ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ БАЗОВОЙ СИСТЕМЫ ВВОДА-ВЫВОДА ПЛАТЫ СЕРВЕРНОЙ ВСМ-МВ

Руководство администратора

643.18184162.00021-01 90

Листов 41

АННОТАЦИЯ

Настоящее руководство администратора содержит сведения об операциях, которые можно осуществлять с помощью программного обеспечения базовой системы ввода-вывода платы серверной ВСМ-МВ (далее по тексту – ПО БСВВ ВСМ-МВ).

В настоящем руководстве администратора содержится информация о назначении ПО БСВВ ВСМ-МВ, его функциях, ограничениях на применение, сведения о технических средствах, обеспечивающих его выполнение. Также представлены сведения о настройке ПО БСВВ ВСМ-МВ, работе, приводятся информационные сообщения, сообщения об ошибках и способы их устранения.

Данное руководство ориентировано на системных администраторов.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Обозначение и наименование

Полное наименование программного обеспечения – «Программное обеспечение базовой системы ввода-вывода платы серверной ВСМ-МВ».

Краткое наименование программного обеспечения – ПО БСВВ ВСМ-МВ.

Обозначение программного обеспечения – 643.18184162.00021-01.

1.2. Назначение

ПО БСВВ ВСМ-МВ представляет собой программный код, предназначенный для инициализации аппаратного обеспечения и загрузки операционной системы (ОС).

1.3. Функции и возможности

ПО БСВВ ВСМ-МВ обеспечивает:

1) выполнение ядра UEFI с функциями проверки целостности других компонентов прошивки;

2) инициализацию и тестирование низкоуровневого аппаратного обеспечения;

3) загрузку и выполнение дополнительных модулей прошивки, которые либо расширяют возможности системного BIOS, либо инициализируют другие аппаратные компоненты, необходимые для загрузки системы. Эти дополнительные модули могут храниться внутри той же самой флэш-памяти, что и системный UEFI, либо могут храниться в аппаратных устройствах, которые они инициализируют (например, в видеокарте, сетевой карте);

4) выбор устройства загрузки (например, жесткого диска, оптического привода, USB-накопителя) и выполнение загрузчика, хранящегося на этом устройстве;

5) загрузку ОС.

1.4. Условия применения

1.4.1. Требования к программному обеспечению

ПО БСВВ ВСМ-МВ должно обеспечивать:

– встроенные механизмы защиты ПО БСВВ ВСМ-МВ должны контролировать доступ наименованных субъектов к функциональным элементам в соответствии с заданной ролью. Должны присутствовать роли «Администратор» и «Пользователь»:

а) Роль «Администратор»:

1) задание паролей доступа в ПО БСВВ ВСМ-МВ;

2) изменение настроек ПО БСВВ ВСМ-МВ.

б) Роль «Пользователь»:

1) ограниченный доступ к разделу меню «Настройки» (нельзя менять параметры «ACPI и управление питанием», «Настройка параметров USB»);

2) недоступно изменение параметров раздела меню «Управление»;

3) недоступно изменение параметров раздела меню «Безопасность» (кроме смены пароля «Пользователя»).

– должен проводиться контроль целостности ПО БСВВ ВСМ-МВ. Контроль целостности по требованию администратора должен осуществляться путем сравнения значений, отображаемых в интерфейсе ПО, со значениями, указанными в формуляре 643.18184162.00021-01 30.

ПО БСВВ ВСМ-МВ поставляется исключительно в предустановленном виде на плату серверную ВСМ МВ.

Обновление ПО БСВВ ВСМ-МВ при эксплуатации не предусмотрено. В случае необходимости, обновление ПО может быть произведено на заводе изготовителе.

1.4.2. Требования к аппаратному обеспечению

Для работы ПО БСВВ ВСМ-МВ необходима плата серверная ВСМ-МВ с микросхемой SPI Flash объемом не менее 16 МБ.

1.5. Правила поведения администратора

Должны быть приняты организационные (организационно-технические) меры, исключающие неконтролируемый доступ посторонних лиц к рабочему месту администратора в нерабочее время, а также в рабочее время при его отсутствии.

Администратор должен работать в соответствии с настоящим документом 643.18184162.00021-01 90 «Программное обеспечение базовой системы ввода-вывода платы серверной ВСМ-МВ. Руководство администратора».

2. ОПИСАНИЕ СТРУКТУРЫ

2.1. Структура ПО БСВВ ВСМ-МВ

ПО БСВВ ВСМ-МВ разбито на разделы, каждый из которых имеет модульную структуру. Логическая структура ПО БСВВ ВСМ-МВ приведена на рисунке 2.1.

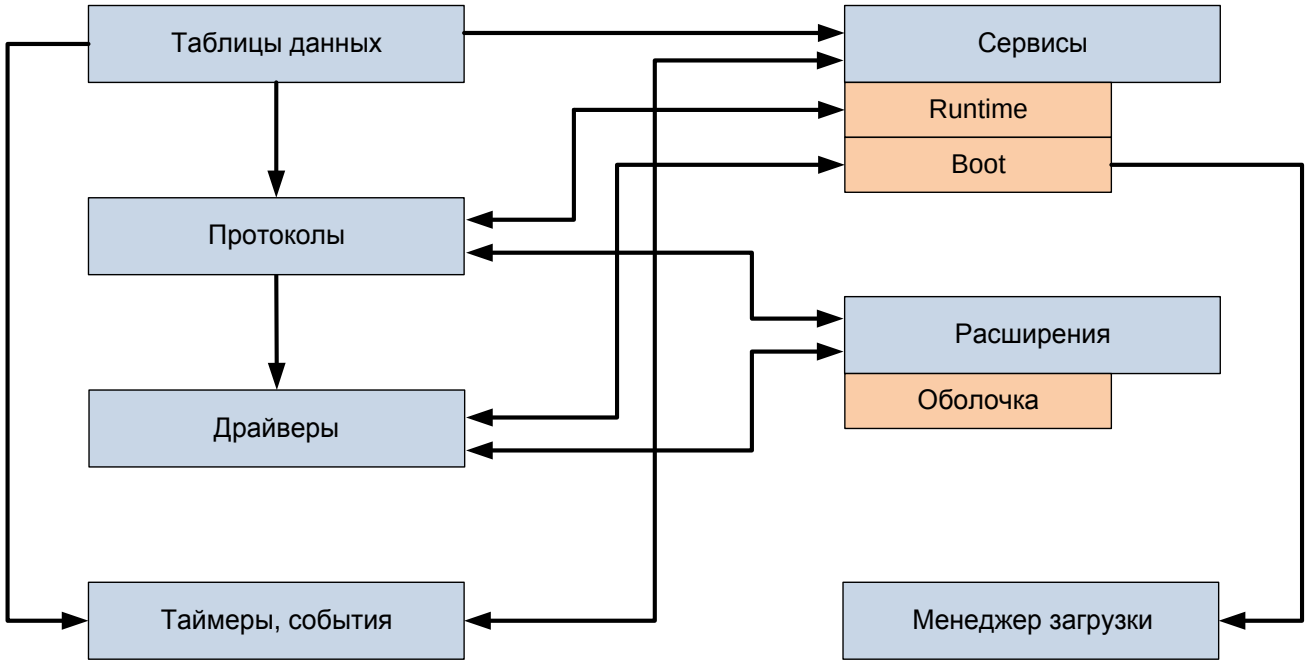

Рис. 2.1

Объектно-управляемый интерфейс ПО БСВВ ВСМ-МВ представляет собой множество различных типов объектов. Данные объекты взаимодействуют между собой посредством сервисов, предоставляемых ПО БСВВ ВСМ-МВ.

ПО БСВВ ВСМ-МВ состоит из следующих логических блоков:

– таблицы данных: содержат информацию о платформе, загрузочных, runtime-сервисах, протоколах и драйверах, которые доступны в процессе работы ПО БСВВ ВСМ-МВ, а также для загрузчика ОС и самой ОС;

– сервисы – включают поддержку текстовой и графической консоли на различных устройствах, шин, блоков и файловых сервисов, runtime-сервисы, например: дата, время и энергонезависимая память;

– драйверы устройств – в дополнение к стандартным, архитектурно-зависимым драйверам устройств, спецификация UEFI предусматривает независимую от платформы среду драйверов,

называемую EFI Byte Code (EBC). От системного встраиваемого ПО спецификацией UEFI требуется иметь интерпретатор для любых образов EBC, которые загружены или могут быть загружены в среду. Некоторые архитектурно-зависимые (non-EBC) типы драйверов UEFI могут иметь интерфейсы для использования ОС. Это позволяет ОС использовать UEFI для базовой поддержки графики и сети до загрузки драйверов, определенных в ОС;

– таймеры и события, как и другие типы объектов ПО БСВВ ВСМ-МВ, управляются посредством сервисов. Поскольку UEFI не поддерживает прерывания, то наиболее часто события от таймера используются драйверами ПО БСВВ ВСМ-МВ для периодического опроса устройств;

– протоколы – набор указателей на функции и структуры данных или API, которые определены соответствующей спецификацией. Функции протоколов содержатся в соответствующих драйверах;

– менеджер загрузки – используется для выбора и загрузки ОС, исключая потребность в специализированном механизме загрузки (загрузчик ОС является приложением ПО БСВВ ВСМ-МВ);

– расширения – могут быть загружены с практически любого энергонезависимого устройства хранения данных, присоединенного к компьютеру;

– оболочка – открытая среда оболочки (shell environment). Пользователь для выполнения некоторых операций может загрузить оболочку вместо того, чтобы загружать ОС. Оболочка - приложение ПО БСВВ ВСМ-МВ, она может постоянно находиться в постоянном запоминающем устройстве (ПЗУ) платформы или на устройстве, драйверы для которого находятся в ПЗУ. Оболочка может использоваться для выполнения других приложений ПО БСВВ ВСМ-МВ, таких как настройка, установка ОС, диагностика, утилиты конфигурации и обновления прошивок. Команды оболочки ПО БСВВ ВСМ-МВ также позволяют копировать или перемещать файлы и каталоги в поддерживаемых файловых системах, загружать и выгружать драйверы. Также оболочкой может использоваться полный TCP/IP стек. Оболочка ПО БСВВ ВСМ-МВ поддерживает сценарии в виде файлов .nsh, аналогичных пакетным файлам в DOS. Названия команд оболочки часто наследуются от интерпретаторов командной строки (COMMAND.COM или Unix shell). Оболочка ПО БСВВ ВСМ-МВ может рассматриваться как функциональная замена интерпретатора командной строки и текстового интерфейса BIOS.

3. РАБОТА С ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ

3.1. Описание интерфейса

Управление и навигация в BIOS Setup осуществляются с помощью клавиатуры, список командных клавиш и выполняемые ими функции перечислены в таблице 3.1.

Таблица 3.1 – Клавиши управления в BIOS Setup

Клавиша	Функция	Описание
Enter	Выполнить	Кнопкой «Enter» активируются подменю, вызываются выпадающие меню, подтверждается текущее значение.
ESC	Выход	«ESC» обеспечивает возвращение с любого поля. Ее нажатие отменяет нажатие «Enter». Если клавиша «ESC» нажата во время редактирования настроек, произойдет возврат в предыдущее меню. При нажатии «ESC» в главном меню появляется сообщение о подтверждении выхода и отмены всех изменений, произведенных пользователем.
↑	Выбор элемента	Клавиша «Вверх» используется для выбора предыдущего значения в списке. Для активации служит «Enter».
↓	Выбор элемента	Клавиша «Вниз» используется для выбора следующего значения в списке. Для активации служит «Enter».
<—>	Выбор меню	Клавиши «Вправо» и «Влево» используются для перемещения между страницами основного меню.
TAB	Выбор поля	Используется для перемещения между полями.
PgDown	Изменить значение	Используется для изменения значения текущего поля на предыдущее в списке.
PgUp	Изменить значение	Используется для изменения значения текущего поля на следующее в списке.
F1	Вызов страницы помощи	Нажатие «F1» отобразит окно общей помощи.
F2	Возврат к предыдущему значению	Нажатие «F2» вернет предыдущее значение опции.

Клавиша	Функция	Описание
F3	Установка оптимальных по умолчанию параметров	Нажатие «F3» установит оптимальные по умолчанию параметры.
F4	Сохранить и выйти	Нажатие «F4» вызовет сохранение текущих настроек, произведенных пользователем, затем произойдет выход из утилиты настройки с последующей перезагрузкой.

Для изменения параметров необходимо:

1) Выбрать нужный параметр (рис. 3.1);

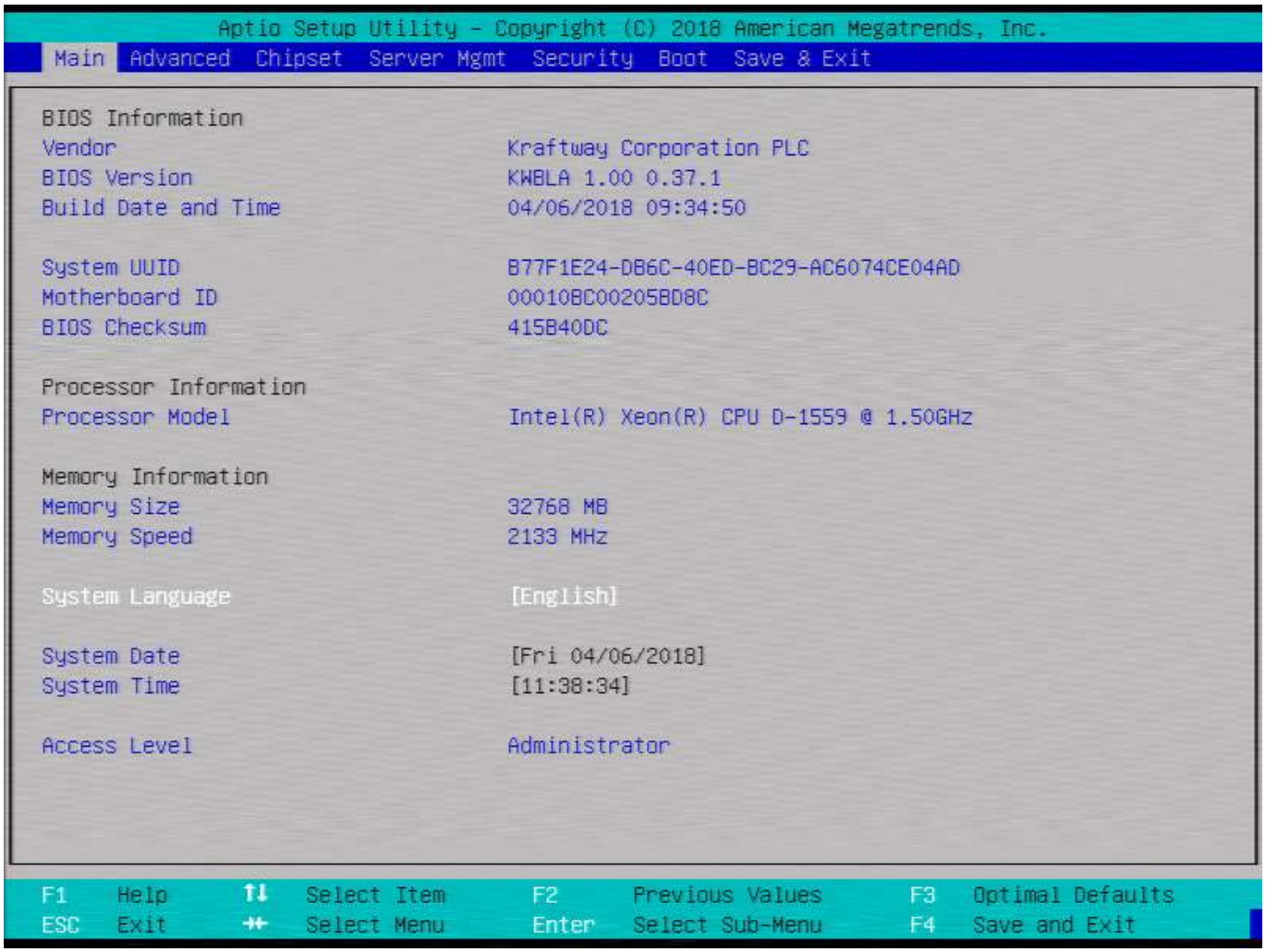

Рис. 3.1

2) *Выполнить*, после выполнения данного действия, откроется подменю с возможными параметрами (рис. 3.2);

Рис. 3.2

3) Выбрать необходимый параметр;
4) *Выполнить*, после выполнения данного действия параметр будет изменен.

Примечание. Некоторые параметры имеют значения, которые необходимо задавать самостоятельно (например: «системная дата»), в таких случаях, необходимо вводить значения с клавиатуры или пользоваться клавишами изменения значения.

3.1.1. Вход в интерфейс

Вход в интерфейс следует осуществлять после включения, или перезагрузки устройства путем нажатия клавиш.

Клавиши, которые используются для входа в BIOS чаще всего:

- DELETE;
- F10;
- F11;
- F12;
- F1;
- F2;
- F3;
- Esc.

3.1.2. Главное меню

Главное меню выводится на экран при запуске ПО БСВВ ВСМ-МВ автоматически по умолчанию. В данном разделе доступна информация о ПО БСВВ ВСМ-МВ и возможность осуществить выбор языка интерфейса и установку текущей даты и времени (рис. 3.3).

Рис. 3.3

Предоставляемая информация:

– *Изготовитель* – производитель BIOS;

– *Версия BIOS* – версия BIOS;

– *Дата и время сборки BIOS* – дата и время создания;

– *Идентификатор системы* – информация о идентификаторе системы;

– *Идентификатор материнской платы* – информация о идентификаторе материнской платы;

– *Контрольная сумма BIOS* – информация о контрольной сумме BIOS;

– *Модель процессора* – информация о процессоре;

– *Объем памяти* и *Частота памяти* – информация об оперативной памяти;

– *Уровень доступа* – уровень доступа к настройкам BIOS.

Изменяемые параметры:

– *Язык системы* – язык, используемый в интерфейсе программы;

– *Системная дата* – дата, используемая программой в качестве текущей;

– *Системное время* – время, используемое программой в качестве текущего.

3.1.3. Раздел меню «Настройки»

Раздел меню «Настройки» позволяет настраивать следующие функции (рис. 3.4):

– *ACPI и управление питанием* – настройка параметров ACPI и управление электропитанием (п. 3.1.3.1);

– *Последовательные порты* – настройка параметров последовательных портов (п. 3.1.3.2);

– *Настройка протокола IP в UEFI* – настройка параметров протокола IP в UEFI (п. 3.1.3.3);

– *Настройка модуля совместимости* – настройка модуля совместимости: включить/отключить, порядок выполнения модулей расширения (п. 3.1.3.4);

– *Настройка параметров USB* – настройка параметров работы портов USB (п. 3.1.3.5);

– *LSI SAS3 MPT Controller SAS3008* – настройка параметров RAID-контроллера;

– *Intel (R) Ethernet Connection X552 10 Gbe Backplane* – настройка сетевого адаптера;

– *Intel (R) 10 Gigabit Network Connection* – настройка сетевых параметров;

– *Intel (R) IP10 Gigabit Network Connection* – настройка сетевых параметров.

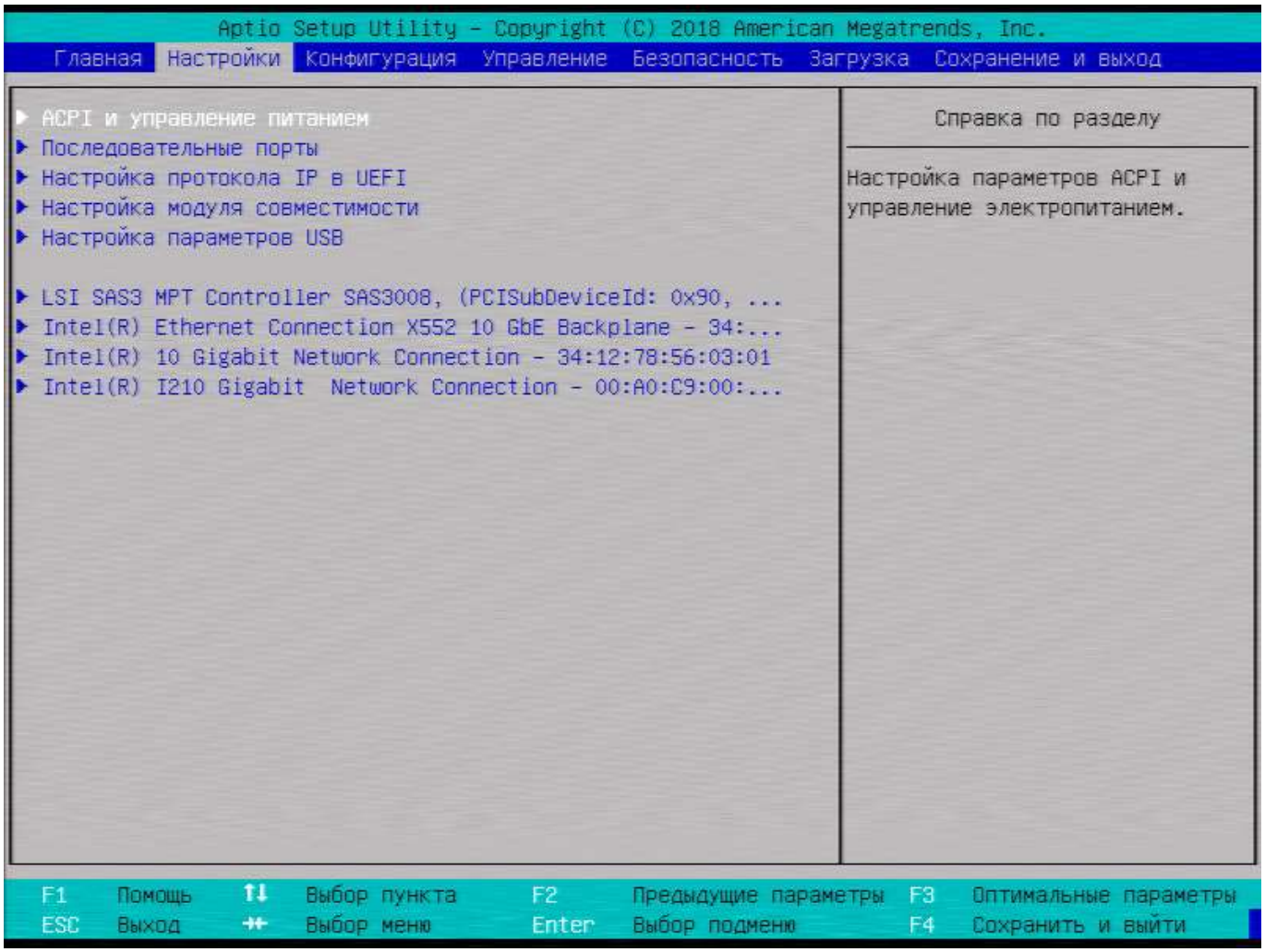

Рис. 3.4

3.1.3.1. Настройки ACPI и управление питанием

Функция меню «Настройки ACPI и управление питанием» позволяет настраивать следующие параметры (рис. 3.5):

– *Разрешить автонастройку ACPI* – включает/выключает автонастройку ACPI;

– *Разрешить гибернацию* – включает/отключает возможность гибернации системы (состояние ACPI S4);

– *Блокировка наследуемых ресурсов* – включает/отключает блокировку наследуемых ресурсов.

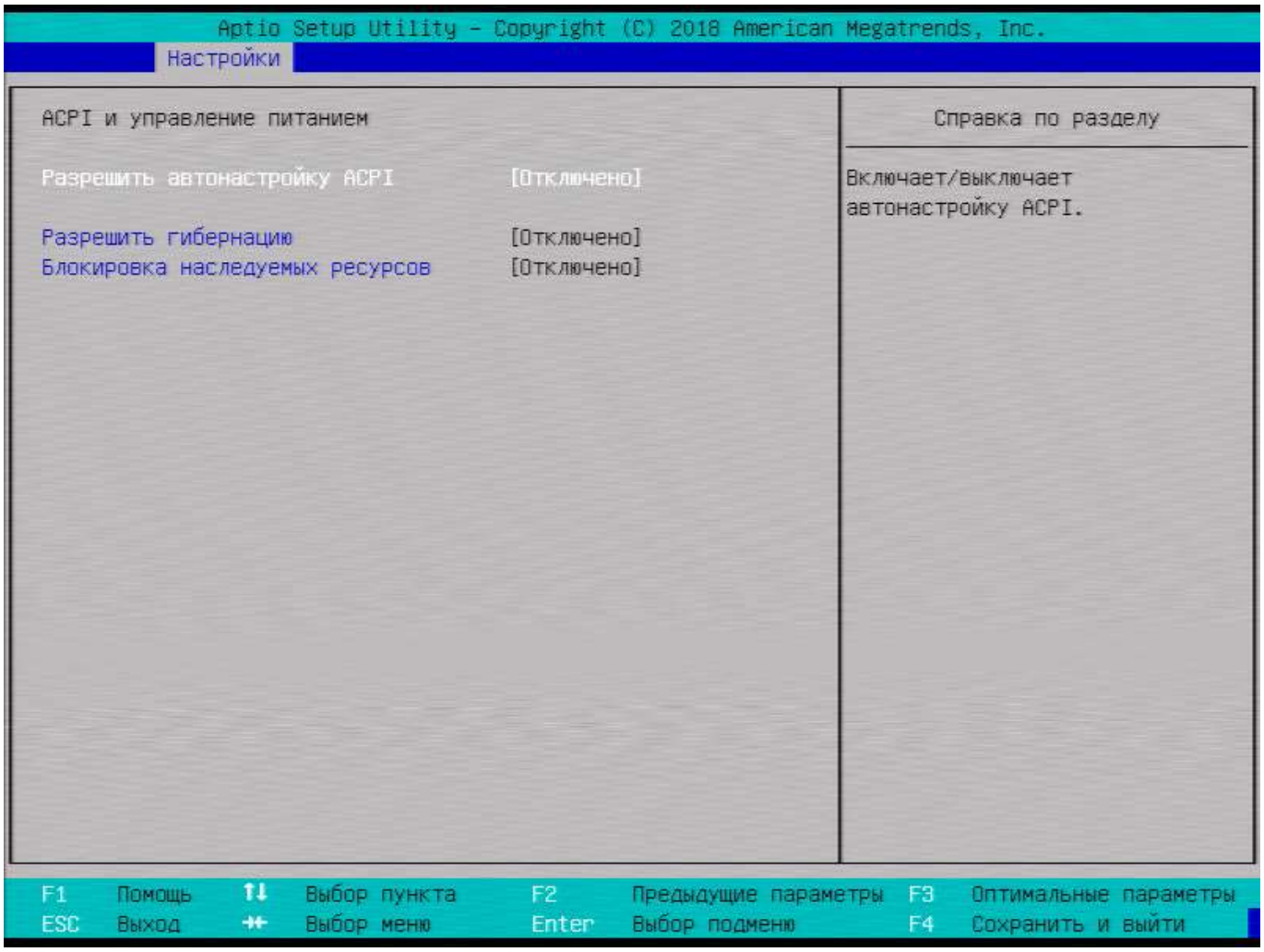

Рис. 3.5

3.1.3.2. Настройка последовательных портов

Функция меню «Последовательные порты» позволяет настроить следующие параметры (рис. 3.6):

– *Последовательный порт 1* – установка параметров последовательного порта 1 (COM1);

– *Последовательный порт 2* – установка параметров последовательного порта 2 (COM2).

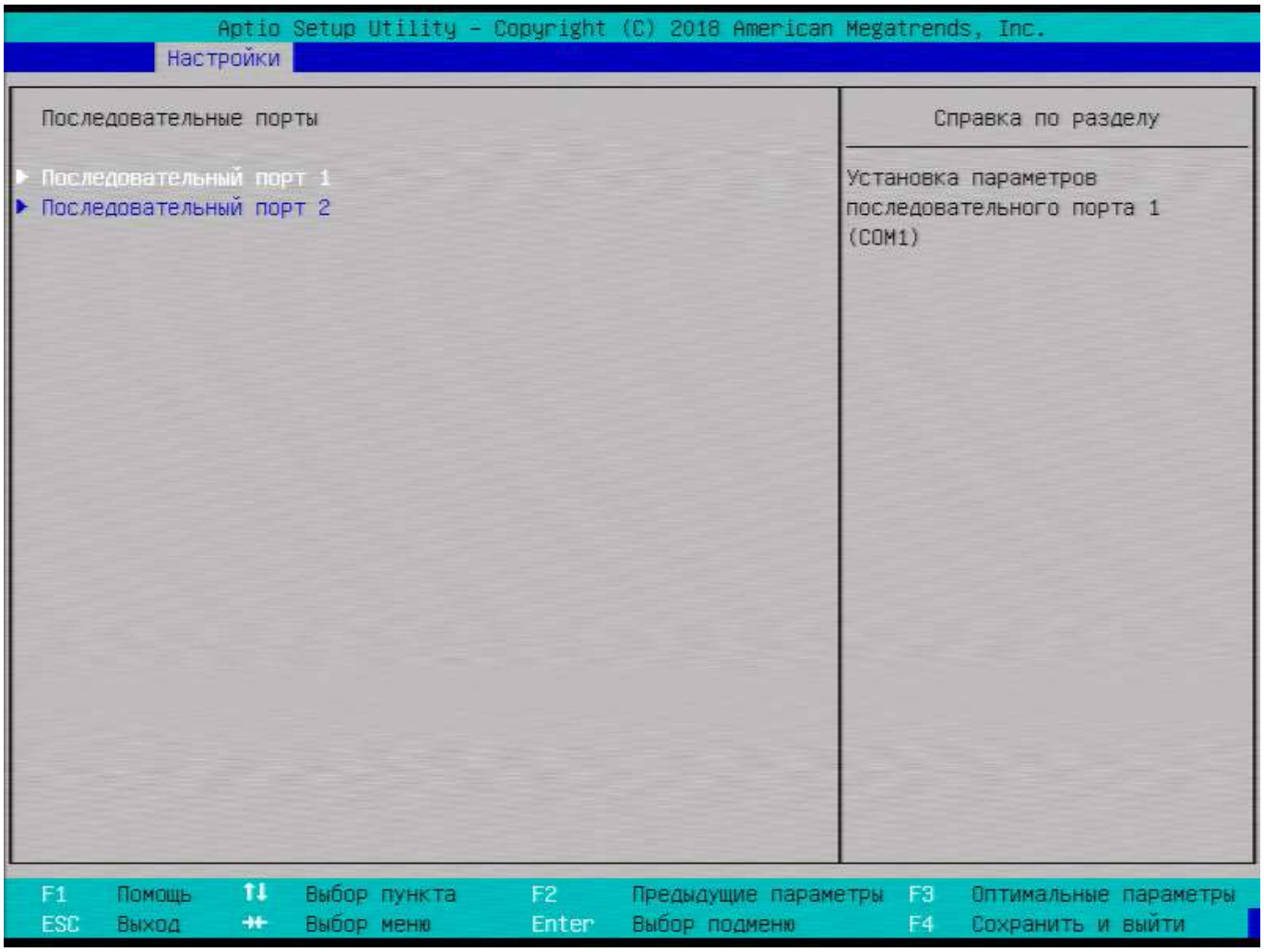
Aptio Setup Utility – Copyright (C) 2018 American Megatrends, Inc.
Настройки
Последовательные порты
Последовательный порт 1
Последовательный порт 2
Справка по разделу
Установка параметров последовательного порта 1 (COM1)
F1 Помощь
ESC Выход
Выбор пункта
Выбор меню
F2 Предыдущие параметры
Enter Выбор подменю
F3 Оптимальные параметры
F4 Сохранить и выйти

Рис. 3.6

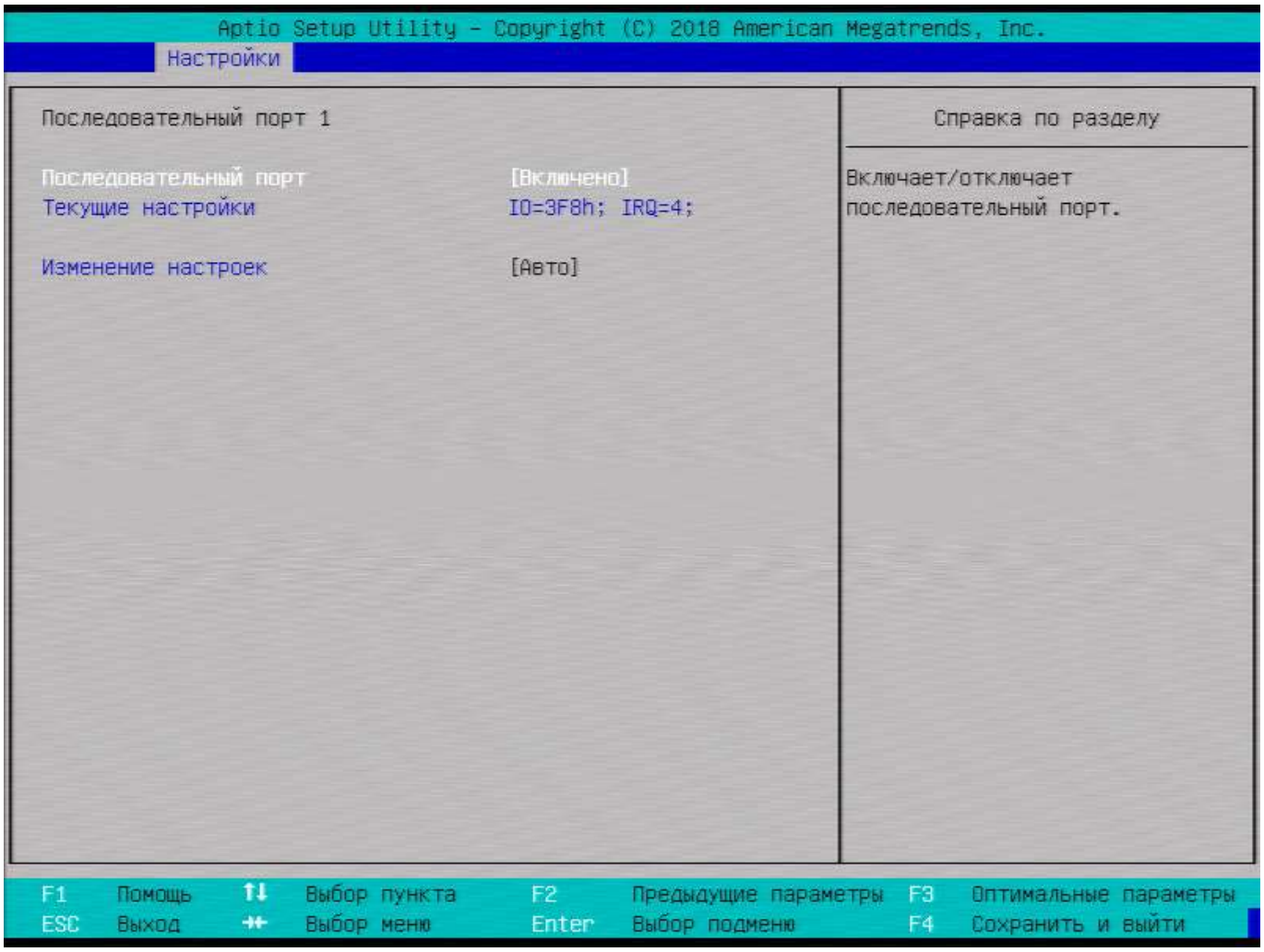

Рис. 3.7

Функция меню «Последовательный порт 1» позволяет просмотреть текущие настройки и настроить следующие параметры последовательного порта 1 (рис. 3.7):

– *Последовательный порт* – включает или отключает последовательный порт;

– *Изменение настроек* – установка параметров последовательного порта 1 (COM1).

Примечание. Настройка последовательного порта 2 выполняется аналогично настройке последовательного порта 1.

3.1.3.3. Настройка протокола IP в UEFI

Функция меню «Настройка протокола IP в UEFI» позволяет настраивать следующий параметр (рис. 3.8, 3.9):

– *Поддержка протокола IP* – включает/отключает поддержку протокола IP в UEFI;

Примечание. По умолчанию поддержка протокола IP в UEFI отключена (рекомендуемое значение).

– *PXE для IPv4* – включает возможность загрузки по PXE для IPv4;

– *Задержка загрузки по PXE* – устанавливает время ожидания (в секундах) до прерывания загрузки по PXE;

– *Обнаруживать подключение* – количество попыток, в течение которых будет происходить обнаружение физического подключения по сетевому интерфейсу.

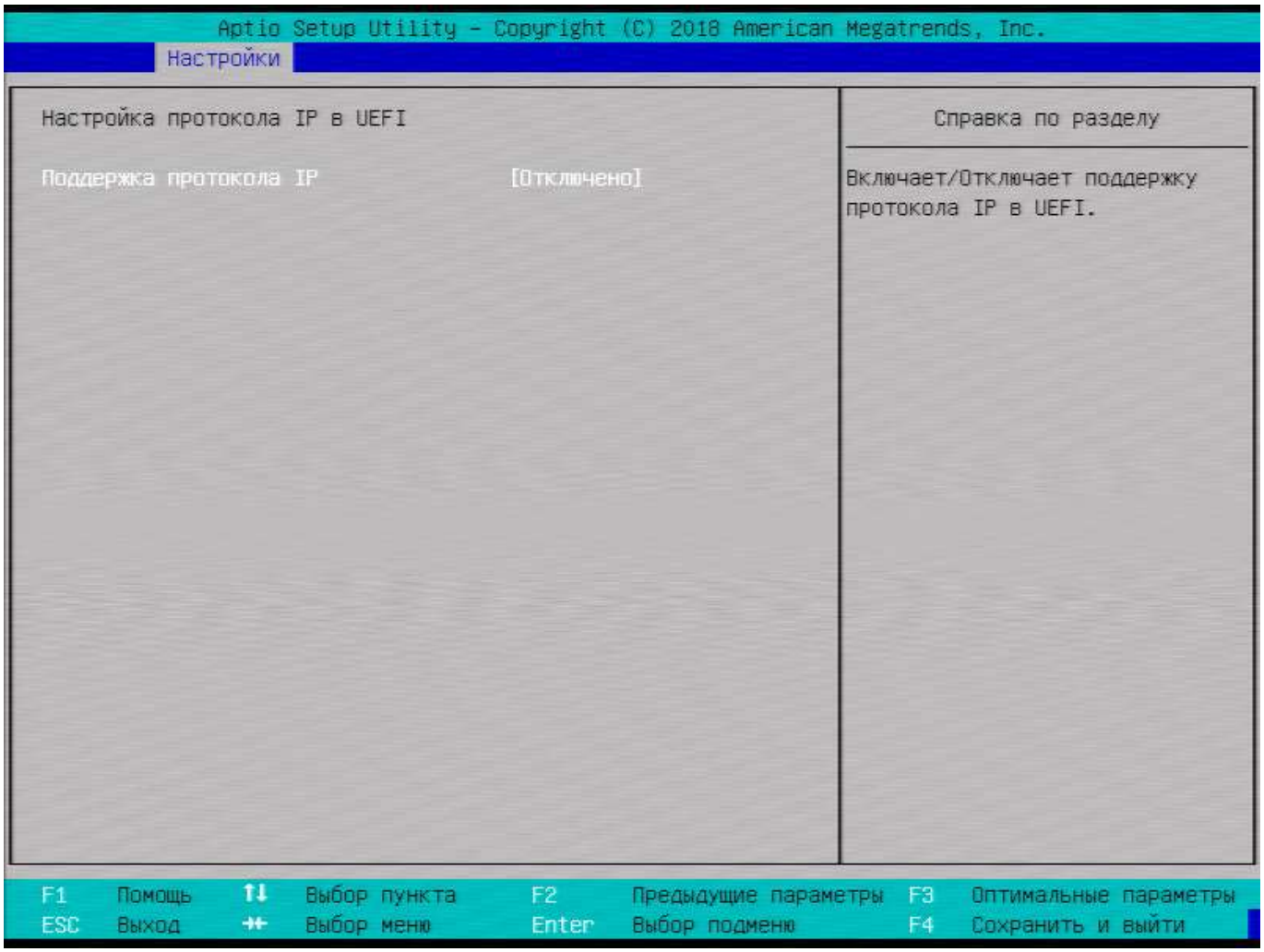

Рис. 3.8

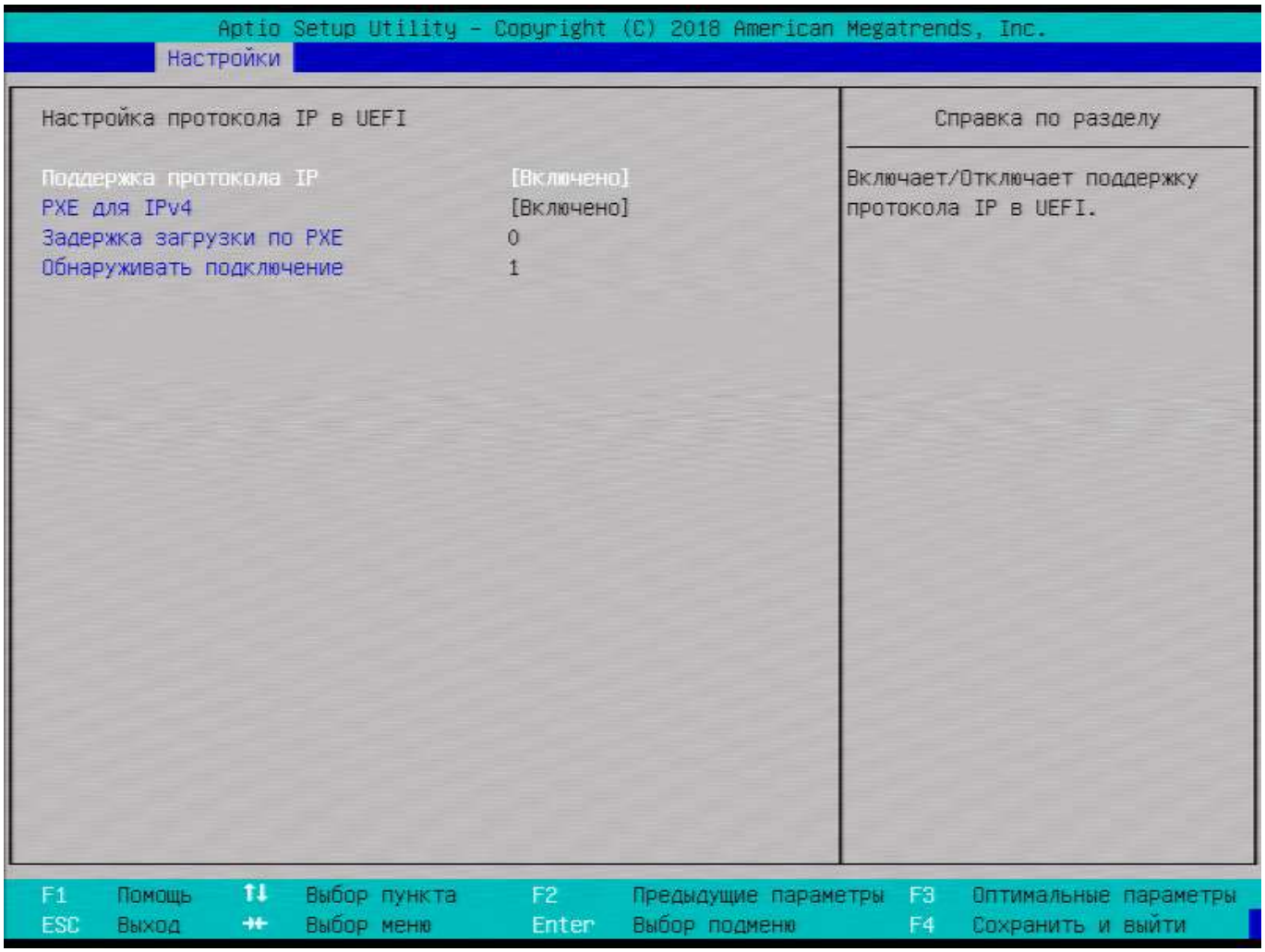

Рис. 3.9

3.1.3.4. Настройка модуля совместимости

Функция меню «Настройка модуля совместимости» выводит сведения о версии модуля совместимости и позволяет настраивать следующие параметры (рис. 3.10):

– *Поддержка модуля совместимости* – включить/выключить поддержку модуля совместимости;

– *Фильтр начальной загрузки* – определяет приоритет загрузки модулей расширения BIOS;

– *Выполнять расширение PXE* – задает правила выполнения модуля расширения PXE (OpROM);

– *Выполнять расширение Storage* – задает правила выполнения модуля расширения подсистемы хранения (OpROM);

– *Выполнять расширение Видео* – задает правила выполнения модуля расширения видео (OpROM).

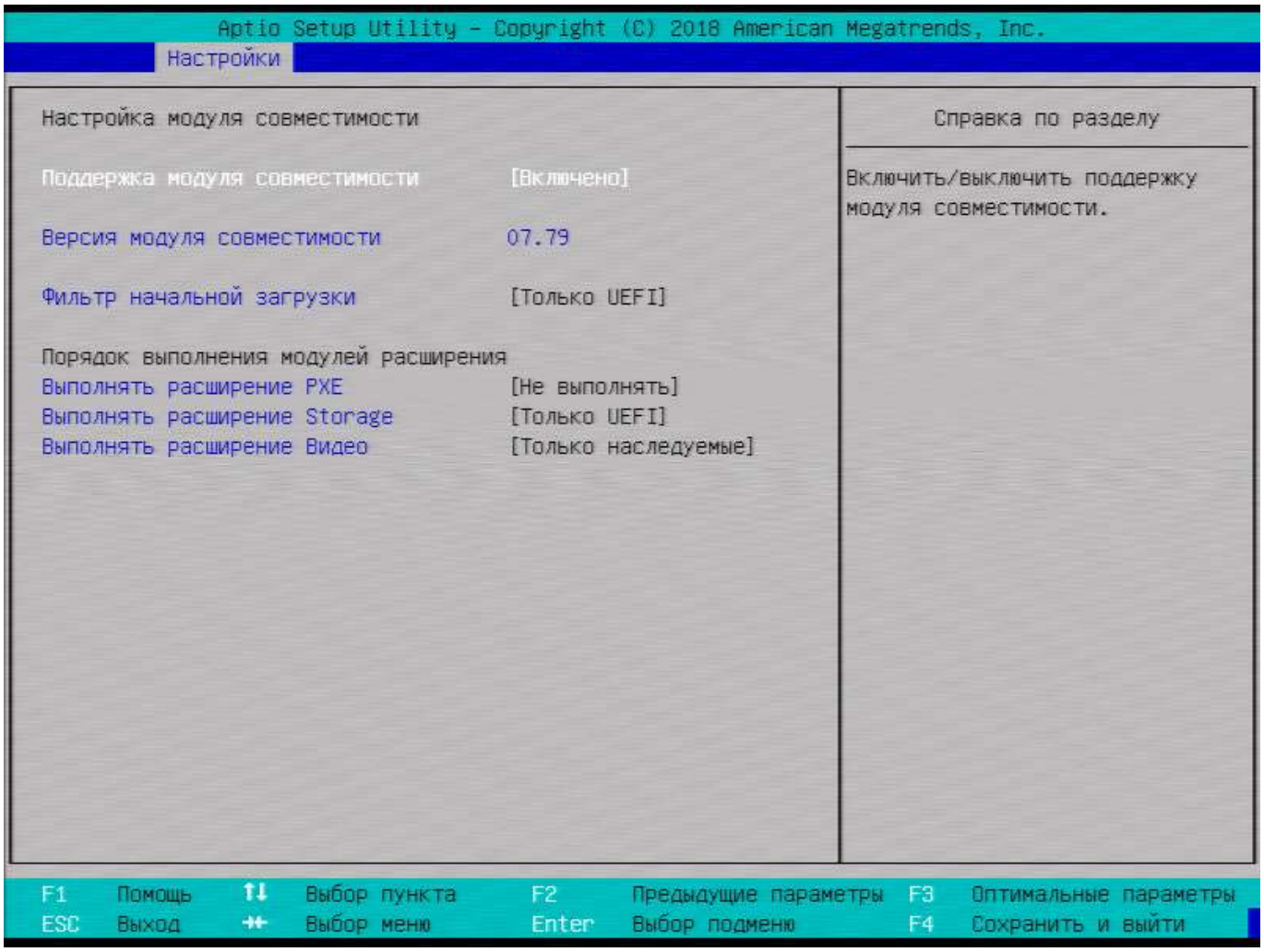

Рис. 3.10

3.1.3.5. Настройка параметров USB

Функция меню «Настройки параметров USB» позволяет просмотреть информацию об обнаруженных USB устройствах и настраивать следующие параметры (рис. 3.11):

– *Поддержка наследуемого USB* – параметр АВТО отключает поддержку наследуемого USB, если отсутствуют любые подключенные USB устройства;

– *Передача управления EHCI* – вспомогательная процедура для операционных систем без возможности передачи управления другому устройству EHCI. Смену владельца EHCI должен инициировать контроллер EHCI;

– *Поддержка накопителей USB* – включает/отключает поддержку накопителей USB;

– *Эмуляция порта 60/64* – необходимо включить данный параметр, чтобы использовать USB клавиатуру в операционных системах без поддержки USB;

– *Эмуляция работы накопителей* – режим работы накопителей USB. АВТО – присваивает устройству тип, в соответствии с форматом носителя, оптическим устройствам присваивается тип CDROM, устройствам без носителей присваивается тип, в соответствии с типом самого устройства.

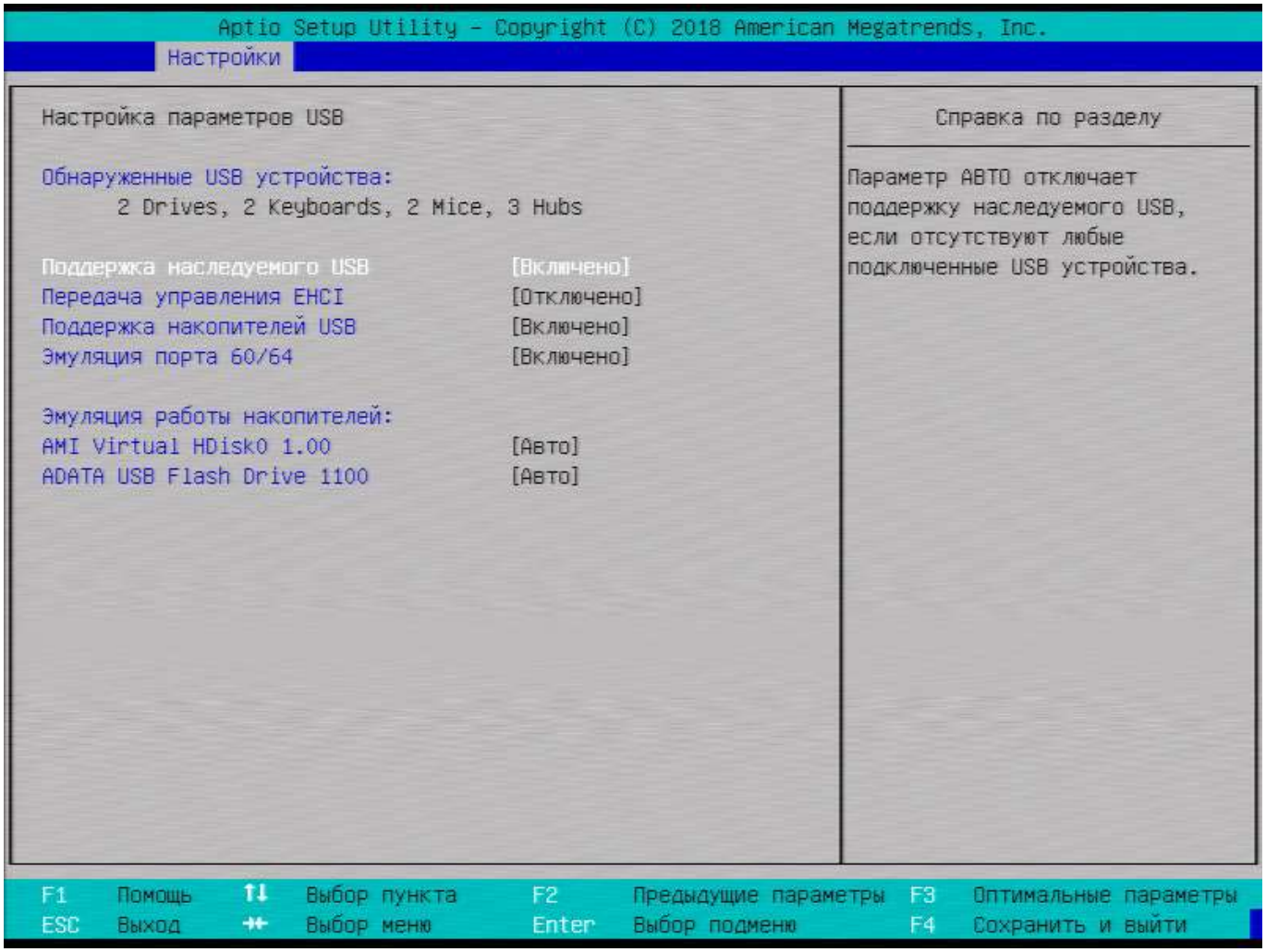

Рис. 3.11

3.1.4. Раздел меню «Конфигурация»

Раздел меню «Конфигурация» позволяет настраивать следующие функции (рис. 3.12):

– *Настройка параметров процессора* – отображение характеристик и изменение параметров процессора (п. 3.1.4.1);

– *Энергопотребление процессора* – настройка для управления потребляемой мощностью и производительностью (п. 3.1.4.2);

– *Виртуализация прямого В/В* – настройка технологии Intel VD для виртуализации прямого ввода/вывода (VT-d) (п.3.1.4.3);

– *Восстановление питания после сбоя* – определяет поведение системы после сбоя электропитания (п. 3.1.4.4).

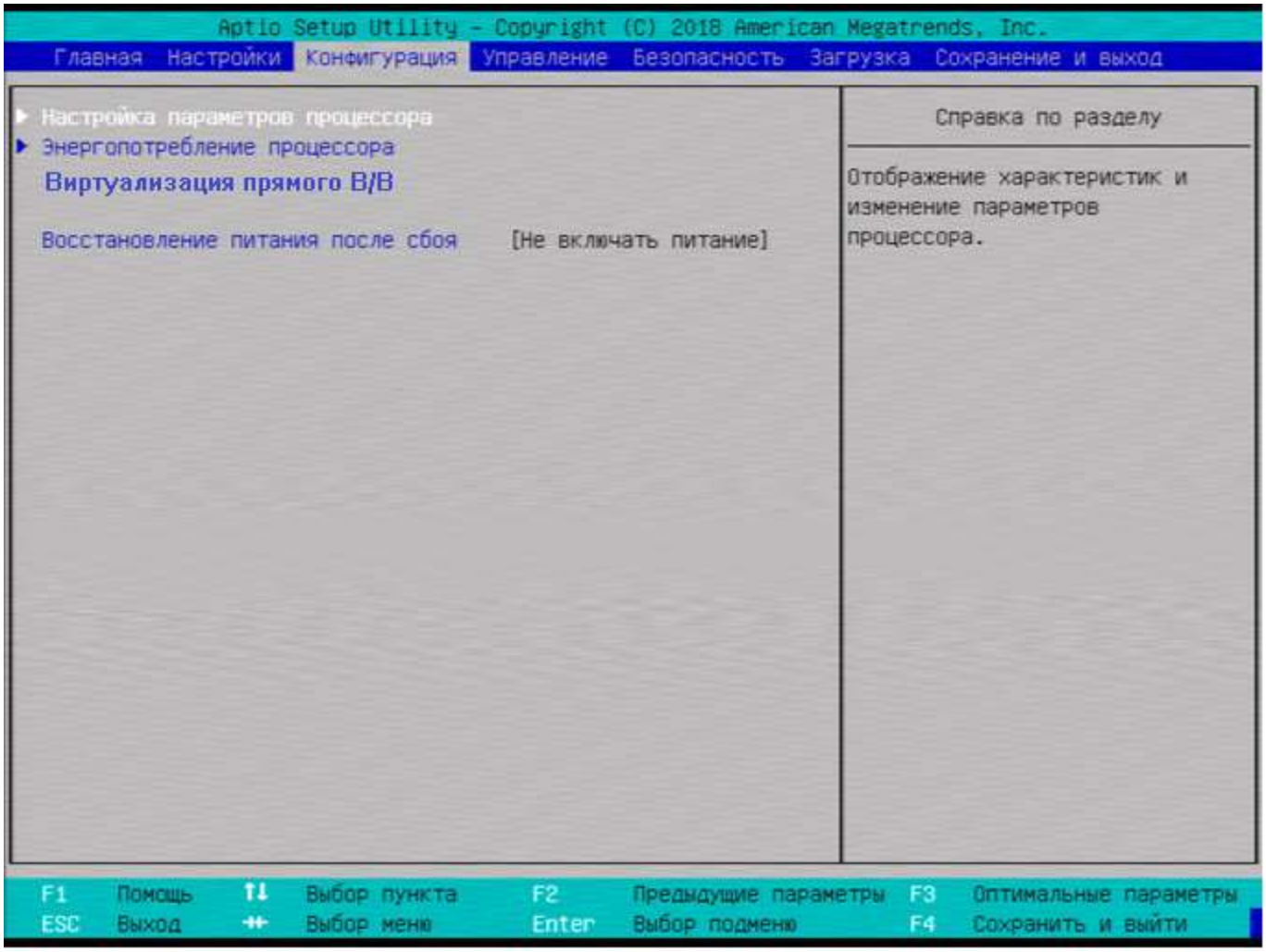

Рис. 3.12

3.1.4.1. Настройка параметров процессора

Функция меню «Настройка параметров процессора» позволяет просматривать характеристики и настраивать параметры процессора (рис. 3.13):

– *Технология Hyper-Threading* – включает/отключает технологию Intel Hyper-Threading;

– *Контроль простоя* – включает/отключает управление энергопотреблением неактивного состояния (Monitor Mwait);

– *Запрет выполнения* – технология Execute Disable Bit может предотвратить некоторые виды атак по переполнению буфера;

– *Аппаратная виртуализация* – включает/отключает поддержку аппаратной виртуализации;

– *Поддержка SMX* – включает/отключает поддержку дополнительных инструкций процессора Safer Mode Extensions;

– *Аппаратная предвыборка* – включает/отключает механизм аппаратной предвыборки данных из памяти;

– *Предвыборка смежных строк* – включает/отключает механизм аппаратной предвыборки данных двух смежных строк кэша;

– *Расширенный APIC* – включает/выключает поддержку расширенного APIC;

– *AES-NI* – включает/отключает поддержку набора команд шифрования.

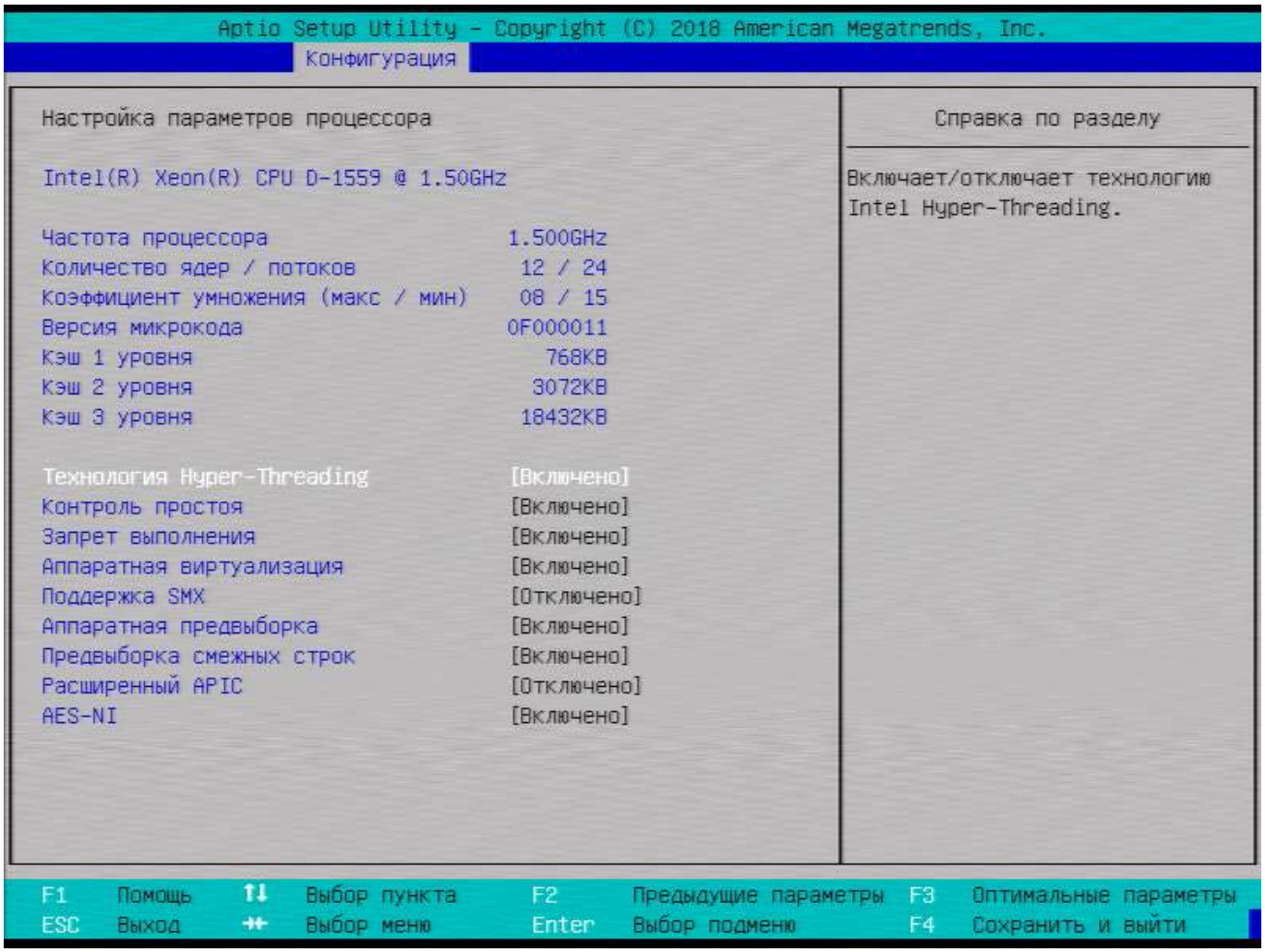

Рис. 3.13

3.1.4.2. Энергопотребление процессора

Функция меню «Энергопотребление процессора» позволяет настраивать следующие параметры (рис. 3.14):

– *EIST (P-состояния)* – если включено, позволяет операционной системе регулировать частоту процессора согласно нагрузке. Если включено, то процессор всегда работает на максимальной частоте;

– *Управляемый TDP* – включает/выключает ограничение максимального энергопотребления. Зависит от используемой операционной системы;

– *Максимальная частота ядра* – ограничение максимальной частоты ядра процессора;

– *P-состояния процессора* – управление частотой процессора;

– *C-состояния процессора* – конфигурирование режима простоя процессора;

– *T-состояния процессора* – конфигурирование режима тротлинга процессора;

– *Контроль температуры процессора* – управление температурой процессора и поведением системы в случае перегрева.

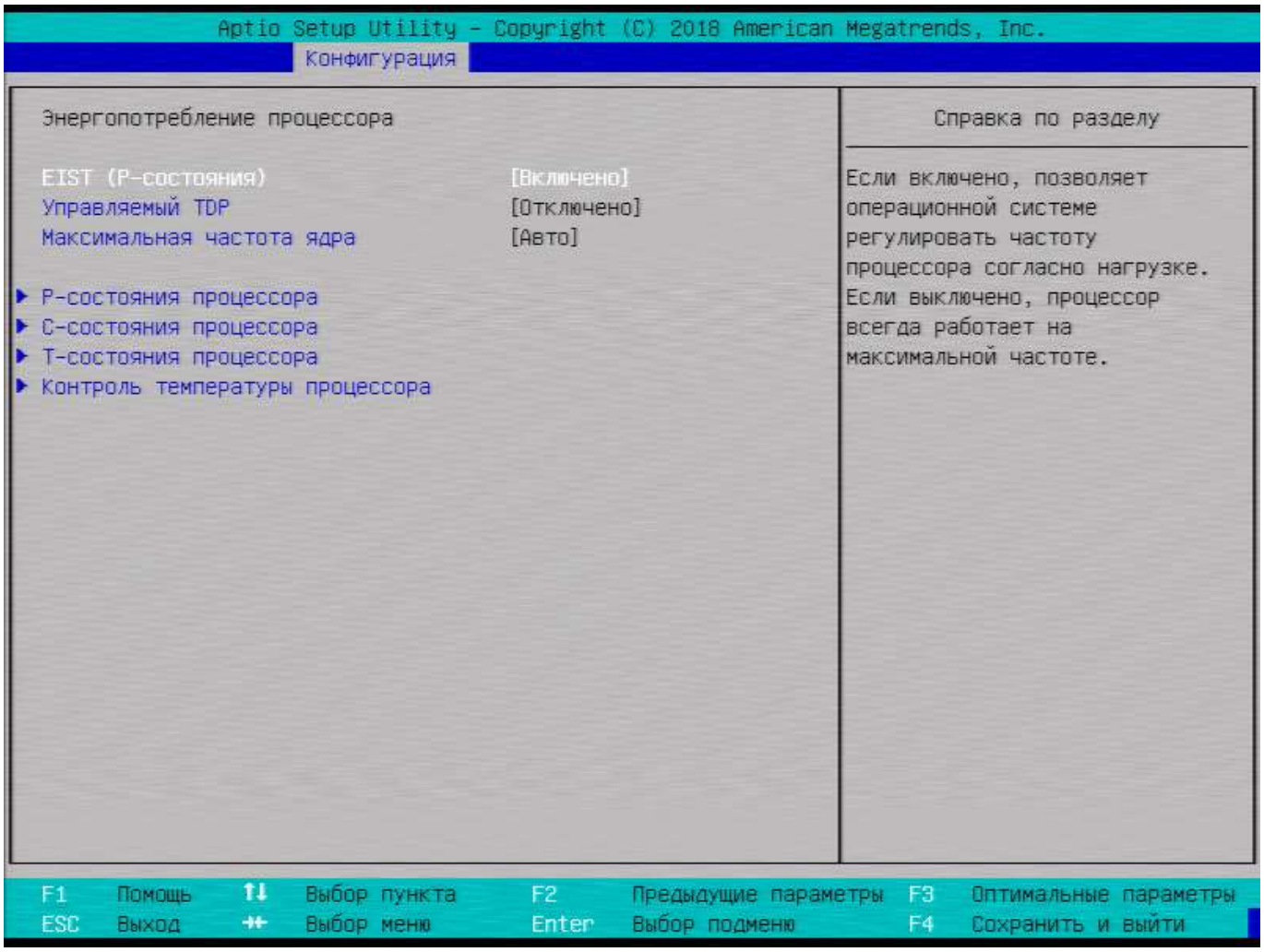

Рис. 3.14

3.1.4.3. Виртуализация прямого В/В

Функция меню «Виртуализация прямого В/В» позволяет настраивать следующие параметры:

– *Виртуализация прямого В/В* – настройка технологии Intel VD для виртуализации прямого ввода/вывода (VT-d);

– *ACS Control* – включено: поддержка виртуальной функция контроля доступа (ACS) только для корневых портов чипсетов PCIe; выключено: поддержка ACS для всех мостов PCIe;

– *Перенаправление прерываний* – включает/отключает аппаратную возможность перенаправления и маршрутизации прерываний в виртуальных средах

– *Когерентность (Non-Isoch)* – включает/отключает аппаратную поддержку синхронизации настроек и параметров между процессорами и устройствами;

– *Когерентность (Isoch)* – включает/отключает аппаратную поддержку синхронизации настроек и параметров между процессорами и устройствами;

3.1.4.4. Восстановление питания после сбоя

Функция меню «Восстановление питания после сбоя» позволяет настраивать следующие параметры:

– *Восстановление питания после сбоя* – определяет поведение системы после сбоя электропитания.

3.1.5. Раздел меню «Управление»

Раздел меню «Управление» позволяет просматривать информацию о BMC и настраивать следующие функции (рис. 3.15):

– *Поддержка BMC* – включает/выключает поддержку BMC;

– *Ожидать готовности BMC* – ожидать ответа от BMC. Время инициализации BMC составляет примерно 40 секунд;

– *Время ожидания готовности BMC* – время, в течение которого BIOS будет ждать перед отправкой первой команды в BMC, если FW еще не проинициализировано;

– *Сторожевой таймер OS* – при включении запускает таймер, который возможно отключить после загрузки ОС. Если ОС не удалось загрузить, дальнейшее поведение системы определяется политикой сторожевого таймера;

– *Период срабатывания таймера* – задает значение таймера;

– *Правила срабатывания таймера OS* – определяет правила поведения системы после срабатывания сторожевого таймера;

– *Журнал событий* – настройка журнала системных событий (п. 3.1.5.1);

– *Настройка сети BMC* – настройка сетевых параметров BMC для удаленного управления (п. 3.1.5.2);

– *Перезапуск BMC* – принудительный перезапуск BMC.

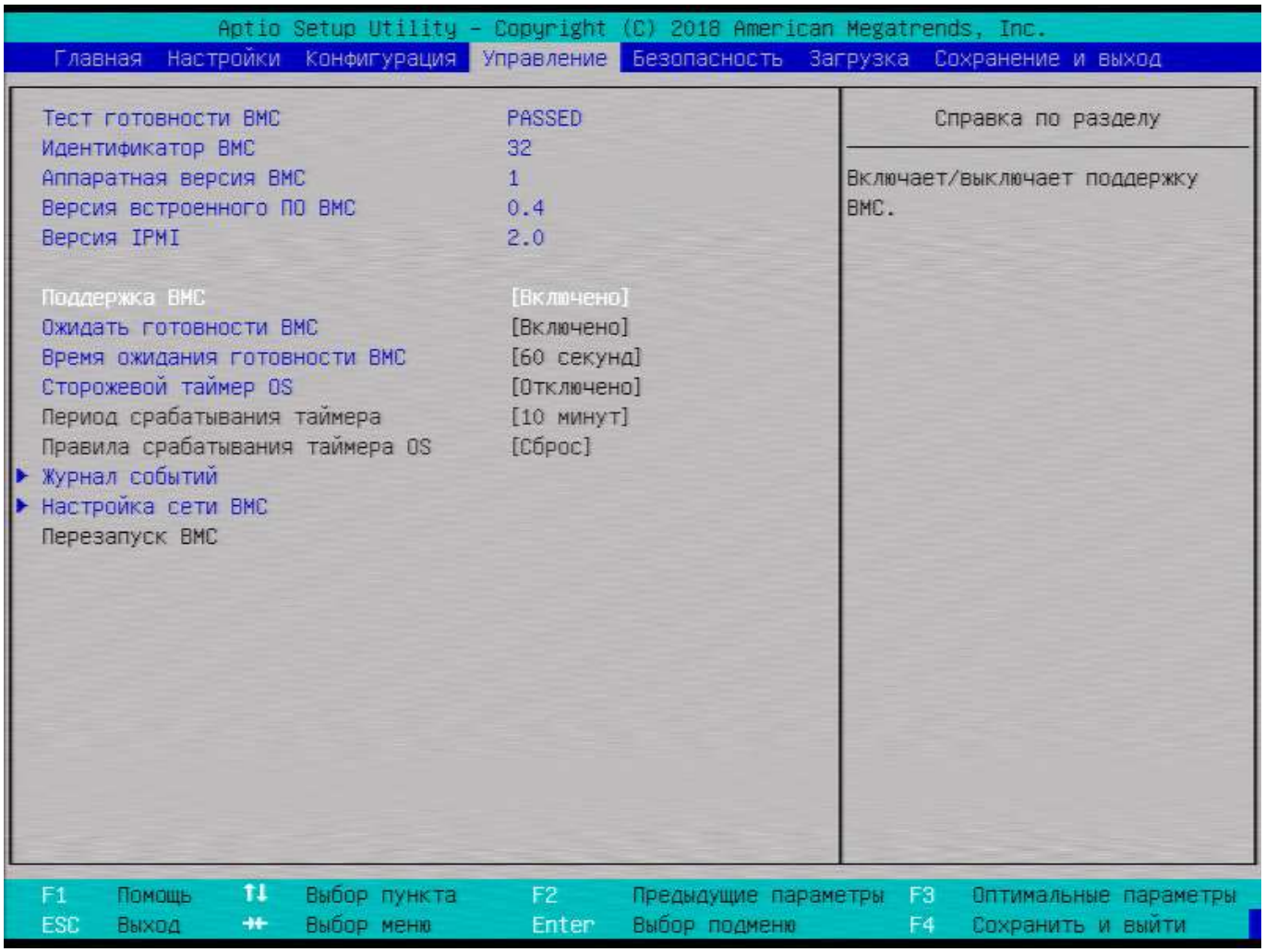

Рис. 3.15

3.1.5.1. Журнал событий

Функция меню «Журнал событий» позволяет настраивать следующие параметры (рис. 3.16):

– *Поддержка журнала* – включает/отключает возможность настройки записи системных событий в процессе загрузки;

– *Очистить журнал* – варианты очистки журнала событий;

– *Когда журнал переполнен* – варианты поведения при переполнении системного журнала событий;

– *Занесение EFI событий* – варианты записи в журнал событий EFI кодов.

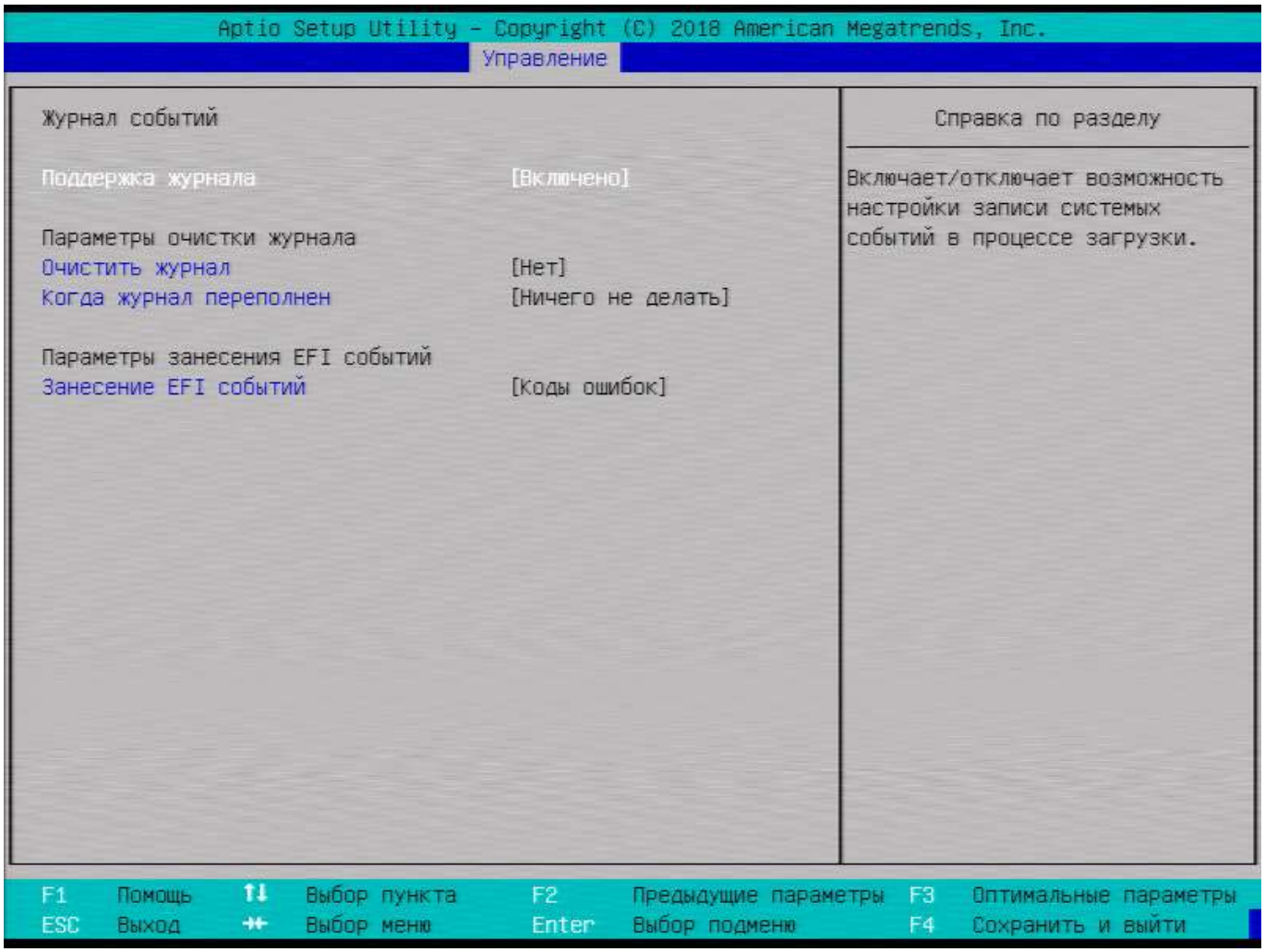

Рис. 3.16

3.1.5.2. Настройка сети BMC

Функция меню «Настройка сети BMC» позволяет просматривать информацию о сетевых параметрах и настраивать следующий параметр (рис. 3.17):

– *Тип получения IP адреса* – настройка параметров сетевого соединения BMC контроллера.

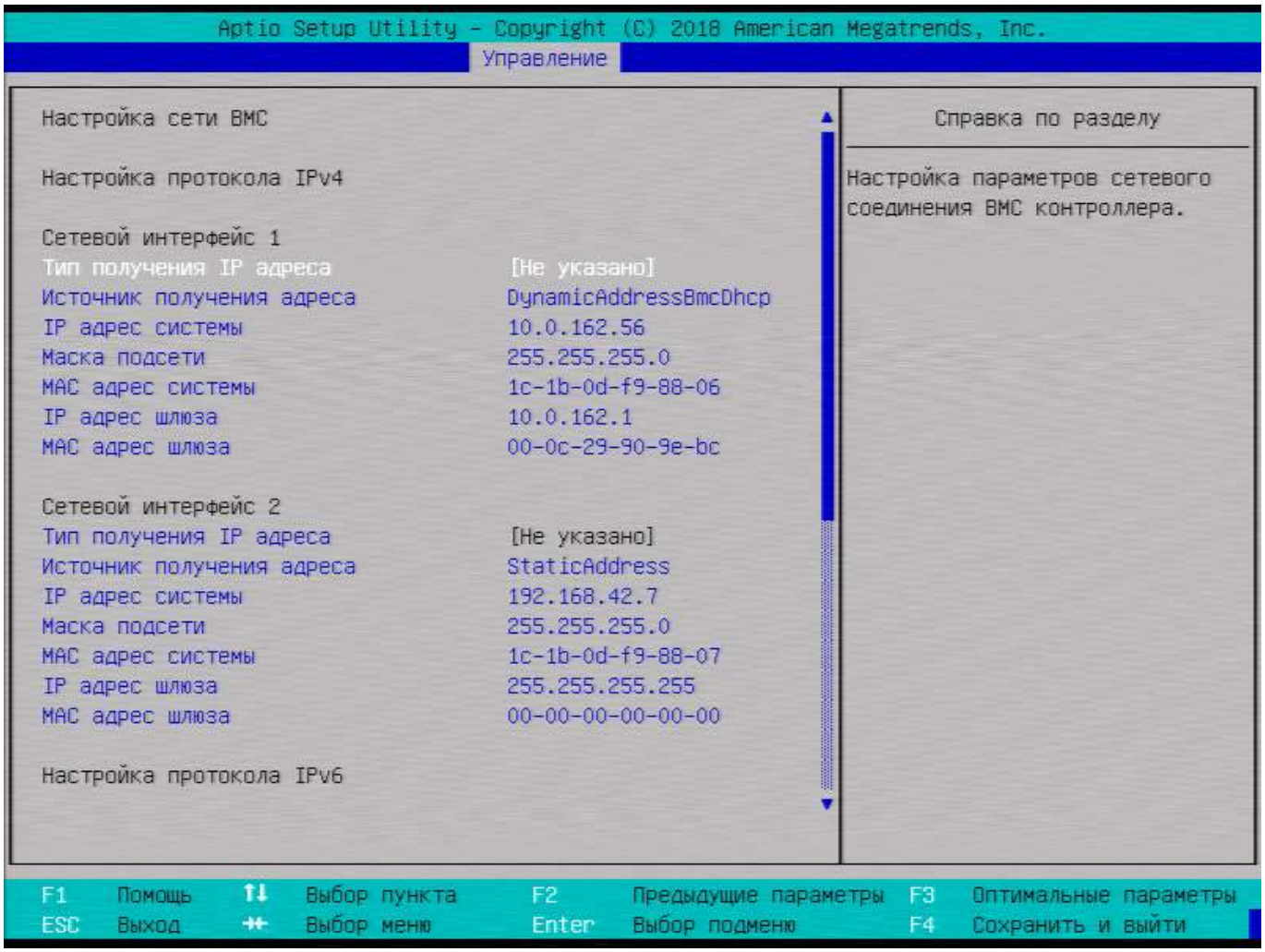

Рис. 3.17

3.1.6. Раздел меню «Безопасность»

Раздел меню «Безопасность» (рис. 3.18) позволяет:

– *Пароль администратора* – если задан только пароль администратора, доступ будет ограничен только в настройки BIOS, а пароль будет запрашиваться только при попытке зайти в настройки BIOS;

– *Пароль пользователя* – если задан только пароль пользователя, его необходимо будет вводить в процессе загрузки и при попытке зайти в настройки BIOS. В настройках BIOS пользователь будет иметь права администратора;

– *Удалить модули поддержки локальной сети* – удаляет из BIOS все модули поддержки работы с локальной сетью. После данной операции загрузка по сети будет невозможной;

– *Защита региона BIOS* – защита региона BIOS от записи. Активируется перед загрузкой;

– *Защита региона NVRAM* – защита региона NVRAM от записи. Активируется перед загрузкой;

– *Меню загрузки для Пользователя* – управляет возможностью использования меню загрузки Пользователем (см. п. 3.1.6.1);

– *Вход в BIOS Setup для Пользователя* – управляет возможностью входа в BIOS Setup Пользователем;

– *Загрузку с SATA CD/DVD* – управляет опцией загрузки с SATA CD/DVD привода;

– *Загрузка с USB устройств* – управляет опцией загрузки с USB устройств;

– *Безопасная загрузка* – настройка параметров безопасной загрузки (см. п. 3.1.6.2).

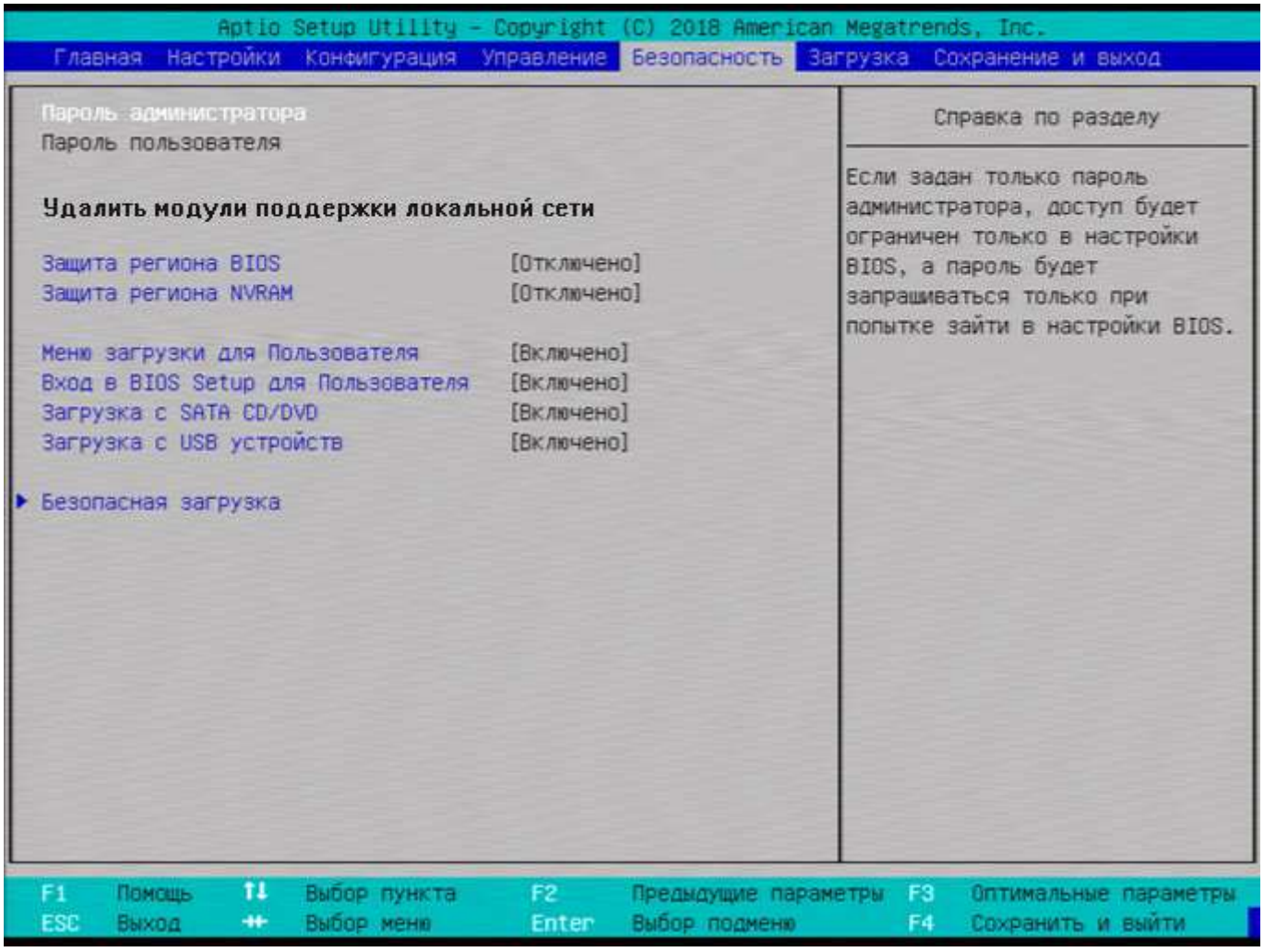

Рис. 3.18

Для задания паролей *Администратора* и *Пользователя* необходимо ввести и подтвердить пароль в открывшемся окне (рис. 3.19).

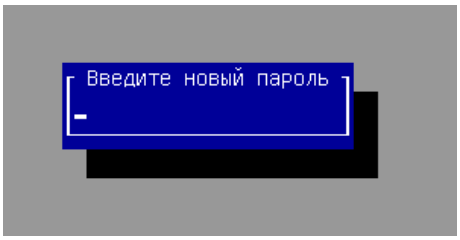

Рис. 3.19

Примечания:

1. Количество символов в пароле может принимать любое значение, в пределах допустимого интервала, заданного разработчиком. Границы данного интервала (от 3 до 20 символов) указаны в полях «Минимальное количество символов», «Максимальное количество символов», соответственно.

2. Если задан только пароль *Администратора*, то для оператора будет ограничен доступ только к настройкам BIOS, и пароль будет запрашиваться только при попытке зайти в настройки BIOS.

3. Если задан только пароль *Пользователя*, то платформа потребует от оператора ввести пароль в момент запуска. При положительном вводе пароля оператор сможет зайти в настройки BIOS. В этом случае, в настройках BIOS *Пользователь* будет иметь права *Администратора*.

4. При создании паролей *Администратора* и *Пользователя* оператор действует в рамках присвоенного *Уровня доступа* и установленных ограничений.

5. Пароль *Пользователя* должен отличаться от пароля *Администратора*.

6. Увидеть значение *Уровня доступа*, с которым оператор осуществил вход в BIOS можно в разделе меню «Главная» (рис. 3.3).

3.1.6.1. Меню загрузки для Пользователя

В разделе меню «Безопасность», при отключении *Меню загрузки для Пользователя,* происходит ограничение прав *Пользователя* на выбор загрузочного устройства, как в BIOS *Произвести загрузку с:* в разделе меню «Сохранение и выход», так и по горячей клавише F11.

При вызове меню загрузки, и попытке выбора и загрузки с другого устройства *Пользователю* выдается информационное окно «Загрузка компьютера остановлена» (рис. 3.20):

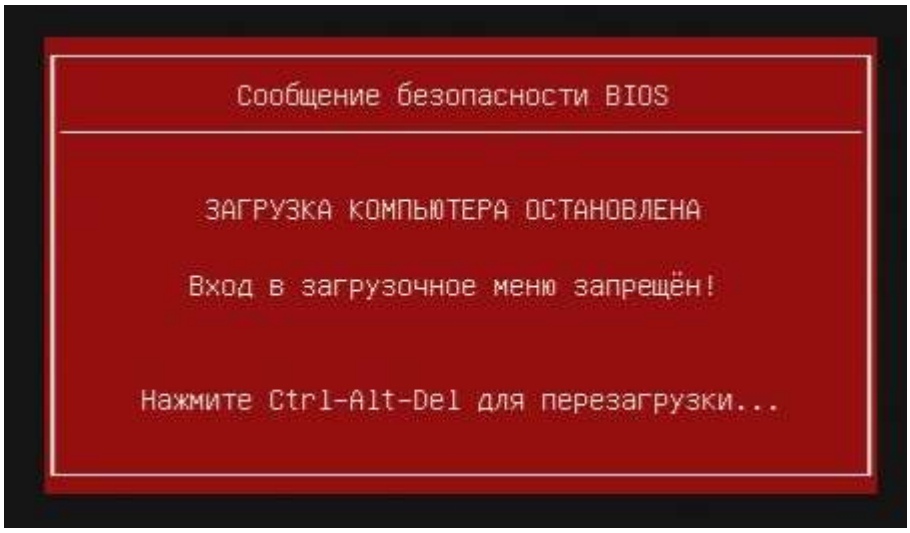

Рис. 3.20

При этом для *Пользователя* остается доступным выбор *Приоритеты загрузки* раздела меню «Загрузка».

Для полного ограничения *Пользователя* в выборе загрузочного устройства отключите *Вход в BIOS Setup для Пользователя*.

Примечание. Для того, чтобы ограничения для *Пользователя* вступили в силу, необходимо задать как пароль *Пользователя*, так и пароль *Администратора*.

3.1.6.2. Безопасная загрузка

Функция меню «Безопасная загрузка» позволяет настраивать следующие параметры (рис. 3.21):

– *Безопасная загрузка*:

1) осуществить безопасную загрузку возможно только при наличии ключа платформы (PK), а сама платформа должна работать в режиме пользователя;

2) режим совместимости должен быть отключен;

– *Режим безопасной загрузки* – выбор режима безопасной загрузки. НАСТРАИВАЕМЫЙ- позволяет более гибко изменять политику передачи управления дополнительными модулями расширения и управлять ключами безопасной загрузки;

– *Управление ключами* – позволяет гибко настраивать переменные безопасной загрузки.

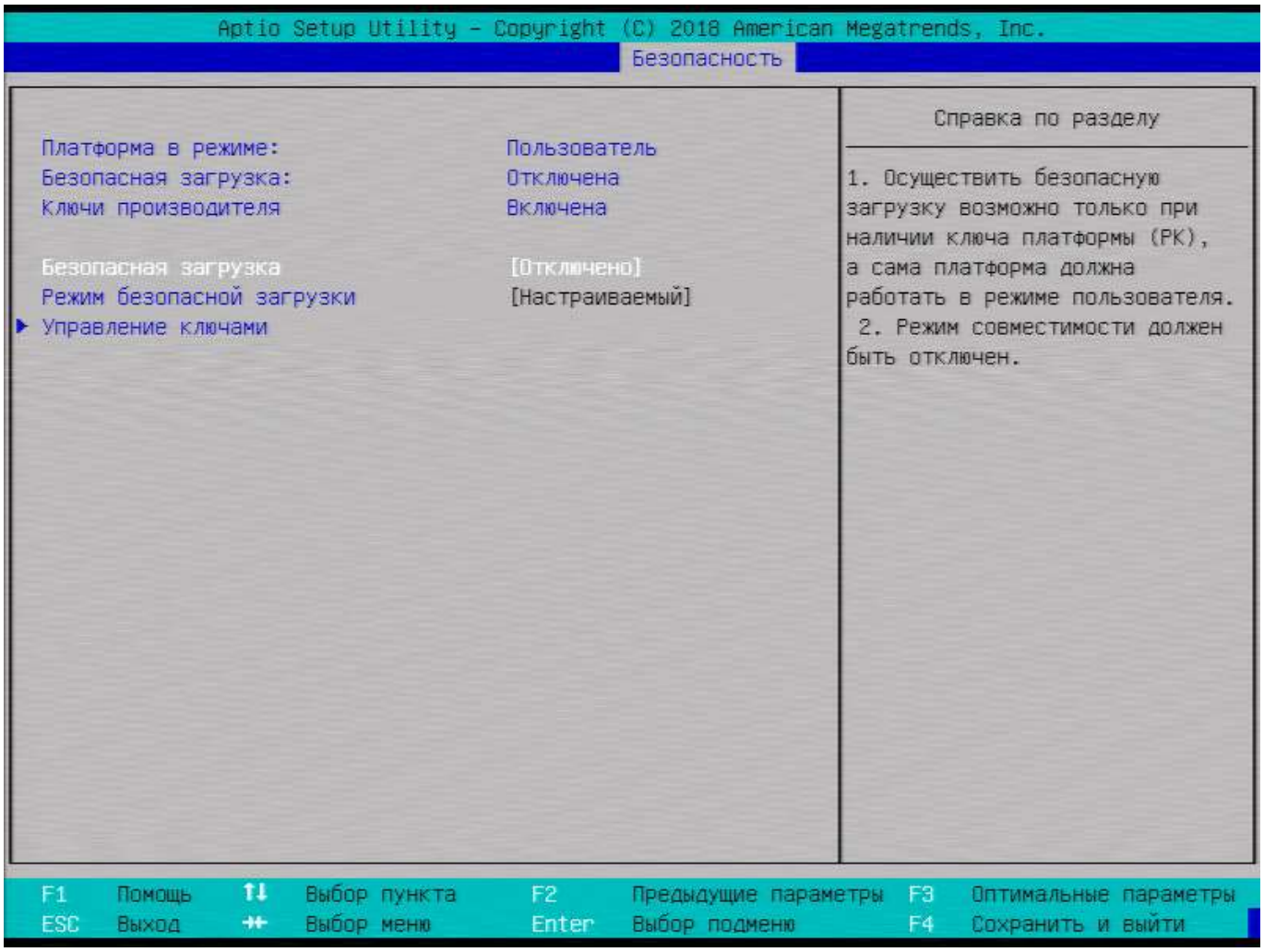

Рис. 3.21

3.1.7. Раздел меню «Загрузка»

Раздел меню «Загрузка» позволяет настраивать следующие функции (рис. 3.22):

– *Состояние Numlock при загрузке* – выбор состояния клавиши «Numlock» при загрузке;

– *Экранная заставка* – включает или отключает вывод на экран результатов начального тестирования системы;

– *1-й приоритет* – устанавливает приоритет загрузки с устройства;

– *2-й приоритет* – устанавливает приоритет загрузки с устройства.

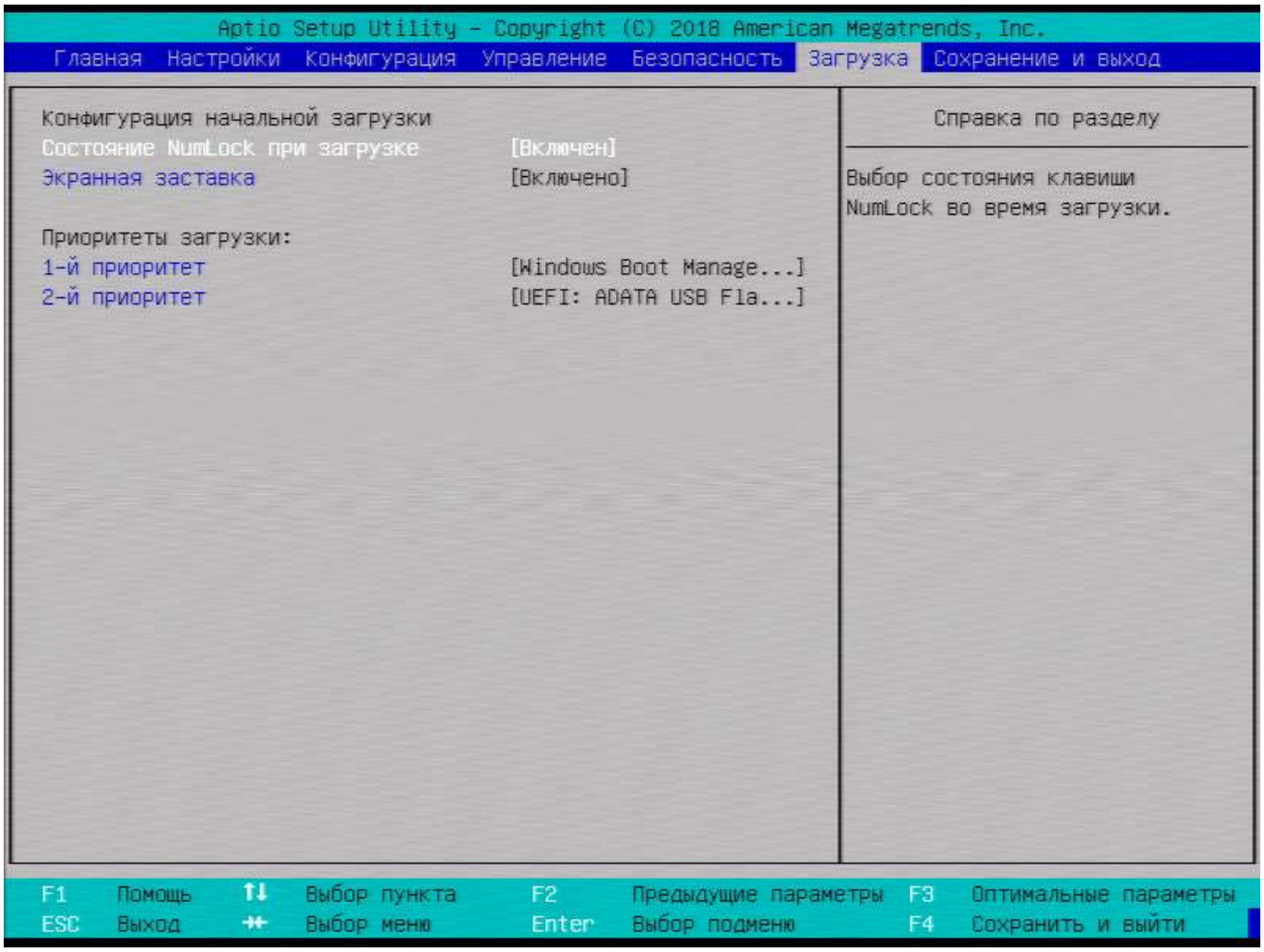
Aptio Setup Utility – Copyright (C) 2018 American Megatrends, Inc.
Главная Настройки Конфигурация Управление Безопасность Загрузка Сохранение и выход
Конфигурация начальной загрузки
Состояние NumLock при загрузке [Включен]
Экранная заставка [Включено]
Приоритеты загрузки:
1-й приоритет [Windows Boot Manage...]
2-й приоритет [UEFI: ADATA USB Fla...]
Справка по разделу
Выбор состояния клавиши NumLock во время загрузки.
F1 Помощь ↑↓ Выбор пункта F2 Предыдущие параметры F3 Оптимальные параметры
ESC Выход ↔ Выбор меню Enter Выбор подменю F4 Сохранить и выйти

Рис. 3.22

3.1.8. Раздел меню «Сохранение и выход»

Раздел меню «Сохранение и выход» (рис. 3.23) позволяет:

– *Действия с текущими параметрами:*

1) *Сохранить изменения и выйти* – после сохранения изменений выйти из настроек системы и продолжить загрузку;

2) *Отменить изменения и выйти* – выйти из настроек системы без сохранения произведенных изменений и продолжить загрузку;

3) *Сохранить изменения и перезагрузиться* – после сохранения настроек перезагрузить систему;

4) *Отменить изменения и перезагрузиться* – перезагрузить систему без сохранения произведенных изменений;

5) *Сохранить изменения* – сохранить любые изменения, произведенные в параметрах системы;

6) *Отменить изменения* – отменить любые изменения, произведенные в параметрах системы.

– *Сохранить/восстановить настройки:*

1) *Восстановить заводские настройки* – восстановить значения по умолчанию для всех параметров системы;

2) *Сохранить настройки как пользовательские* – сохранить значения параметров системы, как профиль пользователя, включая все внесенные изменения;

3) *Восстановить пользовательские настройки* – восстановить значения параметров системы из профиля пользователя.

– *Произвести загрузку с устройства.*

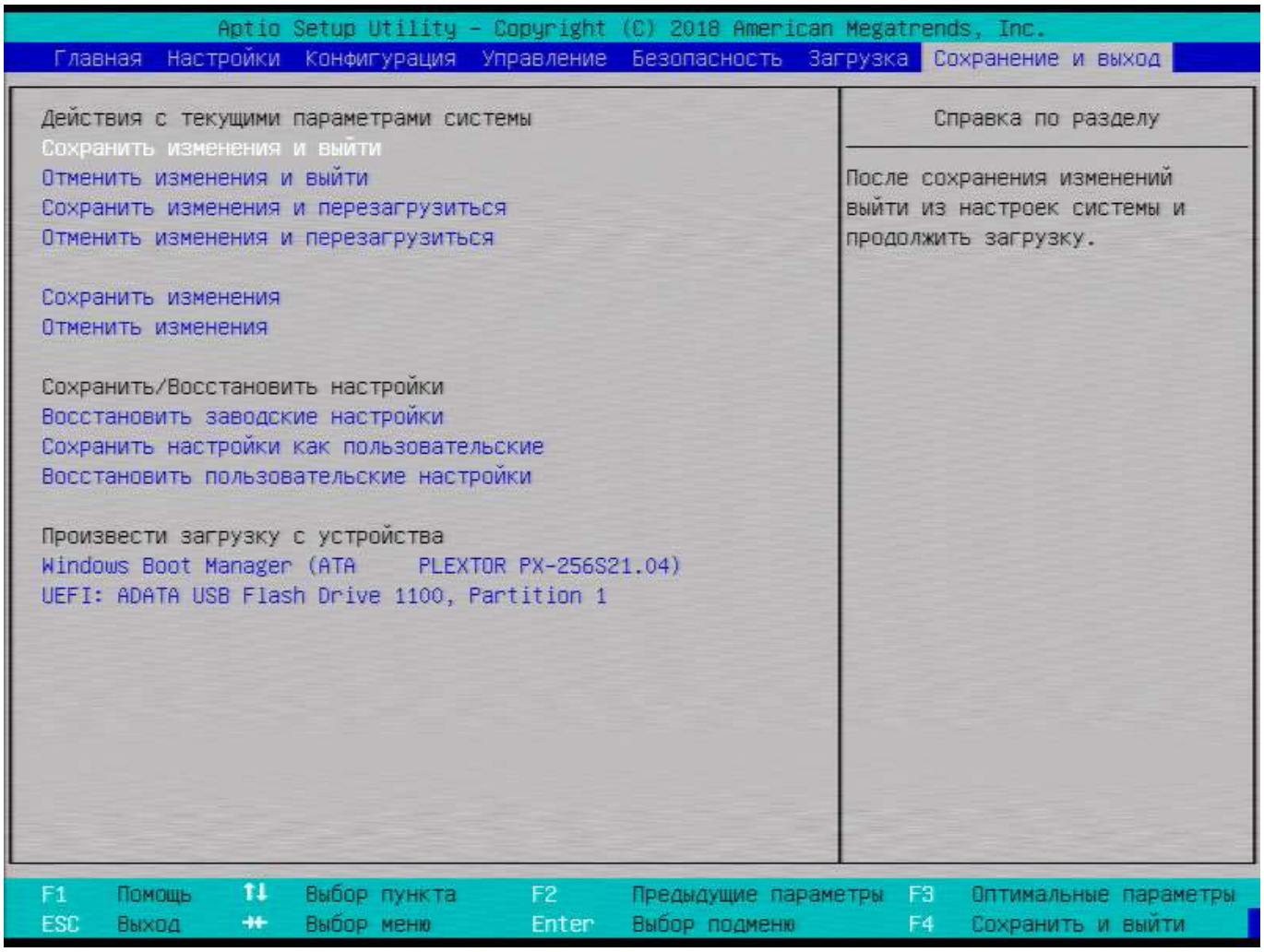
Aptio Setup Utility – Copyright (C) 2018 American Megatrends, Inc.
Главная Настройки Конфигурация Управление Безопасность Загрузка Сохранение и выход
Действия с текущими параметрами системы
Сохранить изменения и выйти
Отменить изменения и выйти
Сохранить изменения и перезагрузиться
Отменить изменения и перезагрузиться
Сохранить изменения
Отменить изменения
Сохранить/Восстановить настройки
Восстановить заводские настройки
Сохранить настройки как пользовательские
Восстановить пользовательские настройки
Произвести загрузку с устройства
Windows Boot Manager (ATA PLEXTOR PX-256S21.04)
UEFI: ADATA USB Flash Drive 1100, Partition 1
Справка по разделу
После сохранения изменений выйти из настроек системы и продолжить загрузку.
F1 Помощь
ESC Выход
Выбор пункта
Выбор меню
F2 Предыдущие параметры
Enter Выбор подменю
F3 Оптимальные параметры
F4 Сохранить и выйти

Рис. 3.23

4. ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

При возникновении различных проблем, связанных с работой ПО БСВВ ВСМ-МВ, а также для получения консультации администратор может обратиться в Центр поддержки пользователей. Перед обращением в Центр поддержки пользователей системному администратору предлагается подготовить следующую информацию:

– версию программного обеспечения;

– версии компонентов программного обеспечения;

– подробное описание неисправностей или ошибок;

– «скриншоты» ошибок программного обеспечения.

Консультацию Центра поддержки пользователей можно получить по телефонам:

тел. №1: 8 (495) 969-24-04 – для Москвы;

тел. №2: 8 (800) 200-03-55 – для регионов.

Через Интернет-форму:

http://www.kraftway.ru/support/support.php.

5. ПРАВИЛА ПРИЕМКИ

5.1. Общие положения

Для контроля качества и приемки готовых изделий устанавливают следующие основные категории испытаний:

- предъявительские;
- периодические.

5.2. Предъявительские испытания

Предъявительские испытания проводит отдел технического контроля перед предъявлением изделия для приемки представительству заказчика, потребителю или другим органам приемки. Предъявительские испытания проводятся силами и средствами предприятия-изготовителя.

На предъявительские испытания изделия с предустановленным ПО предъявляются поштучно или партиями:

− при поштучном предъявлении изделий на испытания или партией до пяти экземпляров всем видам проверок, предусмотренных в таблице 3.1, подвергаются 100 % предъявленных экземпляров;

− при предъявлении изделий партией свыше пяти экземпляров всем видам проверок по таблице 3.1 подвергаются 20 %, но не менее пяти экземпляров.

Остальные экземпляры этой партии подвергаются проверкам по п. 1 таблицы 3.1.

Таблица 3.1 – Состав предъявительских испытаний

Наименование вида испытаний	Номер пункта ТУ	
	технических требований	методов контроля
1 Проверка комплектности ПО	2.4	4.2
2 Проверка требований к упаковке и маркировке	2.6	4.3
3 Проверка требований к носителям данных ЭД	2.5	4.4
4 Проверка требования к ЭД	2.3	4.5
5 Проверка функциональных возможностей ПО:	2.2	4.6.1

Наименование вида испытаний	Номер пункта ТУ	
	технических требований	методов контроля
– проверка ролевого механизма контроля доступа к управлению и настройкам ПО; – контроль неизменности ПО.	2.2	4.6.2
Примечание. Последовательность проверок может быть изменена по согласованию с представителем заказчика.		

5.3. Периодические испытания

Периодические испытания проводит предприятие-изготовитель для периодической проверки соответствия ПО всем требованиям, указанным в ТУ, контроля стабильности технологического процесса производства ПО, подтверждения возможности продолжения его изготовления по действующей технологической документации и приемки.

Периодические испытания проводят на изделии, прошедшем предъявительские испытания с предустановленным ПО. Периодические испытания проводят в соответствии с годовым графиком, не реже одного раза в год.

Перечень периодических испытаний приведен в таблице 3.2.

Таблица 3.2 – Состав периодических испытаний

Наименование вида испытаний	Номер пункта ТУ	
	технических требований	методов контроля
1 Проверка комплектности ПО	2.4	4.2
2 Проверка требований к упаковке и маркировке	2.6	4.3
3 Проверка требования к носителям данных ЭД	2.5	4.4
4 Проверка требований к ЭД	2.3	4.5
5 Проверка функциональных возможностей ПО: – проверка ролевого механизма контроля доступа к управлению и настройкам ПО; – контроль неизменности ПО.	 2.2 2.2	 4.6.1 4.6.2
Примечание**.** Последовательность проверок может быть изменена по согласованию с представителем заказчика.		

6. РЕАЛИЗАЦИЯ ФУНКЦИЙ БЕЗОПАСНОСТИ СРЕДЫ ФУНКЦИОНИРОВАНИЯ

При реализации функций безопасности, связанных со средой функционирования ПО БСВВ ВСМ-МВ, необходимо придерживаться политик безопасности организации. В данные политики безопасности должны быть включены меры по организационной и физической защите доступа к ПО БСВВ ВСМ-МВ.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Наименование и определение
ОС	Операционная система
ПЗУ	Постоянное запоминающее устройство – энергонезависимая память, используется для хранения массива неизменяемых данных
ПО БСВВ ВСМ-МВ	Программное обеспечение базовой системы ввода-вывода платы серверной ВСМ-МВ
BIOS	англ. Basic Input/Output System – «базовая система ввода-вывода» – реализованная в виде набора микропрограмм часть системного программного обеспечения, которая предназначается для предоставления операционной системе API-доступа к аппаратуре компьютера и подключенным к нему устройствам
EBC	англ. Extensible Firmware Interface Byte Code – байткод интерфейса между операционной системой и микропрограммами, управляющими низкоуровневыми функциями оборудования
TCP/IP	англ. Transmission Control Protocol (TCP)/Internet Protocol (IP) – набор сетевых протоколов передачи данных, используемых в сетях, включая сеть Интернет
UEFI	англ. Unified Extensible Firmware Interface – стандартизированный расширяемый интерфейс встроенного программного обеспечения