УТВЕРЖДЕН
УПТЛ.00001-01 34 01 – УЛ

Инв. № подл.	Подпись и дата	Взам. Инв. №	Инв. № дубл.	Подп. и дата

Программа начального старта (UEFI) Иртыш

Руководство пользователя

УПТЛ.00001-01 34 01

Листов 34

2026 г.

Содержание

Термины и определения....3
ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ....5
Введение....6
1 Назначение и условия применения....8
1.1 Назначение программы начального старта (UEFI) Иртыш....8
1.2 Реализация....8
1.3 Материнские платы....8
2 Установка UEFI....9
3 Порядок работы с UEFI....10
3.1 Особенности интерфейса....10
3.2 Раздел «Main»....10
3.3 Раздел «Set. Date And Time»....11
3.4 Раздел «Securite»....12
3.5 Раздел «Power»....16
3.6 Раздел «Advanced»....16
3.7 Раздел «Device Manager»....21
3.8 Раздел «Boot Manager»....28
3.9 Раздел «Boot Maintenance Manager»....29
3.10 Раздел «Save & Exit»....32
4 Аварийные ситуации....33
Лист регистрации изменений....34

Термины и определения

Above 4G Decoding – опция, которая позволяет системе использовать адресное пространство свыше 4 ГБ для устройств, подключённых через *PCI Express*, в первую очередь – для современных видеокарт с большим объёмом видеопамяти.

SR-IOV Switch – опция, которая позволяет виртуальным машинам получать прямой доступ к физическим устройствам хоста, минуя программные коммутаторы гипервизора.

ResizableBar Switch – технология, позволяющая центральному процессору обращаться ко всему объёму видеопамяти видеокарты, а не только к ограниченному блоку (до 256 МБ).

EMU Switch (Embedded Management Unit) – режим или приглашение командной строки. Этот режим используется для восстановления или диагностики устройства при сбое программного обеспечения.

PCIe DSM#5 Support – поддержка спецификации *Device Specific Management (DSM)* для устройств, подключаемых через интерфейс *PCI Express (PCIe).*

Dvfs Setup DVFS (*Dynamic Voltage and Frequency Scaling*) – это технология динамического изменения напряжения и частоты процессора для оптимизации энергопотребления и производительности. Настройка DVFS позволяет процессору автоматически подстраивать свои параметры под текущую нагрузку.

HttpBoot – способ загрузки операционной системы по сети с использованием протокола HTTP.

Ipv4PxeSupport – способ загрузки операционной системы по сети с использованием протокола IPv4.

Ipv6PxeSupport – способ загрузки операционной системы по сети с использованием протокола IPv6.

iSCSI Target – сервер, предоставляющий доступ к своим дискам или образам.

iSCSI Initiator – клиент, который подключается к *target* и использует удалённое хранилище как локальный диск.

TLS Auth Configuration – настройка, связанная с использованием протокола **TLS** (*Transport Layer Security*) для аутентификации и обеспечения безопасности соединений между клиентом и сервером.

Enroll Cert (или **Certificate Enrollment**) – процесс запроса и получения цифрового сертификата от удостоверяющего центра (*Certificate Authority, CA*).

GMAC (*Galois Message Authentication Code*) – режим работы алгоритма *GCM* (*Galois/Counter Mode*), который используется для аутентификации данных, но не для их шифрования. Он применяется для проверки целостности и подлинности сообщений.

IOMMU (*Input/Output Memory Management Unit)*, блок управления памятью ввода-вывода) – это аппаратный компонент, который отвечает за трансляцию виртуальных адресов, используемых устройствами ввода-вывода, в физические адреса оперативной памяти.

UEFI Apacer – загрузочные внешние носители информации (накопители) в формате USB-флэш или диска Apacer, предназначенные для установки ОС в режиме *UEFI.*

Boot Maintenance Manager – инструмент, встроенный в *UEFI/BIOS* некоторых компьютеров и серверов, предназначенный для расширенного управления параметрами загрузки системы.

COM Attribute Setup Page – страница настройки атрибутов COM (Component Object Model). На этой странице осуществляется задание или изменение параметров (атрибутов) COM-объектов.

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

UEFI	Unified Extensible Firmware Interface	Единый расширяемый интерфейс программного обеспечения
BIOS	Basic Input/Output System	Базовая система ввода-вывода
CSM	Compatibility Support Module	Модуль поддержки совместимости
EDK2	Embedded Development Kit 2	Встроенный набор для разработки
HII	Human Interface Infrastructure	Инфраструктура интерфейса для пользователя
TPM	Trusted Platform Module	Аппаратный модуль безопасности
EMU	Embedded Management Unit	Режим командной строки
DSM	Device Specific Management	Поддержка спецификации
DVFS	Dynamic Voltage and Frequency Scaling	Технология динамического изменения напряжения и частоты процессора
TLS	Transport Layer Security	Транспортный уровень безопасности
CA	Certificate Authority	Удостоверяющий центр
GMAC	Galois Message Authentication Code	Режим работы алгоритма GCM
GCM	Galois/Counter Mode	Алгоритм, используемый для аутентификации данных
IOMMU	Input/Output Memory Management Unit	Блок управления памятью ввода-вывода

Введение

Unified Extensible Firmware Interface (UEFI) (единый расширяемый интерфейс программного обеспечения) – интерфейс между операционной системой и микропрограммами, управляющими низкоуровневыми функциями оборудования.

UEFI – программный слой, который запускается при включении компьютера и отвечает за инициализацию аппаратных компонентов и передачу управления операционной системе.

UEFI работает через прошивку, установленную на материнской плате компьютера.

Предназначен для замены интерфейса BIOS.

В современных компьютерах UEFI является надстройкой над BIOS, поэтому часто используют термин «UEFI BIOS», то есть UEFI содержит базовые функции BIOS и может работать в режиме совместимости CSM.

Преимущества UEFI:

1. Существует четкая спецификация на интерфейсы, которые прошивка предоставляет внешним сущностям. Например, загрузчику операционной системы. Прошивка может взаимодействовать с загрузчиками операционных систем, самими операционными системами или программами, которые занимаются инициализацией оборудования.

2. Встроенный командный интерпретатор (UEFI Shell). Это приложение может быть встроено в прошивку или запущено с внешнего носителя, например, в формате USB-флэш.

3. Наличие референсной реализации (Tianocore EDK2) представляет собой одновременно и референсную имплементацию спецификации UEFI, и пакет разработчика UEFI (UDK, UEFI Development Kit).

4. Наличие технологии Secure Boot, которая проверяет цифровую подпись загрузчика или других программ.

5. Архитектура HII (Human Interface Infrastructure). Эта архитектура предназначена для создания пользовательских интерфейсов, что обеспечивает поддержку мультиязычности.

В UEFI реализована модульная концепция – интерфейс системы состоит из отдельных элементов — модулей, каждый из которых выполняет свои функции. Примеры модулей: загрузочные, тестовые и рабочие сервисы.

Требования к уровню подготовки пользователя

1. Навыки работы с операционной системой, файловой системой и периферийными устройствами.

2. Знания и навыки работы с профессиональными программами и сложными техническими задачами.

3. Умение работать с конкретным интерфейсом, инструментами и форматами данных.

4. Знание назначения и особенностей функционирования интерфейса BIOS.

1 Назначение и условия применения

1.1 Назначение программы начального старта (UEFI) Иртыш

Программа выполяет следующие функции:

– первичная проверка и инициализация аппаратных ресурсов системной (материнской) платы;

– обеспечение базовых функций и интерфейсов системной (материнской) платы;

– поиск и передача управления ОС (или ее загрузчику);

– предоставление пользовательского интерфейса по начальной настройке материнской платы и ее интерфейсов;

– инициализация интерфейсов;

– осуществление выбора порядка загрузки операционных систем;

– обеспечение базовой совместимости аппаратных средств системной (материнской) платы.

1.2 Реализация

UEFI работает через прошивку, установленную на материнской плате компьютера. Информацию о инициализации и запуске системы UEFI хранит в файле EFI, который хранится в разделе EFI System Partition (ESP) на жёстком диске.

1.3 Материнские платы

Типы материнских плат с установленными процессорами:

1. AC612A0_V1.1 – материнская плата с процессором Иртыш C616.

2. TD622E0_V1.2 – материнская плата с процессором Иртыш C632.

2 Установка UEFI

Порядок установки UEFI изложен в документе «Программа начального старта (UEFI) Иртыш. Руководство по установке».

3 Порядок работы с UEFI

3.1 Особенности интерфейса

Интерфейс управляется с клавиатуры:

– навигация – клавиши-стрелки;

– Enter – выбор пункта;

– Esc – возврат на предыдущий уровень;

– клавиша F2 – вход в меню;

– клавиша F10 сохраняет изменения и выход из Setup;

– клавиша F9 сбрасывает все настройки на значения по умолчанию.

3.2 Раздел «Main»

Данный раздел содержит основную информацию о системе.

Для входа в раздел подайте напряжение на материнскую плату и далее нажмите клавишу F2. При этом откроется окно (рисунок 1).

Рисунок 1 – Установочные утилиты

Для получения информации о системе перейдите в раздел «Main». При этом откроется окно (рисунок 2).

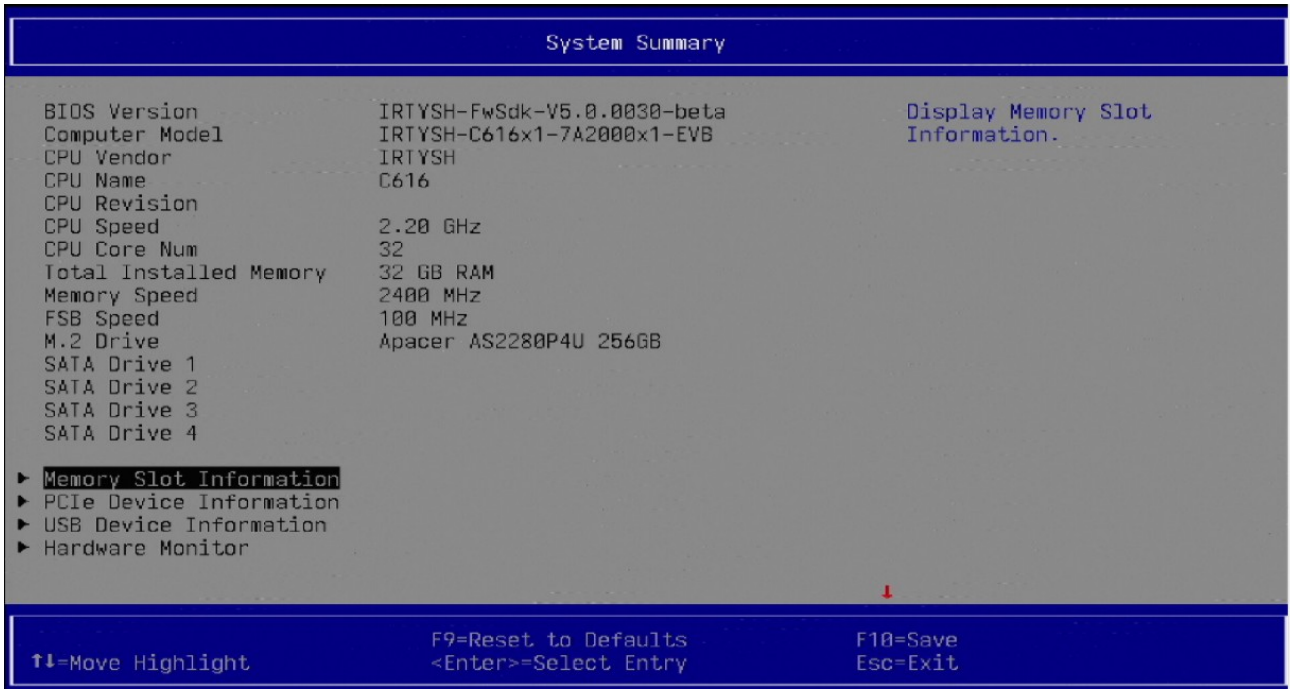

Рисунок 2 – Информация о системе

Здесь можно получить информацию о версии интерфейса, о процессоре, о накопителях, а также:

– о памяти компьютера – в подразделе «Memory Slot Information»;

– об устройствах, подключенных к шине PCIe – в подразделе «PCIe Device Information»;

– об устройствах, подключенных к USB-порту – в подразделе «USB Device Information»;

– о состоянии оборудования (температура процессора и температура материнской платы) – в подразделе «Hardware Monitor».

3.3 Раздел «Set. Date And Time»

Перейдя в раздел «Set. Date And Time» (Установка даты и времени), можно установить системные дату и время (рисунок 3).

Значения используются операционной системой до запуска службы синхронизации времени.

Рисунок 3 – Установка даты и времени

3.4 Раздел «Securite»

Раздел «Securite» (Настройки безопасности) содержит подразделы (рисунок 4):

– Secure Boot Configuration (Настройка безопасной загрузки);

– Factory (Восстановление заводских настроек);

– Password (Пароли);

– Update Firmware (обновление прошивки).

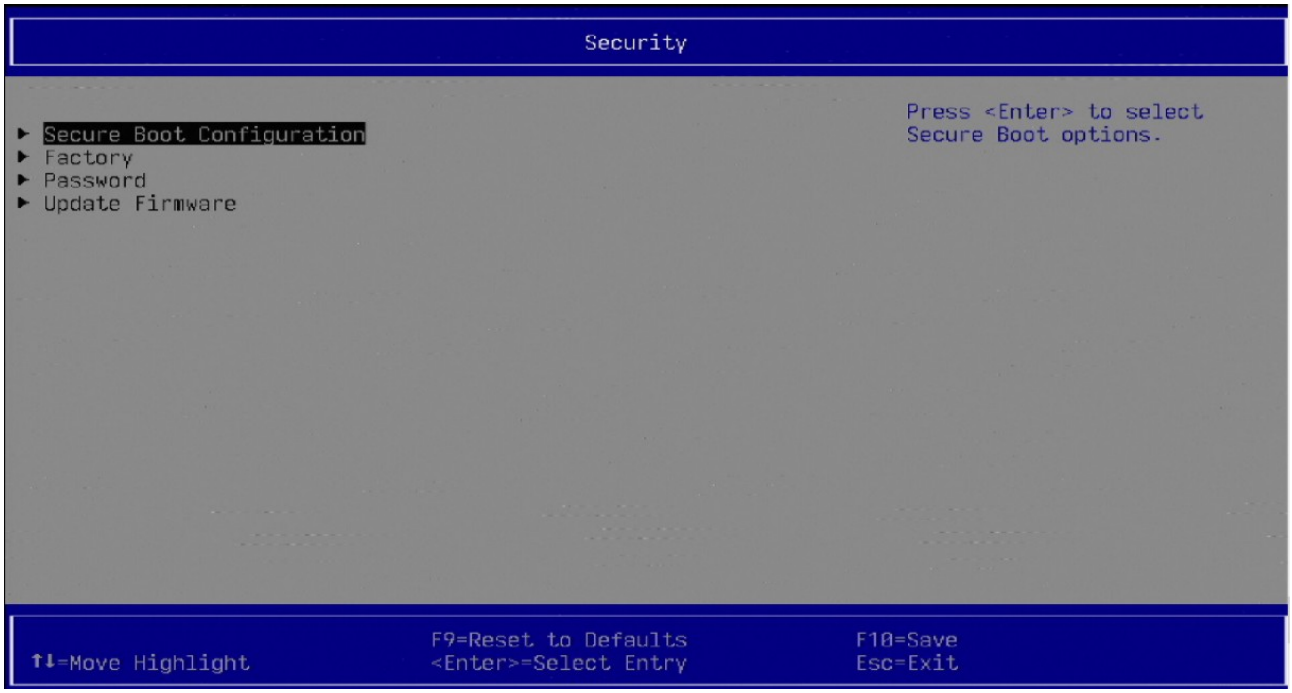

Рисунок 4 – Раздел «Securite»

В подразделе «Secure Boot Configuration» производится выбор режима безопасной загрузки. В данном случае – Standard Mode (стандартный режим).

Рисунок 5 – Настройки безопасной загрузки

В подразделе «Factory» есть возможность восстановить заводские настройки (рисунок 6).

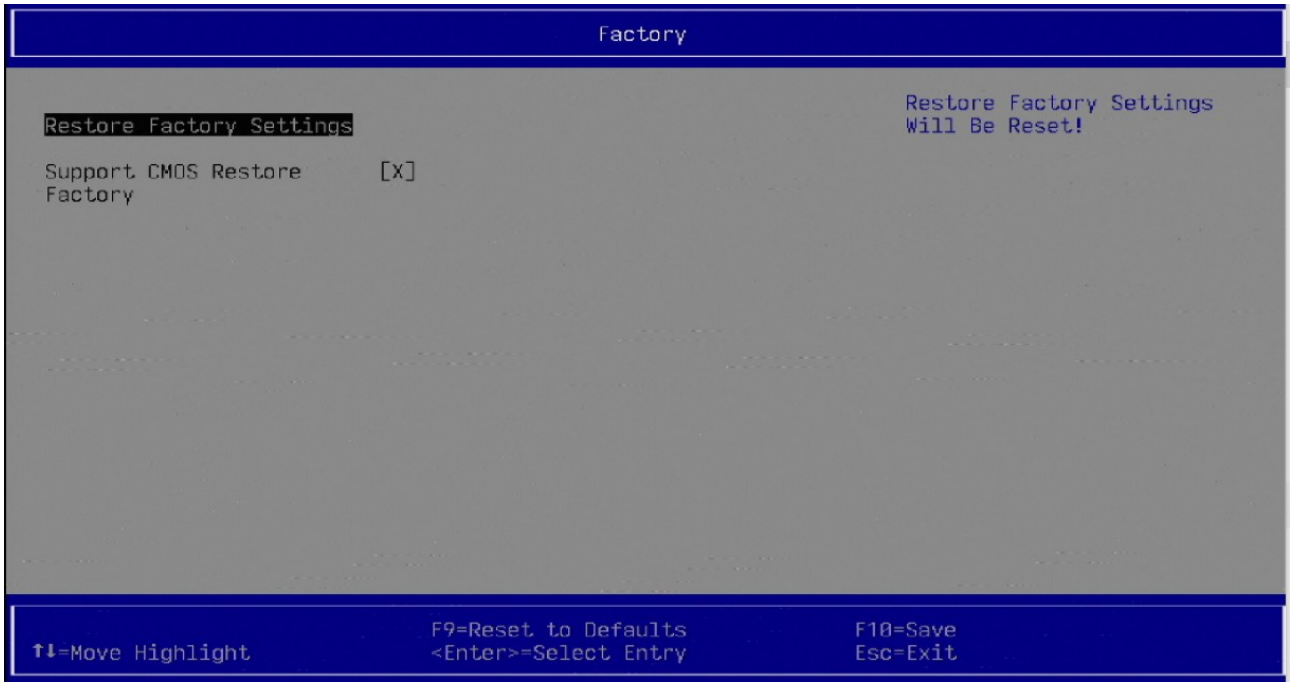

Рисунок 6 – Раздел «Factory»

В подразделе «Password» устанавливается пароль администратора (рисунок 7).

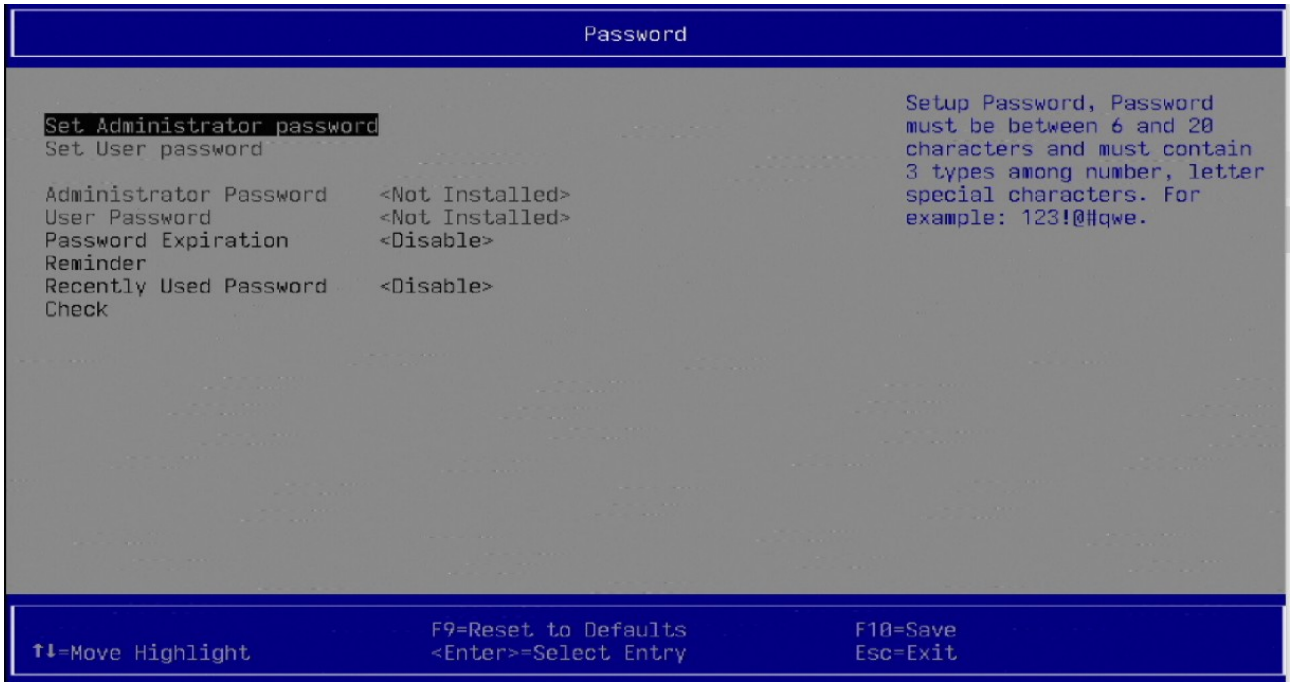

Рисунок 7 – Раздел «Password»

В разделе «Update Firmware» (рисунок 8) можно оставить «Retain» или удалить «Clear» конфигурацию прошивки (рисунок 9).

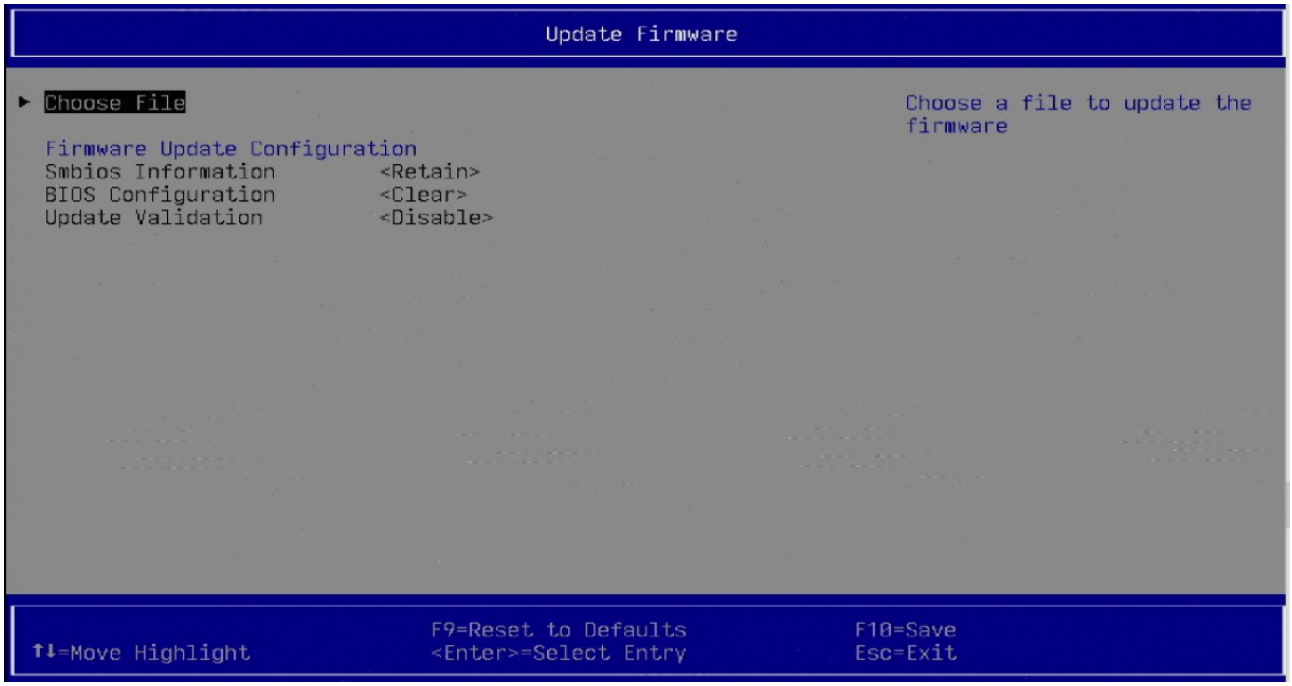

Рисунок 8 – Раздел «Update Firmware»

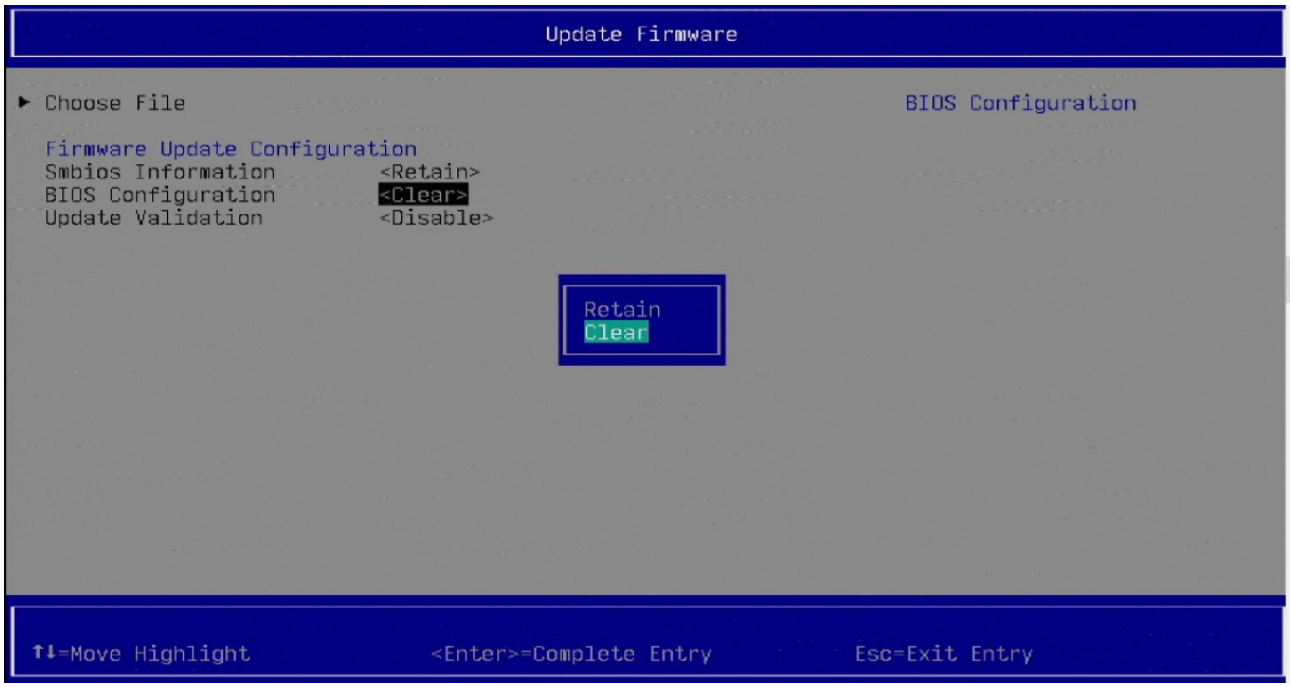

Рисунок 9 – Обновление конфигурации прошивки

3.5 Раздел «Power»

В разделе «Power» производятся настройки управления питанием: в данном случае возобновление работы по времени (рисунок 10).

Рисунок 10 – Раздел «Power»

3.6 Раздел «Advanced»

В разделе «Advanced» (Расширения) производятся расширенные настройки платформы.

Раздел «Advanced» содержит следующие подразделы (рисунок 11):

– PCI Subsystem Settings (настройки подсистемы шины PCI);

– Legasy Boot Mode (стандартный режим загрузки);

– Primary Display (основной дисплей);

– Console Settings (настройки консоли);

– System Management Controller (управляющий контроллер системы).

Рисунок 11 – Раздел «Advanced»

Подраздел «PCI Subsystem Settings» (рисунок 12) содержит вкладки:

– Above 4G Decoding;

– SR-IOV Switch;

– ResizableBar Switch;

– EMU Switch;

– PCIe DSM#5 Support.

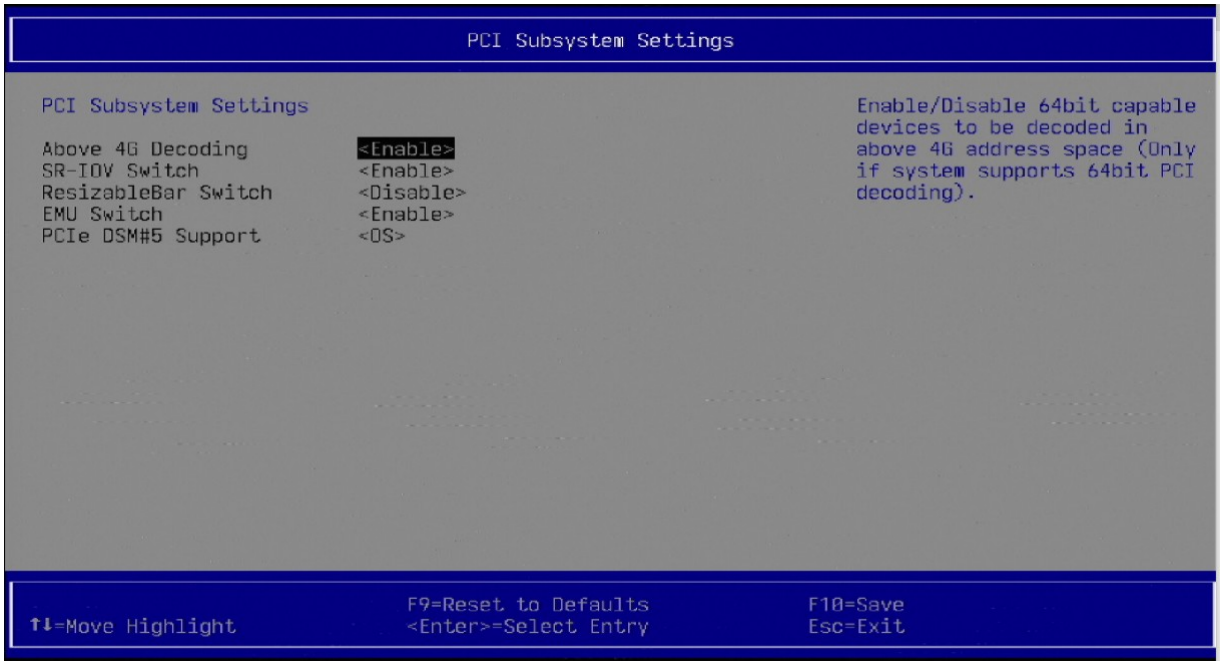

Рисунок 12 – Подраздел «PCIe Subsystem Settings»

Переходя на вкладки можно получить информацию о включении/выключении той или иной опции.

В подразделе «Legasy Boot Mode» представлена информация о включении режима загрузки с использованием ISO-файла (рисунок 13).

В подразделе «Primary Display» представлена информация об автоматическом включении основного дисплея (рисунок 14).

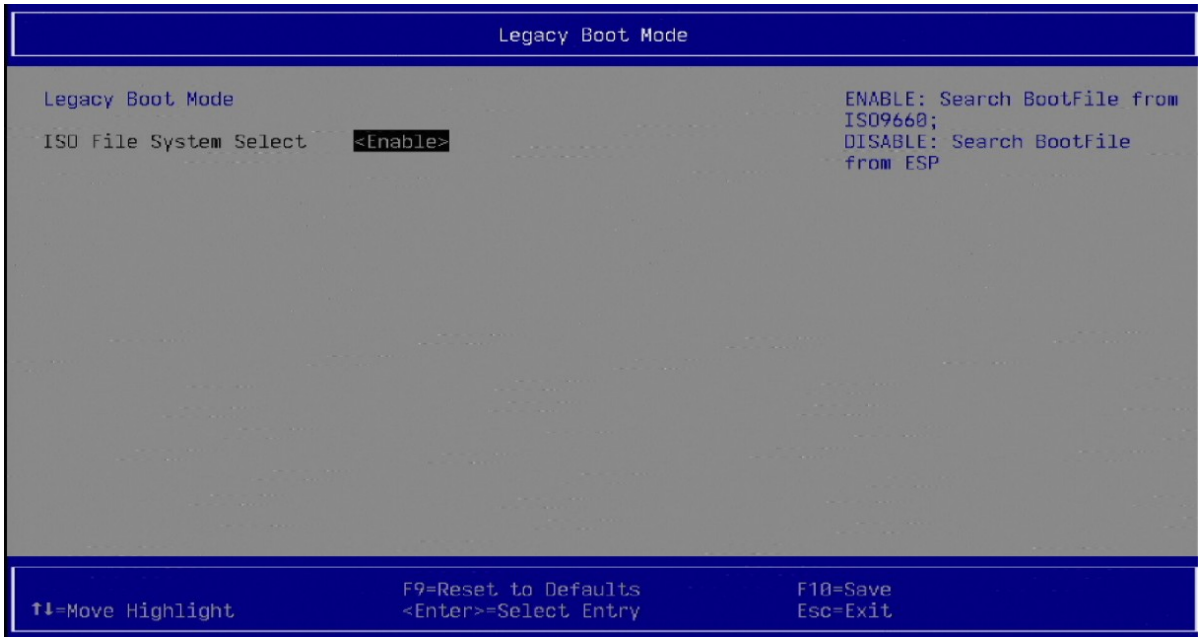

Рисунок 13 – Подраздел «Legasy Boot Mode»

Рисунок 14 – Подраздел «Primary Display»

В подразделе «Console Settings» есть возможность включить/отключить направление вывода консольных программ, а также – приоритетный канал вывода (рисунок 15). Кроме того, можно выбрать тип терминала.

Поразделе «System Management Controller» содержит вкладки (рисунок 16):

– Dvfs Setup – динамическое изменение напряжения и частоты процессора;

– Power Limit Setup – установка ограничения энергопотребления.

Рисунок 15 – Подраздел «Console Settings»

Рисунок 16 – Подраздел «System Management Controller»

3.7 Раздел «Device Manager»

В данном разделе представлен обзор всех устройств, обнаруженных прошивкой.

Раздел содержит следующие подразделы (рисунок 17):

– Network Control – контроль сети;

– iSCSI Configuration – конфигурация блочных устройств;

– Tls Auth Configuration – настройка, связанная с использованием протокола **TLS;**

– Control Various Controllers – управление контроллерами;

– Network Device List – список сетевых устройств.

Рисунок 17 – Раздел «Device Manager»

3.7.1 Подраздел «Network Control» содержит вкладки:

Перейдя на вкладку «HttpBoot», можно включить/отключить данный способ загрузки операционной системы по сети (рисунок 18).

Аналогично, перейдя на вкладки Ipv4PxeSupport и Ipv6PxeSupport можно включить/отключить данные способы загрузки операционной системы по сети.

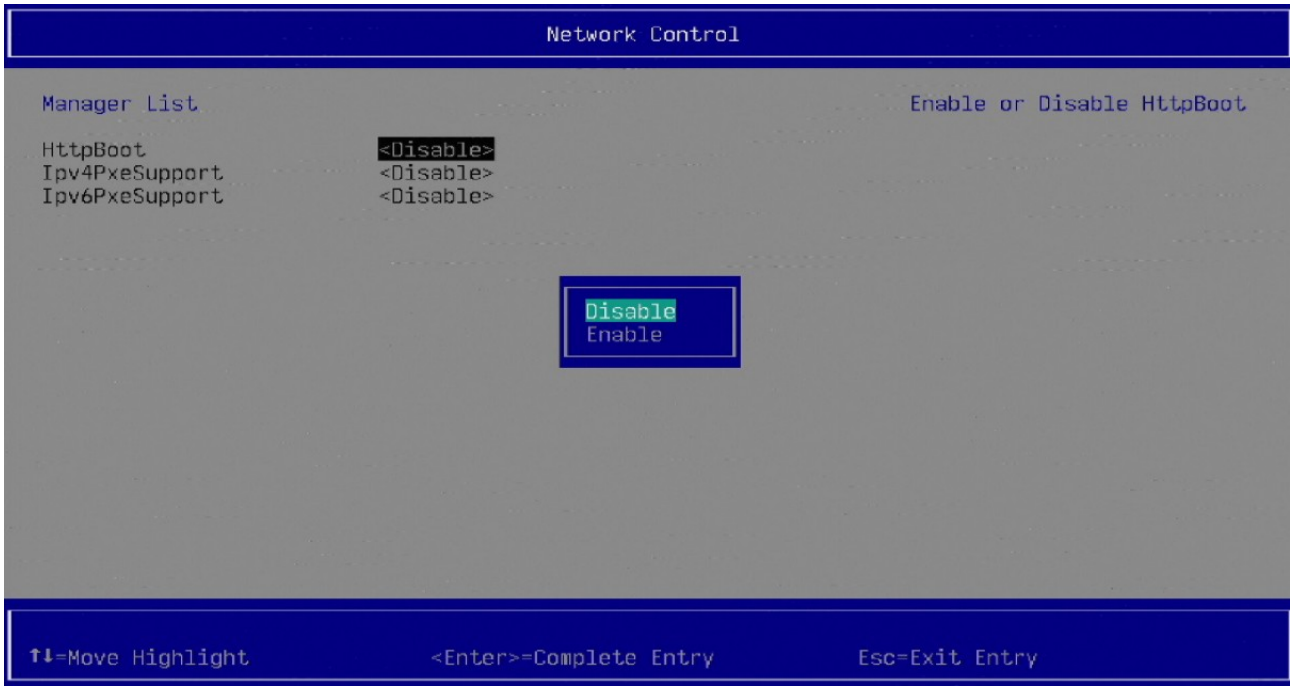

Рисунок 18 – Включение/выключение HttpBoot

3.7.2 Подраздел «SCSI Configuration» содержит имена iSCSI Initiator – клиентов, подключающихся к серверу iSCSI Target (рисунок 19):

В данном подразделе представлены вкладки:

– Add an Attempt – попытка присоединения;

– Delete Attempts – удаление попыток присоединения клиентов;

– Change Attempt Order – изменить порядок попыток.

Переходя на указанные вкладки, производятся присоединение клиентов, их удаление и изменение порядка попыток.

Рисунок 19 – Подраздел «iSCSI Configuration»

3.7.3 Подраздел «Tls Auth Configuration»

Данный подраздел содержит настройки, связанные с протоколом TLS для аутентификации и обеспечения безопасности соединений (рисунок 20).

Подраздел содержит вкладки:

Server CA Configuration. На данной вкладке осуществляется запрос сертификата безопасности от удостоверяющего центра (CA) – Enroll Cert и Delete Cert – удаление сертификата для сервера (рисунок 21).

Client Cert Configuration. На данной вкладке осуществляется запрос сертификата безопасности от удостоверяющего центра (CA) – Enroll Cert и Delete Cert – удаление сертификата для клиента.

Рисунок 20 – Подраздел «Tls Auth Configuration»

Рисунок 21 – Вкладка « Delete Cert»

3.7.4 Подраздел «Control Various Controllers» содержит следующие вкладки (рисунок 22):

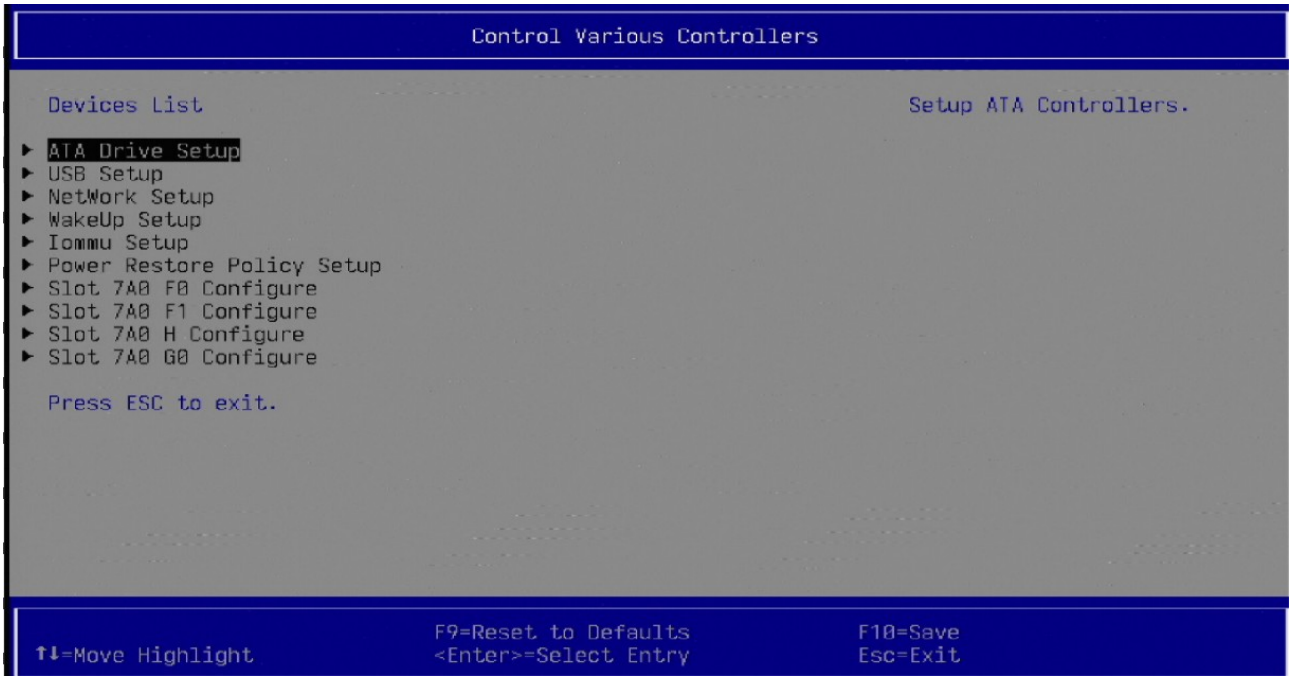

Рисунок 22 – Подраздел «Control Various Controllers»

Описание вкладок подраздела приведено в таблице 1.

Таблица 1 – Подраздел «Control Various Controllers»

Наименование вкладки	Описание	Содержит	Состояние	Примечание
ATA Drive Setup	SATA-контроллер – контроллер на материнской плате компьютера, который отвечает за обмен данными между устройствами хранения (жёсткими дисками, SSD, оптическими приводами) и остальными компонентами системы	Serial ATA Controller0 Serial ATA Controller1 Serial ATA Controller2 Serial ATA Controller3	<Enable> <Disable>	Если контроллер «Serial ATA Controller0» выключен, то будут также выключены и контроллеры 1 и 2
USB Setup	Универсальная последовательная шина	USB0 Controller USB1 Controller USB2 Controller	<Enable> <Disable>	Если контроллер «USB0 Controller» выключен», то будет также выключен и контроллер «USB1»

Наименование вкладки	Описание	Содержит	Состояние	Примечание
Network Setup	Установка сети	Ethernet Controller0 Ethernet Controller1	<Enable> <Disable>	Если контроллер «Ethernet Controller0» выключен», то будет также выключен и контроллер «Ethernet Controller1»
WakeUp Setup Wake-Up With On-LAN and Pcie and USB	Установка возобновления работы по локальной сети по шине PCIe и USB	Возобновление работы GMAC и USB по шине PCIe	<Enable> <Disable>	Возобновление работы с помощью USB-устройства или GMAC. Позволяет вывести систему из режима энергосбережения
Iommu Setup	Блок управления памятью ввода/вывода		<Enable> <Disable>	По умолчанию выключен. Если установлено <Enable>, то IOMMU включен
Power Restore Policy Setup	Настройка политики восстановления питания		<Power Off>	Если установлено <Power Off>, то необходимо выключить питание перед восстановлением системы
Slot 7AO F0 Configure	Настройка слотов расширения	Slot 7AO F0 Slot F0 Mode Slot F0 Gen Rate	<Enable> <X1> <3.0>	Количество линий: (X1 или X4) Поколение интерфейса: (1.0, 2.0 или 3.0)
Slot 7AO F1 Configure		Slot 7AO F1 Slot F1 Mode	<Enable> <X4>	Количество линий: (X1 или X4)

Наименование вкладки	Описание	Содержит	Состояние	Примечание
		Slot F1 Gen Rate	<3.0>	Поколение интерфейса: (1.0, 2.0 или 3.0)
Slot 7AO H Configure		Slot 7AO H Slot H Mode Slot H Gen Rate	<Enable> <X8> <3.0>	 Количество линий: (X4 или X8) Поколение интерфейса: (1.0, 2.0 или 3.0)
Slot 7AO G0 Configure		Slot 7AO G0 Slot G0 Mode Slot G0 Gen Rate	<Enable> <X8> <3.0>	 Количество линий: (X8 или X16) Поколение интерфейса: (1.0, 2.0 или 3.0)

3.7.5 Подраздел «Network Device List»

При переходе в подраздел «Network Device List» откроется окно (рисунок 23). Здесь представлены MAC-адреса сетевых устройств.

Рисунок 23 – Подраздел «Network Device List»

3.8 Раздел «Boot Manager»

При выборе раздела «Boot Manager» (Управление загрузкой) откроется окно (рисунок 24). Здесь представлено Boot Manager Menu (Меню управления загрузкой).

UEFI Apacer – загрузочная внешнего носителя информации (накопителя) в формате USB-флэш или диск Apacer, предназначенные для установки ОС в режиме UEFI.

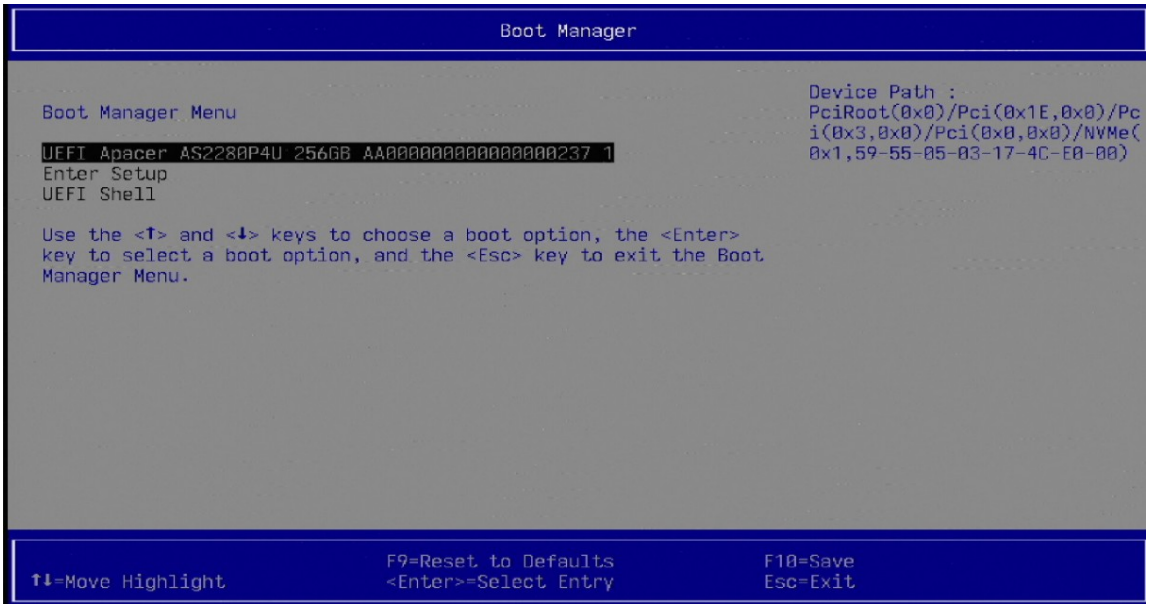

Рисунок 24 – Раздел «Boot Manager»

3.9 Раздел «Boot Maintenance Manager»

При выборе раздела «Boot Maintenance Manager» (Расширенное управление параметрами загрузки системы) откроется окно (рисунок 25).

Рисунок 25 – Раздел «Boot Maintenance Manager»

Раздел «Boot Maintenance Manager» содержит вкладки:

– Boot Options – опции загрузки;

– Driver Options – опции драйвера;

– Console Options – опции консоли;

– Boot From File – загрузка из файла.

Вкладка «Boot Options» содержит дополнительные вкладки (рисунок 26):

Go Back To Main Page – возврат на главную страницу;

– Add Boot Option – добавить опцию загрузки;

– Delete Boot Option – удалить опцию загрузки;

– Change Boot Order – изменить порядок загрузки;

– Boot Type Disable – отключить тип загрузки;

– Boot Disable Value – значение отключения загрузки.

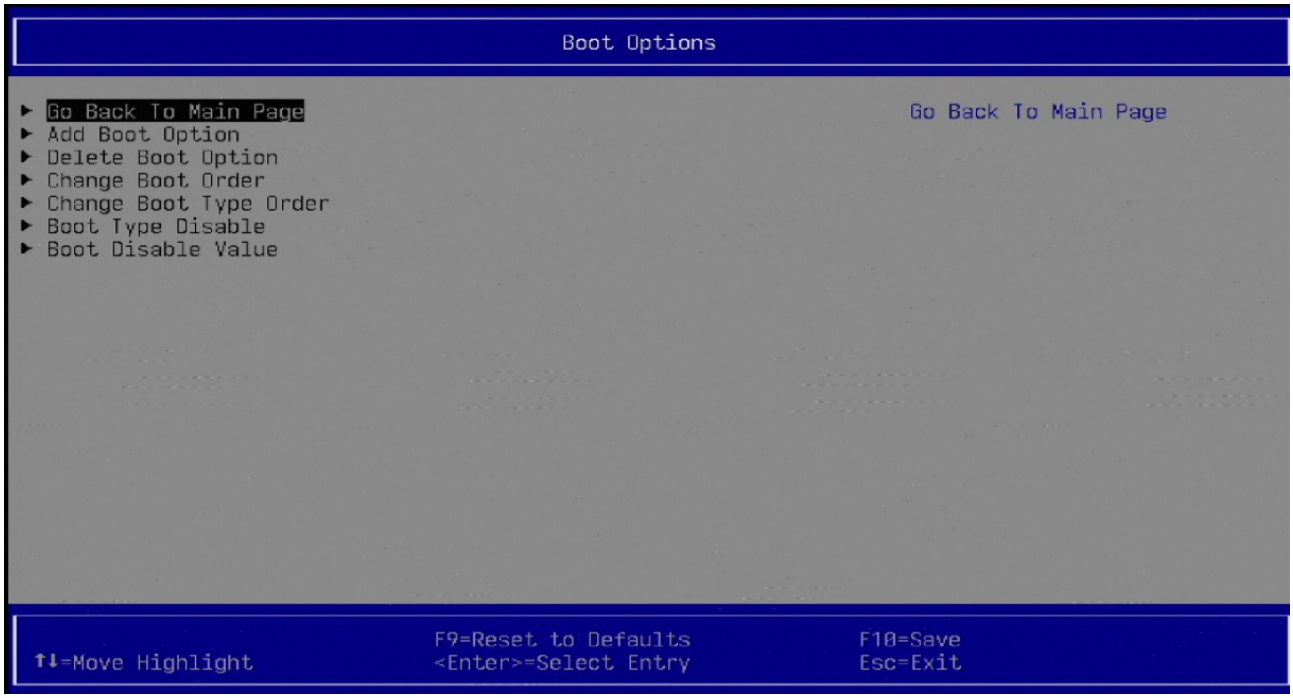

Рисунок 26 – Вкладка «Boot Options»

Вкладка «Driver Options» содержит дополнительные вкладки (рисунок 27):

Рисунок 27 – Вкладка **«Driver Options»**

– Go Back To Main Page – возврат на главную страницу;

– Add Driver Option – добавить опцию загрузки;

– Delete Driver Option – удалить опцию загрузки;

– Change Driver Order – изменить порядок драйверов.

Вкладка **«Console Options»** содержит дополнительные вкладки (рисунок 28):

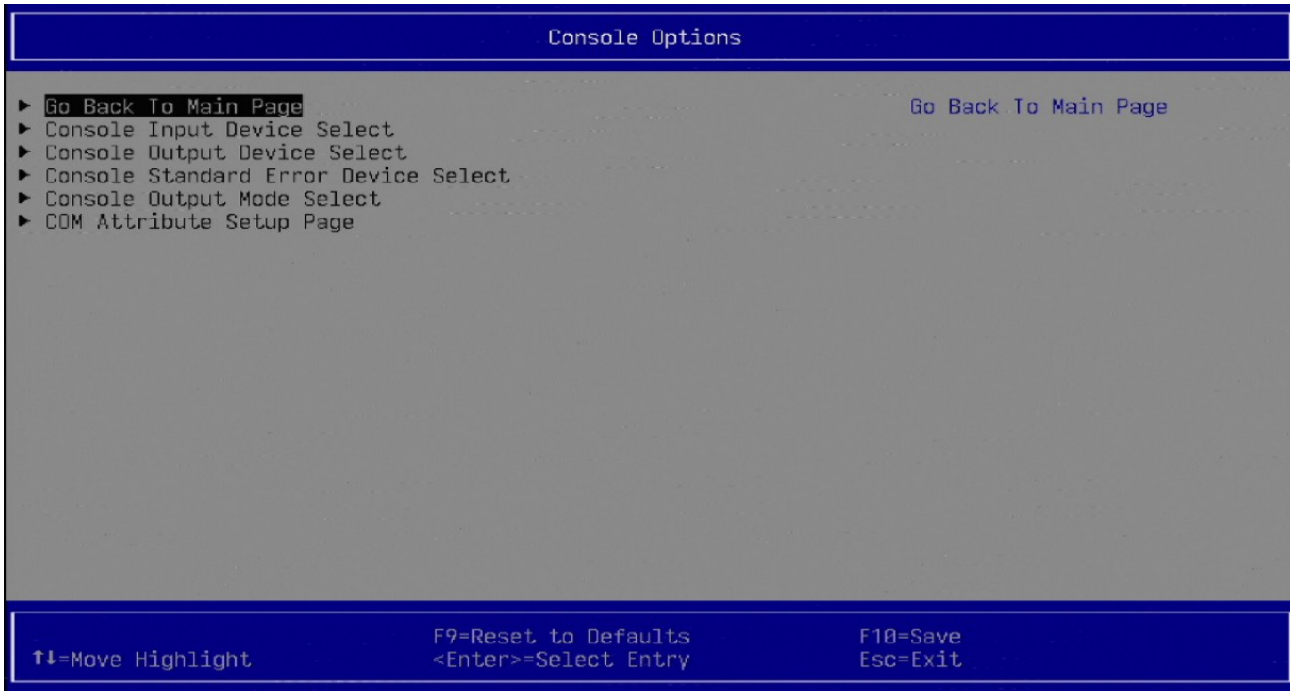

Рисунок 28 – Вкладка «Console Options»

– Go Back To Main Page – возврат на главную страницу;

– Console Input Device Select – выбор входного устройства в консоли;

– Console Output Device Select – выбор выходного устройства в консоли;

– Console Standart Error Device Select – выбор стандартных ошибок устройств в консоли;

– Console Output Mode Select – выбор выходного режима в консоли;

– COM Attribute Setup Page – страница настройки атрибутов COM.

– Вкладка «Boot From File» содержит файлы загрузки.

3.10 Раздел «Save & Exit»

При выборе раздела «Save And Exit» откроется окно (рисунок 29).

Рисунок 29 – Раздел «Save And Exit»

Раздел «Save And Exit» содержит вкладки:

– Save Changes and Reset – сохранить изменения и выйти;

– Discard Changes and Exit – отменить изменения и выйти;

– Shutdown – выключение.

4 Аварийные ситуации

Основные виды аварийных ситуаций представлены в таблице 2.

Таблица 2 – Основные виды аварийных ситуаций

Вид ситуации	Примеры	Последствия
Аварийное завершение	Вылет, краш, зависание программы	Потеря несохранённых данных, простой в работе
Сбой баз данных	Ошибка СУБД, повреждение таблиц	Нарушение целостности данных, невозможность работы с информацией
Программные конфликты	Несовместимость приложений, антивирусы	Блокировка работы, ложные срабатывания защиты
Вирусные атаки	Заражение ПО вредоносным кодом	Потеря или кража данных, нарушение работы системы
Аппаратные сбои	Отключение питания, неисправность диска	Потеря данных, повреждение файлов

Причины возникновения аварийных ситуаций:

– ошибки в коде программного обеспечения;

– некорректные действия пользователя;

– программные и аппаратные конфликты;

– вирусные и хакерские атаки;

– внешние факторы (отключение питания, сбои сети).

Рекомендации по предотвращению и устранению:

– регулярно создавать резервные копии данных;

– своевременно обновлять ПО и антивирусные базы;

– проводить тестирование и анализ кода;

– обучать пользователей правильной работе с программами;

– использовать средства мониторинга и журналирования для быстрого выявления и устранения ошибок.

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопрово-дительного документа и дата	Подп.	Дата
	изменен-ных	заменен-ных	новых	аннули-рованных					