Универсальное базовое программное обеспечение для вычислительных устройств, основанных на процессорах с архитектурой X86 «Fplus BIOS»

Руководство пользователя

На данный документ распространяется действие
Соглашения о Соблюдении Конфиденциальности

Содержание

1. Введение

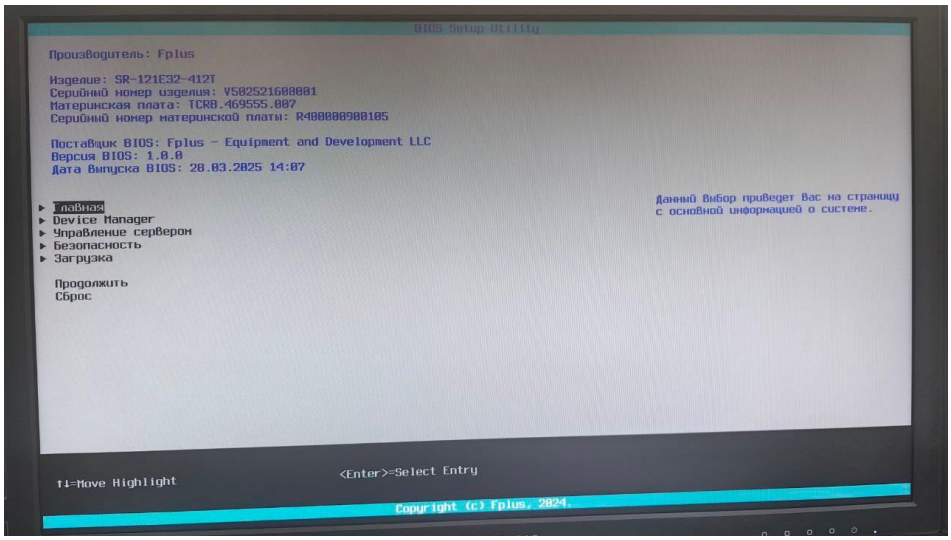
Настоящее описание предназначено для ознакомления с функционалом универсального базового программного обеспечение для вычислительных устройств, основанных на процессорах с архитектурой X86 «Fplus BIOS» (далее ПО) и процессом настройки работы аппаратной платформы изделия.

2. Основные функции

2.1. Процесс загрузки

Для загрузки в пользовательский интерфейс ПО необходимо по время процедуры POST (от англ. Power-On Self-Test – проверка аппаратного обеспечения компьютера, выполняемая при его включении) при появлении сообщения «Press F2 or Esc to enter BIOS» нажать клавишу F2 или Esc. После этого пользователь попадает на приветственную форму (рис. 2.1.1).

Рис. 2.1.1 – Приветственная форма



2.2. Приветственная форма

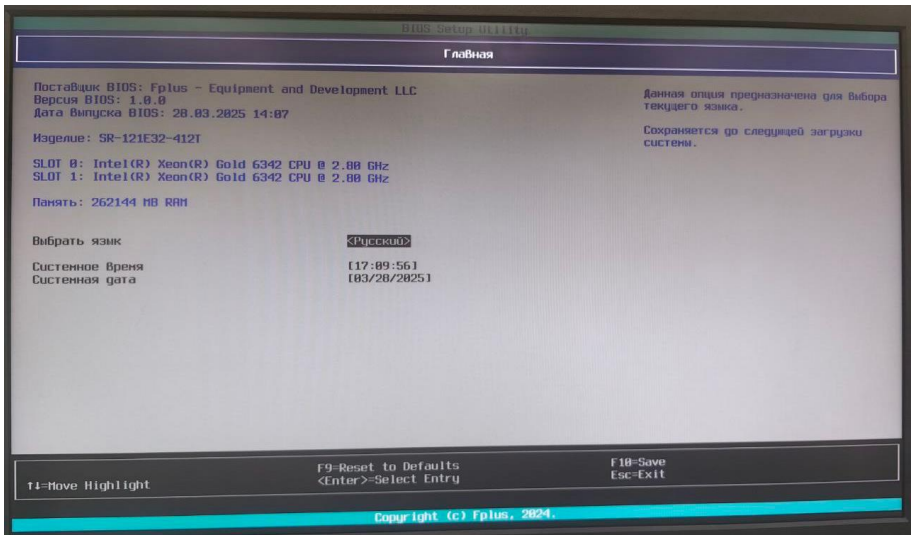
На приветственной форме расположена основная правовая информация об изделии, а именно: модель, серийный номер, модель и серийный номер материнской платы. Информация о поставщике, версии и дате сборки ПО.

Тут же расположено меню ПО, позволяющего просмотреть или настроить режимы работы.

2.3. Пункт меню «Главная»

Пункт меню «Главная» (рис. 2.3.1) предоставляет информацию об установленных процессорах и оперативной памяти.

Рис. 2.3.1 – Пункт меню «Главная»

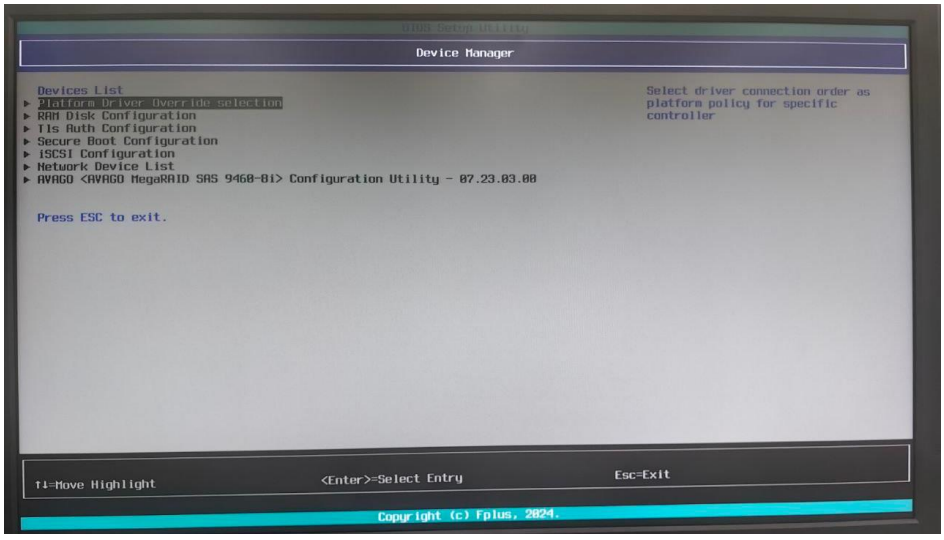


Так же, в данном пункте меню возможно выбрать локализацию и установить дату и время.

2.4. Пункт меню «Device Manager»

Пункт меню «Device Manager» (рис. 2.4.1) – диспетчер устройств, представляет собой комбинацию подменю и список устройств с поддержкой технологии «OpROM» (это часть встроенного ПО, которое находится в ПЗУ на карте расширения и выполняется для инициализации устройства и добавления поддержки устройства в BIOS. При обычном использовании это, по сути, драйвер, который взаимодействует между API BIOS и оборудованием). Он предназначен для настройки работы периферийных устройств изделия.

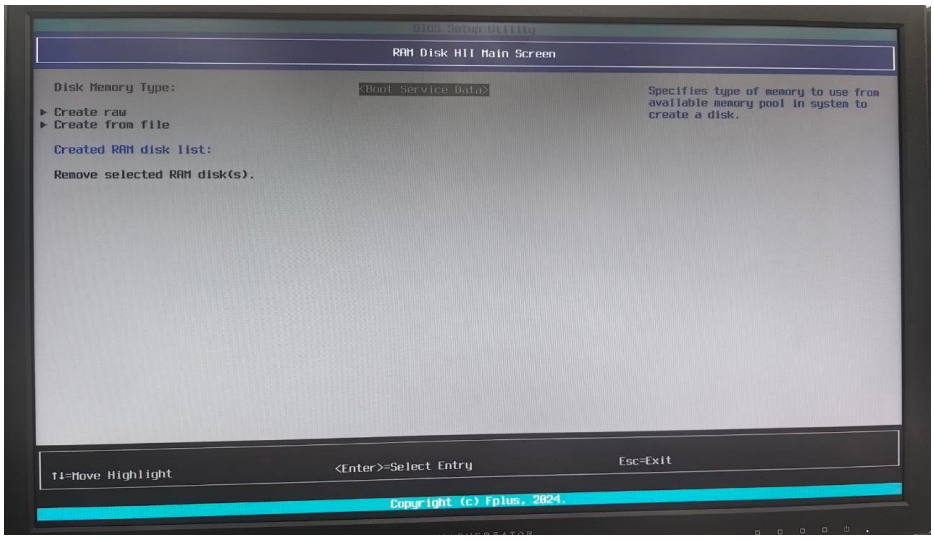
Рис. 2.4.1 – Пункт меню «Device Manager»



2.4.1. Пункт подменю «RAM Disk Configuration»

Пункт подменю «RAM Disk Configuration» (рис. 2.4.1.2) предназначен для создания и управления виртуальным диском в оперативной памяти.

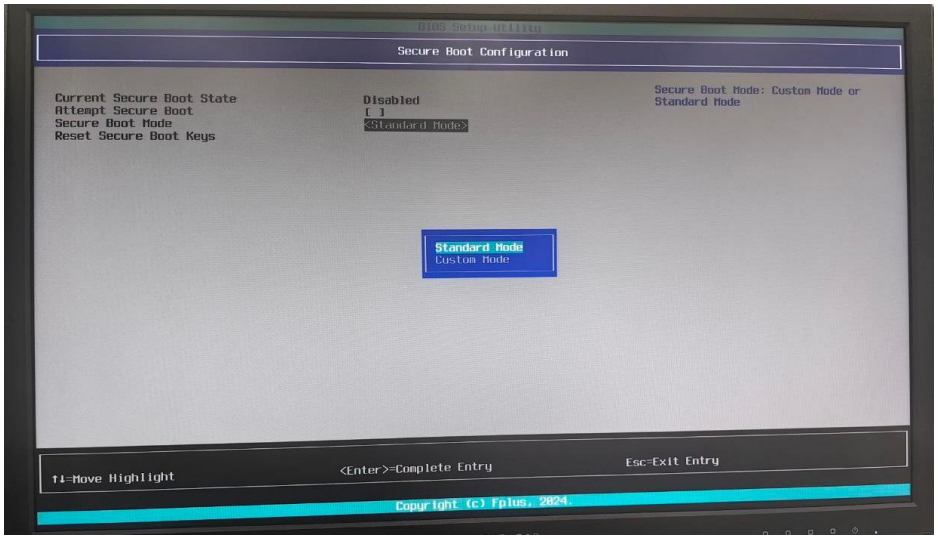
Рис. 2.4.1.2 - Пункт подменю «RAM Disk Configuration»



2.4.2.Пункт подменю «Secure Boot Configuration»

Пункт подменю «Secure Boot Configuration» (рис. 2.4.2.1) предназначен для защиты системы и разрешает в процессе загрузки только аутентифицированные двоичные файлы, предотвращая загрузку несанкционированных операционных систем и вредоносного программного обеспечения во время процесса загрузки устройства.

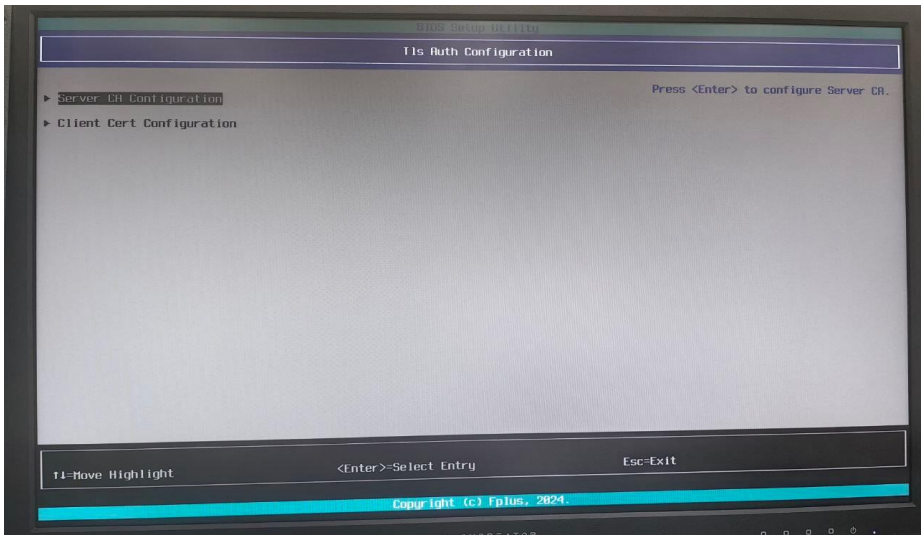
Рис. 2.4.2.1 - Пункт подменю «Secure Boot Configuration»



2.4.3.Пункт подменю «Tls Auth Configuration»

Пункт подменю «Tls Auth Configuration» (рис. 2.4.3.1) предназначен для настройки аутентификации на основе протокола Transport Layer Security (TLS).

Рис. 2.4.3.1 - Пункт подменю «Tls Auth Configuration»



Этот раздел связан с обеспечением безопасности при сетевых операциях на уровне прошивки, таких как загрузка по сети (PXE), обновление прошивки через интернет или взаимодействие с удалёнными серверами. Это необходимо для:

- Безопасная загрузка по сети (HTTPS Boot) - позволяя загружать операционную систему или образы по защищённому HTTPS-соединению вместо незашифрованного протокола (HTTP или TFTP). Необходимо добавить корневые сертификаты доверенных центров сертификации (CA), чтобы UEFI доверял только подписанным ими серверам.

- Аутентификация для обновлений прошивки - проверяя подлинность сервера при загрузке обновлений микропрограммы, через Capsule Update. UEFI проверяет цифровую подпись сервера с использованием TLS, чтобы избежать установки вредоносных обновлений.

- Клиент-серверная аутентификация – позволяет в корпоративных средах устройству аутентифицироваться на сетевых ресурсах с помощью TLS-сертификата. Необходимо загрузить клиентские сертификаты и приватные ключи, чтобы система могла подтвердить свою подлинность.

2.4.4.Пункт подменю «iSCSI Configuration»

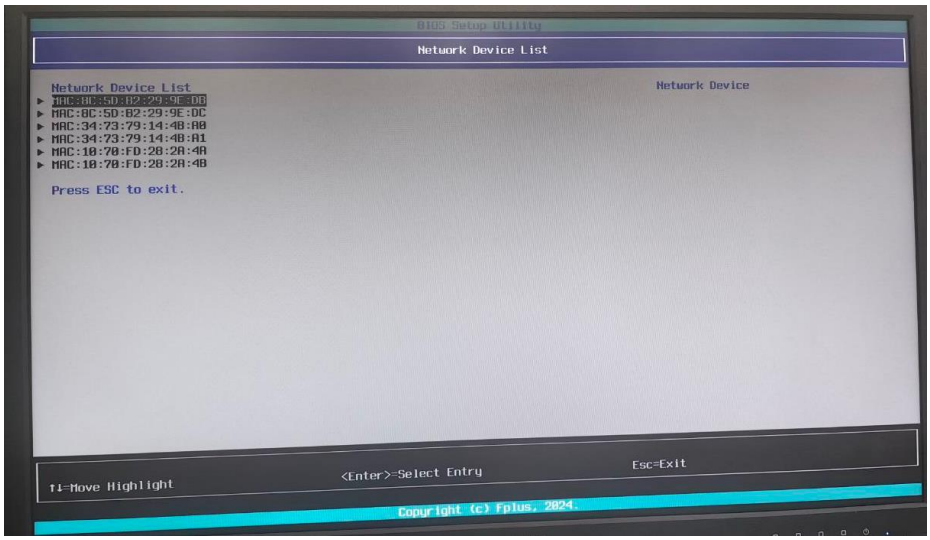
Пункт подменю «iSCSI Configuration» (рис. 2.4.4.1) – предназначен для настройки загрузки компьютера через протокол iSCSI (Internet Small Computer System Interface). Этот протокол позволяет использовать удалённые сетевые хранилища (SAN — Storage Area Network) как локальные диски, что особенно полезно в корпоративных средах, облачных инфраструктурах или для загрузки операционной системы с сетевого ресурса.

Рис. 2.4.4.1 - Пункт подменю «iSCSI Configuration»

2.4.5.Пункт подменю «Network Device List»

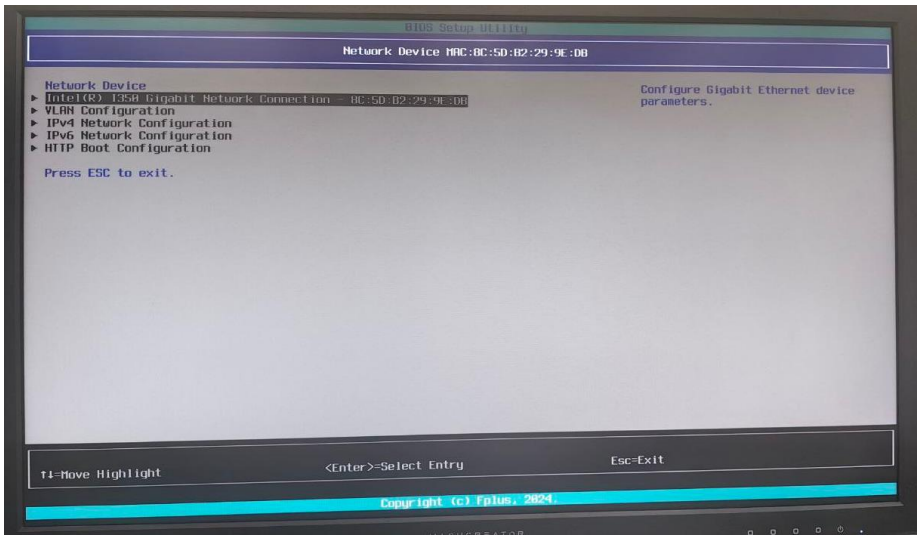
Пункт подменю «Network Device List» (рис. 2.4.5.1) – предназначен для настройки всех обнаруженных совместимых сетевых адаптеров изделия.

Рис. 2.4.5.1 - Пункт подменю «Network Device List»



Выбрав из списка интересующий MAC адрес можно перейти к настройкам сетевого адаптера (рис.2.4.5.2).

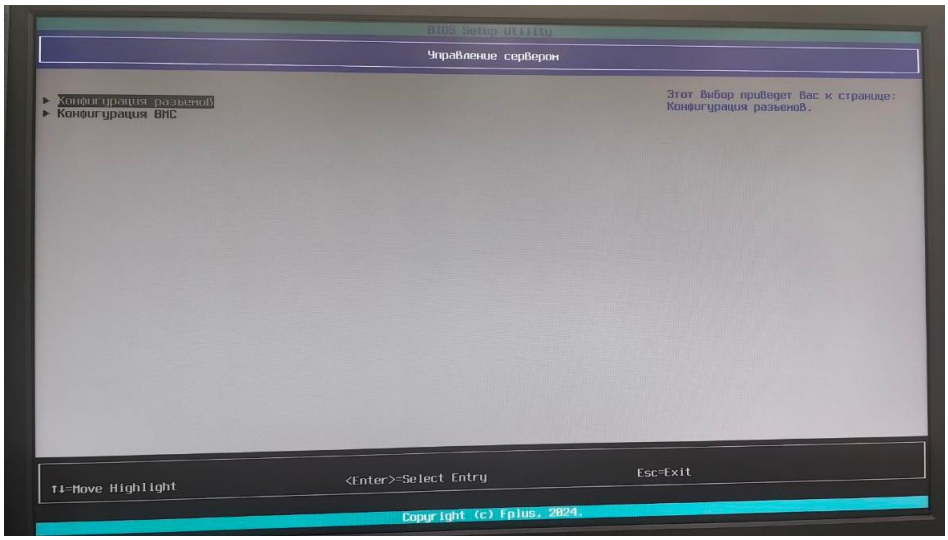
Рис. 2.4.5.2 – Настройка параметров сетевого адаптера



2.5. Пункт меню «Управление сервером»

Пункт меню «Управление сервером» (рис. 2.5.1) представляет собой набор подменю для настройки технологий связанных с работой процессоров и модуля управления BMC.

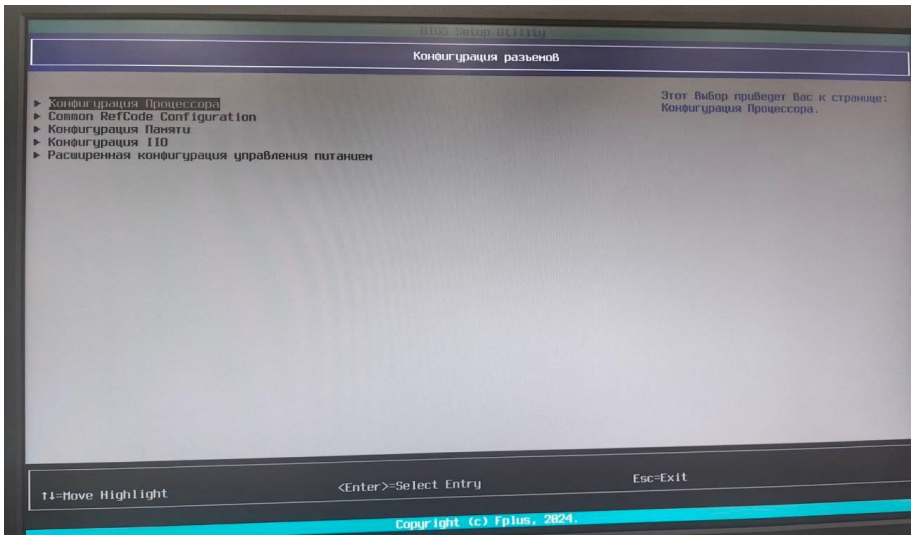
Рис. 2.5.1 - Пункт меню «Управление сервером»



2.5.1. Пункт подменю «Управление разъемами»

Пункт подменю «Управление разъемами» (рис. 2.5.1.1) – предназначен для настройки технологий, связанных с работой центрального процессора с учетом сокета установки.

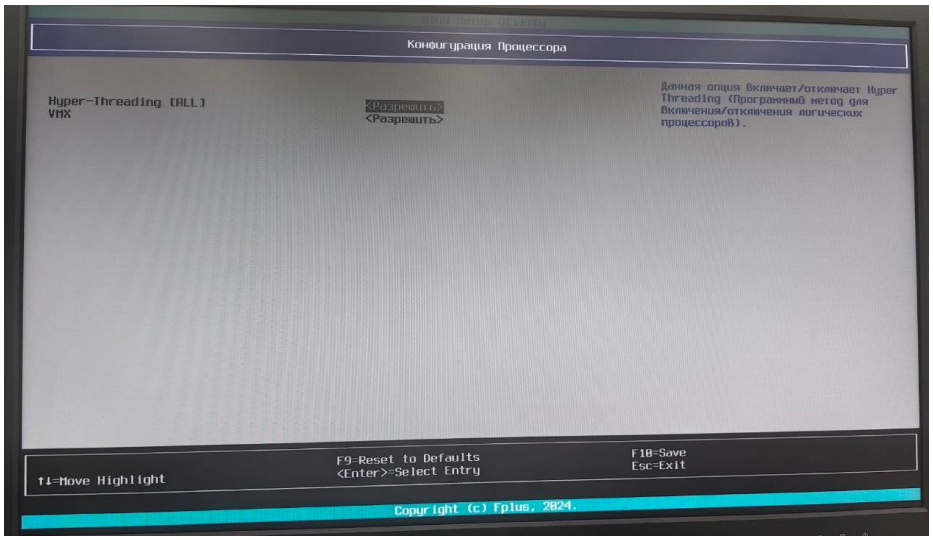
Рис. 2.5.1.1 - Пункт подменю «Управление разъемами»



2.5.1.1. Конфигурация процессора

В подменю «Конфигурация процессора» (рис. 2.5.1.1.1) пользователь может включить или выключить поддержку технологий виртуализации и гиперпоточности.

Рис. 2.5.1.1.1 - Конфигурация процессора



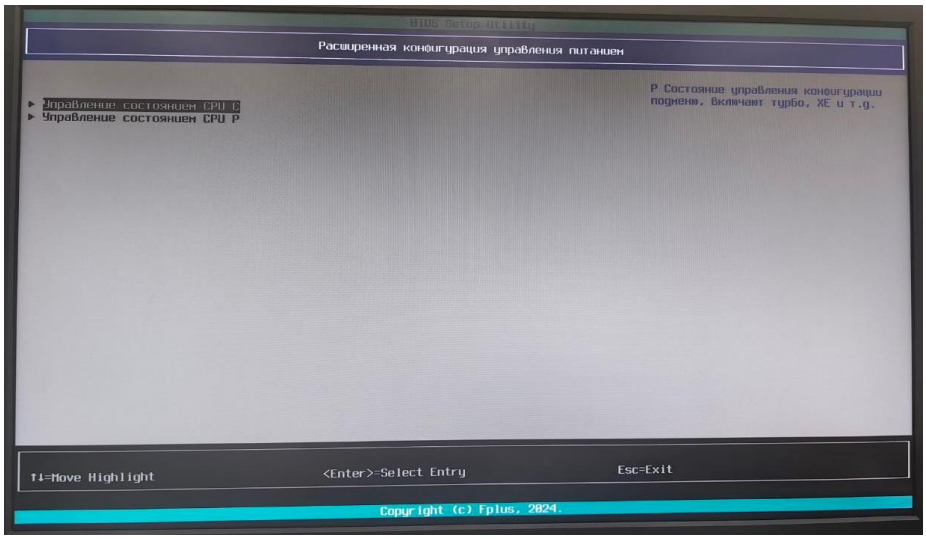
2.5.1.2. Расширенная конфигурация управления питанием

В подменю «Расширенная конфигурация управления питанием» (рис. 2.5.1.2.1) пользователь может включить или выключить поддержку технологий, зависящих/влияющих на энергопотребление процессоров, а именно:

- Turbo Mode – позволяет динамически изменять частоты ядер процессора

- Поддержка команд Monitor MWAIT – необходима для корректной работы виртуализации

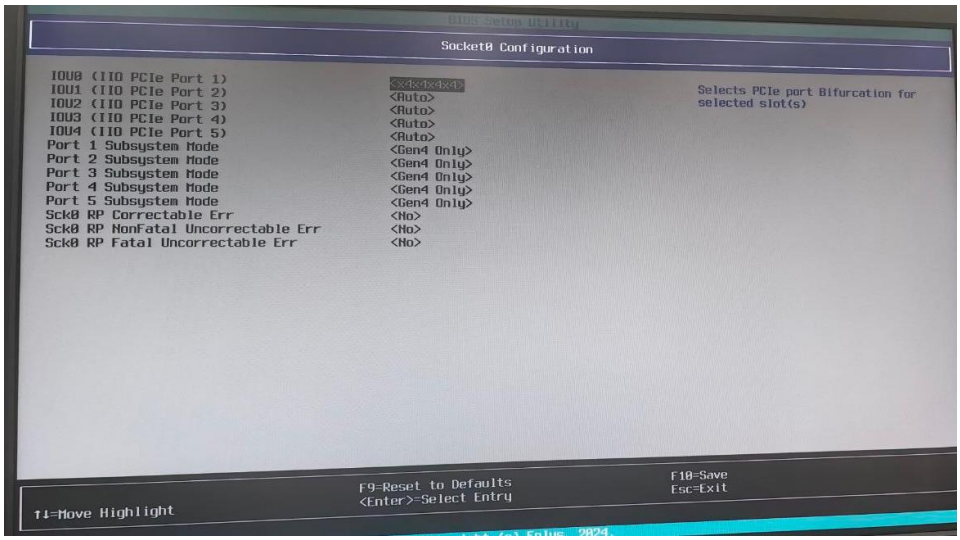
Рис. 2.5.1.2.1 - Расширенная конфигурация управления питанием



2.5.1.3. IIO Конфигурация

В подменю «IIO Конфигурация» (рис. 2.5.1.3.1) пользователь может настроить режимы работы PCIe в разрезе каждого из сокетов.

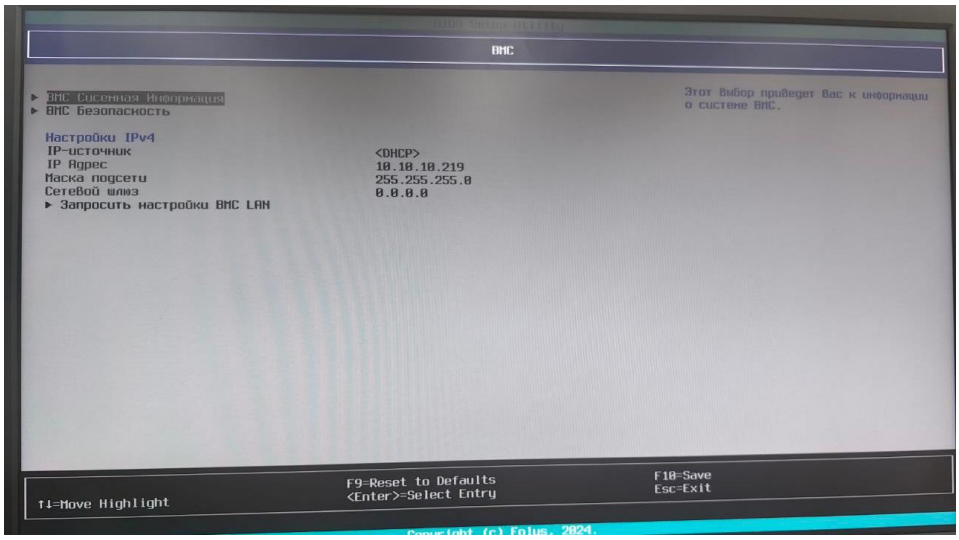
Рис. 2.5.1.3.1 - IIO Конфигурация



2.5.2.Пункт подменю «Конфигурация BMC»

Пункт подменю «Конфигурация BMC» (рис. 2.5.2.1) позволяет настраивать параметры для BMC.

Рис. 2.5.2.1 - Пункт подменю «Конфигурация BMC»



В данном подпункте можно получить и настроить параметры сетевого интерфейса.

«BMC Безопасность» - позволяет устанавливать новый пароль для встроенных административных учетных записей BMC.

«BMC Системная информация» - позволяет посмотреть версию BMC.

2.6. Пункт меню «Безопасность»

Пункт меню «Безопасность» (рис. 2.6.1) позволяет установить/сбросить пароль администратора изделия. Данный пароль необходим для доступа в ПО или UEFI Shell при загрузке изделия.

Рис. 2.6.1 - Пункт меню «Безопасность»

2.7. Пункт меню «Загрузка»

Пункт меню «Загрузка» предназначен для настройки источников и порядка загрузки операционной системы на изделии (рис. 2.7.1), а также выбора однократного источника загрузки (рис. 2.7.2)

Рис. 2.7.1 – настройка источников и порядка загрузки операционной системы

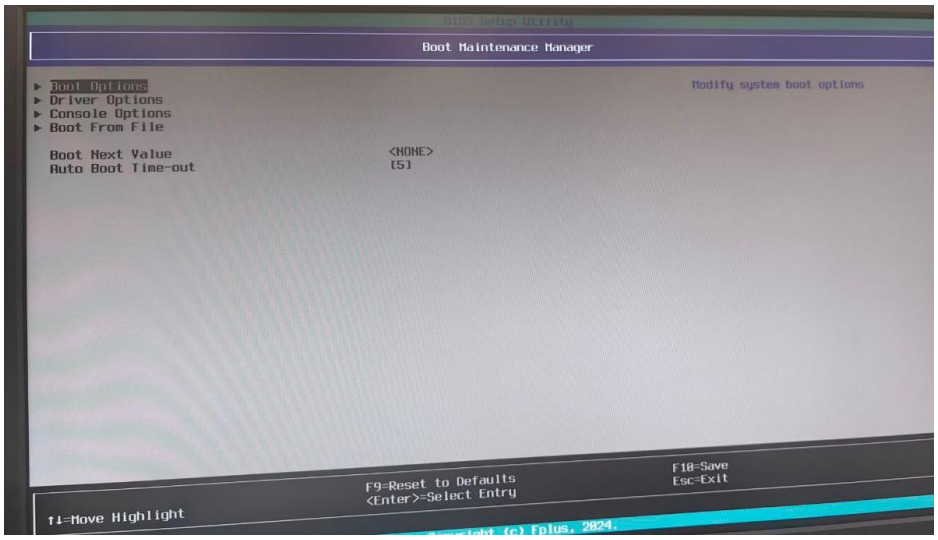


Рис. 2.7.2 – выбор однократного источника загрузки операционной системы