

УТВЕРЖДЕН

АДМГ.30031-01 91 01-ЛУ

СРЕДСТВО ДОВЕРЕННОЙ ЗАГРУЗКИ АВРОРА

Руководство администратора

АДМГ.30031-01 91 01

Листов 78

АННОТАЦИЯ

Настоящий документ является руководством администратора Средства доверенной загрузки Аврора (далее - Аврора СДЗ) АДМГ.30031-01 релиз 1.3.

Документ содержит общую информацию об Аврора СДЗ, требованиях к системе и оборудованию, сведения о комплектности поставки Аврора СДЗ, описание загрузочных модулей Аврора СДЗ и утилит.

В документе также приведен порядок установки загрузочных модулей Аврора СДЗ на устройство, описана работа с инструментом настройки Аврора СДЗ, приведена информация о подписи ядра Linux.

ПРИМЕЧАНИЕ. Перед началом работы администратору необходимо ознакомиться с положениями настоящего документа, а также с информацией, приведенной в документе «Руководство пользователя» АДМГ.30031-01 90 01.

СОДЕРЖАНИЕ

1. Общая информация	5
1.1. Назначение	5
1.2. Основные характеристики и возможности	5
1.3. Область применения	7
2. Указания по эксплуатации.....	9
2.1. Ограничения по эксплуатации	9
2.2. Условия выполнения программы	10
3. Ввод в эксплуатацию.....	11
3.1. Идентификация комплектности поставки.....	12
3.2. Описание загрузочных модулей	13
3.3. Описание утилит.....	14
4. Порядок установки загрузочных модулей на устройство.....	17
4.1. Формирование ключевой информации	17
4.2. Формирование команд активации Аврора СДЗ	18
4.3. Подпись загрузочных модулей Аврора СДЗ.....	19
4.4. Установка загрузочных модулей.....	21
4.4.1. Установка с использованием программатора	21
4.4.2. Установка с использованием внешнего USB-накопителя.....	22
4.5. Примеры обновления загрузочных модулей	22
4.5.1. Пример обновления Аврора СДЗ с новым индексом RP	22
4.5.2. Пример обновления индекса RP ОС	23
5. Подпись ядра Linux	25
5.1. Подпись ядра Linux	25
5.2. Подпись initrd	25
5.3. Подпись ядра Linux и initrd из поставки предприятия-разработчика.....	26
6. Выполнение программы.....	27

6.1. Экран «Параметры»	33
6.1.1. Включение/выключение доверенной загрузки.....	34
6.1.2. Параметры идентификации и аутентификации.....	35
6.1.3. Управление ключевой информацией.....	37
6.1.4. Управление доверенной меткой времени.....	45
6.2. Экран «Пользователи».....	46
6.2.1. Действия над пользователем.....	47
6.2.2. Добавление пользователя.....	50
6.3. Экран «Журнал»	52
6.4. Экран «Диагностика»	53
6.4.1. Проверка целостности Аврора СДЗ	54
6.4.2. Проверка целостности журнала аудита	57
6.5. Экран «Обновление Аврора СДЗ»	59
6.6. Экран «Информация об Аврора СДЗ»	61
6.7. Экран «Управление устройствами».....	62
6.8. Экран «Менеджер загрузки»	63
6.9. Экран «Настройки загрузки»	64
6.9.1. Добавить вариант загрузки	66
6.9.2. Удалить вариант загрузки.....	70
6.9.3. Сменить порядок загрузки	71
Перечень терминов и сокращений.....	73
Приложение 1.....	74

1. ОБЩАЯ ИНФОРМАЦИЯ

1.1. Назначение

Аврора СДЗ предназначена для безопасной загрузки операционных систем (ОС) общего назначения, совместимых со стандартом UEFI, в том числе для ОС Alt Linux, Astra Linux и ОС Аврора для использования на устройствах на базе процессора Baikal-M BE-M1000.

Аврора СДЗ представляет собой программно-техническое средство, которое встраивается в базовую систему ввода-вывода и обеспечивает невозможность подключения нарушителя в разрыв между базовой системой ввода-вывода и Аврора СДЗ для несанкционированного доступа.

1.2. Основные характеристики и возможности

Аврора СДЗ состоит из следующих подсистем:

- подсистема доверенной загрузки в SCP-процессоре выполняет функции безопасности и служит для реализации корня доверия Аврора СДЗ в SCP-процессоре;
- подсистема доверенной загрузки цепочки загрузчиков AP-процессора выполняет функции безопасности и осуществляет последовательную верификацию загрузчиков, исполняющихся на AP-процессоре (AP_BL2, AP_BL31, AP_BL32, AP_BL33);
- подсистема доверенной загрузки ОС выполняет разграничение доступа к функциям управления параметрами доверенной загрузки на основе идентификации и аутентификации пользователей, осуществляет регистрацию событий, сигнализацию о событиях безопасности, обеспечение безопасности после завершения работы Аврора СДЗ, а также проводит контроль целостности загружаемого ядра ОС общего назначения, на основе проведенного анализа целостности осуществляется либо передача управления в ядро ОС, либо блокирование загрузки устройства;

АДМГ.30031-01 91 01

- подсистема администрирования Аврора СДЗ управляет компонентами, данными и параметрами СДЗ;

- подсистема Аврора ТЕЕ используется для загрузки в иерархии загрузчиков на уровне AP_BL32 в качестве компонента «заглушки» обработчика исключений, вызванных SMC командами, адресованными на уровень исключений S-EL1.

Аврора СДЗ обеспечивает следующие возможности:

- регистрация возникновения событий, относящихся к безопасности и контролируемых Аврора СДЗ;

- реагирование на обнаружение событий, указывающих на возможное нарушение безопасности;

- контроль целостности загружаемой ОС;

- возможность со стороны администраторов Аврора СДЗ управлять режимом выполнения функций безопасности Аврора СДЗ;

- возможность со стороны администраторов Аврора СДЗ управлять данными (данными Аврора СДЗ), используемыми функциями безопасности Аврора СДЗ;

- поддержка определенных ролей (учетных записей пользователей) для Аврора СДЗ и их ассоциации с конкретными администраторами Аврора СДЗ и пользователями информационных систем;

- тестирование (самотестирование) функций безопасности Аврора СДЗ, проверки целостности программного обеспечения (ПО) Аврора СДЗ и целостности данных Аврора СДЗ;

- блокирование загрузки ОС в следующих случаях:

- выявление попыток загрузки нештатной ОС;
- превышение числа неудачных попыток аутентификации пользователя;
- нарушение целостности Аврора СДЗ;
- нарушение целостности загружаемой программной среды;
- критичные типы сбоев и ошибок.

В Аврора СДЗ реализованы функции безопасности, описание которых приведены в документе «Задание по безопасности» АДМГ.30031-01 94 01.

1.3. Область применения

Аврора СДЗ применяется на аппаратных платформах, поддерживающих спецификацию программного интерфейса взаимодействия с функциями безопасности, встроенными в процессор.

Аврора СДЗ может быть использована, но не ограничиваться, в следующих системах и объектах:

- в государственных информационных системах, не содержащих информации, составляющей государственной тайны, до 1 класса защищенности включительно в соответствии с документом «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденным приказом ФСТЭК России от 11 февраля 2013 г. № 17;

- в информационных системах персональных данных до 1 уровня защищенности включительно в соответствии с документом «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденным приказом ФСТЭК России от 18 февраля 2013 г. № 21;

- в автоматизированных системах управления до 1 класса защищенности включительно в соответствии с документом «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды», утвержденным приказом ФСТЭК России от 14 августа 2014 г. № 31;

– на значимых объектах критической информационной инфраструктуры до 1 категории включительно в соответствии с документом «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», утвержденным приказом ФСТЭК России от 25 декабря 2017 г. № 239.

2. УКАЗАНИЯ ПО ЭКСПЛУАТАЦИИ

2.1. Ограничения по эксплуатации

Для работы с загрузочным модулем Аврора СДЗ требуется 64-битный дистрибутив ОС Linux со следующими установленными программами:

- bash – командный интерпретатор с открытым исходным кодом;
- openssl – криптографическая библиотека с открытым исходным кодом;
- gost-engine – эталонная реализация российских криптоалгоритмов ГОСТ для OpenSSL с открытым исходным кодом;
- sha256sum программа подсчета контрольных сумм (КС), входит в состав пакета GNU Coreutils с открытым исходным кодом;
- «ФИКС 2.0.2» (разработчик ЗАО «ЦБИ-сервис», сертификат соответствия ФСТЭК России № 1548, действителен до 15 января 2025 г.), «Уровень-3», константа по умолчанию.

Для безопасного функционирования Аврора СДЗ следует использовать (подписывать и загружать) только образы ОС, полученные из доверенных источников.

ВНИМАНИЕ! В обязательном порядке необходимо уточнить у производителя платы наличие возможности записи в однократно-программируемую память (efuse).

При выполнении Аврора СДЗ необходимо учитывать следующие особенности:

- Аврора СДЗ блокирует исполнение кода на PCI устройствах;
- Аврора СДЗ блокирует использование сторонних UEFI драйверов;
- Аврора СДЗ блокирует использование сетевого интерфейса во время своей работы.

2.2. Условия выполнения программы

Аврора СДЗ предназначена для функционирования на устройствах на базе процессора Baikal-M BE-M1000 архитектуры ARMv8, отвечающих требованиям профиля «Профиль защиты средства доверенной загрузки уровня базовой системы ввода-вывода четвертого класса защиты ИТ.СДЗ.УБ4.ПЗ», описание и характеристики которых приведены документе «Формуляр» АДМГ.30031-01 30 01.

ВНИМАНИЕ! Содержащиеся в настоящем документе описания сформированы на примере использования платы ET101-MB.

Производителем платы ET101-MB является компания Элпитех (<https://elpitech.ru/upload/iblock/185/wzl7o96j5xty7zh6cjjc8c6008e6p884.pdf>).

Для установки Аврора СДЗ на устройство требуется программатор Olimex ARM-USB-OCD-H (<https://www.olimex.com/Products/ARM/JTAG/ARM-USB-OCD-H>) либо внешний USB-накопитель.

3. ВВОД В ЭКСПЛУАТАЦИЮ

Загрузочные модули Аврора СДЗ содержатся в архиве Aurora_TB_release_1.3-et101_signed.tgz, входящем в комплектность поставки Аврора СДЗ.

ПРИМЕЧАНИЕ. Информация о комплектности поставки Аврора СДЗ приведена в документе «Формуляр» АДМГ.30031-01 30 01.

Распаковка архива осуществляется при помощи соответствующих программ-распаковщиков, которые являются бесплатными, широкодоступными и по умолчанию содержатся в любом современном дистрибутиве ОС Linux. Для распаковки архива и идентификации файлов комплектности поставки необходимо использовать любую современную ОС Linux либо совместимую с таковыми версию ОС.

Описание файлов и папок комплектности поставки после распаковки приведено в таблице (Таблица 1).

Таблица 1

Элемент поставки	Назначение
example-keys	Тестовый набор ключей
omp-signed-images	Загрузочные модули Аврора СДЗ, подписанные ключом предприятия-разработчика
Updater	Приложение для первичной установки Аврора СДЗ с внешнего носителя
Utils	Набор вспомогательных утилит
board-flash-firmware.sh	Утилита прошивки загрузочных модулей Аврора СДЗ на устройство
sign-images.sh	Утилита подписи и формирования образа прошивки
spi.asb.template.layout	Шаблон файла раскладки образа на SPI флэш-памяти
spi.efuse.emul.layout	Раскладка данных эмуляции eFuse на SPI флэш-памяти

3.1. Идентификация комплектности поставки

Идентификация комплектности поставки Аврора СДЗ осуществляется посредством расчета КС загрузочного модуля и файлов после распаковки архива.

Расчет КС файлов возможно осуществлять 2 способами:

– первый способ — с использованием программы «Программа фиксации и контроля исходного состояния программного комплекса «ФИКС 2.0.2» (разработчик ЗАО «ЦБИ-сервис», сертификат соответствия ФСТЭК России № 1548, действителен до 15 января 2025 г.), «Уровень-3», константа по умолчанию. Для этого необходимо:

- выбрать режим «Фиксация версий», статус комплекса «New»;
- в качестве алгоритма выбрать «Уровень-3», код - Const=1 по умолчанию;
- в окне «Контролируемые файлы» выбрать носитель или каталог, содержащий загрузочный модуль;
- нажать кнопку «Пуск»;
- при необходимости подтвердить предложенные программой значения и дождаться завершения процесса;
- сверить получившиеся значения КС с приведенными в документе «Формуляр» АДМГ.30031-01 30 01;

– второй способ — с использованием программы, осуществляющей расчет по алгоритму SHA256. Для этого необходимо:

- с помощью утилиты sha256sum по алгоритму SHA-256 выполнить команду:

```
sha256sum [путь_к_файлу_архива_комплектности_поставки_СДЗ_Аврора.tgz];
```

- сверить получившиеся значения КС с приведенным в документе «Формуляр» АДМГ.30031-01 30 01.

ПРИМЕЧАНИЕ. При выборе второго способа расчета КС необходимо использовать ОС Linux, в которую уже входит консольная программа подсчета КС SHA-256sum.

АДМГ.30031-01 91 01

Расчет КС содержимого каталога, в котором находятся распакованные из архива загрузочные модули Аврора СДЗ, возможно осуществлять 2 способами:

– первый способ — с использованием программы «ФИКС 2.0.2». Для этого необходимо:

- выполнить процедуру, аналогичную описанной выше, относительно носителя или каталога, на котором находятся распакованные файлы из архива комплектности поставки Аврора СДЗ;

- сверить получившиеся значения КС с приведенными в документе «Формуляр» АДМГ.30031-01 30 01;

– второй способ — с помощью утилиты sha256sum по алгоритму SHA-256. Для этого необходимо:

- выполнить команду:

```
sha256sum  
[путь_к_каталогу_с_извлеченными_файлами_комплектности_поставки_СДЗ_Аврора]
```

- сверить получившиеся значения КС с приведенными в документе «Формуляр» АДМГ.30031-01 30 01.

3.2. Описание загрузочных модулей

Загрузочные модули Аврора СДЗ поставляются в бинарном виде и подписываются предприятием-разработчиком.

Для установки на устройство загрузочные модули Аврора СДЗ необходимо подписать:

– модуль SCP — ключом SCP;

– модули BL1, BL2, BL31, BL32, BL33, DTB, VAR, CMD, SBAJ — ключом vendor (Таблица 2).

Таблица 2

Имя модуля	Файлы модуля	Подпись	Назначение
SCP	.scp.flash.bin	– предприятие-разработчик; – SCP	Файл прошивки управляющего процессора
BL1	.bl1.bin	– предприятие-разработчик; – vendor	Файл прошивки загрузчика BL1
BL2	..bl2.bin	– предприятие-разработчик; – vendor	Файл прошивки загрузчика BL2
BL31	.bl31.bin	– предприятие-разработчик; – vendor	Файл прошивки загрузчика BL31
BL32	.tee-header_v2.bin .tee-pageable_v2.bin .tee-pager_v2.bin	– предприятие-разработчик; – vendor	Файлы прошивки Аврора TEE
BL33	.efi.fd	– предприятие-разработчик; – vendor	Файл прошивки UEFI
DTB	.dtb	– предприятие-разработчик; – vendor	Двоичный файл дерева устройств
VAR	.var.fd	– предприятие-разработчик; – vendor	Файл первичной конфигурации Аврора СДЗ
CMD	.cmd.img	vendor	Файл командного пакета
SBAJ	.sbaj	– предприятие-разработчик; – vendor	Файл журнала

ПРИМЕЧАНИЕ. Модуль командного пакета CMD не поставляется предприятием-разработчиком и формируется непосредственно перед установкой или обновлением Аврора СДЗ.

3.3. Описание утилит

1) **Sign-images.sh** — утилита подписи загрузочных модулей Аврора СДЗ и формирования файлов прошивки;

АДМГ.30031-01 91 01

Использование: `./sign-images.sh <цель> <опции>`

Поддерживаемые цели:

tf307	- Системная плата Edelweiss TF-307-MB-S-D
et101	- Системная плата Elpitech ET101-MB
aqbm1000	- Системная плата Aquarius AQBM1000

Опции:

<code>--all</code>	синоним набора опций <code>--scp --bl1 --dtb --var --fip --sbaj</code>
<code>--scp</code>	подпись образа SCP
<code>--bl1</code>	подпись образа BL1
<code>--dtb</code>	подпись образа DTB
<code>--var</code>	подпись образа VAR
<code>--fip</code>	подпись образа FIP
<code>--sbaj</code>	подпись образа SBAJ
<code>--kernel IMAGE</code>	подпись образа ядра Линукс
<code>--initrd IMAGE</code>	подпись образа Initrd
<code>--cmd CMD1 [--cmd CMDN]</code>	сборка и подпись командного пакета
<code>--verbose</code>	подробный вывод

Переменные окружения:

<code>KEYS</code>	переопределить директорию с ключами (по умолчанию <code>example-keys</code>)
<code>RP_IDX_BL=NUM</code>	переопределить значение индекса RP образов
<code>AP_BLx</code> (по умолчанию 0)	
<code>RP_IDX_OS=NUM</code>	переопределить значение индекса RP образов
<code>OS</code> (по умолчанию 0)	

2) **Board-flash-firmware.sh** — утилита прошивки загрузочных модулей

Аврора СДЗ;

Использование: `sudo ./board-flash-firmware.sh <цель> <файл образа> <файл раскладки образа> [<опции>]`

Поддерживаемые цели:

tf307	- Системная плата Edelweiss TF307-MB-S-C
et101	- Системная плата Elpitech ET101-MB
aqbm1000	- Системная плата Aquarius AQBM1000

Поддерживаемые программаторы:

olimex (по умолчанию)	- Программатор Olimex ARM-USB-OCD-H
elpitech	- Программатор Elpitech

Поддерживаемые чипы SPI флеш-памяти:

MT25QU256	
W25Q256.W	(по умолчанию)

Опции:

<code>--programmer PROGRAMMER</code>	задать программатор
<code>--chip CHIP</code>	задать чип SPI флеш-памяти
<code>--erase-efuse</code>	очистка региона efuse на SPI (только для тестовых прошивок)

3) **Utils/cmd-gen** — генератор команд SCP.

Использование:

Генерация команды инициализации корневого публичного vendor ключа:

```
cmd-gen --vrootkinit --pubk FILE.PUBK --key FILE.PRVK --output FILE.OUT
```

Генерация команды инициализации публичного vendor ключа:

```
cmd-gen --vkinit --pubk FILE.PUBK --key FILE.PRVK --output FILE.OUT
```

Генерация команды инвалидации публичного vendor ключа:

```
cmd-gen --vkinv --pubk FILE.PUBK --key FILE.PRVK --output FILE.OUT
```

Генерация команды установки RP индекса:

```
cmd-gen --rpset --rpgrp GRP --rpidx IDX --key FILE.PRVK --output FILE.OUT
```

Генерация команды установки HUK:

```
cmd-gen --hukset --huk HEX --output FILE.OUT
```

Генерация команды инициализации SCP ключа (включение доверенной загрузки):

```
cmd-gen --sbooten --pubk FILE.PUBK --output FILE.OUT
```

Где:

FILE.PUBK	файл публичного ключа
FILE.PRVK	файл приватного ключа
FILE.OUT	выходной файл
GRP	номер группы RP (0 - AP_BLx, 1 - OC)
IDX	индекс группы RP
HEX	значение ключа HUK в шестнадцатеричном формате 0123456789ABCDEF (32 символа)

4. ПОРЯДОК УСТАНОВКИ ЗАГРУЗОЧНЫХ МОДУЛЕЙ НА УСТРОЙСТВО

ПРИМЕЧАНИЕ. Для последующих обновлений Аврора СДЗ этапы формирования ключевой информации и формирования команд активации Аврора СДЗ могут быть пропущены.

4.1. Формирование ключевой информации

Формирование ключевой информации производится при помощи библиотеки OpenSSL, а также расширения для нее — gost-engine, реализующего набор криптографических алгоритмов по стандарту ГОСТ.

Для формирования первичной ключевой информации необходимо выполнить следующие действия:

- подготовить директории для ключей с помощью команды:

```
mkdir -p keys  
cd keys
```

- сгенерировать ключ SCP с помощью команды:

```
openssl genpkey -algorithm gost2012_256 -pkeyopt paramset:A -out  
keys/scp.key
```

- экспортировать публичный ключ SCP с помощью команды:

```
openssl pkey -pubout -in keys/scp.key -out keys/scp-pubk.key
```

- сгенерировать ключ vendor с помощью команды:

```
openssl genpkey -algorithm gost2012_256 -pkeyopt paramset:A -out  
keys/vendor.key
```

- экспортировать публичный ключ vendor с помощью команды:

```
openssl pkey -pubout -in keys/vendor.key -out keys/vendor-pubk.key
```

- сгенерировать ключ ОС с помощью команды:

```
openssl genpkey -algorithm gost2012_256 -pkeyopt paramset:A -out  
keys/image.key
```

- экспортировать публичный ключ ОС с помощью команды:

```
openssl pkey -pubout -in keys/image.key -out keys/image-pubk.key
```

- создать сертификат vendor (для подписи сертификата ОС) с помощью команды:

```
openssl req -x509 -days 1095 -key keys/vendor.key --out  
keys/vendor_cert.pem
```

- создать запрос на подпись сертификата ОС с помощью команды:

```
openssl req -new -key keys/image.key -out keys/image_cert_req.pem
```

- подписать сертификат ОС ключом vendor с помощью команды:

```
openssl x509 -req -in keys/image_cert_req.pem -days 1095 -CA  
keys/vendor_cert.pem -CAkey keys/vendor.key -CAcreateserial -outform  
DER -out keys/image_cert.der
```

- разместить публичный ключ предприятия-разработчика рядом с остальными ключами с помощью команды:

```
cp example-keys/omp-pubk.key keys/
```

ПРИМЕЧАНИЕ. Необходимо обеспечить безопасность процесса формирования, хранения и эксплуатации ключевой информации. Безопасность ключевой информации может быть обеспечена совокупностью организационных и технических мер эксплуатанта.

4.2. Формирование команд активации Аврора СДЗ

Аврора СДЗ активируется с момента размещения корня доверия в eFuse. Корень доверия состоит из ключа SCP и корневого ключа vendor. Для размещения ключей на eFuse необходимо сформировать соответствующие команды для SCP, собрать, подписать командный пакет и прошить его на устройство одновременно с образом SCP при помощи программатора или USB обновления поверх предустановленного Baikal SDK версии 5.6 или выше. При первом включении SCP вычитает командный пакет и после успешной верификации применит команды из пакета.

Для формирования SCP команд инициализации корня доверия необходимо выполнить следующие действия:

- сгенерировать команду инициализации SCP ключа с помощью команды:

```
./utils/cmd-gen --sbooten --pubk keys/scp-pubk.key --output  
sbooten.cmd
```

- сгенерировать команду инициализации корневого ключа vendor с помощью команды:

```
./utils/cmd-gen --vrootkinit --pubk keys/vendor-pubk.key --key  
keys/scp.key --output vrootkeyinit.cmd
```

Сборка и подпись командного пакета осуществляется в процессе подписи загрузочных модулей Аврора СДЗ.

ПРИМЕЧАНИЕ. При первичной установке Аврора СДЗ можно пропустить внесение корневого ключа vendor. В таком случае необходимо подписать все образы ключом SCP. Корневой ключ vendor можно будет внести позднее (пп. 6.1.3.1).

4.3. Подпись загрузочных модулей Аврора СДЗ

При первичной установке Аврора СДЗ необходимо подписать все загрузочные модули ключом vendor, а также сформировать командный пакет с командами активации Аврора СДЗ.

Пример команды подписи всех загрузочных модулей Аврора СДЗ ключами из директории «keys», сформированными в соответствии с подразделом 4.1, включая командный пакет с командами активации Аврора СДЗ для платы ET-101:

```
KEYS=keys ./sign-images.sh et101 --scp --bl1 --dtb --var --fip --sbaj  
--cmd sbooten.cmd --cmd vrootkeyinit.cmd  
Подписывается SCP...  
Образ SCP подписан ключом SCP  
Версия: v1.0-58-gcf657f1  
  
Подписывается DTB...  
Образ DTB подписан ключами ОМП и vendor  
Версия: v5.4.197+sdk-5.6+omp1-1-gf116d12e7  
  
Подписывается VAR...
```

Образ VAR подписан ключами ОМП и vendor
Версия: edk2-202211+sdk-5.8+omp1/0.0.0.0+454

Подписывается SBAJ...

Образ SBAJ подписан ключами ОМП и vendor

Версия: 0

Подписывается TF-A BL2...

Образ TF-A BL2 подписан ключами ОМП и vendor

Версия: v2.8+sdk-5.8+omp1+15

Подписывается TF-A BL31...

Образ TF-A BL31 подписан ключами ОМП и vendor

Версия: v2.8+sdk-5.8+omp1+15

Подписывается Aurora TEE BL32 Header...

Образ Aurora TEE BL32 Header подписан ключами ОМП и vendor

Версия: 3.16.0+omp2

Подписывается Aurora TEE BL32 E1...

Образ Aurora TEE BL32 E1 подписан ключами ОМП и vendor

Версия: 3.16.0+omp2

Подписывается Aurora TEE BL32 E2...

Образ Aurora TEE BL32 E2 подписан ключами ОМП и vendor

Версия: 3.16.0+omp2

Подписывается UEFI BL33...

Образ UEFI BL33 подписан ключами ОМП и vendor

Версия: edk2-202211+sdk-5.8+omp1/0.0.0.0+454

Подписывается TF-A BL1...

Образ TF-A BL1 подписан ключами ОМП и vendor

Версия: v2.8+sdk-5.8+omp1+15

В процессе подписи отображаются версии загрузочных модулей Аврора СДЗ, которые после установки и загрузки Аврора СДЗ можно сверить в подразделе 6.6. Также на этом шаге проверяется, что файлы образов подписаны предприятием-разработчиком, и производится подпись файлов vendor-ключами заказчика.

ПРИМЕЧАНИЕ. При обновлении необходимо подписать только обновляемые модули.

4.4. Установка загрузочных модулей

Установка загрузочных модулей Аврора СДЗ на устройство возможна 2 способами:

- с использованием программатора;
- с использованием внешнего USB-накопителя.

4.4.1. Установка с использованием программатора

Для установки загрузочных модулей Аврора СДЗ на устройство с использованием программатора необходимо выполнить следующую последовательность действий:

- проверить, что устройство обесточено;
- подключить программатор к устройству;
- выполнить подключение к консоли UART при помощи терминальной программы;
- подать питание на устройство;
- в консоли UART ввести команды:

```
>: pins bootseq  
>: pins cpu_off
```

- в терминале ОС выполнить команду прошивки устройства. Пример команды для платы ET-101:

```
sudo ./board-flash-firmware.sh et101 out/et101/et101.full.img  
out/et101/et101.image.layout
```

ПРИМЕЧАНИЕ. На плате ET-101 могут быть установлены различные чипы SPI флеш-памяти: MT25QU256 или W25Q256.W. В случае если команда прошивки выдает ошибку, необходимо запустить команду с указанием чипа SPI флеш-памяти, отличного от заданного по умолчанию:

```
sudo ./board-flash-firmware.sh et101 out/et101/et101.full.img  
out/et101/et101.image.layout --chip MT25QU256
```

- по окончании прошивки в консоли UART выполнить команду:

```
>: pins board_off
```

4.4.2. Установка с использованием внешнего USB-накопителя

ПРИМЕЧАНИЕ. Установка с использованием внешнего USB-накопителя возможна только поверх предустановленной Baikal SDK версии не ранее 5.6 или поверх уже установленной Аврора СДЗ.

Для установки загрузочных модулей Аврора СДЗ на устройство с использованием внешнего USB-накопителя необходимо выполнить следующую последовательность действий:

- подготовить USB-накопитель с разделом в формате FAT32 и наличием свободного места не менее 100 МБ. Пример команды:

```
sudo mkfs.vfat /dev/sdX
```

- скопировать на USB-накопитель установочные файлы Аврора СДЗ, сформированные в соответствии с п. 4.4.1. Пример команды для ОС Linux и устройства ET-101:

```
cp -r out/et101/USB/EFI/ <точка монтирования /dev/sdX>
```

- включить устройство для установки Аврора СДЗ и подключить к нему подготовленный USB-накопитель;

- по окончании процесса загрузки UEFI зайти в меню UEFI при помощи кнопки «Esc»;

- в разделе «Boot Options» выбрать подключенный USB накопитель;

- по окончании процесса установки Аврора СДЗ выполнить перезагрузку устройства.

4.5. Примеры обновления загрузочных модулей

4.5.1. Пример обновления Аврора СДЗ с новым индексом RP

Для обновления Аврора СДЗ с новым индексом RP необходимо выполнить следующие действия:

1) Сгенерировать команду установки индекса RP загрузочных модулей AP_BLx с помощью команды:

```
./utils/cmd-gen --rpset --rpgrp 0 --rpidx 1 --key example-  
keys/vendor.key --output rpset_bl_1.cmd
```

2) Подписать все AP_BLx группы RP 1 загрузочных модулей Аврора СДЗ и установки индекса RP AP_BLx в 1 с помощью команды:

```
RP_IDX_BL=1 ./sign-images.sh et101 --scp --bl1 --dtb --var --fip --  
sbaj --cmd rpset_bl_1.cmd
```

3) Обновить загрузочные модули, выполнив следующие действия:

– при помощи программатора выполнить команду:

```
sudo ./board-flash-firmware.sh et101 out/et101/et101.full.img  
out/et101/et101.image.layout
```

– через интерфейс Аврора СДЗ выполнить следующие действия:

- скопировать на USB-носитель файлы out/et101/et101.full.img и out/et101/et101.image.layout;
- подключить USB-носитель с файлами обновлений к обновляемому устройству с Аврора СДЗ;
- запустить устройство с Аврора СДЗ, перейти в конфигуратор, затем в раздел «Обновление Аврора СДЗ»;
- выбрать файл обновления с USB носителя et101.image.layout;
- запустить обновление;
- по окончании процесса перезагрузить устройство.

4.5.2. Пример обновления индекса RP ОС

Для создания образа обновления, включающего только команду установки индекса RP ОС, необходимо выполнить следующие действия:

1) Сгенерировать команду установки индекса RP образов ОС с помощью команды:

```
./utils/cmd-gen --rpset --rpgrp 1 --rpidx 1 --key example-  
keys/vendor.key --output rpset_os_1.cmd
```

2) Подписать ядра Linux с группой RP 1 и установки индекса RP ОС в 1 с помощью команды:

```
RP_IDX_OS=1 ./sign-images.sh et101 --kernel <путь к файлу ядра ОС> --  
initrd <путь к файлу initrd> --cmd rpset_os_1.cmd
```

- установить индекс RP ОС с помощью интерфейса обновления Аврора СДЗ:
 - скопировать на USB-носитель файлы out/et101/et101.full.img и out/et101/et101.image.layout;
 - подключить USB-носитель с файлами обновлений к обновляемому устройству с Аврора СДЗ;
 - запустить устройство с Аврора СДЗ, перейти в configurator и далее в раздел «Обновление Аврора СДЗ»;
 - выбрать файл обновления с USB-носителя et101.image.layout;
 - запустить обновление;
 - по окончании процесса перезагрузить устройство.

5. ПОДПИСЬ ЯДРА LINUX

После установки Аврора СДЗ и включения доверенной загрузки (п. 6.1.1) устройство будет загружать только подписанные ядра Linux. Использование промежуточных загрузчиков типа GRUB исключено, ядро должно быть собрано с опцией CONFIG_EFI_STUB. Ядро Linux и его подпись необходимо размещать на загрузочном FAT разделе внешнего носителя.

5.1. Подпись ядра Linux

Для подписи ядра Linux необходимо использовать утилиту sign-images из комплектности поставки.

Пример команды подписи файла ядра image.bin с индексом RP 0 с использованием ключей из примеров для платы et101:

```
./sign-images.sh et101 --kernel image.bin
...
Подписывается Kernel...
Образ Kernel подписан ключом ОС

*****
* Результат *
*****
Файл образа ядра Линукс:
.../delivery_set/image.bin
Файл подписи образа ядра Линукс:
.../delivery_set/image.bin.sign
```

Подпись будет записана в отдельный файл image.bin.sign, который необходимо разместить на устройстве рядом с файлом ядра image.bin.

5.2. Подпись initrd

Для подписи собственного initrd необходимо использовать утилиту sign-images из комплектности поставки.

Пример команды подписи файла ядра initrd.img с индексом RP 0 с использованием ключей из примеров для платы et101:

```
./sign-images.sh et101 --initrd initrd.img
...
```

Подписывается Initrd...
Образ Initrd подписан ключом ОС

```
*****
* Результат *
*****
Файл образа Initrd:
.../delivery_set/initrd.img
Файл подписи образа Initrd:
.../delivery_set/initrd.img.sign
```

Подпись будет записана в отдельный файл initrd.sign, который необходимо разместить на устройстве рядом с файлом initrd.

5.3. Подпись ядра Linux и initrd из поставки предприятия-разработчика

Комплектность поставки Аврора СДЗ может содержать тестовое ядро Linux и образ initrd. Такое ядро содержит функции для работы с Аврора ТЕЕ и используется с целью тестирования Аврора СДЗ.

Пример команды подписи ядра Linux предприятия-разработчика для платы et101:

```
./sign-images.sh et101 --initrd omp-signed-images/et101/initrd --
kernel omp-signed-images/et101/et101.Image.gz
...
*****
* Результат *
*****
Файл образа ядра Линукс: /delivery_set/omp-signed-
images/et101/et101.Image.gz
Файл подписи образа ядра Линукс: /delivery_set/omp-signed-
images/et101/et101.Image.gz.sign
Файл образа Initrd: /delivery_set/omp-signed-images/et101/initrd
Файл подписи образа Initrd: /delivery_set/omp-signed-
images/et101/initrd.sign
```

6. ВЫПОЛНЕНИЕ ПРОГРАММЫ

Для входа в систему необходимо нажать клавишу «Esc» во время отображения экрана загрузки (Рисунок 1).

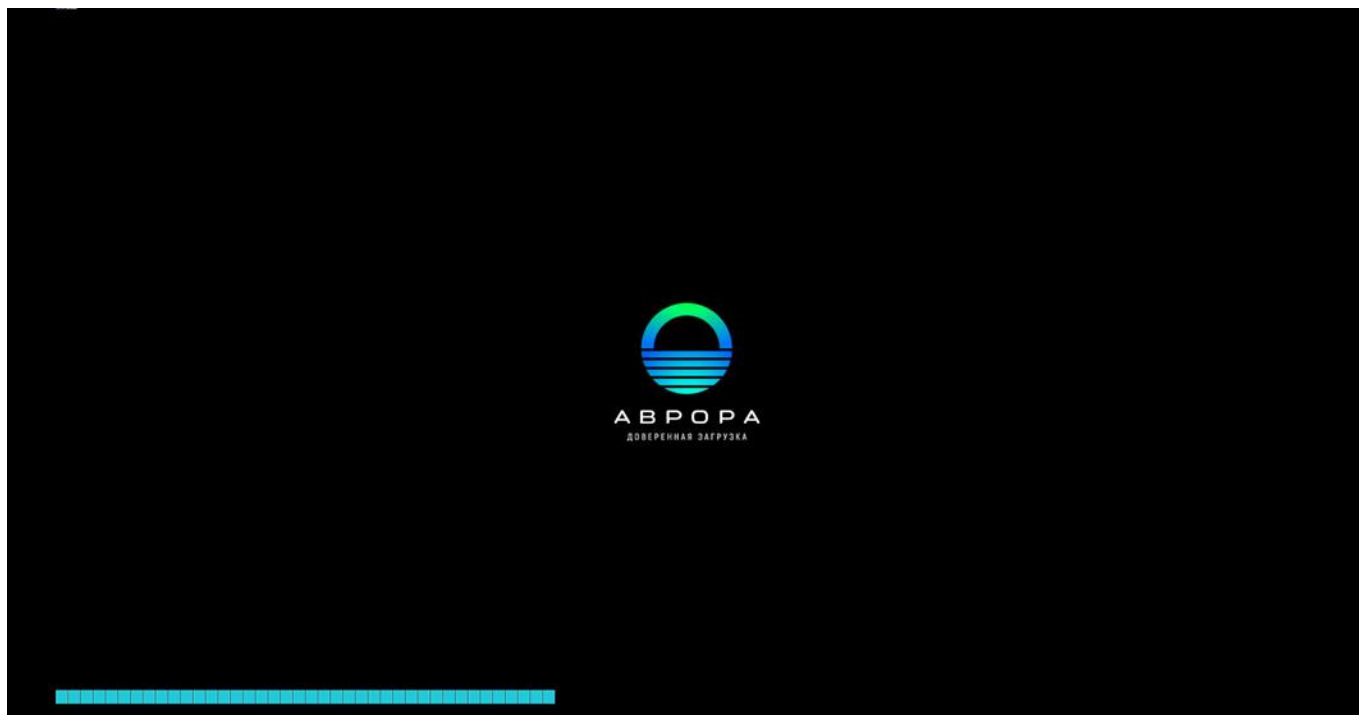


Рисунок 1

На экране входа (Рисунок 2) возможно выбрать следующие опции:

- «Конфигуратор Аврора СДЗ»;
- «Продолжить загрузку»;
- «Перезагрузить».



Рисунок 2

Опция «Конфигуратор Аврора СДЗ» осуществляет доступ к настройкам СДЗ после авторизации администратора.

Опция «Продолжить загрузку» осуществляет загрузку ОС по умолчанию после авторизации пользователя (если авторизация включена).

Опция «Перезагрузить» перезагружает устройство с Аврора СДЗ.

Для входа в настройки СДЗ (Рисунок 3) необходимо выполнить следующие действия:

- выбрать пункт «Конфигуратор Аврора СДЗ»;
- ввести имя пользователя и пароль администратора в соответствующие поля;
- выбрать пункт «Продолжить».

ПРИМЕЧАНИЯ:

- ✓ При первичном входе в систему доступен только 1 пользователь — администратор с именем «admin» и паролем «Admin123»;
- ✓ Потребуется выполнить смену пароля данного пользователя, т.к. изначально пароль считается истекшим.

Аутентификация Аврора СДЗ

Пользователь:

Пароль:

Введите имя пользователя (с учётом регистра)

▶ Продолжить

▶ Смена истекшего пароля

↑↓=Перемещаться <Enter>=Выбрать Esc=Выйти

Рисунок 3

Для смены пароля пользователя администратору необходимо выполнить следующие действия (см. Рисунок 3):

- выбрать «Смена истекшего пароля»;
- нажать кнопку «Enter»;
- в отобразившемся окне (Рисунок 4) в соответствующие поля ввести следующие данные:
 - имя пользователя, для которого необходимо сменить пароль;

- старый пароль;
- новый пароль.

По умолчанию к паролю выставляются следующие требования:

- минимальная длина пароля — 8 символов;
- должен содержать цифры;
- должен содержать буквы в нижнем и верхнем регистре.

ПРИМЕЧАНИЕ. Возможность смены данных метрик приведена в разделе 6.1.2;

The screenshot shows a terminal-style interface for changing a password. At the top, a blue header bar contains the title 'Смена истекшего пароля'. Below this, on a grey background, are labels for 'Пользователь:', 'Старый пароль:', and 'Новый пароль:', each followed by a black rectangular input field. To the right of these fields, blue text reads 'Введите имя пользователя (с учётом регистра)'. Below the input fields is a blue arrow icon followed by the text 'Продолжить'. At the bottom, a black bar contains three white text labels: '↑↓=Перемещаться', '<Enter>=Выбрать', and 'Esc=Выйти'.

Рисунок 4

- нажать «Продолжить», в результате чего в случае успешной смены пароля отобразится соответствующее сообщение (Рисунок 5);
- нажать кнопку «Enter».

Смена истекшего пароля

Пользователь: admin

Старый пароль:

Новый пароль:

▶ **Продолжить**

Продолжить вход в
Конфигуратор Аврора СДЗ

Пароль изменен успешно
Нажмите ENTER для продолжения...

↑↓=Перемещаться <Enter>=Выбрать Esc=Выйти

Рисунок 5

После смены пароля администратор может авторизоваться, введя имя пользователя «admin» в поле «Пользователь», новый пароль в поле «Пароль» и нажав «Продолжить» (Рисунок 6), в результате чего отобразится основной экран системы (Рисунок 7).

Аутентификация Аврора СДЗ		
Пользователь:	admin	Продолжить вход в Конфигуратор Аврора СДЗ
Пароль:		
▶ Продолжить ▶ Смена истекшего пароля		
↑↓=Перемещаться <Enter>=Выбрать Esc=Выйти		

Рисунок 6



Рисунок 7

6.1. Экран «Параметры»

Экран «Параметры Аврора СДЗ» (Рисунок 8) позволяет включить или выключить доверенную загрузку, а также содержит формы, необходимые для настройки Аврора СДЗ.



Рисунок 8

6.1.1. Включение/выключение доверенной загрузки

Для включения/выключения доверенной загрузки необходимо выполнить следующие действия:

- после входа в систему на главном экране выбрать пункт «Параметры»;
- установить/снять чекбокс «Включить Доверенную Загрузку» (Рисунок 8).

При снятом чекбоксе, при загрузке любого варианта загрузки (подраздел 6.9), будет появляться сообщение «Внимание! Доверенная загрузка отключена» с обратным отсчетом времени отображения сообщения - 10 секунд (Рисунок 9).

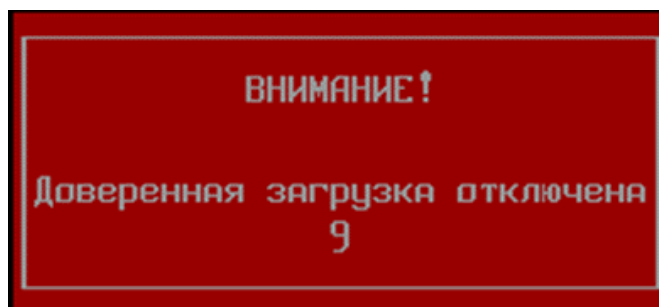


Рисунок 9

6.1.2. Параметры идентификации и аутентификации

Экран «Параметры Идентификации и Аутентификации» приведен на рисунке (Рисунок 10).

Параметры Идентификации и Аутентификации		
Требуется идентификация	[1]	Запрашивать имя пользователя при загрузке ОС
Минимальная длина пароля администратора	[8]	
Минимальная длина пароля пользователя	[4]	
Максимальное количество неудачных попыток входа	[10]	
Срок действия пароля	[30]	
Срок автоблокировки администраторов	[1]	
Парольная политика	<Цифры и буквы в нижнем и верхнем регистре>	
Сохранить изменения и выйти		
Отклонить изменения и выйти		

↑↓=Перемещаться	F9=Сбросить к умолчаниям <Spacebar>Сменить значение	F10=Сохранить Esc=Выйти
-----------------	--	----------------------------

Рисунок 10

Экран «Параметры Идентификации и Аутентификации» позволяет настроить приведенные в таблице (Таблица 3) параметры входа в систему для пользователей и администраторов.

Таблица 3

Название	Описание	Состояние по умолчанию
Требуется идентификация	Параметр указывает, требуется ли от пользователя ввод имени пользователя для загрузки рабочей ОС	Отключен
Требуется аутентификация	Параметр указывает, требуется ли от пользователя ввод пароля в дополнение к имени пользователя. Требуется активации параметра «Требуется Идентификация»	Отключен
Минимальная длина пароля администратора	Параметр контролирует минимальную длину пароля для пользователей с ролью «администратор»	8 символов (допустимые значения от 1 до 127)
Минимальная длина пароля пользователя	Параметр контролирует минимальную длину пароля для пользователей с ролью «пользователь»	4 символа (допустимые значения от 1 до 127)
Максимальное количество неудачных попыток входа	Параметр контролирует количество попыток, которые предоставляются пользователю для входа в систему, а также при попытке загрузки рабочей ОС в случае включенной аутентификации	10 попыток (допустимые значения от 10 до 255)
Срок действия пароля	Параметр контролирует время действия паролей в днях	30 дней (допустимые значения от 1 до 120)
Срок автоблокировки администраторов	Инструмент настройки Аврора СДЗ, который в случае превышения попыток входа в систему контролирует время блокировки администраторов	1 день (допустимые значения от 1 до 120)
Парольная политика	Параметр позволяет выбрать минимальный набор символов, которые должны присутствовать в каждом пароле	Возможные опции: — «Цифры» — пароль должен обязательно содержать цифры от 0 до 9; — «Цифры и буквы в нижнем регистре» — пароль должен

Название	Описание	Состояние по умолчанию
		обязательно содержать цифры от 0 до 9, а также латинские буквы в нижнем регистре; –«Цифры и буквы в нижнем и верхнем регистре» — пароль должен обязательно содержать цифры от 0 до 9, а также латинские буквы в нижнем и верхнем регистре (значение по умолчанию); –«Цифры, буквы в нижнем и верхнем регистре, специальные символы и знаки пунктуации» — пароль должен обязательно содержать цифры от 0 до 9, латинские буквы в нижнем и верхнем регистре, а также специальные символы или знаки пунктуации

6.1.3. Управление ключевой информацией

Экран «Управление Ключевой Информацией» (Рисунок 11) позволяет выбрать команды для выполнения следующих действий:

- внесение корневого публичного ключа (пп. 6.1.3.1);
- внесение публичного ключа (пп. 6.1.3.2);
- инвалидация публичного ключа (пп. 6.1.3.3);
- просмотр информации о ключах и индексах Rollback Prevention (RP) (п. 4.5.1).



Рисунок 11

6.1.3.1. Внесение корневого публичного ключа

Для внесения корневого публичного ключа необходимо выполнить следующие действия:

– выбрать пункт «Внести Корневой Публичный Ключ Используя Файл» (Рисунок 12), в результате чего будет предоставлен выбор внешнего носителя (формат FAT32), с которого необходимо получить файл команды;



Рисунок 12

- выбрать внешний носитель, а затем желаемый файл команды внесения корневого публичного ключа в файловой системе носителя (Рисунок 13, Рисунок 14);
- нажать «Выполнить командный файл и выйти» для выполнения файла команды.

Для выхода без внесения корневого публичного ключа выбрать пункт «Выйти без выполнения командного файла».

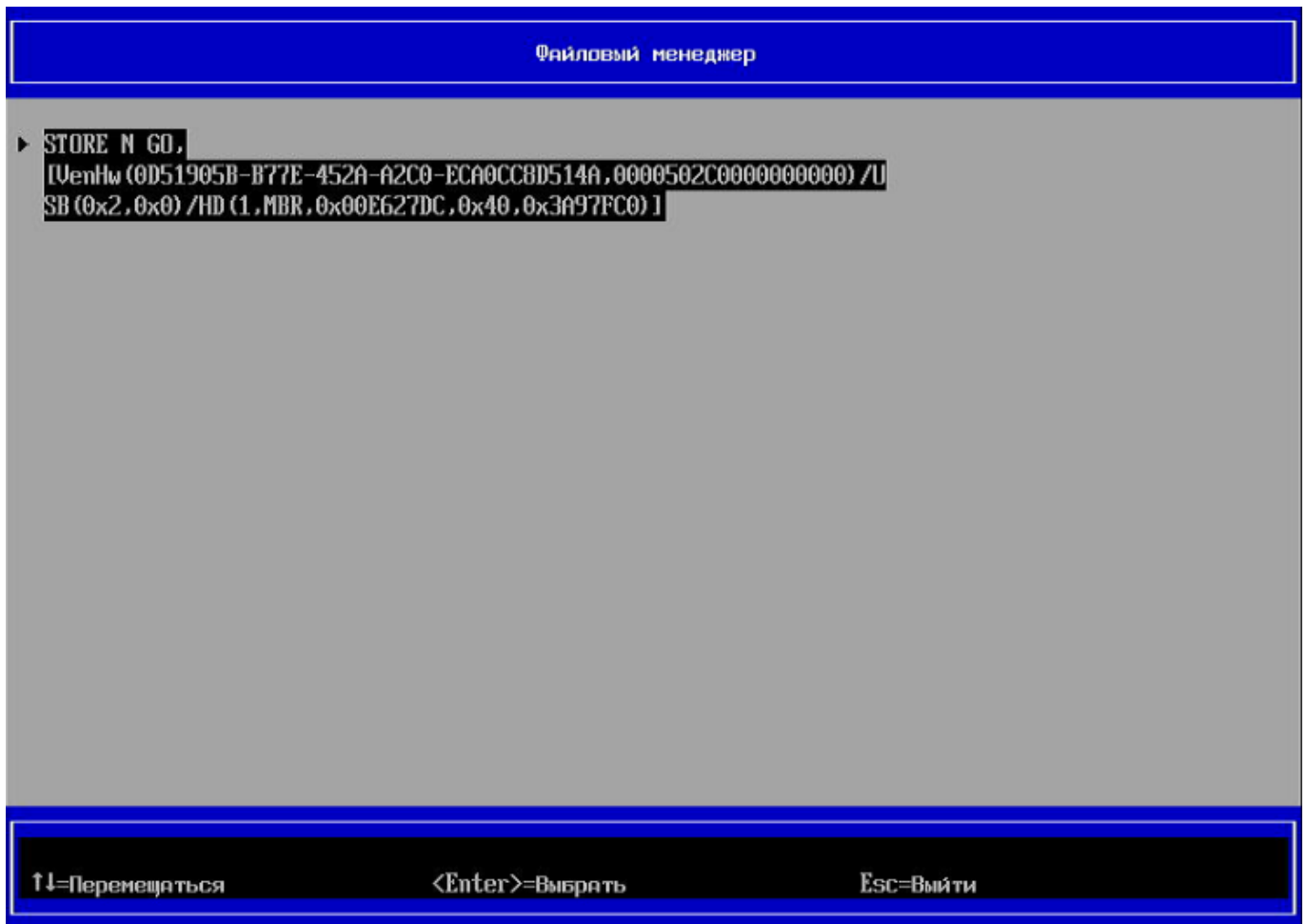


Рисунок 13

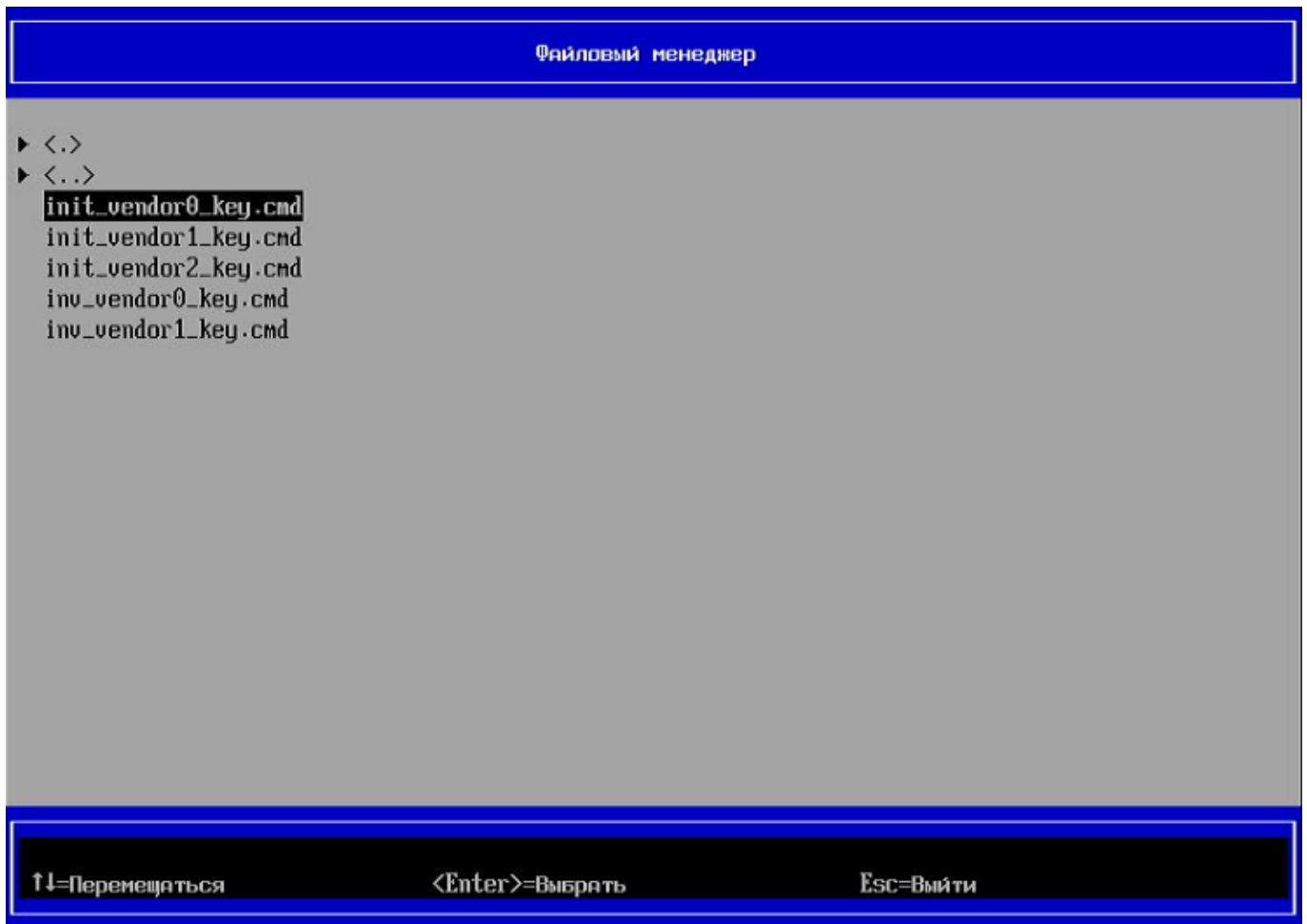


Рисунок 14

6.1.3.2. Внесение публичного ключа

Экран «Внесение Публичного Ключа» идентичен экрану «Внесение Корневого Публичного ключа», однако применяется для ключей 1 и 2, вместо ключа 0.

Для внесения публичного ключа необходимо выполнить следующие действия:

- внести необходимый корневой публичный ключ (пп. 6.1.3.1);
- выбрать пункт «Внесение Публичного Ключа»;
- выбрать пункт «Внести Публичный Ключ Используя Файл» (Рисунок 15);
- выбрать внешний носитель, а затем желаемый файл команды внесения публичного ключа в файловой системе носителя;
- нажать «Выполнить командный файл и выйти» для выполнения файла команды.

Для выхода без внесения публичного ключа выбрать пункт «Выйти без выполнения командного файла».



Рисунок 15

6.1.3.3. Инвалидация публичного ключа

Экран «Инвалидация Публичного Ключа» используется для отключения публичных ключей с помощью командных файлов.

Для инвалидации публичного ключа необходимо выполнить следующие действия:

- выбрать пункт «Инвалидация Публичного Ключа»;
- выбрать пункт «Инвалидировать Публичный Ключ Используя Файл»

(Рисунок 16);

– выбрать внешний носитель, а затем желаемый файл команды инвалидации публичного ключа в файловой системе носителя;

– нажать «Выполнить командный файл и выйти» для выполнения файла команды.

Для выхода без инвалидации публичного ключа выбрать пункт «Выйти без выполнения командного файла».

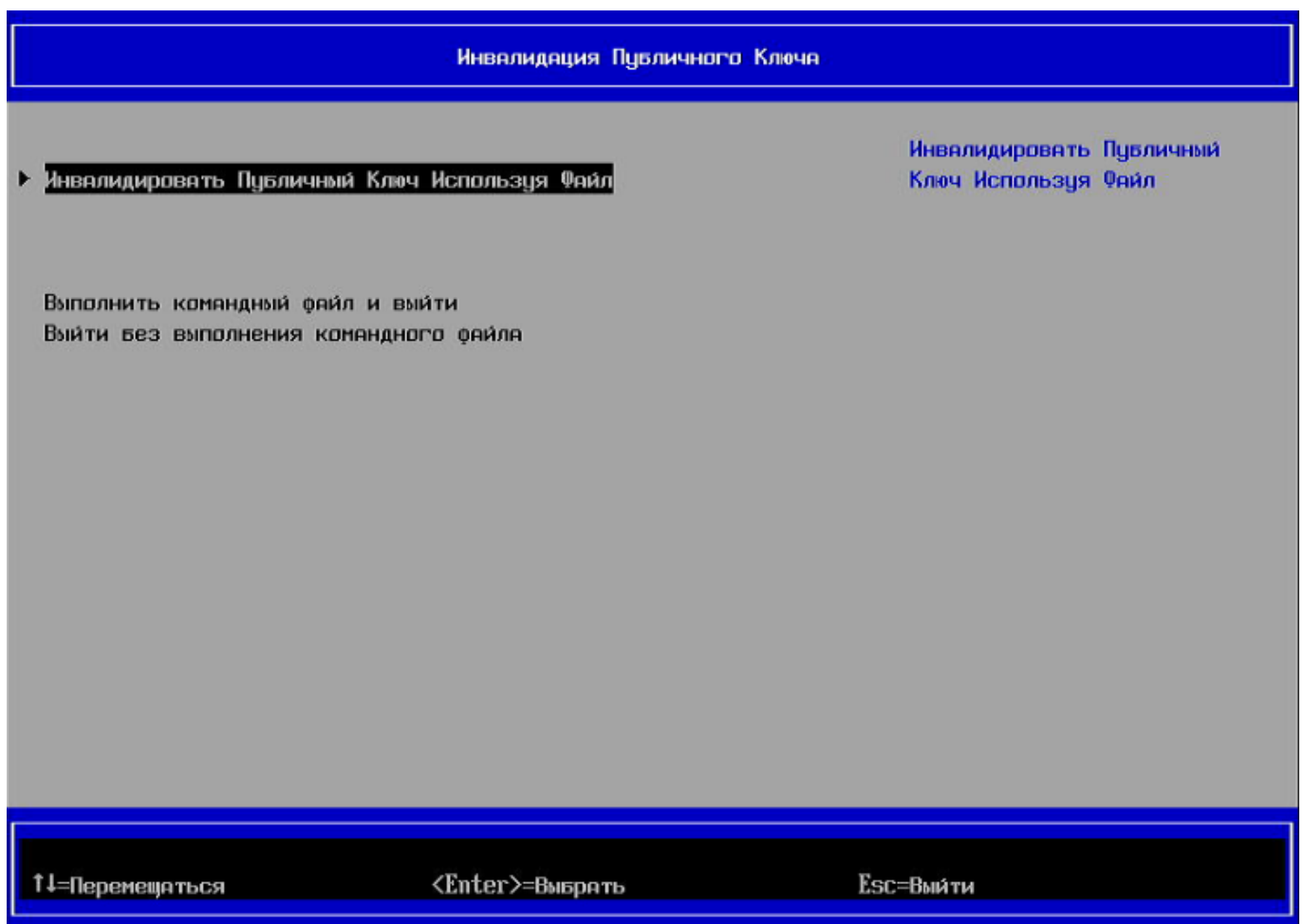


Рисунок 16

6.1.3.4. Ключевая информация

Экран «Ключевая Информация» отображает хэши и состояние публичных ключей, а также индексы RP (Рисунок 17, Рисунок 18).

Ключевая Информация	
Ключ SCP	Используется
Хеш:	3E14CA20F5D2ED50 29C6443E67981B87 D97DFD81DCF41C30 B28A7701934F8078
Ключ 0	Используется
Хеш:	58BCDF5FF817B0D5 B4F55E305E81F086 CAFC58FE8CDB8CA7 1A25FBE1EA7960AC
Ключ 1	Не используется
Хеш:	C6ED03DCB68D9C65 EBEB3F54FA1D5F4D CEA988CD67442F11 462948B67AD02EE1
Ключ 2	Используется
Хеш	064898D629278767

↑↓=Перемещаться Esc=Выйти

Рисунок 17

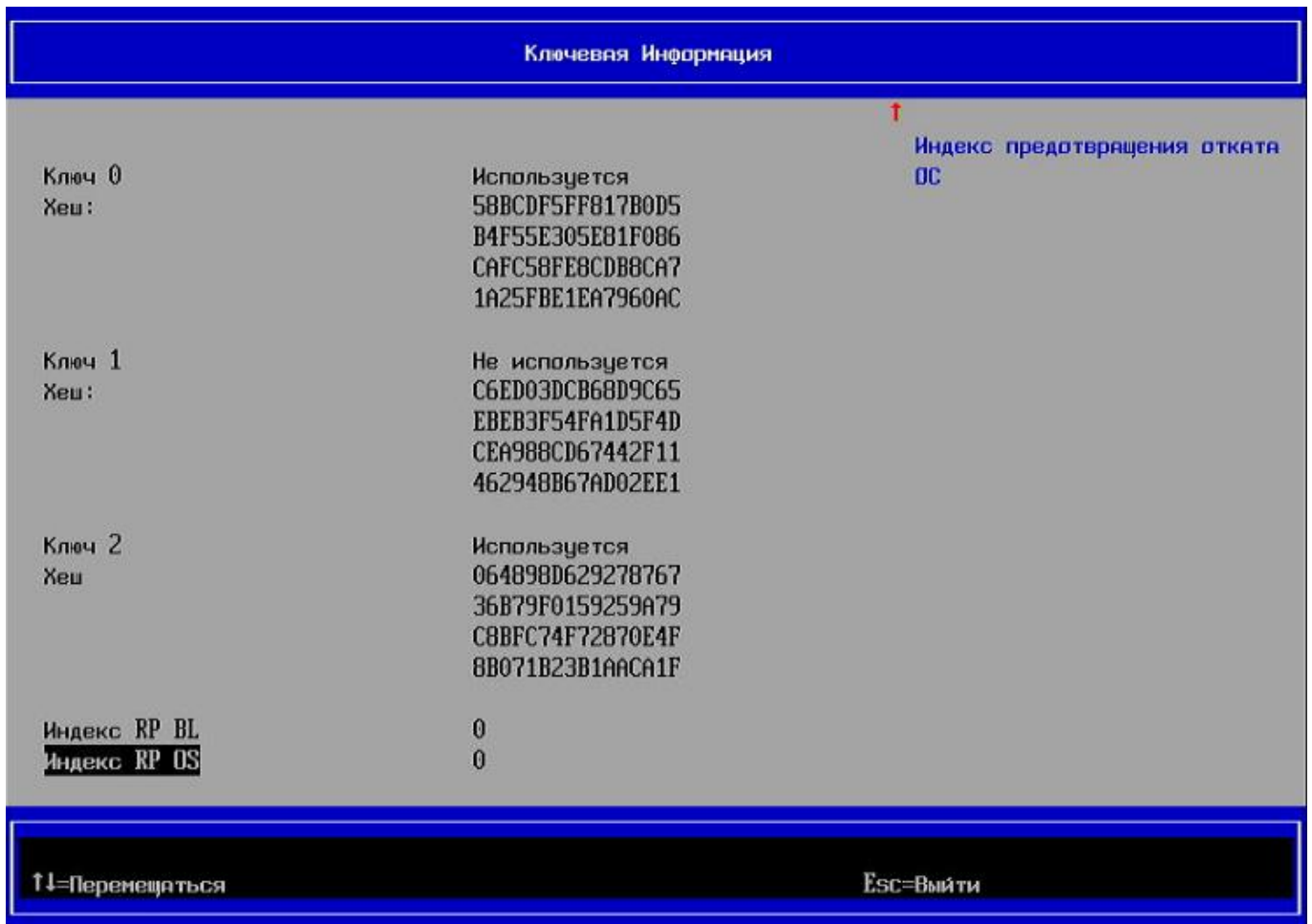


Рисунок 18

6.1.4. Управление доверенной меткой времени

Экран «Управление Доверенной Меткой Времени» (Рисунок 19) позволяет изменить время и дату, сохраненные в системе.

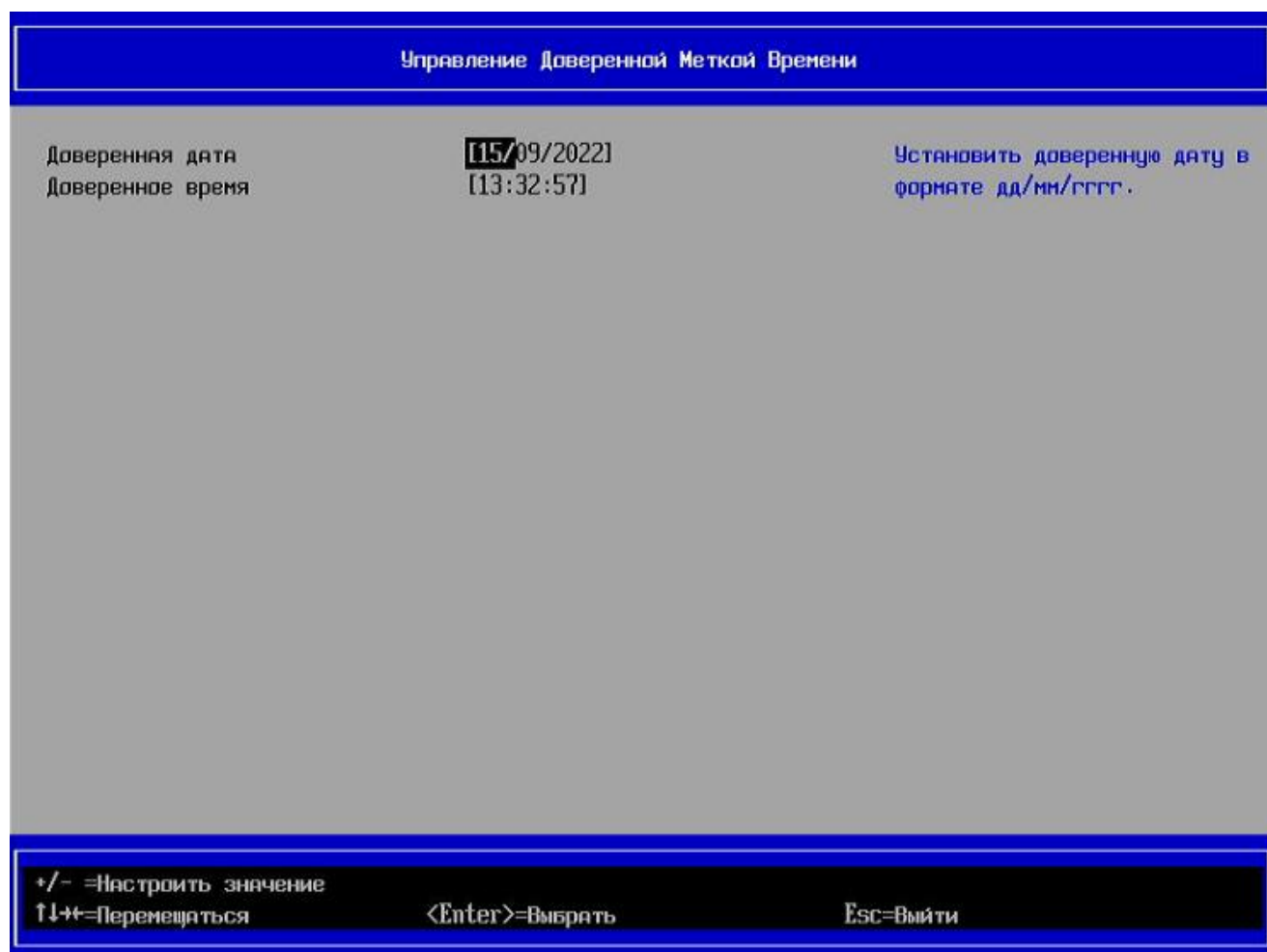
В текущей реализации отсутствует возможность изолировать доверенную метку времени от доступа из ОС. Уровень доверия к метке времени соответствует уровню доверия к ОС.

Для изменения метки даты и времени необходимо выполнить следующие действия:

- после входа в систему на главном экране выбрать пункт «Параметры» (см. Рисунок 7);
- на экране «Параметры» выбрать «Управление Доверенной Меткой Времени» (см. Рисунок 8);

– в полях «Доверенная дата» и «Доверенное время» выставить желаемую дату и время.

ПРИМЕЧАНИЕ. Метка времени сохранится сразу после ввода.



Управление Доверенной Меткой Времени		
Доверенная дата	[15/09/2022]	Установить доверенную дату в формате дд/мм/гггг.
Доверенное время	[13:32:57]	

+/- =Настроить значение
↑↓←→=Перемещаться <Enter>=Выбрать Esc=Выйти

Рисунок 19

6.2. Экран «Пользователи»

Экран «Пользователи Аврора СДЗ» (Рисунок 20) позволяет:

- совершать действия над списком пользователей Аврора СДЗ (п. 6.2.1);
- создавать пользователей Аврора СДЗ (п. 6.2.2).



Рисунок 20

6.2.1. Действия над пользователем

Для выполнения действий над пользователем необходимо на экране «Список Пользователей» (Рисунок 21) выбрать имя пользователя и нажать кнопку «Enter».

На появившемся экране «Просмотр пользователя» (Рисунок 22) доступны следующие действия:

- сменить пароль;
- заблокировать пользователя;
- удалить пользователя.

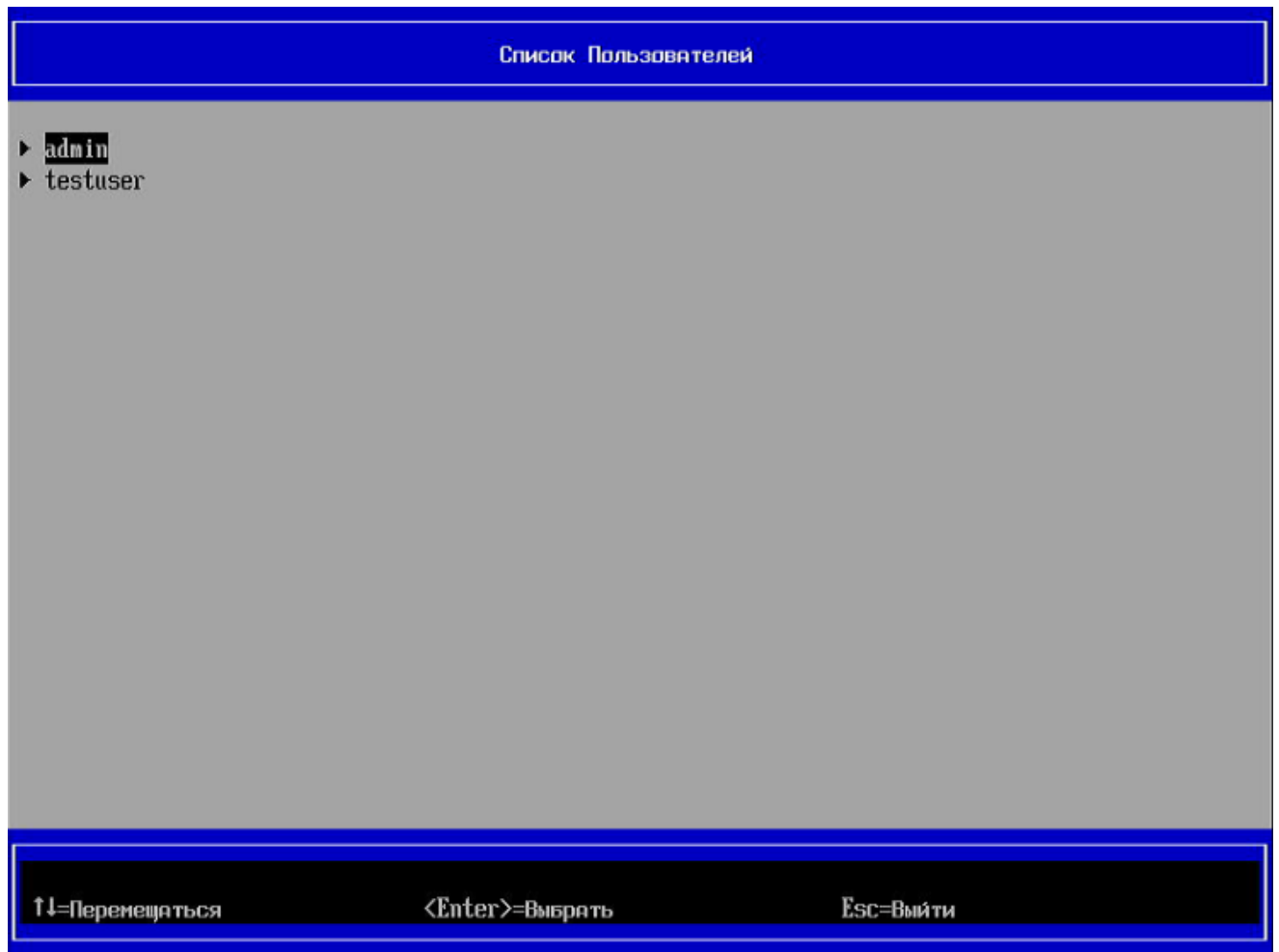


Рисунок 21



Рисунок 22

6.2.1.1. Смена пароля пользователя

Для смены пароля пользователя необходимо выполнить следующие действия:

- в списке пользователей выбрать имя пользователя для смены пароля;
- нажать «Сменить пароль» (Рисунок 22) и ввести новый пароль. В случае ошибки будет отображено сообщение с информацией об ошибке.

6.2.1.2. Блокировка пользователя

Для блокировки пользователя необходимо выполнить следующие действия:

- в списке пользователей выбрать имя пользователя для блокировки;
- нажать «Заблокировать пользователя» (см. Рисунок 22).

ПРИМЕЧАНИЯ:

- ✓ Выбор пункта «Заблокировать пользователя» позволяет как заблокировать, так и разблокировать пользователя, в том числе в случае автоматической блокировки, вызванной превышением количества неудачных попыток входа;
- ✓ Блокировка недоступна для администратора, под учетной записью которого совершен вход в инструмент настройки Аврора СДЗ.

6.2.1.3. Удаление пользователя

Для удаления пользователя необходимо выполнить следующие действия:

- в списке пользователей выбрать имя пользователя для удаления;
- нажать «Удалить пользователя» (см. Рисунок 22) и подтвердить удаление.

ПРИМЕЧАНИЯ:

- ✓ При выборе пункта «Удалить пользователя» происходит удаление пользователя без возможности его восстановления;
- ✓ Пользователь не будет удален в случае попытки удаления администратора, под учетной записью которого совершен вход в инструмент настройки Аврора СДЗ.

6.2.2. Добавление пользователя

Экран «Добавить Пользователя» приведен на рисунке (Рисунок 23) и позволяет заполнить следующие поля:

- «Пользователь» — имя пользователя, необходимое для загрузки ОС и входа в инструмент настройки Аврора СДЗ;
- «Пароль» — пароль пользователя, используемый для загрузки ОС и входа в инструмент настройки Аврора СДЗ;
- «Администратор» — чек-бокс указывает принадлежность пользователя к роли «администратор».

Для добавления нового пользователя необходимо выполнить следующие действия:

- после входа в систему на главном экране выбрать пункт «Пользователи» (см. Рисунок 7);
- на экране «Пользователи» выбрать пункт «Добавить Пользователя» (см. Рисунок 20);
- ввести имя для нового пользователя в поле «Пользователь»;
- ввести пароль для нового пользователя в поле «Пароль»;
- для наделения нового пользователя ролью «администратор» установить чек-бокс «Администратор»;
- по завершении заполнения всех полей нажать кнопку «Добавить Пользователя» для добавления пользователя.

Добавить Пользователя

Пользователь:

Пароль:

Администратор: ☐

Добавить Пользователя

Введите имя пользователя, 4-40 символов (с учётом регистра)

↑↓=Перемещаться <Enter>=Выбрать Esc=Выйти

Рисунок 23

6.3. Экран «Журнал»

Экран «Журнал Аврора СДЗ» (Рисунок 24) позволяет просматривать записи журнала аудита безопасности и предоставляет доступ к следующим опциям:

- «Размер журнала» — изменяет размер занимаемой журналом памяти на SPI Flash. Изменение памяти приведет к полной очистке журнала;
- «Очистить журнал» — удаляет все записи в журнале и создает новую запись об очистке журнала;
- «Пометить все записи как «прочитанные» — помечает все записи в журнале как «прочитанные». Непрочитанные события ошибок блокируют загрузку рабочей ОС.

При наведении курсора на запись отображается информация о данной записи: время, тип и состояние «прочитано».

Для работы с журналом необходимо выполнить следующие действия:

- после входа в систему на главном экране выбрать «Журнал» (см. Рисунок 7)
- для изменения размера журнала выставить желаемый размер в поле «Размер журнала»;

ВНИМАНИЕ! Изменение размера журнала в меньшую сторону приведет к удалению старых данных, для очистки журнала необходимо нажать «Очистить журнал».

- для того, чтобы пометить все записи, находящиеся в журнале, как прочитанные, необходимо нажать «Пометить все записи как «прочитанные»;
- не прочитанные записи журнала помечаются сочетанием символов «[+]».

При изменении размера журнала будет создана запись в журнале об изменении размера журнала.

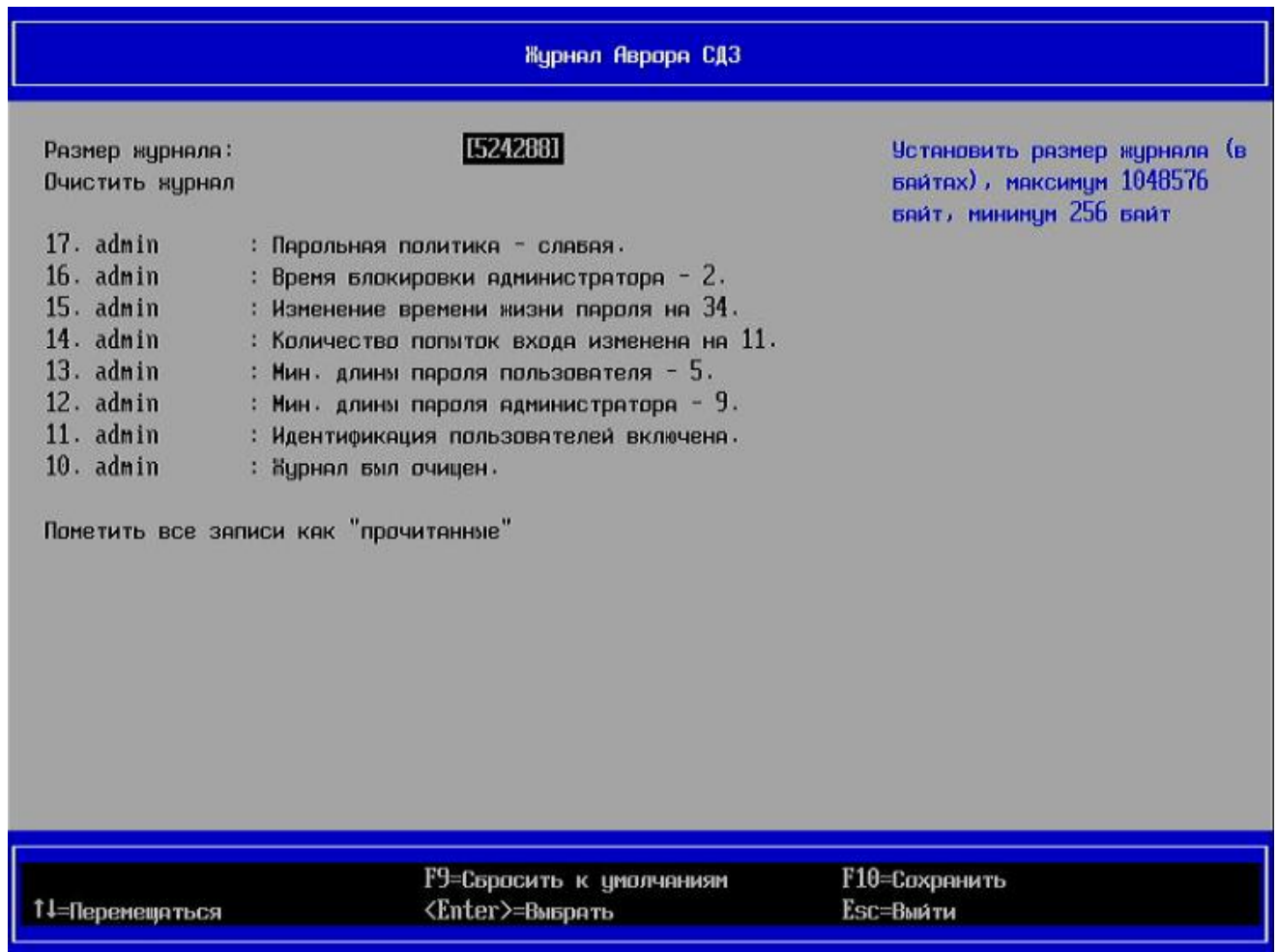


Рисунок 24

6.4. Экран «Диагностика»

Экран «Диагностика Аврора СДЗ» (Рисунок 25) позволяет проверить целостность Аврора СДЗ и журнала аудита безопасности.

На экране доступны следующие действия:

- «Проверка целостности Аврора СДЗ»;
- «Проверка целостности Журнала аудита».



Рисунок 25

6.4.1. Проверка целостности Аврора СДЗ

Проверка целостности Аврора СДЗ позволяет проконтролировать неизменность основных компонентов Аврора СДЗ.

Для проверки целостности Аврора СДЗ необходимо выполнить следующие действия:

- на экране «Диагностика Аврора СДЗ» выбрать пункт «Проверка целостности Аврора СДЗ»;
- на экране «Меню проверки целостности Аврора СДЗ» (Рисунок 27) нажать «Запуск проверки»;
- дождаться завершения проверки;

– исправить ошибки при их наличии и провести диагностику (проверку целостности) Аврора СДЗ повторно, пока все ошибки не будут устранены. Подробное описание кодов ошибок приведено в приложении (Приложение 1).

В случае успешной проверки целостности Аврора СДЗ будет отображаться экран, приведенный на рисунке (Рисунок 26).



Рисунок 26

После проверки целостности Аврора СДЗ будет отображаться экран «Меню проверки целостности Аврора СДЗ», приведенный на рисунке (Рисунок 27).



Рисунок 27

В случае неуспешной проверки целостности Аврора СДЗ будет отображаться экран с сообщением об ошибке, приведенный на рисунке (Рисунок 28).

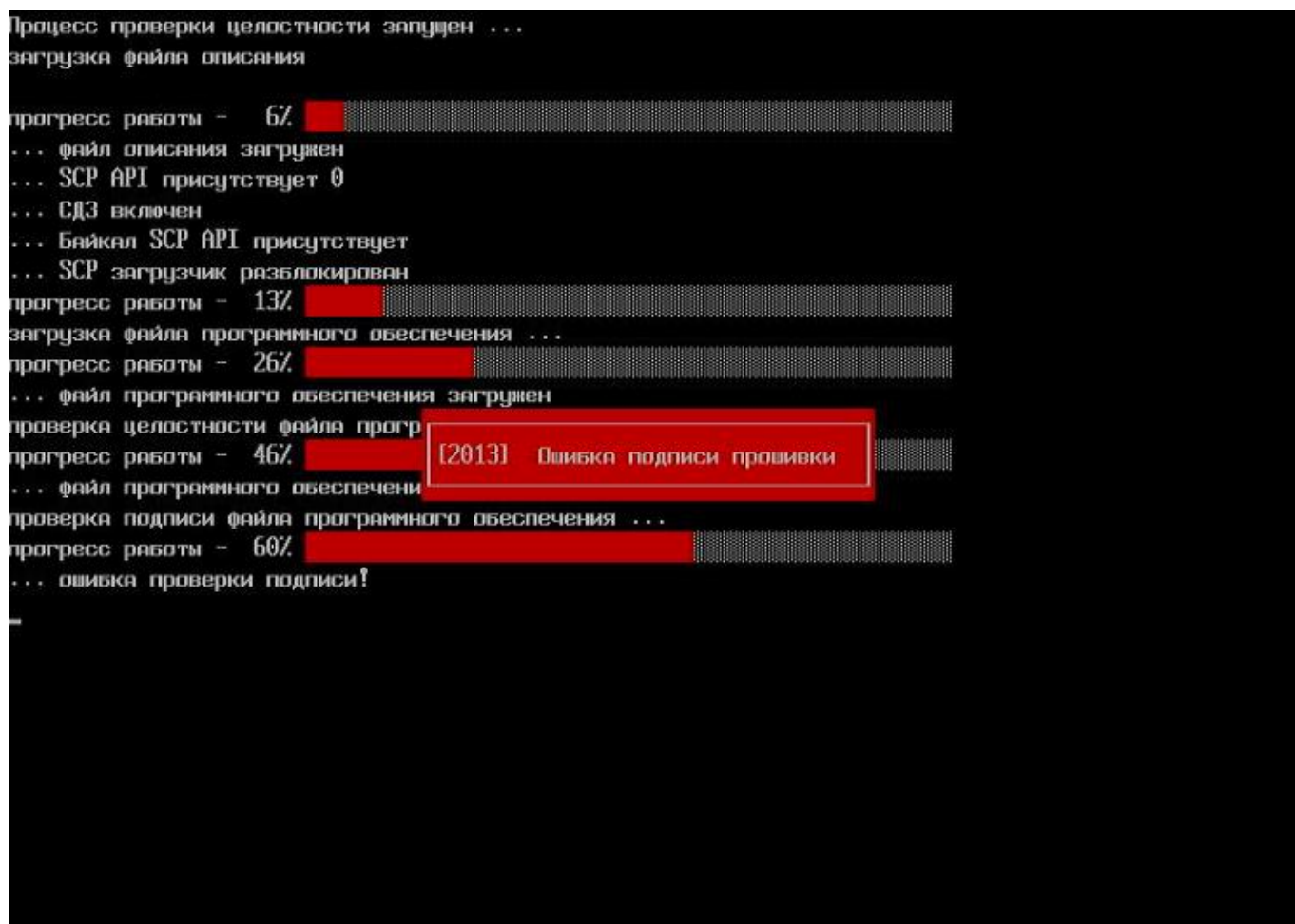


Рисунок 28

6.4.2. Проверка целостности журнала аудита

Проверка целостности журнала аудита позволяет проконтролировать корректность записей журнала аудита Аврора СДЗ.

Для проверки целостности журнала аудита необходимо выполнить следующие действия:

- на экране «Диагностика Аврора СДЗ» выбрать пункт «Проверка целостности Журнала аудита»;
- дождаться завершения проверки;
- исправить ошибки при их наличии и провести проверку целостности журнала повторно, пока все ошибки не будут устранены.

В случае успешной проверки целостности журнала аудита будет отображаться экран корректного завершения проверки, приведенный на рисунке (Рисунок 29).

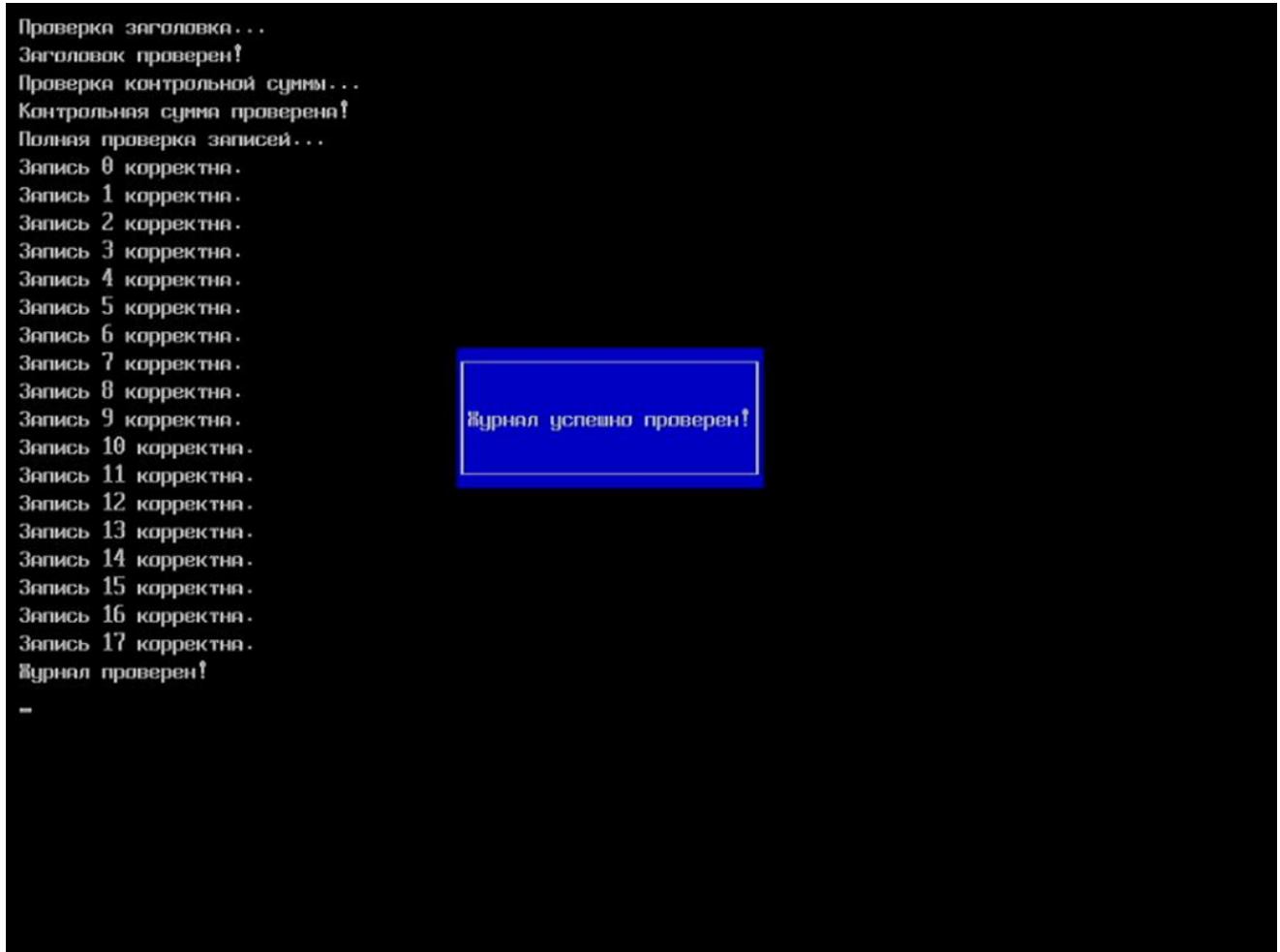


Рисунок 29

В случае ошибки проверки целостности журнала аудита будет отображаться экран с ошибкой, приведенный на рисунке (Рисунок 30).

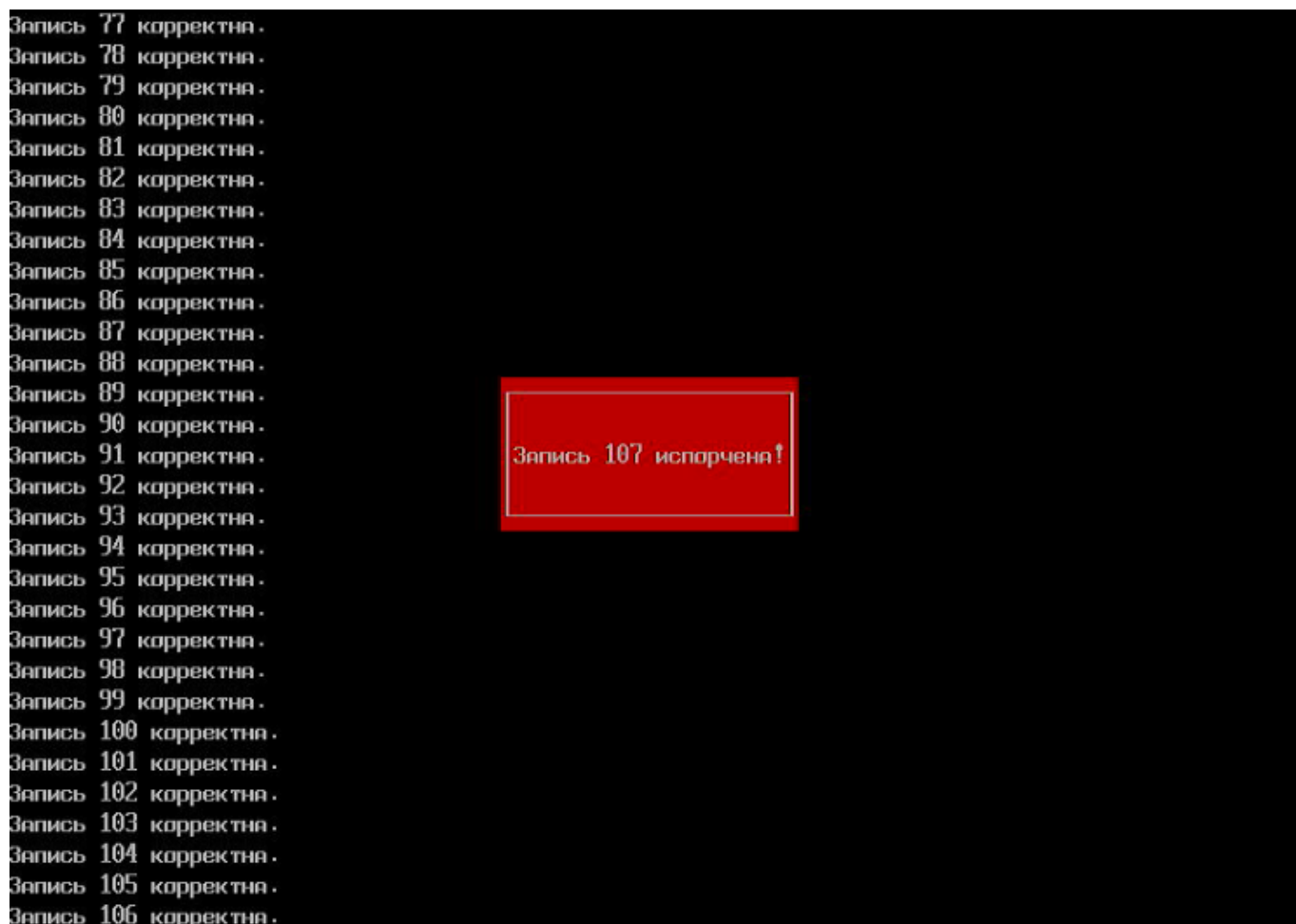


Рисунок 30

6.5. Экран «Обновление Аврора СДЗ»

Экран «Меню Обновления Аврора СДЗ» (Рисунок 31) позволяет выбрать файл обновления Аврора СДЗ.

Для обновления Аврора СДЗ необходимо выполнить следующие действия:

- загрузить необходимые файлы схемы обновления и файл с образом на внешний носитель (формат FAT32);
- подключить внешний носитель к устройству;
- войти в инструмент настройки Аврора СДЗ;
- на главном экране выбрать пункт «Обновление Аврора СДЗ» (см. Рисунок 7);

- на экране «Меню Обновления Аврора СДЗ» выбрать пункт «Выбрать файл программного обеспечения»;
- выбрать внешний носитель, с которого следует получить файл обновления, затем выбрать желаемый файл схемы обновления в файловой системе носителя;
- проверить, что изменения затрагивают только желаемые разделы и правильную платформу;
- нажать «Обновление программного обеспечения».

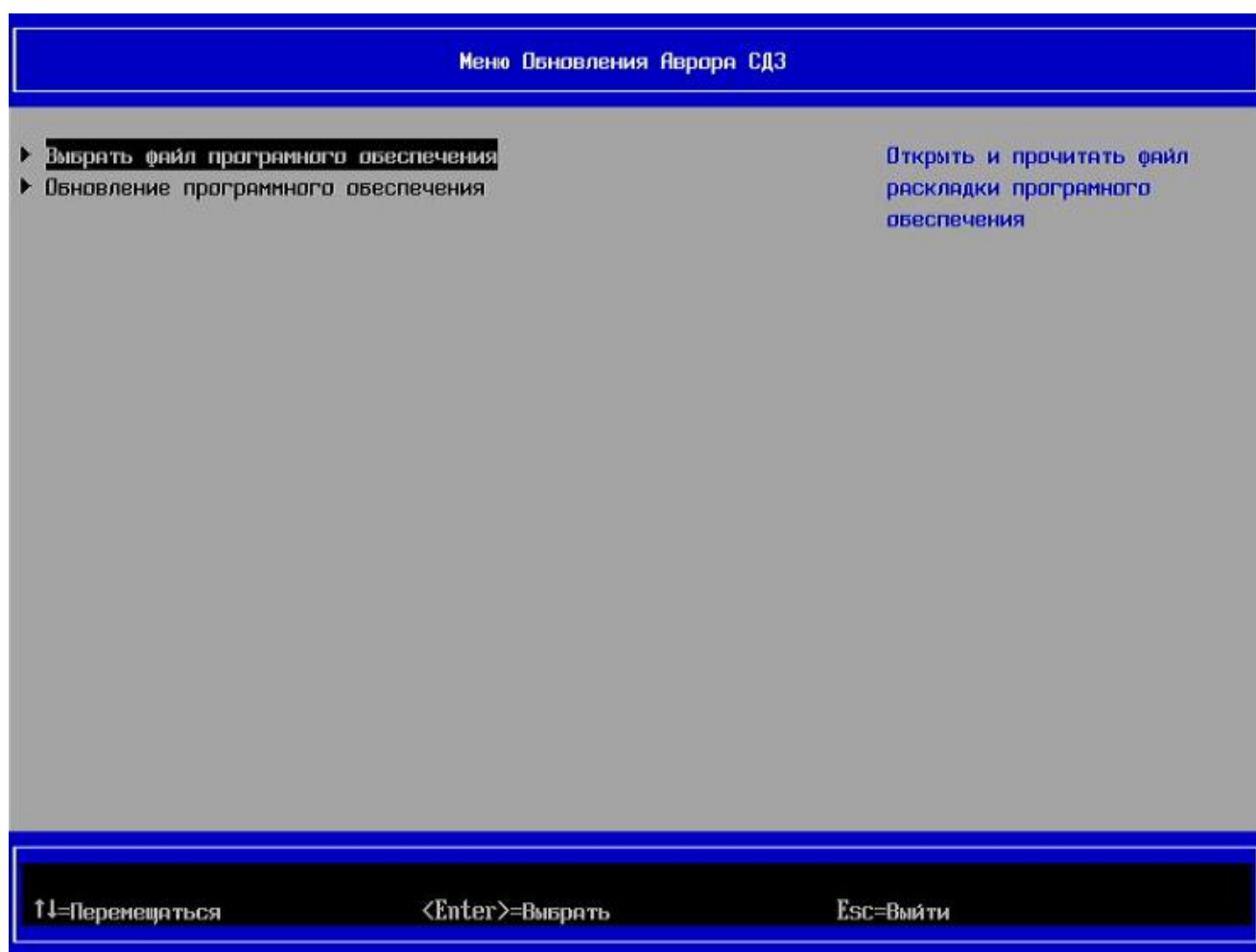


Рисунок 31

После выбора файла обновления информация о нем отобразится на экране «Меню Обновления Аврора СДЗ» (Рисунок 32). Возможные ошибки приведены в приложении (Приложение 1).



Рисунок 32

6.6. Экран «Информация об Аврора СДЗ»

Экран «Меню информации об Аврора СДЗ» (Рисунок 33) содержит информацию о версиях загрузочных модулей Аврора СДЗ. Возможные ошибки компонентов СДЗ приведены в приложении (Приложение 1).

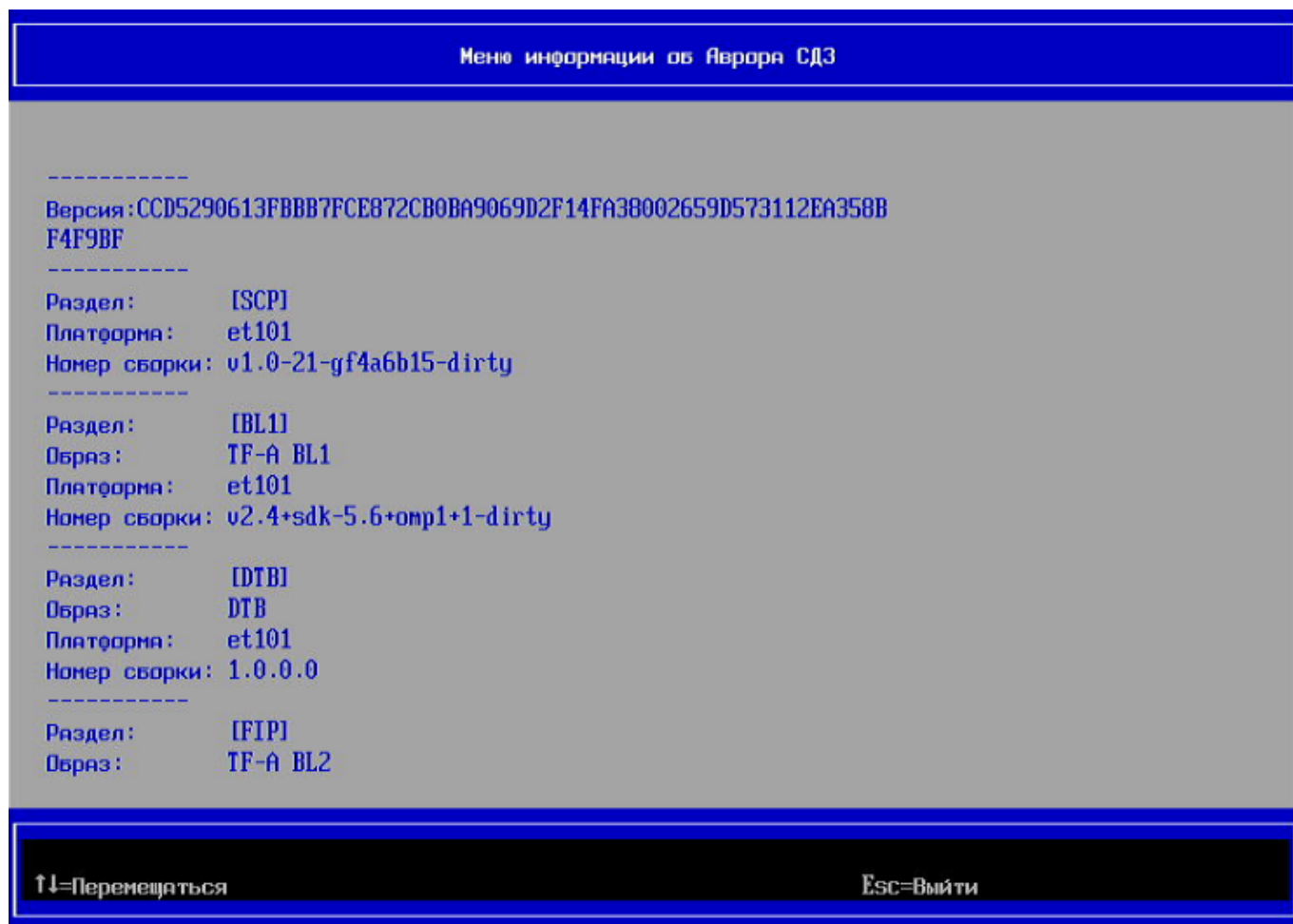


Рисунок 33

6.7. Экран «Управление устройствами»

Экран «Управление устройствами» (Рисунок 34) содержит формы для настроек драйверов, не связанных с Аврора СДЗ. Набор форм может отличаться в зависимости от устройства, на котором установлена Аврора СДЗ, а их содержимое не является частью Аврора СДЗ.

ПРИМЕЧАНИЕ. Экран «Управление устройствами» приведен для платы Elpitech ET101.

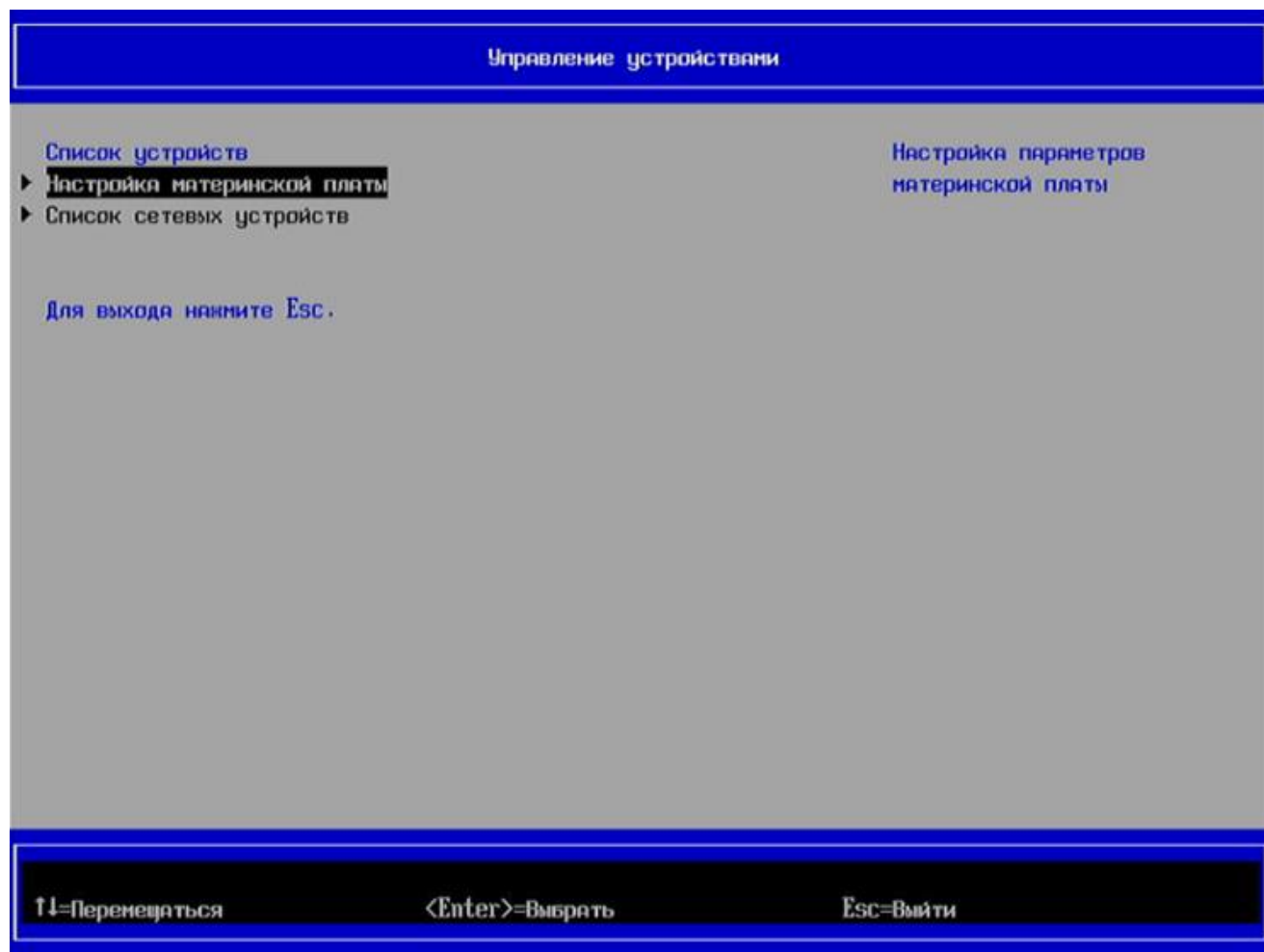


Рисунок 34

6.8. Экран «Менеджер загрузки»

Экран «Менеджер загрузки» (Рисунок 35) содержит список загрузочных опций (вариантов загрузки). Загрузочную опцию можно выбрать с помощью кнопок «Стрелки», после чего выполнить загрузку в выбранную опцию нажатием кнопки «Enter». В результате продолжится загрузка по выбранной опции.

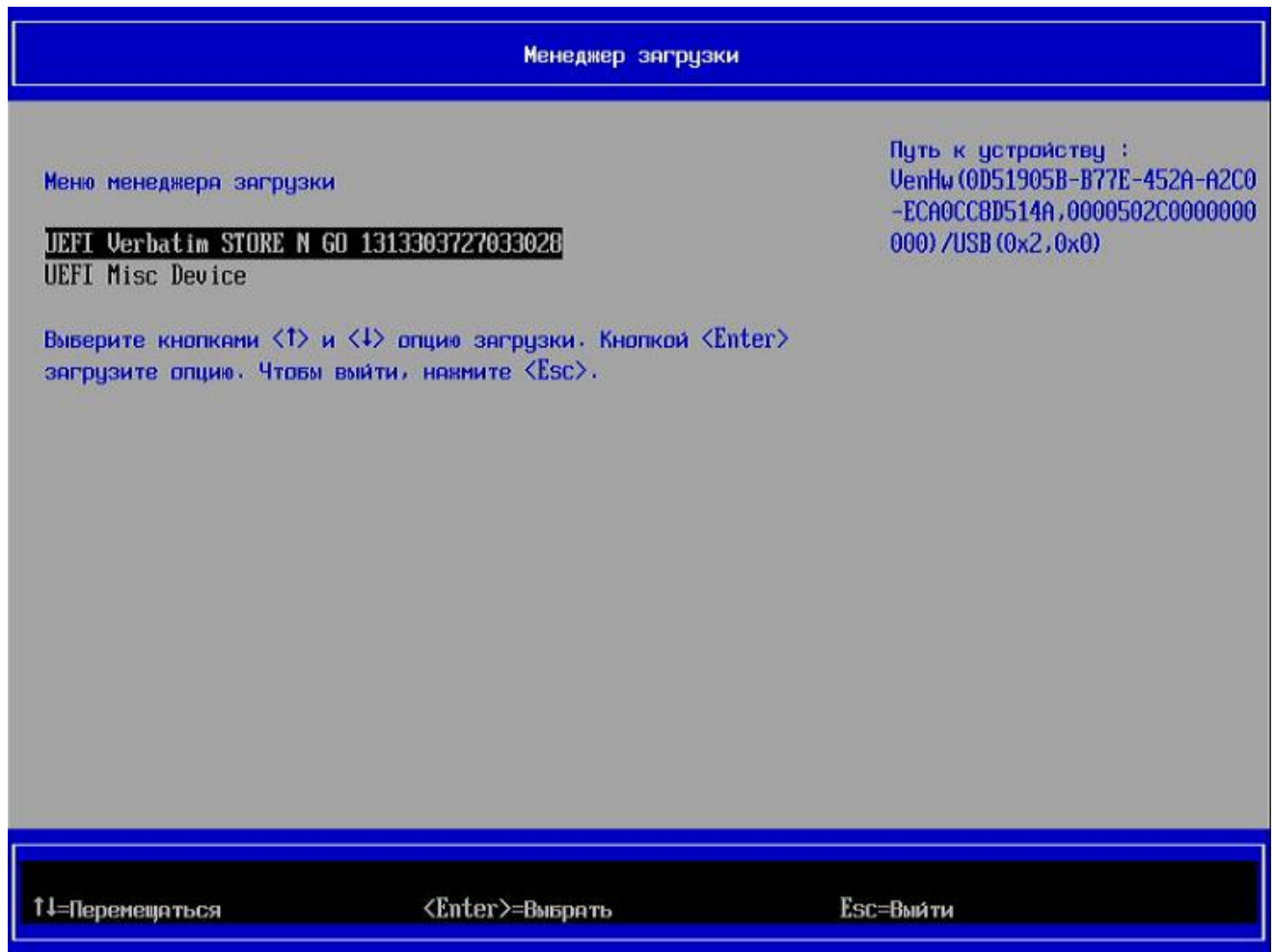


Рисунок 35

6.9. Экран «Настройки загрузки»

Экран «Настройки загрузки» (Рисунок 36) служит для настройки вариантов загрузки ОС.

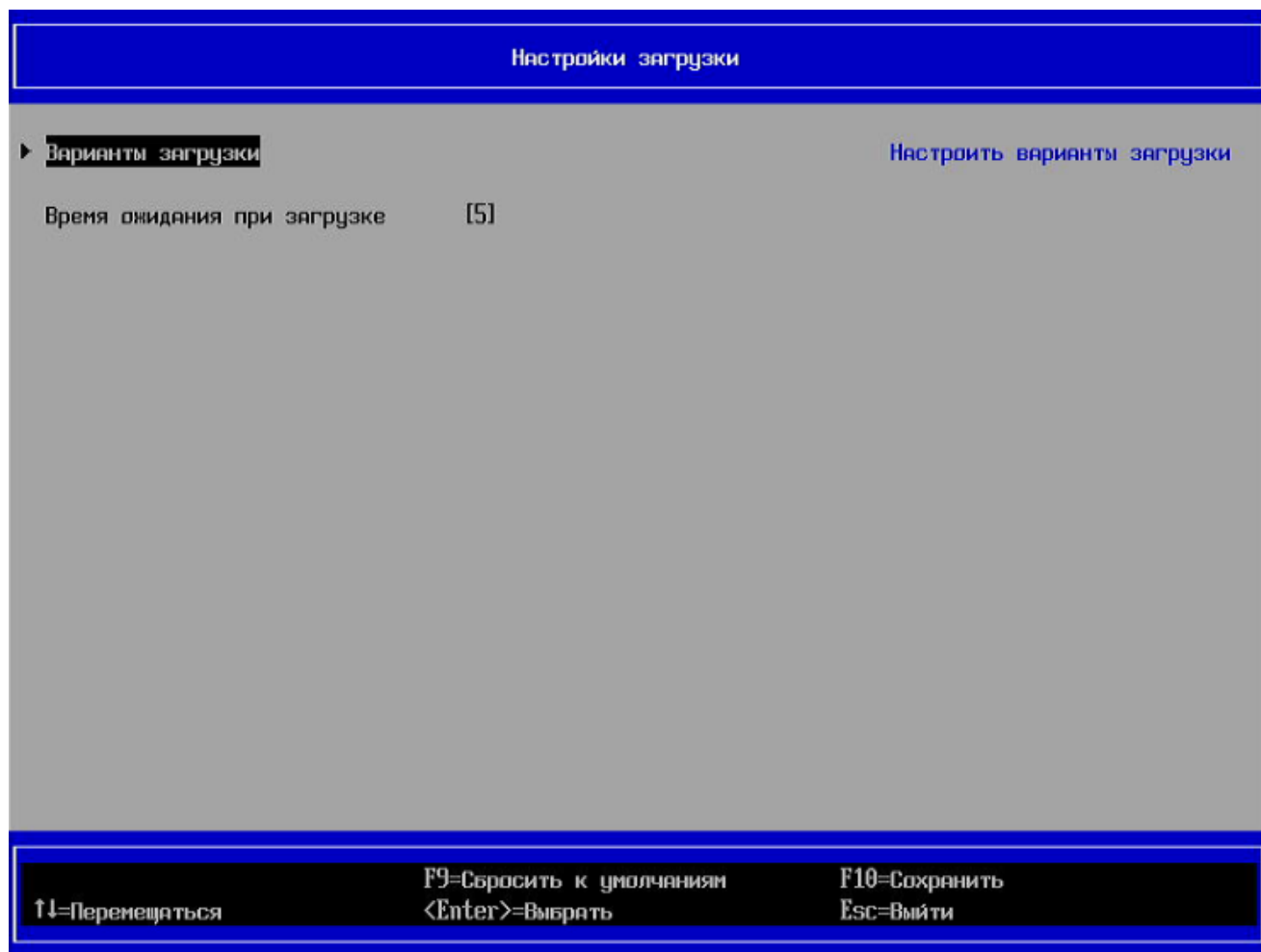


Рисунок 36

«Варианты загрузки» – позволяет добавить вариант загрузки ОС, удалить вариант и сменить порядок загрузки ОС (Рисунок 37).

«Время ожидания при загрузке» – позволяет выставить время ожидания входа в настройки СДЗ при загрузке системы в секундах (допустимые значения от 0 до 65535). По прошествии данного периода времени СДЗ продолжит загрузку установленной ОС.



Рисунок 37

6.9.1. Добавить вариант загрузки

При выборе пункта «Добавить вариант загрузки» отображается файловый менеджер (Рисунок 38) со списком носителей информации, подключенных к системе.

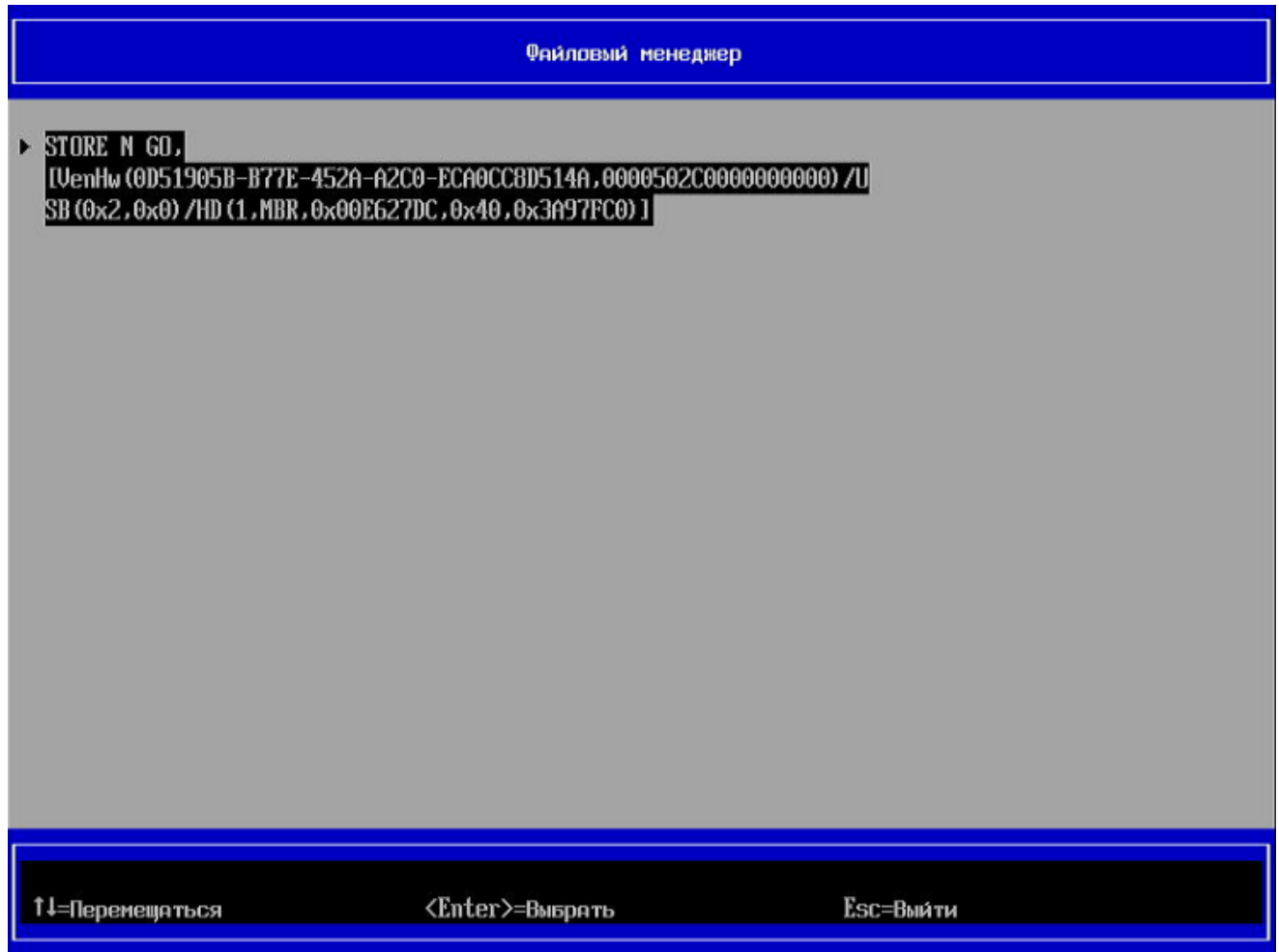


Рисунок 38

При выборе носителя отображается список образов ОС на выбранном носителе, доступных к загрузке (Рисунок 39).



Рисунок 39

При выборе доступного образа ОС отображается окно редактирования описания варианта загрузки (Рисунок 40).

В окне редактирования описания варианта загрузки доступны следующие опции:

- «Введите описание» – позволяет ввести описание для данного варианта загрузки, понятное пользователю, которое затем будет отображаться в списке вариантов загрузки;

- «Введите опции загрузки» – здесь указываются необходимые опции загрузки для загрузки данного варианта;

- «Сохранить и выйти» – для сохранения варианта загрузки;

- «Забыть изменения и выйти» – для выхода без сохранения.

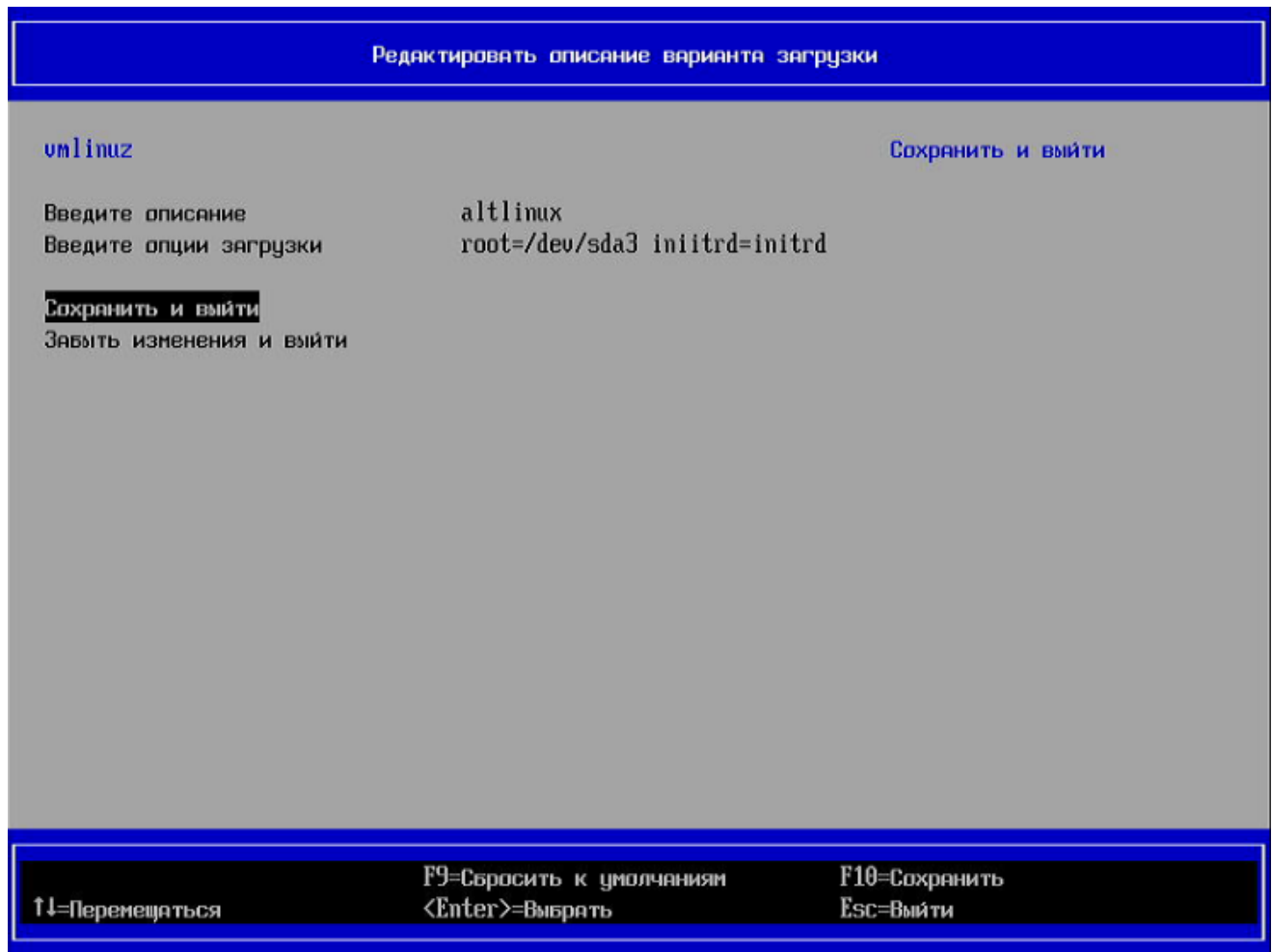


Рисунок 40

Для добавления нового варианта загрузки необходимо выполнить следующие действия:

- загрузить желаемый образ и его подпись на внешний носитель (формат FAT32);
- подключить внешний носитель к устройству;
- после входа в систему на главном экране выбрать пункт «Настройки загрузки» (см. Рисунок 7);
- на экране «Настройки загрузки» выбрать пункт «Варианты загрузки»;
- на экране «Варианты загрузки» выбрать «Добавить вариант загрузки»;
- выбрать внешний носитель, затем выбрать желаемый образ в файловой системе носителя;

- ввести описание и опции загрузки для нового варианта загрузки (Рисунок 40);
- для сохранения варианта загрузки нажать «Сохранить и выйти»;
- в случае если сохранять изменения не требуется, выбрать пункт «Забыть изменения и выйти».

6.9.2. Удалить вариант загрузки

Экран «Удалить вариант загрузки» отображает список присутствующих в системе вариантов загрузки (Рисунок 41) и позволяет удалить выбранные варианты.

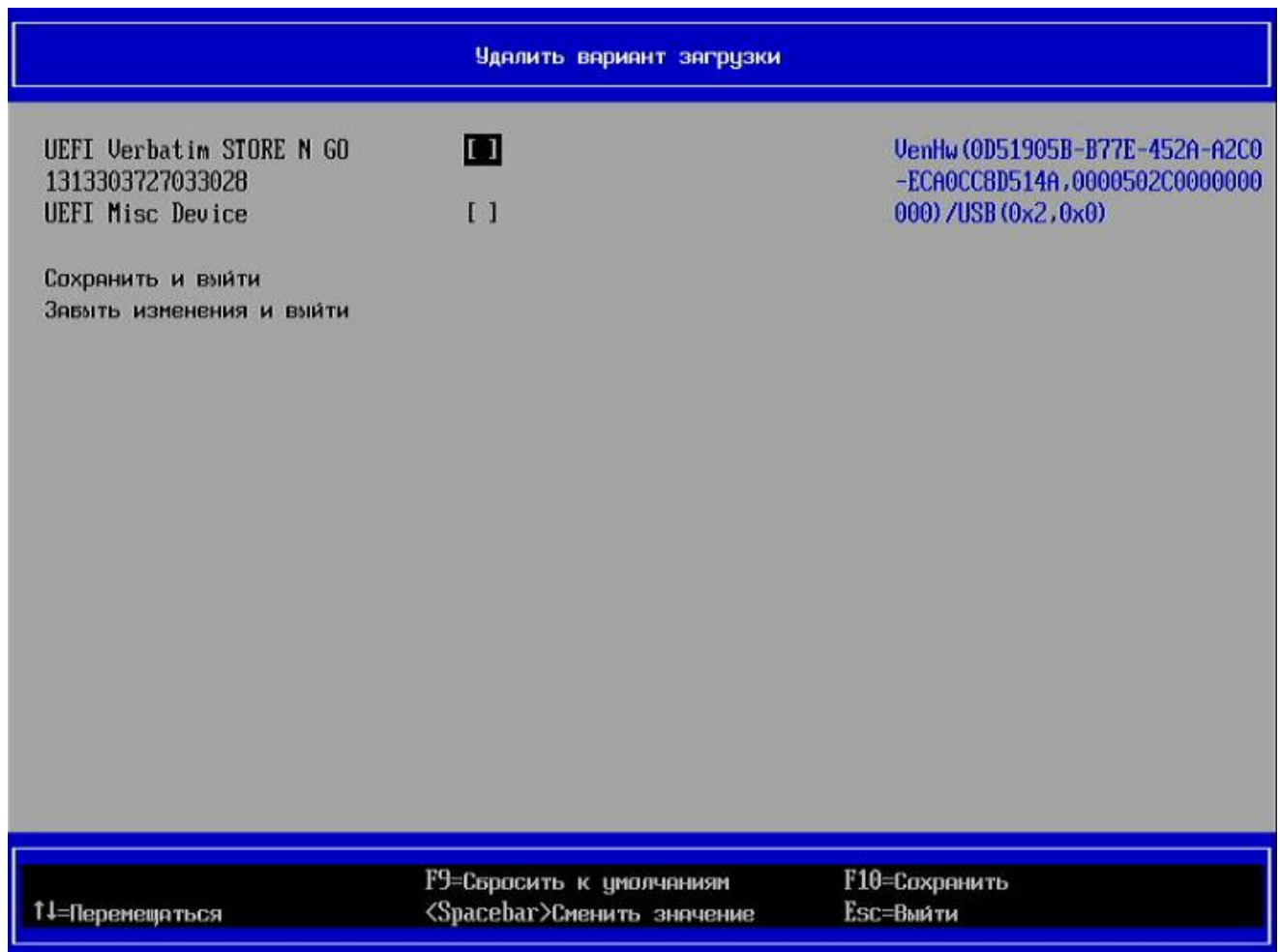


Рисунок 41

Для удаления вариантов загрузки необходимо выполнить следующие действия:

- выбрать варианты загрузки для удаления;

- для сохранения изменений нажать «Сохранить и выйти»;
- в случае если сохранять изменения не требуется, выбрать пункт «Забыть изменения и выйти».

6.9.3. Сменить порядок загрузки

Экран «Сменить порядок загрузки» приведен на рисунке (Рисунок 42).

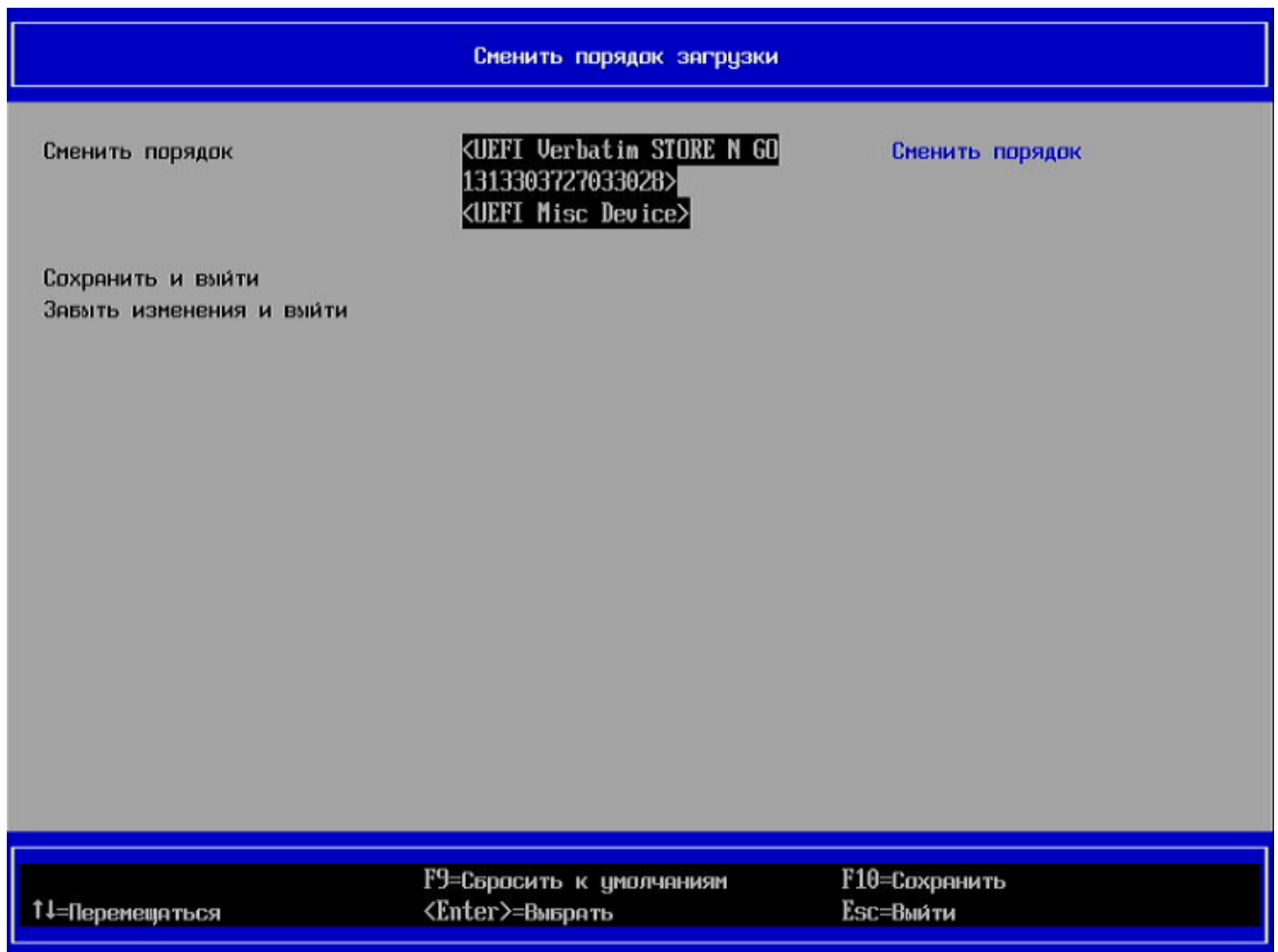


Рисунок 42

На данном экране отображаются все установленные в системе варианты загрузки.

Данный список определяет порядок, в котором система будет пытаться запустить указанный вариант загрузки. По умолчанию система пытается загрузить первый (верхний) вариант в списке. В случае неуспеха первого варианта система автоматически загрузит следующий и т.д.

Для изменения порядка вариантов загрузки необходимо выполнить следующие действия:

- выбрать пункт «Сменить порядок». При нажатии на список вариантов загрузки будет выведено окно (Рисунок 43), позволяющее изменить порядок загрузки установленных вариантов загрузки;
- выбрать желаемый вариант для перемещения нажатием «Enter». Изменения осуществляются нажатием кнопок «+» или «-» для перемещения варианта;
- после перемещения всех желаемых вариантов зафиксировать порядок, нажав «Enter»;
- для сохранения изменений нажать «Сохранить и выйти»;
- в случае если сохранять изменения не требуется, выбрать пункт «Забыть изменения и выйти».

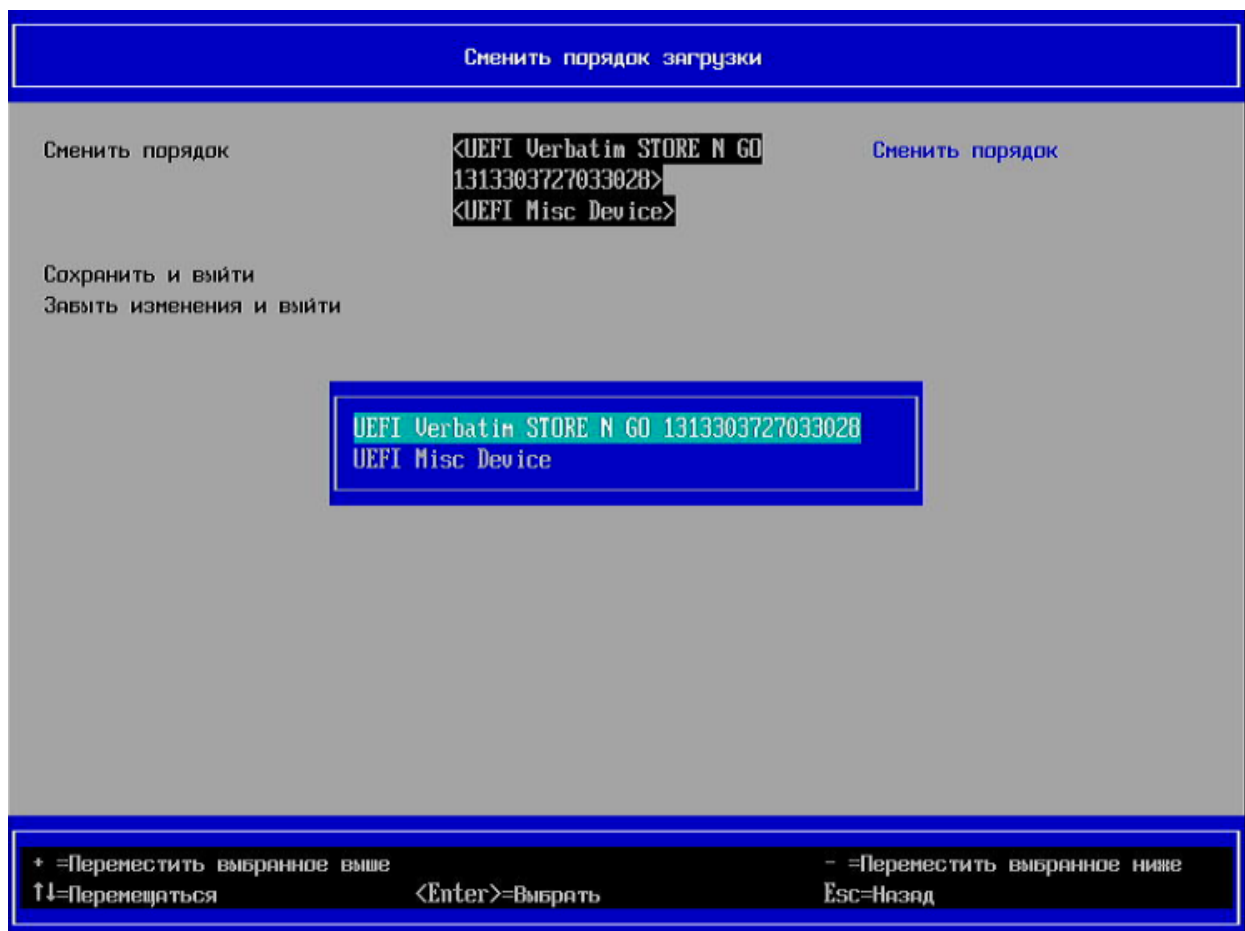


Рисунок 43

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

Используемые в настоящем документе термины и сокращения приведены в таблице (Таблица 4).

Таблица 4

Термин/Сокращение	Расшифровка
Аврора СДЗ	Средство доверенной загрузки Аврора
Администратор	Пользователь, обладающий правами на выполнение операций, связанных с администрированием системы
КС	Контрольная сумма
Пользователь	Лицо, использующее систему для выполнения заложенных в ней функций
ПО	Программное обеспечение
Предприятие-разработчик	Общество с ограниченной ответственностью «Открытая мобильная платформа» (ООО «Открытая мобильная платформа»)
ОС	Операционная система
ФСТЭК России	Федеральная служба по техническому и экспортному контролю Российской Федерации
AP	Application Processor – прикладной процессор
eFuse	Electronic Fuse – однократно программируемая память
SCP	System Control Processor – управляющий процессор
SPI	Serial Peripheral Interface – последовательный периферийный интерфейс
TEE	Trusted Execution Environment – защищенная область главного процессора
UEFI	Unified Extensible Firmware Interface – унифицированный расширяемый микропрограммный интерфейс
USB	Universal Serial Bus – последовательный интерфейс для подключения периферийных устройств к вычислительной технике

ПРИЛОЖЕНИЕ 1

Описание кодов ошибок

Формат кода ошибки -[XXYY], где:

- XX- число-код функции;
- YY – число-код ошибки.

Формат числа – шестнадцатеричный.

Описание кодов функции приведено в таблице (Таблица 1.1).

Таблица 1.1

Код функции (XX)	Описание
00	Код основных функций
10	Код функций работы с файлом описания
20	Код функций работы с файлом образом прошивки
30	Код функций драйвера поддержки процесса обновления прошивки

Описание кодов ошибок основных функций приведено в таблице (Таблица 1.2).

Таблица 1.2

Код ошибки (YY)	Описание
02	Внутренняя ошибка. Неверный параметр. Неисправимая ошибка. Необходимо обновить ПО
09	Внутренняя ошибка. Недостаточно ресурсов. Необходимо перезагрузить систему или добавить в систему оперативной памяти
0A	SCP flash заблокирована Неустранимая ошибка. Обновление SCP невозможно
0B	Ошибка получения информации SCP flash. Неустранимая ошибка. Параметры flash не определены, обновление невозможно

Описание кодов ошибок функций работы с файлом приведено в таблице (Таблица 1.3).

Таблица 1.3

Код ошибки (YY)	Описание
02	Внутренняя ошибка. Неверный параметр. Неисправимая ошибка. Необходимо обновить ПО
09	Внутренняя ошибка. Недостаточно ресурсов. Необходимо перезагрузить систему или добавить в систему оперативной памяти
0A	Ошибка формирования имени файла описания. Системная ошибка. Необходимо перезагрузить систему или добавить в систему оперативной памяти
0B	Ошибка загрузки файла описания. Системная ошибка. Необходимо перезагрузить систему или добавить в систему оперативной памяти
0C	Файл описания испорчен. Нарушена целостность файла описания. Необходимо выбрать целый файла описания
0D	Отсутствует файл прошивки. Отсутствует файл образа или указано неверное имя файла образа
0E	Ошибка формата файла описания. Формат файла описания не поддерживается или сформирован неправильно. Необходимо выбрать поддерживаемый файл описания

Описание кодов ошибок функций работы с файлом образа прошивки приведено в таблице (Таблица 1.4).

Таблица 1.4

Код ошибки (YY)	Описание
02	Внутренняя ошибка. Неверный параметр. Неисправимая ошибка. Необходимо обновить ПО
09	Внутренняя ошибка. Недостаточно ресурсов. Необходимо перезагрузить систему или добавить в систему оперативной памяти
0A	Файл прошивки не найден. Отсутствует файл образа или указано неверное имя файла образа

Код ошибки (YY)	Описание
0B	Размер прошивки не совпадает с заданным в файле описания. Файл описания не соответствует файлу прошивки
0C	Ошибка загрузки прошивки. Системная ошибка. Необходимо перезагрузить систему или добавить в систему оперативной памяти
0D	Неизвестный тип региона. Неподдерживаемый файл образа прошивки
0E	Ошибка разбора контейнера. Неподдерживаемый файл образа прошивки
0F	Образ прошивки испорчен. Нарушена целостность файла образа прошивки. Необходимо заменить файл образа
10	Ошибка получения метаданных прошивки. Внутренняя ошибка. Необходимо перезагрузить систему или добавить в систему оперативной памяти
11	Прошивка для другого устройства. Файл образа прошивки не соответствует системе. Необходимо заменить файл образа прошивки на соответствующий данному устройству
12	Ошибки в командном пакете. Ошибка в формате командного пакета. Необходимо заменить командный пакет в файле образе прошивки
13	Ошибка подписи прошивки. Подпись образа прошивки отсутствует или неправильная. Необходимо заменить файл образа прошивки
14	Неверная версия прошивки. Попытка записать образ предыдущей версии. Необходимо заменить файл образа прошивки
15	Ошибка записи Системная ошибка. Необходимо перезагрузить систему или заменить SPC flash
16	Внутренняя ошибка. Не соблюдены условия выполнения. Попытка нарушения процесса обновления прошивки. Необходимо перезагрузить систему
17	Нарушены правила по количеству регионов в образе. Неподдерживаемый файл образа прошивки

Описание кодов ошибок драйвера поддержки процесса обновления прошивки приведено в таблице (Таблица 1.5).

Таблица 1.5

Код ошибки (YY)	Описание
02	Внутренняя ошибка. Неверный параметр. Неисправимая ошибка. Необходимо обновить ПО
09	Внутренняя ошибка. Недостаточно ресурсов. Необходимо перезагрузить систему или добавить в систему оперативной памяти

[illegible]