УТВЕРЖДЕН

АДМГ.30031-01 90 01-ЛУ

СРЕДСТВО ДОВЕРЕННОЙ ЗАГРУЗКИ АВРОРА

Руководство пользователя

АДМГ.30031-01 90 01

Листов 20

2024

АННОТАЦИЯ

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

Документ содержит общую информацию о взаимодействии пользователей с Аврора СДЗ.

Пользователь имеет доступ только к функциям и настройкам Аврора СДЗ, описанным в настоящем документе.

ПРИМЕЧАНИЕ. Перед началом работы пользователю необходимо ознакомиться с положениями настоящего документа, а также с информацией, приведенной в документе «Руководство администратора» АДМГ.30031-01 91 01.

СОДЕРЖАНИЕ

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;

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

– подсистема Аврора TEE 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, проверка целостности программного обеспечения 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. ПОРЯДОК ВХОДА

В зависимости от настроек Аврора СДЗ возможны 3 варианта загрузки ОС, описание которых приведено в подразделах 2.1 - 2.3.

2.1. Загрузка без идентификации и аутентификации

В случае если требования аутентификации и идентификации пользователя отключены в Аврора СДЗ, загрузка ОС будет осуществляться без дополнительных действий со стороны пользователя.

2.2. Загрузка с идентификацией

В случае если требование идентификации пользователя без аутентификации включено в Аврора СДЗ, при загрузке ОС отобразится экран для ввода имени пользователя (Рисунок 1).

Для продолжения загрузки необходимо выполнить следующие действия:

- указать имя учетной записи пользователя в соответствующем поле;
- нажать кнопку «Продолжить».

При необходимости перезагрузить устройство следует нажать кнопку «Перезагрузить».

ПРИМЕЧАНИЕ. Вход в систему с идентификацией является событием безопасности и фиксируется в журнале безопасности.

Рисунок 1

2.3. Загрузка с идентификацией и аутентификацией

В случае если требования аутентификации и идентификации пользователя включены в Аврора СДЗ, при загрузке ОС отобразится экран для ввода имени и пароля учетной записи пользователя (Рисунок 2).

Для продолжения загрузки необходимо выполнить следующие действия:

– указать имя пользователя и пароль в соответствующих полях;

– нажать кнопку «Продолжить».

При необходимости перезагрузить устройство следует нажать кнопку «Перезагрузить».

ПРИМЕЧАНИЕ. Вход в систему с идентификацией и аутентификацией является событием безопасности и фиксируется в журнале безопасности.


Средство Доверенной Загрузки Аврора
Пользователь:
testuser
Пароль:
Продолжить
Перезагрузить
Введите пароль (с учётом регистра)
↑↓=Перемещаться
<Enter>=Выбрать

Рисунок 2

3. РЕКОМЕНДАЦИИ ПО УСТРАНЕНИЮ ВОЗМОЖНЫХ ОШИБОК

В ходе работы с Аврора СДЗ пользователю могут выводиться сообщения об ошибках, описание которых приведено в подразделах 3.1 - 3.8.

3.1. Неверное имя пользователя

Причина ошибки: опечатка при вводе имени пользователя (Рисунок 3).

Решение: перепроверить ввод. В случае если имя пользователя введено верно, необходимо обратиться к администратору для проверки наличия нужного пользователя в системе.

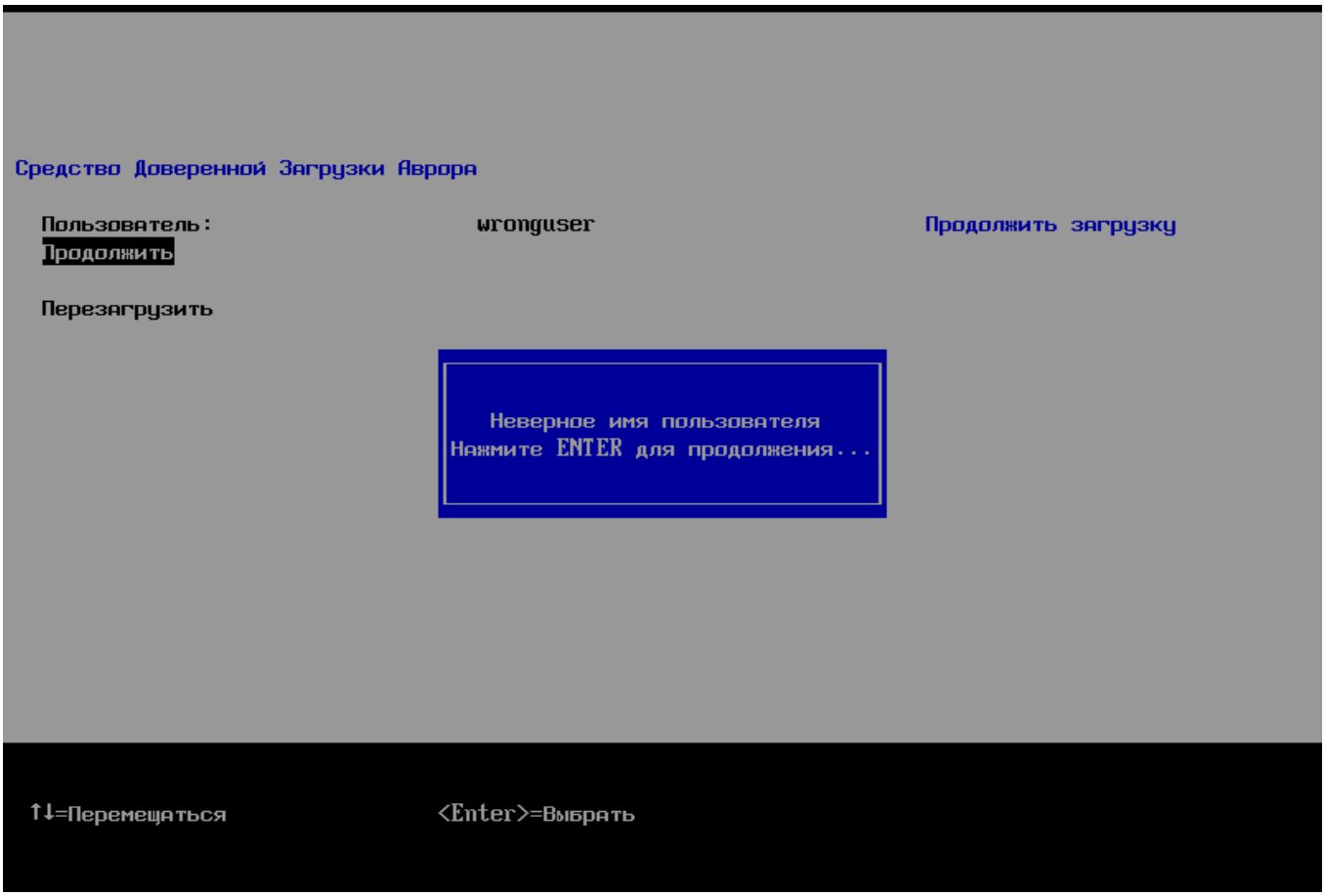

Рисунок 3

3.2. Неверное имя пользователя или пароль

Причина ошибки: ввод неверного имени пользователя, неверного пароля либо несоответствие пароля и имени пользователя при включенных требованиях идентификации и аутентификации (Рисунок 4).

Решение: перепроверить ввод. В случае если имя пользователя и пароль введены верно, необходимо обратиться к администратору для проверки наличия нужного пользователя в системе и возможной смены пароля.

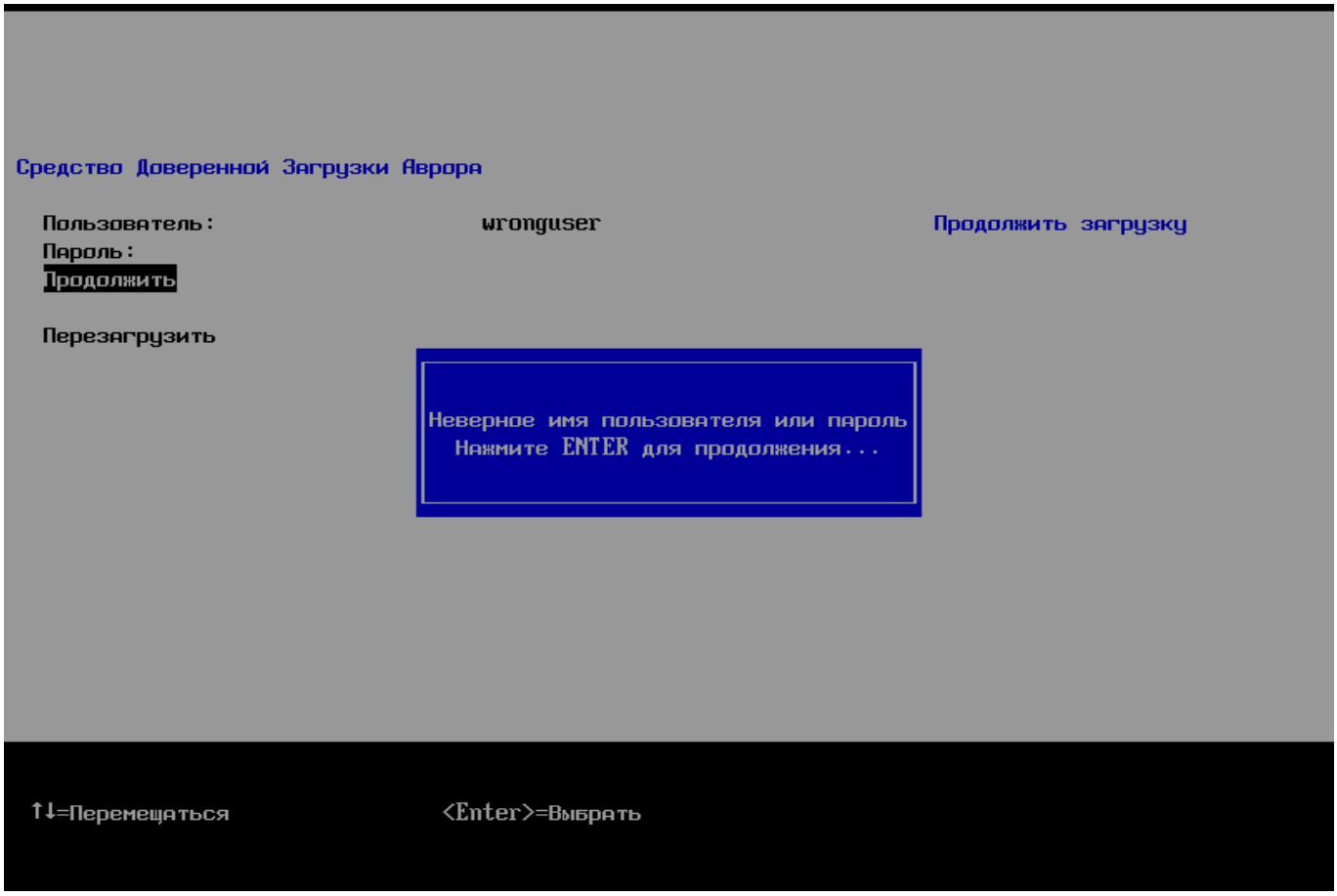

Рисунок 4

3.3. Истечение срока действия пароля

Причина ошибки: истечение срока действия пароля учетной записи пользователя (Рисунок 5).

Решение: обратиться к администратору для создания нового пароля.

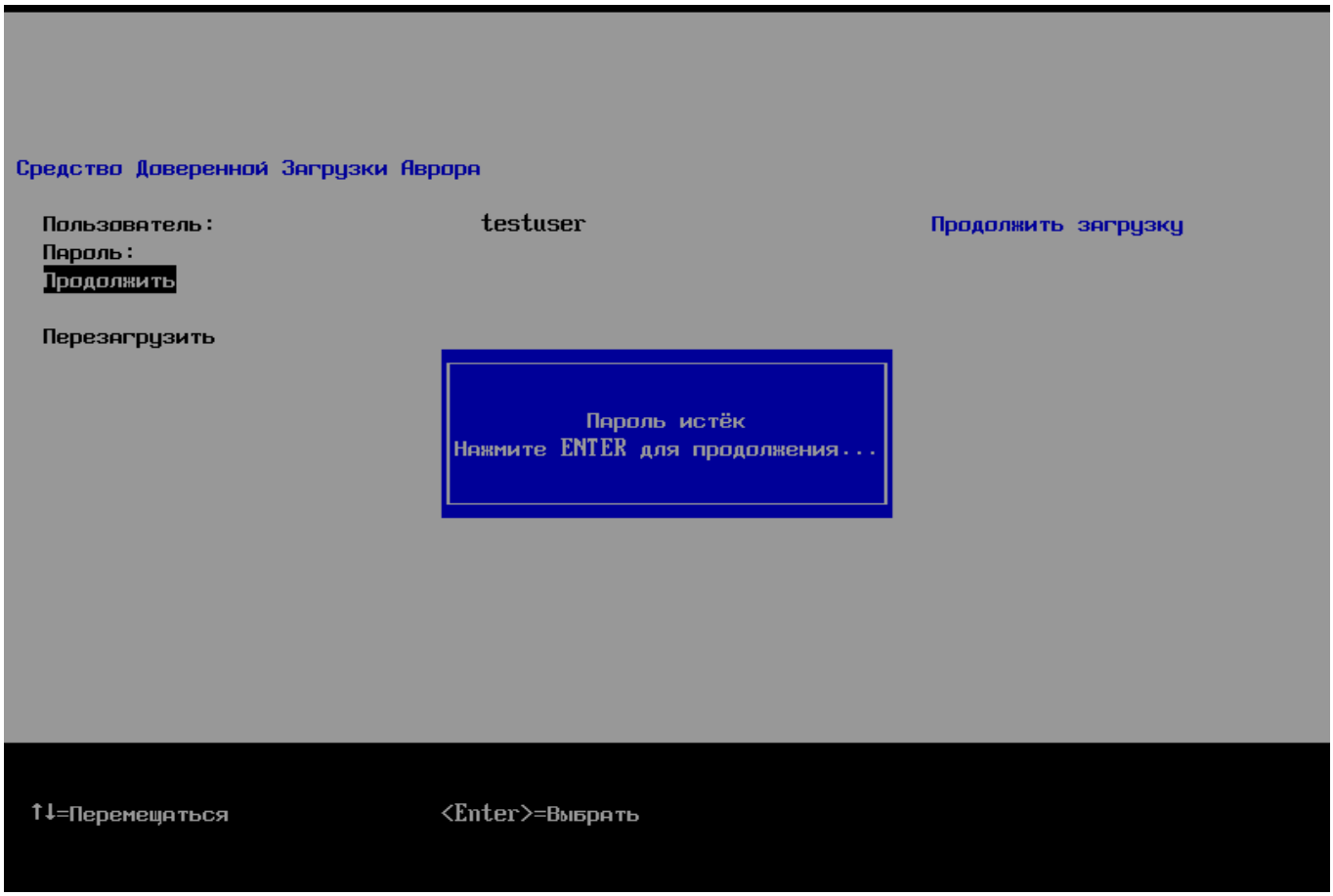

Рисунок 5

3.4. Превышение количества неуспешных попыток входа

Причина ошибки: большое количество неправильных вводов пароля для существующего пользователя (Рисунок 6, Рисунок 7).

Решение: обратиться к администратору.

ПРИМЕЧАНИЯ:

✓ По умолчанию каждому пользователю предоставляется 10 попыток для входа в систему;

✓ По истечении заданного количества попыток, а также в случае превышения максимального количества неуспешных входов произойдет блокировка пользователя и возможности загрузки системы;

✓ Количество неудачных попыток обнуляется при успешном входе в систему или при разблокировке пользователя администратором.

В случае если таким образом блокируется администратор, для разблокировки необходимо повторить вход через установленный в настройках период времени. Время ожидания по умолчанию – 1 рабочий день.

Рисунок 6

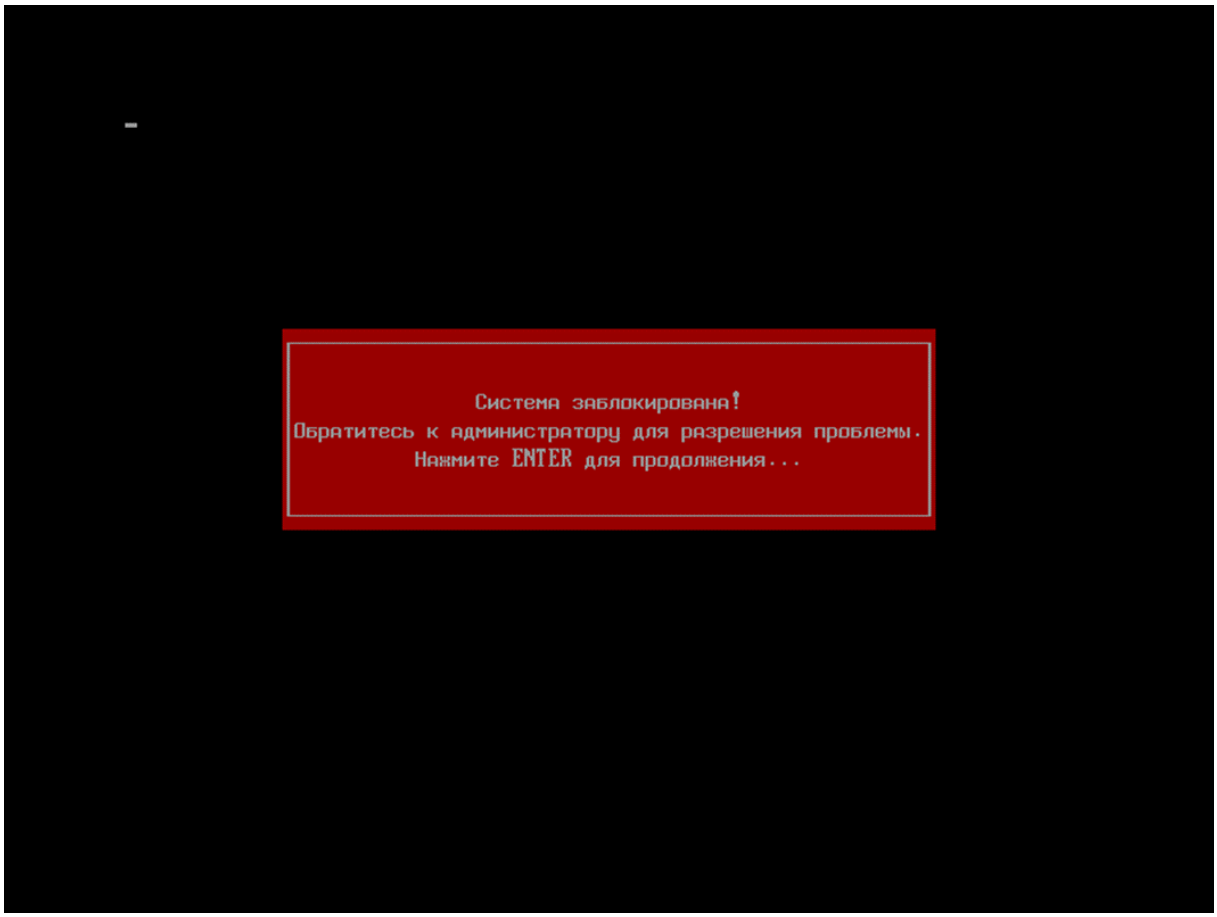

Рисунок 7

3.5. Блокировка учетной записи

Причины ошибки (Рисунок 8):

– попытка входа с использованием корректных имени и пароля заблокированной учетной записи пользователя;

– превышение количества неуспешных попыток входа;

– ручная блокировка со стороны учетной записи администратора.

Решение: обратиться к администратору для разблокировки учетной записи пользователя.

В случае если учетная запись администратора заблокирована из-за превышения количества неуспешных попыток входа, для разблокировки необходимо подождать установленный в настройках период времени, после чего повторить вход. Время ожидания по умолчанию – 1 рабочий день.

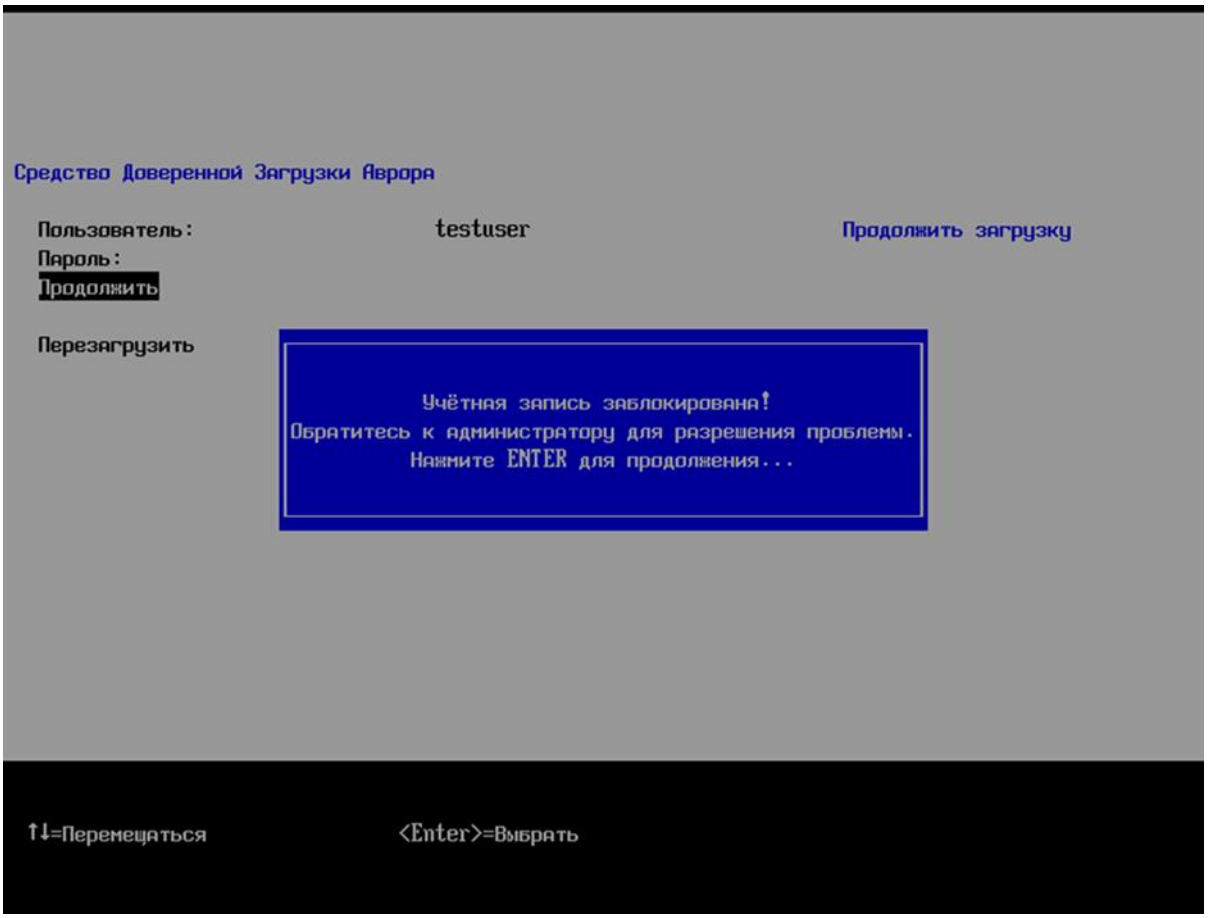

Рисунок 8

3.6. Отключенная доверенная загрузка

Причина ошибки: отключение доверенной загрузки (Рисунок 9).

Решение: обратиться к администратору для включения доверенной загрузки.

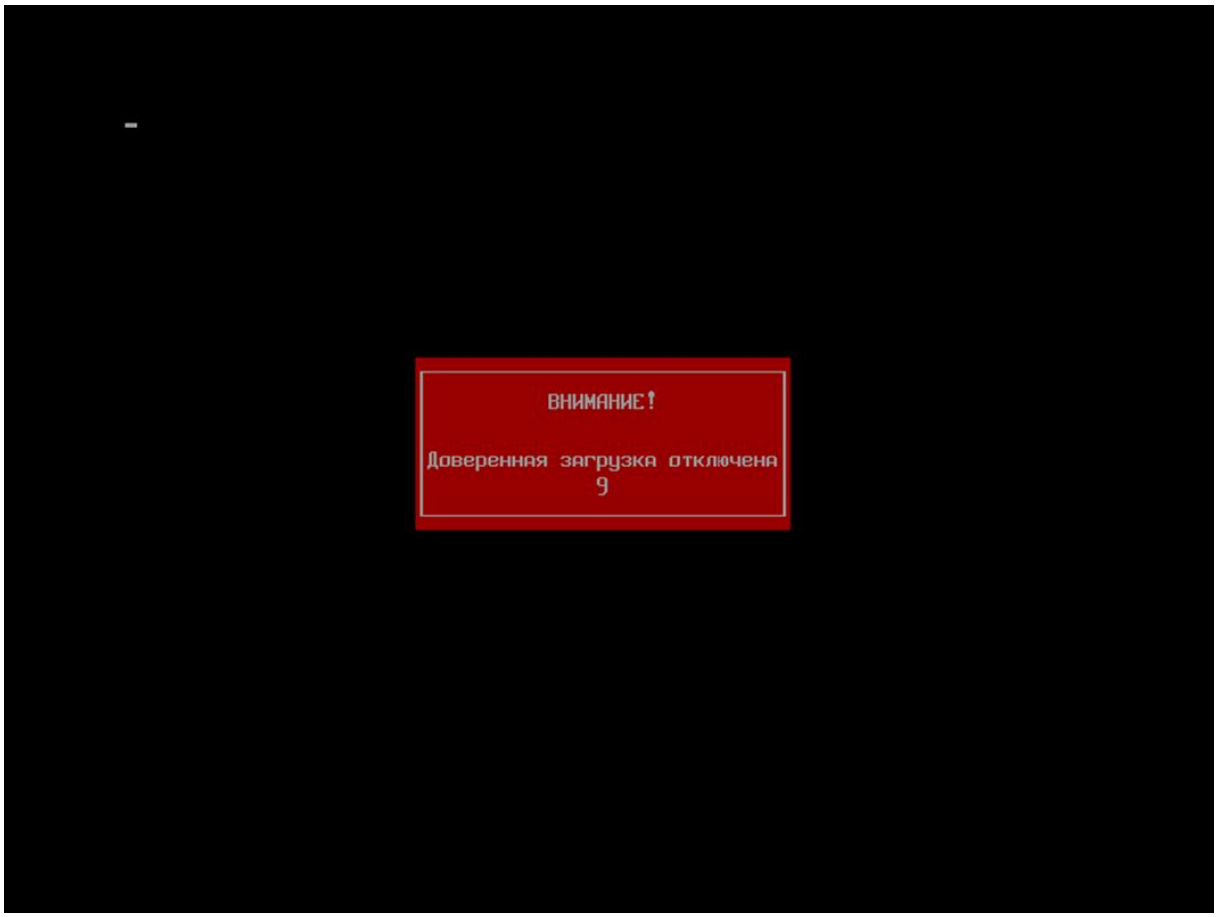

Рисунок 9

3.7. Ошибка системы

Причина ошибки: появление ошибки во время текущей или одной из предыдущих загрузок устройства (Рисунок 10).

Решение: обратиться к администратору для проверки журнала и решения возникших проблем.

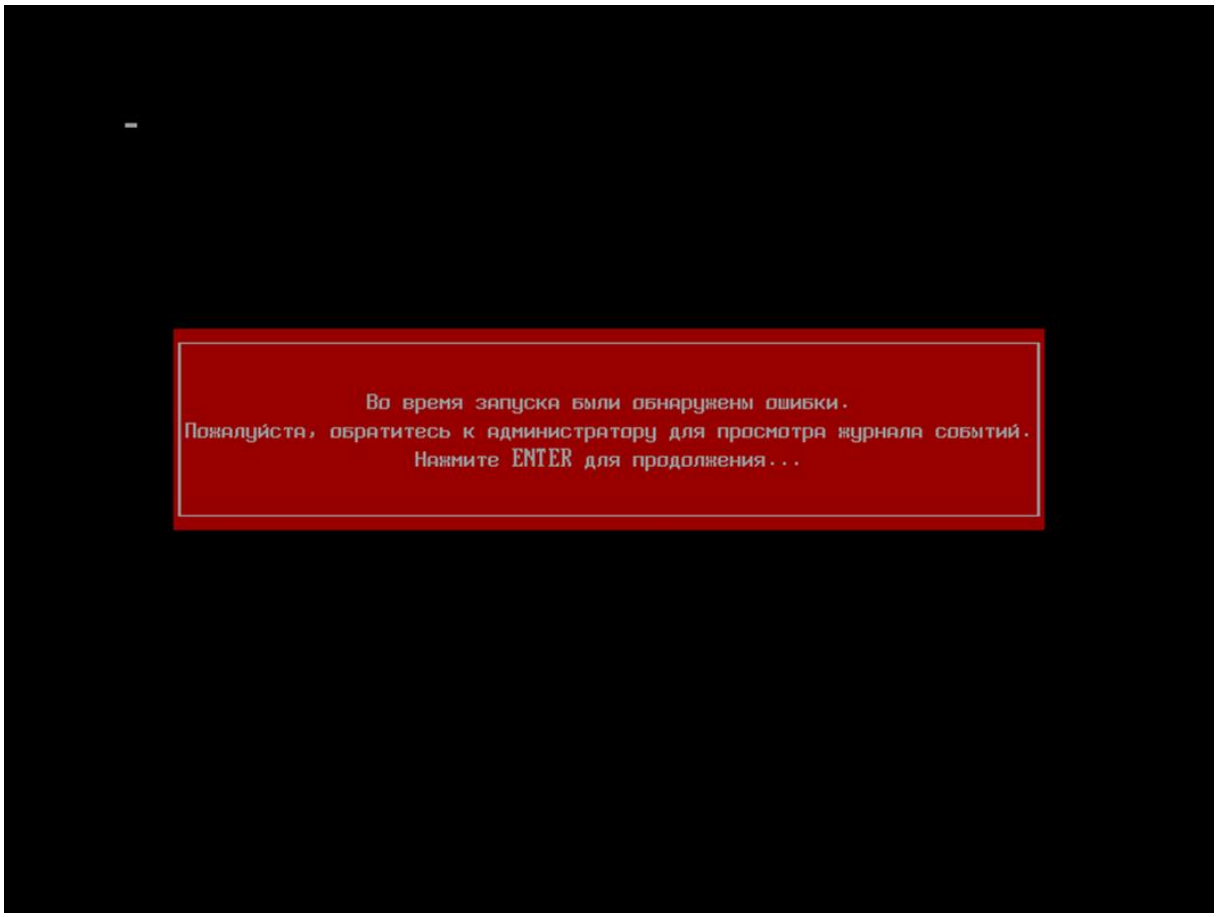

Рисунок 10

3.8. Черный экран

Причина ошибки: отображение черного экрана и отсутствие признаков загрузки ОС могут означать ошибку работы ОС или невозможность установить какой-либо вариант загрузки.

Решение: обратиться к администратору для проверки вариантов загрузки и целостности образов ОС.

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

Используемые в настоящем документе термины и сокращения приведены в таблице (Таблица 1).

Таблица 1

Термин/ Сокращение	Расшифровка
Аврора СДЗ	Средство доверенной загрузки Аврора
Администратор	Пользователь, обладающий правами на выполнение операций, связанных с администрированием системы
ОС	Операционная система
Пользователь	Лицо, использующее систему для выполнения заложенных в ней функций
AP	Application Processor - прикладной процессор
SCP	System Control Processor - управляющий процессор
UEFI	Unified Extensible Firmware Interface - унифицированный расширяемый микропрограммный интерфейс

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					