Описание функциональных характеристик программного обеспечения и информацию, необходимую для установки и эксплуатации программного обеспечения «Микропрограммное обеспечение OYBoot»

на 26 листах

Москва, 2024г

Содержание

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Общие сведения

Рассматриваемый программный продукт предназначен для базовой инициализации системы ввода-вывода (BIOS) серверных вычислительных устройств, построенных на базе процессоров Intel семейства Xeon Scalable (начиная с 3-го поколения). Программный продукт полностью совместим со спецификацией UEFI, что позволяет применять его в таких изделиях, как серверы и СХД.

1.2 Информация, необходимая для установки и настройки

Программный продукт устанавливается во флеш-накопитель аппаратной платформы в виде бинарного файла

1.3 Описание структуры

Программа полностью соответствует спецификации UEFI и реализует в себе следующие фазы загрузки системы:

- Secure boot;
- PEI (Pre EFI инициализация);
- DXE (фаза загрузки базовых драйверов устройств);
- BDS (готовность к старту операционной системы)

Помимо этого, программа содержит пользовательскую оболочку для изменения конфигурации запуска без пересборки комплекта программного обеспечения, встроенную оболочку Efi Shell для осуществления низкоуровневой диагностики системы, а также выполнения процедур обновления рассматриваемого программного обеспечения, а также встроенный модуль повышенной защищенности, осуществляющий контроль изменения аппаратного обеспечения изделия и изменения настроек UEFI. С целью повышения безопасности исполнения кода UEFI на платформе, где установлено настоящее программное обеспечение, в состав рассматриваемого ПО включены модули для контроля изменения конфигурации сервера, а также блокировки изменения UEFI-переменных.

2 НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ

2.1 Языки программирования, применявшиеся при разработке ПО:

- Си;
- Assembler

Среда разработки ПО:

- Visual Studio 2017;

2.2 Условия применения

2.2.1 Требования к аппаратному обеспечению

Для корректной работы экземпляра программного обеспечения требуется следующая конфигурация оборудования:

- Процессор Intel Xeon Scalable
- Не менее 8GB ОЗУ
- Монитор с поддержкой VGA/HDMI
- Клавиатура с интерфейсом USB

2.2.2 Требования к программному обеспечению

Требования к программному обеспечению не предъявляются

3 ПОДГОТОВКА К РАБОТЕ

Действия по настройке и установке Заказчику выполнять не требуется, поскольку жизненный цикл системы предполагает однократную настройку системы на платформе и дальнейшую поддержку работы системы в режиме 100% доступности силами персонала Исполнителя.

4 ОПИСАНИЕ РАБОТЫ

4.1 Установка и настройка ПО

Программное обеспечение должно быть запрограммировано на флеш-носитель, установленный на аппаратную платформу (материнская плата сервера).

4.2 Установка обновлений

Обновления производятся системным администратором Заказчика с участием службы технической поддержки исполнителя

4.3 Штатное функционирование

Программное обеспечение функционирует в составе материнской платы вычислительного устройства (сервера)

5 Аварийные ситуации

Информацию об аварийных ситуациях Исполнитель узнает через:

- Жалобы Заказчика

При ошибках в работе аппаратных средств или смежных систем, восстановление функций ПО возлагается на персонал исполнителя в рамках срока гарантийного обслуживания. После истечения сроков гарантии работы по восстановлению функционала ПО возлагаются на заказчика

6 Эксплуатация системы

6.1 Подготовка к работе

Программное обеспечение должно быть запрограммировано на флеш-носитель, установленный на аппаратную платформу (материнская плата сервера).

6.2 Использование ИС по назначению

Для использования программного продукта необходимо подать электропитание на вычислительную платформу и дождаться ее запуска.

При появлении на экране сообщения «Press DEL to enter setup» необходимо зажать клавишу DEL на клавиатуре и дождаться входа в утилиту Setup (внешний вид окна представлен на рисунке ниже)

Меню настройки BIOS, описанные в этой главе, предназначены только для справки и могут отличаться в зависимости от версии BIOS.

- Системная информация (System Information)
  Эта страница настройки включает в себя все элементы стандартного совместимого BIOS.
- Расширенное меню (Device manager)
  Эта страница настройки включает в себя все элементы специальных расширенных функций OYBot. (например: настройки блочных устройств, портов ввода-вывода, а также модули расширения безопасности)
- Загрузка (Boot Manager)
  На этой странице настройки представлены элементы для выбора устройства загрузки.
- Управление режимами загрузки и консолью вывода (Boot Maintance Manager)
  Включение дополнительных функций загрузки
- Сброс (Reset)
  Опция для сброса настроек OYBoot в начальное состояние
- Продолжение работы (Continue)
  Опция для продолжения работы с сохранением настроек или без сохранения
- Сохранить и выйти. Сохраняет все изменения, внесенные в программе настройки BIOS, в CMOS и выйдите из настройки BIOS. (Нажатие <F10> также может выполнить эту задачу.)

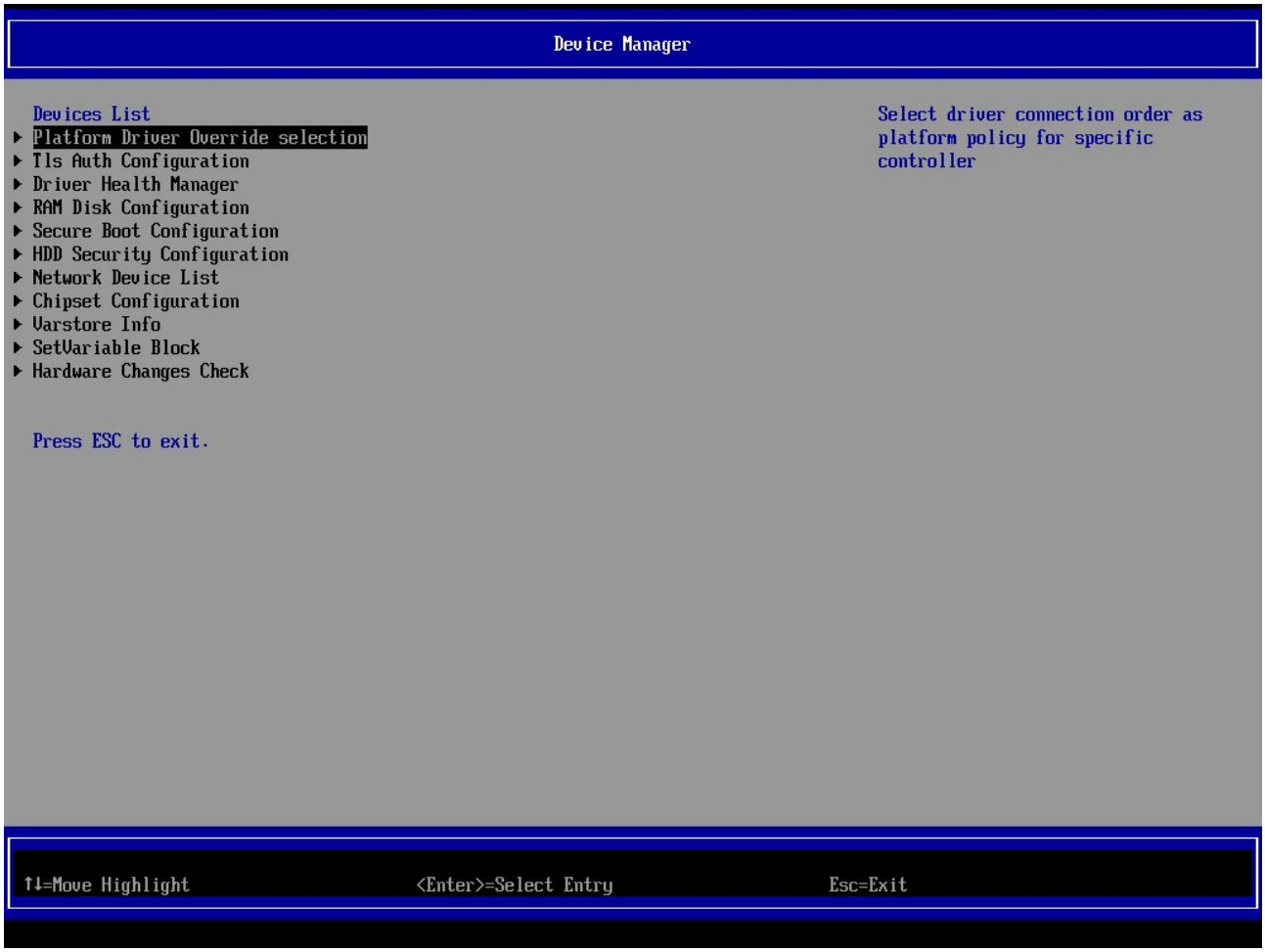
- Отмените все изменения, и предыдущие настройки останутся в силе. Нажатие <Y> в ответ на подтверждающее сообщение приведет к выходу из настройки BIOS. (Нажатие <Esc> также позволяет выполнить эту задачу.)

Параметр	Описание
Информация о BIOS	
Модель устройства	Отображает информацию о модели устройства, на котором развернут OYBoot
Процессор	Наименование процессора (процессоров), установленных в системе
Частота процессора	Максимальная частота работы процессора
Версия проекта	Отображает номер версии утилиты настройки BIOS.
Дата и время	Отображает текущую дату и время
Информация об оперативной памяти	
Наименование памяти	Отображает информацию об установленной памяти.
Частота памяти	Отображает информацию о частоте установленной памяти.

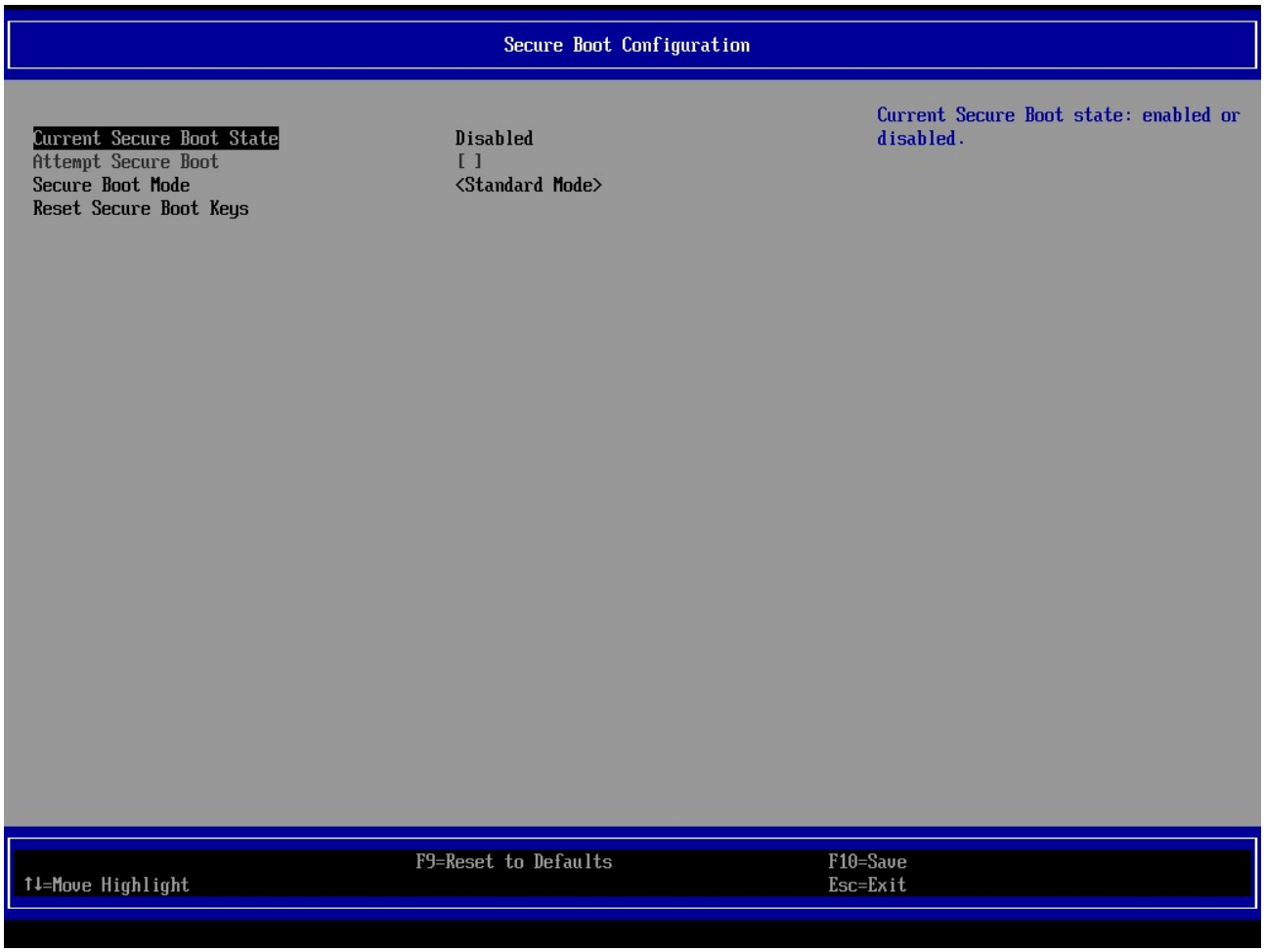

Memory topology
CPU0_DIMM_A1: Samsung M393A8G40BB4-CWE 4210D4CC 31GB 3200MT/s
↑↓=Move Highlight
Esc=Exit

Расширенное меню отображает параметры настройки работы различных аппаратных компонентов. Выберите элемент подменю, затем нажмите <Enter>, чтобы получить доступ к экрану соответствующего подменю.

Для OYBoot доступен исключительно режим работы UEFI



Подменю «Безопасная загрузка» применимо, если на вашем устройстве установлена операционная система Windows (линейки 8 или выше).



Параметр	Описание
Secure Boot Mode	Отображается, если система находится в режиме пользователя или режиме настройки.
Current Secure Boot State	Включить/отключить функцию безопасной загрузки. Параметры доступны: Включено, Отключено. Настройка по умолчанию: Отключено.
Secure Boot Mode(*1)	Безопасная загрузка требует, чтобы все приложения, запущенные во время процесса загрузки, были предварительно подписаны действительными цифровыми сертификатами. Таким образом, система узнает обо всех загружаемых файлах до того, как Windows загрузится при входе в систему. Если установлено значение «Стандарт», ключи безопасной загрузки будут автоматически загружены из базы данных BIOS.

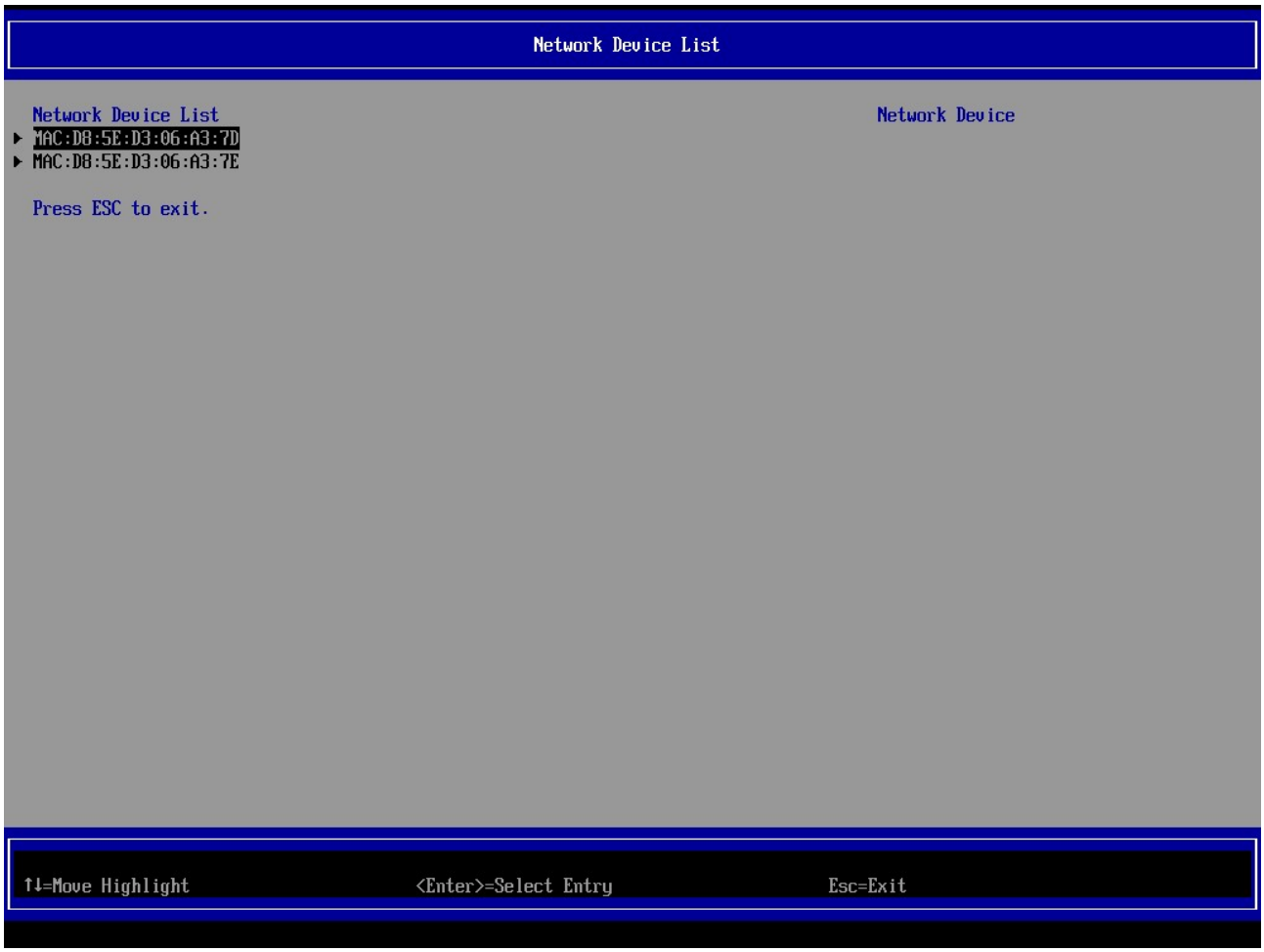
	Если установлено значение «Пользовательский», вы можете настроить параметры безопасной загрузки и вручную загрузить его ключи из базы данных BIOS. Доступные варианты: Стандартный, Пользовательский. Настройка по умолчанию: Пользовательский.

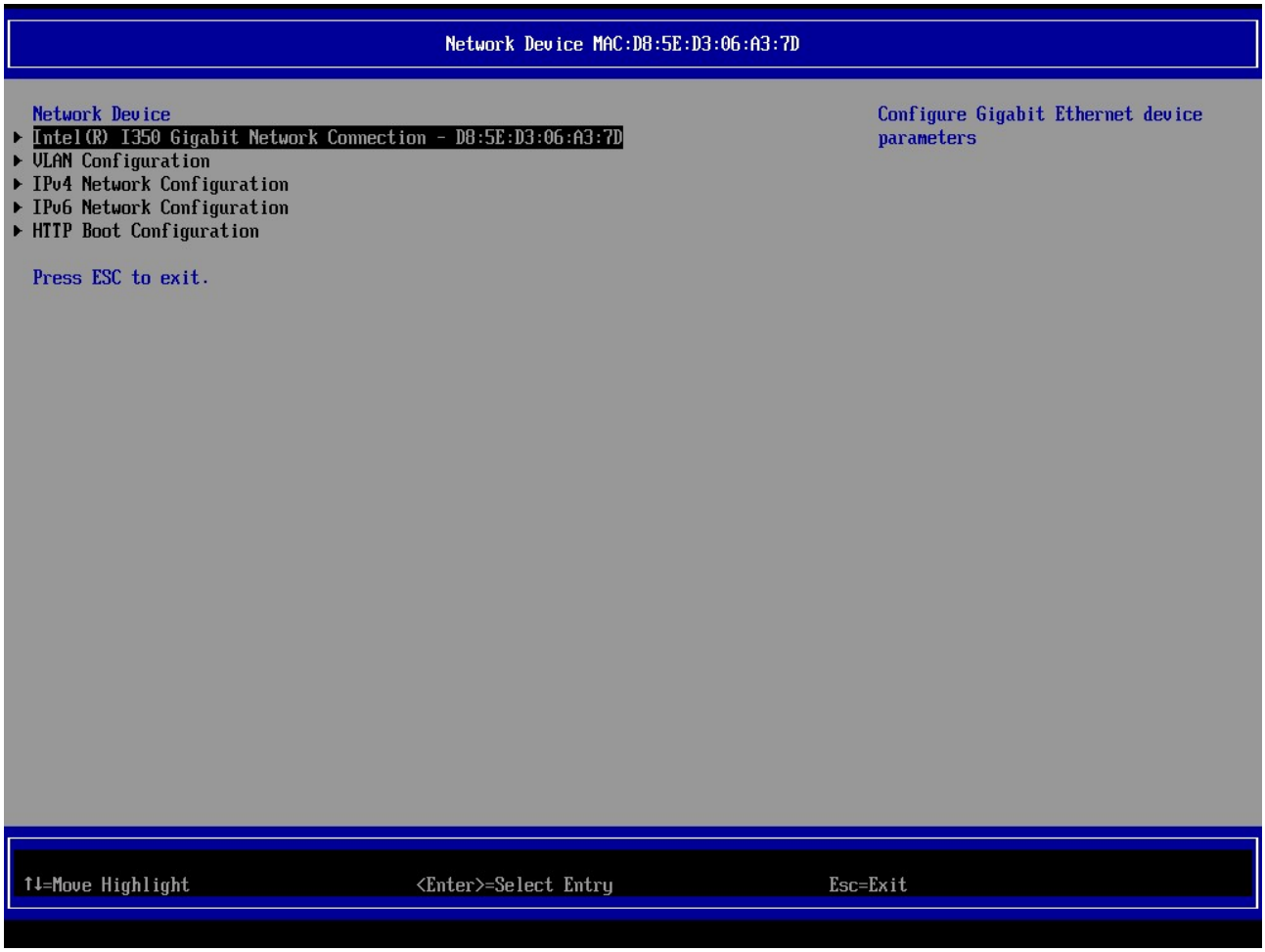
ПРИМЕЧАНИЕ:

1. Дополнительные элементы запрашиваются, когда установлено значение «Пользовательский».

Параметр	Описание
Reset Secure Boot Keys	Переводит систему в пользовательский режим и устанавливает заводские настройки. Безопасная загрузка по умолчанию: База данных.

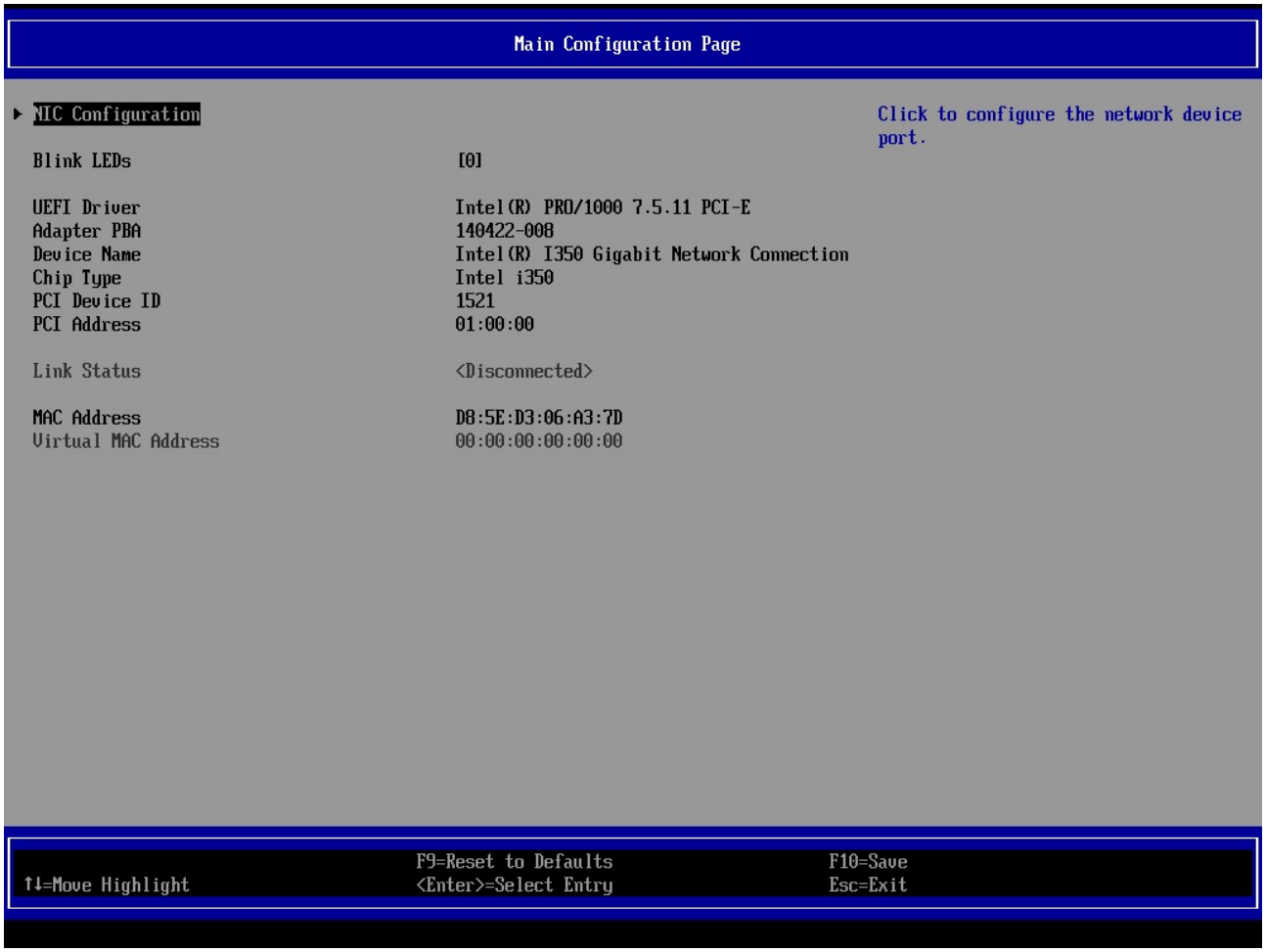
Меню конфигурации сетевого стека





Параметр	Описание
Ipv4 Network Configuration	Включите/отключите функцию Ipv4 PXE. Доступные параметры: Включено, Отключено. Настройка по умолчанию — Включено. Включите/отключите функцию Ipv4 HTTP. Доступные параметры: Включено, Отключено. Настройка по умолчанию — Отключено.
Ipv6 Network Configuration	Включите/отключите функцию Ipv6 PXE. Доступные параметры: Включено, Отключено. Настройка по умолчанию — Отключено. Включите/отключите функцию Ipv6 HTTP. Доступные параметры: Включено, Отключено. Настройка по умолчанию — Отключено.
VLAN Configuration	Нажмите [Enter] для настройки дополнительных элементов. • Создать новую VLAN • Идентификатор виртуальной локальной сети

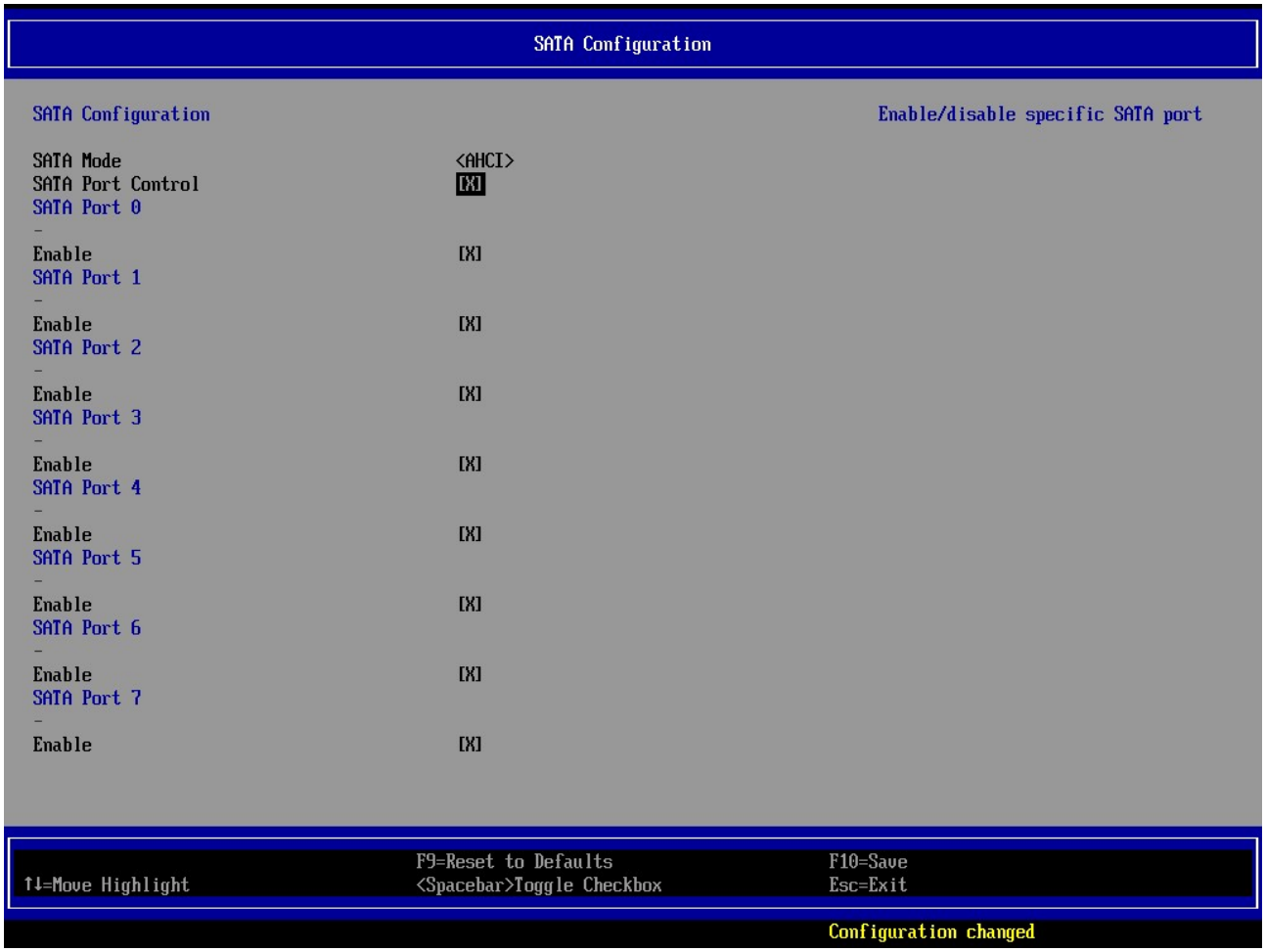
	○ Устанавливает идентификатор VLAN для новой или существующей VLAN ○ Нажмите клавиши <+> / <-> для увеличения или уменьшения желаемых значений. ○ Допустимый диапазон: от 0 до 4094. • Приоритет ○ Устанавливает приоритет 802.1Q для новой или существующей VLAN. ○ Нажмите клавиши <+> / <->, чтобы увеличить или уменьшить нужные значения. ○ Текущий диапазон от 0 до 7. • Добавить VLAN ○ Нажмите [Enter], чтобы создать новую VLAN или обновить существующую VLAN. • Настроенный список VLAN • Удалить VLAN Нажмите [Enter], чтобы удалить существующую VLAN



Параметр	Описание
NIC Configuration	Нажмите [Enter] для настройки дополнительных элементов. • Скорость соединения ○ Позволяет автоматически ограничивать скорость соединения. ○ Доступные варианты: автоматическое согласование, половинная скорость 10 Мбит/с, полная скорость 10 Мбит/с, половинная скорость 100 Мбит/с, полная скорость 100 Мбит/с. Настройка по умолчанию — «Автосогласование». • Wake On LAN ○ Включает/отключает возможность выхода из состояния сна системы через локальную сеть. Обратите внимание, что настройка Wake on LAN в операционной системе не меняет значение этого параметра, но переопределяет поведение Wake on LAN в ОС ○ Доступные варианты: Включено, Отключено. Настройка по умолчанию — Включено.
Blink LEDs	Подсвечивает физический сетевой порт, мигая соответствующим светодиодом. Нажмите цифру на клавиатуре для настройки желаемых значений (до 15 секунд).
UEFI Driver	Отображает технические характеристики контроллера сетевого интерфейса.
Adapter PBA	Отображает технические характеристики контроллера сетевого интерфейса.
Device Name	Отображает технические характеристики контроллера интерфейса
Chip Type	Отображает технические характеристики контроллера сетевого интерфейса.
PCI Device ID	Отображает технические характеристики контроллера сетевого интерфейса.
PCI Address	Отображает технические характеристики контроллера интерфейса
Link status	Отображает технические характеристики контроллера сетевого интерфейса.
MAC Address	Отображает технические характеристики контроллера сетевого интерфейса.
Virtual MAC Address	Отображает технические характеристики контроллера интерфейса

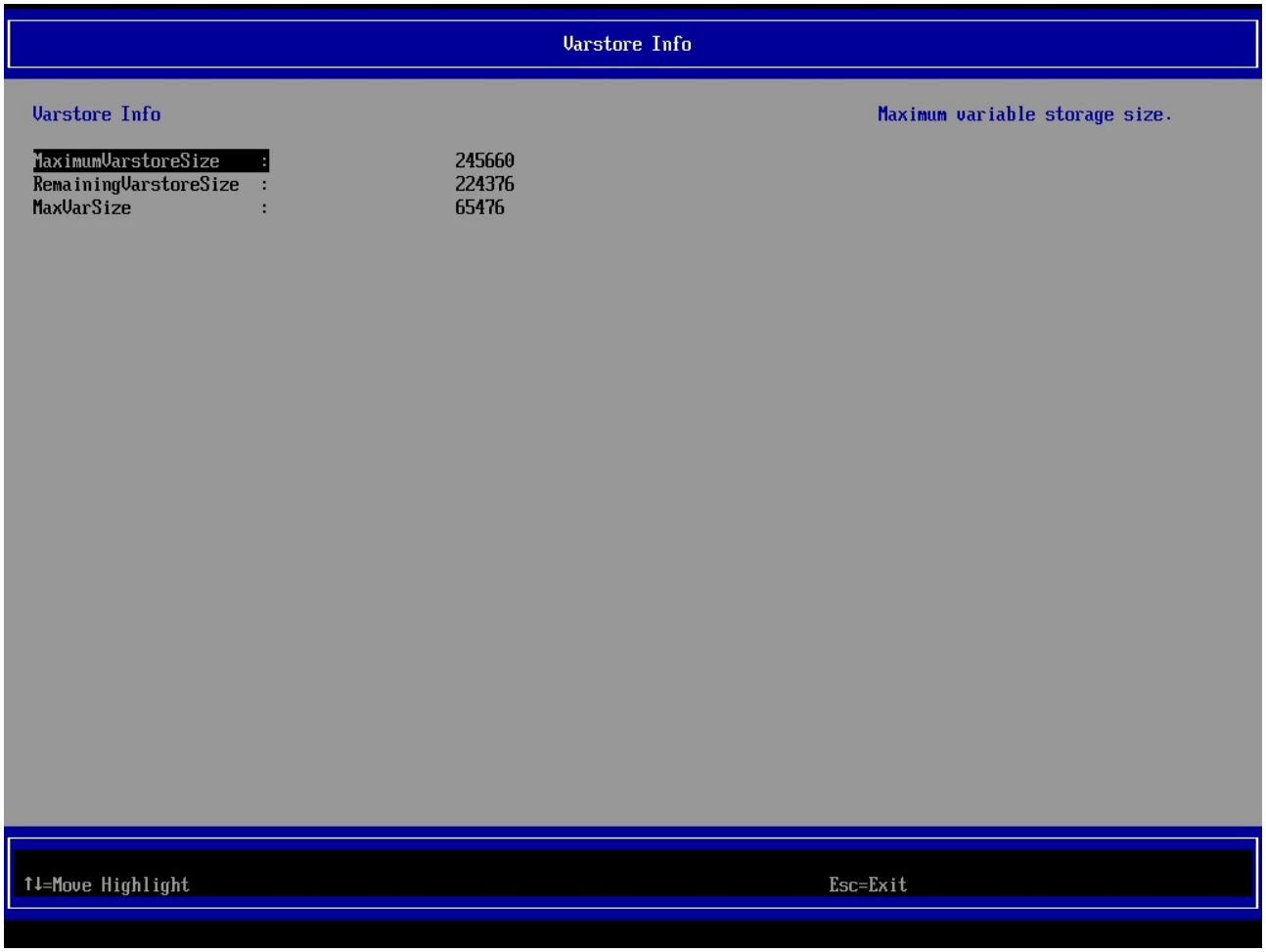
Настройки портов ввода-вывода

Параметр	Описание
USB Configuration	
USB Filter	Задает режим использования USB-портов (HID-only, любое применение)
USB Read-only	Установка режима «только чтение» для USB
USB Port control	Включение-выключение опции управления USB. При включении отображаются опции Front panel / Rear panel для фильтрации настраиваемых портов

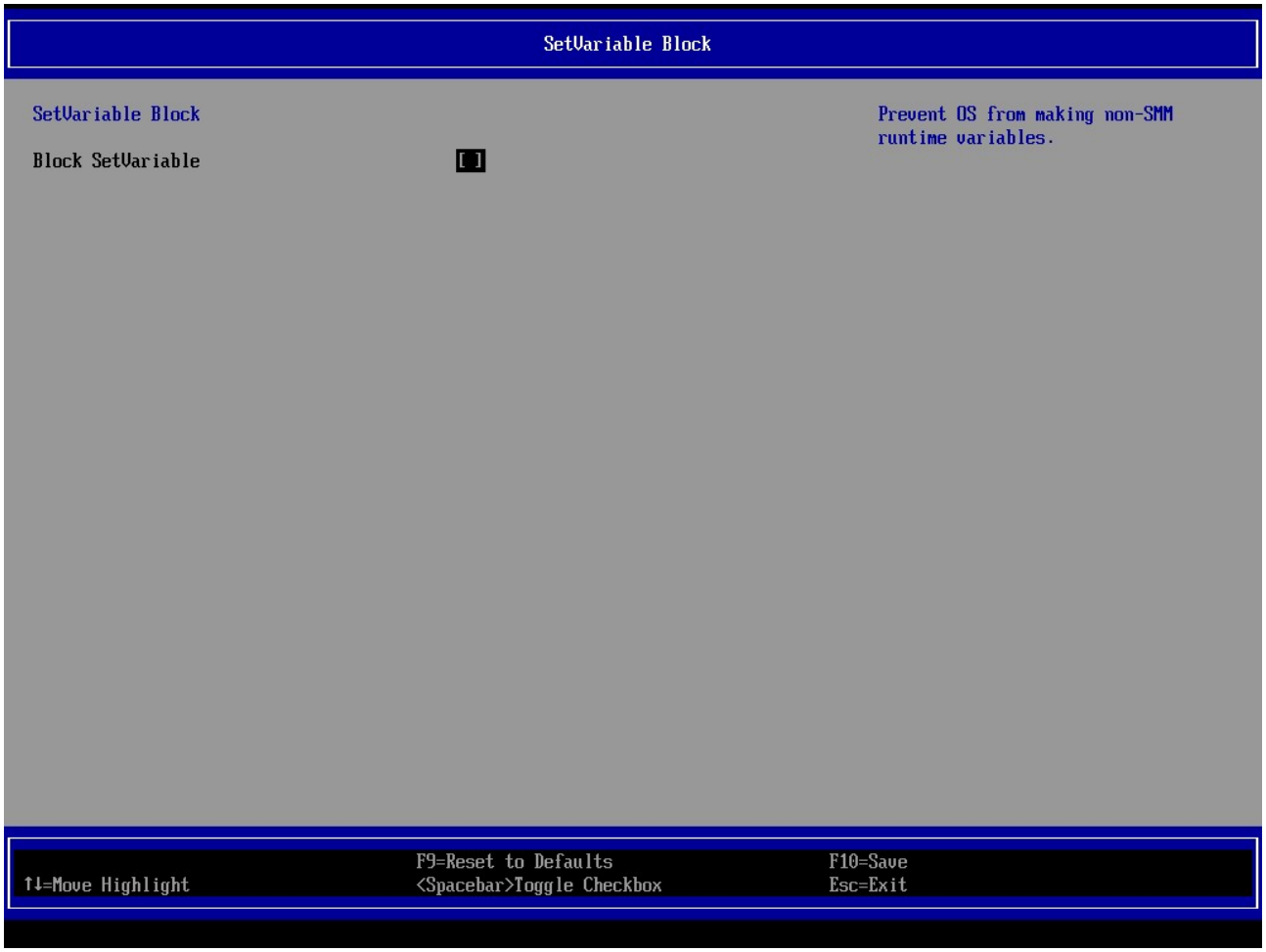


Параметр	Описание
SATA Configuration	
SATA Mode	Установка режима работы SATA контроллера (AHCI / RAID)
SATA Port Control	Включение/выключение опции управления портами SATA
SATA Port X	Включение/выключение порта X SATA

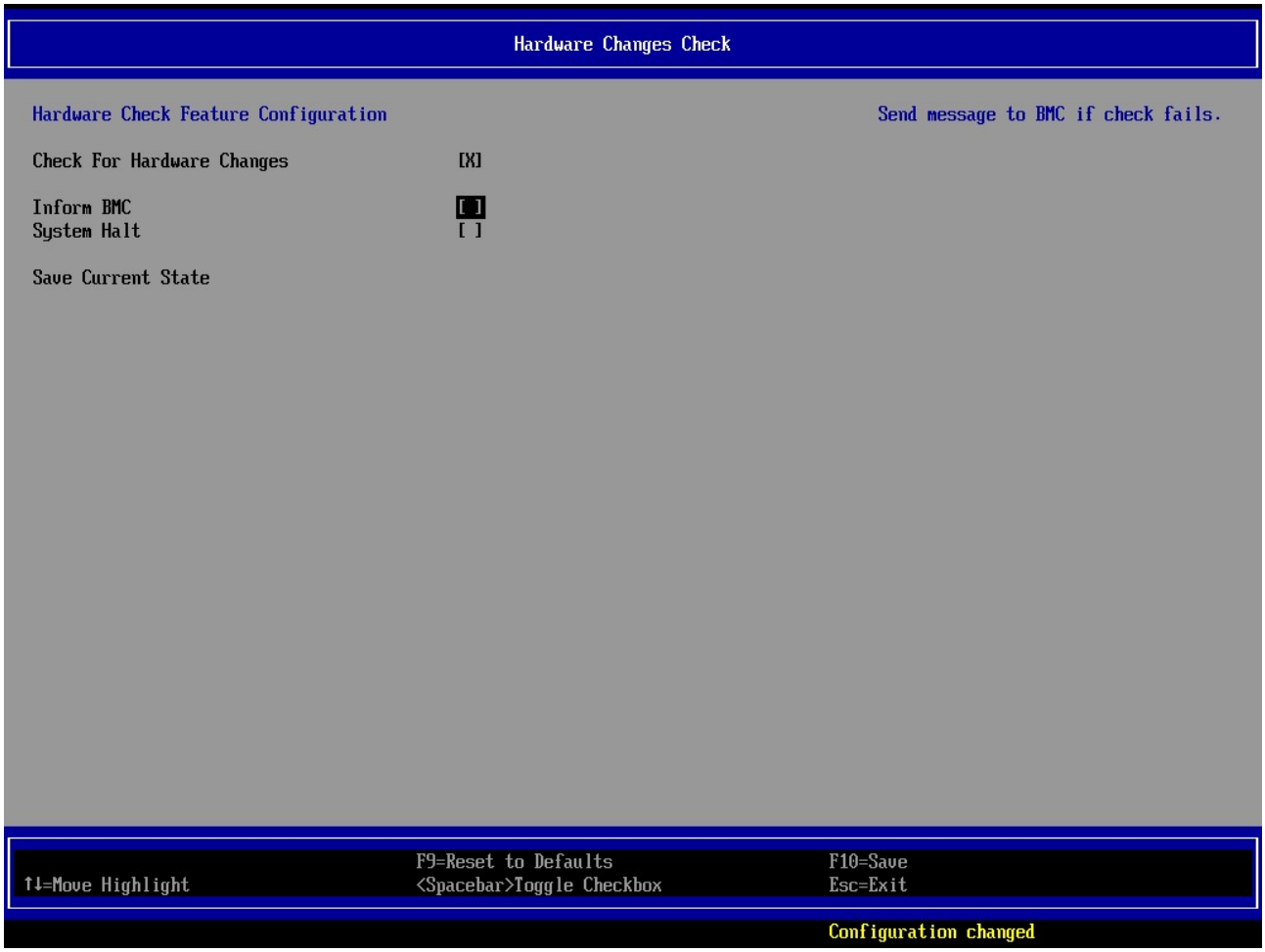
Функционал расширения безопасности



В данном окне отображена информация о системных переменных, используемых UEFI/SMM: максимальный объем занимаемый переменными, текущий объем, максимальный размер переменной



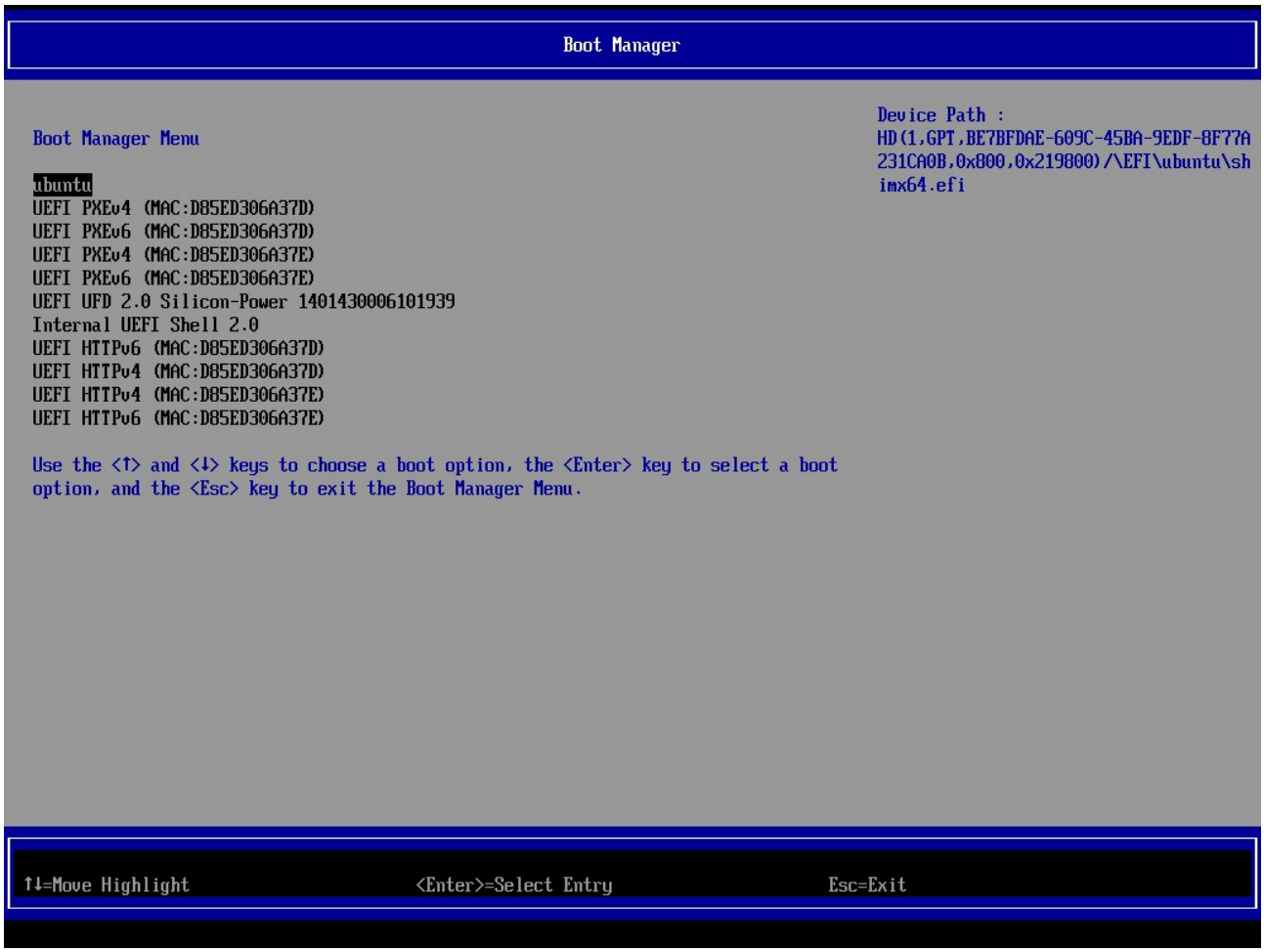
Данная опция осуществляет блокировку записи и изменения системных UEFI-переменных, как при работе SMM, так и в процессе работы операционной системы, что осложняет доступ к аппаратным системам со стороны нежелательного (вредоносного) программного обеспечения, исполняемого на стороне ОС

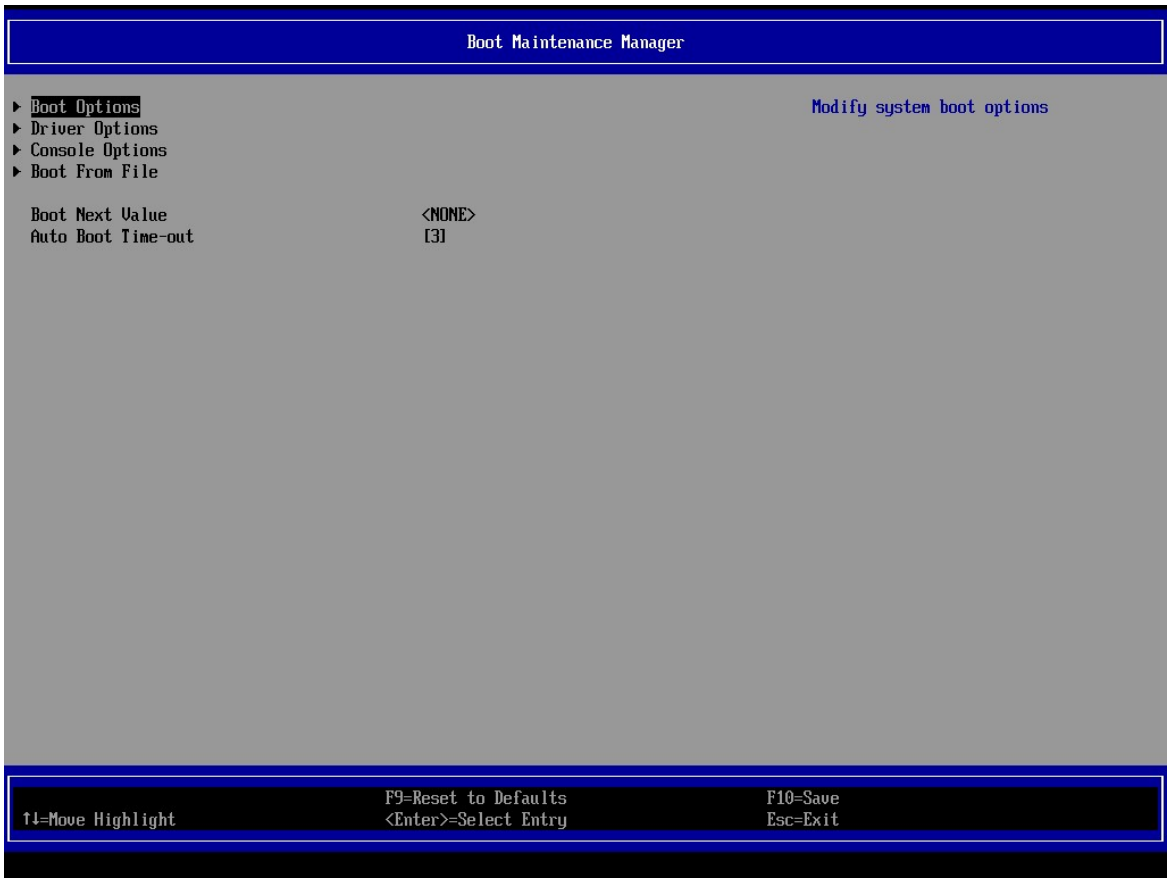


Данный функционал отслеживает изменение аппаратного состояния сервера (установка/удаление оборудования, такого как процессора, планки оперативной памяти и карт расширения).

Путем установки флагов оператор может выбрать способ информирования о факте изменения

Из меню загрузки можно выбрать устройство, с которого будет осуществлена загрузка





Параметр	Описание
BOOT Options	Установка приоритетов загрузочных устройств: -HDD/SSD devices; -PXE network boot; - Build-in EfiShell
Driver Options	Управление процедурой инициализации OpROM
Console Options	Управление последовательной консолью ввода-вывода системы. В данном меню задаются такие параметры, как: - скорость работы (baudrate); - количество бит данных; - наличие бита четности/паритета; - выбор адреса виртуальной консоли (в контексте SuperIO устройства)
Boot From File	Данный раздел раскрывает блочные устройства с UEFI-совместимой файловой системой. Позволяет осуществить загрузку в случае обнаружения там загрузочного раздела (EFI)