СИГНАЛТЕК

# «Базовая система ввода-вывода» RU.ТДРС.01.01.223-1.0

## РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

# Содержание

ВВЕДЕНИЕ ..... 3
1. Общие сведения ..... 4
1.1. Назначение программного обеспечения ..... 4
1.2. Системные требования ..... 4
2. Функциональные возможности ..... 5
3. Настройка ПО БСВВ ..... 6
3.1 Main ..... 8
3.2 Advanced ..... 9
3.3 Platform Configuration ..... 10
3.4 Socket Configuration ..... 12
3.5 Server Management ..... 13
3.6 Security ..... 15
3.7 Boot ..... 17
3.8 Save & Exit ..... 19

## ВВЕДЕНИЕ

Настоящее Руководство по эксплуатации содержит сведения необходимые для настройки и администрирования программного обеспечения «Базовая система ввода-вывода» RU.ТДРС.01.01.223-1.0 (БСВВ).

# 1. ОБЩИЕ СВЕДЕНИЯ

## 1.1. Назначение программного обеспечения

ПО БСВВ – является системной программой низкого уровня, хранящейся в постоянном запоминающем устройстве (Flash-память) на материнской плате ТДРС.467449.003 производства АО «СИГНАЛТЕК», и предоставляет пользователю возможность полного управления системой при загрузке. С помощью ПО БСВВ можно настроить параметры работы аппаратной системы в соответствии с требованиями пользователя или использовать параметры, заданные по умолчанию.

## 1.2. Системные требования

БСВВ применяется для реализации функций базовой загрузки и первичной инициализации оборудования, с последующей передачей управления системному ПО аппаратной платформы сервера на базе материнской платы ТДРС.467449.003 производства АО «СИГНАЛТЕК».

Технические характеристики платы материнской ТДРС.467449.003:

| Параметр | Значение | |
|---|---|---|
| Процессор | Архитектура и модель | До двух микропроцессоров Intel Xeon SPR/EMR (x86) |
| | Тип процессорного разъема (сокет) | Два сокета LGA-4677 (Socket E) |
| Оперативная память | Тип | DDR5 RDIMM/ECC |
| | Количество каналов, шт. | 16 |
| | Максимальный объем | до 8 ТБ (32 x 256 ГБ) |
| | Слот | 32 × 288-pin RDIMM socket |
| Накопители данных | Количество разъемов шт., тип интерфейса | 2 x M2 NVMe\SATA (для системных накопителей данных);<br>3 x Simline |
| | Максимальный объем | До 8 ТБ (4x 2 ТБ) |
| Слоты расширения | 20 разъемов MCIOx8 для организации интерфейсного подключения | |
| Интерфейсы ввода/вывода | Тип | USB 3.1<br>VGA |
| Охлаждение | 8 × 8-pin разъёмов для подключения вентиляторов с регулировкой ШИМ | |

| | |
|---|---|
| Удаленное управление | BMC Aspeed AST2600<br>подключение по сетевому интерфейсу 1000 Base-T (RJ-45) |
| Электропитание | +12 В |

## 2. ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

БСВВ обладает следующими функциями:

1. При включении питания сервера обеспечение загрузки в оперативную память программного обеспечения БСВВ;
2. Выполнение инициализации и тестирования компонентов материнской платы;
3. По окончании загрузки БСВВ передача управления операционной системе сервера;
4. Выполнения заранее определенных действий при обнаружении ошибок в процедуре загрузки БСВВ (повторная загрузка, остановка с выдачей информации об ошибке и др.);
5. Предоставление возможности выполнения отладки ПО с выдачей диагностической информации;
6. Ведение журнала системных событий (логов) и оповещения о событиях (alerts);
7. Обеспечение настройки конфигурации и параметров работы процессоров, оперативной памяти, интерфейсов ввода вывода (SATA, USB, PCI, Ethernet);
8. Настройка доступа к функционалу BMC материнской платы для удаленного управления;
9. Настройка системы безопасности путем определения паролей администратора и пользователя;
10. Сохранение изменений конфигурации и параметров в энергонезависимой памяти при выходе из режима настройки БСВВ.

## 3. НАСТРОЙКА ПО БСВВ

Настройки ПО могут быть изменены посредством пользовательского интерфейса. Сброс в значения настроек по умолчанию производится через пользовательский интерфейс или переключателями на материнской плате (Jumper).

Для входа в программу настройки ПО БСВВ нажмите клавишу Del в момент прохождения POST-теста.

*Некорректно работающее ПО БСВВ может нанести вред оборудованию. Все изменения в настройках должны проводиться квалифицированными специалистами*.

Для перемещения курсива по экрану, выбора и установки значений параметров используются следующие клавиши:

| Клавиша | Действие |
|---|---|
| ← → | Перемещает курсор влево или вправо для выбора экрана. |
| ↑ ↓ | Перемещает курсор вверх или вниз по списку для выбора пункта раздела меню. |
| Enter | Позволяет открыть подменю или выбрать команду. |
| + / – | Смена опции. |
| F1 | Общая помощь. |
| F2 | Предыдущее значение. |
| F9 | Оптимальные настройки по умолчанию. |
| F10 | Сохранение и выход. |
| Esc | Выход из текущего раздела. |

Приведенная выше информация присутствует в качестве подсказки в окне меню на правом нижнем поле выбранной вкладки.

После входа в программу настройки БСВВ на экране появляется окно интерфейса, открытое на вкладке Main (Основное) (Рисунок 1).

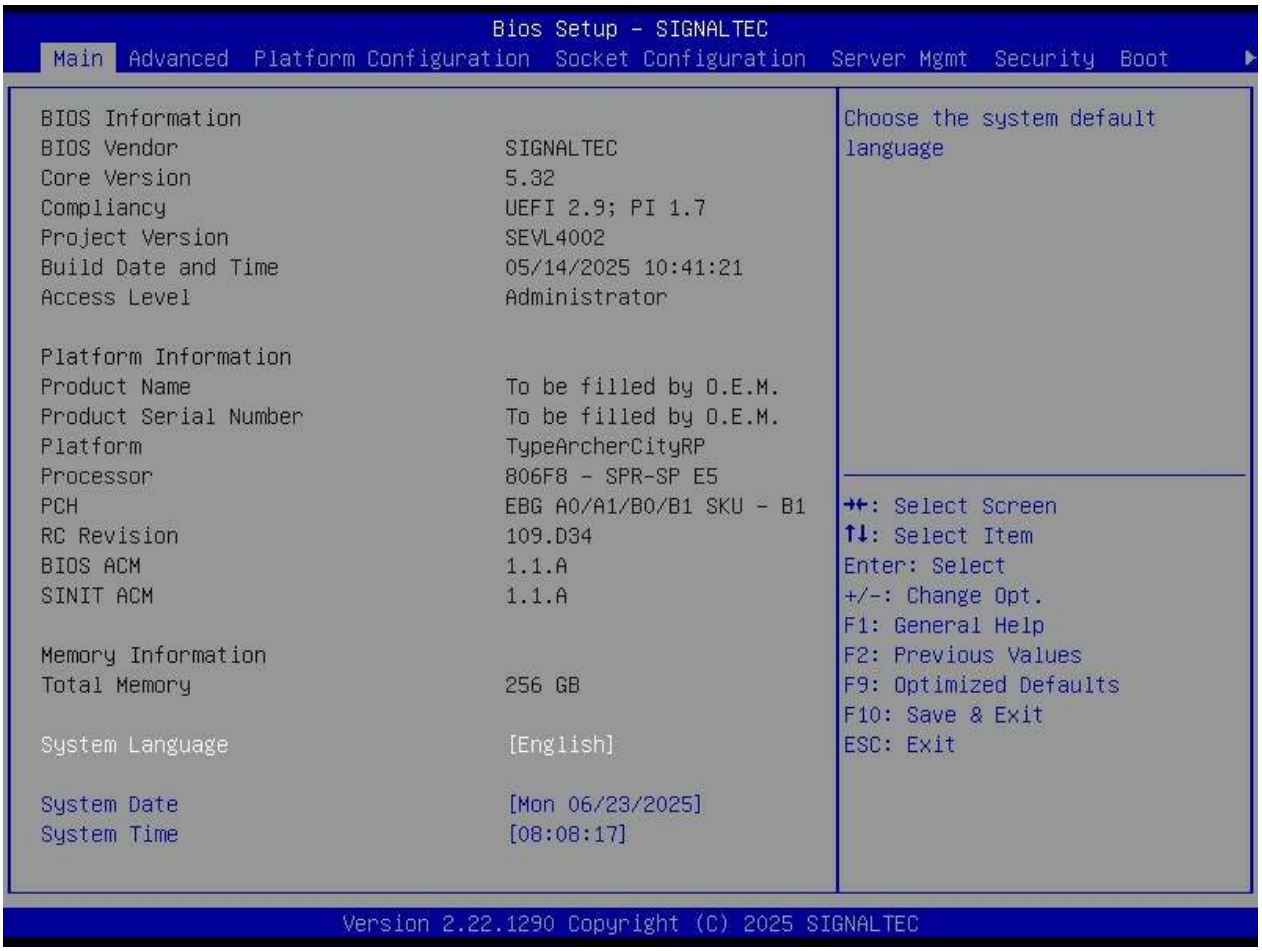


Рисунок 1 Пользовательский текстовый интерфейс ПО

Главное меню интерфейса содержит 8 вкладок:

- *Main* - Вкладка «Main» содержит основную информацию о системе и позволяет установить настройки системной даты и времени;
- *Advanced* - Вкладка «Advanced» содержит расширенные настройки и позволяет осуществить настройку интерфейса управления через сетевой порт материнской платы, а также интерфейсов PCI, USB, VLAN, параметров IP сети для системы удаленного управления*;*
- *Platform Configuration* - Вкладка «Platform Configuration» содержит настройки параметров, связанных с аппаратной платформой (материнской платой), и позволяет осуществить настройку SATA интерфейса, активировать / деактивировать доступ к отдельным USB портам, а также настроить функции, обеспечивающие отладку и запись в журнал информации о возникающих ошибках*;*

- *Socket Configuration* - Вкладка «*Socket Configuration*» содержит настройки параметров, связанных с управлением процессорных сокетов и их окружения, и позволяет осуществить настройку конфигурации процессоров, оперативной памяти для работы в многопроцессорной конфигурации, интегрированного контроллера ввода/вывода, а также настройку управления питанием*;*
- *Server Mgmt* - Вкладка «Server Mgmt» содержит системную информацию и меню управления сервером. Через меню управления сервером имеется возможность активировать поддержку функционала управления аппаратной платформы сервера BMC, В меню также настраиваются параметры, определяющие действия БСВВ в случае возникновения ошибок или неисправностей проверяемых компонент материнской платы в процессе загрузки операционной системы*;*
- *Security* - Вкладка «Security» содержит настройки параметров системы безопасности, в том числе пароли администратора и пользователя*;*
- *Boot* - Вкладка «Boot» содержит расширенные настройки процедуры загрузки сервера*;*
- *Save&Exit* - На вкладке «Save&Exit» обеспечивается выполнение выхода из процедуры настроек параметров БСВВ с сохранением или без сохранения произведённых пользователем настроек. Имеется также возможность возврата настроек всех параметров к значениям «по умолчанию»*.*

### 3.1 Main

Вкладка «Main» содержит основную информацию о системе и позволяет установить настройки системной даты и времени (рисунок 1).

*Информация о БСВВ:*

- Разработчик БСВВ,
- название проекта,
- дата и время сборки,
- уровень доступа пользователя БСВВ.

*Информация о серверной платформе:*

- наименование сервера,

- серийный номер продукта,
- наименование серверной платформы,
- тип процессора,
- тип PCH (Platform Controller Hub),
- номер версии эталонного кода, который используется для создания или обновления микропрограммы БСВВ (RC Revision),
- версия программного модуля, который используется для проверки подлинности и целостности кода БСВВ (BIOS ACM),
- версия программного модуля, который используется для инициализации и проверки доверенной среды исполнения кода (SINIT ACM).

*Информация об установленной оперативной памяти:*

- Суммарный объем установленной оперативной памяти.

*Информация о языке пользовательского интерфейса (System Language).*

*Установка системной даты.*

*Установка системного времени.*

### 3.2 Advanced

Вкладка «Advanced» содержит расширенные настройки (рисунок 2) и состоит из следующих разделов:

*Trusted Computing* (средства доверенного функционирования сервера),

*ACPI Settings* (настройки управления электропитанием - ACPI),

*Serial Port Console Redirection* (настройки функции перенаправления вывода консоли на последовательный порт),

*SIO Common Settings* (установка настроек SIO контроллера),

*SIO Configuration* (настройки SIO контроллера),

*Option ROM Dispatch Policy (*политики загрузки и выполнения дополнительных ПЗУ, которые находятся на платах расширения*);*

*PCI Subsystem Settings* (настройки параметров PCI интерфейса),

*USB Configuration* (настройки интерфейса USB),

*Network Stack Configuration* (настройки стека сетевых протоколов),

*NVMe Configuration* (настройки устройств, подключенных по интерфейсу NVMe),

*Tls Auth Configuration* (настройки аутентификации соединений, использующих протокол TLS),

*RAM Disk Configuration* (создание и настройка виртуального диска за счет части оперативной памяти),

*VLAN Configuration* (настройка VLAN),

*IPv4 Network Configuration* (настройка сетевых параметров IPv4),

*IPv6 Network Configuration* (настройка сетевых параметров IPv6).

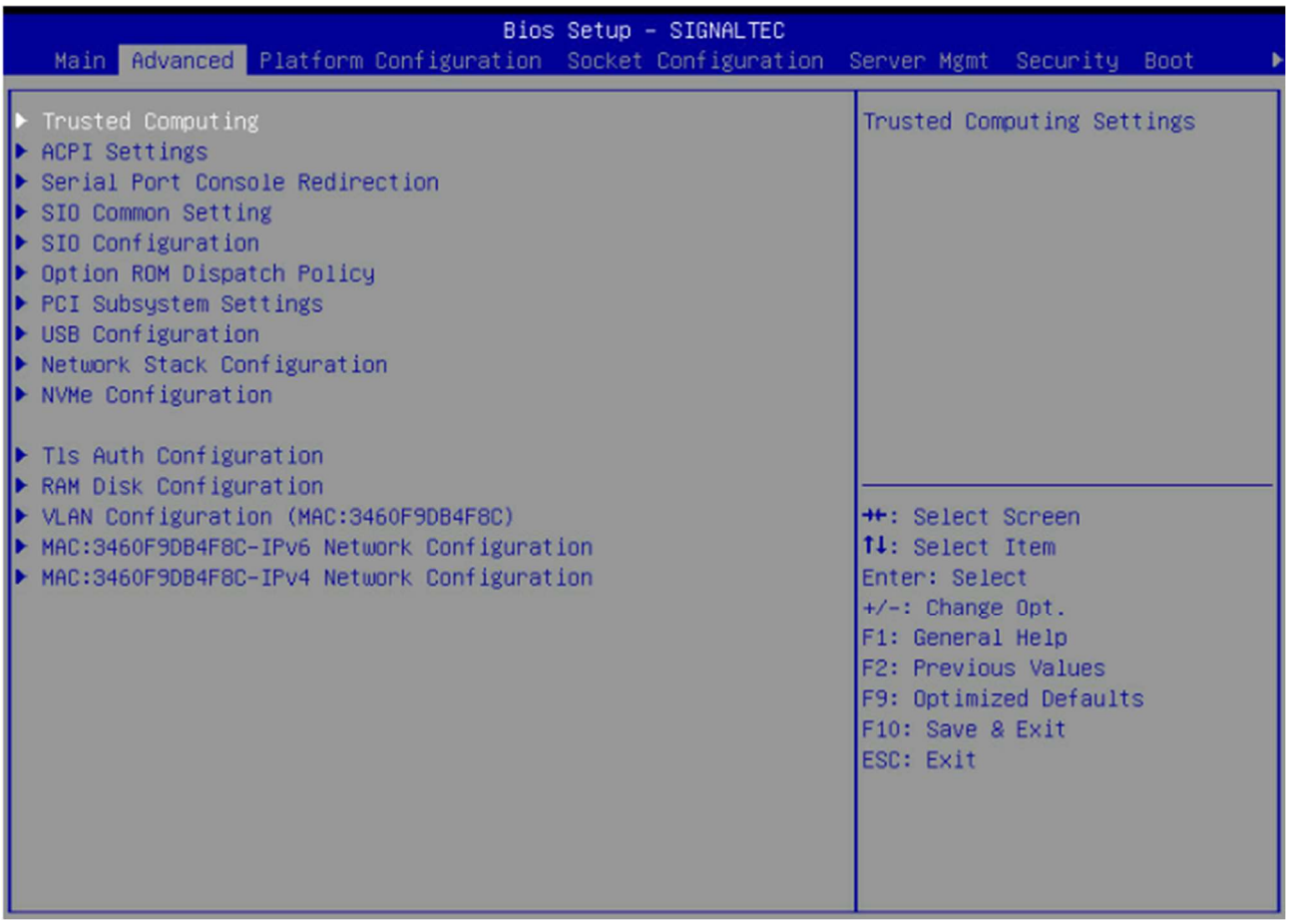


Рисунок 2

### 3.3 Platform Configuration

Вкладка «Platform Configuration» содержит настройки параметров, связанных с аппаратной платформой (материнской платой), и состоит из следующих разделов (Рисунок 3):

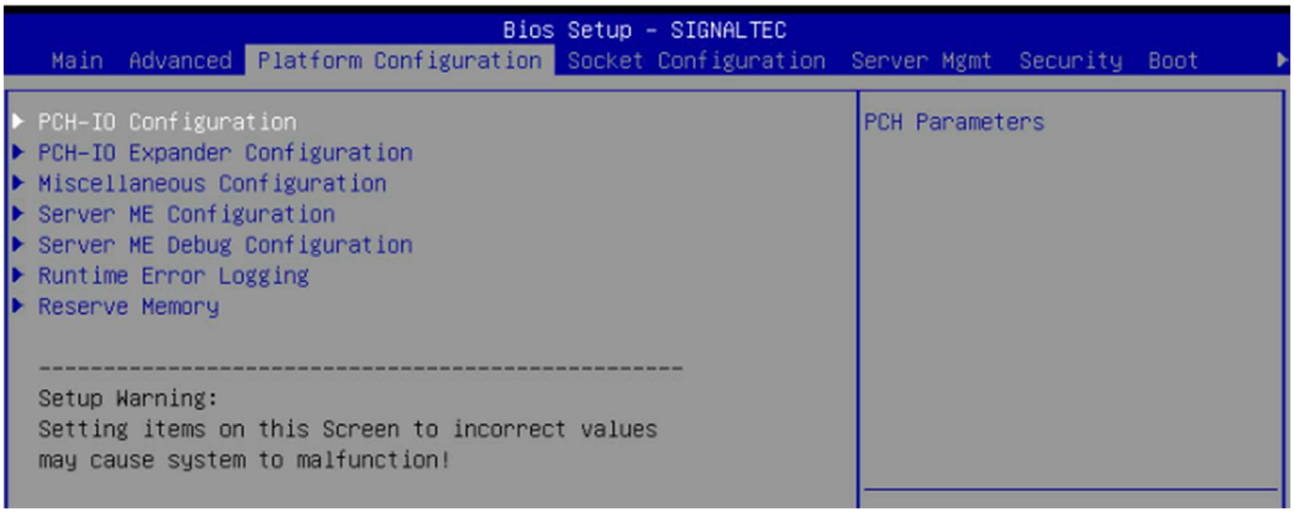


Рисунок 3

- *PCH-IO Configuration* – в данном разделе содержаться настройки контроллера SATA и интерфейса USB;
- *PCH-IO Expander Configuration* – расширенные настройки контроллера SATA и интерфейса USB
- *Miscellaneous Configuration* – в данном разделе содержится дополнительные настройки связанные с аппартаной платформой (материнской платой);
- *Server ME Configuration* – в данном разделе отображена информация о конфигурации ME;
- *Server ME Debug Configuration – раздел настройки параметров ME;*
- *Runtime Error Logging* – в данном разделе содержаться настройки позволяющие записывать в системный журнал информацию об ошибках, возникающих в процессе работы;
- *Reserve Memory* - резервирование определённой области оперативной памяти для использования конкретным устройством или программой.

### 3.4 Socket Configuration

Вкладка «*Socket Configuration*» содержит настройки параметров, связанных с управлением процессорных сокетов и их окружения и состоит из следующих разделов (Рисунок 4):

- *Processor Configuration* – настройка параметров работы процессора(ов);
- *Common RefCode Configuration* – общие настройки работы архитектуры памяти для многопроцессорных систем;
- *Uncore Configuration* – настройки «Uncore» параметров процессора (процессоров): контроллер памяти, кэш памяти, межпроцессорные соединения;
- *Memory Configuration* – настройки оперативной памяти;
- *IIO Configuration* – настройки интегрированного контроллера ввода-вывода (Integrated I/O);
- *Advanced Power Management Configuration* – углубленные настройки управления питанием процессоров.

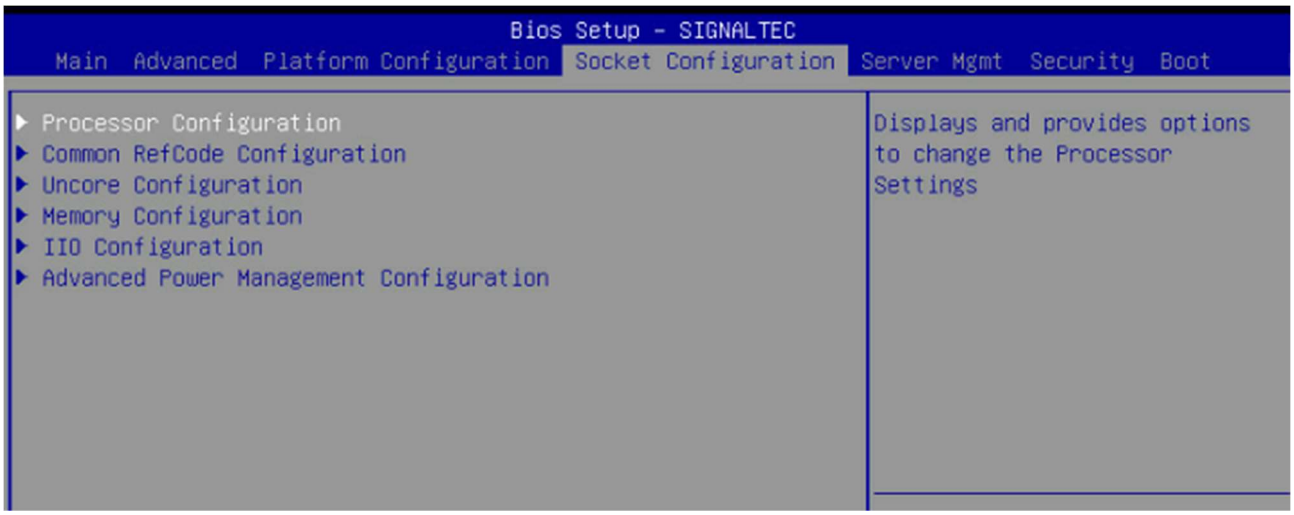


Рисунок 4

### 3.5 Server Management

Раздел обеспечивает управление сервером (рисунок 5).

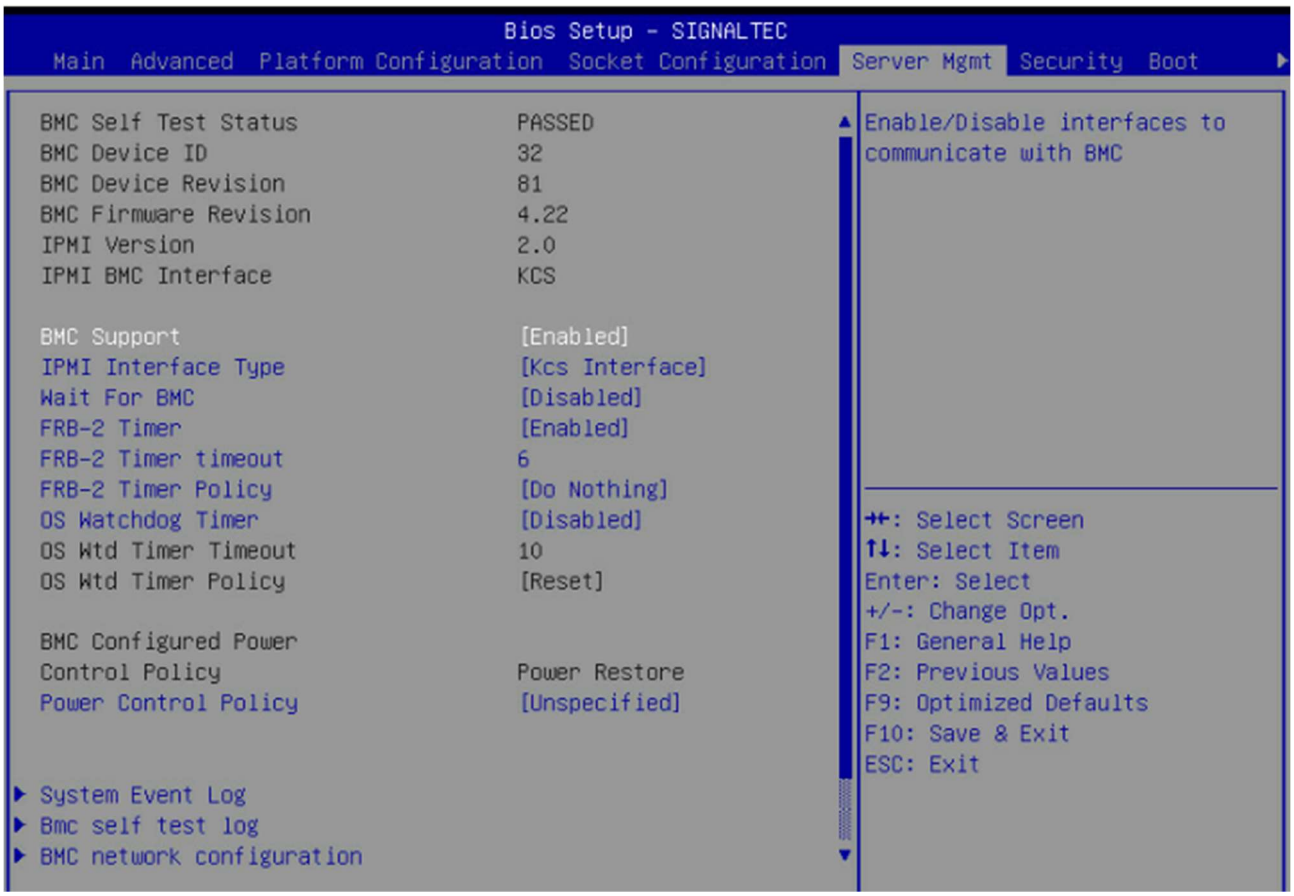


Рисунок 5.

На вкладке «Server Mgmt» отображается следующая системная информация:

- *BMC Self Test Status* – результат самотестирования BMC;
- *BMC Device ID* – идентификатор контроллера BMC*;*
- *BMC Device Revision* - версия аппаратного чипа BMC. Она показывает, какую именно модификацию микросхемы использует материнская плата;
- *BMC Firmware Revision* – ревизия прошивки BMC;
- *IPMI Version* – версия IPMI;
- *IPMI BMC Interface* – интерфейс IPMI BMC.

Управление BMC.

*BMC Support* - активирует/деактивирует интерфейс коммуникации с BMC;

*IPMI Interface Type* – выбор типа интерфейса IPMI;

*Wait For BMC* - если опция «Wait For BMC» активирована (по умолчанию), система будет ждать ответа BMC после включения питания сервера.

*FRB-2 Timer* - активирует/деактивирует FRB 2 таймер (FRB - Fault Resilient Booting)

*FRB-2 Timer timeout* – опция задает выдержку времени для таймера FRB-2. Значение задается в диапазоне 1-30 минут.

*FRB-2 Timer Policy* - опция определяет действие системы по истечении таймера FRB 2. Возможны следующие варианты действий:

– перезагрузка сервера,

– выключение питания,

– выключение питания с последующим включением,

– не выполнять никаких действий (действие по умолчанию).

*OS Watchdog Timer* – включение/выключение сторожевого таймера BMC который следит за "живучестью" операционной системы.

*OS Wtd Timer Timeout* - установка периодичности с которой будут посылаться запросы на проверку «живучести» ОС.

*OS Wtd Timer Policy* - расширенная настройка, которая определяет как именно, в каких условиях и с какими приоритетами работает аппаратный сторожевой таймер, следящий за операционной системой.

*Power Control Policy* - опция определяет действие системы в случае пропадания питания. Возможны следующие варианты действий:

– не включать питание,

– восстановить питание,

– возврат к сохраненному последнему состояния питания.

– не выполнять никаких действий (действие по умолчанию).

На вкладке управления сервером (Server Mgmt) вызываются следующие дополнительные меню настроек:

– *System Event Log* - В данном разделе обеспечивается настройка журнала событий, которые генерирует операционная система.

- *BMC network configuration* - В данном разделе отображается информация о параметрах сетевого подключения BMC для настроенных каналов (режим получения адреса, IP адрес, маска сети, MAC адрес, IP адрес маршрутизатора, MAC адрес маршрутизатора).
- *BMC self test log* – в данном разделе отображается log-информация в результате работы самотеста BMC.
- *View System Event Log* - В данном разделе отображается количество записей о событиях, и список записей с указанием даты, времени и описания события.
- BMC User Settings- В данном разделе осуществляется настройка параметров доступа пользователей к BMC.

### 3.6 Security

Вкладка «Security» содержит настройки параметров системы безопасности (рисунок 6).

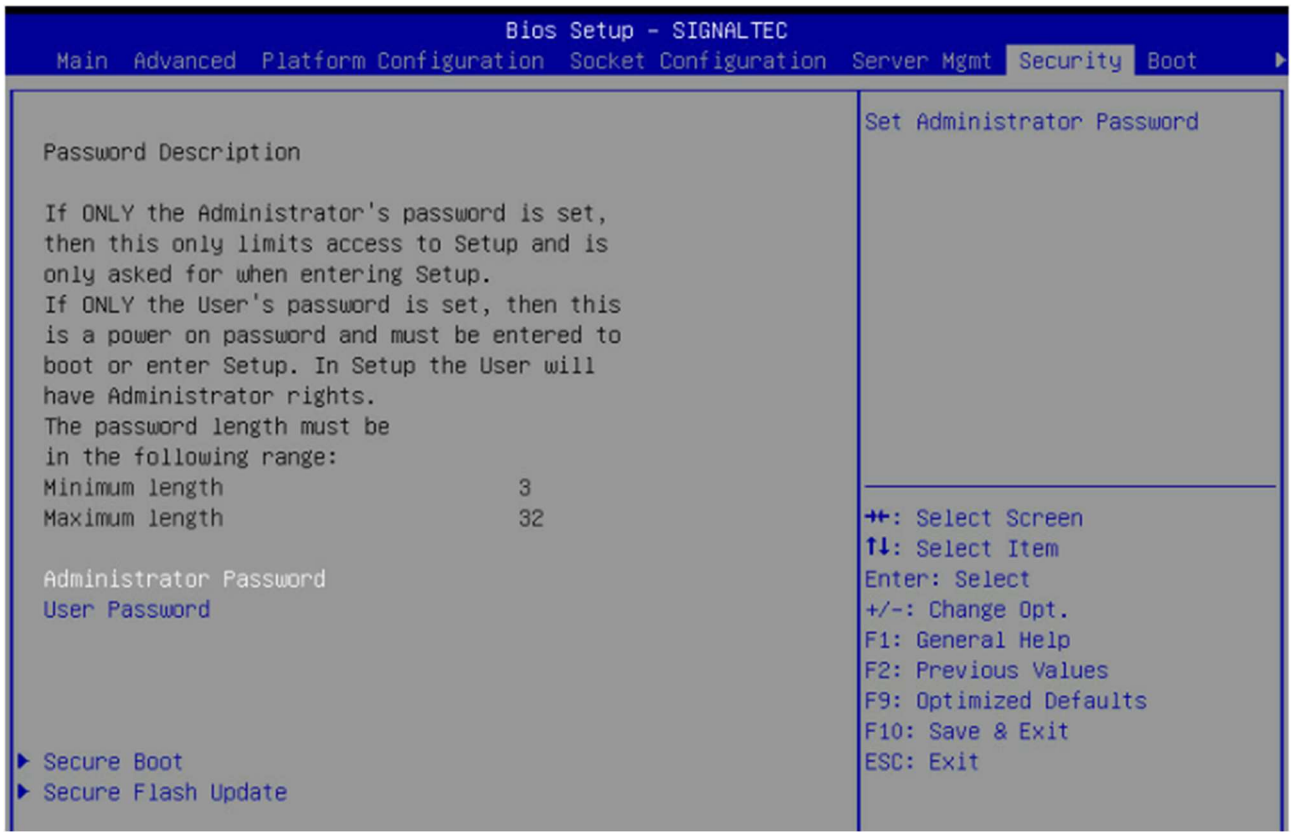


Рисунок 6

Для обеспечения безопасности используется пароль. В настройках задается минимальная (3 знака) и максимальная длина пароля (32 знака).

Может быть задан пароль Администратора *(Administrator password)* и пароль Пользователя (*User Password*).

Если определен только пароль Администратора, то ограничивается только доступ к Setup. Пароль запрашивается при входе в Setup.

Если определен только пароль пользователя, то пароль запрашивается при включении питания и должен быть введен для выполнения загрузки или входа в Setup.

*Secure Boot* – Эта функция позволяет осуществлять проверку цифровой подписи по ключу в хранилище PK (Platform Key).

*Secure Flash Update* – активация механизма обновления БСВВ, который проверяет подлинность и целостность обновления БСВВ перед тем, как записать его в микросхему флеш-памяти.

### 3.7 Boot

Вкладка «Boot» содержит расширенные настройки процедуры загрузки сервера (рисунок 7).

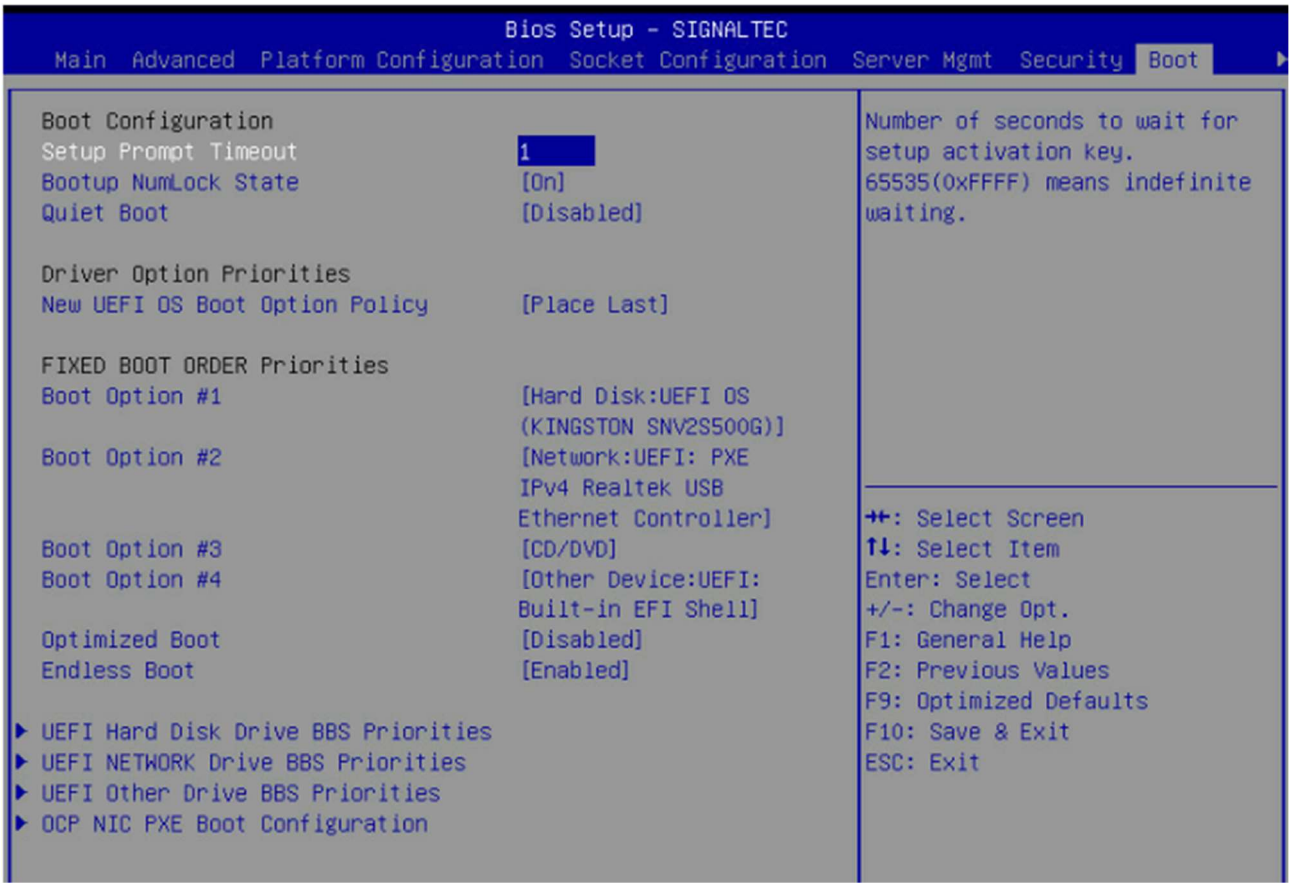


Рисунок 7

В разделе *Boot Configuration* выполняется настройка общих параметров загрузки.

*Setup Prompt Timeout* – количество секунд ожидания установки ключа активации.

*Bootup Numlock State* - выбор начального состояния ключа NumLock на клавиатуре (*On/Off*).

*Quiet Boot* - активация / деактивация режима *Quiet Boot.*

*New UEFI OS Boot Option Policy* – управление расположением обнаруженных новых опций загрузки UEFI.

В разделе *FIXED BOOT ORDER Priorities* настраиваются дополнительные опции процедуры загрузки.

*Boot Option #x* – установка последовательности выбора системных устройств загрузки. Последовательность выбора по умолчанию: *Hard Disk -> Network -> CD/DVD -> Other Device.*

*Optimized Boot* – режим оптимизированной загрузки БСВВ, который сокращает время загрузки компьютера за счёт пропуска некоторых проверок, инициализации устройств и задержек.

*Endless Boot* – если разрешена данная опция, то после ошибки загрузки БСВВ снова пытается выполнить все опции загрузки.

*UEFI Hard Disk Drive BBS Priorities* – установка порядка загрузки жёстких дисков и SSD. Он позволяет выбрать, с какого именно физического диска будет загружаться система, если у вас установлено несколько накопителей.

*UEFI Network Drive BBS Priorities* – установка порядка загрузки с сетевых устройств. Опция позволяет выбрать, с какого именно сетевого интерфейса (порта) или типа сетевой загрузки будет загружаться система.

*UEFI Other Drive BBS Priorities* – установка порядка загрузки устройств отличных от дисков и сетевых устройств: Flash память, оптические приводы и т.п.

*OCP NIC PXE Boot Configuration* — это настройка которая управляет сетевой загрузкой (PXE) через сетевое устройство в форм-факторе OCP.

### 3.8 Save & Exit

На вкладке «Save&Exit» обеспечивается выполнение выхода из процедуры настроек параметров БСВВ (рисунок 8).

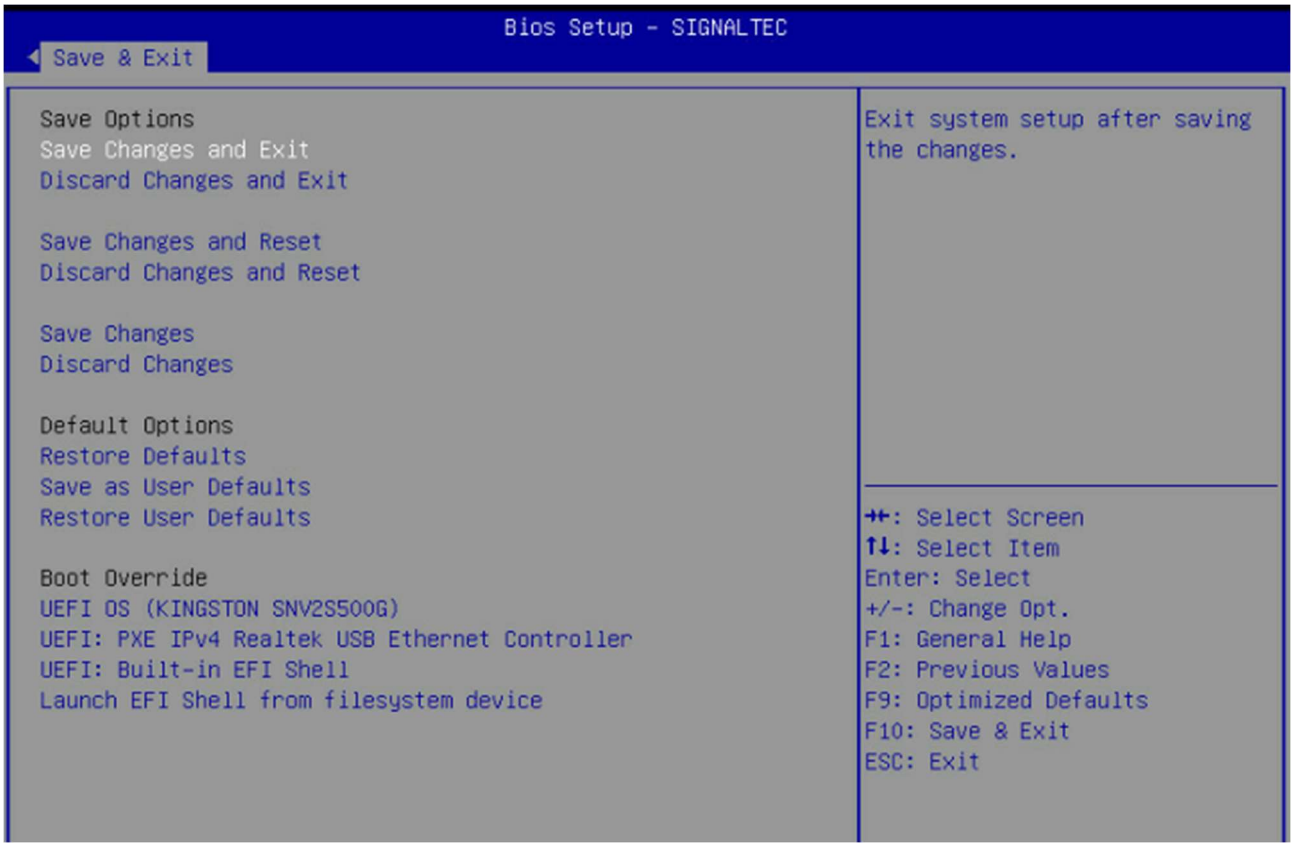


Рисунок 8

Возможны следующие варианты:

- *Save Changes and Exit* – сохранить изменения и выполнить выход из процедуры настройки.
- *Discard Changes and Exit* - выполнить выход из процедуры настройки без сохранения настроек.
- *Save Changes and Reset* - сохранить изменения и выполнить перезагрузку (Reset) системы.
- *Discard Changes and Reset* - выполнить перезагрузку (Reset) системы без сохранения настроек.
- *Save Changes* – сохранить внесенные изменения в настройки параметров
- *Discard Changes* – не сохранять внесенные изменения в настройки параметров.

Также доступны следующие опции в разделе.

- *Restore Defaults* – восстановить значения по умолчанию для всех параметров.
- Save as User Defaults - сохраняем текущие настройки как пользовательский шаблон (профиль) настроек по умолчанию.
- *Restore as User Defaults* – востстановить пользовательский шаблон настроек по умолчанию.

*Boot Override* – установка однократной загрузки с выбранного устройства