычек по умолчанию в BIOS

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 (и) питания.
2. Снимите с системой верхней крышки и переместить в «BIOS DFLT» перемычку из Контактков 1 - 2 (по умолчанию) для штифтов 2 - 3 (Set BIOS Defaults).
3. Подождите 5 секунд, а затем перейти на перемычку обратно к штифтам 1 - 2.
4. Установите на место верхнюю крышку системы.
5. Переустановите шнуры питания системы.
6. Во время процедуры POST откройте служебную программу настройки BIOS <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 <F2> отобразятся две ошибки:

- 0012 Дата/время системы RTC не установлены;
- 5220 Настройки BIOS сброшены до настроек по умолчанию.

10.2 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. 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 Контактков 1 - 2 (по умолчанию) для штифтов 2 - 3 (пароль ясно положение).
4. Установите на место верхнюю крышку системы и снова подсоедините шнуры питания.
5. Сила вверх на сервере и доступ <F2> BIOS Setup утилита.
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 шнуры питания переменного тока.
8. Снимите верхнюю крышку системы и переместите перемычку «Сброс пароля» обратно на контакты 1–2 (по умолчанию).
9. Установите на место верхнюю крышку системы и подсоедините шнуры питания переменного тока.
10. Включите сервер.
11. Настоятельно рекомендуется: немедленно загрузитесь в BIOS Setup <F2>, перейдите на вкладку «Безопасность» и установите пароли администратора и пользователя, если вы собираетесь использовать защиту паролем BIOS

10.3 Блок перемычек принудительного обновления микропрограммы Management Engine (ME)

Когда перемычка принудительного обновления прошивки 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 системы включены в пакеты обновления системы (SUP), размещенные на веб-сайте Центра загрузок Intel http://downloadcenter.intel.com.

1. Выключите систему.
2. Отсоедините шнуры питания переменного тока.

Примечание. Если переместить перемычку ME FRC UPD при подаче питания переменного тока на систему, ME не будет работать должным образом.

3. Снимите верхнюю крышку системы.
4. Переместить в «*ME FRC UPD»* Перемычка из штифтов 1 - 2 (по умолчанию), чтобы штифты 2 - 3 (Сила обновления позиции).
5. Установите на место верхнюю крышку системы и снова подсоедините шнуры питания переменного тока.
6. Включите систему.
7. Загрузитесь в оболочку EFI.
8. Измените каталоги на папку, содержащую файлы обновлений.
9. Обновите прошивку ME с помощью следующей команды:

iflash32/u/ni <номер версии> _ ME.cap

10. После успешного завершения обновления выключите систему.
11. Отсоедините шнуры питания переменного тока.
12. Снимите верхнюю крышку системы.
13. *Верните* перемычку «*ME FRC UPD* » на контакты 1-2 (по умолчанию).
14. Снова подсоедините шнуры питания переменного тока.
15. Включите систему.

10.4 Блок перемычек принудительного обновления BMC

Перемычка BMC Force Update используется для перевода BMC в режим восстановления загрузки для 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 системы включены в пакеты обновления системы (SUP), размещенные на веб-сайте Центра загрузок Intel http://downloadcenter.intel.com

1. Выключите систему.
2. Отсоедините шнуры 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 системы.
4. Переместить в «*BMC FRC UPD»* Перемычка из штифтов 1 - 2 (по умолчанию), чтобы штифты 2 - 3 (Сила обновления позиции).
5. Установите на место верхнюю крышку системы и снова подсоедините шнуры питания переменного тока.
6. Включите систему.
7. Загрузитесь в оболочку EFI.
8. Измените каталоги на папку, содержащую файлы обновлений.
9. Обновление прошивки 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 шнуры питания переменного тока.
12. Снимите верхнюю крышку системы.
13. Верните перемычку «BMC FRC UPD» на контакты 1-2 (по умолчанию).
14. Снова подсоедините шнуры 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.

10.5 Блок перемычек восстановления BIOS

Когда блок перемычки восстановления BIOS перемещается из положения 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 веб-сайта центра загрузки Intel. Эта перемычка используется, когда системная BIOS повреждена и не работает, что требует загрузки нового образа BIOS на серверную 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 с веб-сайта центра загрузки Rikor® http://downloadcenter.rikor.com

1. Выключите систему.
2. В целях безопасности отсоедините шнуры питания переменного тока.
3. Снимите верхнюю крышку системы.
4. Переместите перемычку «*Восстановление BIOS*» с контактов 1–2 (по умолчанию) на контакты 2–3 (положение для восстановления BIOS).
5. Установите на место верхнюю крышку системы и снова подсоедините шнуры питания переменного тока.
6. Включите систему.
7. Система автоматически загрузится с оболочкой EFI. Обновите BIOS, используя стандартные инструкции по обновлению BIOS, прилагаемые к пакету обновления системы.
8. После успешного завершения обновления BIOS выключите систему. В целях безопасности отсоедините шнуры питания переменного тока от системы.
9. Снимите верхнюю крышку системы.
10. Верните перемычку восстановления BIOS к контактам 1-2 (по умолчанию).
11. Установите на место верхнюю крышку системы и снова подсоедините шнуры питания переменного тока.
12. Мощность на в системе и доступ <F2> BIOS Setup утилита.
13. Настройте желаемые параметры BIOS.
14. Нажмите кнопку <F10> для сохранения и выхода из утилиты.

11. Световая диагностика

Семейство серверных плат Rikor® КДБА.469555.003 включает несколько встроенных светодиодных индикаторов, помогающих в поиске и устранении неисправностей на различных уровнях платы.

11.2 Системные светодиоды

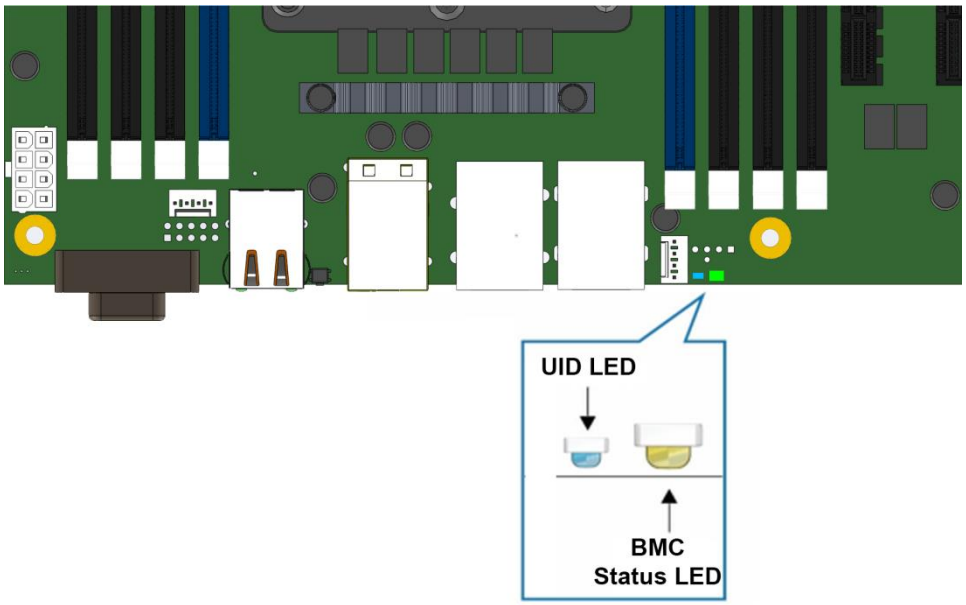


Рисунок 31. Светодиодный индикатор состояния системы и идентификационный светодиодный индикатор

11.2.1 Светодиод идентификатора системы

На серверной 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 серверной материнской плате напрямую связан со светодиодным индикатором идентификатора системы на передней панели системы, если он имеется.

11.2.2 Светодиод состояния системы

Серверная плата оснащена двухцветным светодиодным индикатором состояния системы. Светодиод состояния системы на серверной 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 или S5), BMC все еще находится в режиме ожидания и сохраняет состояние датчика и светодиодного индикатора состояния 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 подробно описаны в Таблице 37.

Таблица 37. 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 и при постоянном включении идентификатора шасси BMC загружает Linux *. Управление передано от BMC uBoot самой BMC Linux *. Он будет в этом состоянии ~ 10-20 секунд.
Зеленый	~ 1 Гц мигает	Деградированный	Система деградировала: 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 превышает минимальное количество, необходимое для охлаждения системы. 3. Номера критический порог пересекла - Температура (в том числе HSBP температуры), напряжения, входной мощности к источнику питания, выходного тока для главной шины питания от источника питания и процессора Thermal Control 2. Датчики (Therm Ctrl). 3. Прогнозируемый сбой блока питания произошел при наличии конфигурации резервного блока питания. 4. Невозможно использовать всю установленную память (установлено более 1 модуля DIMM) 1. 5. Исправимые ошибки, превышающие пороговое значение, и переход на запасной модуль DIMM (резервирование памяти). Это указывает на то, что у пользователя больше нет модулей DIMM, указывающих на состояние потери избыточности. Соответствующий индикатор DIMM горит. 6. В зеркальной конфигурации, когда происходит зеркальное отображение памяти, и система теряет избыточность памяти. 7. Выход из строя аккумуляторной батареи. 8. Выполнение BMC в uBoot. (Обозначается идентификатором шасси, мигающим с частотой 3 Гц). 9. Система в деградированном состоянии (нет управляемости). BMC uBoot запущен, но не передал управление BMC Linux *. Сервер будет в этом состоянии через 6-8 секунд после сброса BMC, пока он загружает образ Linux * во флэш-память. 10. BMC Watchdog сбросил BMC. 11. Заявлено смещение датчика блока питания для ошибки конфигурации. 12. HDD HSC отключен или неисправен. 13. 13. Неисправность жесткого диска.
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. Заявление VRD Hot. 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)

11.4 Светодиоды сбоя ЦП

На серверной материнской плате имеется светодиод сбоя ЦП для каждого разъема ЦП. Светодиод сбоя ЦП горит, если обнаружена ошибка несоответствия MSID (т. Е. Номинальная мощность ЦП несовместима с платой).

11.5 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. (Источник питания постоянного включения/выключения будет не сброс BMC.) BMC сброс будет происходить после того, как в BMC встроенного программного обеспечение обновления на прием в BMC команды сброса холодной, и после сброса инициированного BMC Watchdog. В следующей таблице определены состояния светодиодных индикаторов во время процесса загрузки/сброса BMC.

Таблица 38. Светодиодные индикаторы состояния загрузки/сброса BMC

Состояние загрузки/сброса BMC	**Шасси ID LED**	**Состояние LED**	**Комментарий**
BMC/тест видеопамяти не прошел	Горит синим	Горит желтым	Неустранимое состояние. Свяжитесь с вашим представителем Intel ® для информация по замене этой материнской платы.
Оба универсальных загрузчика (u-Boot) плохие образы	Мигает синим 6 Гц	Горит желтым	Неустранимое состояние. Свяжитесь с вашим представителем Intel ® для информация по замене этой материнской платы.
BMC в u-Boot	Мигает синим 3 Гц	Мигает зеленым 1 Гц	Мигающий зеленый указывает на ухудшение состояния (отсутствие управляемости), мигание синего цвета означает, что u-Boot запущен, но не передал управление BMC Linux. Сервер будет в этом состоянии через 6-8 секунд после сброса BMC пока он загружает образ Linux во флеш-память.
BMC Загрузка Linux	Горит синим	Горит зеленым	Горит зеленым и синим после сброса цикла переменного тока/BMC, указывает что управление было передано от u-Boot самой BMC Linux. Он будет в этом состоянии ~ 10-20 секунд.
Конец процесса загрузки/сброса BMC. Нормальная работа системы	Выключен	Твердый Зеленый	Указывает, что BMC Linux загружен и функциональность управляемости запущен и работает. Светодиоды неисправности/состояния работают как обычно.

12. Обзор BIOS

12.1 POST Меню

В данном документе объясняется функционал меню BIOS, который отображает настройки конфигурации системы и позволяет изменять эти настройки для настройки системы.

Примечание. Внешний вид интерфейса BIOS материнской платы может несколько отличаться от приведенного в настоящем разделе.

Чтобы войти в меню BIOS, нажмите <Esc> на клавиатуре во время процедуры самотестирования при включении питания. Появится POST-меню BIOS (Рисунок 32):

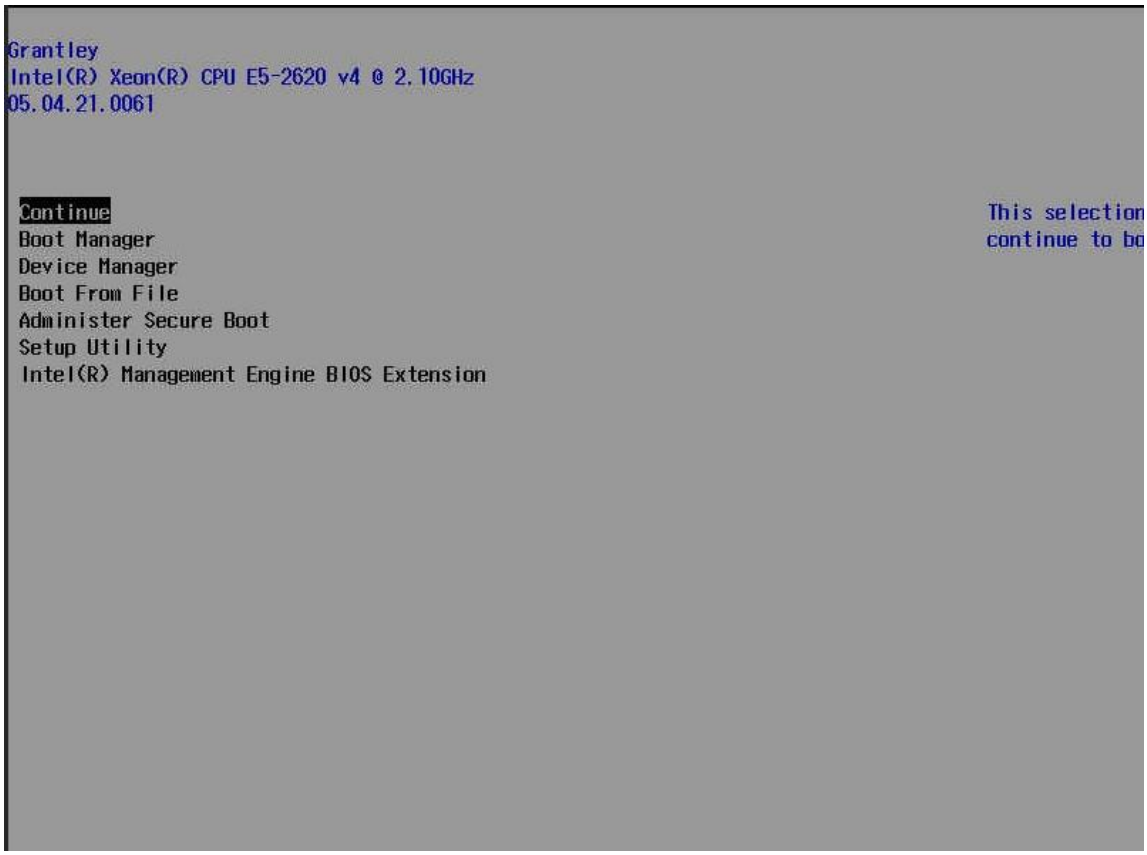


Рисунок 32. POST-меню BIOS

Для доступа к меню настройки BIOS, вы можете выбрать **'Setup Utility'** и нажать клавишу **‘Enter’**.

12.2 Меню настройки BIOS

Зайдя в меню настройки BIOS, вы увидите следующие пункты меню:

Рисунок 33. Разделы меню настройки BIOS

Разделы меню	Описание
Main (Главный)	Отображает системную информацию, такую как тип процессора и скорость, скорость системной шины, скорость системной памяти, общая 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. Настоящее описание является общим для платформ Рикор на базе Grantley

12.2.1 Main - главное меню

Раздел "**Main**" BIOS содержит краткий обзор основной информации о системе и возможность изменения языка отображения BIOS и системного времени.

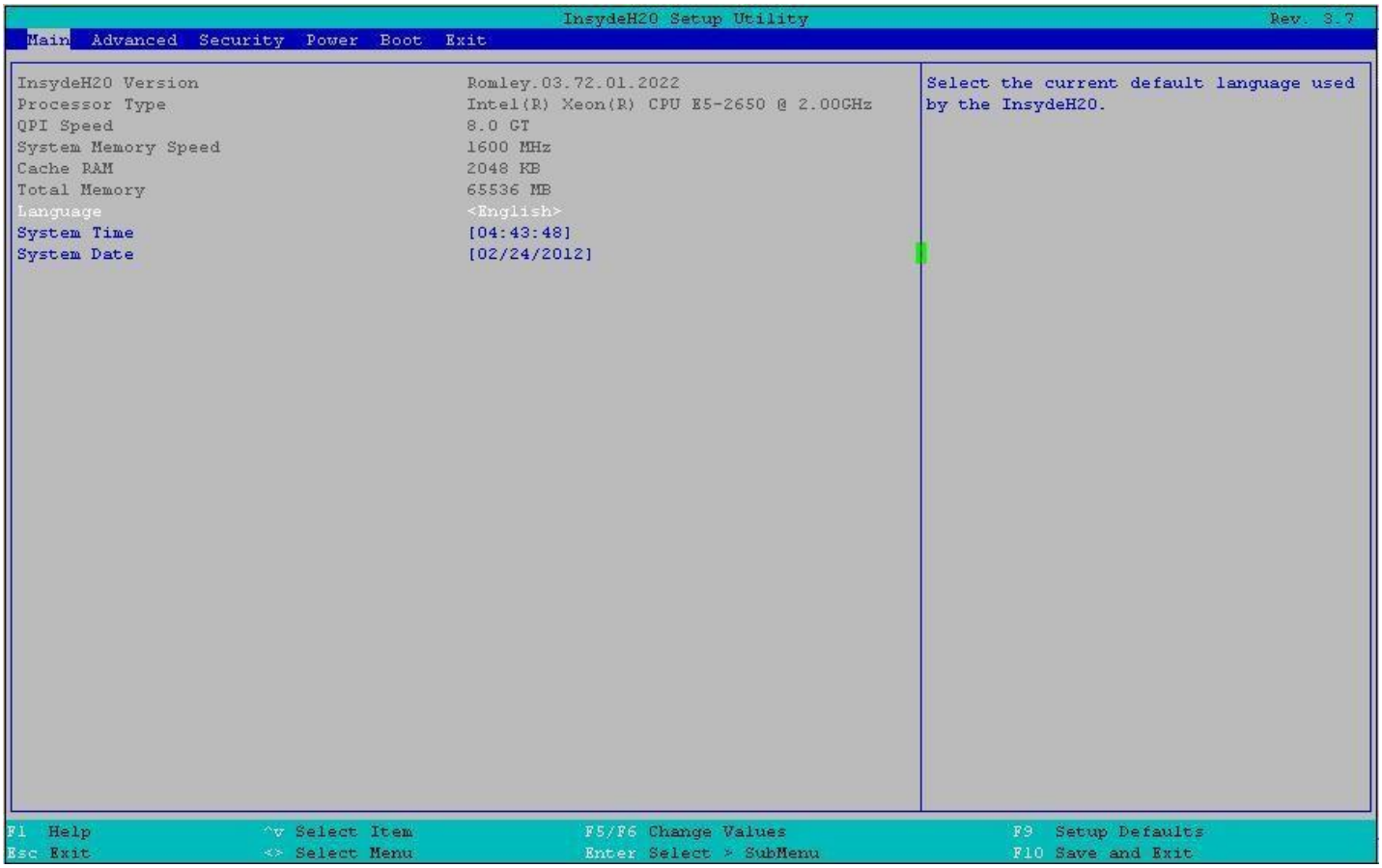


Рисунок 34

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 скорость автоматического определения QPI системы
System Memory Speed *(Скорость системной памяти)*	Нет вариантов	Отображает автоматически определяемую скорость системной памяти
Cache RAM *(Кэш ОЗУ)*	Нет вариантов	Отображает текущий объем оперативной памяти кэша в системе
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.

12.2.2 Advanced - расширенное меню

Раздел "**Advanced**" меню BIOS позволяет настраивать расширенные системные настройки.

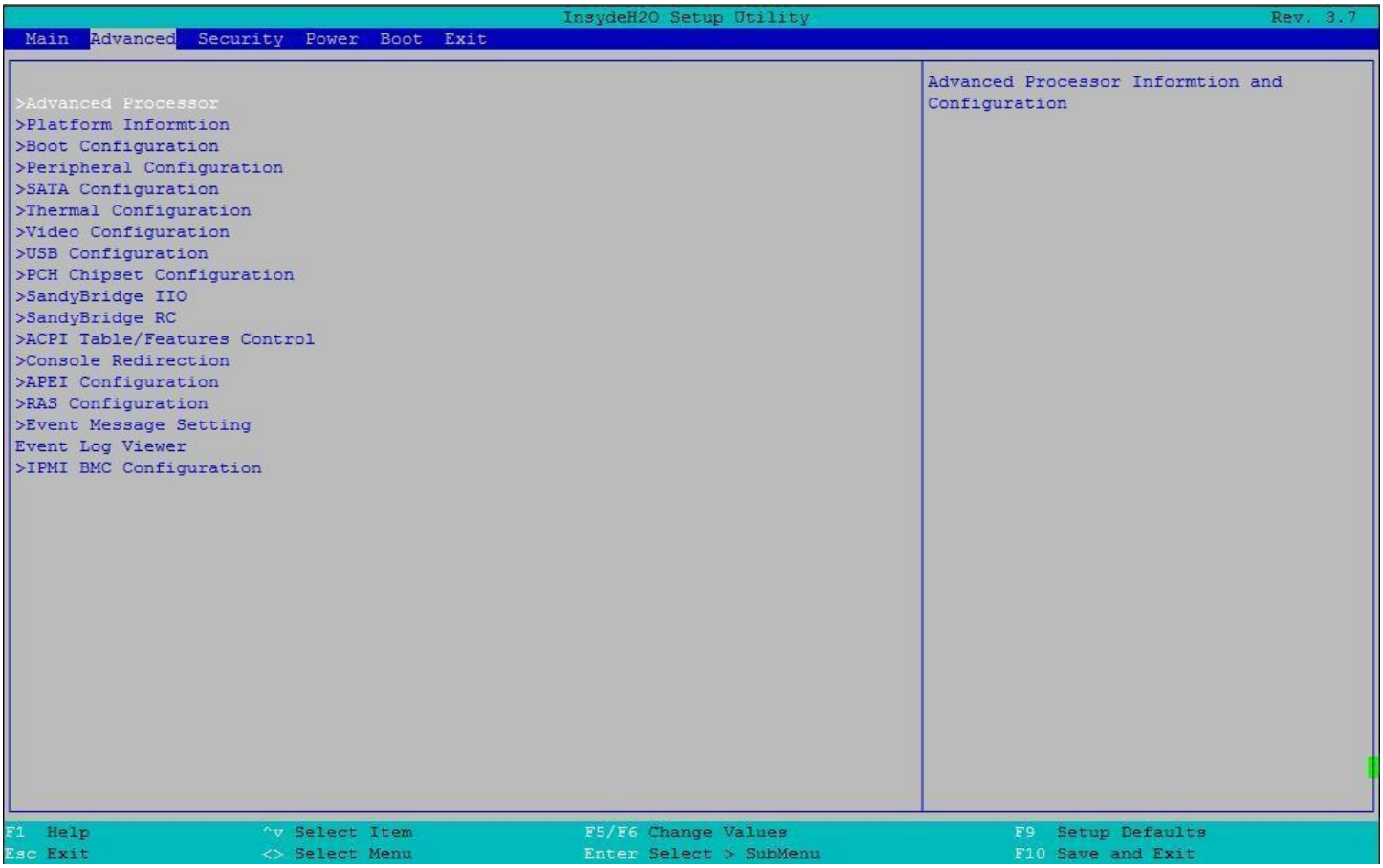


Рисунок 35

Настройка BIOS	Опции	Описание
Advanced Processor *(Расширенные настройки Процессора)*	См. раздел 12.2.2.1.	Расширенные настройки Процессора и гонфигурация
Platform Information *(Информация о платформе)*	См. раздел 12.2.2.2.	Форма для информации о платформе
Boot Configuration *(Конфигурация загрузки)*	См. раздел 12.2.2.3.	Настраивает настройки загрузки.
Peripheral Configuration *(Периферийная конфигурация)*	См. раздел 12.2.2.4.	Настраивает периферийные устройства.
SATA Configuration *(Конфигурация SATA)*	См. раздел 12.2.2.5.	Выберите контроллер SATA и тип драйвера жесткого диска, установленный в вашем сервере.
Termal Configuration *(Тепловая конфигурация)*	См. раздел 12.2.2.6.	Настройки тепловой конфигурации
Video Configuration *(Видео конфигурация)*	См. раздел 12.2.2.7.	Настройка параметров видео
USB Configuration *(Конфигурация USB)*	См. раздел 12.2.2.8.	Настраивает поддержку USB-порта
PCH Chipset Configuration *(Конфигурация набора микросхем PCH)*	См. раздел 12.2.2.9.	Расширенная конфигурация набора микросхем. Варианты

Настройка BIOS	Опции	Описание
SandyBridge IIO *(Мост интерфейса ввода/вывода)*	См. раздел 12.2.2.10.	Выберите, какой SandyBridge IIO компонентов для настройки.
SandyBridge RC *(Мост RC)*	См. раздел 12.2.2.11.	Относительная настройка моста SandyBridge RC
ACPI Table/Features Control *(ACPI-таблица/настройка характеристик)*	См. раздел 12.2.2.12.	Настройка ACPI-таблиц/установка характеристик
Console Redirection *(Переадресация консоли)*	См. раздел 12.2.2.13.	Настройки перенаправления консоли
APEI Configuration	См. раздел 12.2.2.14.	APEI-конфигурация
RAS Configuration	См. раздел 12.2.2.15.	RAS-конфигурация
Event Message Setting	См. раздел 12.2.2.16.	Настройка сообщений о событиях
Event Log Viewer	См. раздел 12.2.2.17.	Утилита предназначена для просмотра журнала событий.
IPMI BMC Configuration *(Конфигурация IPMI BMC)*	См. раздел 12.2.2.18.	Отображает информацию IPMI BMC

12.2.2.1 Advanced/Advanced Processor

Расширенные настройки/Расширенные настройки Процессора

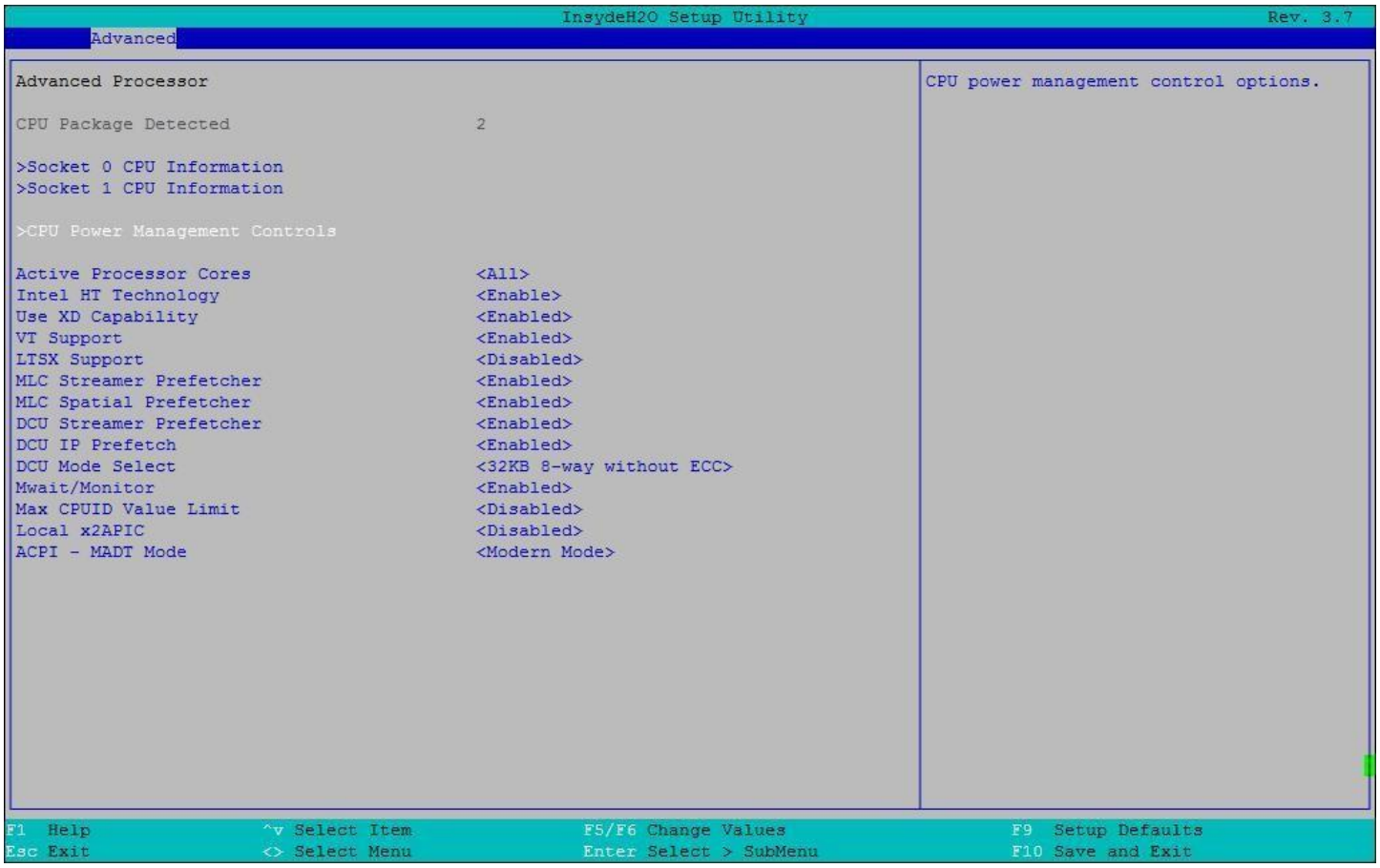


Рисунок 36

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 12.2.2.1.1.1.	Подробная информация для сокета процессора 0 или 1
CPU Power Management Controls *(Управление питанием процессора)*	См. раздел 12.2.2.1.2.2.	Возможности управления питанием процессора.
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 Vanderpool

Настройка BIOS	Опции	Описание
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 кэш 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 кэша L2 (MLC) для сокращения времени задержки кэша и настройки производительности для конкретного использования. По умолчанию - Enabled (Включено)
DCU Streamer Prefetcher	Отключено Включено	Позволяет включать и отключать предвыборку стримера блока кэша данных (L1 Data Cache Unit). По умолчанию - Enabled (Включено).
DCU IP Prefetch	Отключено Включено	Позволяет включать и отключать, основанную на адресах инструкций (IP - Instruction Pointer-Based) предвыборку блока кэша данных (DCU) для настройки производительности процессора. По умолчанию - Enabled (Включено).
DCU ModeSelect *(Выбор режимаDCU)*	32KB 8-полосный без ECC 16KB 4-полосный без ECC 16KB с ECC	Выбор режима работы DCU (L1 Data Cache Unit). Выберите размер блока данных и тип памяти (с ECC или без ECC).
Mwait/Monitor	Отключено Включено	Включение/отключение инструкций МОНИТОРА 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.

12.2.2.1.1 Advanced/Advanced Processor/Socket 0 CPU Information

Расширенные настройки/Расширенные настройки Процессора/Сокет 0 Информация о процессоре

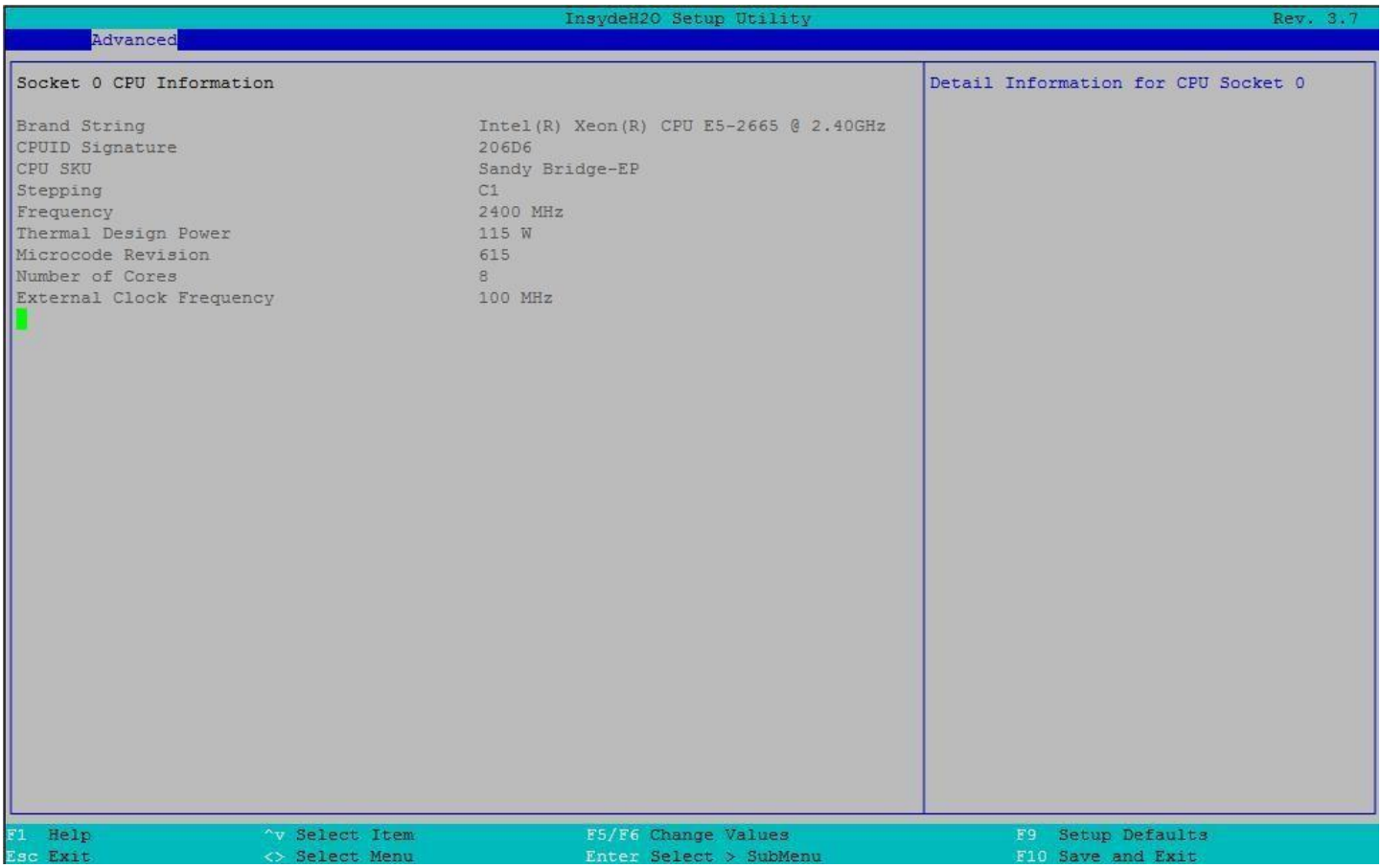


Рисунок 37

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	Processor stepping
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
External Clock Frequency	Нет опций	Внешняя тактовая частота

12.2.2.1.2 Advanced/Advanced Processor/CPU Power Management Controls

Расширенные настройки/Расширенные настройки Процессора/Управление питанием процессора

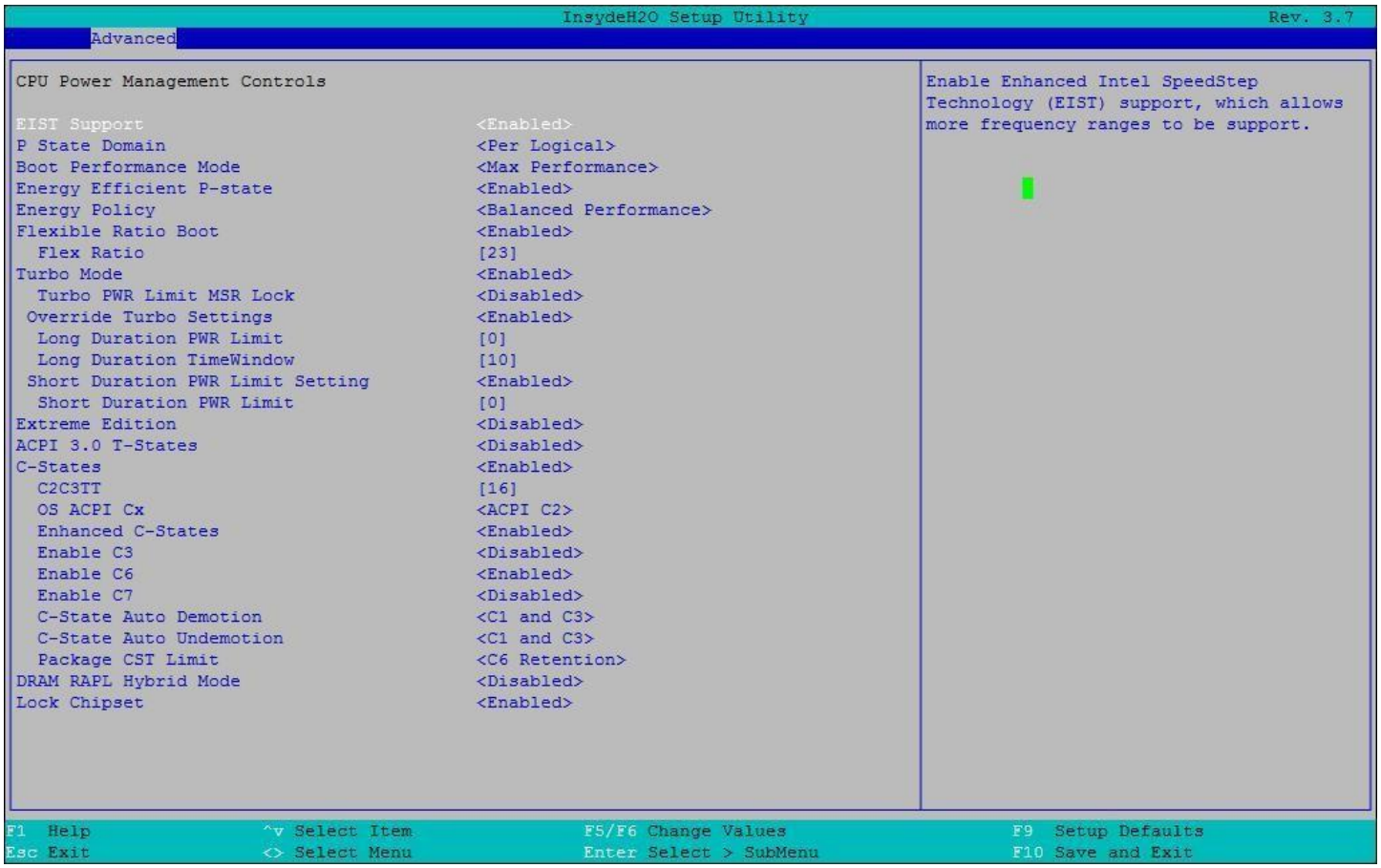


Рисунок 38

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.
Energy Efficient P-State	Отключено/Включено	Включение/выключение функции энергосберегающего P-состояния.
Energy Policy	• Баланс производительности • Баланс производительности и энергоэффективности • Энергоэффективно сть	Энергоэффективность используется процессором для внутреннего контроля параметров соотношения мощности и производительности.

Настройка BIOS	Опции	Описание
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 610h разблокированным для OS/SW для 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. Не будет запрограммировано значение TDP, превышающее значение плавления.
Long Duration TimeWindow	Значение настройки [0 - 128]	Предел мощности 1 Значение времени в секундах. 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 Короткая продолжительность 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, значение вниз в 1:10:1:74 бита [11:0].
OS ACPI Cx	ACPI C2 ACPI C3	Отчет CC3/CC6 для ОС ACPI C2 или ACPI C3.
Enhanced C-states	Отключено/Включено	Обеспечить возможность перехода от одного P-State к другому в сочетании с C-States.
Enable C3	Отключено/Включено	Включить/выключить Core C3

Настройка BIOS	Опции	Описание
Enable C6	Отключено/Включено	Включить/выключить Core C6
Enable C7	Отключено/Включено	Включить/выключить Core C7
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	Гибридный режим DRAM RAPL включает/выключает.
Lock Chipset	Отключено/Включено	Решите, нужно ли устанавливать безопасную блокировку SMBUS или нет.

12.2.2.2 Advanced/Advanced Processor/Platform Information

Расширенные настройки/ Расширенные настройки Процессора/Информация о платформе

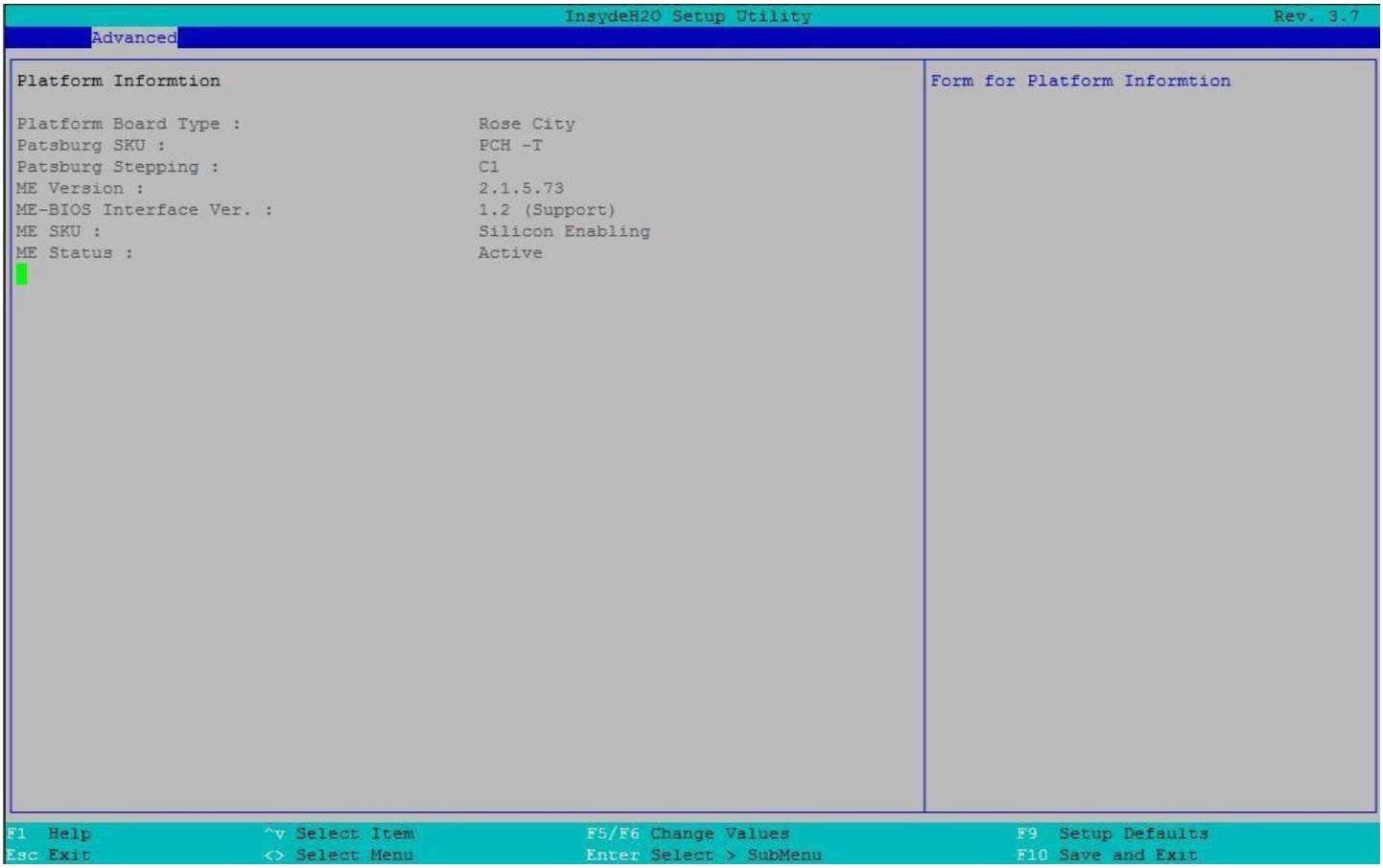


Рисунок 39

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	Описание версии ME F/W
ME-BIOS Interface Ver.	Нет	Описание Версия интерфейса ME-BIOS, это команда ME HECI для получения версии интерфейса (спецификация версии)
ME SKU	Нет	Описание: ME SKU be Silicon Enabling/Node Manager/DNM/DM
ME Status	Нет	Descript ME's Status be Active/Recovery

12.2.2.3 Advanced/Boot Configuration

Расширенные настройки/Конфигурация загрузки

Рисунок 40

Настройка BIOS	Опции	Описание
SCU Resolution	640*480 800*600 1024*768	Изменение разрешения программы настройки
Numlock	Вкл./Выкл	Selects Power-on state for Numlock

12.2.2.4 Advanced/Peripheral Configuration

Расширенные настройки/Периферийная конфигурация

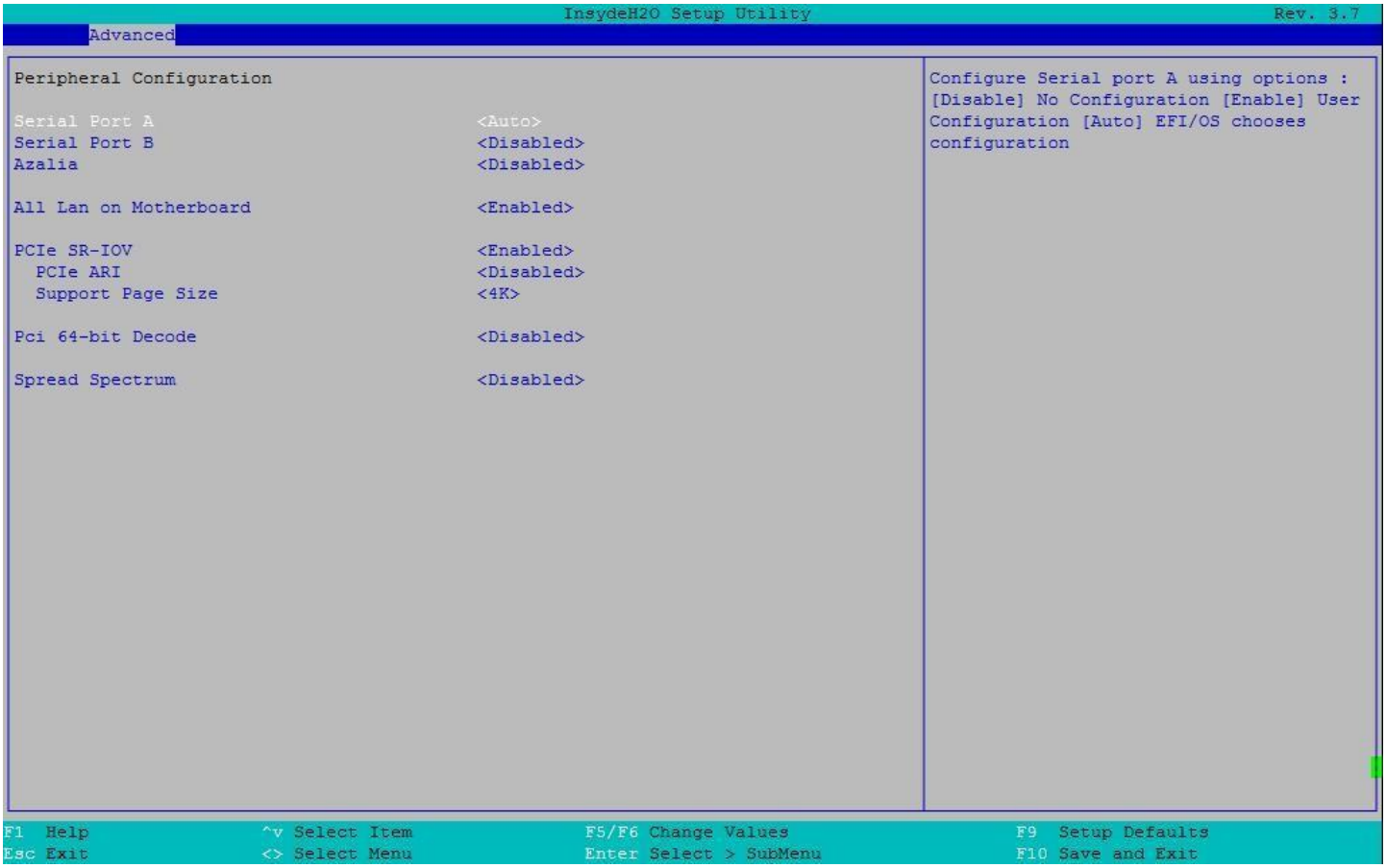


Рисунок 41

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 включают или выключают.
PCIe SR-IOV	Disable Enable	Отключить: Отключите функцию SR-IOV, если поддерживается карта PCIe Add-in Card. Включить: Включите функцию SR-IOV, если поддерживается карта PCIe Add-in.

Настройка BIOS	Опции	Описание
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	Spread Spectrum Disable/Enable настройку для уменьшения EMI

12.2.2.5 Advanced/SATA Configuration

Расширенные настройки/Конфигурация SATA

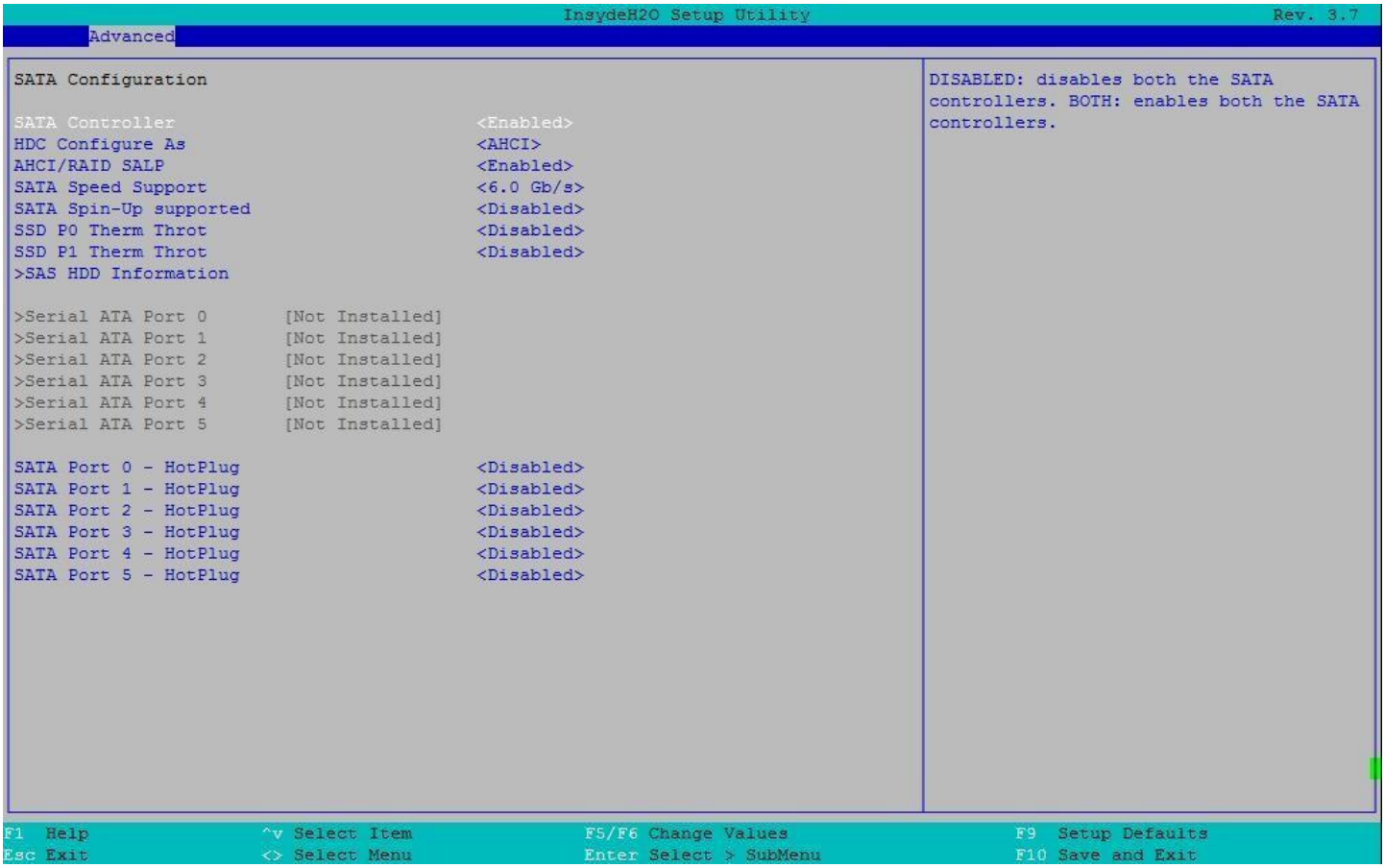


Рисунок 42

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.
SSD P0 Therm Throt	Включено Отключено	Reference BWG 16.4.6, if Port 0/1 have SSD on it, enable for Thermal Throttling setting. Disable for HDD, Enable for SSD.

Настройка BIOS	Опции	Описание
SSD P1 Therm Throt	Включено Отключено	Reference BWG 16.4.6, if Port 0/1 have SSD on it, enable for Thermal Throttling setting. Disable for HDD, Enable for SSD.
SAS HDD Information	См. раздел 12.2.2.5.1.	
SATA Port 0 - HotPlug	Включено Отключено	Включение/выключение SATA-порта 0 HotPlug.
SATA Port 1 - HotPlug	Включено Отключено	Включение/выключение SATA-порта 1 HotPlug.
SATA Port 2 – HotPlug	Включено Отключено	Включение/выключение SATA-порта 2 HotPlug.
SATA Port 3 – HotPlug	Включено Отключено	Включение/выключение SATA-порта 3 HotPlug.
SATA Port 4 – HotPlug	Включено Отключено	Включение/выключение SATA-порта 4 HotPlug.
SATA Port 5 – HotPlug	Включено Отключено	Включение/выключение SATA-порта 5 HotPlug.

12.2.2.5.1 Advanced/SATA Configuration/SAS HDD Information

Расширенные настройки/Конфигурация SATA/Информация о жестких дисках SAS

Рисунок 43

Настройка BIOS	Опции	Описание
SATA HDD-DiskX	Нет	Информация о жестких дисках на портах контроллера SCU.

12.2.2.6 Advanced/Thermal Configuration

Расширенные настройки/Тепловая Конфигурация

Рисунок 44

Настройка BIOS	Опции	Описание
Platform Thermal Configuration	См. раздел 12.2.2.6.1.	Тепловая конфигурация платформы
CPU Thermal Configuration	См. раздел 12.2.2.6.2.	Тепловая конфигурация процессора

12.2.2.6.1 Advanced/Thermal Configuration/Platform Thermal Configuration

Расширенные настройки/Тепловая Конфигурация/Тепловая конфигурация платформы

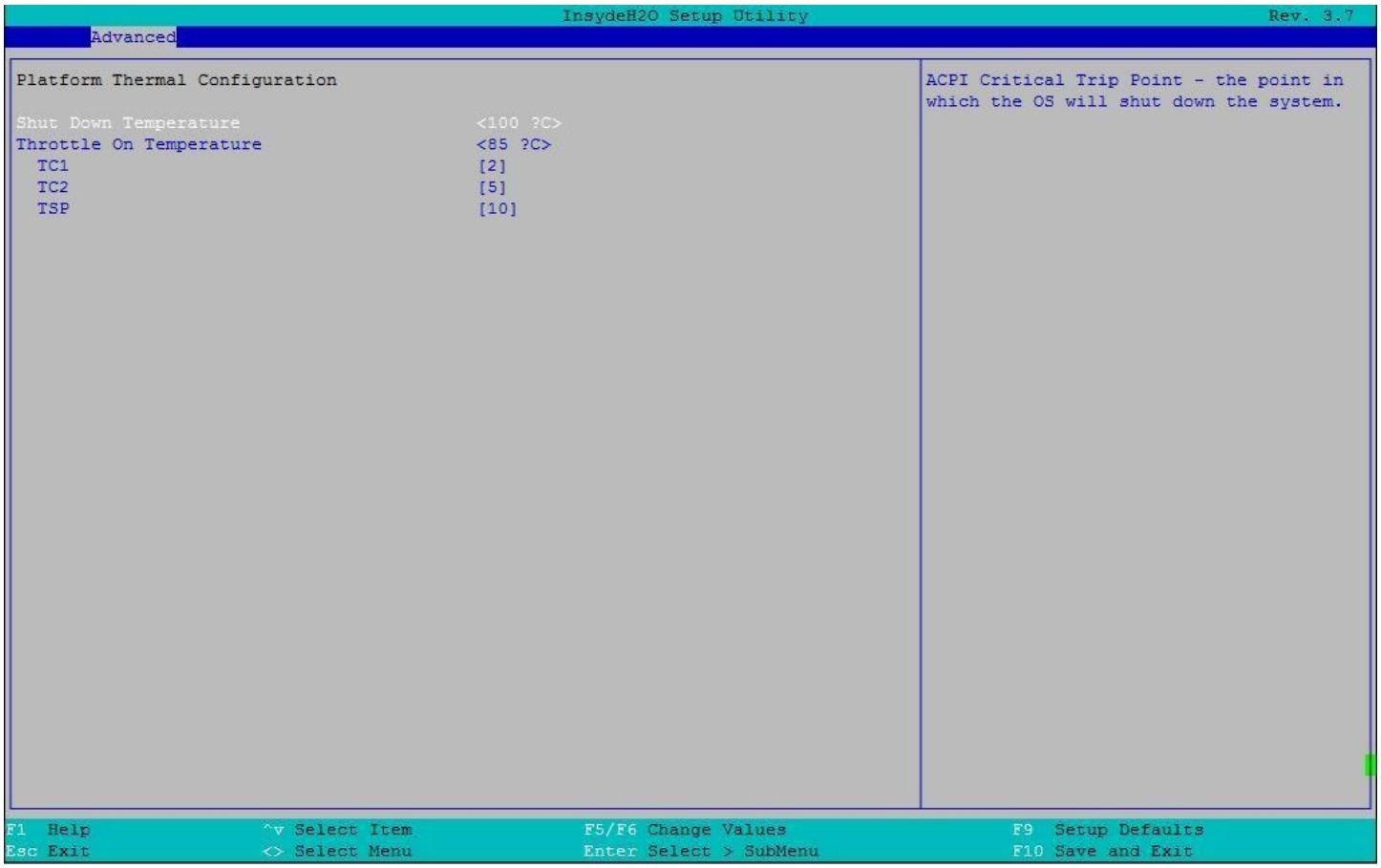


Рисунок 45

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 - точка в критической точке операционная система отключит систему.
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]	Thermal constant TC1 for the ACPI Passive Cooling (CPU Throttle On) Formula.
TC2	Значение настройки [1-16]	Thermal constant TC2 for the ACPI Passive Cooling (CPU Throttle On) Formula.
TSP	Значение регулировки [2-32].	В десятых долях секунды отображается, как часто ОС будет считывать температуру, когда включено пассивное охлаждение.

12.2.2.6.2 Advanced/Thermal Configuration/Cpu Thermal Configuration

Расширенные настройки/Тепловая Конфигурация/Тепловая конфигурация процессора

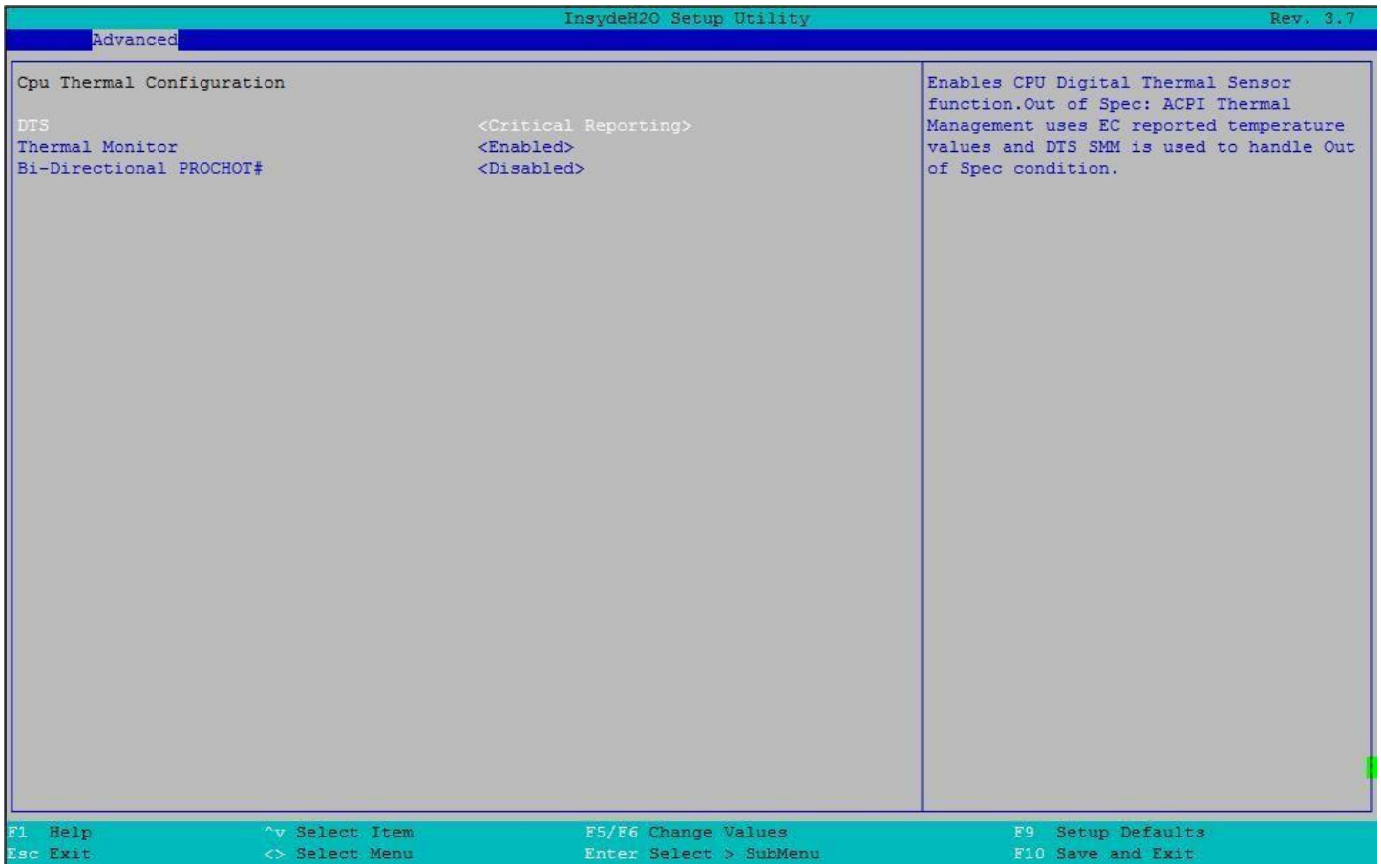


Рисунок 46

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 (любой из ядер), будет активирован PROCHOT#.

12.2.2.7 Advanced/Video Configuration

Расширенные настройки/Конфигурация Видео

Рисунок 47

Настройка BIOS	Опции	Описание
Display Mode	On Board First Plug In First	Установка типа настройки режима отображения.

12.2.2.8 Advanced/USB Configuration

Расширенные настройки/Конфигурация USB

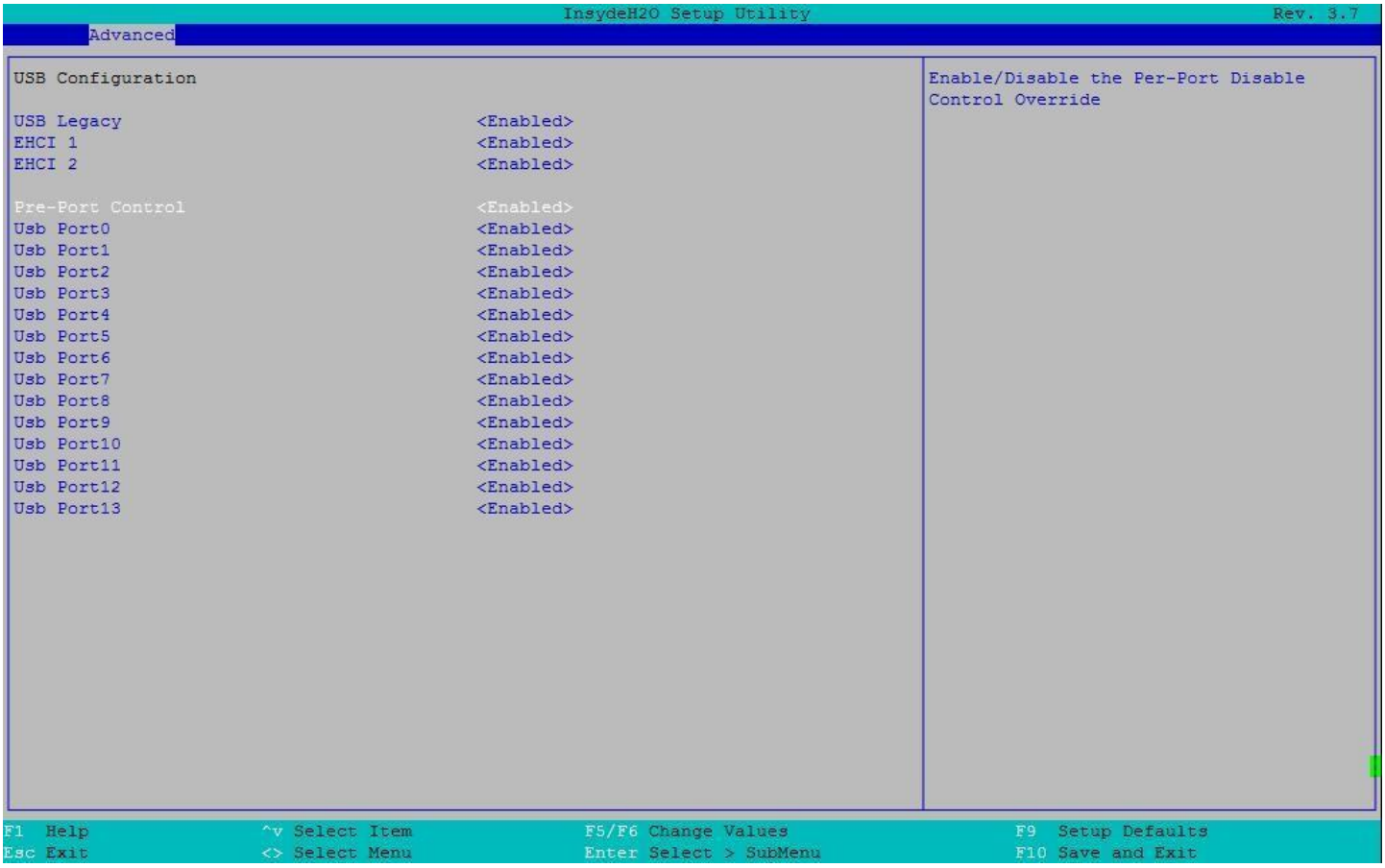


Рисунок 48

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	Позвольте пользователю управлять тем, чтобы каждый USB-порт был включен или выключен.
Порт USB 0-13	Отключить Включить	Выключить/Включить ток Выберите порт USB.

12.2.2.9 Advanced/PCH Chipset Configuration

Расширенные настройки/Конфигурация PCH чипсета

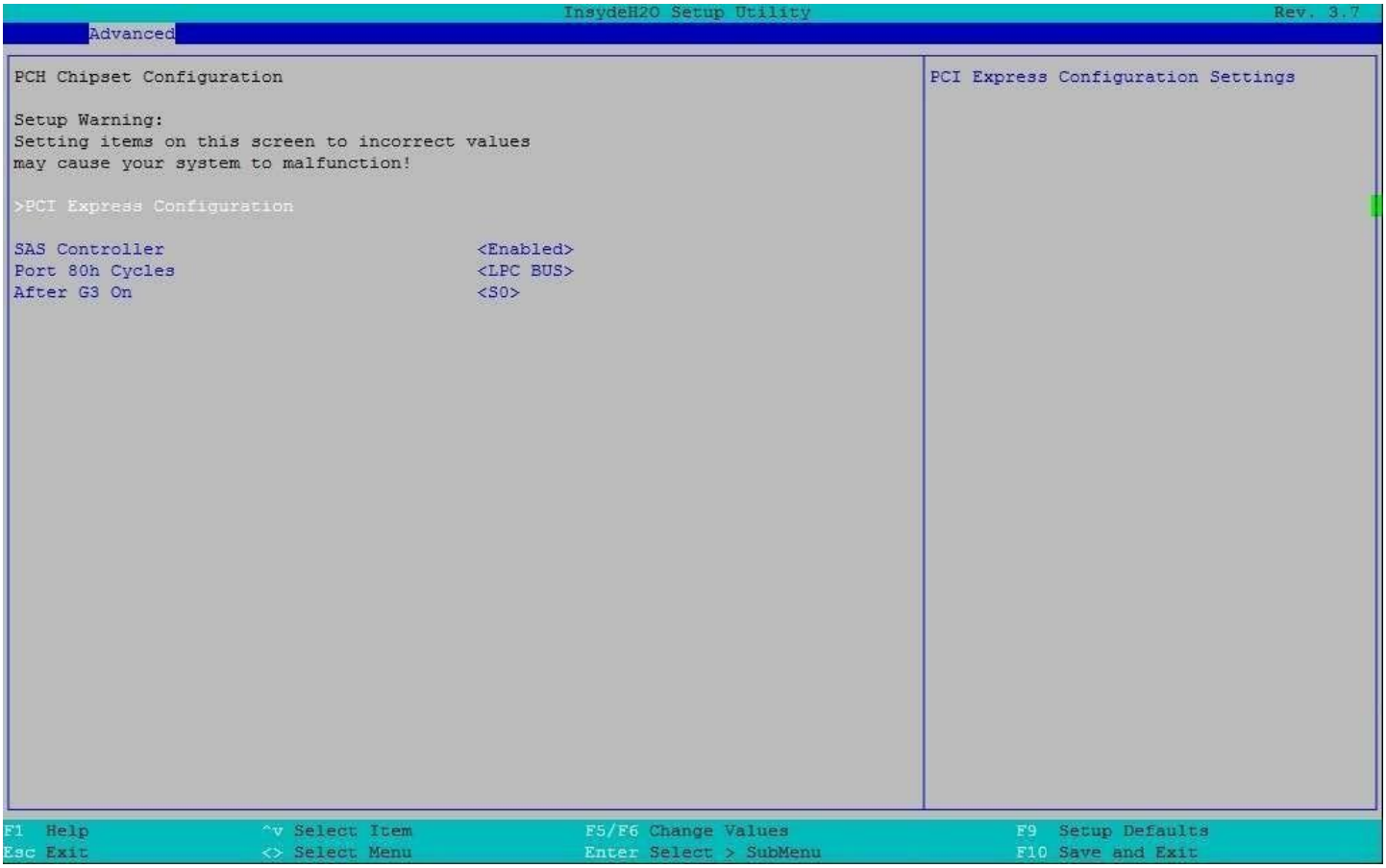


Рисунок 49

Настройка BIOS	Опции	Описание
PCI Express Configuration	См. раздел 12.2.2.9.1.	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 состояния платформенной ACPI после G3 (Mechanical Off) в ACPI S0/S5/Последнее состояние.

12.2.2.9.1 Advanced/PCH Chipset Configuration/PCI Express Configuration

Расширенные настройки/Конфигурация PCH чипсета/Конфигурация PCI Express

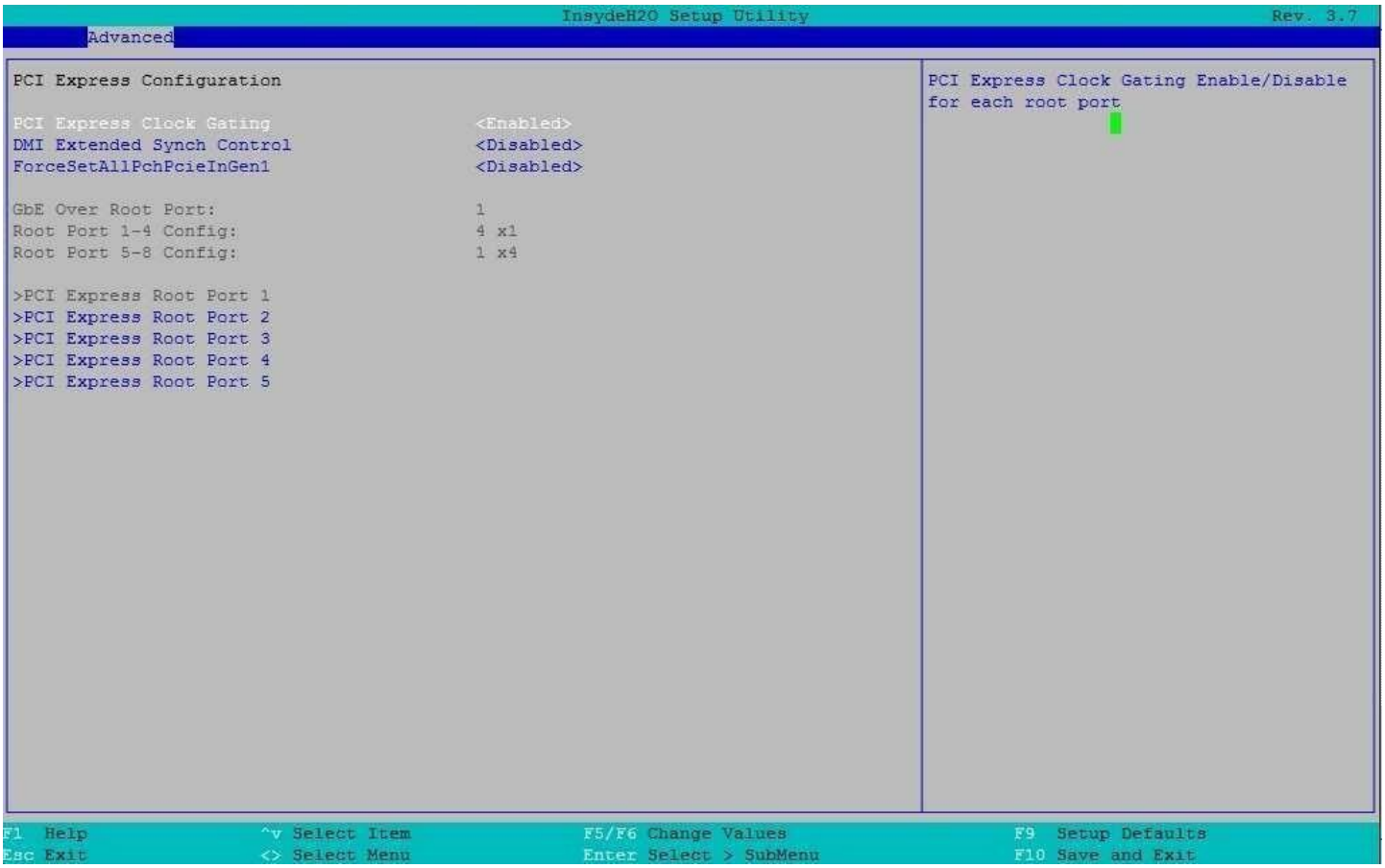


Рисунок 50

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
ForceSetAllPchPcieInGen1	Отключить Включить	Установите все PCIe корневой порт PCH на 1-е поколение.
After G3 On	S0 S5 Последнее состояние	Установите состояние платформы ACPI после G3 (механическое выключение) на ACPI S0/S5/Последнее состояние.
PCI Express Root Port 1	См. раздел 12.2.2.9.1.1.	Настройки корневого Порта 1 PCH PCI Express
PCI Express Root Port 2	См. раздел 12.2.2.9.1.1.	Настройки корневого Порта 2 PCH PCI Express
PCI Express Root Port 3	См. раздел 12.2.2.9.1.1.	Настройки корневого Порта 3 PCH PCI Express
PCI Express Root Port 4	См. раздел 12.2.2.9.1.1.	Настройки корневого Порта 4 PCH PCI Express
PCI Express Root Port 5	См. раздел 12.2.2.9.1.1.	Настройки корневого Порта 5 PCH PCI Express
PCI Express Root Port 6	См. раздел 12.2.2.9.1.1.	Настройки корневого Порта 6 PCH PCI Express
PCI Express Root Port 7	См. раздел 12.2.2.9.1.1.	Настройки корневого Порта 7 PCH PCI Express
PCI Express Root Port 8	См. раздел 12.2.2.9.1.1.	Настройки корневого Порта 8 PCH PCI Express

12.2.2.9.1.1 Advanced/PCH Chipset Configuration/PCI Express Configuration/PCI Express Root Port

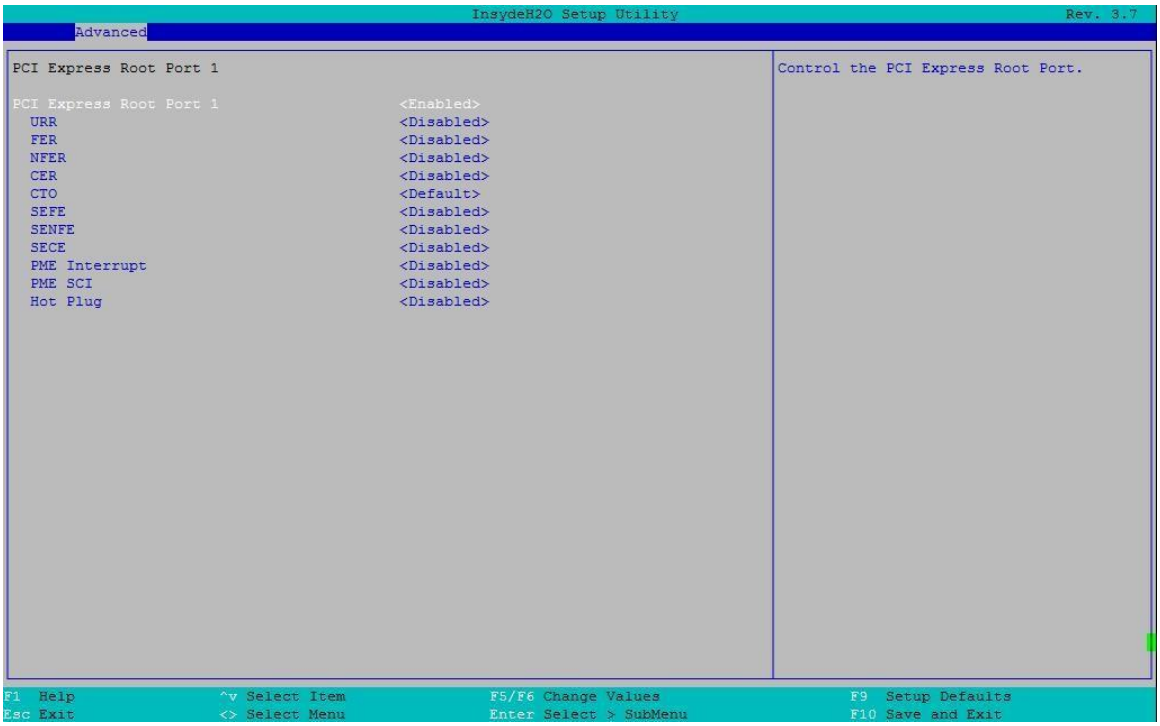


Рисунок 51

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 1-3,5 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.

12.2.2.10 Advanced/SandyBridge IIO Configuration

Расширенные настройки/Конфигурация SandyBridge IIO

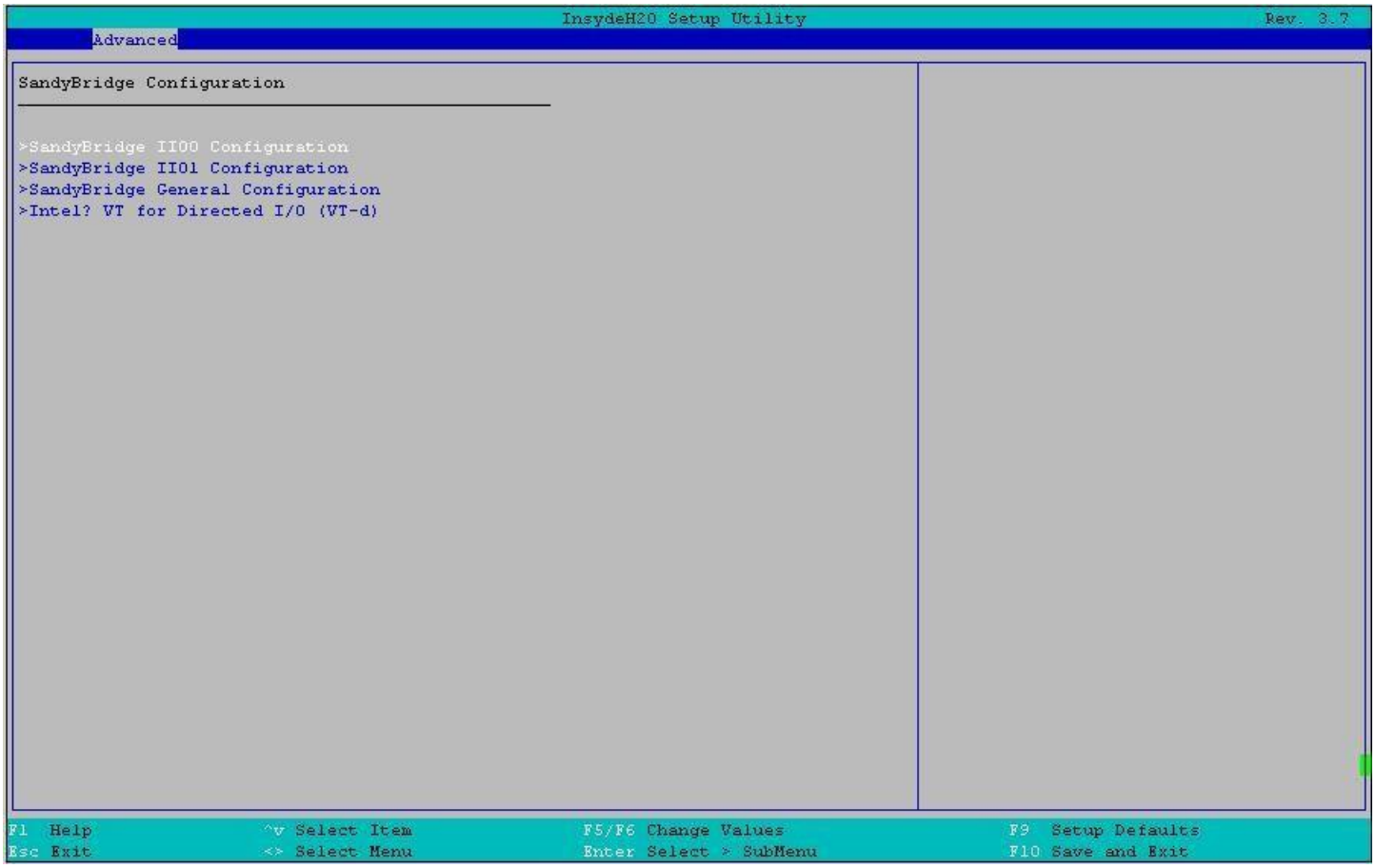


Рисунок 52

Настройка BIOS	Опции	Описание
SandyBridge IIO0 Configuration	См. раздел 12.2.2.10.1.	Конфигурирование IIO PCIe
SandyBridge IIO1Configuration	См. раздел 12.2.2.10.1.	Конфигурирование IIO PCIe
SandyBridge General Configuration	См. раздел 12.2.2.10.2.	Общая конфигурация для всех интерфейсов ввода/вывода
Intel VT for Directed I/O (VT-d)	См. раздел 12.2.2.10.3.	Настройка VT-d

12.2.2.10.1 Advanced/SandyBridge IIO/ SandyBrideg IIO 0, 1

Расширенные настройки/Конфигурация SandyBridge IIO/SandyBrideg IIO 0, 1

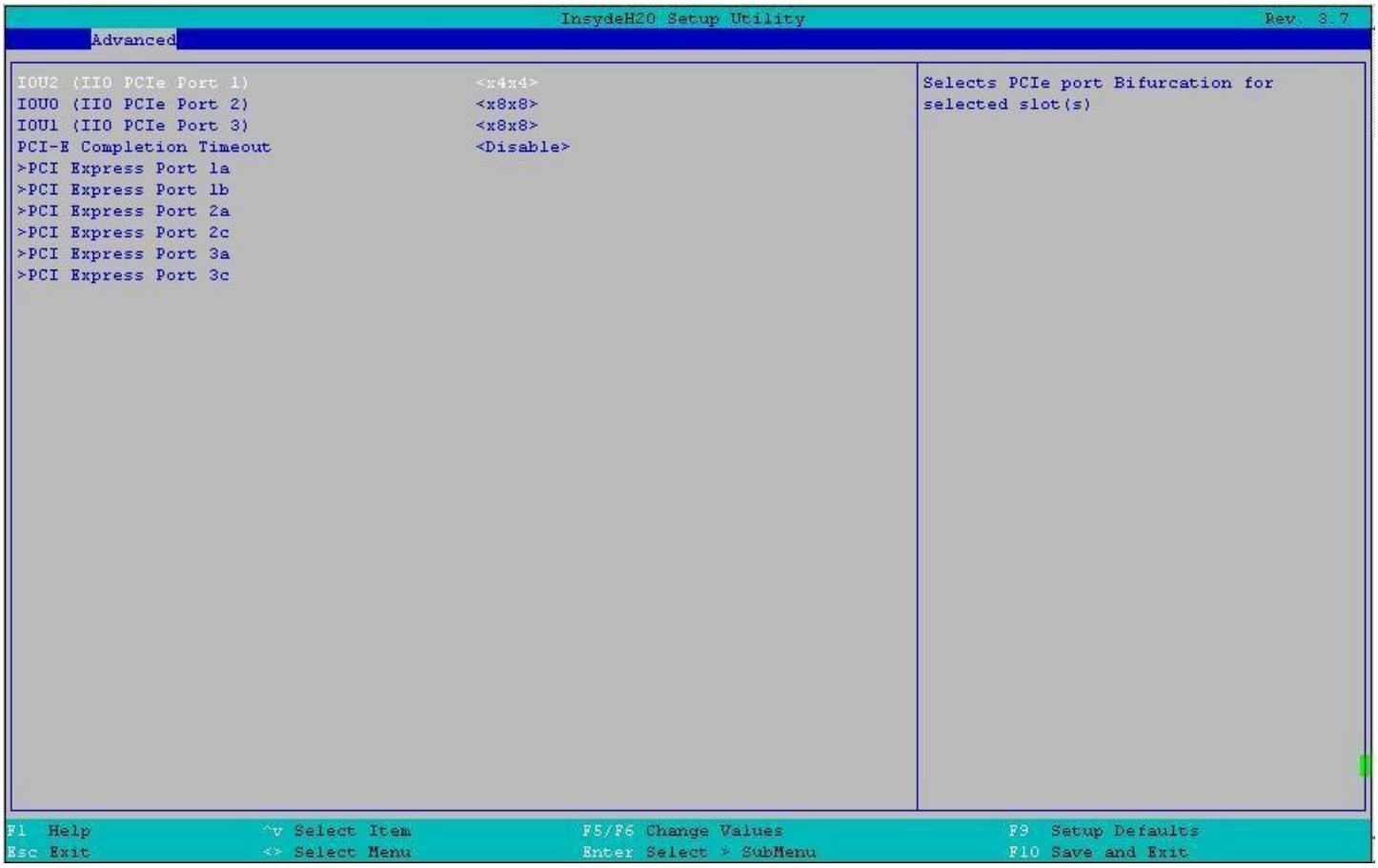


Рисунок 53

Настройка BIOS	Опции	Описание
IOU2 (IIO PCIe Port 1)	x4x4 x8	Выбор разделения портов PCIe для выбранного разъема(ов).
IOU0 (IIO PCIe Port 2)	x4x4x4x4 x4x4x8 x8x4x4 x16	Выбор разделения портов PCIe для выбранного разъема(ов).
IOU1 (IIO PCIe Port 3)	x4x4x4x4 x4x4x8 x8x4x4 x16	Выбор разделения портов 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 12.2.2.10.1.1.	Настройки, связанные с портом PCI Express 0-10
Порт PCI Express 1b	См. раздел 12.2.2.10.1.1.	Настройки, связанные с портом PCI Express 0-10
Порт PCI Express 2a	См. раздел 12.2.2.10.1.1.	Настройки, связанные с портом PCI Express 0-10
PCI Express Port 2c	См. раздел 12.2.2.10.1.1.	Настройки, связанные с портом PCI Express 0-10
Порт PCI Express 3a	См. раздел 12.2.2.10.1.1.	Настройки, связанные с портом PCI Express 0-10
Порт PCI Express 3c	См. раздел 12.2.2.10.1.1.	Настройки, связанные с портом PCI Express 0-10

12.2.2.10.1.1 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

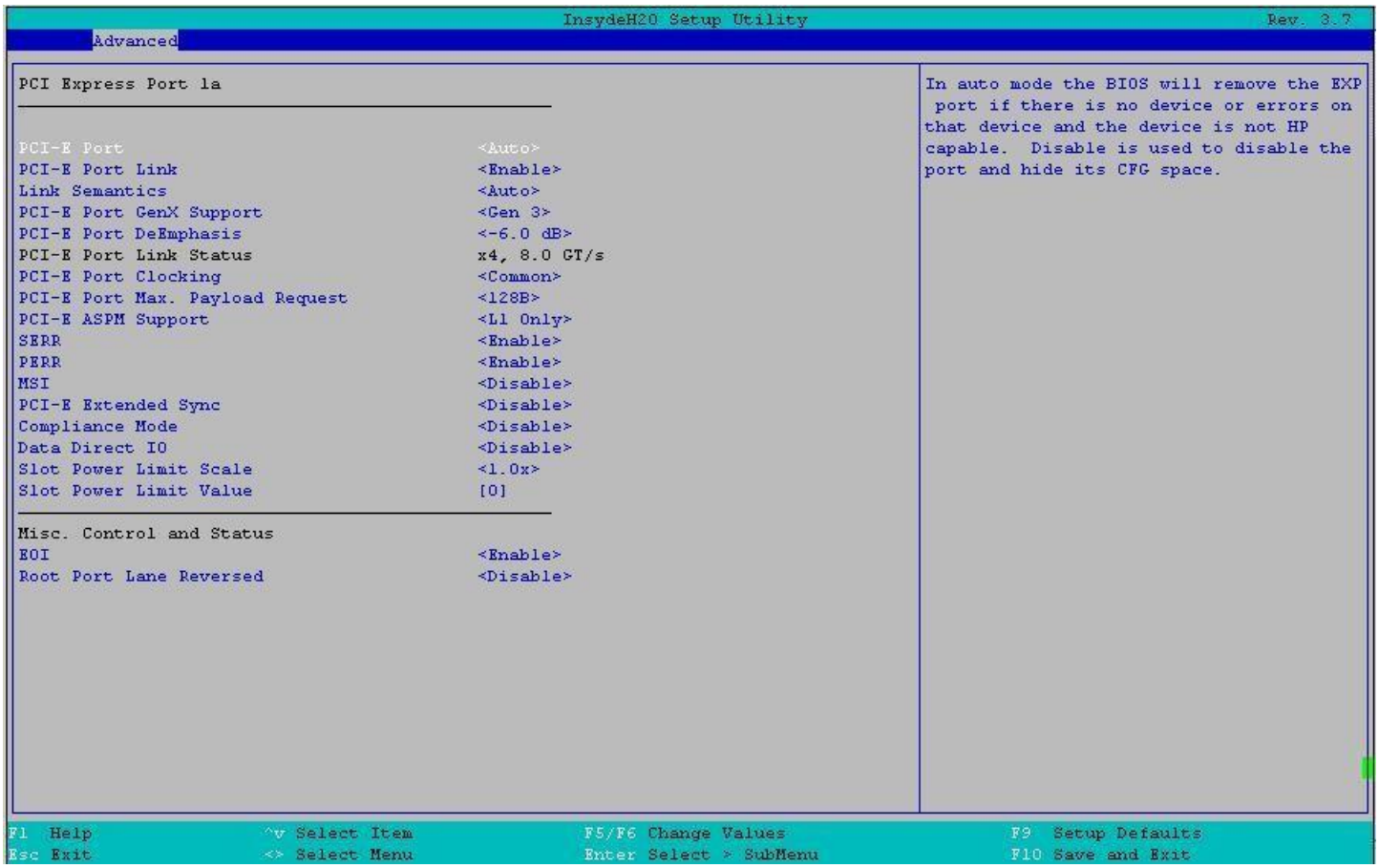


Рисунок 54

Настройка BIOS	Опции	Описание
PCI-E Port	Авто Включить Отключить	В автоматическом режиме BIOS удалит порт EXP
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	Force Link to Gen 1
PCI-E Port GenX support	Gen 1 Gen 2 Gen 3	ВыберитеподдержкугенерацииPCIедляпортаPCI Express. Gen1, пожалуйста, также установите De-Emphais = -6dB
PCI-E Port DeEmphasis	-6.0 дБ -3,5 дБ	Управление De-Emphais(LNKCON2[6]) для данного порта PCIe.
PCI-E Port Link Status	Нет	Показать состояние соединения с портом

Настройка BIOS	Опции	Описание
PCI-E Port Clocking	Distinct Common	Это относится к этим компонентам и компоненту нисходящего потока.
PCI-E Port Max. Payload Request	128B 256B Авто	Установите размер Maxpayload равным 256B, 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 0-9
Compliance Mode	Отключить Включить	Отключение/заключение режима соответствия для данного порта PCIe
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	Устройство 1-10 MISCCTRLSTS (Reg 0x188) Bit 26
Root Port Lane Reversed	Отключить Включить	Force root port to do Lane Reversal

12.2.2.10.2 Advanced/SandyBridge IIO/ SandyBridge General Configuration

Расширенные настройки/SandyBridge IIO/SandyBridge общая конфигурация

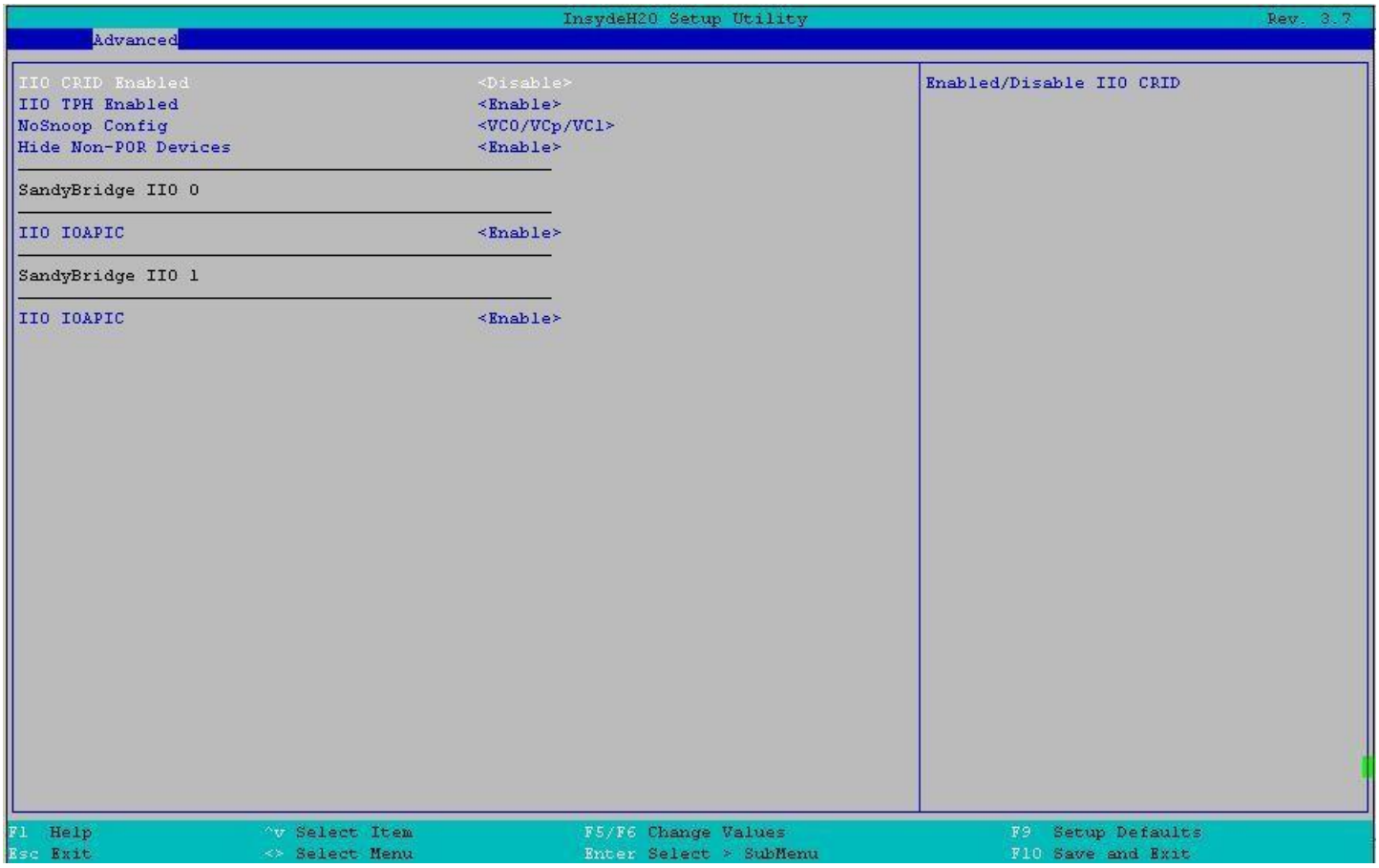


Рисунок 55

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,VC1,VCp
Hide Non-POR Devices	Отключить Включить	Скрыть не-POR устройства
IIO IOAPIC	Отключить Включить	Разрешить/Отключить IIO IOAPIC

12.2.2.10.3 Advanced/SandyBridge IIO/ Intel VT для прямого ввода-вывода (VT-d)

Расширенные настройки/SandyBridge IIO/Intel VT для прямого ввода/вывода (VT-d)

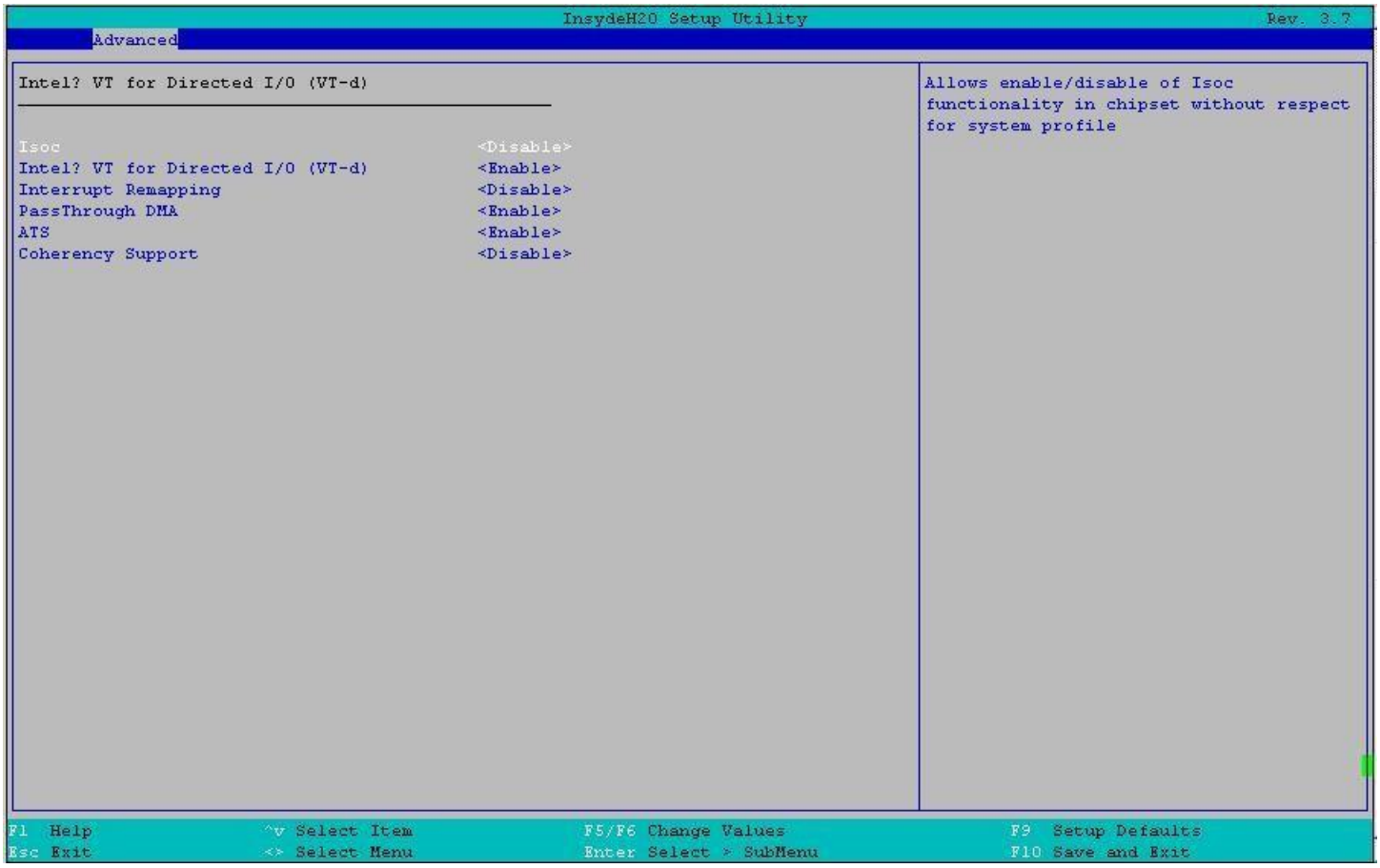


Рисунок 56

Настройка BIOS	Опции	Описание
Isoc	Включить Отключить АВТО	Позволяет включать/выключать функциональностьIsocв чипсетебезучета профиля системы.
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 Поддержка переопределения прерываний
PassThrough DMA	Включить Отключить	Включение/выключение не-Iscoh VT_D Двигателя, проходящего через поддержку DMA
ATS	Включить Отключить	Включение/выключение поддержки не-Iscoh VT_D Двигатель ATS
Coherency Support	Включить Отключить	Включение/выключение Non-Iscoh VT_D Engine Coherency support

12.2.2.11 Advanced/SandyBridge RC

Расширенные настройки/SandyBridge RC

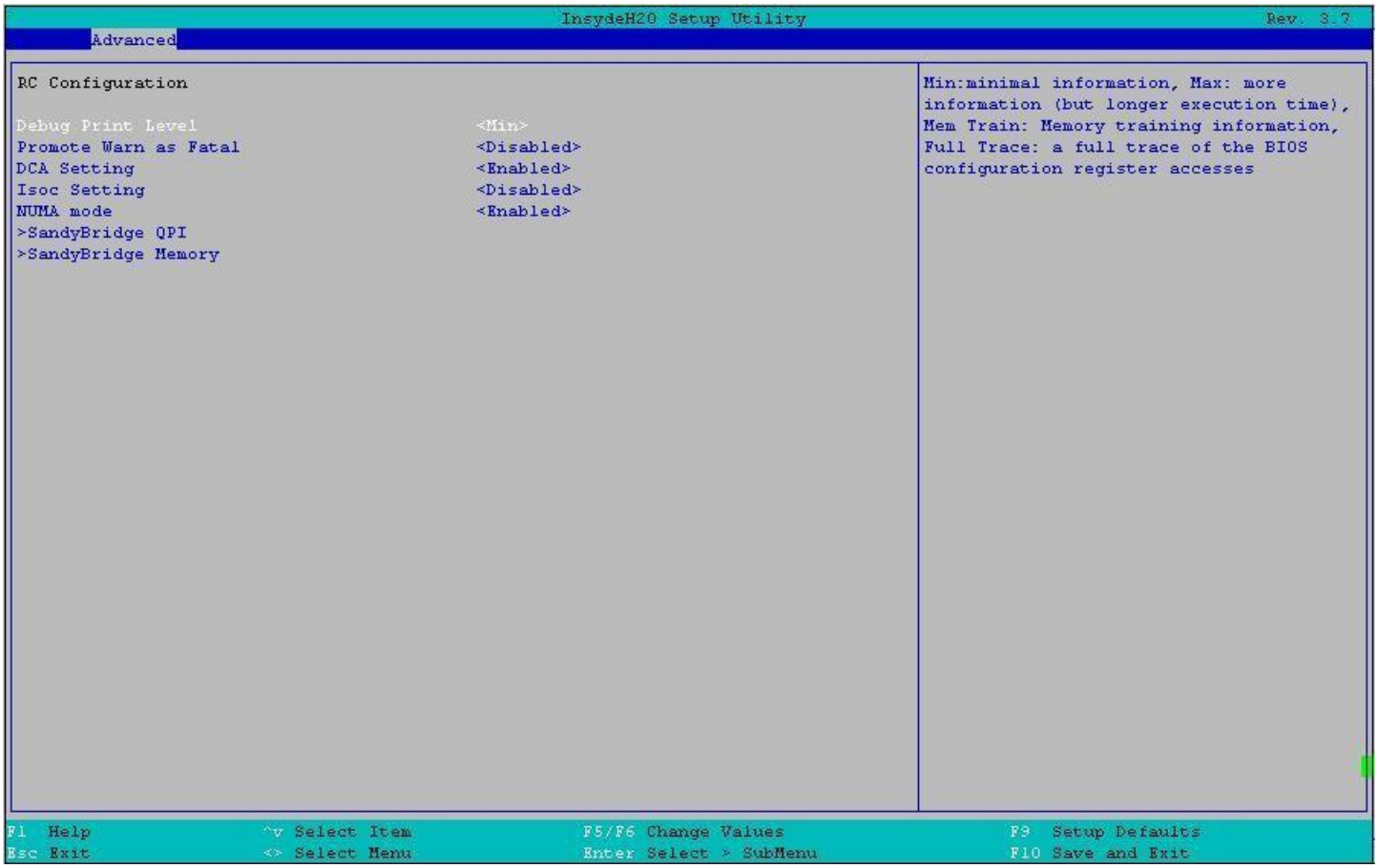


Рисунок 57

Настройка BIOS	Опции	Описание
Debug Print Level	Отключить Мин Max Полная трассировка Mem Train	Min: минимальная информация, Max: больше информации (но более длительное время выполнения), Mem Train: информация о тренировке памяти, Full Trace: полная трассировка обращений к регистру конфигурации BIOS
Promote Warn as Fatal	Включить Отключить	Promote warnning as fatal error
DCA Setting	Включить Отключить	Включить/выключить DCA
Isoc Setting	Включить Отключить	Включить/выключить Isoc, (BIOS заставит отключиться для 4 Socket case)
NUMA mode	Включить Отключить	Отключить: режим NUMA
>SandyBridge QPI	См. раздел 12.2.2.11.1.	Относительная настройка QPI
>SandyBridge Memory	См. раздел 12.2.2.11.2.	Относительная настройка памяти

12.2.2.11.1 Advanced/SandyBridge RC/SandyBridge QPI

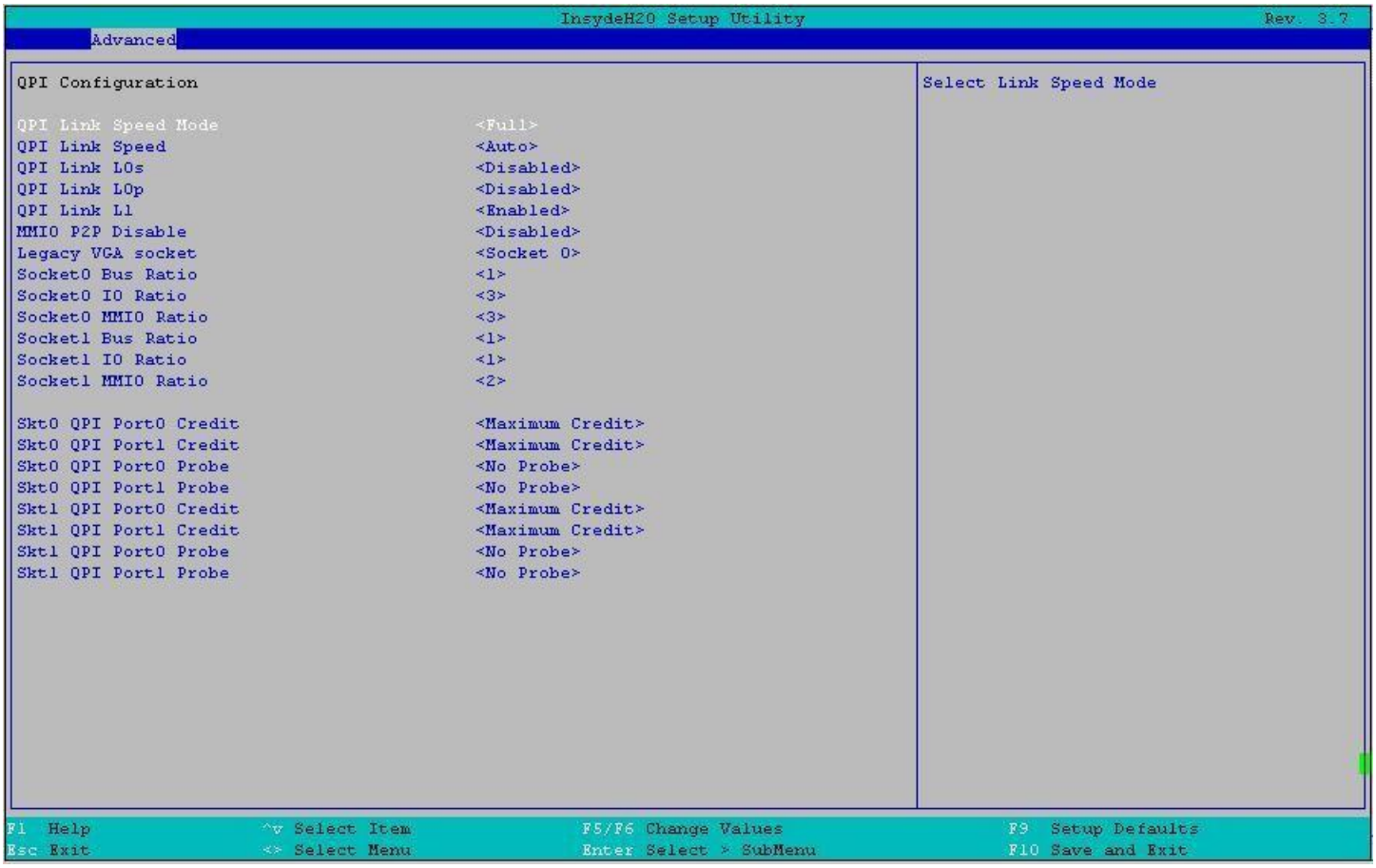


Рисунок 58

Настройка BIOS	Опции	Описание
QPI Link Speed Mode	Медленный Быстрый	Выбор режима скорости соединения
QPI Link Speed	Авто 6.4GTs 7.2GTs 8.0GTs	Выберите скорость соединения: 6.2GTs/7.2GTs/8.0GTs
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
MMIO P2P Disable	Отключено / Включено	Эта опция контролирует P2P-трафик через сокеты. Это не влияет на P2P-трафик. Значение 0 включит P2P; Значение 1 отключит P2P
Legacy VGA socket	Socket 0 Socket 1 Socket 2 Socket 3	Выбор legacy VGA socket
Socket0/1 Bus Ratio	1 2 3 4	Configure Socket 0/1 bus ratio
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	To force reduced link credit operation
Skt0/1 QPI Port 0/1 Probe	No Probe COHASSET VSR	To specify a midbus type probe.

12.2.2.11.2 Advanced/SandyBridge RC/SandyBridge Memory

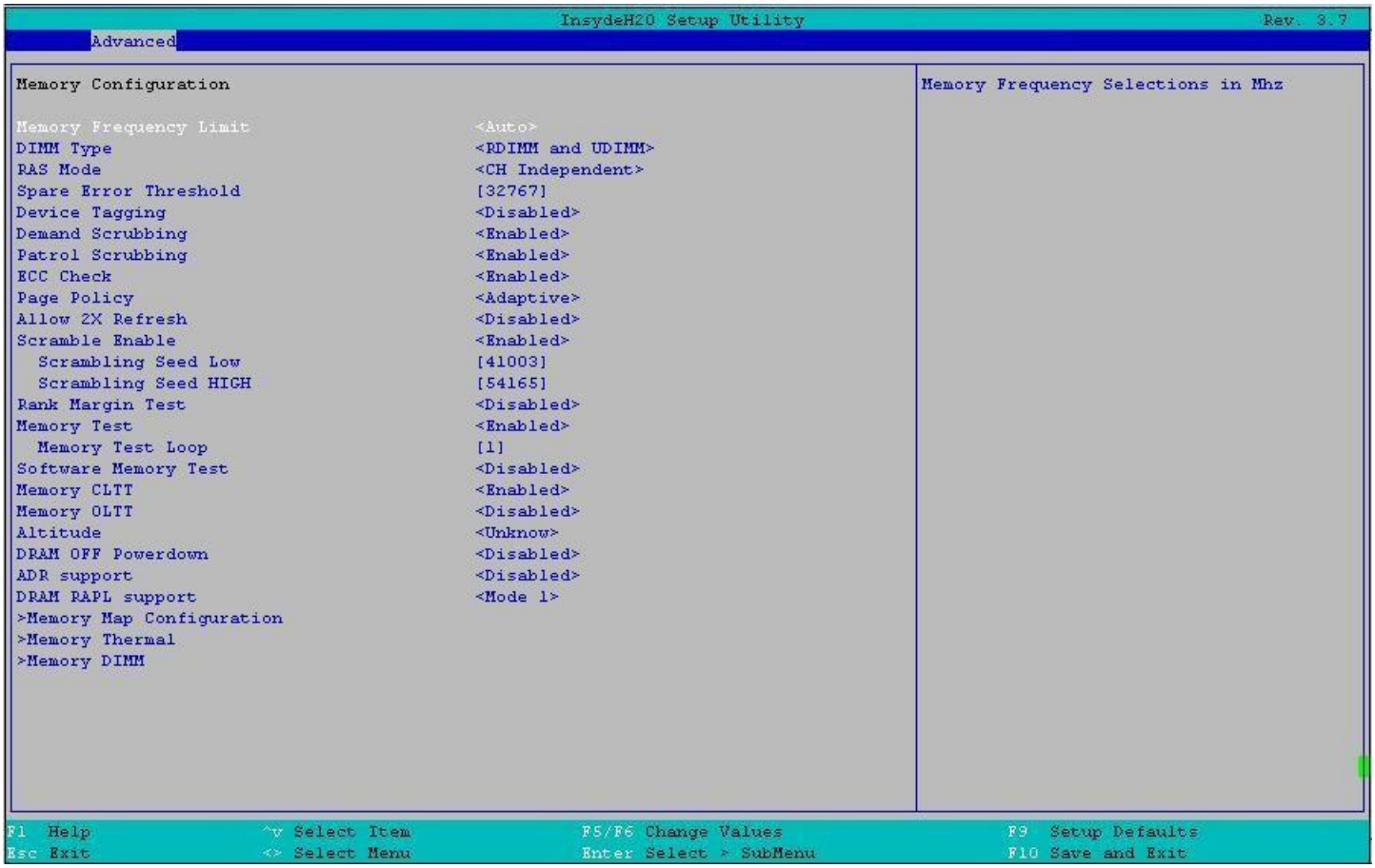


Рисунок 59

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
Spare Error Threshold	Отрегулируйте значение [1 – 32767]	Запасной 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 (32767). Максимальное значение 0x7FFF (32767).
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

Настройка BIOS	Опции	Описание
Page Policy	Закрыть открыть адаптивный	Выбор политики страницы
Allow 2X Refresh	Включено Отключено	Включить/выключить 2X обновление
Scramble Enable	Включено Отключено	Включить/выключить схватку
Scrambling Seed Low	Отрегулируйте значение [1 – 65535]	Низкий 32 бита посевного материала для шифрования данных
Scrambling Seed HIGH	Отрегулируйте значение [1 – 65535]	Высокие 32 бита зашифрованного посевного материала.
Rank Margin Test	Включено Отключено	Тест на разницу в уровне памяти, длина по умолчанию 1000
Memory Test	Включено Отключено	Включить тест памяти
Memory Test Loop	Отрегулируйте значение [1 – 65535]	Цикл тестирования памяти, минимум 1, максимум 65535.
Software Memory Test	Включено Отключено	Включить тест памяти программного обеспечения
Memory CLTT	Включено Отключено	Включить/выключить CLTT памяти
Memory OLTT	Включено Отключено	Включить/выключить память OLTT
Altitude	Неизвестно 300m или менее 301m - 900m 901m - 1500m Выше 1500m	Selects the system altitude for memory thermal throttling calculations.
DRAM OFF Powerdown	Включено Отключено	When set, enables DRAM OFF Powerdown Slow Mode in DIMM when performing self refresh.
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 12.2.2.11.2.1	Относительная настройка карты памяти
>Memory Thermal	См. раздел 12.2.2.11.2.2	Память Тепловая относительная настройка
>Memory DIMM	См. раздел 12.2.2.11.2.3.1	Показывать/настраивать информацию о DIMM-памяти

12.2.2.11.2.1 Advanced/SandyBridge RC/.../Memory Map Configuration

Конфигурация карты памяти

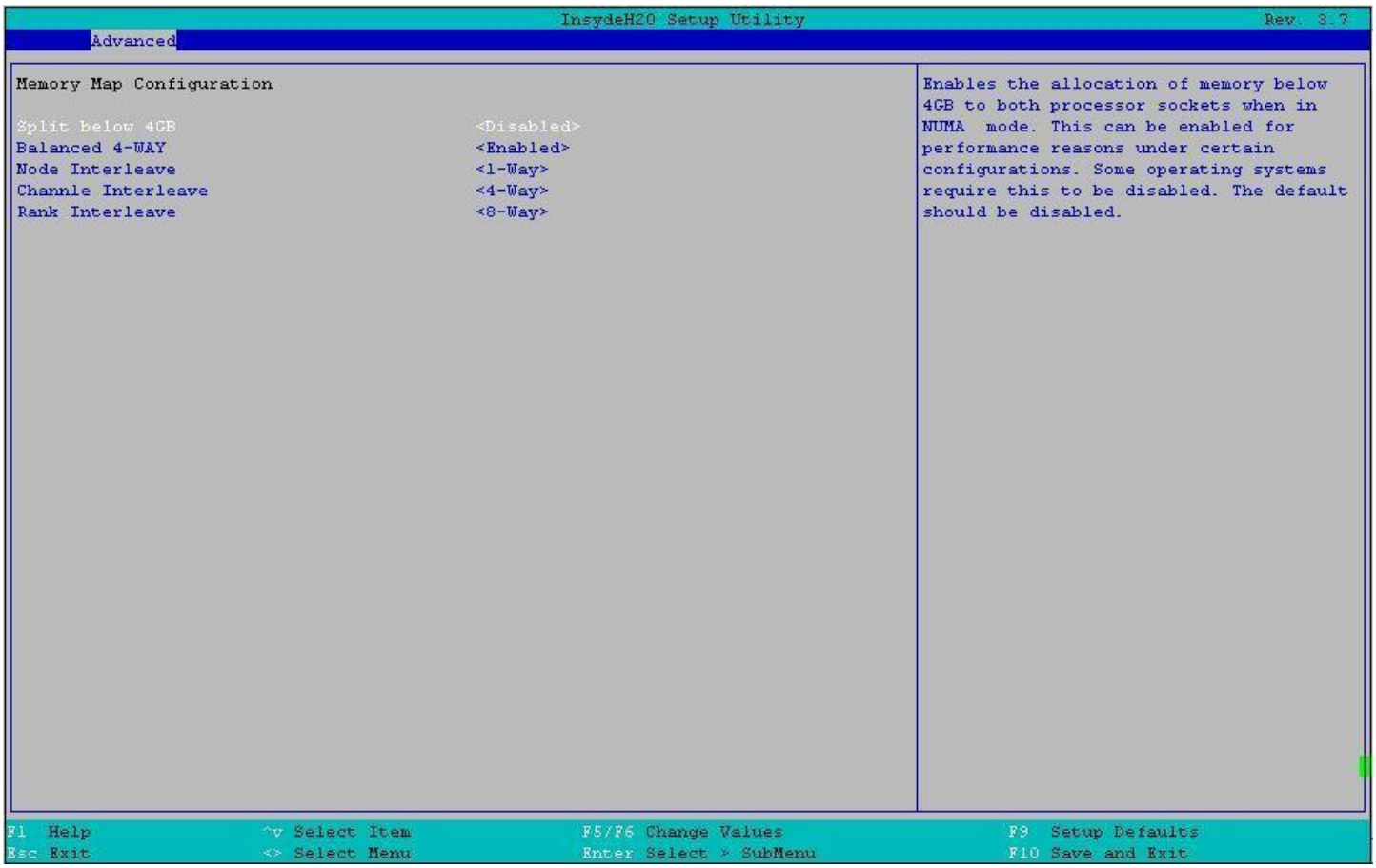


Рисунок 60

Настройка BIOS	Опции	Описание
Split below 4GB	Отключено Включено	Позволяет распределить память емкостью менее 4 Гб между обоими сокетами процессора в NUMA режим. Это может быть включено по причинам производительности при определенных конфигурациях. Некоторые операционные системы требуют, чтобы эта функция была отключена. Значение по умолчанию должно быть отключено
Balanced 4-WAY	Включено Отключено	Включает более оптимальный способ объединения не-NUMA DP платформ, имеющих конфигурацию каналов 2-1-1 (2 DIMM на один канал и 1 DIMM на два других канала). Если самые большие 2 канала находятся на разных разъемах и сумма 2 самых больших каналов больше, чем у следующих 4 каналов, а запланированный интерлейв равен 6, заставьте 4-полосную интерлейву, чтобы сделать производительность более симметричной.
Node Interleave	Авто 1-Way 2-Way 4-Way	Настройка чередования узлов
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 рангов чередования

12.2.2.11.2.2 Advanced/SandyBridge RC/.../Memory Thermal

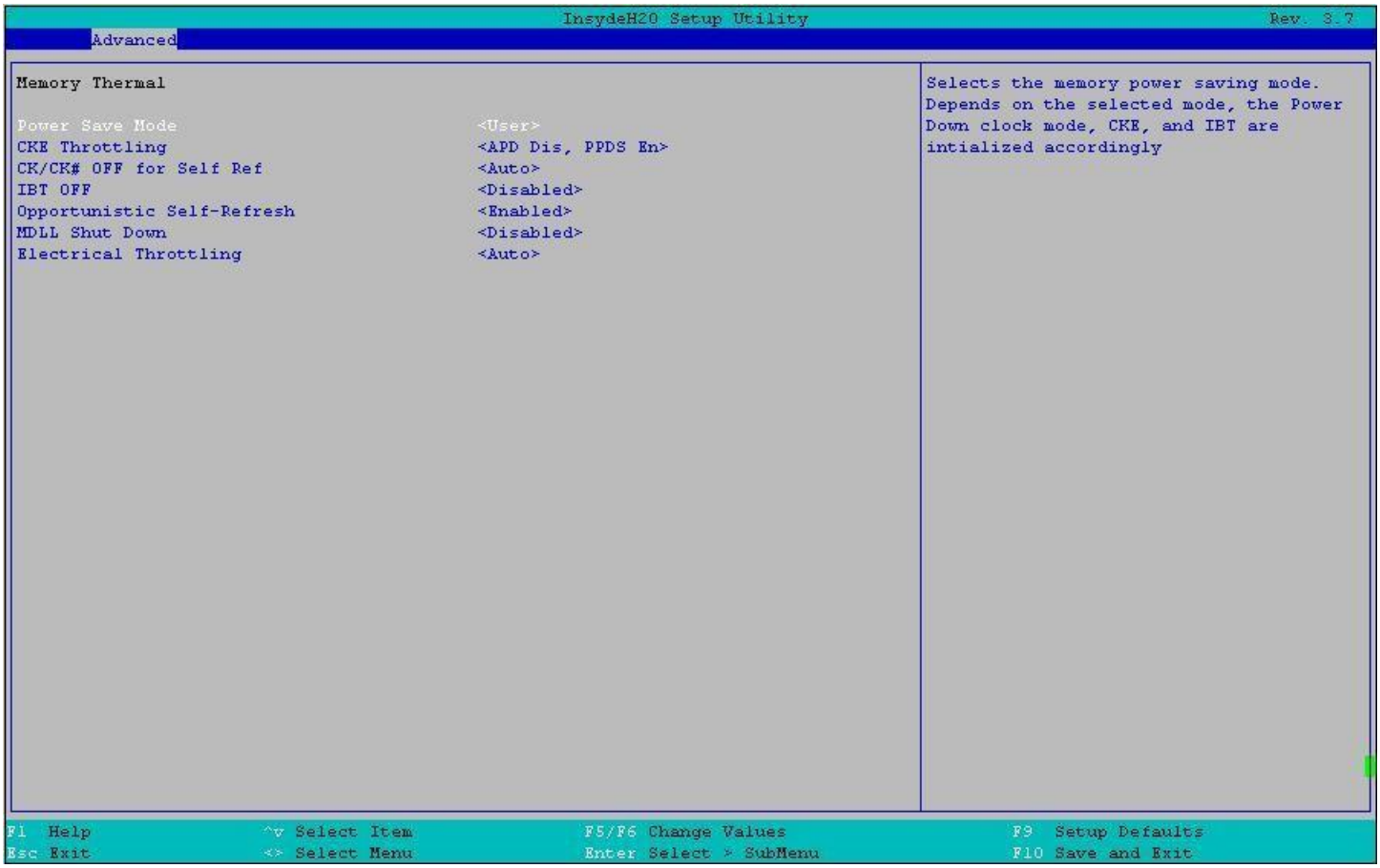


Рисунок 61

Настройка BIOS	Опции	Описание
Power Save Mode	Откл Медленный Быстрый Собственные настройки	Выбор режима энергосбережения памяти.
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	Выключение во время самообновления MDLL
Electrical Throttling	Включено Отключено Авто	Настройка электрического регулирования памяти

12.2.2.11.2.3 Advanced/SandyBridge RC/.../Memory DIMM

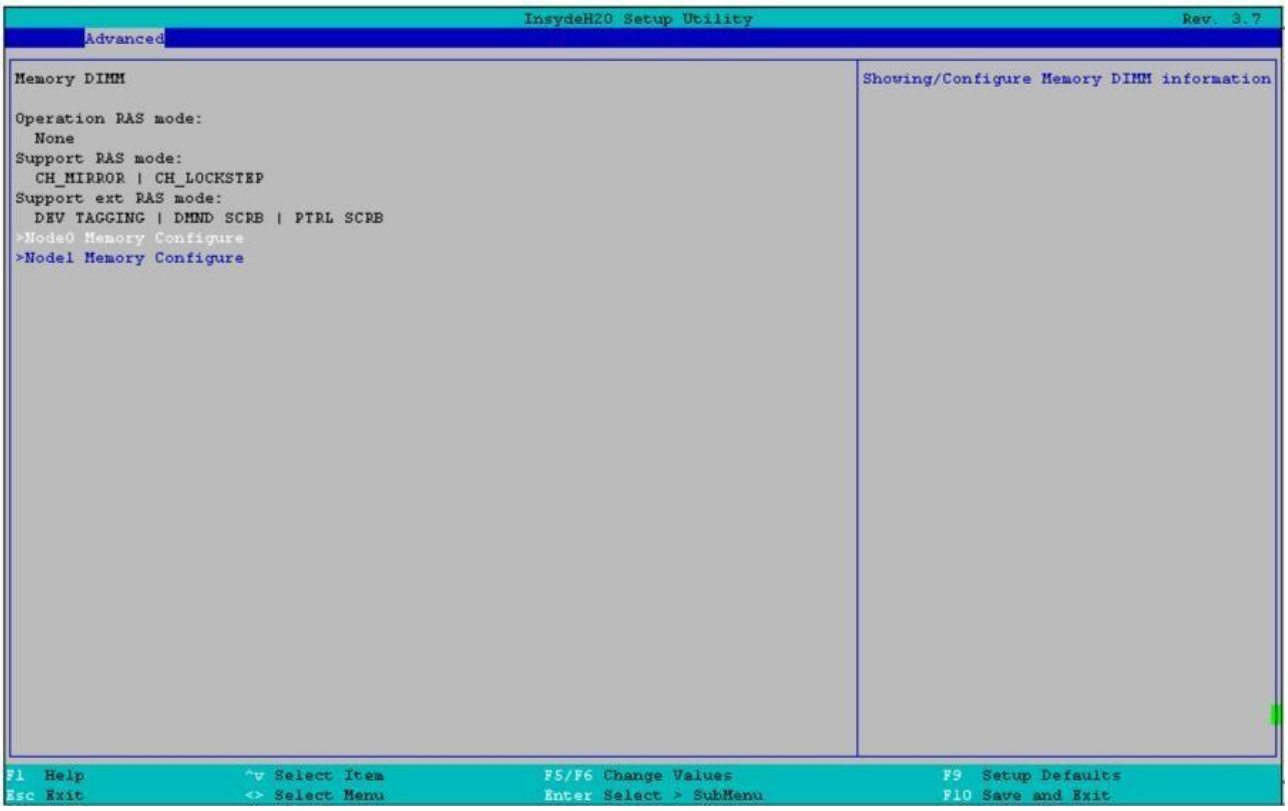


Рисунок 62

Настройка BIOS	Опции	Описание
>Node0 Memory Configure	См. раздел 12.2.2.11.2.3.1.	Показывать/настраивать информацию о DIMM-памяти
>Node1 Memory Configure	См. раздел 12.2.2.11.2.3.1.	Показывать/настраивать информацию о DIMM-памяти

12.2.2.11.2.3.1 Advanced/SandyBridge RC/.../Memory DIMM/Node0, 1 MEM CFG

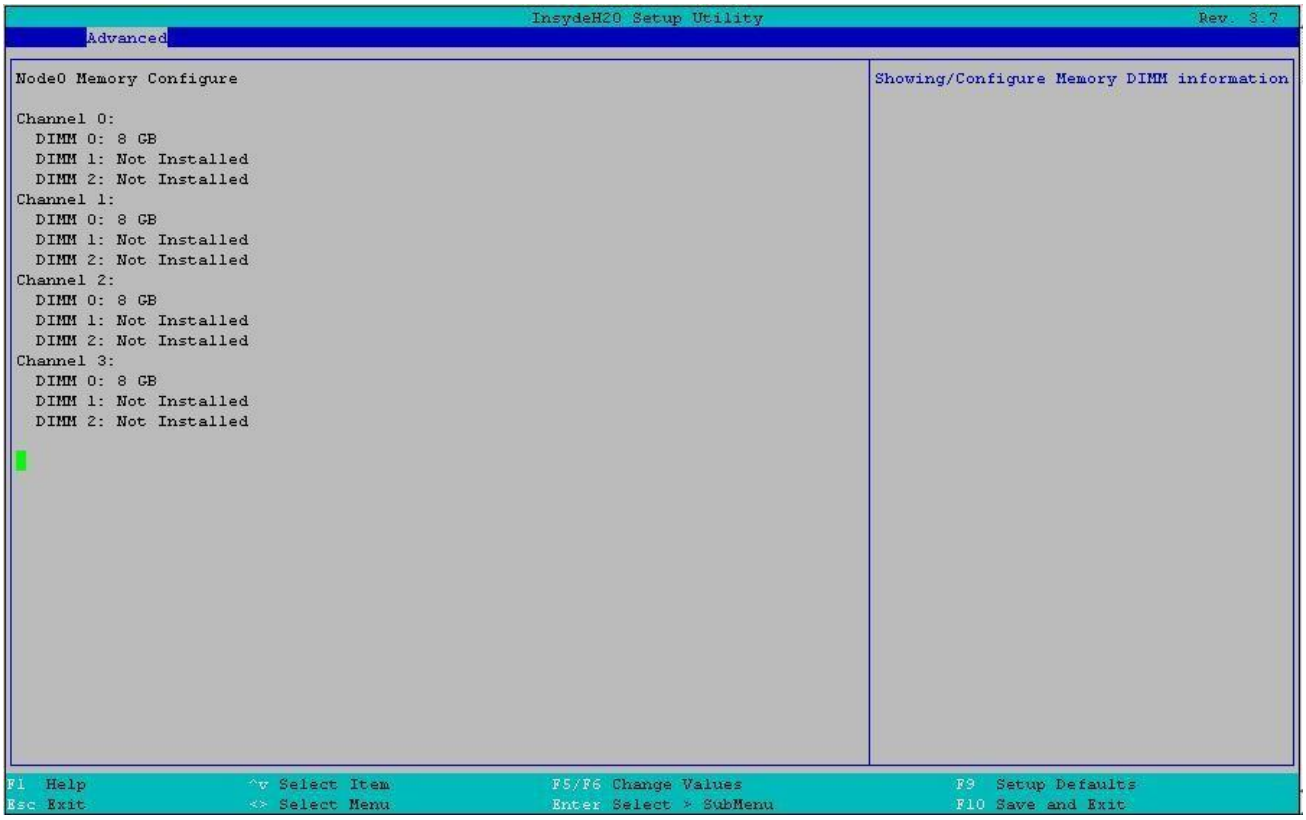


Рисунок 63

12.2.2.12 Advanced/ACPI Table/Features Control

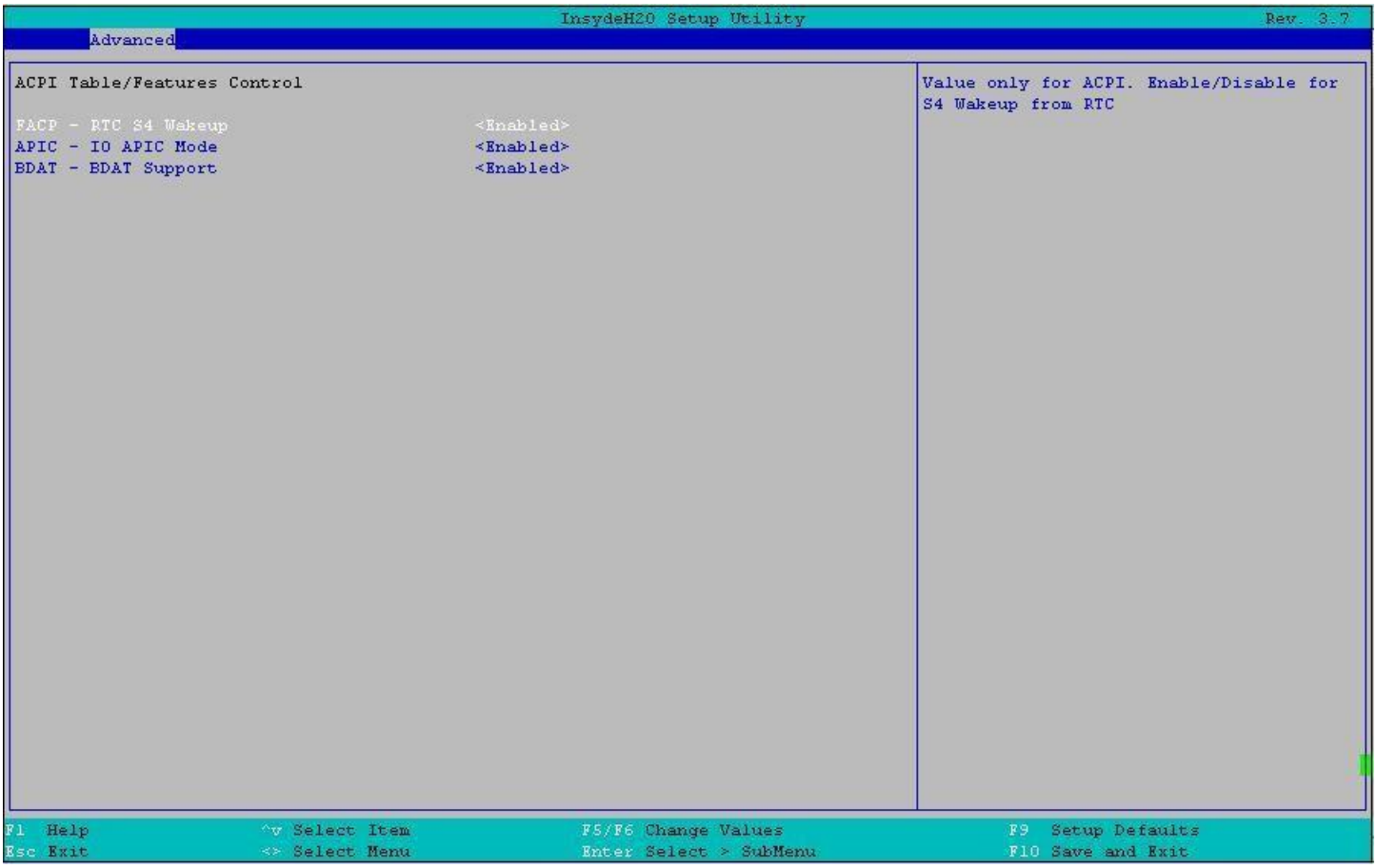


Рисунок 64

Настройка BIOS	Опции	Описание
FACP – RTC S4 Wakeup	Отключено Включено	Значение только для ACPI. Разрешить/запретить для S4 Wakeup from RTC
APIC – IO APIC Mode	Отключено Включено	Этот элемент действителен только для WIN2k и WINXP. Также, новая установка ОС должна произойти, когда APIC режим необходим. протестируйте IO ACPI, установив параметр Enable. the APIC Table будет затем указан RSDT, локальный APIC будет инициализирован, и соответствующие биты разрешения будут установлены в ICH4M.
BDAT – BDAT Support	Отключено Включено	Включение/Отключить публикацию таблицы ACPI BDAT

12.2.2.13 Advanced/Console Redirection

Расширенные настройки/Переадресация консоли.

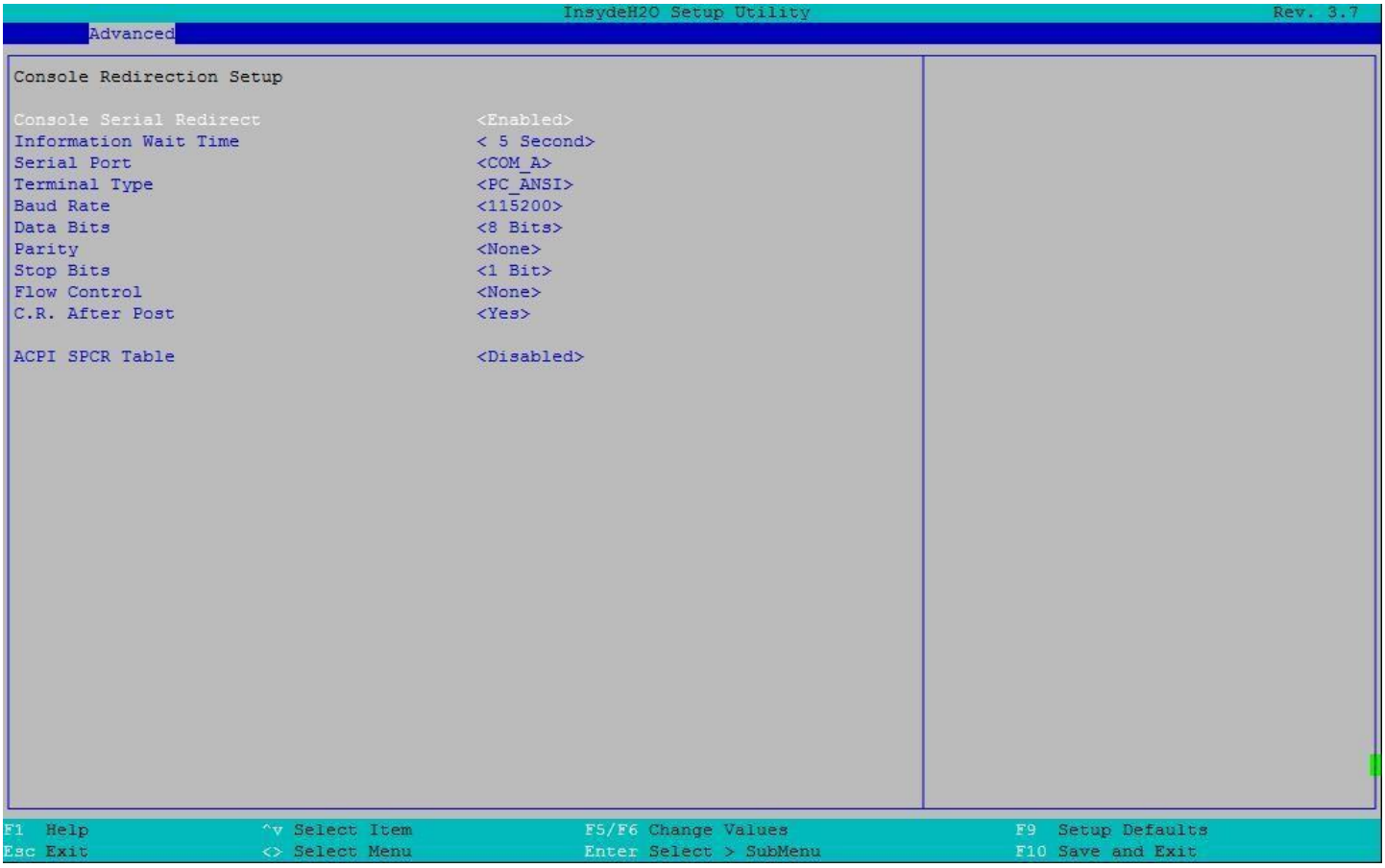


Рисунок 65

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	Решите, как долго будет ожидание, пока загрузится OPROM перенаправления консоли.
Serial Port *(Последовательный порт)*	COM_A COM_B COM_B COM_C COM_D Все порты	Решите, какой последовательный порт будет перенаправлением консоли. Только COM A/B/C/D или все последовательный порт (включая последовательный порт PCI)
Terminal Type *(Тип терминала)*	VT_100 VT_100 VT_100+ VT_UTF8 PC_ANSI	Установите тип терминала VT100/VT100 +/UTF8/PC_ANSI.

Настройка BIOS	Опции	Описание
Baud Rate *(Скорость передачи данных)*	115200 57600 38400 19200 9600 4800 2400 1200	Установите скорость передачи данных последовательного порта на перенаправление консоли.
Data Bits *(Число битов в байте данных)*	7 бит 8 бит	Set Serial transaction data bits on serial port for Console Redirection.
Parity *(Паритет)*	None Event Odd	Установите параметр Событие паритета/Нечетный / Нет проверки на последовательном порту для переадресации консоли.
Stop Bits *(Количество стоп-битов)*	1 Bit 2 Bits	Установите Stop Bits на последовательном порту для перенаправления консоли.
Flow Control *(Управление потоком)*	None RTS/CTS Xon/Xoff	Установите управление потоком на последовательный порт для 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)

12.2.2.14 Advanced/APEI Configuration

Расширенные настройки/Конфигурация APEI

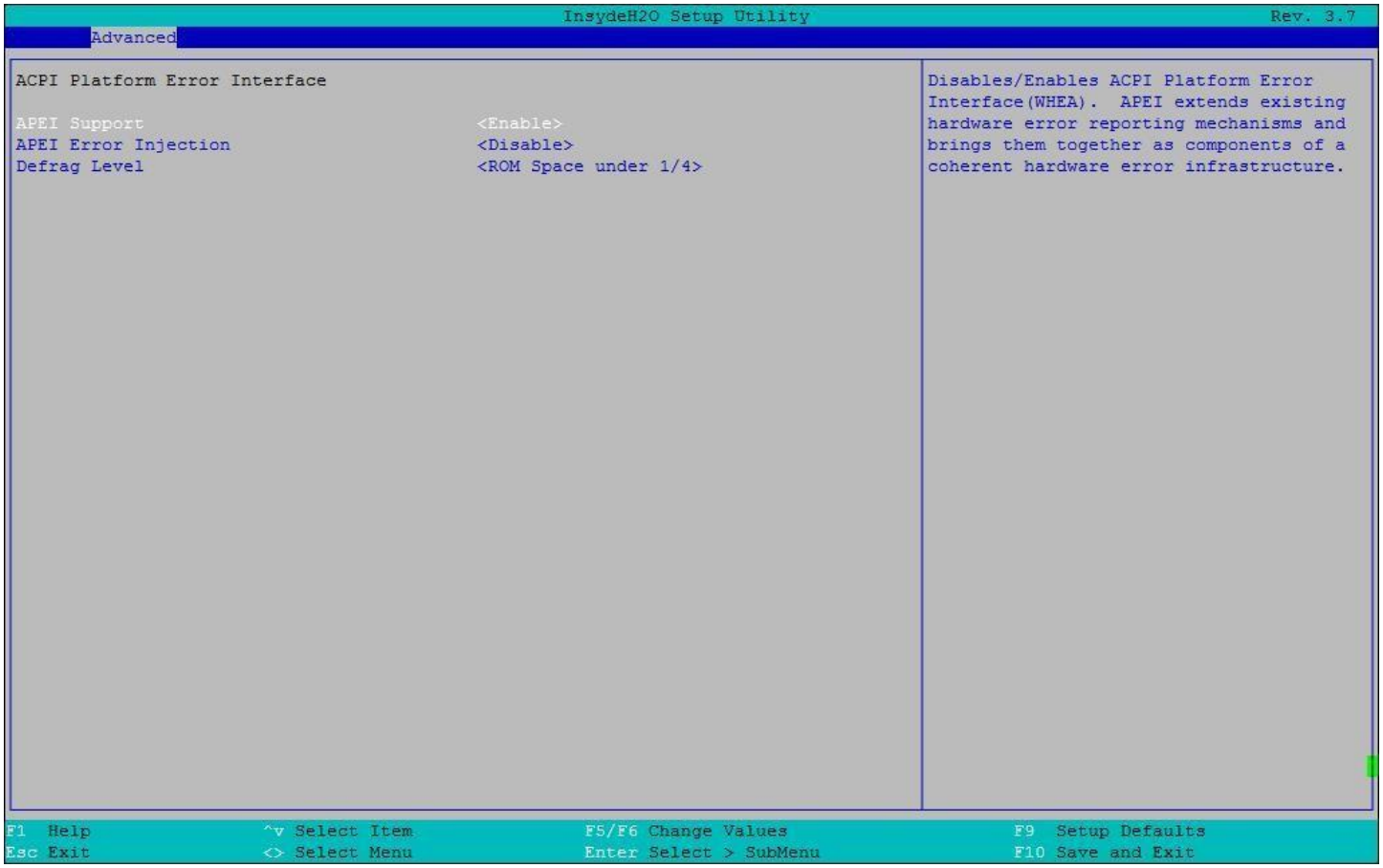


Рисунок 66

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_F ATAL MEMORY_ UE_FATAL PCIE_CE PCIE_UE_N ON_FATAL PCIE_UE_F ATAL	Введите ошибку, чтобы проверить функцию APEI
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

12.2.2.15 Advanced/RAS Configuration

Расширенные настройки/Конфигурация RAS

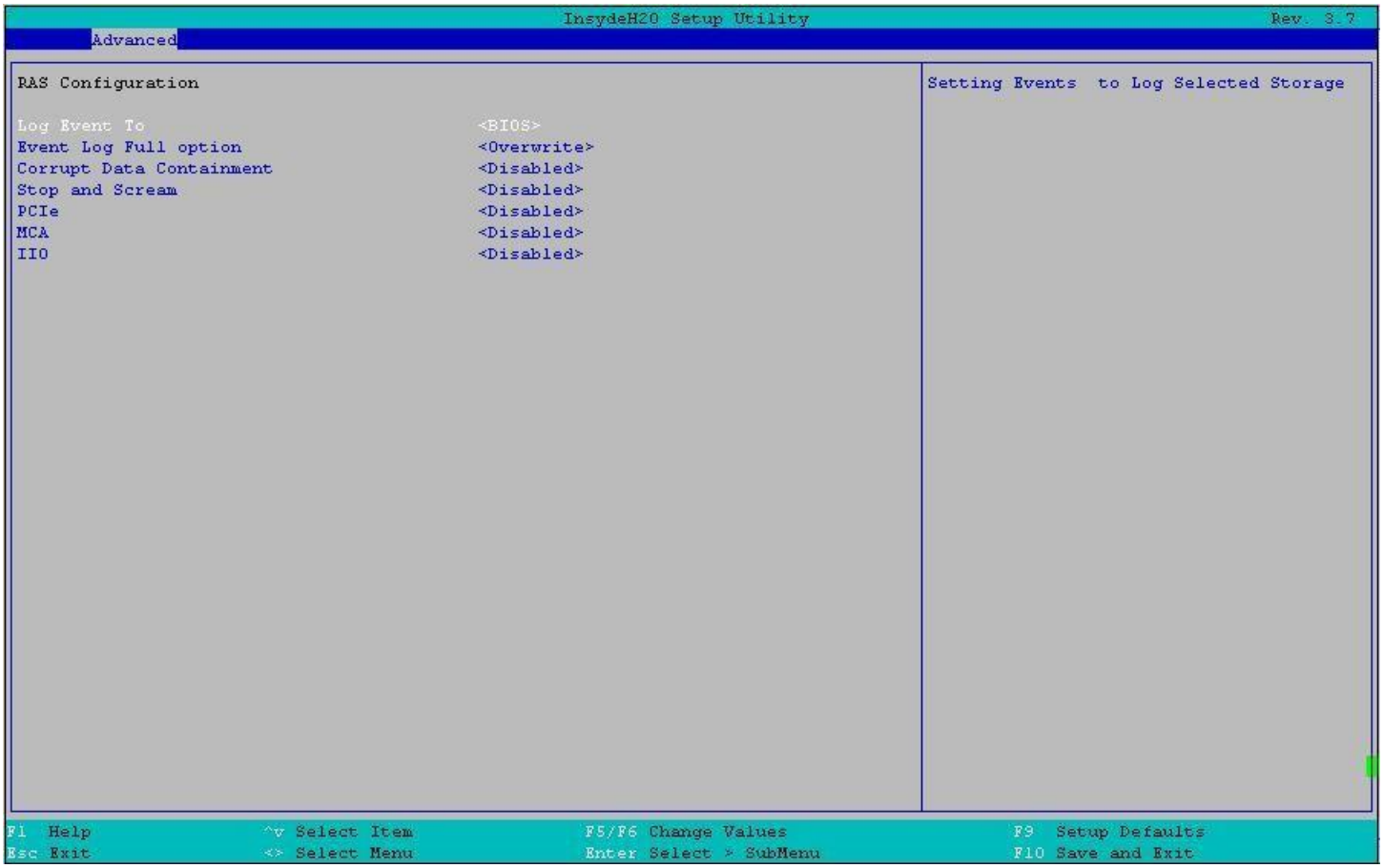


Рисунок 67

Настройка BIOS	Опции	Описание
Log Event To *(Войти в журнал)*	ALL BIOS BMC SEL DCMI SEL MEMORY	Настройка журнала событий на выбранное хранилище.
Event Log Full option *(Журнал событийПолный Вариант)*	Перезаписать Очистить все Стоп Logging	
Corrupt Data Containment *(Повреждение данных)*	Отключить Включить	Включить/выключить поврежденную защиту данных.
Stop and Scream *(защита от кражи)*	Отключить Включить	Включить/выключить
PCIe	Отключить Включить	Включение/выключение PCIe RAS.
MCA	Отключить Включить	Включение/выключение MCA RAS.
IIO	Отключить Включить	Включение/выключение IIO RAS.

12.2.2.16 Advanced/Event Message Setting

Расширенные настройки/Настройка сообщений о событии

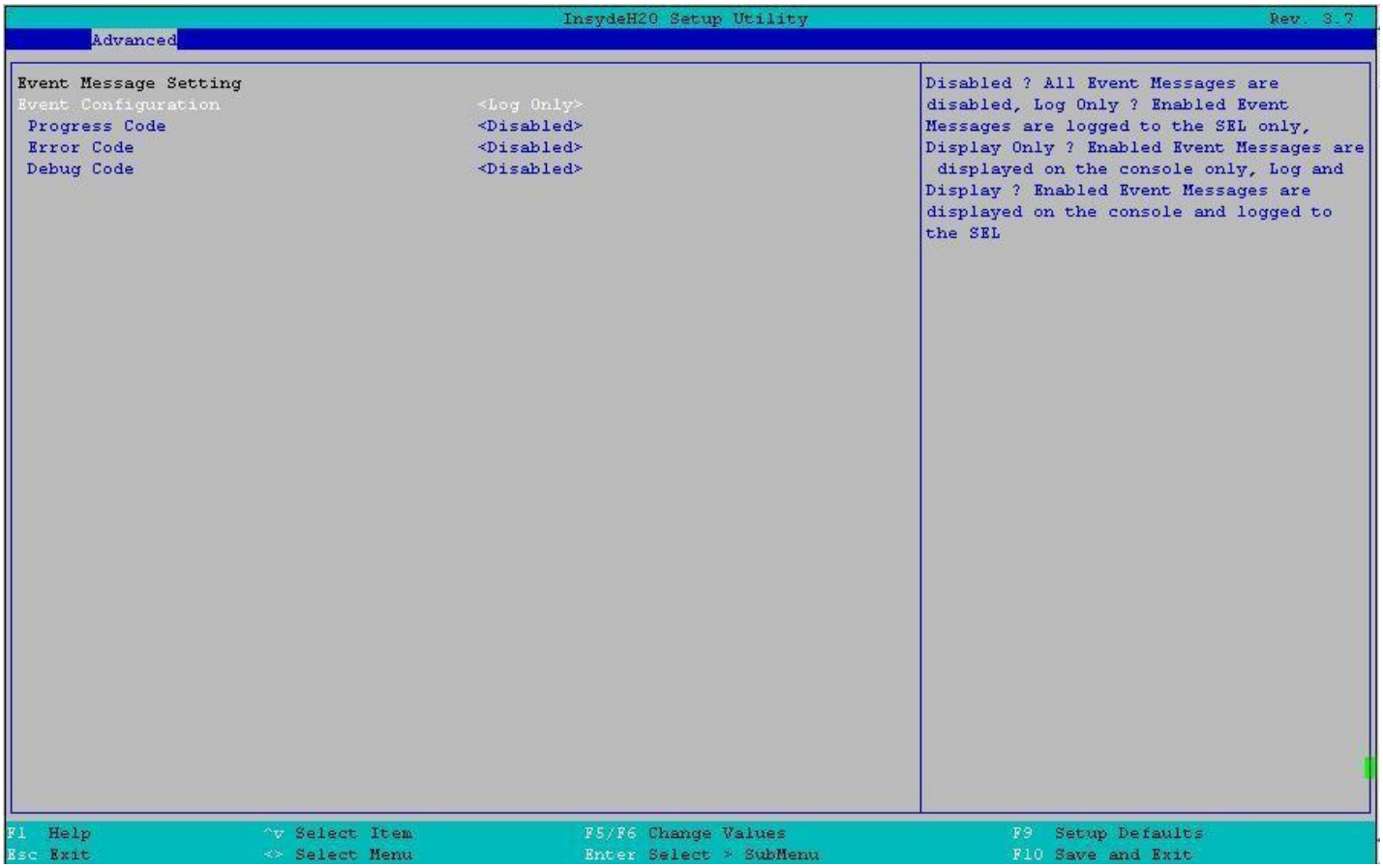


Рисунок 68

Настройка BIOS	Опции	Описание
Event Configuration *(Конфигурация события)*	Отключено Только журнал Только дисплей Журнал и Дисплей	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 включены в BIOS, сообщения с кодами прогресса отключены в BIOS.
Error Code *(Код ошибки)*	Отключено Включено	Сообщения с кодами ошибок включены в BIOS, сообщения с кодами ошибок отключены в BIOS.
Debug Code *(Отладочный код)*	Отключено Включено	Сообщения об отладке кода включены в BIOS, сообщения об отладке кода отключены в BIOS.

12.2.2.17 Advanced/Event Log Viewer

Расширенные настройки/Просмотр журнала событий

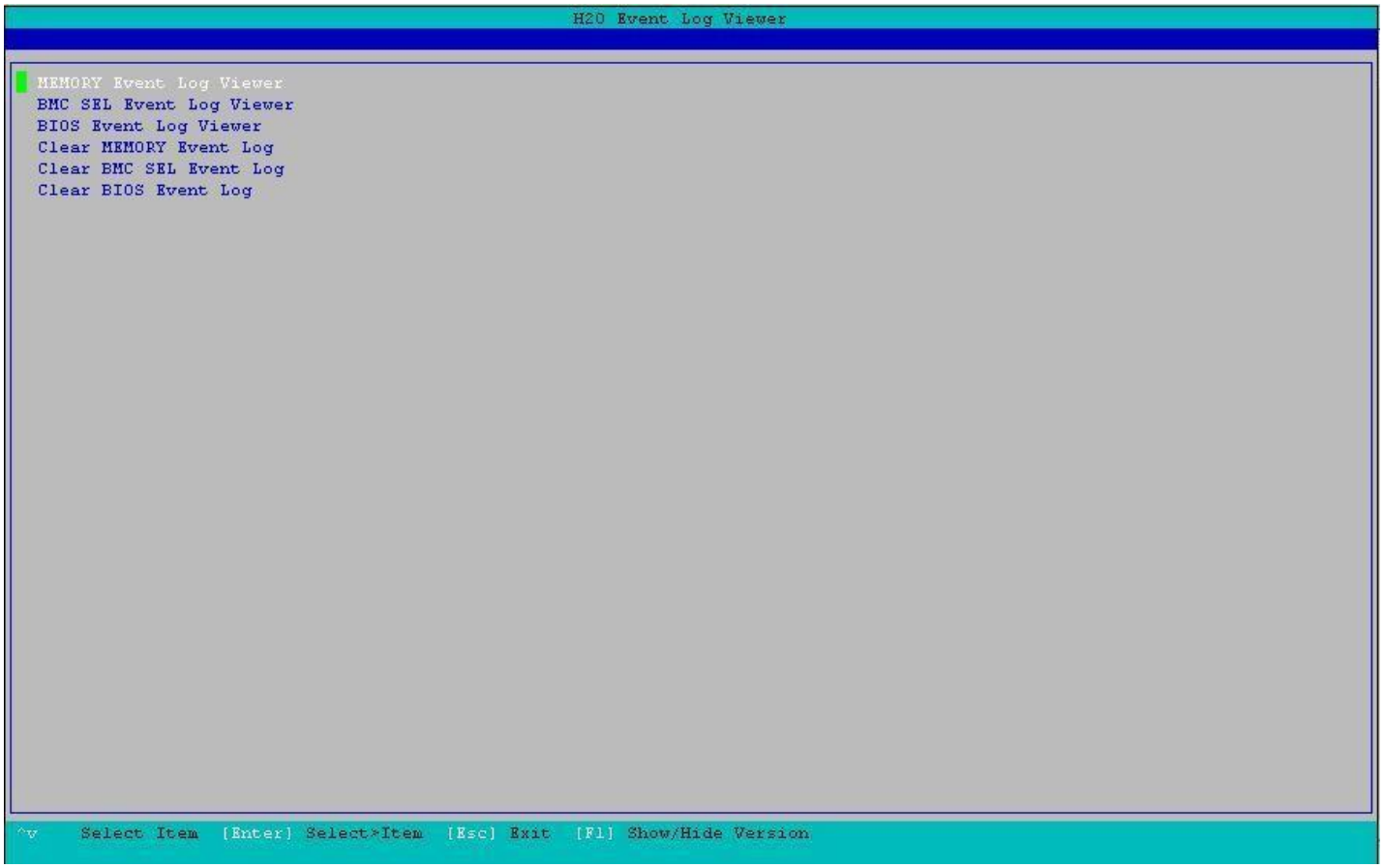


Рисунок 69

12.2.2.18 Advanced/IPMI BMC Configuration

Расширенная конфигурация BMC IPMI

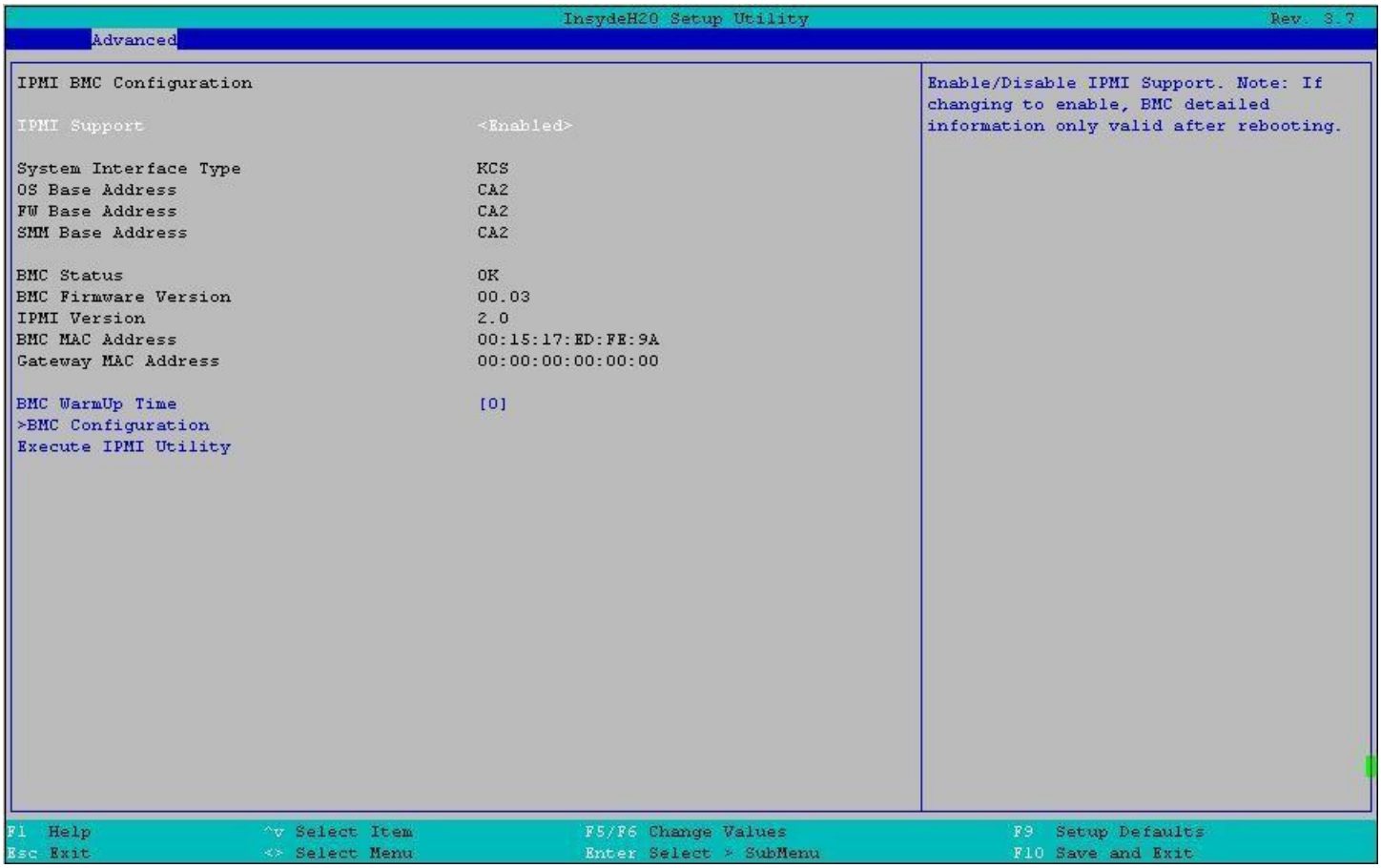


Рисунок 70

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.
System Interface Type *(Тип системного интерфейса)*	Нет	Показать тип системного интерфейса IPMI
OS Base Address *(Базовый адрес ОС)*	Нет	Показать, как ОС использует IO-порт для IPMI
FW Base Address *(Базовый адрес FW)*	Нет	Показать FW Использовать IO-порт для IPMI
SMM Base Address *(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

Настройка BIOS	Опции	Описание
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 12.2.2.18.1.	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

12.2.2.18.1 Advanced/IPMI BMC Configuration/ BMC Configuration

Расширенные настройки/Конфигурация IPMI BMC/Конфигурация BMC

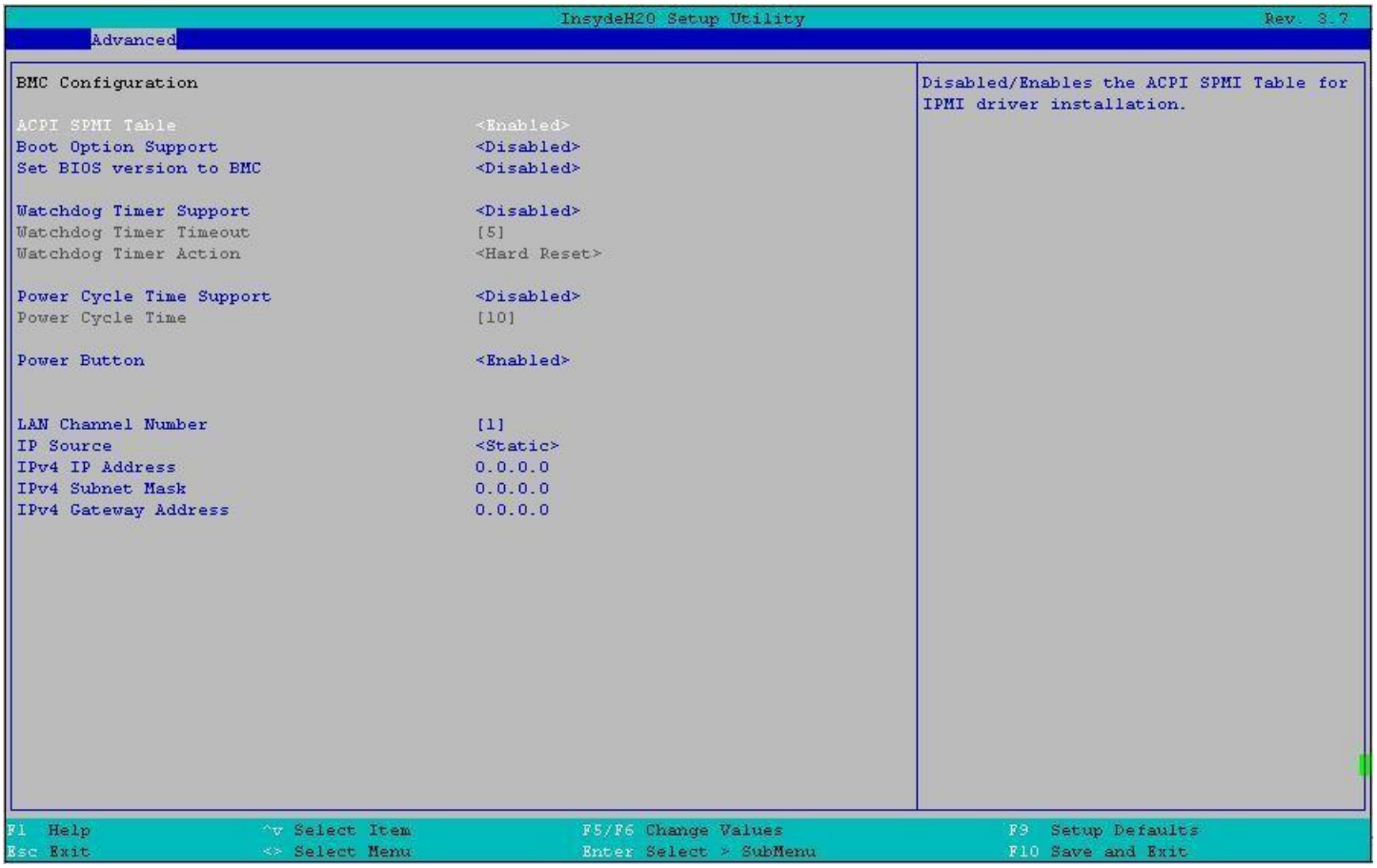


Рисунок 71

Настройка BIOS	Опции	Описание
ACPI SPMI Table *(Таблица ACPI SPMI)*	Отключить Включить	Отключить/Включает 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/выключениеустановкиверсииBIOS на BMC. Если опция включена, BMC сохранит версию bios.
Watchdog Timer Support	Отключить Включить	Enable/Disable Watchdog Timer When Booting
Watchdog Timer Timeout	Установите значение [2-8].	Введите количество минут, в течение которых системная прошивка должна загрузить ОС, прежде чем произойдет действие Timeout. Допустимые значения: от 2 до 8 минут.
Watchdog Timer Action	Жесткий сброс Выключить питание Перезагрузка	Выбор действия: Жесткий сброс, отключение питания или перезагрузка

Настройка BIOS	Опции	Описание
Power Cycle Time Support	Отключить Включить	Включение/выключение Отправить команду времени цикла питания в BMC во время POST
Power Cycle Time	Отрегулируйте 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	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

12.2.3 Security Menu

Меню безопасности

Меню Security предоставляет конфигурацию для настройки параметров безопасности системы:

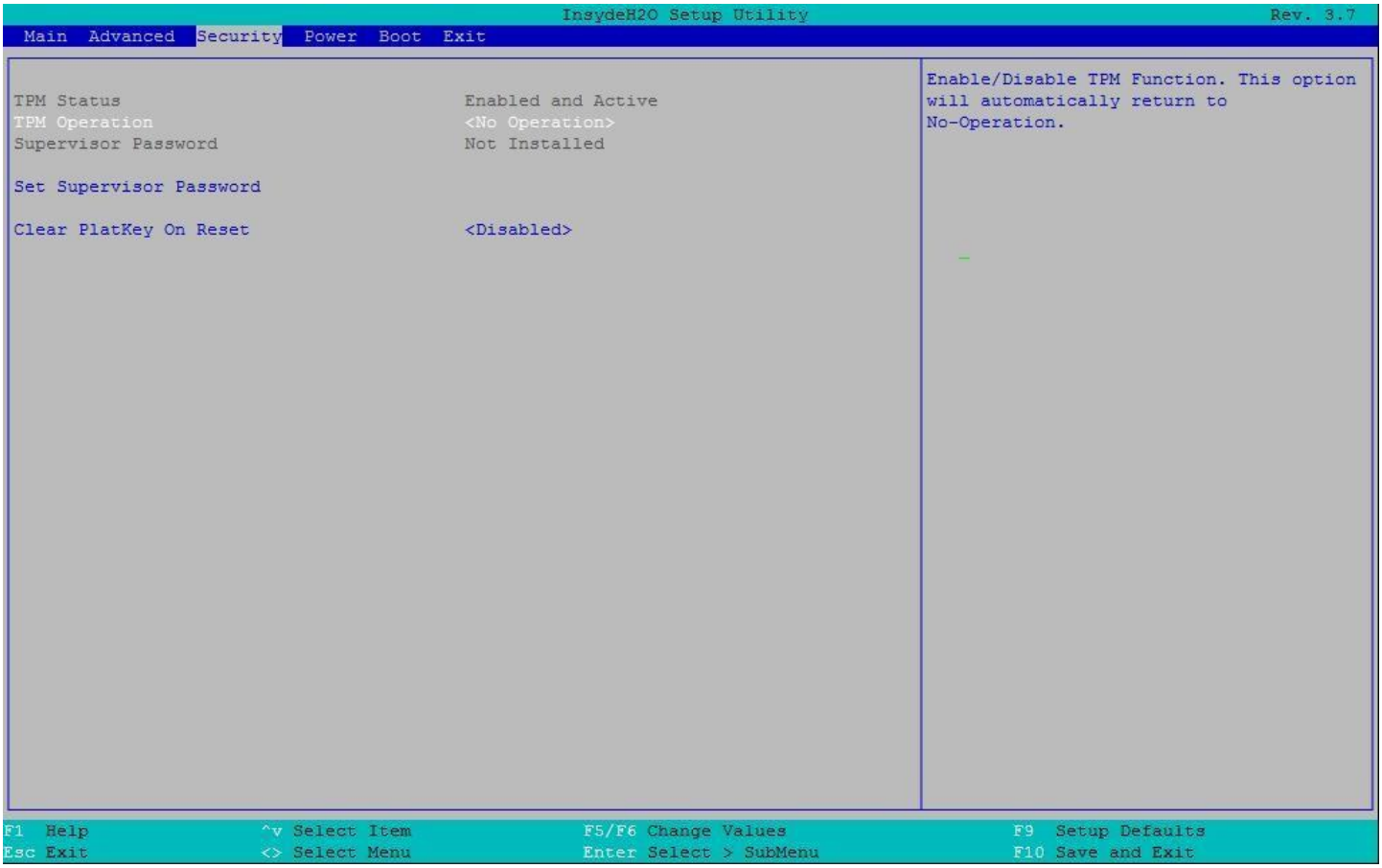


Рисунок 72

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 Админа
Clear PltKey On Reset *(Очистить PltKey при перезагрузке)*	Отключить Включить	Включить/Выключить очистку ключа безопасности платформы при перезагрузке

Установить пароль администратора

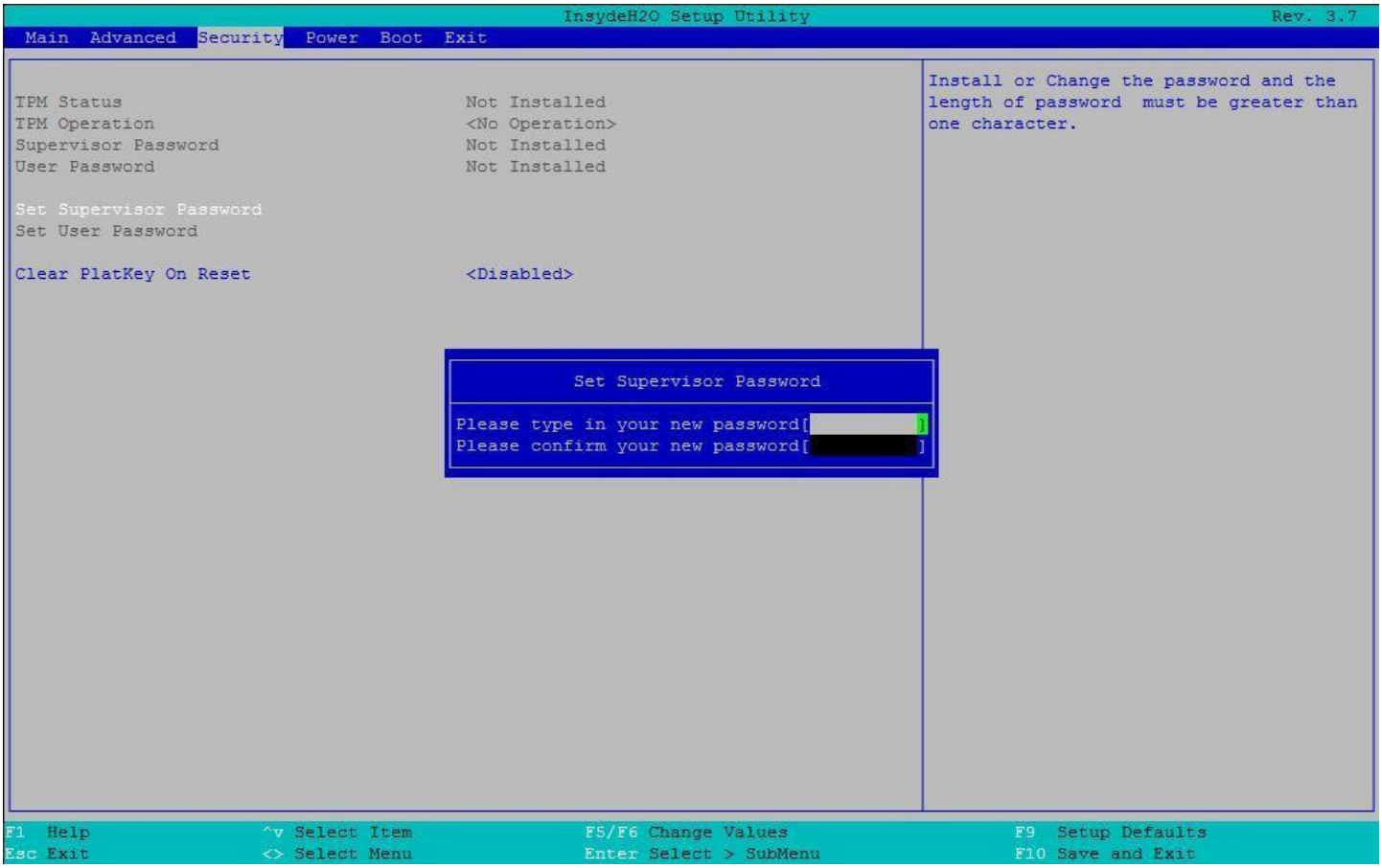


Рисунок 73. Установить пароль администратора

12.2.4 Power Menu

Меню электропитания

Меню «Power» (Рисунок 77) позволяет пользователям задавать или контролировать различные режимы управления электропитанием, температурой и спящим состоянием.

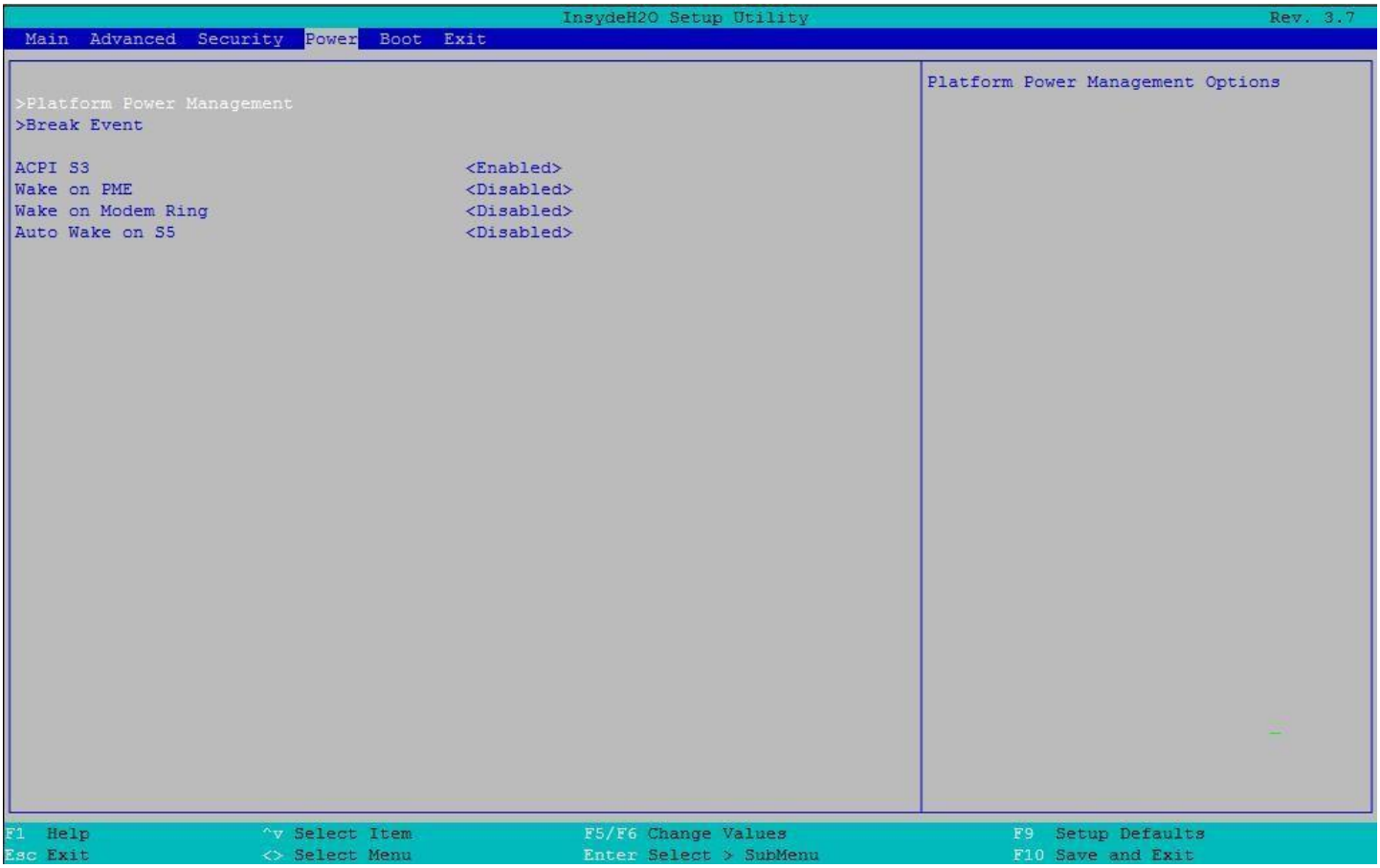


Рисунок 74. Меню электропитания

Настройка BIOS	Опции	Описание
Platform Power Management	См. раздел 12.2.4.1.	Управления электропитанием платформы
Break Event	См. раздел 12.2.4.2.	Goto the form controls break event parameters
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.

12.2.4.1 Power/Platform Power Management

Электропитание/Управление электропитанием платформы

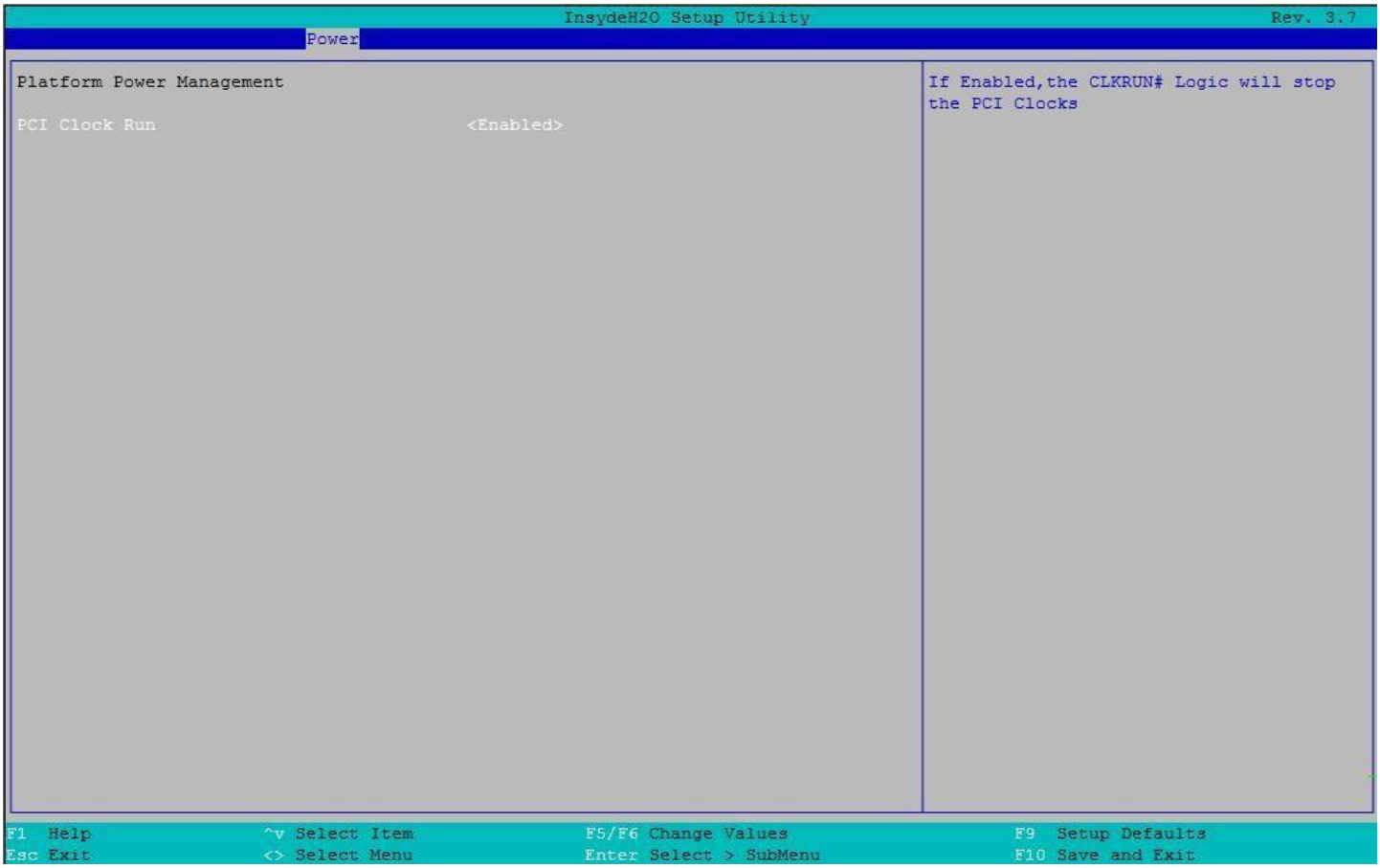


Рисунок 75

Настройка BIOS	Опции	Описание
PCI Clock Run *(Запуск часов PCI)*	Отключено Включено	Если включено, логика CLKRUN # остановит тактовый генератор PCI

12.2.4.2 Power/Break Event

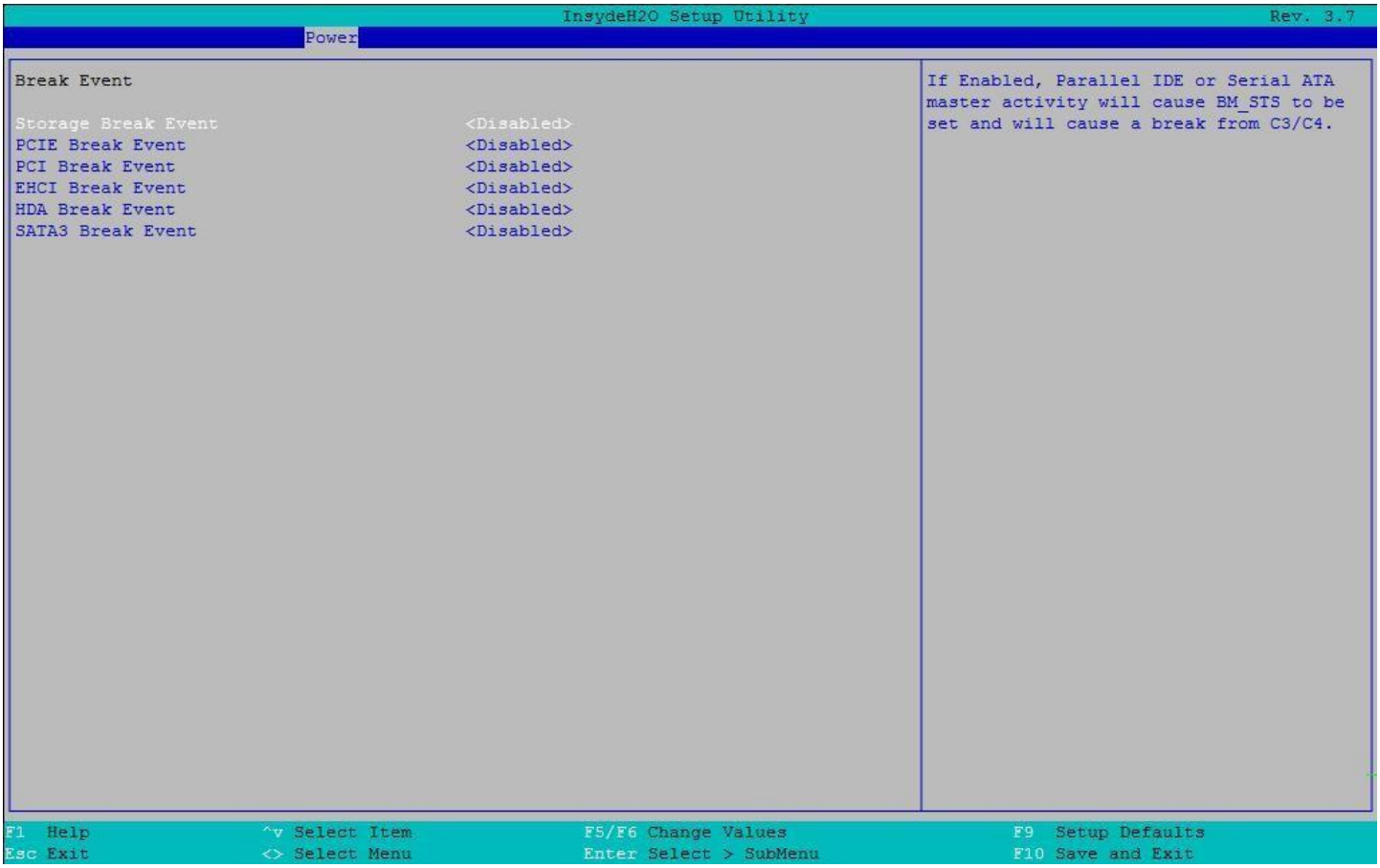


Рисунок 76

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 Enable (Включить), 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 Enable (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 аудио высокой четкости Intel приведет к установке BM_STS и отказу от C3/C4.
SATA 3 Break Event	Отключить Включить	Если Enable (Включить), активность ведущего устройства Intel SATA3 Master приведет к установке BM_STS и отказу от C3/C4.

12.2.5 Boot Menu

Загрузочное меню

Меню загрузки позволяет настроить настройки и последовательность загрузки загрузочного устройства. Оно включает следующее:

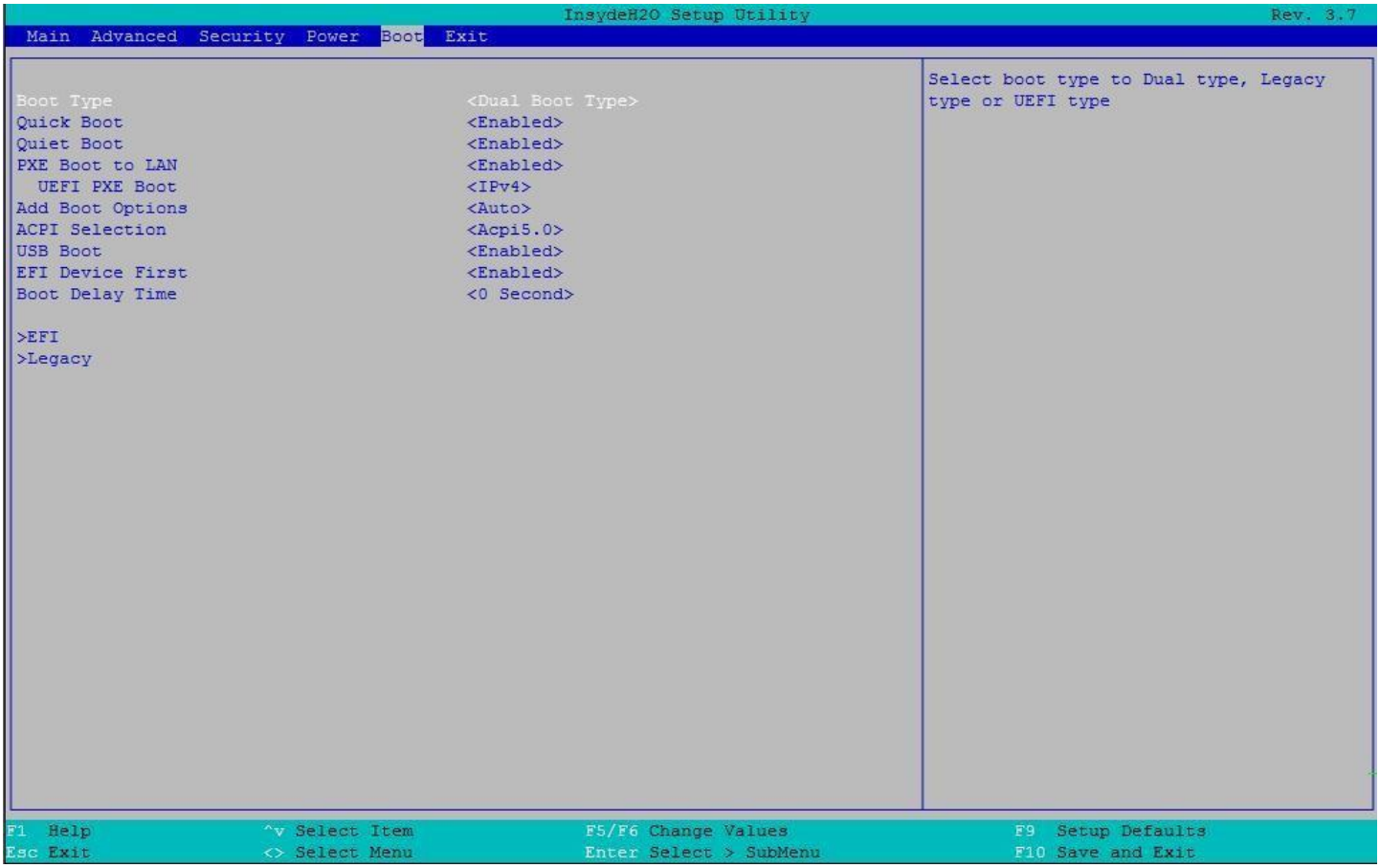


Рисунок 77

Настройка BIOS	Опции	Описание
Boot Type *(Тип загрузки)*	Dual Boot Type Legacy Boot Type UEFI Boot Type	Выберите тип загрузки: Dual type (Двойной), Legacy type или UEFI type (Тип UEFI).
Quick Boot *(Быстрая загрузка)*	Отключено Включено	Позволяет BIOS пропускать определенные тесты при загрузке. Это уменьшит время, необходимое для загрузки системы.
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.

Настройка BIOS	Опции	Описание
Add Boot Options *(Добавить настройки загрузки)*	Первый Последний Авто	Положение в порядке загрузки для оболочки, сети и съемных устройств
ACPI Selection *(Выбор ACPI)*	Acpi1.0B Acpi3.0 Acpi4.0 Acpi5.0	Выберите загрузку в Acpi3.0/Acpi1.0B.
USB Boot *(Загрузка по USB)*	Отключено Включено	Отключение или включение загрузки с загрузочных устройств USB
EFI Device First	Отключено Включено	Определяет какое первое 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 12.2.5.1.	Настройка порядка загрузочных EFI-устройств
Legacy	См. раздел 12.2.5.2.	Настройка порядка загрузочных Legacy -устройств

12.2.5.1 Boot/EFI

Рисунок 78

Настройка BIOS	Опции	Описание
Internal EFI Shell *(Внутренняя оболочка EFI)*	Нет опций	Настройки загрузки EFI

12.2.5.2 Boot/Legacy

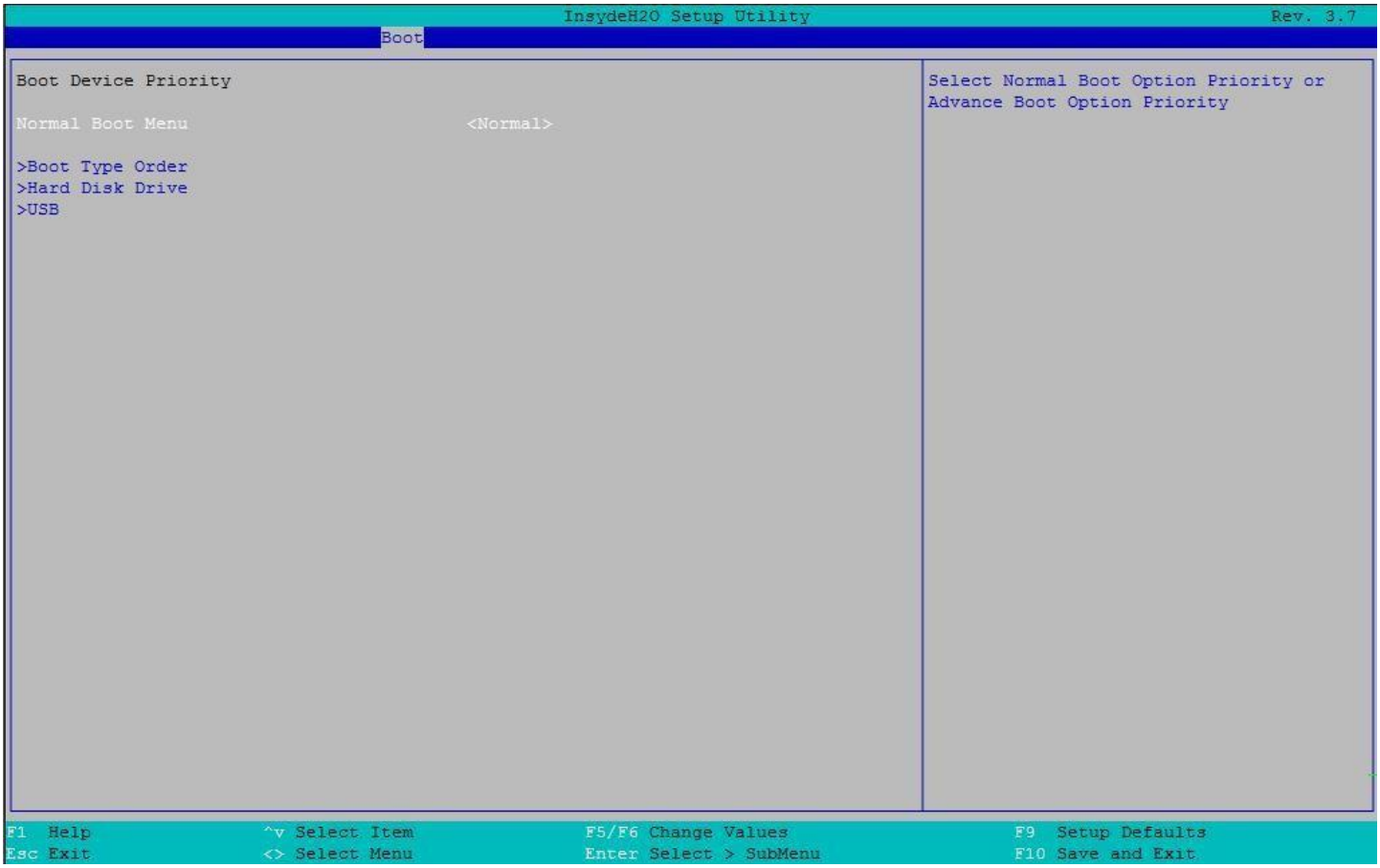


Рисунок 79

Настройка BIOS	Опции	Описание
Normal Boot Menu *(Обычное меню загрузки)*	Обычная расширенная	Выберите Приоритет Обычной загрузки или Приоритет расширенной опции загрузки
Boot Type Order *(Порядок типов загрузки)*	См. раздел 12.2.5.2.1.	Изменить порядок типов загрузки
Hard Disk Driver *(Драйвер жесткого диска)*	См. раздел 12.2.5.2.2.	Изменить порядок загрузки CD/DVD-ROM драйвера загрузочного устройства
USB	См. раздел 12.2.5.2.3.	Отключение или включение загрузки на загрузочные устройства USB

12.2.5.2.1 Boot/Legacy/Boot Type Order

Порядок типов загрузки

Рисунок 80

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

12.2.5.2.2 Boot/Legacy/Hard Disk Drive

Выбор жесткого диска для загрузки

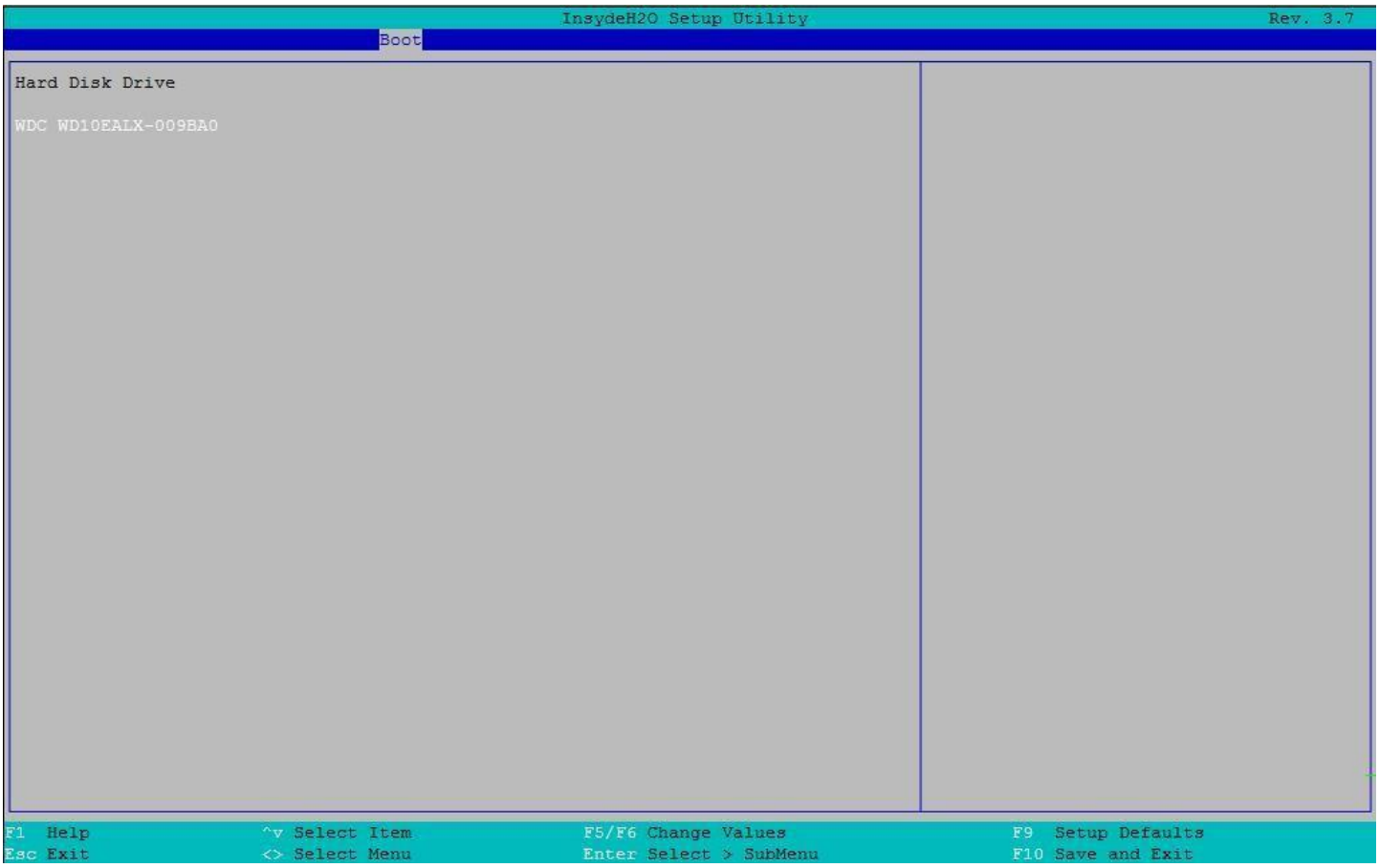


Рисунок 81

Настройка BIOS	Опции	Описание
Hard Disk Driver *(Драйвер жесткого диска)*	Нет опций	Модель драйвера жесткого диска, подключенного к этой платформе.

12.2.5.2.3 Boot/Legacy/USB

Загрузка с USB

Рисунок 82

Настройка BIOS	Опции	Описание
USB Flash Driver *(Длайвер USB Flash)*	Нет опций	Модельзагрузочногофлэш-накопителяUSB, подключенного к этой платформе.

12.2.6 Exit menu

Выход из меню. Меню выхода предоставляет следующие опции:

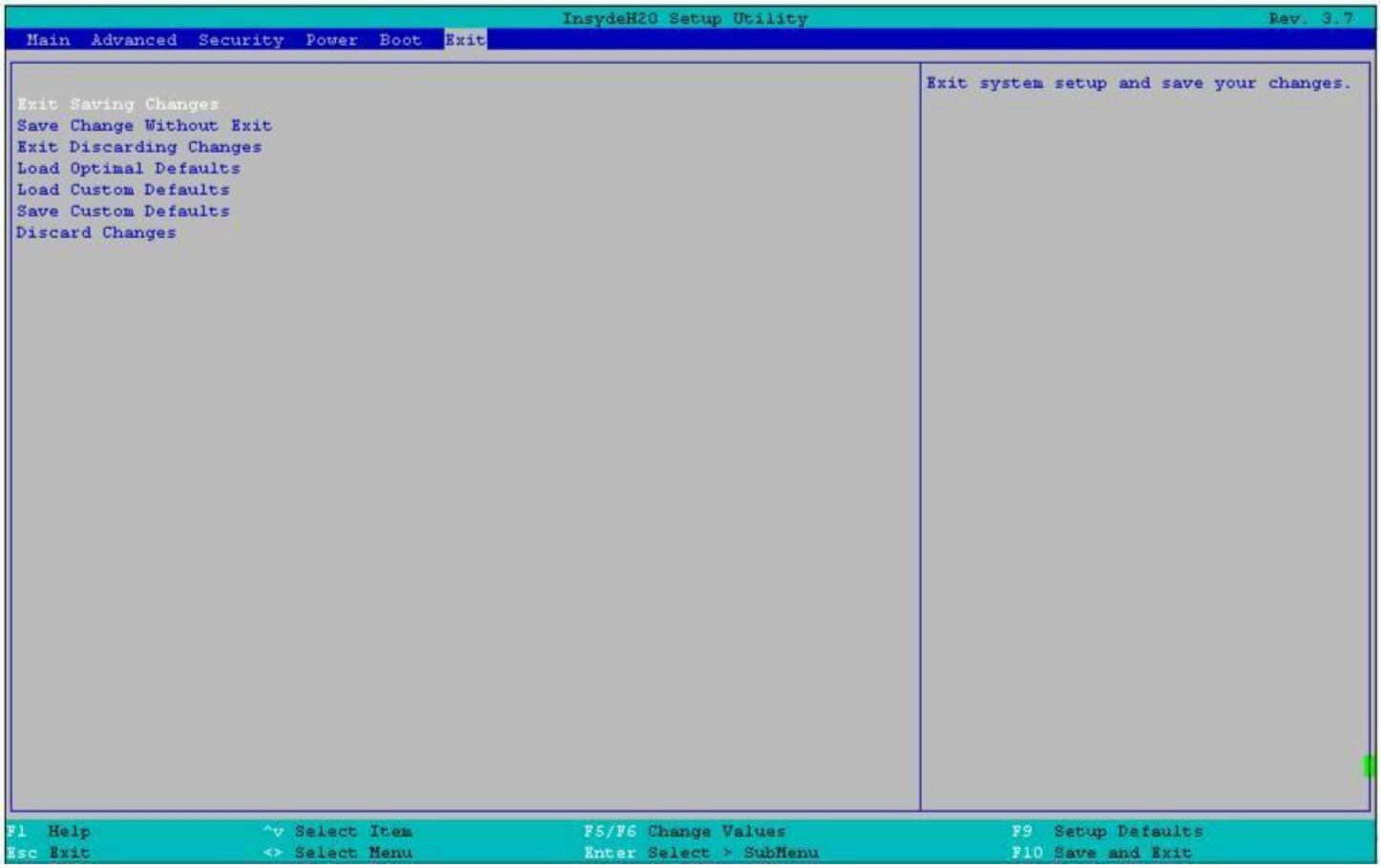


Рисунок 83

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.
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.

12.2.7 General Help

Общая помощь.

Вы можете нажать клавишу "F1" в любом месте меню и получить страницу общей справки, как показано ниже.

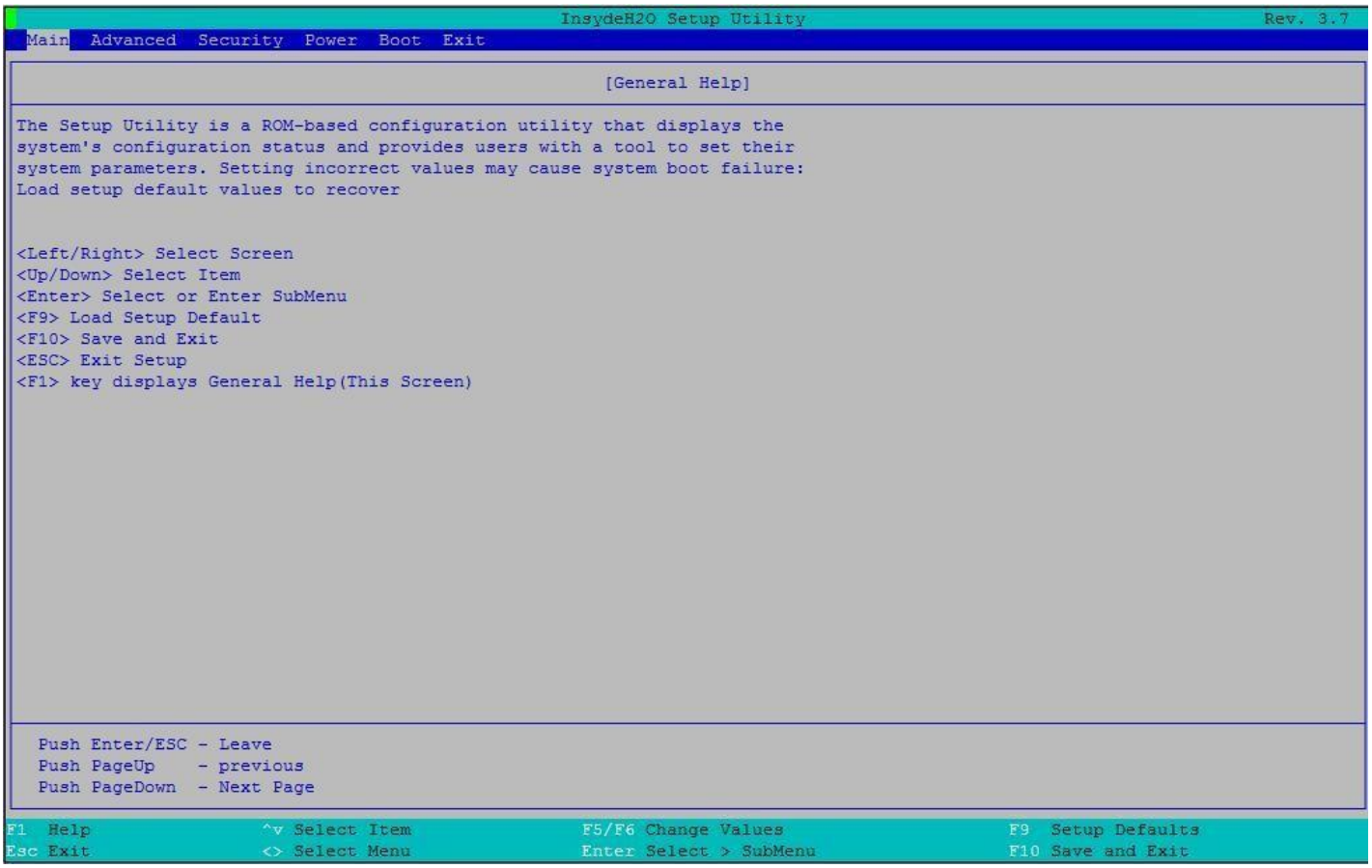


Рисунок 84

12.3 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 85

12.4 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*».

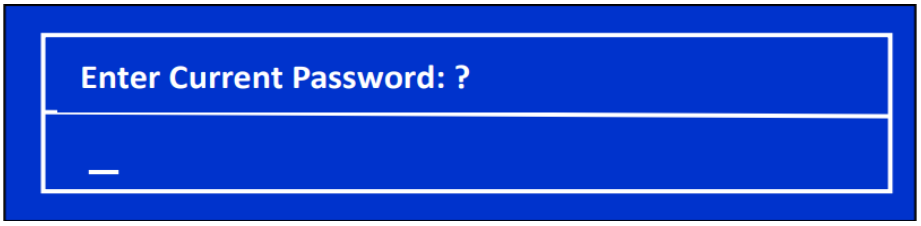


Рисунок 86

(2) Любые введенные символы не отображаются, но отображаются символы "*".

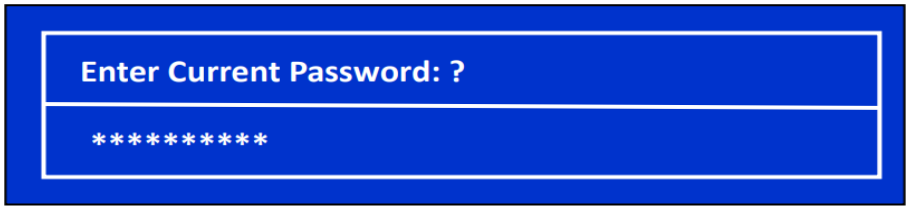


Рисунок 87

(3) При вводе неверного пароля отображается следующее сообщение *«Неправильный пароль»*.

Рисунок 88

(4) При трехкратном вводе неправильного пароля отображается следующее сообщение («*Состояние ошибки. Введен неправильный пароль 3 раза. Пожалуйста, перезапустите систему*»), после чего система останавливается.

Рисунок 89

Приложение А. Советы по интеграции и использованию

- При добавлении или удалении компонентов или периферийных устройств с серверной материнской платы шнуры питания должны быть отсоединены от сервера. Когда к серверу подано питание, резервное напряжение все еще присутствует, даже если серверная плата выключена.
- Эта серверная системная плата поддерживает семейство процессоров Intel® Xeon® Scalable с расчетной тепловой мощностью (TDP) до 205 Вт включительно. Предыдущие поколения процессоров Intel® Xeon® не поддерживаются. Серверные системы, использующие эту серверную плату, могут соответствовать расчетным ограничениям TDP серверной материнской платы, а могут и не соответствовать. Перед выбором процессора проверьте пределы TDP серверной системы.
- Процессоры должны устанавливаться начиная с CPU 1.
- Для достижения наилучшей производительности количество установленных модулей DDR4 DIMM должно быть сбалансировано как для процессорных сокетов, так и для каналов памяти.
- Светодиодный индикатор состояния системы горит желтым цветом для всех критических ошибок, обнаруженных во время инициализации процессора.
- 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.

Приложение C. Ошибки кода 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 (OOB) управление.

Существуют исключительные случаи на 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 они передаются диагностическим светодиодным дисплеем 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 включают незначительные, серьезные и критические. Действия BIOS для каждого из них определяются следующим образом:

- **Фатальные (Fatal)**: Если система не может загрузки, POST останавливается и отображения на 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 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 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.

- **Основные (Major)**: сообщение об ошибке отображается на экране диспетчера ошибки и ошибка регистрируется в журнале событий. Если в BIOS включена опция «Пауза после ошибки», для продолжения загрузки системы требуется вмешательство оператора. Если параметр настройки BIOS «Пауза при ошибке POST» отключен, система продолжит загрузку.

Примечание. Для 0048 «Ошибка проверки пароля» система останавливается, а затем после следующего 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 ухудшенном состоянии. Пользователь может захотеть заменить ошибочный блок. Параметр «Пауза при ошибке POST» в настройках BIOS не влияет на эту ошибку.

Примечание. Коды ошибок POST в Таблице 39 являются общими для всех серверных платформ Rikor® текущего поколения. Функции, присутствующие на данной серверной материнской плате/системе, определяют, какие из перечисленных кодов ошибок поддерживаются.

Таблица 39. 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
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
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
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

Код ошибки	Сообщение об ошибке	Сообщение о действиях	Тип ошибки
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
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
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
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
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
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

Код ошибки	Сообщение об ошибке	Сообщение о действиях	Тип ошибки
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
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
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
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

Код ошибки	Сообщение об ошибке	Сообщение о действиях	Тип ошибки
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
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
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

C.1 Звуковые коды ошибок POST

В Таблице 40 перечислены звуковые коды ошибок POST. 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 40. 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 или вставляется или извлекается во время выполнения.
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 ЦП/ядер/кэша.
2 коротких	BIOS recovery started	N/A	Начата загрузка для восстановления.
4 коротких	BIOS recovery failed	N/A	Восстановление не удалось. Обычно это происходит так быстро после начала восстановления, что звучит как 2-4 звуковых сигнала.

Встроенный BMC может генерировать звуковые коды при обнаружении условий отказа. Звуковые коды звучат каждый раз, когда обнаруживается проблема, например, при каждой попытке включения питания, но не звучат постоянно. Коды, общие для всех серверных систем Intel®, использующих набор микросхем одного поколения, перечислены в Таблице 41. Каждая цифра в коде представлена последовательностью звуковых сигналов, количество которых равно цифре.

Таблица 41. 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 заполнены неправильно. CPU1 должен быть заполнен перед CPU2.
1-5-2-2	Утверждение об ошибке CPU CAT (IERR)	CPU обнаружил ошибку при инициализации.
1-5-2-3	Подтверждение тайм-аута CPU ERR2	CPU Не удалось инициализировать систему за указанное время.
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 заполнен перед CPU2.
1-5-4-2	Неисправность питания.	Неожиданное отключение питания постоянного тока (обрыв питания) - датчики блока питания сообщают о смещении отказа блока питания.
1-5-4-4	Ошибка управления питанием (тайм-аут подтверждения питания).	Тайм-аут подтверждения хорошего питания - датчики блока питания сообщают о смещении сбоя программного управления мощностью.
1-5-1-2	Утверждение датчика сторожевого таймера VR.	Последовательность включения постоянного тока контроллера VR не была выполнена вовремя.
1-5-1-4	Состояние источника питания.	Система не включается или неожиданно отключается, и присутствует блок питания (PSU), который является несовместимой моделью с одним или несколькими другими блоками питания в система.

Приложение D. Заявление о волатильности

В этом приложении описаны энергозависимые и энергонезависимые компоненты серверной материнской платы Rikor® КДБА.469555.003 (Таблица 42 и Таблица 43). Описание столбцов приводится ниже таблиц.

Примечание. В этот раздел не входят какие-либо компоненты, не входящие непосредственно в перечисленные серверные платы Intel®, такие как компоненты корпуса, процессоры, память, жесткие диски или дополнительные карты.

Таблица 42. Энергозависимые и энергонезависимые компоненты серверной материнской платы Rikor® КДБА.469555.003

Тип компонента	Размер	Позиционное обозначение	Данные пользователя	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 43. Энергозависимые и энергонезависимые компоненты на плате расширения LAN

Тип компонента	Размер	Позиционное обозначение	Данные пользователя	название
ЭнергоНезависимый	512 КБ	EU2A1	Нет	Inphi * PHY EEPROM
ЭнергоНезависимый	2 Кбит	EU3A1	Нет	LAN Riser FRU

- **Тип компонентов**: Серверная плата Rikor® КДБА.469555.003 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 сервера, и очистка этих областей может вывести серверную плату из строя.
  - **Энергозависимая**: Энергозависимая память очищается автоматически при отключении питания от системы.
  - **Батарея питание RAM**: батареи питание RAM является похож на летучую память, но это питание от батареи на плате сервера. Данные в оперативной памяти с питанием от батареи сохраняются до тех пор, пока батарея не будет снята с серверной материнской платы.
- **Размер**: размер каждого компонента в битах, кбитах, мегабитах, байтах, килобайтах (КБ) или мегабайтах (МБ).
- **Расположение платы**: **Расположение** платы - это физическое расположение каждого компонента, соответствующее информации на шелкографии серверной материнской платы.
- **Пользовательские данные**: компоненты флэш-памяти на серверных платах 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. Постоянство информации, записанной в каждый компонент, определяется его типом, как описано в таблице.

  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 и не связаны с паролями операционной системы. Конкретные компоненты, которые могут содержать данные пароля:

  - **BIOS** : **BIOS** серверной материнской платы обеспечивает возможность предотвращения неавторизованных пользователей от настройки параметров BIOS, когда установлен пароль BIOS. Этот пароль хранится во флэш-памяти BIOS и используется только для установки ограничений доступа к конфигурации BIOS.

- **BMC** : серверные платы поддерживают контроллер управления базовой платой (BMC), соответствующий интерфейсу интеллектуального управления платформой (IPMI) 2.0. BMC обеспечивает возможности мониторинга состояния, оповещения и удаленного управления питанием для серверной материнской платы Intel®. 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 настроен, BMC поддерживает пароли пользователей для управления этим доступом. Эти пароли хранятся во флеш-памяти BMC.

Приложение E. Нормативная информация и сертификация

E.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.), кроме приложений ITE, потребует дополнительной оценки и разрешения регулирующих органов.

Компания Rikor® подтвердила, что все продукты **сконфигурированные и проданные Rikor® своим клиентам,** соответствуют требованиям для всех нормативных сертификатов, определенных в следующей таблице. Заказчик Rikor® 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 системы.

Таблица 44. Нормативная сертификация

	Серверная платформа Rikor		Комментарии
	Только плата	Серверный корпус	Уровень интеграции продукта
	R-BD-SXRM-XS16.EA.V6.0 КДБА 469 555.003	Корпус серверной платформы Rikor модели RCXXXXX-XX	Семейство продуктов, указанных при сертификации
Нормативная сертификация			
Сертификация CU (Россия/Беларусь/Казахстан)	✓	✓	Серверная платформа
Европейская декларация соответствия CE	○	○	

Таблица Ключ

Не протестировано/не сертифицировано	○
Испытано/Заверенная - только Limited OEM SKUs	●
Тестирование/Сертификация (Планируется)	(Дата)
Протестировано/сертифицировано	✓

[1] 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.

EU Директива ЕС 2019/424 (лот 9)

С 1 марта 2020 года вст UPIт в силу дополнительный компонент нормативной схемы маркировки CE Европейского Союза (ЕС), обозначенный как EU Директива ЕС 2019/424 (лот 9). После этой даты все новые серверные системы, поставленные или развернутые на территории ЕС, должны соответствовать всем требованиям маркировки CE, включая те, которые определены дополнительными правилами EU Lot 9.

Rikor® подтвердила, что все серверные продукты L3, L6 и L9 [2], **как сконфигурированные и продающиеся Intel** для своих клиентов соответствуют нормативным требованиям полной CE, необходимым для данного вида продукции, в том числе тех, которые определены Лота ЕС 9.

Посетите следующий веб-сайт для получения дополнительной информации о EU Директиве ЕС 2019/424 (Lot9):
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0424

В соответствии с требованиями к эффективности материалов, указанными в EU Директиве ЕС 2019/424 (лот 9), компания Rikor® предоставляет все необходимые сопутствующие товары, указанные ниже:

- **Технические характеристики продукта**
  - *Серверная плата Rikor® КДБА.469555.003 - Техническая спецификация продукции (TPS) - Этот документ*

https://www.rikor.com/support/UserManual_Rikor_KDBA.469555.003.pdf

- **Система BIOS/Firmware и обновление безопасности - Серверная плата Rikor® КДБА.469555.003**
  - Пакет обновления системы (SUP) - только uEFI
  - Intel® One Boot Flash Update (OFU) - Поддержка различных ОС

https://server.rikor.com/support/scalable

- **Intel® RAID Controller Firmware Updates и другие вспомогательные коллатерали**
  - Примечание: для конфигураций систем, которые могут быть настроены с помощью RAID-контроллера Rikor®

https://server.rikor.com/support/scalable/raid

[2] Конфигурация системы L9 - это серверная система, готовая к включению, без установленной операционной системы. Конфигурация системы L6 требует установки дополнительных компонентов, чтобы она была готова к включению. L3 - это варианты строительных блоков, которые требуют интеграции в шасси для создания функциональной серверной системы.

Приложение F. 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
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
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

Термин	Definition	Определение
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
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
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
RESTful	Representational State Transfer	Изобразительное State Transfer
RCiEP	Root Complex Integrated Endpoint	Интегрированная конечная точка корневого комплекса
RDIMM	Registered DIMM	Зарегистрированный DIMM

Термин	Definition	Определение
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
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
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 ЦП
VRD	Voltage Regulator-Down	Регулятор понижения напряжения
Intel® VT	Intel® Virtualization Technology	Технология виртуализации Intel

Приложение G. Список совместимости

В документе «Список совместимых комплектующих и операционных систем» приведен список совместимости со следующими комплектующими и ОС:

- Центральный процессор (CPU):
  - Intel Xeon Scalable Bronze processors 1,2nd Gen
  - Intel Xeon Scalable Silver processors 1,2nd Gen
  - Intel Xeon Scalable Gold processors 1,2nd Gen
- Модули памяти
- HDD жесткие диски 3.5 дюйма
- HDD жесткие диски 2.5дюйма
- SSD накопители
- Операционные системы:
  - Windows
  - Linux
  - VMware
  - Hyper-V

Список серверных платформ Rikor®, совместимых с серверной материнской платой Rikor® КДБА.469555.003:

- RP-6212.3D-PS35-0721.0-62.0.0.0.0
- RP-6212.3D-PS35-0721.0-64.0.0.0.0
- RP-6104.3X-PS35-071F.0-62.R.0.0.0
- RP-6224.3X-PS25-0721.0-62.0.0.0.0
- RP-6216.3X-PS25-0721.0-62.0.0.0.0
- RP-6208.3X-PS35-0721.0-62.0.0.0.0
- RP-5108.3X-PS25-0720.0-62.R.0.0.0
- RP-6436.3X-PS35-0721.0-62.0.0.0.0
- RP-6316.3X-PS35-0721.0-62.0.0.0.0

Комплектация

Серверная материнская плата Rikor® КДБА.469555.003 упаковывается в стандартную и заводскую упаковку. Пожалуйста, проверьте наличие в комплекте стандартных деталей, перечисленных ниже:

Таблица 45. Комплектация Серверной материнской платы Rikor® КДБА.469555.003

Объект		Стандартная подарочная упаковка	Стандартная заводская упаковка	Примечание
Материнская плата		1	1	
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 Rikor:

Сервисная горячая линия: 8-495-414-11-92.