Тринити

РОССИЙСКИЙ ПРИЗВОДИТЕЛЬ ОБОРУДОВАНИЯ

ДЛЯ ПОСТРОЕНИЯ ИТ-ИНФРАСТРУКТУРЫ

ВСТРОЕННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ BIOS RU.ТВЛФ.00001-01

Документация, содержащая информацию, необходимую для эксплуатации экземпляра программного обеспечения

на 50 листах

г. Москва

2025

Содержание

1. Перечень сокращений и обозначений

ОС	Операционная система
ПЗУ	Постоянное запоминающее устройство
ПК	Персональный компьютер
ПО	Программное обеспечение
СТП	Служба технической поддержки
ЭВМ	Электронно-вычислительная машина
API (Application Programming Interface)	Описание способов взаимодействия программного обеспечения с аппаратными и программными компонентами системы
BIOS (Basic Input/Output System)	Базовая система ввода-вывода
UEFI (Unified Extensible Firmware Interface)	Интерфейс между операционной системой и микропрограммами, управляющими оборудованием
Программатор	Аппаратно-программное устройство для чтения и записи информации в ПЗУ, флэш-память или внутреннюю память микроконтроллеров (МК)

2. Общие сведения

Документ содержит информацию, необходимую для эксплуатации экземпляра встроенного программного обеспечения BIOS RU.ТВЛФ.00001-01 (далее – ВПО).

ВПО предназначено для обеспечения взаимодействия между аппаратными и программными компонентами платы материнской Тринити ТВЛФ.469555.001 (далее – материнская плата) в составе серверов Тринити, построенных на базе процессоров Intel Xeon 3-го поколения. ВПО разработано для облегчения процесса начального запуска вычислительной техники и предназначена для инициализации и запуска основных устройств вычислительной техники и ее компонентов. ВПО обеспечивает передачу управления операционной системе в соответствии с предварительно заданными настройками.

ВПО использует технические средства платы материнской Тринити ТВЛФ.469555.001 производства АО «ТРИНИТИ СОЛЮШНС».

3. Назначение программного обеспечения

ВПО – программа начального запуска, является системной программой низкого уровня, хранящейся в микросхеме ПЗУ на материнской плате, и предоставляет пользователю возможность полного управления системой при загрузке.

ВПО состоит из ряда драйверов, приложений и экранных форм, с помощью которых можно настроить параметры работы системы в соответствии с требованиями пользователя или использовать параметры, заданные по умолчанию.

ВПО предоставляет расширенные функциональные возможности UEFI, унифицированного расширяемого интерфейса микропрограмм для ПО низкого уровня, которое запускается автоматически при старте сервера перед тем, как загрузится операционная система.

Функции ВПО:

- начальная инициализация серверной платформы;
- проверка работоспособности аппаратных компонентов;
- загрузка операционной системы.

ВПО разработано в соответствии со спецификацией UEFI для решения проблемы переносимости встроенного программного обеспечения и расширяемости на будущие платформы, расширения использования различных драйверов, средств разработки, утилит поддержки и загрузочных приложений.

Особенности ВПО:

- поддержка UEFI 2.8, PI 1.7;
- интеграция с Intel Boot Guard;
- Secure Flash для безопасного обновления;
- модульная архитектура.

4. Аппаратные и программные требования

Для корректной работы ВПО установлены следующие минимальные и рекомендуемые требования:

1) Аппаратные требования:

- Процессор:
  - минимальные: Intel Xeon 3-го поколения (Ice Lake);
  - рекомендуемые: процессоры последнего выпуска в семействе Xeon Ice Lake с расширенными возможностями для оптимальной производительности.
- Материнская плата:
  - ВПО предназначено для использования в материнской плате Тринити ТВЛФ.469555.001 производства АО «ТРИНИТИ СОЛЮШНС».
- Оперативная память и прочие компоненты:
  - минимальные: 16 Гб оперативной памяти;
  - рекомендуемые: 32 Гб и более.

2) Программные требования:

- Совместимость с операционными системами:

- минимальные: поддержка основных операционных систем, оптимизированных для работы с UEFI, включая определённые версии Windows, Linux и другие ОС, соответствующие требованиям платформы;

- рекомендуемые: последние версии операционных систем с актуальными обновлениями безопасности и драйверов, обеспечивающие стабильную работу и взаимодействие с BIOS.

- Дополнительное программное обеспечение:

- для полного функционала системы может потребоваться установка специализированных драйверов и утилит;

- рекомендуется регулярное обновление этих компонентов согласно рекомендациям производителя для обеспечения максимальной совместимости и безопасности.

- Для реализации удаленного доступа к ВПО необходимо следующее ПО сторонних разработчиков:

браузер для доступа через Web-интерфейс;

программа для доступа посредством командной строки по протоколу IPMI.

Для удаленного доступа к ВПО через IPMI/BMC необходимо обеспечить сетевой доступ к сервисному процессору материнской платы.

5. Состав модулей и автоматизируемые функции

ВПО представляет собой систему инициализации, запуска и управления вычислительной техникой и ее компонентами. Основная цель ВПО – обеспечить базовую загрузку оборудования, гарантируя его совместимость с последними отраслевыми стандартами.

ВПО имеет модульную архитектуру, включающую следующие компоненты:

- модуль инициализации процессора (CPU Initialization Module): отвечает за проверку и настройку процессора;
- модуль инициализации памяти (Memory Initialization Module): выполняет тестирование и настройку оперативной памяти;
- модуль управления периферийными устройствами (Peripheral Management Module): обеспечивает взаимодействие с устройствами ввода-вывода;
- модуль управления энергопотреблением (Power Management Module): контролирует режимы энергосбережения и управления питанием;
- модуль обновления прошивки (Firmware Update Module): предоставляет инструменты для безопасного обновления BIOS.

ВПО обеспечивает следующие функции:

1) Инициализация аппаратного обеспечения при запуске системы

При включении питания система запускается с выполнения процедуры самодиагностики (POST), в ходе которой проверяется работоспособность основных компонентов, таких как процессор, оперативная память, устройства хранения данных и другие периферийные устройства. Это позволяет гарантировать корректное и безопасное начало работы системы.

2) Обеспечение интерфейса между операционной системой и аппаратными компонентами

BIOS служит промежуточным звеном, создающим стандартизированный программный интерфейс (API) для взаимодействия операционной системы с аппаратными средствами. Данный интерфейс обеспечивает стабильное и эффективное управление ресурсами системы, способствуя повышению её производительности и надёжности.

3) Поддержка специфических функций, реализованных компанией АО «ТРИНИТИ СОЛЮШНС»

Помимо стандартного функционала AMI BIOS, система включает дополнительные возможности, адаптированные под уникальные требования предприятия. К таким функциям относятся расширенные механизмы безопасности, оптимизированные процедуры обновления, а также возможности тонкой настройки параметров системы для удовлетворения специфических задач и повышения общей эффективности работы.

4) Поддержка драйверов и средств разработки

ВПО обеспечивает поддержку различных драйверов и средств разработки, что позволяет расширять функциональность системы и использовать различное аппаратное обеспечение.

5) Загрузка операционной системы

После завершения инициализации аппаратного обеспечения и настройки параметров ВПО загружает операционную систему с жесткого диска или другого носителя данных.

6) Обеспечение безопасной загрузки

ВПО может обеспечивать безопасную загрузку системы, проверяя подлинность и целостность загрузочных компонентов для предотвращения атак и вредоносных вмешательств.

ВПО использует расширенные функциональные возможности UEFI, которые обеспечивают:

- поддержку жестких дисков большего объема – UEFI поддерживает работу с жесткими дисками большего объема, что увеличивает гибкость системы;
- быструю загрузку – UEFI работает на более низком уровне, чем традиционный BIOS, поэтому загрузка системы происходит быстрее;
- высокий уровень безопасности – UEFI предоставляет дополнительные механизмы безопасности, такие, как проверка цифровых подписей, что делает процесс загрузки более безопасным;
- графический интерфейс и поддержку мыши – UEFI обеспечивает более удобный и интуитивно понятный интерфейс для пользователей, включая поддержку мыши;
- возможность удаленной настройки и отладки – позволяет проводить настройку и отладку системы удаленно, что особенно важно для серверных и удаленных систем;
- различные способы хранения – UEFI может храниться во флэш-памяти на материнской плате, на жестком диске или на общем сетевом ресурсе.

6. Режим функционирования ВПО

6.1. Подготовка к работе

6.1.1. Установка и настройка ВПО

1) Установка

Встроенное программное обеспечение BIOS RU.ТВЛФ.00001-01 записывается в энергонезависимую память материнской платы на этапе производства. Запись выполняется с использованием специального оборудования – программаторов SPI Flash.

На момент поставки серверной платформы ВПО уже установлено, а его базовые настройки соответствуют требованиям производителя. Пользователь не нуждается в дополнительной установке.

2) Первичный вход в настройки

При включении системы необходимо войти в меню настроек BIOS (обычно с помощью клавиши DEL, F2 или иной, указанной в руководстве).

3) Конфигурация параметров

При необходимости настроить основные параметры, включая порядок загрузки, режимы работы процессора и оперативной памяти, а также конфигурацию периферийных интерфейсов. Также следует убедиться, что выбран правильный режим работы UEFI.

4) Сохранение изменений

После завершения настройки необходимо сохранить все внесённые изменения и перезагрузить систему для применения новой конфигурации.

6.1.2. Проверка совместимости аппаратного обеспечения

1) Аппаратные компоненты

Проверить соответствие всех компонентов системы минимальным требованиям (процессор Intel Xeon 3-го поколения (Ice Lake), совместимая материнская плата, оперативная память и др.).

2) Тестирование через POST

Выполнить встроенную процедуру самодиагностики (POST) для выявления аппаратных сбоев и проверки корректности работы всех узлов.

3) Обновления

При наличии, установить актуальные версии прошивок и драйверов для компонентов системы.

6.1.3. Настройка параметров безопасности

1) Аутентификация и контроль доступа

Настроить механизмы аутентификации для предотвращения несанкционированного доступа к настройкам ВПО.

2) Проверка целостности

Включить функции проверки целостности загрузочных компонентов и настройте шифрование, если это предусмотрено конфигурацией ВПО.

3) Резервное копирование конфигураций

Рекомендуется создать резервную копию текущих настроек ВПО для быстрого восстановления в случае возникновения проблем.

6.2. Штатное функционирование

После подачи питания на сервер ВПО загружается автоматически и выполняет инициализацию системы.

Для обеспечения бесперебойной работы системы и своевременного устранения неполадок предлагаются следующие рекомендации:

1) Для консультаций по настройке, обновлению или устранению проблем с ВПП обращаться в техническую поддержку АО «ТРИНИТИ СОЛЮШНС»;

2) Рекомендуемые процедуры обновления ВПО:

- через web-интерфейс BMC – обновление может проводиться дистанционно посредством web-интерфейса базового контроллера управления (BMC), что позволяет централизованно управлять обновлениями в серверных и корпоративных средах.
- через программатор – использование специализированного программатора позволяет выполнить прямое программирование BIOS-чипа. Данный метод полезен для восстановления системы после возникновения сбоев или повреждений микропрограммы.

3) Рекомендации по устранению распространенных проблем

- проблемы с загрузкой системы – проверить правильность настроек загрузочного устройства и последовательность загрузки, а также убедиться в корректности установки всех аппаратных компонентов.
- диагностика аппаратных сбоев – использовать встроенную процедуру POST для выявления и устранения аппаратных неисправностей. При необходимости заменить неисправные компоненты.
- ошибки обновления ВПО – при возникновении проблем с обновлением микропрограммы восстановить предыдущую рабочую версию из резервной копии или обратиться в службу технической поддержки для получения подробных инструкций.

6.3. Численность, функции и квалификация персонала, работающего с ВПО

Количество пользователей программного обеспечения определяется текущими потребностями заказчика программного обеспечения.

Пользователи должны иметь базовые навыки работы с ОС Linux и Windows, навыки пользователя сети Интернет, а также изучить эксплуатационную документацию на ВПО.

Перечень задач, выполняемых пользователями:

- поддержание работоспособности ВПО и ОС;
- резервное копирование системы;
- конфигурирование пользователей и их учетных записей;
- конфигурирование политики безопасности;

- конфигурирование действий при восстановлении питания;
- обновление ВПО.

7. Описание работы

7.1. Вход в программу

Для входа в программу необходимо выполните следующие ниже действия:

- подать электропитание и включить сервер;
- нажать и удерживать клавишу «Delete» или «F2» на клавиатуре, подключенной к серверу;
- дождаться появления главного меню ВПО.

На экране появится главное меню ВПО (открытое на вкладке «Main»), из которого можно зайти во все остальные меню.

На вкладке «Main» отображается общая информация о системе и ВПО:

- BIOS Information (Информация о ВПО):
  - BIOS Vendor – разработчик ВПО;
  - Core Version – версия ядра;
  - Compliancy – номер версии UEFI и номер версии Platform Initialization (PI);
  - Project Version – версия проекта;
  - Build Date and Time – дата в формате «ММ/ДД/ГГГГ» и время в формате «чч/мм/сс»;
  - Access Level – уровень прав доступа к ВПО (например, Administrator);
- Platform Information (Общая информация о платформе):
  - Platform – название платформы;
  - Processor – информация о процессоре;
  - PCH – информация о контроллере PCH (Platform Controller Hub);
  - RC Revision – версия Intel RC;
- System Language – язык интерфейса ВПО (по умолчанию английский, может быть изменен на другой);
- System date – текущая дата в формате «День_недели ММ/ДД/ГГГГ» (может быть изменена);
- System time – текущее время в формате чч/мм/сс (может быть изменено).

7.2. Навигация в ВПО

Для навигации во вкладках и меню ВПО необходимо использовать клавиши клавиатуры согласно таблице 1.

Таблица 1 – Клавиши навигации

Клавиша	Действие
← →	Перемещает курсор влево или вправо для выбора меню
↑ ↓	Перемещает курсор вверх или вниз по списку для выбора пункта раздела меню
Enter	Позволяет открыть подменю или команду
+/-	Смена опции
F1	Общая помощь

F7	Предыдущее значение
F9	Оптимальные настройки по умолчанию
F10	Сохранение и выход
Esc	Выход из текущего раздела

Краткое описание функций клавиш для навигации отображается в нижнем правом поле интерфейса ВПО.

В верхнем правом поле размещается краткая информация по назначению пунктов вкладок и меню.

7.3. Меню «Advanced» (раздел с дополнительными настройками)

Меню «Advanced» (см. рисунок 1) предназначено для настройки дополнительных опций сервера в соответствии с предпочтениями пользователя, а именно:

- настройка доверенного компьютера;
- дистанционное управление консолью;
- конфигурация интерфейсов USB;
- сетевая конфигурация;
- аутентификация;
- конфигурация оперативной памяти;
- другие настройки.

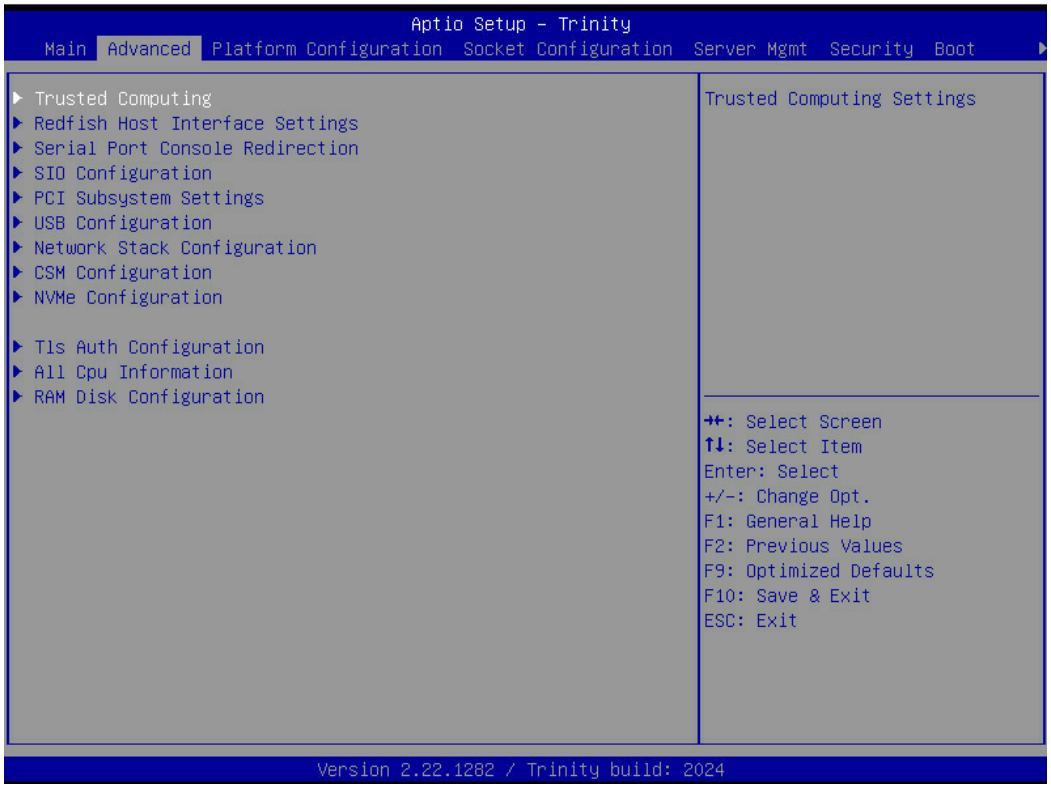

Рисунок 1 – Вкладка «Advanced»

На производительность сервера влияет настройка «PCI Subsystem Settings». Окно с настройками подсистемы PCI (вкладка «PCI Subsystem Settings») показано на рисунке 2.

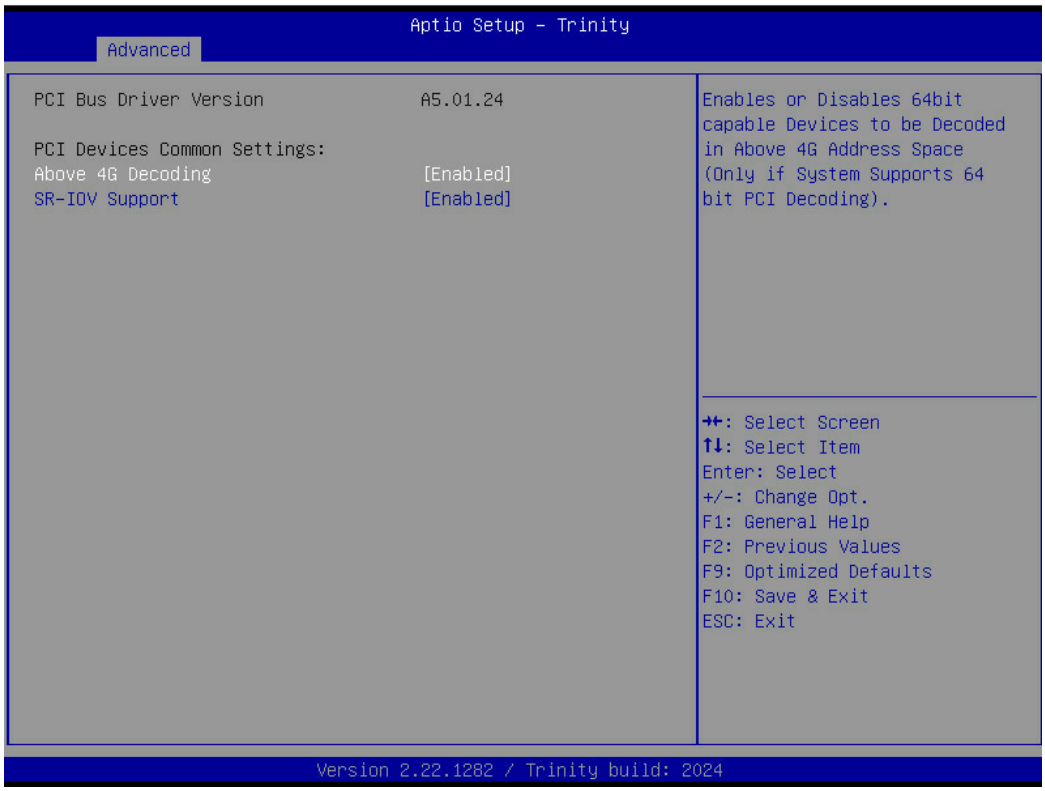

Рисунок 2 – Вкладка «PCI Subsystem Settings»

На рисунке 2 видны два настраиваемых поля: «Above 4G Decoding» и «SR-IOV Support»

Above 4G Decoding – настройка, которая позволяет системе адресовать и использовать устройства PCI Express, требующие более 4 Гб адресного пространства памяти. Это особенно важно для современных видеокарт с большим объемом видеопамяти (VRAM).

Возможные параметры: Enabled (Включен) / Disabled (Выключен).

SR-IOV Support – спецификация PCI Express, которая позволяет одному физическому устройству PCIe (например, сетевой карте) представляться как несколько виртуальных устройств операционной системе. Это позволяет нескольким виртуальным машинам напрямую и независимо обращаться к одному и тому же физическому сетевому адаптеру, минуя гипервизор для операций ввода-вывода.

Возможные параметры: Enabled (Включен) / Disabled (Выключен).

7.4. Меню «Platform Configuration» (раздел с настройками платформы)

7.4. Меню «Platform Configuration» предоставляет возможность дополнительной конфигурации платформы.

Установка некорректных значений параметров для вкладок этого меню может привести к сбою всей системы.

Внешний вид меню показан на рисунке 3.

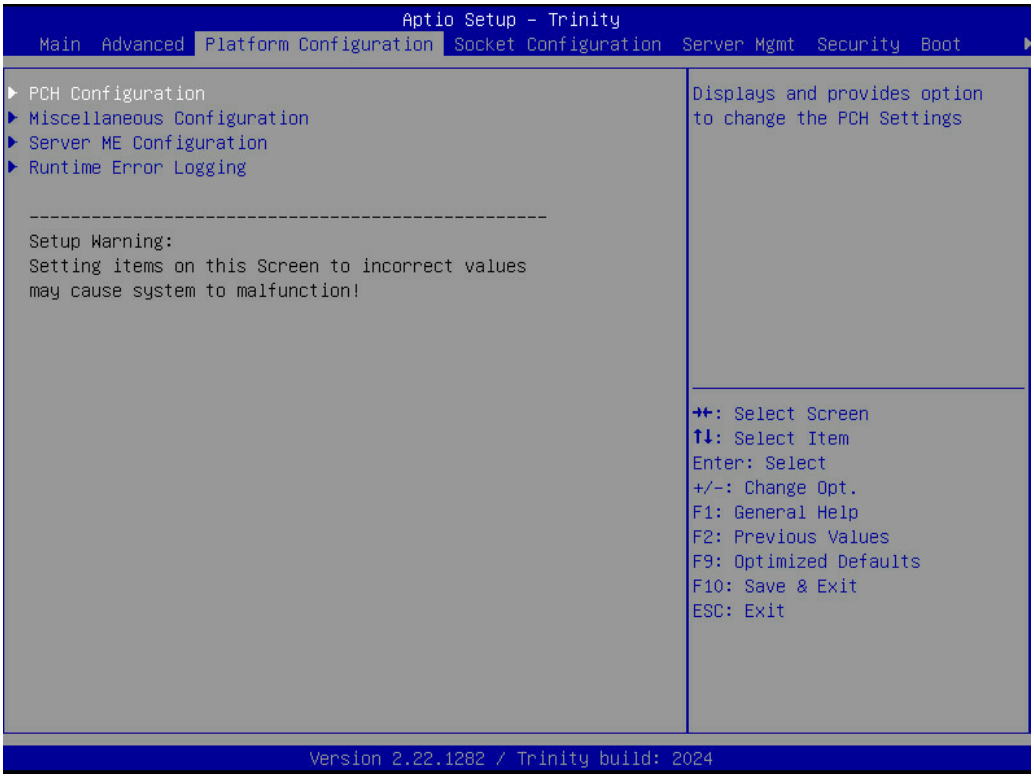

Рисунок 3 – Меню «Platform Configuration»

Наиболее важным в данном меню являются настройки интерфейсов PCI Express в пункте «PCH Configuration» меню «Platform Configuration». Чтобы открыть эти настройки, необходимо выбрать пункт «PCH Configuration», в открывшемся окне перейти на пункт «PCI Express Configuration», затем выбрать порт интерфейса (см. рисунок 4)

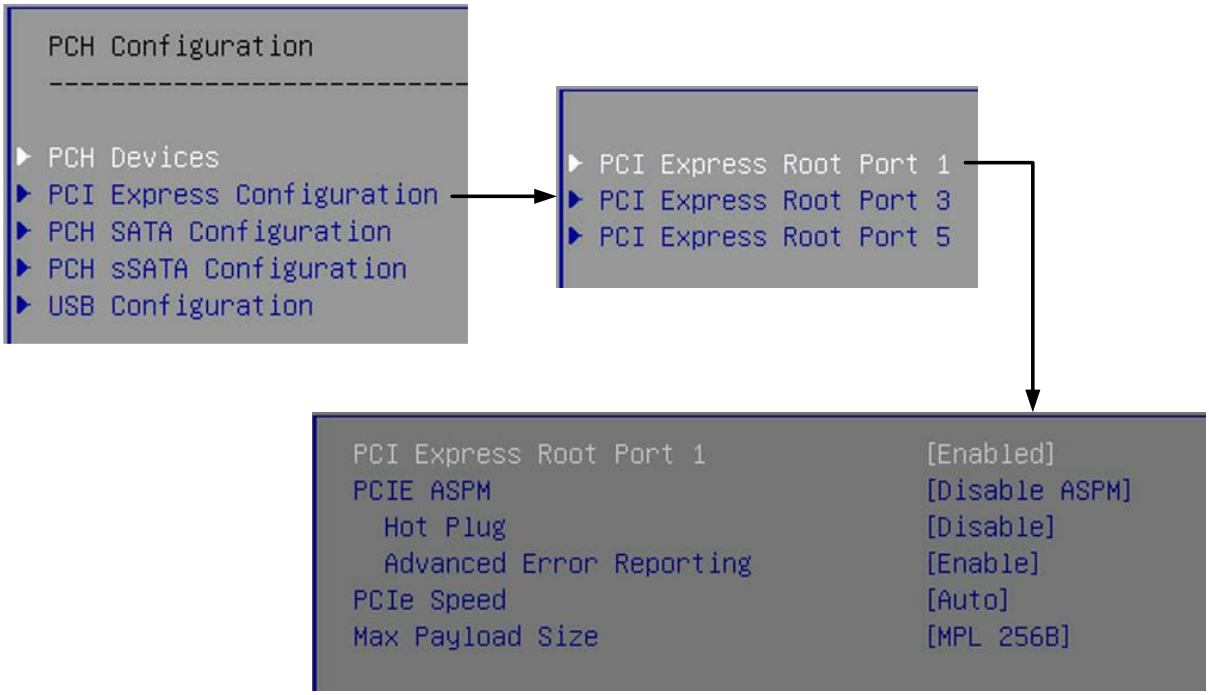

Рисунок 4 – Навигация по вкладкам меню «Platform Configuration»

PCI Express Root Port – ключевой компонент системы, обеспечивающий связь между процессором/чипсетом и устройствами PCIe. Он является «корнем» (root) иерархии PCIe. Все устройства PCIe, подключенные к слотам, взаимодействуют через него.

Настройки «PCI Express Root Port»:

- PCI Express Root Port:

Возможные параметры: Enabled (Включен) / Disabled (Выключен);

- PCIE ASPM – Управление питанием устройств PCIe в активном состоянии:

Возможные параметры: Disable ASPM (ASPM выключен) / ASPM L1 / ASPM Auto;

- ASPM L1 – состояние ввода устройства в режим пониженного энергопотребления, что значительно влияет на производительность;

- ASPM Auto – режим, в котором BIOS сам решает вводить устройство в ASPM L1 или нет;

- Hot Plug – технология, позволяющая подключать и отключать устройства без необходимости выключения питания:

Возможные параметры: Enable (Включен) / Disable (Выключен);

- Advanced Error Reporting (AER) – функция, обеспечивающая расширенные возможности обнаружения и обработки ошибок:

Возможные параметры: Enable (Включен) / Disable (Выключен);

- PCIe Speed – настройка, которая определяет скорость работы слотов PCI Express на материнской плате. Она указывает, какое поколение PCIe будет использоваться для связи между процессором/чипсетом и устройствами, подключенными к слотам PCIe.

Возможные параметры: Auto / Gen1 / Gen2 / Gen3:

- Auto – автоматический режим;
- Gen1 – установка скорости PCIe 1.0;
- Gen2 – установка скорости PCIe 2.0;
- Gen3 – установка скорости PCIe 3.0;

- Max Payload Size – настройка, которая определяет максимальный размер полезной нагрузки в каждом пакете, передаваемом по шине PCI Express. Измеряется в байтах;

Возможные параметры: MPL 128B / MPL 256B:

- MPL 128B – устанавливает максимальную длину пакета данных в 128 байт;
- MPL 256B – устанавливает максимальную длину пакета данных в 256 байт.

Во вкладке «PCH Configuration» меню «Platform Configuration» также присутствуют пункты «PCH SATA Configuration» и «PCH sSATA Configuration» (см. рисунок 4).

PCH SATA Configuration – позволяет управлять работой SATA-портов, выбирать режим работы контроллера и настраивать параметры подключенных SATA-устройств (жестких дисков, SSD, оптических приводов).

PCH sSATA Configuration – Позволяет управлять работой sSATA-портов, выбирать режим работы контроллера и настраивать параметры подключенных sSATA-устройств (жестких дисков, SSD, оптических приводов).

Окно настроек «PCH SATA Configuration» показано на рисунке 5. Выбор и описание настроек «PCH sSATA Configuration» аналогичены.

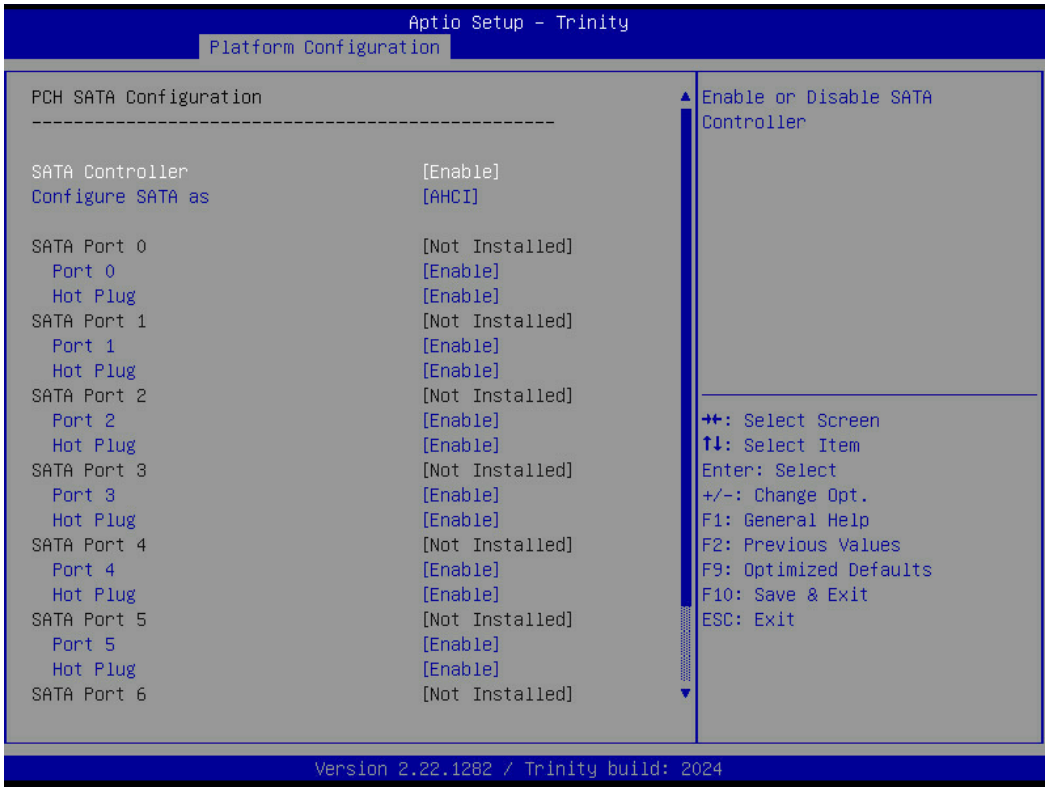

Рисунок 5 – Окно настроек «PCH SATA Configuration»

Описание настроек «PCH SATA Configuration» и «PCH sSATA Configuration»:

- SATA Controller – контроллер, который обеспечивает связь между операционной системой и SATA-устройствами хранения данных:

Возможные параметры: Enable (Включен) / Disable (Выключен);

- Configure SATA as – выбор режима работы контроллера:

Возможные параметры: AHCI / RAID.

AHCI (Advanced Host Controller Interface) – Стандарт для оптимальной работы одного или нескольких SATA дисков, позволяющий использовать функции вроде NCQ и Hot Plug.

RAID (Redundant Array of Independent Disks) – Технология объединения нескольких дисков в массив для скорости, защиты данных или и того, и другого.

- Port X – позволяет включить/отключить выбранный порт.
- Hot Plug – позволяет включить/отключить режим Hot Plug.

7.5. Меню «Socket Configuration» (раздел конфигурации сокета)

Данный раздел ВПО служит для настройки и конфигурации центрального процессора сервера и его окружения. Большинство настроек оказывают существенное влияние на общую производительность сервера.

Установка некорректных значений параметров для вкладок этого меню может привести к сбою всей системы.

Внешний вид меню «Socket Configuration» показан на рисунке 6.

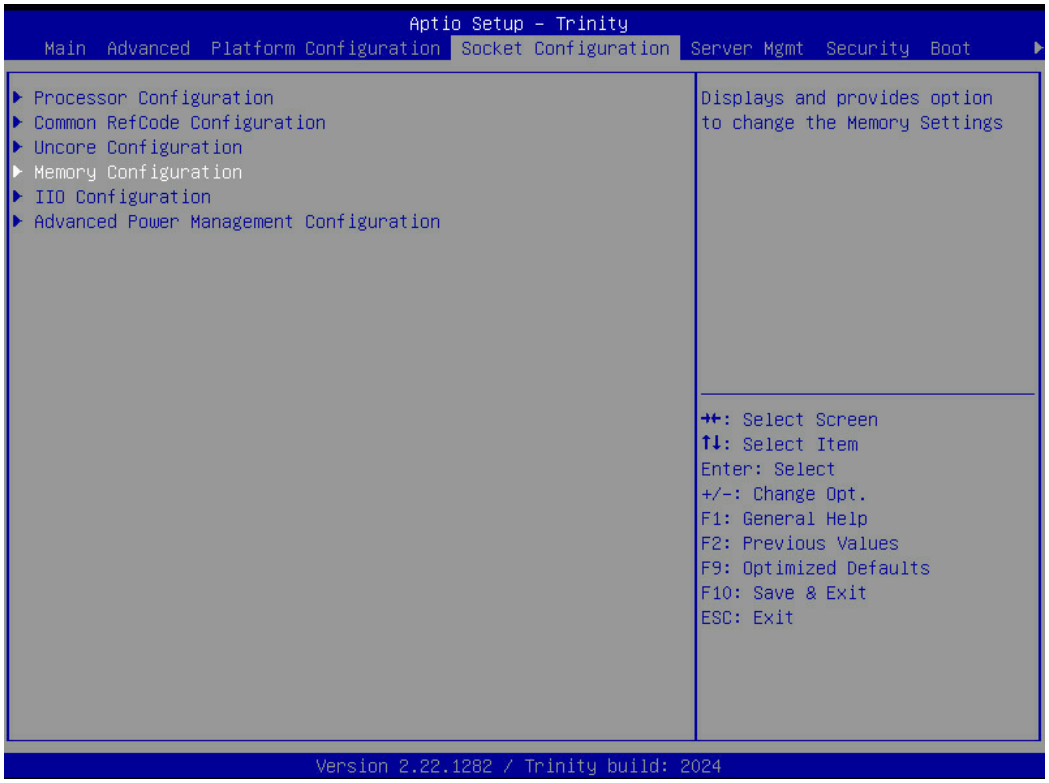

Рисунок 6 – Меню «Socket Configuration»

7.5.1. Подраздел «Processor Configuration» показан на рисунке 7.

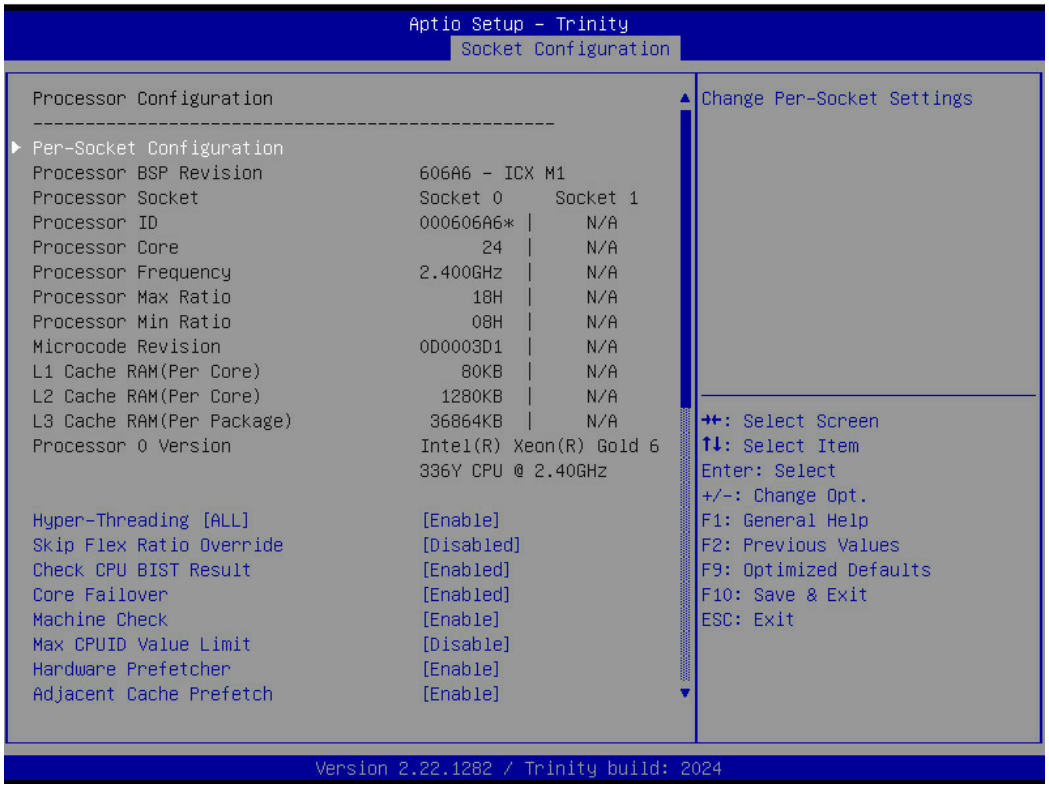

Рисунок 7 – Окно настроек «Processor Configuration»

Подраздел «Processor Configuration» содержит следующие настройки:

- Pre-Socket Configuration – меню, содержащее настройки для ранней инициализации и конфигурирования процессора. Данное меню содержит параметр «Core Disable Bitmap» – настройка, позволяющая в ручном режиме отключить все или какое-то количество ядер процессора. Значения в нём проставляются в

шестнадцатеричной системе. При значении 0 включены все ядра процессора. При значении FFFFFFFFFF выключены все ядра процессора.

- Hyper-Threading – технология, которая позволяет одному физическому ядру процессора представляться операционной системе как два логических ядра. Это достигается за счет того, что каждое физическое ядро может одновременно выполнять две отдельные нити (threads) инструкций, что позволяет более эффективно использовать ресурсы процессора. Возможные параметры: Enable (Включен) / Disable (Выключен).
- Skip Flex Ratio Override – функция, позволяющая процессору снижать множитель частоты ниже номинального (базового) значения, определенного Intel. Возможные параметры: Enabled (Включен) / Disabled (Выключен).
- Check CPU BIST Result – выполняет проверку самотестирования (Built-In Self-Test) и проверяет результат. Возможные параметры: Enabled (Включен) / Disabled (Выключен).
- Core Failover – функция, предназначенная для повышения надежности системы путем автоматического отключения и переназначения неисправного ядра процессора на резервное (если оно доступно) или перераспределения задач на оставшиеся исправные ядра. Возможные параметры: Enabled (Включен) / Disabled (Выключен).
- Machine Check – аппаратный механизм обнаружения ошибок, встроенный в современные процессоры и чипсеты, который используется для выявления серьезных сбоев и ошибок на уровне аппаратного обеспечения. Возможные параметры: Enable (Включен) / Disable (Выключен).
- Max CPUID Value Limit – настройка, которая определяет, какое максимальное значение CPUID (идентификатор процессора) будет возвращено операционной системе и приложениям. Возможные параметры: Enable (Включен) / Disable (Выключен).
- Hardware Prefetcher – аппаратная функция процессоров Intel и AMD, предназначенная для повышения производительности за счет предсказания, какие данные понадобятся процессору в ближайшем будущем, и предварительной загрузки этих данных в кэш-память. Возможные параметры: Enable (Включен) / Disable (Выключен).
- Adjacent Cache Prefetch – аппаратная функция процессоров, являющаяся частным случаем Hardware Prefetcher, и предназначенная для повышения производительности путем предварительной загрузки в кэш соседних (adjacent) строк кэша. Возможные параметры: Enable (Включен) / Disable (Выключен).
- DCU Streamer Prefetcher – разновидность Hardware Prefetcher, разработанная Intel и присутствующая в их процессорах. DCU означает Data Cache Unit, то есть компонент процессора, отвечающий за кэширование данных. Streamer Prefetcher предназначен для обнаружения и предварительной загрузки данных при последовательных (streaming) доступах к памяти. Возможные параметры: Enable (Включен) / Disable (Выключен).
- DCU IP Prefetcher – разновидность Hardware Prefetcher. Он предсказывает, какие данные понадобятся, основываясь на анализе указателя инструкции (instruction

pointer) и потока инструкций, выполняемых процессором. Возможные параметры: Enable (Включен) / Disable (Выключен).

- LLC Prefetch – аппаратная функция, которая работает на уровне кэша последнего уровня (Last Level Cache) процессора. LLC является последним и самым большим уровнем кэш-памяти, общим для всех ядер процессора. Возможные параметры: Enable (Включен) / Disable (Выключен).

- DCU Mode – определяет режим работы Data Cache Unit. Возможные параметры: Normal (Обычный) / Mirror-mode (Зеркальный). Где:

  - Normal mode – выбирается в большинстве случаев. Высокая производительность.

  - Mirror-mode – пишет сразу в две разные области кэш-памяти. Больше надежность – меньше производительность.

- BSP Selection – позволяет выбрать начальный процессор для запуска системы. Возможные параметры: Socket X (Выбрать сокет) / Auto (Автоматический выбор).

- Extended APIC – настройка, которая включает или отключает использование расширенного программируемого контроллера прерываний (x2APIC). Возможные параметры: Enable (Включен) / Disable (Выключен).

- APIC Physical Mode – определяет, как прерывания направляются к ядрам процессора: напрямую (физический режим) или через логические группы. Возможные параметры: Enable (Включен) / Disable (Выключен).

- PECI (Platform Environment Control Interface) – интерфейс, который обеспечивает связь между процессором и другими компонентами системы для целей мониторинга и управления параметрами окружающей среды. Возможные параметры: Enable (Включен) / Disable (Выключен).

При включенном PECI появляются две дополнительные настройки:

- Legacy Agent – устаревший контроллер шины SMBus
- SMBus Agent – новейший контроллер шины SMBus

Также имеют параметры – Enable (Включен) / Disable (Выключен).

- SMBus Error Recovery – настройка, которая управляет механизмом восстановления после ошибок на шине SMBus. Возможные параметры: Enable (Включен) / Disable (Выключен).

- Intel TXT (Trusted Execution Technology) – технология, разработанная Intel, обеспечивающая аппаратные средства для создания более безопасной вычислительной среды. Она позволяет операционной системе и приложениям создавать доверенные зоны, в которых конфиденциальные данные и критически важный код могут быть изолированы от других частей системы. Возможные параметры: Enable (Включен) / Disable (Выключен).

- VMX (Virtual Machine Extensions) – набор аппаратных расширений, разработанных Intel, позволяет процессору более эффективно поддерживать запуск и управление виртуальными машинами. Возможные параметры: Enable (Включен) / Disable (Выключен).

- SMX (Safer Mode Extensions) – Добавляет дополнительные механизмы защиты в комплекте с Intel TXT. Возможные параметры: Enable (Включен) / Disable (Выключен).

- Lock Chipset – настройка, которая контролирует возможность записи в определенные регистры чипсета после завершения процесса загрузки. Она определяет, насколько защищен чипсет от изменений в его настройках после того, как операционная система начала работать. Возможные параметры: Enable (Включен) / Disable (Выключен).

- MSR Lock Control – настройка, позволяющая заблокировать возможность записи в модельно-специфичные регистры (MSRs) процессора после загрузки системы. Возможные параметры: Enable (Включен) / Disable (Выключен).

- PPIN Control – настройка, которая определяет, кто управляет политикой Physical Presence: BIOS или ОС. Physical Presence используется для подтверждения того, что пользователь физически находится перед компьютером и может подтвердить выполнение определенных действий, требующих повышенной безопасности.

Возможные параметры:

- Unlock/Enable (Разблокирован/Включен);
- Lock/Disable (Заблокирован/Выключен).

- AES-NI (Advanced Encryption Standard New Instructions) – набор инструкций для ускорения шифрования и дешифрования данных с использованием алгоритма AES. Возможные параметры: Enable (Включен) / Disable (Выключен).

- Total Memory Encryption (TME) – технология, которая шифрует всю системную память для защиты от физических атак и других угроз. Возможные параметры: Enabled (Включен) / Disabled (Выключен).

- Limit CPU PA to 46 bits – настройка, которая ограничивает количество бит, используемых процессором для адресации физической памяти. Возможные параметры: Enable (Включен) / Disable (Выключен).

7.5.2. Подраздел «Common RefCode Configuration» показан на рисунке 8.

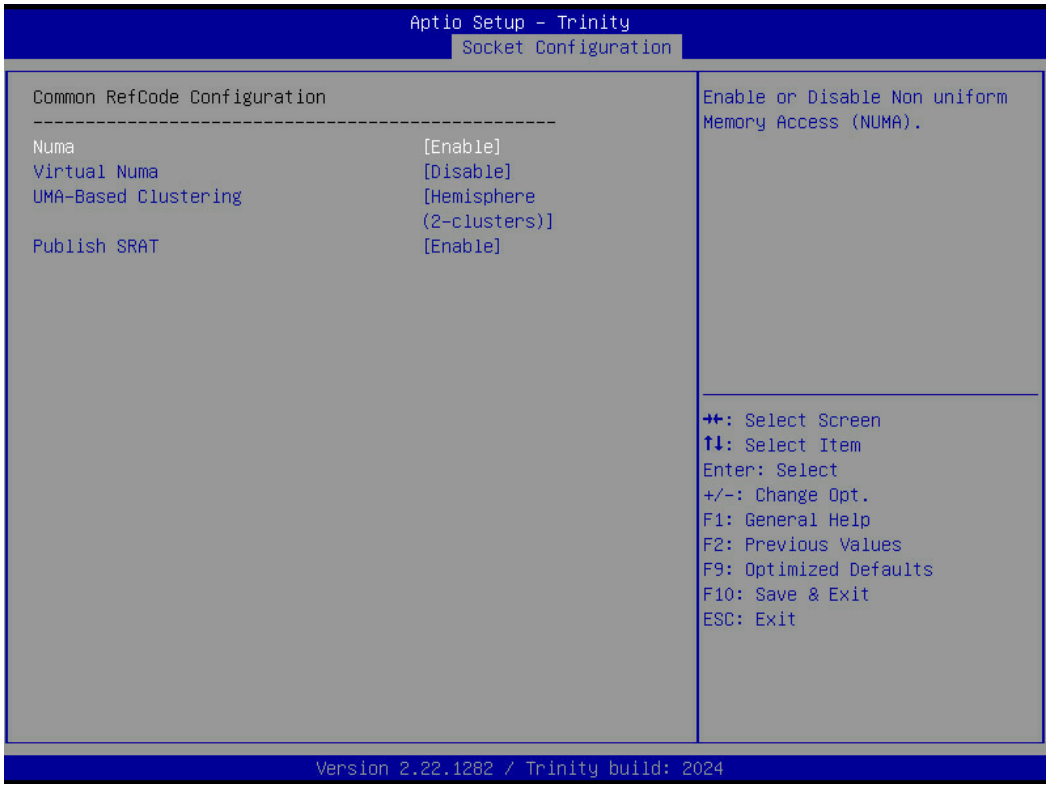

Рисунок 8 – Окно настроек «Common RefCode Configuration»

Подраздел предоставляет возможности по настройке следующих параметров:

- Numa (Non-Uniform Memory Access) – архитектура памяти, используемая в многопроцессорных системах, где время доступа к памяти зависит от местоположения памяти относительно процессора. Возможные параметры: Enable (Включен) / Disable (Выключен).

- Virtual Numa – технология, которая предоставляет виртуальным машинам видимость архитектуры NUMA физической системы, на которой они работают. Возможные параметры: Enable (Включен) / Disable (Выключен).

- UMA-Based Clustering – архитектура многопроцессорных систем, которая объединяет несколько вычислительных узлов в кластер с единым адресным пространством памяти. Возможные параметры:

  - Disable (All2All) – Отключает NUMA-оптимизации, представляя систему как единый блок памяти (UMA), упрощая совместимость.

  - Hemisphere (2-clusters) – Включает NUMA, разделяя систему на два кластера процессоров и памяти.

- Publish SRAT – настройка, которая определяет, должна ли система сообщать операционной системе информацию о SRAT (System Resource Allocation Table). SRAT – таблица ACPI (Advanced Configuration and Power Interface), которая описывает, как физические ресурсы системы (например, процессоры, память, устройства ввода-вывода) распределены между узлами NUMA). Возможные параметры: Enable (Включен) / Disable (Выключен).

7.5.3. Подраздел «Uncore Configuration» показан на рисунке 9.

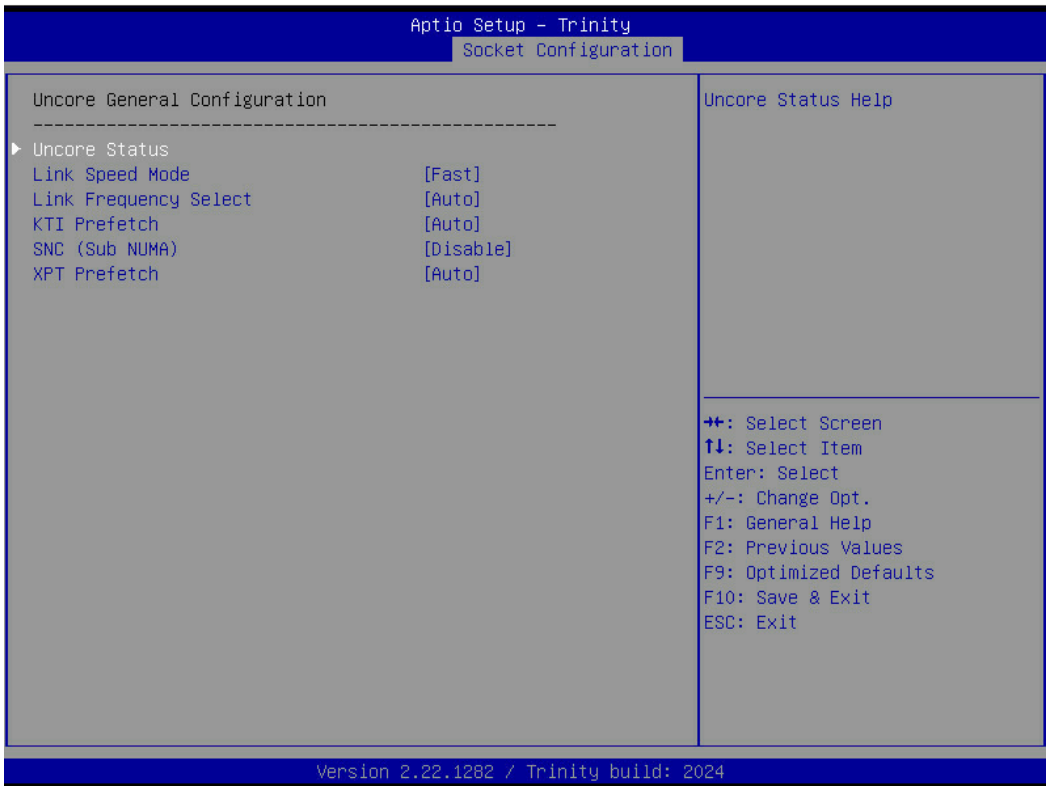

Рисунок 9 – Окно настроек «Uncore Configuration»

Подраздел предоставляет возможности по настройке следующих параметров:

- Uncore Status – информация о состоянии и работе Uncore (не ядерных) компонентов процессора, таких как контроллер памяти, контроллер ввода-вывода и кэш последнего уровня. Предоставляет только данные, параметров не имеет.

- Link Speed Mode – настройка, определяющая скорость межпроцессорного соединения в многопроцессорных системах Intel Xeon. Имеет два режима работы:

  - Fast – работает на скорости POR (Power-On Reset), которая обычно является максимально возможной скоростью, определяемой при старте системы.

  - Slow – работает на скорости по умолчанию, которая является более низкой, чем POR.

- Link Frequency Select – Определяет частоту работы шины или соединения, соединяющего процессор с другими компонентами системы. Возможные параметры:

  - 9.6GT/s – Устанавливает частоту работы шины на 9.6 Gigatransfers;

  - 10.4GT/s – Устанавливает частоту работы шины на 10.4 Gigatransfers;

  - 11.2GT/s – Устанавливает частоту работы шины на 11.2 Gigatransfers;

  - Auto – Автоматически определяет оптимальную частоту работы шины;

  - Use Per Link Setting – Позволяет настраивать частоту для каждой отдельной линии или канала.

- KTI Prefetch – настройка, связанная с предвыборкой данных в системах, использующих технологию KTI, которая является кодовым именем для UPI (Ultra Path Interconnect), используемой в процессорах Intel Xeon Scalable. Возможные параметры: Enable (Включен) / Disable (Выключен) / Auto (Авто-режим).

- SNC (Sub NUMA) – технология, используемая в многопроцессорных системах Intel Xeon Scalable, которая разделяет каждый физический процессор на несколько

логических NUMA-узлов, уменьшая задержки доступа к памяти и снижая конкуренцию за ресурсы. Возможные параметры: Enable SNC2 (Включен) / Disable (Выключен).

- XPT Prefetch – аналог KTI Prefetch для процессоров AMD. Возможные параметры: Enable (Включен) / Disable (Выключен) / Auto (Авто-режим).

7.5.4. Подраздел «Memory Configuration» показан на рисунке» 10.

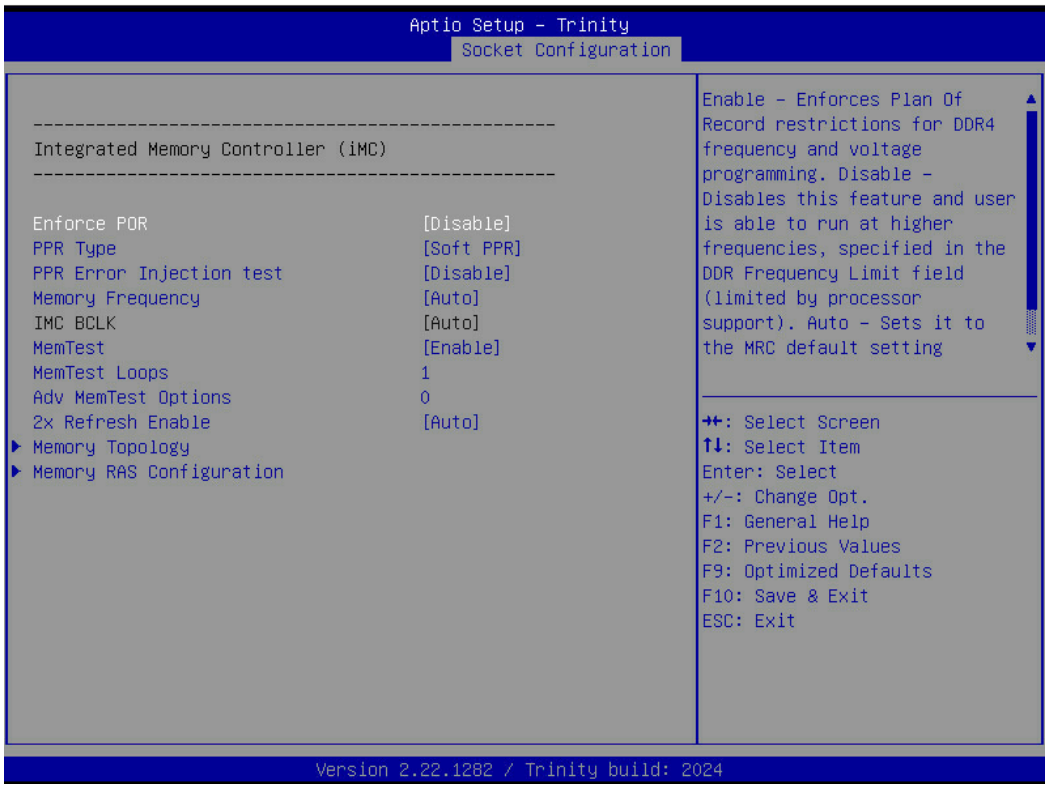

Рисунок 10 – Окно настроек «Memory Configuration»

Подраздел предоставляет возможности по настройке следующих параметров:

- Enforce POR – принудительно загружает оперативную память на безопасной, стабильной скорости, указанной в спецификации. Помогает в диагностике проблем с RAM, временно отключая канал с проблемной планкой. Возможные параметры: POR (Включен) / Disable (Выключен)

В случае включения данной настройки появляется дополнительная возможность конфигурирования – Enforce Population POR. Эта настройка позволяет обеспечить соответствие установленной оперативной памяти конфигурациям, которые были протестированы и признаны производителем материнской платы стабильными и поддерживаемыми. Имеет следующие параметры:

- Disable Enforcement – отключает все ограничения, связанные с конфигурацией оперативной памяти, определенные в POR;

- Enforce Supported Populations – система будет загружаться только в том случае, если установленная конфигурация памяти соответствует поддерживаемым конфигурациям, определенным в POR;

- Enforce Validated Populations – система будет загружаться только в том случае, если установленная конфигурация памяти соответствует валидированным конфигурациям, определенным в POR.

Важное уточнение – поддерживаемые (supported) означает комбинации модулей памяти (количество, тип, емкость), которые были протестированы и признаны работающими производителем материнской платы, но не обязательно оптимизированы.

Валидированные (validated) означает комбинации модулей памяти, которые были не только протестированы и признаны работающими, но и оптимизированы для обеспечения максимальной производительности.

- PPR Type (Post Package Repair) – это механизм, используемый для обнаружения и исправления дефектов в микросхемах памяти. Возможные параметры:
  - PPR Disabled – отключает функцию PPR;
  - Hard PPR – выполняется с использованием аппаратных средств;
  - Soft PPR – выполняется с использованием программных средств.
- PPR Error Injection test – используется для проверки эффективности и корректности работы механизма PPR. Она имитирует ошибки в оперативной памяти, чтобы убедиться, что система PPR правильно обнаруживает и обрабатывает эти ошибки. Возможные параметры: Enable (Включен) / Disable (Выключен).
- Memory Frequency – определяет скорость оперативной памяти. Возможные параметры:

Auto – авторежим;

2133 – устанавливает скорость на 2133 МГц;

2400 – устанавливает скорость на 2400 МГц;

2666 – устанавливает скорость на 2666 МГц;

2933 – устанавливает скорость на 2933 МГц;

3200 – устанавливает скорость на 3200 МГц.

- IMC BCLK – расширенная настройка, позволяющая изменять базовую частоту контроллера памяти. Используется при разгоне оперативной памяти. Изменений параметров не предусмотрено, стоит в автоматическом режиме.
- MemTest – инструмент тестирования оперативной памяти. Возможные параметры: Enable (Включен) / Disable (Выключен).
- MemTest Loops – количество итераций проведения тестирования. Значение 0 запускает бесконечный тест.
- Adv MemTest Options – позволяет выставить дополнительный настройки для теста. Имеет большое количество шаблонов.Для их установки требуется представить набор флагов с помощью битовой маски. Например, значение 00000000000100000000 включит шаблон DATARET.
- 2x Refresh Enable – удваивает стандартную частоту обновления памяти. Возможные параметры: Enable (Включен) / Disable (Выключен) / Auto (Авто-режим).

- Memory Topology – меню, которое включает в себя информацию о количестве модулей памяти, их расположении в слотах, объеме и скорости каждого модуля, и канале памяти, к которому они подключены.
- Memory RAS Configuration:
  - Mirror Mode – режим работы оперативной памяти, при котором данные записываются одновременно в два идентичных набора модулей памяти. Возможные параметры:
    - Disabled (Выключен)
    - Full Mirror Mode (Полностью зеркальный режим) – включение режима полного зеркалирования (Full Mirror Mode) приведет к тому, что вся память, относящаяся к ILM (Intel Local Memory) в системе, будет работать в режиме зеркалирования.
  - Memory Correctable Error Flood Policy – устанавливает политику обработки ошибок корректировок памяти. Возможные параметры:
    - Disable (Выключен) – отключает политику защиты.
    - Once (Один раз) – система выдаст предупреждение только один раз.
    - Frequency (Частота) – система будет выдавать предупреждения с определенной частотой.
  - Memory CE Flood Time Window – определяет временной интервал, в течение которого система отслеживает количество корректируемых ошибок памяти. Задается в секундах.
  - Memory CE Flood Threshold – определяет лимит количества корректируемых ошибок.
  - Correctable Error Threshold – определяет максимальное количество корректируемых ошибок для каждой ячейки памяти, допустимое до активации механизмов. Значение настраивается в диапазоне от 1 (0x01) до 32767 (0x7fff).
  - Trigger SW Error Threshold – определяет, сколько ошибок должно произойти (корректируемых или некорректируемых, в зависимости от того, к чему относится эта настройка), чтобы система выполнила какое-то действие через программное обеспечение. Возможные параметры: Enabled (Включен) / Disabled (Выключен).
  - Leaky bucket time window based interface – когда эта настройка включена, пороговые значения (Threshold) и другие настройки используются для определения того, как система реагирует на ошибки памяти. Если выключен, то эти пороги не действуют. Возможные параметры: Enabled (Включен) / Disabled (Выключен).
  - Leaky bucket low bit и Leaky bucket high bit – эти две настройки определяют, какие биты адреса памяти (от Low Bit до High Bit включительно) используются для разделения всей доступной оперативной памяти на отдельные, логические области - “ведра”.

Возможные значения начинаются от 1 (0x1) до 41 (0x29).

  - Partial Cache Line Sparing (PCLS) – это механизм, который позволяет системе заменять или изолировать дефектные части кэш-линии в оперативной памяти. Возможные параметры: Enabled (Включен) / Disabled (Выключен).

- ADDDC Sparing (Address Data Dependent Data Correction Sparing) – это продвинутый механизм коррекции и замещения ошибок в оперативной памяти, который основывается на более глубоком анализе характера ошибок и адресов, где они возникают. Возможные параметры: Enabled (Включен) / Disabled (Выключен).

- При включении данного механизма появляются дополнительные настройки:

- Enable ADDDC Error Injection – настройка, которая позволяет искусственно внедрять ошибки в оперативную память, когда включен механизм ADDDC Sparing. Возможные параметры: Enabled (Включен) / Disabled (Выключен).

- Column Correction Disable – настройка, позволяющая включать или отключать коррекцию ошибок в колонках DRAM. Возможные параметры: Enable (Включен) / Disable (Выключен).

- Set PMem Die Sparing – настройка, позволяющая включать или отключать замену дефектных кристаллов в модулях энергонезависимой памяти (PMem). Возможные параметры: Enabled (Включен) / Disabled (Выключен).

- Patrol Scrub – настройка, которая управляет механизмом периодического сканирования оперативной памяти для обнаружения и исправления ошибок. Также имеет настройку интервала, от 1 до 24. Значение 0 означает авторежим. Возможные параметры:

  - Enabled (Включена)
  - Disabled (Выключена)
  - Enable at End of POST (Один раз при загрузке)

7.5.5. Подраздел «IIO Configuration» показан на рисунке 11.

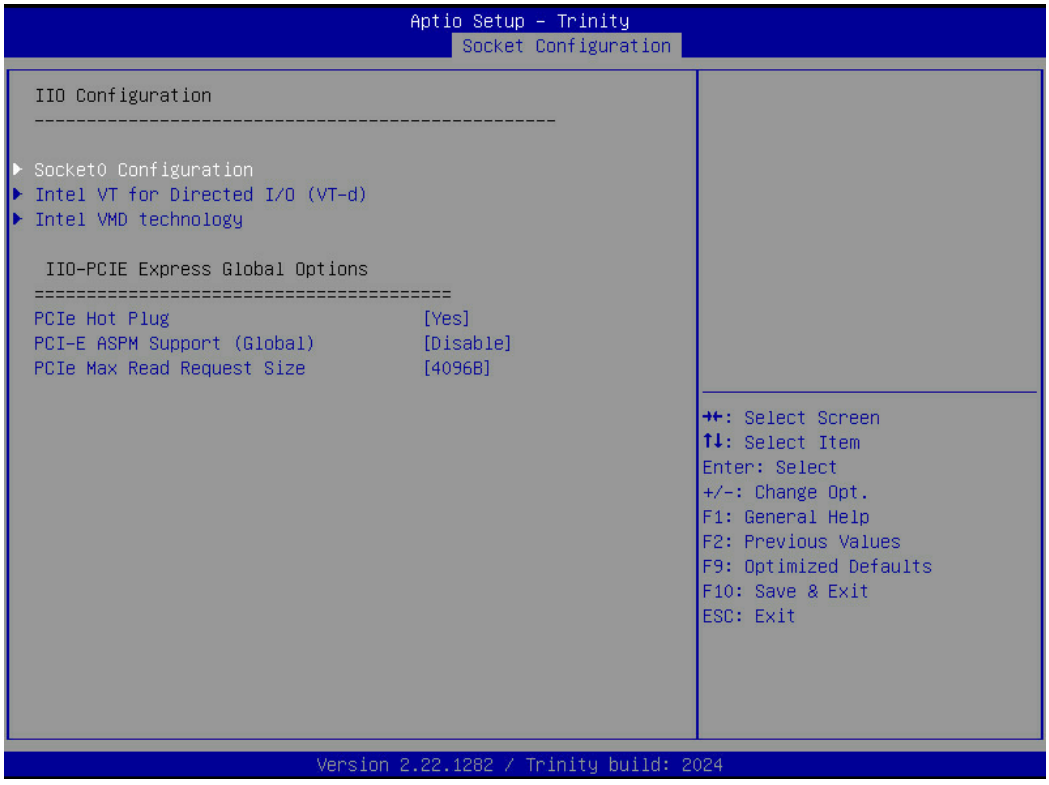

Рисунок 11 – Окно настроек «IIO Configuration»

В данном разделе осуществляется тонкая настройка PCIe линий.

Настройки параметра «Socket0 Configuration» показаны на рисунке 12.

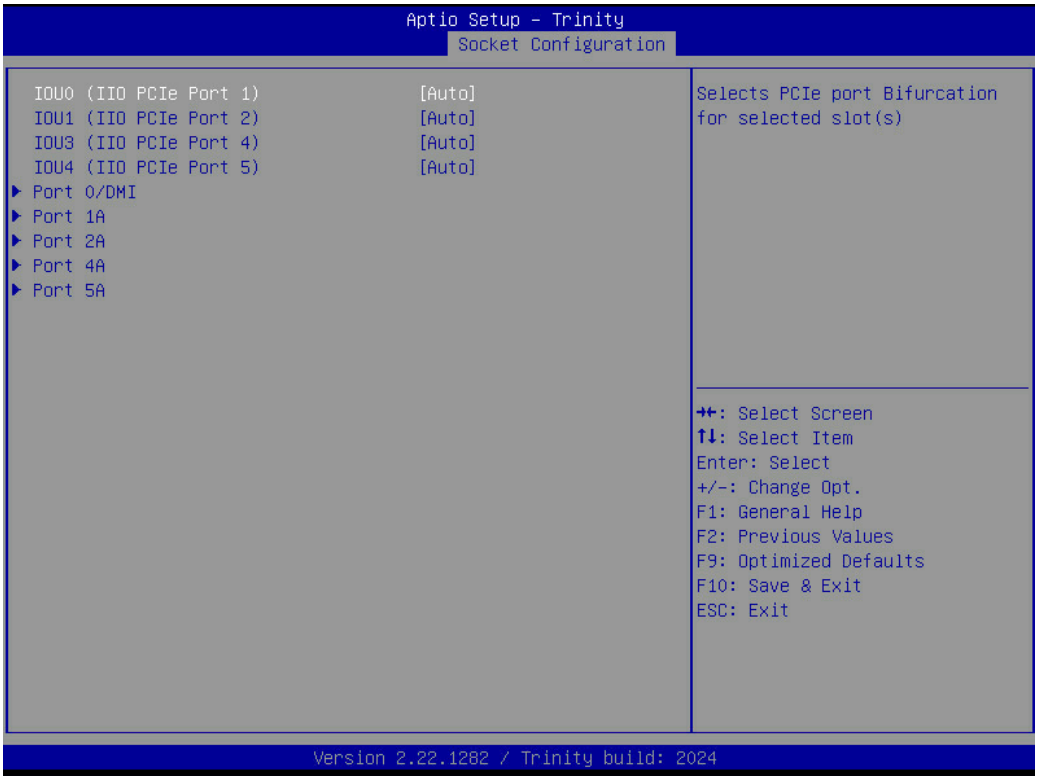

Рисунок 12 – Окно настроек «Socket0 Configuration»

IOU0, IOU1, IOU3, IOU4 – Назначает бифуркацию PCIe портов. Возможные параметры:

- Auto – автоматический режим;
- x4x4x4x4 – выставление ширины шины в режиме PCI x4;
- x4x4x8 – не используется;
- x8x4x4 – не используется;
- x8x8 – выставление ширины шины в режиме PCI x8;
- x16 – выставление ширины шины в режиме PCI x16.

Во вкладках «Port 1A» доступны настройки настроить отдельный PCie слот (см. рисунок 13). Для остальных Port вышеописанные настройки идентичны.

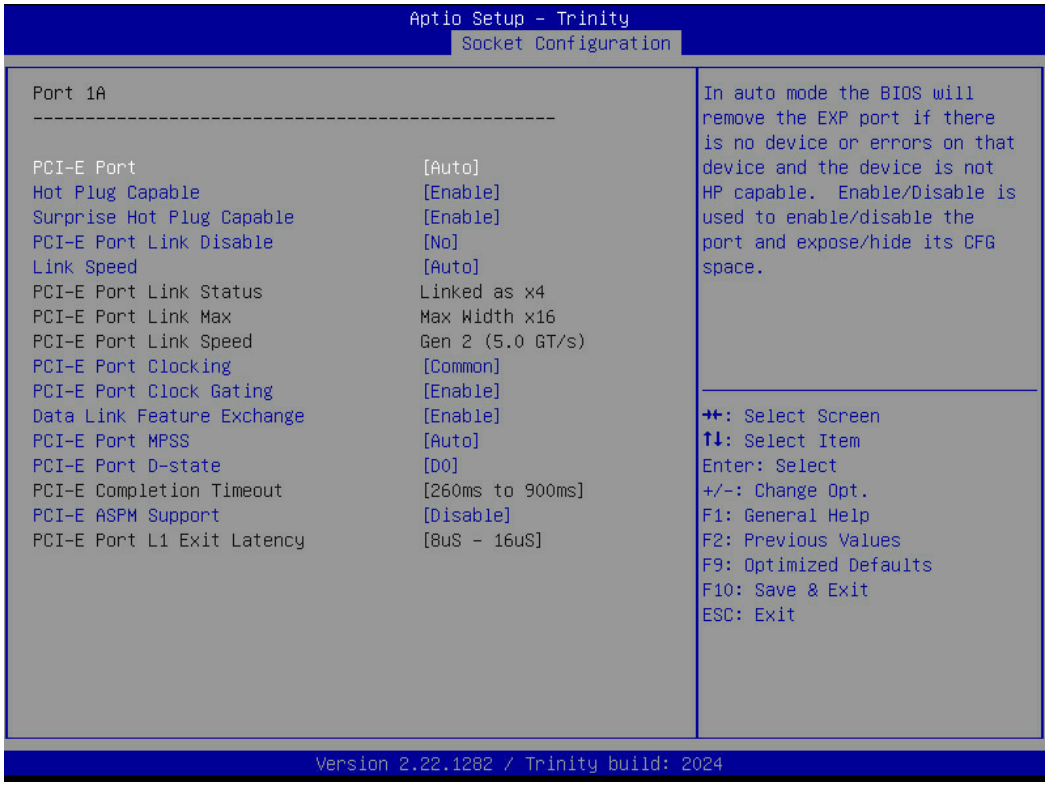

Рисунок 13 – Окно настроек «Port 1A»

PCI-E Port – позволяет включить/выключить порт или оставить его в автоматическом режиме.

Hot Plug Capable – позволяет включить/выключить порт в режиме «Hot Plug» или оставить его в автоматическом режиме.

Surprise Hot Plug Capable – позволяет включить/выключить порт в режиме «Неожиданного горячего подключения». То есть без уведомления ОС об извлечении устройства.

PCI-E Port Link Disable – позволяет заблокировать работу устройства, однако продолжать выдавать о нём конфигурационную информацию. Возможные параметры: Yes (Включен) / No (Выключен).

Link Speed – позволяет установить скорость (поколение) порта.

Возможные параметры:

- Auto – Автоматический режим;
- Gen1 – устанавливает скорость соединения PCI-E 1.0 (2.5 GT/s);
- Gen2 – устанавливает скорость соединения PCI-E 2.0 (5 GT/s);
- Gen3 – устанавливает скорость соединения PCI-E 3.0 (8 GT/s);
- Gen4 – устанавливает скорость соединения PCI-E 4.0 (16 GT/s);

PCI-E Port Link Status – актуальная скорость порта в линиях. (Например, x8)

PCI-E Port Link Max – максимально возможная скорость данного порта (например, x16).

PCI-E Port Link Speed – показывает актуальный режим работы порта (например, Gen2).

PCI-E Port Clocking – настройка определяет, как генерируется тактовый сигнал для PCI-E порта. Тактовый сигнал необходим для синхронизации передачи данных между портом и подключенным устройством. Имеет два параметра:

- Distinct – каждый порт имеет независимый тактовый генератор;
- Common – несколько портов используют общий тактовый генератор.

PCI-E Port Clock Gating – настройка управляет функцией “затвора тактового сигнала” (clock gating) для PCI-E порта. Clock gating – это метод энергосбережения, при котором тактовый сигнал к порту отключается, когда порт не используется активно.

Возможные параметры: Enable (Включен) / Disable (Выключен).

Data Link Feature Exchange – настройка управляет поддержкой обмена информацией о поддерживаемых возможностях между PCI-E портом и устройством через Data Link Layer. Возможные параметры: Enable (Включен) / Disable (Выключен).

PCI-E Port MPSS (Maximum Payload Size Supported) – Определяет максимальный размер полезной нагрузки PCI-E транзакций, поддерживаемый устройством PCI-E. Возможные параметры:

- 128B – фиксирует размер нагрузки в 128 байтах;
- 256B – фиксирует размер нагрузки в 256 байтах;
- 512B – фиксирует размер нагрузки в 512 байтах;
- Auto – автоматический режим.

PCI-E Port D-State – определяет состояние питания для PCI-E порта, когда он находится в режиме простоя. D-states – это различные состояния питания, в которых устройство может находиться для экономии энергии. Возможные параметры:

- D0 – нормальный режим работы;
- D3Hot – состояние пониженного энергопотребления.

Значение настройки PCIe Completion Timeout не меняется и установлено в пределах от 260 миллисекунд до 900 миллисекунд.

PCI-E ASPM Support – поддержка ASPM (Active State Power Management) для PCI-E root порта. Возможные параметры:

- Auto – авторежим;
- Disable – отключение ASPM для данного порта.

PCI-E Port L1 Exit Latency – данная настройка разблокируется в случае выбора авторежима предыдущей настройки. Позволяет контролировать компромисс между энергопотреблением и отзывчивостью системы при использовании состояний пониженного энергопотребления для порта PCI-E. Имеет восемь вариантов параметров: от <1uS (микросекунды) до >64uS.

Сразу после «Socket0 Configuration» идёт настройка – Intel VT for Directed I/O (VT-d) – технология виртуализации, которая позволяет ВМ иметь прямой доступ к периферийным устройствам, повышая производительность, безопасность и эффективность использования ресурсов. Возможные параметры: Enable (Включен) / Disable (Выключен).

И также есть дополнительная – Interrupt Remapping.

Interrupt Remapping – механизм, перенаправляющий прерывания от периферийных устройств к виртуальным машинам более эффективно и безопасно. Возможные параметры: Enable (Включен) / Disable (Выключен) / Auto (Авто-режим).

Intel Volume Management Device (VMD) – это технология, предназначенная для упрощения управления NVMe SSD в корпоративных и серверных средах. Внутри себя имеет настройки для PCH (упомянутых выше) и IOU портов.

Возможные параметры: Enable (Включен) / Disable (Выключен).

Оставшиеся настройки этого подраздела:

PCIe Hot Plug – отключает Hot Plug глобально.

PCI-E ASPM Support (Global) – отключает ASPM глобально.

PCIe Max Read Request Size – определяет максимальный размер запросов на чтение данных, отправляемых устройством PCIe. Возможные значения: от Keep Default (он же авторежим) и 128 байт до 4096 байт.

7.5.6. Подраздел «Advanced Power Management Configuration» показан на рисунке 14.

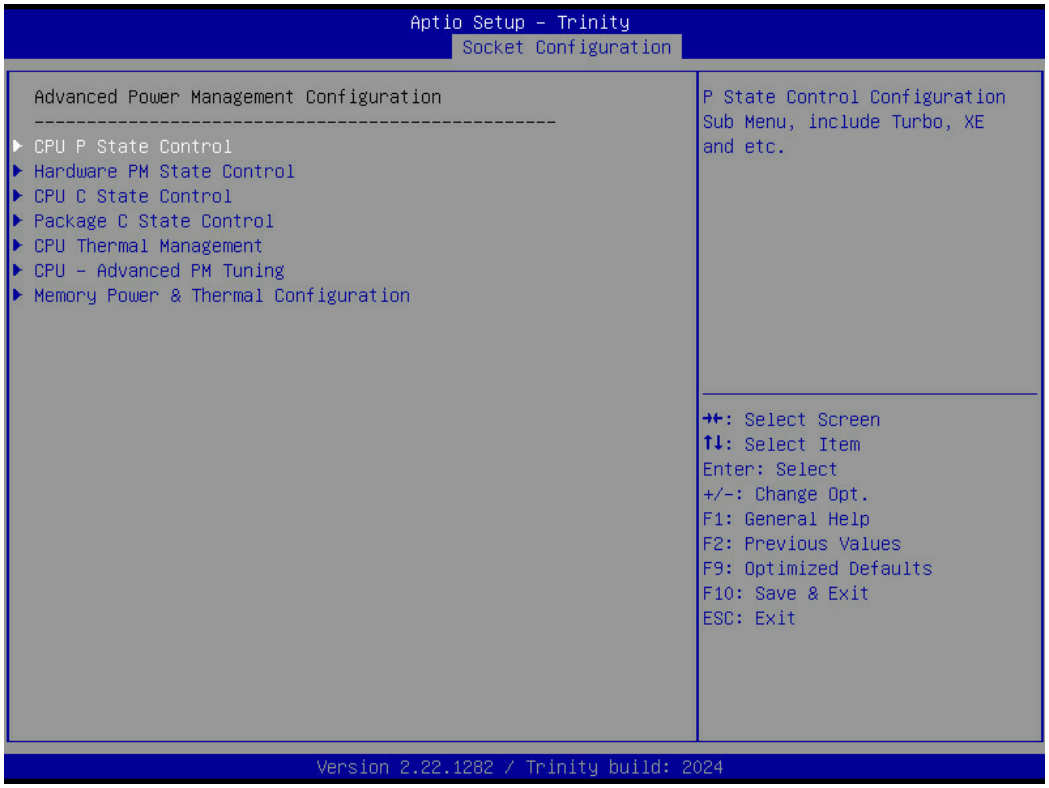

Рисунок 14 – Окно настроек «Advanced Power Management Configuration»

Меню «CPU P State Control» (см. рисунок 15) – технология управления энергопотреблением процессора путем изменения его частоты и напряжения.

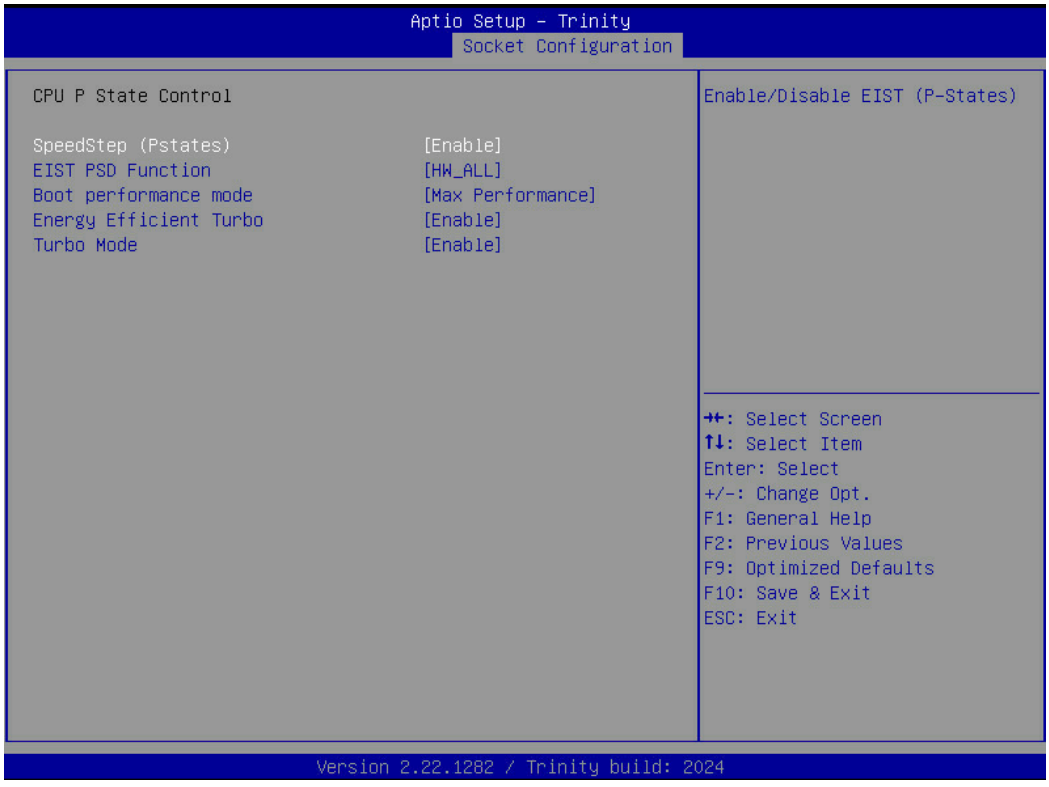

Рисунок 15 – Окно настроек «CPU P State Control»

Внутри данного меню есть пять настроек:

- SpeedStep – технология управления энергопотреблением процессоров Intel, позволяет динамически регулировать частоту и напряжение процессора в зависимости от текущей нагрузки. Возможные параметры: Enable (Включен) / Disable (Выключен).
- EIST PSD Function – механизм, который позволяет SpeedStep более эффективно управлять энергопотреблением, учитывая различные Power Supply Domains (PSD) внутри процессора. Возможные параметры:
  - HW_ALL – управляет аппаратно.
  - SW_ALL – управляет программно.
- Boot performance mode – настройка, которая определяет, как процессор будет вести себя во время начальной загрузки системы. Она влияет на скорость и энергопотребление в момент запуска операционной системы. Имеет три параметра:
  - Max Performance – максимальная производительность при загрузке системы.
  - Max Efficient – минимизирует энергопотребление и тепловыделение при загрузке системы.
  - Set by Intel Node Manager – в этом режиме управление производительностью во время загрузки передается Intel Node Manager.
- Energy Efficient Turbo (EET) – режим работы, в котором частота ядра процессора регулируется в пределах турбо-диапазона в зависимости от нагрузки. Возможные параметры: Enable (Включен) / Disable (Выключен).
- Turbo Mode – определяет возможность динамического повышения тактовой частоты процессора выше базовой (Turbo Boost) в рамках системы управления энергопотреблением. Возможные параметры: Enable (Включен) / Disable (Выключен).

Меню «Hardware PM State Control» (см. рисунок 16) – предоставляет настройки для управления питанием различных аппаратных компонентов системы, таких как процессор, чипсет, жесткие диски, сетевые адаптеры и другие устройства.

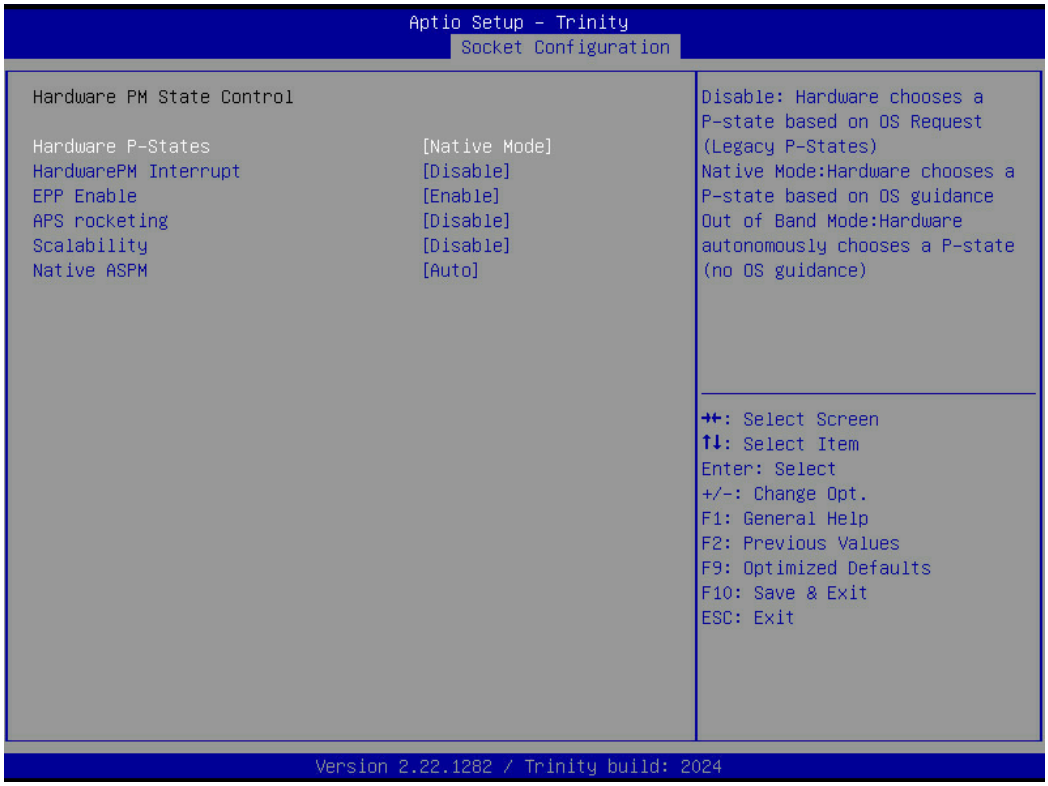

Рисунок 16 – Окно настроек «Hardware PM State Control»

Hardware P-States – определяет, как процессор управляет своими состояниями питания для экономии энергии и регулировки производительности. Возможные параметры:

- Disable (Выключен) – управление частотой и напряжением процессора полностью делегируется ОС;
- Native Mode – в этом режиме BIOS и процессор сотрудничают с ОС для определения оптимальных состояний питания;
- Out of Band Mode - процессор и BIOS полностью игнорируют рекомендации ОС и самостоятельно определяют оптимальные состояния питания, основываясь на аппаратных датчиках и алгоритмах;
- Native Mode with No Legacy Support – тот же Native Mode, но без поддержки Legacy функций.

Каждый из параметров блокирует и\или добавляет новые настройки:

- Hardware PM Interrupt – управляет тем, сообщает ли оборудование операционной системе о событиях, связанных с управлением питанием. Возможные параметры: Enable (Включен) / Disable (Выключен).
- EPP Enable – является переключателем, который определяет, какая из технологий будет использоваться. Возможные параметры:
  - Disable (Выключен) – включает режим Energy Performance Bias (EPB) для управления энергопотреблением.
  - Enable (Включен) – включает режим Energy Performance Preference для управления энергопотреблением.
- EPP Profile – определяет профиль работы EPP технологии. Имеет следующие параметры:
  - Performance (Производительность);

- Balanced Performance (Сбалансированная производительность);
- Balanced Power (Сбалансированное энергосбережение);
- Power (Энергосбережение);

- APS Rocketing – определяет, как быстро процессор достигнет своей максимальной турбо-частоты, когда это необходимо. Возможные параметры: Enable (Включен) / Disable (Выключен).

- Scalability – настройка определяет возможность масштабирования производительности. Возможные параметры: Enable (Включен) / Disable (Выключен).

- Native ASPM – настройка BIOS, которая управляет управлением питанием шины PCIe со стороны операционной системы. Возможные параметры: Enable (Включен) / Disable (Выключен) / Auto (Авто-режим).

Меню «CPU C State Control» (см. рисунок 17) – отвечает за управление режимами простоя процессора, также известными как C-состояния.

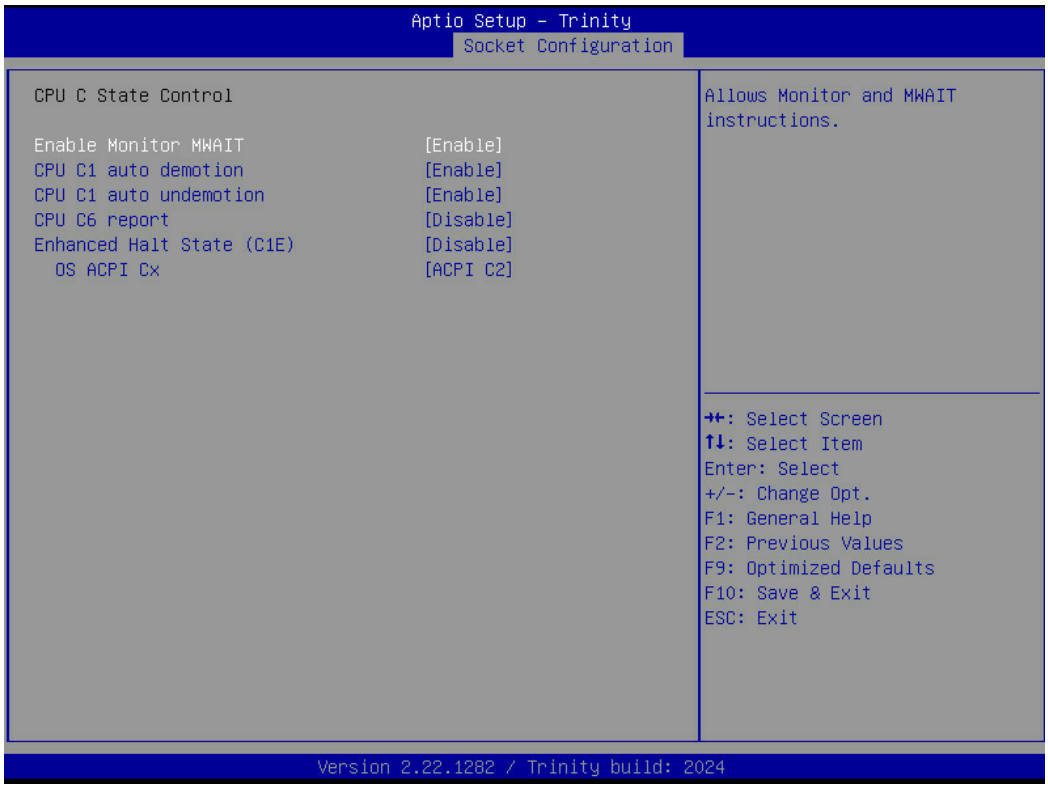

Рисунок 17 – Окно настроек «CPU C State Control»

Enable Monitor MWAIT – это технология управления питанием процессора, которая позволяет операционной системе (ОС) указывать процессору, когда он может переходить в состояние пониженного энергопотребления. Возможные параметры: Enable (Включен) / Disable (Выключен).

CPU C1 auto demotion – управляет тем, как быстро процессор перейдет в C1-состояние, когда он неактивен. Возможные параметры: Enable (Включен) / Disable (Выключен).

CPU C1 auto undemotion – управляет тем, как быстро процессор выйдет из C1-состояния, когда он неактивен. Возможные параметры: Enable (Включен) / Disable (Выключен).

CPU C6 report – управляет тем, будет ли процессор сообщать операционной системе о своей способности переходить в C6-состояние простоя (также известное как

ACPI C3). Возможные параметры: Enable (Включен) / Disable (Выключен) / Auto (Авто-режим).

Enhanced Halt State (C1E) – настройка, которая позволяет процессору переходить в состояние простоя с пониженным энергопотреблением. Возможные параметры: Enable (Включен) / Disable (Выключен).

OS ACPI Cx – определяет, какое максимальное ACPI C-состояние простоя разрешено использовать операционной системе. Возможные параметры: ACPI C2 / ACPI C3.

Меню «Package C State Control» – позволяет вам установить максимальное C-состояние, в которое может переходить все элементы процессора в целом, находящиеся в состоянии простоя. Имеет единственную настройку – Package C State. Возможные параметры:

- C0/C1 state – максимальная производительность;
- C2 state – баланс между производительностью и энергосбережением;
- C6 (non Retention) state – максимальная экономия энергии ;
- Auto – автоматический режим.

Меню «CPU Thermal Management» – управляет тем, как система реагирует на повышение температуры процессора. Внутри себя имеет две настройки:

- PROCHOT Modes (Processor Hot) – позволяет настроить, кто имеет право влиять на снижение производительности процессора в случае перегрева. Имеет 4 параметра:
  - Both Input and Output - предоставляет наиболее полную защиту от перегрева, позволяя как процессору, так и внешним агентам управлять дросселированием;
  - Output-only – позволяет контролировать только процессору;
  - Input-Only – позволяет контролировать только внешним агентам;
  - Disable – отключает PROCHOT.
- Thermal Monitor – обеспечивает базовую возможность следить за температурой процессора. Возможные параметры: Enabled (Включен) / Disabled (Выключен).

Меню «CPU - Advanced PM Tuning» (см. рисунок 18) – предоставляет доступ к продвинутым параметрам управления питанием процессора.

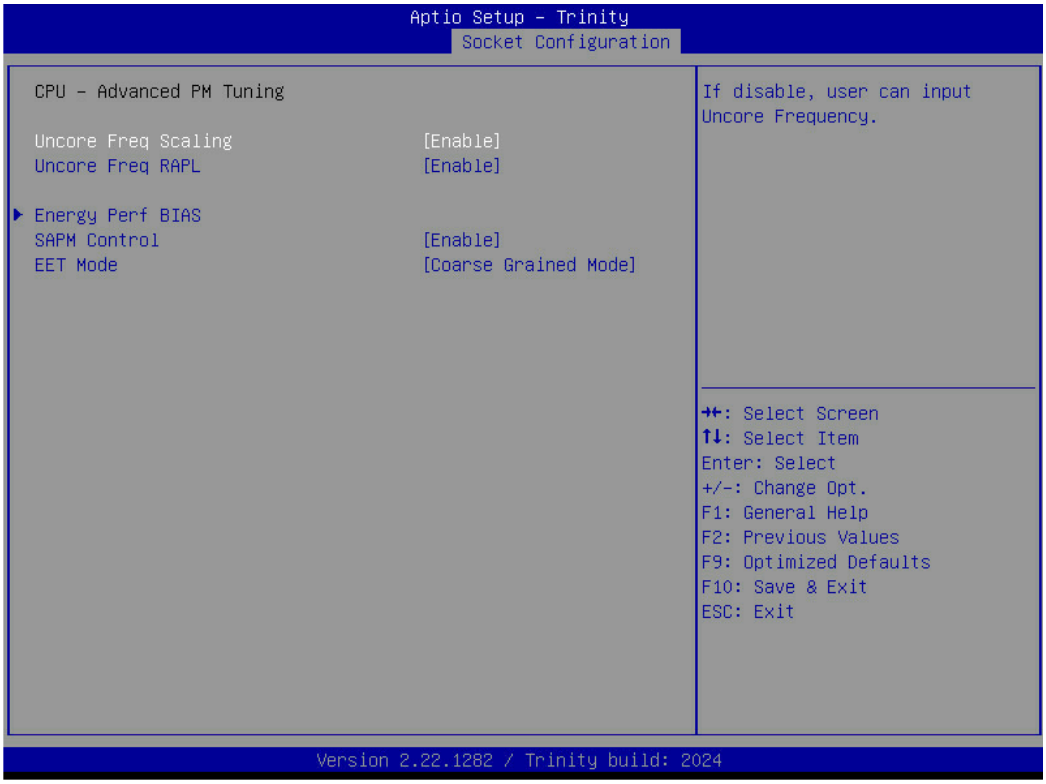

Рисунок 18 – Окно настроек «CPU - Advanced PM Tuning»

Uncore Freq Scaling – настройка управляет тем, как частота Uncore (неядерной части процессора) изменяется в зависимости от нагрузки. Возможные параметры: Enable (Включен) / Disable (Выключен).

Uncore Freq RAPL – настройка позволяет технологии RAPL (Running Average Power Limit) контролировать частоту Uncore. Возможные параметры: Enable (Включен) / Disable (Выключен).

Energy Perf BIAS – настройка, которая сообщает операционной системе, какую стратегию управления питанием использовать. Настройка состоит из:

- Power Performance Tuning – настройка определяет кто будет управлять EPB. Возможные параметры:
  - OS Controls EPB – контролируется операционной системой;
  - BIOS Controls EPB – контролируется BIOS;
  - PECI Controls EPB – контролируется PECI.
- PECI PCS EPB – выбор источника управления балансом производительности и энергосбережения. Возможные параметры:
  - OS Control EPB – контролируется операционной системой;
  - PECI Controls EPB using PCS (Power Control State) – контролируется PECI с помощью PCS.

В случае выбора BIOS Controls EPB в настройке Power Performance Tuning открывается настройка ENERGY_PERF_BIAS_CFG mode.

ENERGY_PERF_BIAS_CFG mode – определяет профиль работы EPBias технологии. Параметры:

- Performance (Производительность);
- Balanced Performance (Сбалансированная производительность);
- Balanced Power (Сбалансированное энергосбережение);

- Power (Энергосбережение).

Dynamic Loadline Switch – управляет тем, как сильно напряжение процессора изменяется в зависимости от нагрузки. Возможные параметры: Enable (Включен) / Disable (Выключен).

Workload Configuration – настройка, позволяющая оптимизировать работу процессора для конкретных типов задач. Имеет параметры:

- Balanced – сбалансированный режим;
- I/O Sensitive – для задач, зависящих от скорости ввода-вывода.

Averaging Time Window – определяет период времени, в течение которого система усредняет данные о температуре, энергопотреблении и других параметрах.

P0 TotalTime Threshold Low и P0 TotalTime Threshold High – Нижний и верхний пороги нахождения процессора в состоянии P0.
Задается в процентах числами hex. Логика такова:

- 50% соответствует примерно 39 / 2 = 1C (hex)
- 25% соответствует примерно 39 / 4 = 9 (hex)
- 75% соответствует примерно (39 * 3) / 4 = 2D (hex)

SAPM Control – управляет битом в регистре MSR процессора, который отвечает за отключение или включение механизмов управления питанием SAPM. Возможные параметры: Enable (Включен) / Disable (Выключен).

EET Mode – определяет, как процессор управляет переходом в турбо-режим или состояние P1 (состояние с пониженной частотой и напряжением). Возможные параметры:

- Coarse Grained Mode – решает, нужно ли вообще переходить в турбо-режим или оставаться в состоянии P1.
- Fine Grained Mode – управляет степенью разгона в турборежиме.

Меню «Memory Power & Thermal Configuration» содержит две настройки:

- Throttling Mode – определяет, как система должна реагировать на перегрев оперативной памяти. Имеет 4 возможных параметра:
  - Disable (Выключено)
  - OLTT – Если температура модулей RAM достигает критического уровня (определяемого датчиком температуры на модуле или на материнской плате вблизи слотов RAM), система начинает снижать ее частоту и/или увеличивать тайминги
  - CLTT – Включает дросселирование на основе Control Logic Thermal Throttling. Опирается на термодатчики на материнской плате рядом с RAM
  - CLTT with PECI – Включает дросселирование на основе Control Logic Thermal Throttling, но с использованием данных, получаемых через интерфейс PECI (Platform Environment Control Interface).
- Select Temperature Refresh Value – позволяет выбрать, как будет определяться частота обновления памяти в зависимости от температуры.

Имеет два режима работы: автоматический и ручной.

Ручное управление предусматривает более тонкую настройку и открывает доступ к трем параметрам:

- Set Halfx Temperature Refresh – температура, при которой частота обновления памяти будет снижена вдвое;
- Set TWOx Temperature Refresh – температура, при которой частота обновления памяти будет увеличена вдвое;
- Set FOURx Temperature Refresh – температура, при которой частота обновления памяти будет увеличена в четыре раза.

7.6. Меню «Server Mgmt» (управление сервером)

Настройки «Server Mgmt» служат для мониторинга и обслуживания серверов через сеть с целью обеспечения максимальной производительности. Помимо этого, меню включает управление оборудованием, программным обеспечением, безопасностью, резервным копированием и обновлением.

Меню «Server Mgmt» показано на рисунке 19.

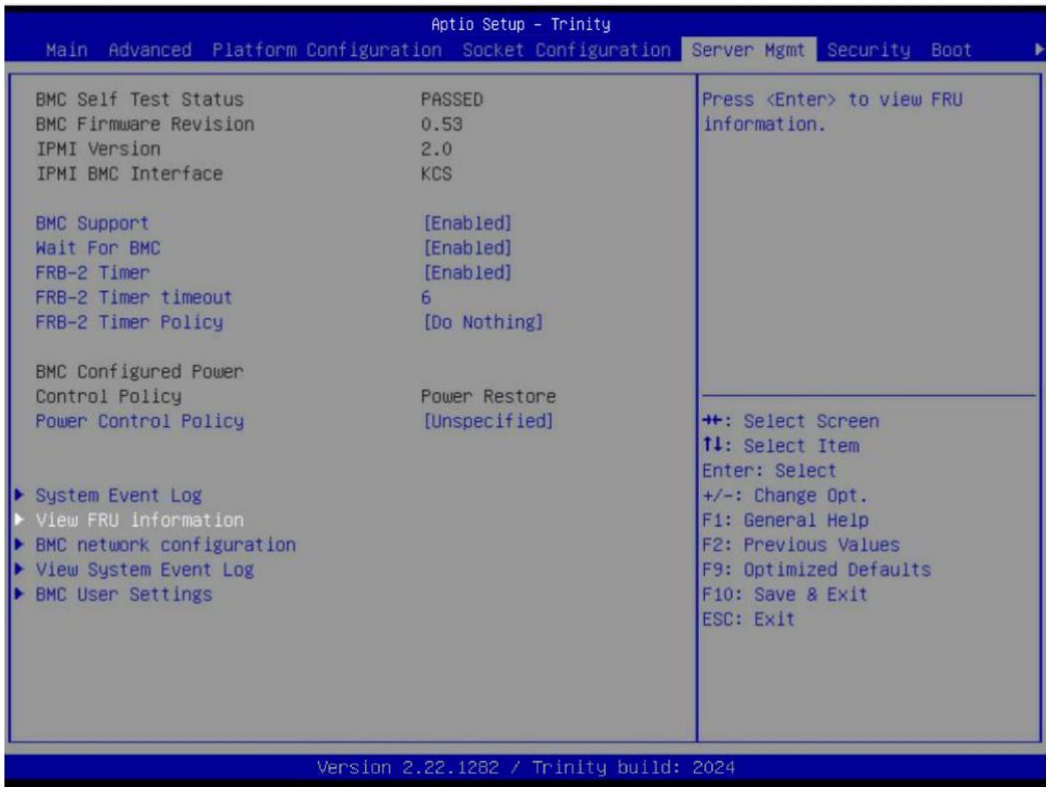

Рисунок 19 – Окно настроек «Server Mgmt»

В верхней части окна отображаются:

- BMC Self-Test Status – тест статуса BMC;
- BMC Firmware Revision – версия BMC;
- IPMI Version – версия IMPI;
- IPMI BMC Interface – интерфейс IPMI BMC.

Далее располагаются настройки BMC, правила, настройки сетевого доступа, журнал событий и настройки пользовательского доступа.

7.7. Меню «Security» (безопасность)

В меню «Security» можно установить пароли администратора и пользователей.

Если установлен пароль администратора, то будет ограничен доступ к программе установки.

Если установлен пароль пользователя, то будет ограничены загрузка и установка программы. В программу установки можно войти только с правами администратора.

Настройки безопасности показаны на рисунке 20.

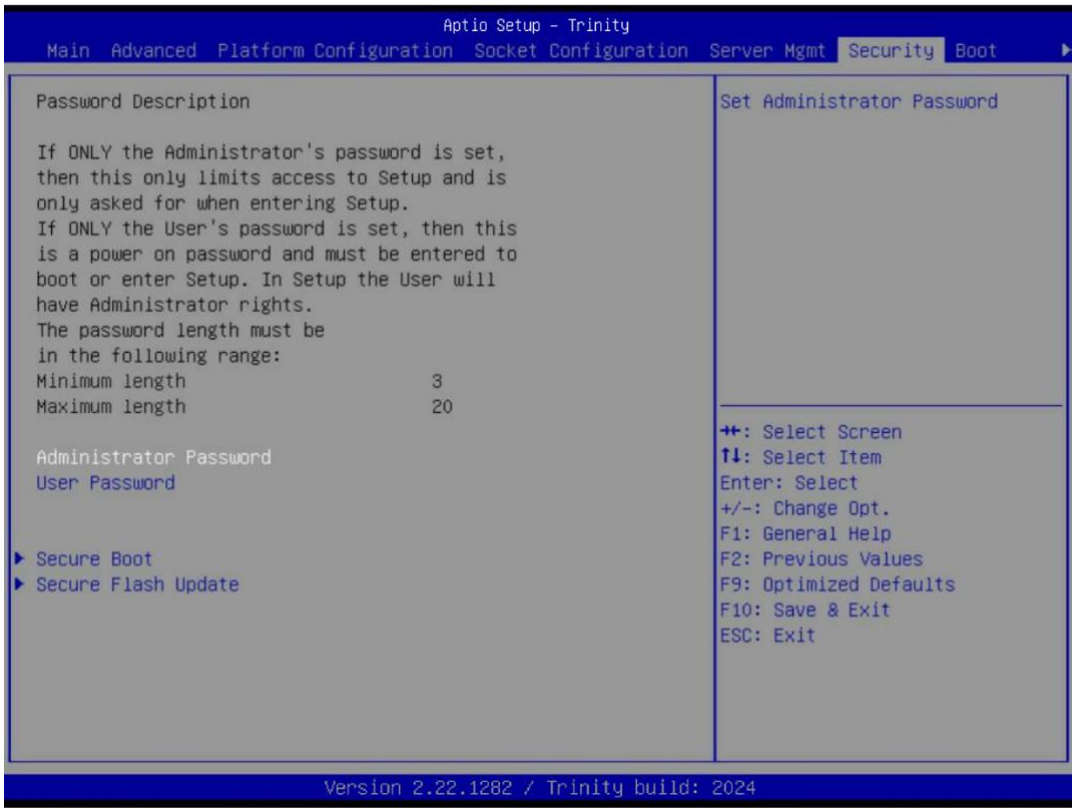

Рисунок 20 – Окно настроек безопасности

7.8. Меню «Boot» (загрузка)

Настройки меню «Boot» определяют режим ВПО и приоритеты при начальной загрузке ОС из списка устройств. В соответствии с установленными приоритетами после включения сервер обращается к устройствам для загрузки ОС с доступных устройств. Также ВПО предоставляет возможность настройки других параметров загрузки, например, приоритет загрузки с локальных или сетевых жёстких дисков, тихая загрузка, и т.д. Окно настроек загрузки показано на рисунке 21.

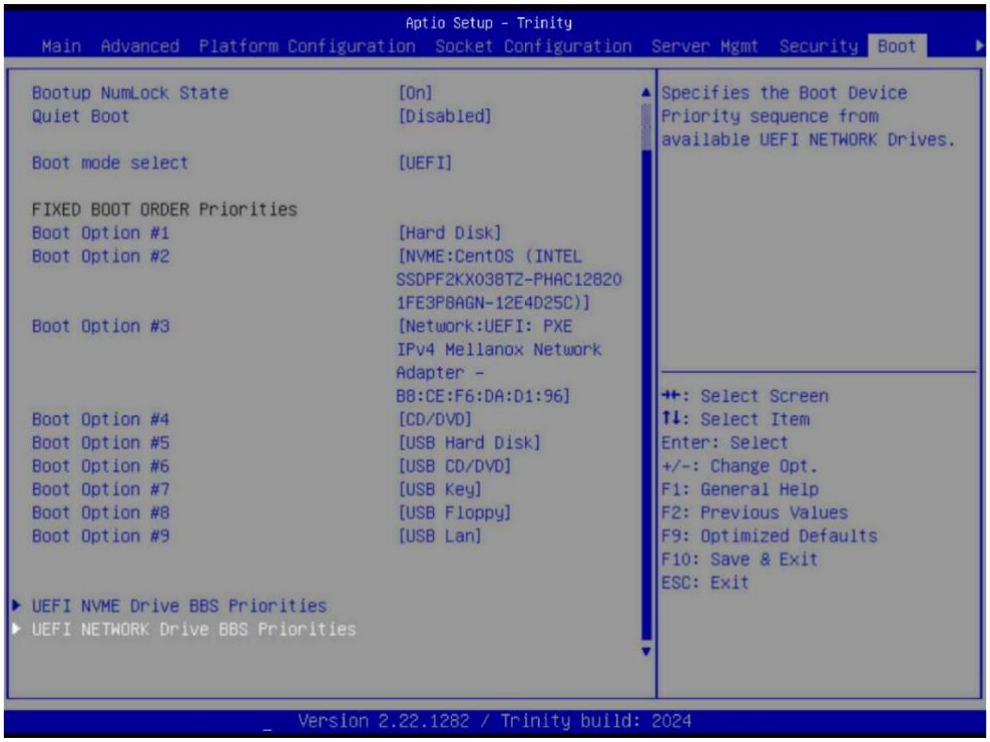

Рисунок 21 – Меню загрузки

7.9. Меню «Save & Exit» (сохранить и выйти)

Раздел отвечает за управление проделанными изменениями: сохранение, отмена, возврат к прежним настройкам или к настройкам по умолчанию, а также за корректный выход из программы.

Окно раздела «Save & Exit» показано на рисунке 22.

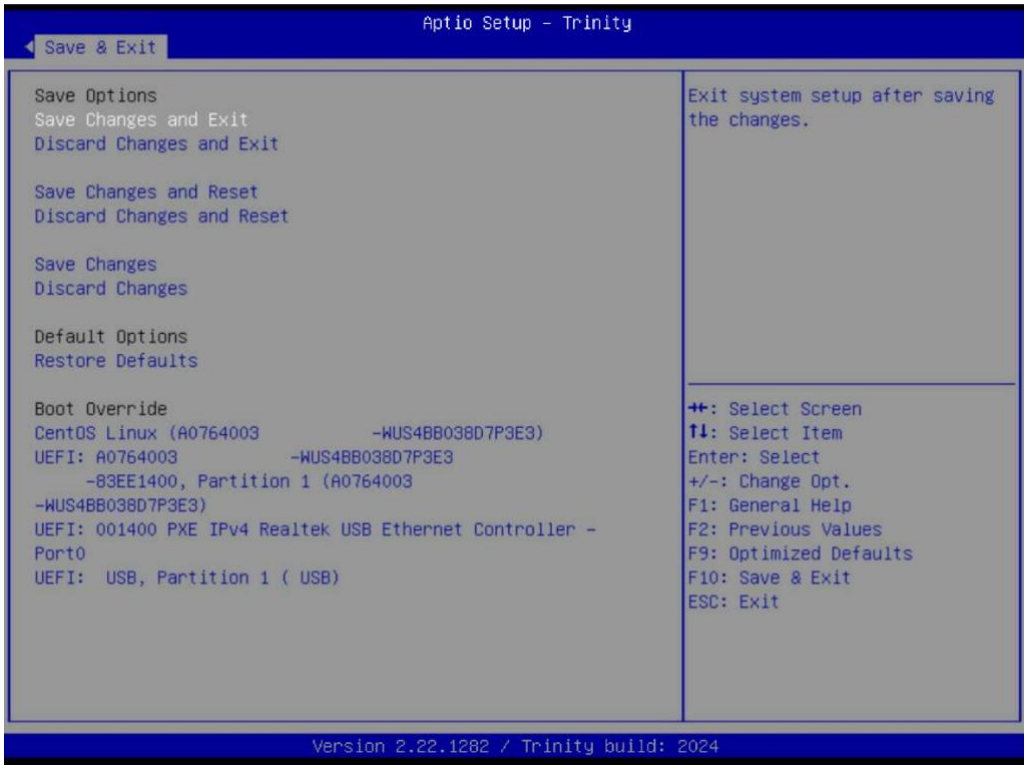

Рисунок 22 – Окно меню «Save & Exit»

8. Функционирование и обновление ВПО

После выполнения подготовительных шагов согласно 6.1. ВПО переходит к стандартным процедурам работы, обеспечивая надежную загрузку и стабильное функционирование системы:

1) Процесс загрузки системы:

- Инициализация оборудования (POST): BIOS выполняет Power-On Self-Test (POST), проверяя процессор, оперативную память, видеокарту и контроллеры;
- Поиск загрузочных устройств: проводится проверка подключенных носителей (NVMe, SATA, USB) для определения источника загрузки;
- Передача управления: после успешного завершения инициализации BIOS передает управление загрузчику операционной системы через режим UEFI или Legacy.

2) Автоматическая коррекция ошибок:

- При обнаружении ошибок BIOS может восстановить настройки по умолчанию, выполнить откат обновления микропрограммы или активировать резервный BIOS (Dual BIOS), если такая функция поддерживается.

3) Взаимодействие с администратором:

- ВПО предоставляет инструменты для диагностики и управления, включая UEFI Setup Utility, UEFI Shell, а также интерфейс IPMI/BMC для удаленного контроля и мониторинга.

4) Мониторинг и управление:

- Осуществляется мониторинг температуры процессора, VRM и других критичных компонентов с помощью датчиков;
- Настраиваются профили работы вентиляторов (PWM-контроль) для оптимизации охлаждения;
- Поддержка стандарта DCMI (Data Center Management Interface) позволяет централизованно управлять состоянием оборудования.

5) Обновление:

- Удаленное обновление через BMC/IPMI: позволяет устанавливать новую версию ВПО без физического доступа к серверу;
- BIOS Recovery Mode: в случае повреждения микропрограммы система автоматически восстанавливает корректную версию BIOS.

Эти процедуры обеспечивают стабильное функционирование ВПО, гарантируя быструю и безопасную загрузку системы, своевременное обновление микропрограммы и оперативное восстановление при возникновении ошибок.

9. Аварийные ситуации

В случае возникновения неисправностей или сбоев при эксплуатации ВПО рекомендуется выполнить следующие шаги для их устранения:

1) Диагностика неисправностей:

- Обратить внимание на сообщения и коды ошибок, отображаемые во время POST или в интерфейсе программы;
- Проверить корректность подключения всех аппаратных компонентов и правильность настроек в программе.

2) Автоматическая коррекция:

- Если программа обнаруживает ошибку, она может автоматически восстановить настройки по умолчанию, выполнить откат обновления или активировать резервный BIOS (Dual BIOS), если эта функция поддерживается.

3) Подготовка информации для техподдержки:

- Зафиксировать коды ошибок и сообщения, возникающие во время загрузки;
- Снять логи и скриншоты или записать подробное описание проблемы.
- Собрать сведения о конфигурации системы, включая версию ВПО, список установленных аппаратных компонентов и подробности об условиях возникновения ошибки.

4) Обращение в техническую поддержку:

- Использовать официальные каналы связи производителя (например, сайт, телефон или электронную почту) для обращения в техническую поддержку;
- Предоставить всю собранную информацию и подробно описать последовательность действий, приведшую к возникновению проблемы;
- Следовать инструкциям специалистов и, при необходимости, выполнить дополнительные рекомендации для устранения неисправности.

Эффективное решение проблем начинается с тщательной диагностики, а своевременное обращение в техническую поддержку позволяет оперативно устранить неисправности и обеспечить стабильную работу системы.

Диапазоны кодов неисправностей приведены в таблице 2.

Таблица 2 – Диапазоны кодов

Диапазон кодов	Описание
0x01 ~ 0x0B	SEC выполнение
0x0C ~ 0x0F	SEC ошибка
0x10 ~ 0x2F	PEI выполнение до обнаружения памяти включительно
0x30 ~ 0x4F	PEI выполнение после обнаружения памяти
0x50 ~ 0x5F	PEI ошибки
0x60 ~ 0x8F	DXE выполнение до BIOS
0x90 ~ 0xCF	BDS выполнение

Диапазон кодов	Описание
0xD0 ~ 0xDF	DXE ошибки
0xE0 ~ 0xE8	S3 Resume (PEI)
0xE9 ~ 0xEF	Ошибки S3 Resume (PEI)
0xF0 ~ 0xF8	Восстановление (PEI)
0xF9 ~ 0xFF	Ошибки восстановления (PEI)

Коды ВПО в фазе SEC приведены в таблице 3.

Таблица 3 – Коды программы в фазе SEC

Код	Описание
Коды хода выполнения	
0x01	Питание включено. Обнаружен сброс (soft/hard)
0x02	Инициализация AP перед загрузкой микрокода
0x03	Инициализация северного моста перед загрузкой микрокода
0x04	Инициализация южного моста перед загрузкой микрокода
0x05	Инициализация OEM перед загрузкой микрокода
0x06	Загрузка микрокода
0x07	Инициализация AP после загрузки микрокода
0x08	Инициализация северного моста после загрузки микрокода
0x09	Инициализация южного моста после загрузки микрокода
0x0A	Инициализация OEM после загрузки микрокода
0x0B	Инициализация кэша
Коды ошибок	
0x0E	Микрокод не обнаружен
0x0F	Микрокод не загружен
0xCA	Не найден процессор
0xCB	Ошибка инициализации ядра
0xCC	Не удалось включить доступ к CSR
0xCD	Ошибка загрузки микрокода
0xD0	Тест данных стека NEM не пройден
0xD1	Тест конфигурации не пройден

Коды ВПО в фазе PEI приведены в таблице 4.

Таблица 4 – Коды программы в фазе PEI

Код	Описание
Коды хода выполнения	
0x10	Ядро PEI запущено
0x11	Инициализация процессора перед использованием памяти начата
0x12 ~ 0x14	Инициализация процессора перед использованием памяти (характерная для модуля CPU)
0x15	Инициализация северного и юного мостов перед использованием памяти начата
0x16 ~ 0x18	Инициализация северного и юного мостов перед использованием памяти (характерная для модулей NB/SB)
0x19	PEICAR_SB_INIT
0x1A ~ 0x1C	Зарезервировано для южного моста
0x1D ~ 0x2A	Зарезервировано для использования OEM
0x2B	PEI_MEMORY_SPD_READ
0x2C	PEI_MEMORY_PRESENCE_DETECT
0x2D	PEI_MEMORY_TIMING
0x2E	PEI_MEMORY_CONFIGURATION
0x2F	PEI_MEMORY_INIT
0x30	Зарезервировано для ASL
0x31	Память установлена
0x32	Инициализация процессора после начала использования памяти начата
0x33	Инициализация процессора после начала использования памяти. Инициализация кэша
0x34	Инициализация процессора после начала использования памяти. Инициализация прикладных процессоров Application Processor(s) (AP)
0x35	Инициализация процессора после начала использования памяти. Выбор процессора загрузки Boot Strap Processor (BSP)
0x36	Инициализация процессора после начала использования памяти. Инициализация режима управления системой System Management Mode (SMM)
0x37 ~ 0x3E	Инициализация NB/SB после начала использования памяти
0x3F ~ 0x4E	Коды инициализации после ввода OEM-памяти
0x4F	Процедура DXE IPL начата
PEI Error Codes	
0x50	Ошибка инициализации памяти. Недопустимый тип памяти или несовместимая скорость памяти

Код	Описание
0x51	Ошибка инициализации памяти. Сбой чтения SPD
0x52	Ошибка инициализации памяти. Неверный размер памяти или модули памяти не совпадают
0x53	Ошибка инициализации памяти. Используемая память не обнаружена
0x54	Неизвестная ошибка инициализации памяти
0x55	Память не установлена
0x56	Недопустимый тип процессора или его скорость
0x57	Несоответствие процессора
0x58	Не удалось выполнить самопроверку процессора CPU или возможная ошибка кэша процессора
0x59	Микрокоды процессора CPU не найдены или обновление микрокодов не выполнено
0x5A	Внутренняя ошибка процессора CPU
0x5B	Перезапуск PPI невозможен
0x5C ~ 0x5F	Зарезервировано для будущих кодов ошибок Тринити

Коды ВПО для памяти приведены в таблице 5.

Таблица 5 – Коды программы, касающиеся памяти

Код	Описание
0xB0	STS_DIMM_DETECT: Обнаружение количества модулей DIMM
0xB1	STS_CLOCK_INIT: Настройка частоты DDR
0xB2	STS_SPD_DATA: Собрать оставшиеся данные SPD
0xB3	STS_GLOBAL_EARLY: Программные регистры на уровне контроллера памяти
0xB4	STS_RANK_DETECT: Оцените режимы RAS и сохраните информацию о ранге
0xB5	STS_CHANNEL_EARLY: Программные регистры на уровне канала
0xB6	STS_DDRIO_INIT: Порядок инициализации DDRIO
0xB7	STS_DDR_CHANNEL_TRAINING: Настройка DDR
0xB8	STS_INIT_THROTTLING: Инициализация CLTT/OLTT
0xB9	STS_MEMBIST: Тест аппаратной памяти и инициализация
0xBA	STS_MEMINIT: Выполнение инициализации памяти
0xBB	STS_DDR_MEMMAP: Схема программной памяти и очередность
0xBC	STS_RAS_CONFIG: Настройка программы RAS
0xBD	STS_GET_MARGINS:

Код	Описание
0xBF	STS_MRC_DONE: MRC выполнено

Коды инициализации ВПО в фазе DXE приведены в таблице 6.

Таблица 6 – Коды программы в фазе DXE

Код	Описание
Коды выполнения	
0x60	DXE ядро запущено
0x61	Инициализация NVRAM
0x62	Установка служб выполнения южного моста
0x63 ~ 0x67	Инициализация CPU DXE (Характерно для модуля CPU)
0x68	Инициализация хост-моста PCI
0x69	Инициализация северного моста DXE начата
0x6A	Инициализация северного моста DXE SMM начата
0x6B ~ 0x6F	Инициализация северного моста DXE (Характерно для модуля North Bridge)
0x70	Инициализация южного моста DXE начата
0x71	Инициализация южного моста DXE SMM начата
0x72	Инициализация устройств южного моста
0x73 ~ 0x77	Инициализация южного моста DXE (Характерно для модуля South Bridge)
0x78	Инициализация модуля ACPI
0x79	Инициализация CSM
0x7A ~ 0x7F	Зарезервировано для будущих кодов DXE Тринити
0x80 ~ 0x8F	Инициализация кодов OEM DXE
0x90	Начинается фаза выбора загрузочного устройства (BDS)
0x91	Подключение драйвера начато
0x92	Инициализация PCI Bus начато
0x93	Инициализация контроллера PCI Bus Hot Plug
0x94	Перечисление шины PCI
0x95	Запрос ресурсов шины PCI
0x96	Назначение ресурсов шины PCI
0x97	Подключение консольных выходных устройств
0x98	Консольные устройства ввода подключаются

Код	Описание
0x99	Инициализация Super IO
0x9A	Инициализация USB начато
0x9B	Перезапуск USB
0x9C	Обнаружение USB
0x9D	USB доступно
0x9E ~ 0x9F	Зарезервировано для будущих кодов Тринити
0xA0 ~ 0xA3	Инициализация IDE
0xA4 ~ 0xA7	Инициализация SCSI
0xA8	Настройка проверки пароля
0xA9	Начало установки
0xAA	Зарезервировано для ASL
0xAB	Ожидание ввода настроек
0xAC	Зарезервировано для ASL
0xAD	Событие готовности к загрузке
0xAE	Событие загрузки Legacy
0xAF	Событие выхода из служб загрузки
0xB0	Начата установка виртуального адреса MAP
0xB1	Закончена установка виртуального адреса MAP
0xB2	Инициализация Legacy опций ROM
0xB3	Перезапуск системы
0xB4	Горячее подключение USB
0xB5	Горячее подключение шины PCI
0xB6	Очистка NVRAM
0xB7	Сброс конфигурации (сброс настроек NVRAM)
0xB8 ~ 0xBF	Зарезервировано для будущих кодов Тринити
0xC0 ~ 0xCF	Инициализация кодов OEM BDS
Коды ошибок	
0xD0	Ошибка инициализации процессора
0xD1	Ошибка инициализации северного моста
0xD2	Ошибка инициализации южного моста

Код	Описание
0xD3	Некоторые из архитектурных протоколов недоступны
0xD4	Ошибка выделения ресурсов PCI. Недостаточно ресурсов
0xD5	Нет места для Legacy опций ROM
0xD6	Консольные устройства вывода не найдены
0xD7	Консольные устройства ввода не найдены
0xD8	Неверный пароль
0xD9	Ошибка параметров загрузки (Возврат ошибки LoadImage)
0xDA	Ошибка загрузки (Возврат ошибки StartImage)
0xDB	Обновление Flash не удалось
0xDC	Протокол сброса недоступен
0xDE ~ 0xDF	Зарезервировано для кодов Тринити

Коды восстановления (Recovery) приведены в таблице 7.

Таблица 7 – Коды Recovery

Код	Описание
0xF0	Состояние восстановления, вызванное прошивкой (Автовосстановление)
0xF1	Состояние восстановления, вызванное пользователем (принудительное восстановление)
0xF2	Процесс восстановления начат
0xF3	Найден образ прошивки для восстановления
0xF4	Образ прошивки для восстановления загружен
Ошибки	
0xF8	Восстановление PPI не доступно
0xF9	Образ восстановления не обнаружен
0xFA	Образ восстановления поврежден
0xFB ~ 0xFF	Зарезервировано для будущих кодов ошибок Тринити

10. Модернизация ВПО

АО «ТРИНИТИ СОЛЮШНС» обеспечивает оценку и ревизию процессов разработки и поддержки ВПО, документирование изменений.

Оценка и ревизия процессов выполняется АО «ТРИНИТИ СОЛЮШНС» при обеспечении контроля качества ВПО, на основании обращений, направленных в службу технической поддержки, а также с учетом:

- определения потребностей в применении передовых технологий;
- обновления российской и международной методологии по усовершенствованию процесса управления разработкой программного обеспечения.

Модернизация ВПО осуществляется путем загрузки обновленной версии образа диска на схему (перепрошивки) через интерфейс или через TFTP сервер.

Введение функциональных возможностей ВПО в дополнение к уже реализованным возможностям не предусмотрено.