ГАЗИНФОРМ СЕРВИС

Средство доверенной загрузки «SafeNode System Loader»

Руководство по эксплуатации
Часть 4

Руководство пользователя

Санкт-Петербург, 2018

Содержание

Введение

Настоящее руководство средства доверенной загрузки (СДЗ) «SafeNode System Loader» (далее по тексту – изделие) является эксплуатационным документом (ЭД), содержащим информацию о действиях пользователя по прохождению аутентификации и идентификации, а также порядок действий при возникновении и устранении ошибок в ходе работы изделия.

Установка изделия должная осуществляться в соответствии с рекомендациями документа «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 1. Руководство по установке. ГМТК.468269.060РЭ1».

Настройка изделия должна осуществляться в соответствии с рекомендациями документов «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 2. Руководство администратора. ГМТК.468269.060РЭ2» или «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 3. Руководство администратора Linux/Windows. ГМТК.468269.060РЭ3».

Сведения по безопасному восстановлению изделия после сбоев приведены в документе «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 5. Руководство по восстановлению. ГМТК.468269.060РЭ5».

Знаки, расположенные на полях руководства, указывают на примечания.

Степени важности примечаний:

 **Важная информация, информация предостерегающего характера.**

 Дополнительная информация, примеры.

1 Назначение и основные функциональные возможности изделия

1.1 Назначение изделия

1.1.1 Изделие является разработкой ООО «Газинформсервис», представляет собой программно-техническое средство, встраиваемое в базовую систему ввода-вывода электронно-вычислительной машины (ЭВМ), и обеспечивающее невозможность подключения нарушителя в разрыв между базовой системой ввода-вывода и СДЗ для несанкционированного доступа.

Изделие обеспечивает доверенную загрузку операционных систем (ОС), установленных на совместимые с архитектурой Intel x86-64 ЭВМ.

Результатом доверенной загрузки ОС является гарантия санкционированной загрузки зарегистрированным пользователем. Загрузка ОС на ЭВМ выполняется только после проведения контроля целостности (КЦ) аппаратной и программной конфигурации ЭВМ, гарантирующей невозможность подмены ОС на этапе загрузки и работу пользователей с доверенной ОС в штатном режиме.

1.2 Основные функциональные возможности изделия

1.2.1 ПО изделия имеет модульную структуру и обеспечивает следующие основные функциональные возможности:

- идентификация пользователей с помощью уникальных учетных записей и соответствующих им паролей;
- аутентификация пользователей с использованием персональных идентификаторов (АНП) и уникальных PIN-кодов к ним. Поддерживается работа со следующими АНП:
  - JaCarta PKI, JaCarta ГОСТ (USB-носитель и смарт-карта), JaCarta PKI/ГОСТ, JaCarta-2 ГОСТ (USB-носитель и смарт-карта);
  - Рутокен ЭЦП, Рутокен ЭЦП 2.0 (USB-носитель и смарт-карта), Рутокен Lite, Рутокен 2151, Рутокен ЭЦП PKI (смарт-карта);
  - eToken Pro Java;
  - SafeNet eToken 5100, SafeNet eToken 5105, SafeNet eToken 5200, SafeNet eToken 5205.

    В таблице 1.2 приведено соответствие между применяемыми идентификаторами и грифами секретности защищаемой с их помощью информации.
- блокировка загрузки пользователями нештатных копий ОС;

- блокировка возможности обхода процесса доверенной загрузки с помощью внешних органов управления;
- обеспечение защищенности паролей пользователей и PIN-кодов при выполнении операций их ввода-вывода;
- КЦ: объектов файловой системы, каталогов, объектов реестра ОС семейства Microsoft Windows, аппаратных устройств ЭВМ, загрузочных секторов устройств хранения данных, переменных и драйверов среды UEFI, таблиц ACPI и SMBIOS среды UEFI, завершенности транзакций журналов файловых систем NTFS, EXT3, EXT4;
- блокировка доверенной загрузки ОС при нарушении пользователями установленных политик безопасности (нарушения политик КЦ и загрузки ОС, аутентификации);
- доверенная загрузка ОС, установленных на совместимые с архитектурой Intel x86-64 ЭВМ;
- доверенная загрузка ОС семейств Linux/Unix, поддерживающих стандарт Linux Standard Base (LSB) версии не ниже 3.0, в том числе систем виртуализации VMware ESX, VMware ESXi, установленных на совместимые с архитектурой Intel x86-64 ЭВМ;
- доверенная загрузка ОС на ЭВМ со стандартным Legacy/PnP BIOS (в режиме «Legacy Boot», спецификация PnP BIOS версии 1.0A);
- доверенная загрузка ОС на ЭВМ с интерфейсами EFI/UEFI (спецификация UEFI версии не ниже 2.0);
- поддержка доверенной загрузки ОС с MBR и GPT-разделов;
- регистрация событий в журнале аудита о действиях пользователей и администратора безопасности (АБ);
- диагностика программных средств изделия.

Таблица 1.2 – Уровни конфиденциальности информации при использовании персональных электронных идентификаторов

№ п/п	Наименование	Производитель	Сведения о сертификате	Гриф секретности	Примечание
1	eToken	ЗАО «АЛАДДИН Р.Д.»	Сертификат ФСТЭК России № 1883	КИ	
2	JaCarta		Сертификат ФСТЭК России № 3449	КИ	
3	SafeNet eToken	ЗАО «СИС»	Сертификат ФСТЭК России № 2730	КИ	

4	Рутокен (Rutoken)	АО «Актив Софт»	Сертификат ФСТЭК России № 1461	С	
5			Сертификат ФСТЭК России № 2584	КИ	
6			Сертификат ФСТЭК России № 2589	КИ	

1.2.2 **Требования к аппаратному и программному обеспечению ЭВМ и указания по эксплуатации изделия** приведены в документе «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 1. Руководство по установке. ГМТК.468269.060РЭ1».

1.3 Организационно-технические меры для обеспечения безопасности при работе пользователя с изделием

1.3.1 Для поддержки необходимого уровня защищенности ЭВМ с установленным изделием пользователю необходимо соблюдать следующие условия:

- работа с изделием должна осуществляться в соответствии с документом «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 4. Руководство пользователя. ГМТК.468269.060РЭ4»;
- хранить в секрете идентификаторы (имена), пароли (коды), а также PIN-коды аутентификационных носителей пользователей (АНП);
- производить периодическую смену паролей и PIN-кодов АНП пользователей, в соответствии с установленными политиками безопасности;
- установка и эксплуатация изделия должна выполняться только с действующей лицензией на использование, входящей в комплект поставки изделия. Не допускается эксплуатация изделия после истечения срока действия лицензии на использование. Изделие не выполняет функции защиты после истечения срока действия лицензии на использование.

2 Описание старта изделия

2.1 Первоначальный запуск изделия

2.1.1 Установка изделия должна осуществляться в соответствии с указаниями ЭД «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 1. Руководство по установке. ГМТК.468269.060РЭ1».

2.1.2 Модуль псевдографического интерфейса СДЗ поддерживает автономную (локальную) модель управления работой изделия, предполагается, что ранее была выполнена предварительная установка и запуск изделия на ЭВМ.

2.1.3 При успешной загрузке ПО изделия (предварительно установленного и настроенного) на экране ЭВМ появится окно псевдографического интерфейса изделия с приглашением к идентификации и аутентификации пользователей (рисунок 2.1).

Рисунок 2.1 – Приглашение к идентификации и аутентификации пользователя

2.2 Ввод идентификационных и аутентификационных данных

2.2.1 Пользователи, на рабочих местах которых установлено изделие, получают доступ к загрузке ОС только после прохождения процедуры аутентификации и идентификации в ПО изделия.

2.2.2 Для начала работы пользователям необходимо получить у АБ учетные данные: логин, пароль и (или) персональный идентификатор и PIN-код.

Если идентификация и аутентификация пользователя осуществляется с использованием персонального идентификатора, то его необходимо подключить к ЭВМ до загрузки ПО изделия.

При работе с АНП необходимо соблюдать следующие рекомендации:

- **на ЭВМ с AMI BIOS запрещается переподключение АНП после старта ПО изделия;**
- **при использовании АНП SafeNet 5200 и SafeNet 5205 на устройстве Acer Veriton N4660G для корректного определения носителей необходимо отключить один из USB-портов устройства в UEFI BIOS.**

2.2.3 Запуск ПО изделия осуществляется автоматически при каждом включении ЭВМ. При успешной загрузке ПО изделия на экране появится окно с приглашением к идентификации и аутентификации пользователя (рисунок 2.1).

2.2.4 Окна ввода идентификационных и аутентификационных данных появляются на экране автоматически и последовательно, в соответствии с политикой аутентификации, назначенной пользователю, и успешной проверкой введенных им данных.

2.2.5 По умолчанию всем пользователям установлены общие количественные (8 попыток) и временные ограничения (15 минут) на идентификацию и аутентификацию (рисунок 2.1). При истечении общего времени аутентификации или количества попыток экран ЭВМ будет автоматически заблокирован и пользователям будет доступна только перезагрузка или выключение ЭВМ (рисунки 2.2 и 2.3 соответственно).

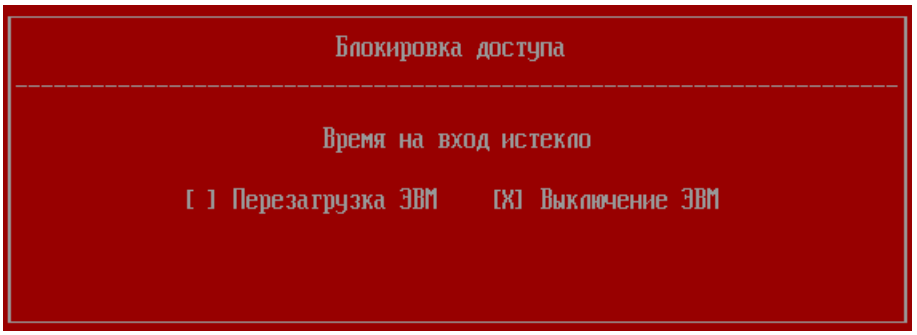


Рисунок 2.2 – Блокировка доступа при истечении времени на аутентификацию пользователей

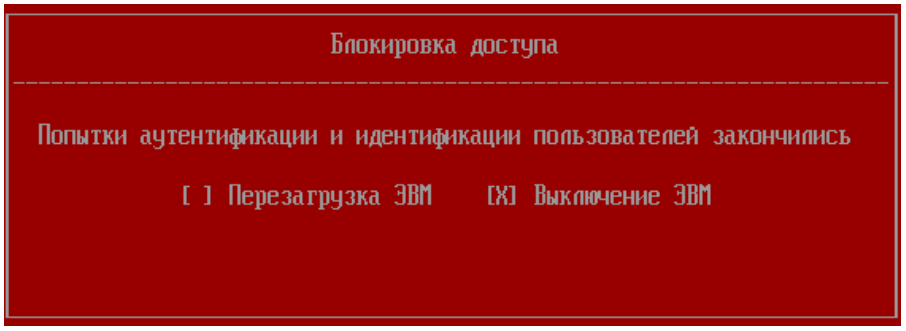


Рисунок 2.3 – Блокировка доступа при исчерпании количества попыток аутентификации пользователей

2.3 Описание псевдографического интерфейса

2.3.1 Псевдографический интерфейс окон изделия имеет интерфейс, похожий на интерфейс базовой системы ввода-вывода UEFI BIOS. Изменение значений параметров в данном интерфейсе осуществляется только при помощи выбора или ввода значений с клавиатуры (рисунок 2.4).

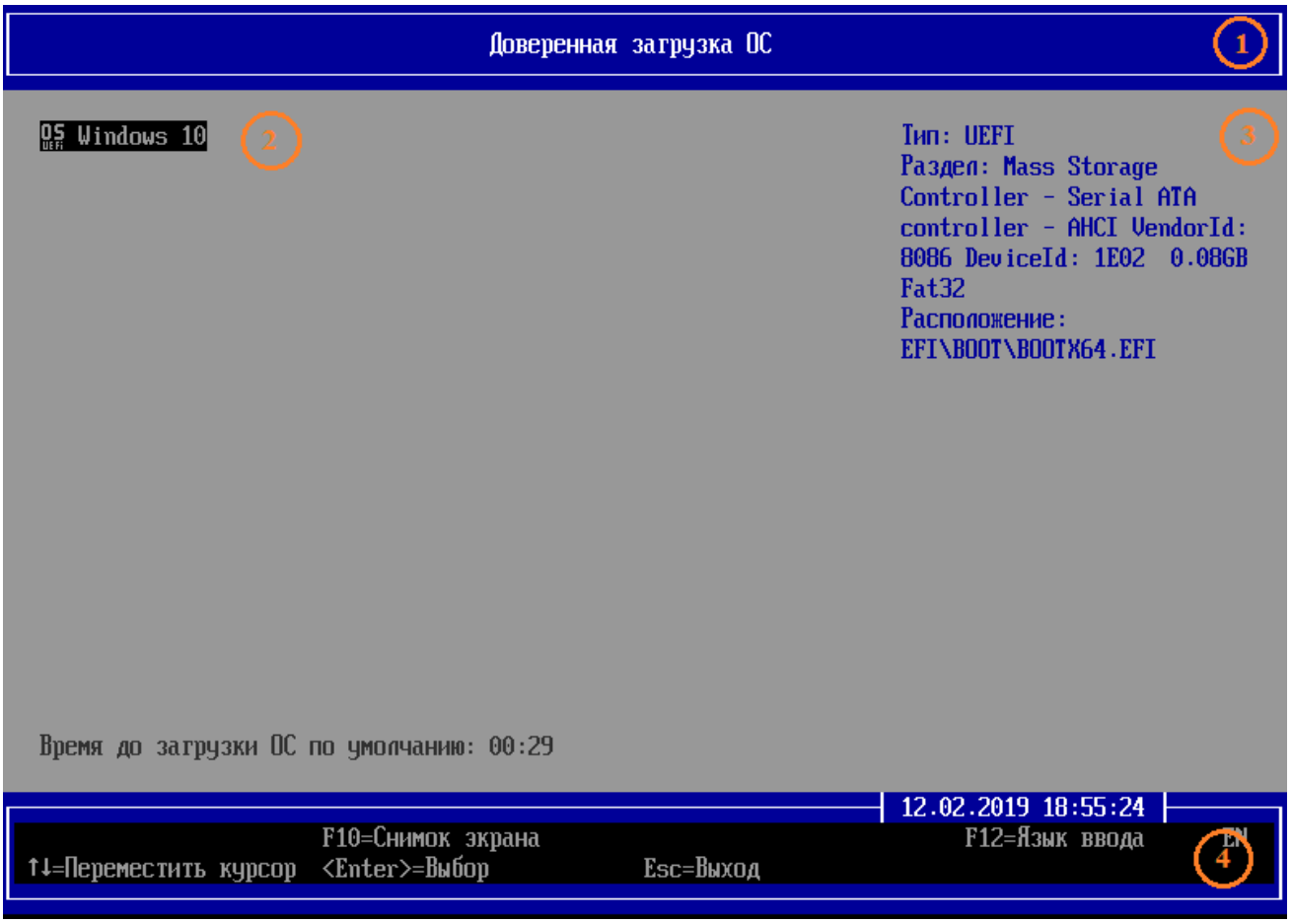


Рисунок 2.4 – Псевдографический интерфейс окон изделия

2.3.2 На рисунке 2.4 цифрами в кругах обозначены:

- поле 1 – заголовок;
- поле 2 – список доступных для просмотра и редактирования групп параметров;
- поле 3 – краткая справка по выделенному курсором параметру;
- поле 4 – подсказка по функциональным клавишам и поле с текущей датой и временем.

2.3.3 Функциональная клавиша ***< F10 >*** сохраняет снимок текущего экрана в предварительно созданную директорию …\SDZ_Scr на любом устройстве хранения данных, в том числе отчуждаемом.

2.3.4 Переключение языков ввода (английский, русский) осуществляется при помощи функциональной клавиши ***< F12 >***. В правом нижнем углу интерфейса отображается текущий язык ввода (рисунок 2.4).

2.3.5 Для выхода из основного окна псевдографического интерфейса (рисунок 2.4) к основному окну идентификации и аутентификации пользователей (рисунок 2.1) пользователю необходимо нажать клавишу ***< Esc >***.

2.3.6 При работе с псевдографическим интерфейсом изделия изменение параметров возможно путем ввода или выбора значений из известного списка **только с помощью клавиатуры.**

При работе с псевдографическим интерфейсом изделия необходимо руководствоваться **следующими правилами:**

- перемещение по разделам и параметрам полей интерфейса изделия осуществляется с помощью **клавиш управления курсором ↓ и ↑**;
- выбор соответствующего поля и подтверждение ввода значения (сохранение параметров) осуществляется при помощи нажатия клавиши ***< Enter >***;
- выход в предыдущее окно, отмена введенного значения или отказ от действия осуществляется при помощи нажатия клавиши ***< Esc >***.

3 Аутентификация и идентификация пользователя

3.1 Идентификация и аутентификация с использованием пароля

3.1.1 Для прохождения аутентификации с использованием пароля пользователю необходимо в окне идентификации и аутентификации (рисунок 2.1):

- в поле ***«Имя пользователя»*** ввести имя пользователя и нажать клавишу **< *Enter* >** (рисунок 3.1);
- в поле ***«Пароль»*** ввести имя пользователя и нажать клавишу **< *Enter* >** (рисунок 3.2).

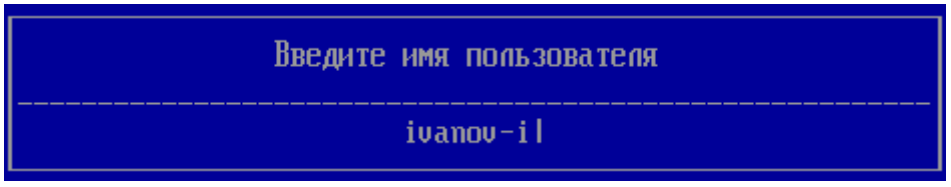


Рисунок 3.1 – Ввод имени пользователя

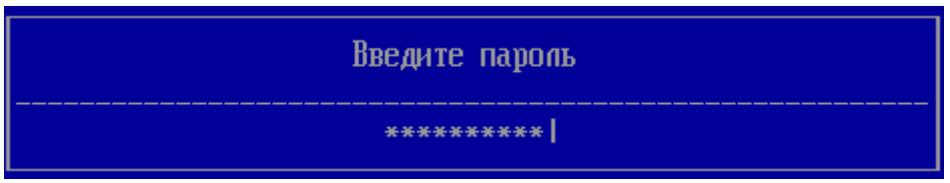


Рисунок 3.2 – Ввод пароля

В окне ввода пароля в целях обеспечения защиты аутентификационных данных при операциях ввода/вывода, на экране ЭВМ отсутствуют в явном виде вводимые пользователями символы, и вместо них на экране ЭВМ отображаются символы « * ».

3.1.2 При правильном вводе логина пользователя и его пароля, изделие выполнит проверку целостности аппаратных и программных объектов ЭВМ. При отсутствии нарушений на экран ЭВМ будет выведено диалоговое окно с разрешением доверенной загрузки ОС (рисунок 3.13).

3.1.3 Сложность пароля или PIN-кода АНП пользователей определяется путем использования в нем сочетания заглавных букв, строчных букв, цифр и специальных символов из определенного разработчиком алфавита пароля, указанного в таблице 3.1.

Таблица 3.1 – Алфавит пароля и PIN-кодов пользователей

№	Наименование	Допустимые символы	Количество символов, шт.
1	Заглавные буквы	A…Z	26
		А…Я	33
2	Строчные буквы	a…z	26
		а…я	33
3	Цифры	0…9	10
4	Специальные символы	! @ # $ % ^ & * ( ) _	11
Итого:			**139**

3.2 Идентификация и аутентификация с использованием персонального идентификатора и PIN-кода

3.2.1 Если в политике аутентификации АБ назначен тип аутентификации пользователя с использованием персонального идентификатора и PIN-кода в окне идентификации и аутентификации после заполнения имени пользователя станут доступны для заполнения поля ***«Персональный идентификатор»*** и ***«PIN-код»*** (рисунки 3.3 – 3.5).

Рисунок 3.3 – Ввод персонального идентификатора

3.2.2 Для выбора персонального идентификатора пользователя и ввода PIN-кода к нему необходимо:

- подключить идентификатор пользователя к ЭВМ;
- перейти курсором в строку ***«Выберите Ваш персональный идентификатор»*** (рисунок 3.3) и в новом диалоговом окне (рисунок 3.4) выбрать требуемый персональный идентификатор из списка поддерживаемых в изделии нажатием клавиши **< *Enter* >**;
- выбранный персональный идентификатор будет выделен < угловыми скобками >;
- нажать клавишу | ***OK*** | (рисунок 3.4), перейти курсором в поле ***«PIN-код»*** (рисунок 3.5) и нажать клавишу **< *Enter* >**;
- ввести PIN-код персонального идентификатора (рисунок 3.5).

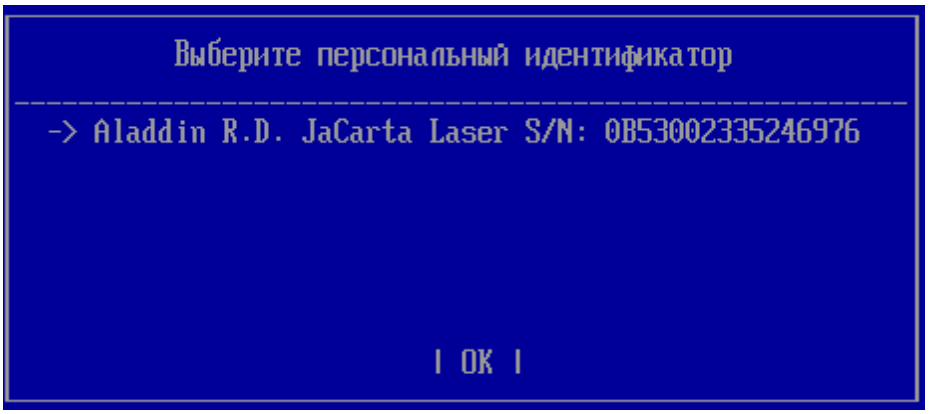


Рисунок 3.4 – Выбор персонального идентификатора пользователя

Рисунок 3.2.1 – Ввод PIN-кода персонального идентификатора пользователя

В случае неверно указанного PIN-кода на экран ЭВМ будет выведено сообщение об ошибке ***«Ошибка аутентификации и идентификации пользователя»***.

3.2.3 После выполнения успешной аутентификации и идентификации пользователя изделие выполнит проверку целостности аппаратных и программных объектов ЭВМ. При отсутствии нарушений на экран ЭВМ будет выведено диалоговое окно с разрешением доверенной загрузки ОС (рисунок 3.13).

3.3 Идентификация и аутентификация с использованием пароля, персонального идентификатора и PIN-кода

3.3.1 Если в политике аутентификации АБ задан тип аутентификации пользователя с использованием пароля, персонального идентификатора и PIN-кода, в окне идентификации и аутентификации, после заполнения имени пользователя, станут доступны поля ***«Пароль»***, ***«Персональный идентификатор»*** и ***«PIN-код»***.

Рисунок 3.3.1 – Аутентификация пользователя с использованием пароля, персонального идентификатора и PIN-кода

3.3.2 Правила заполнения полей ввода пароля, персонального идентификатора и PIN-кода описаны в подразделах 3.1 и 3.2.

3.3.3 После выполнения успешной аутентификации и идентификации пользователя изделие выполнит проверку целостности аппаратных и программных объектов ЭВМ.

При отсутствии нарушений на экран ЭВМ будет выведено диалоговое окно с разрешением доверенной загрузки ОС (рисунок 3.13).

3.4 Смена пароля и/или PIN-кода персонального идентификатора пользователя

3.4.1 Пользователи имеют возможность внесения изменений в свои аутентификационные данные – пароля и/или PIN-кода персонального идентификатора (в зависимости от указанного АБ типа аутентификации пользователя в политике аутентификации). При этом смена пароля и/или PIN-кода пользователем осуществляется принудительно ПО изделия или по требованию самого пользователя.

3.4.2 Смена пароля и/или PIN-кода пользователем осуществляется в следующих случаях:

- АБ при конфигурации учетной записи пользователя установлено требование об изменении аутентификационных данных после первого входа (принудительная смена) (рисунок 3.7);
- при истечении максимального срока действия пароля и/или PIN-кода (равносильно истечению срока действия политики аутентификации).

3.4.3 При возникновении ситуации п. 3.4.2 после успешного прохождения процедуры аутентификации и идентификации на экран ЭВМ будет выведено диалоговое окно, в котором принудительно требуется сменить аутентификационные данные (рисунок 3.7).

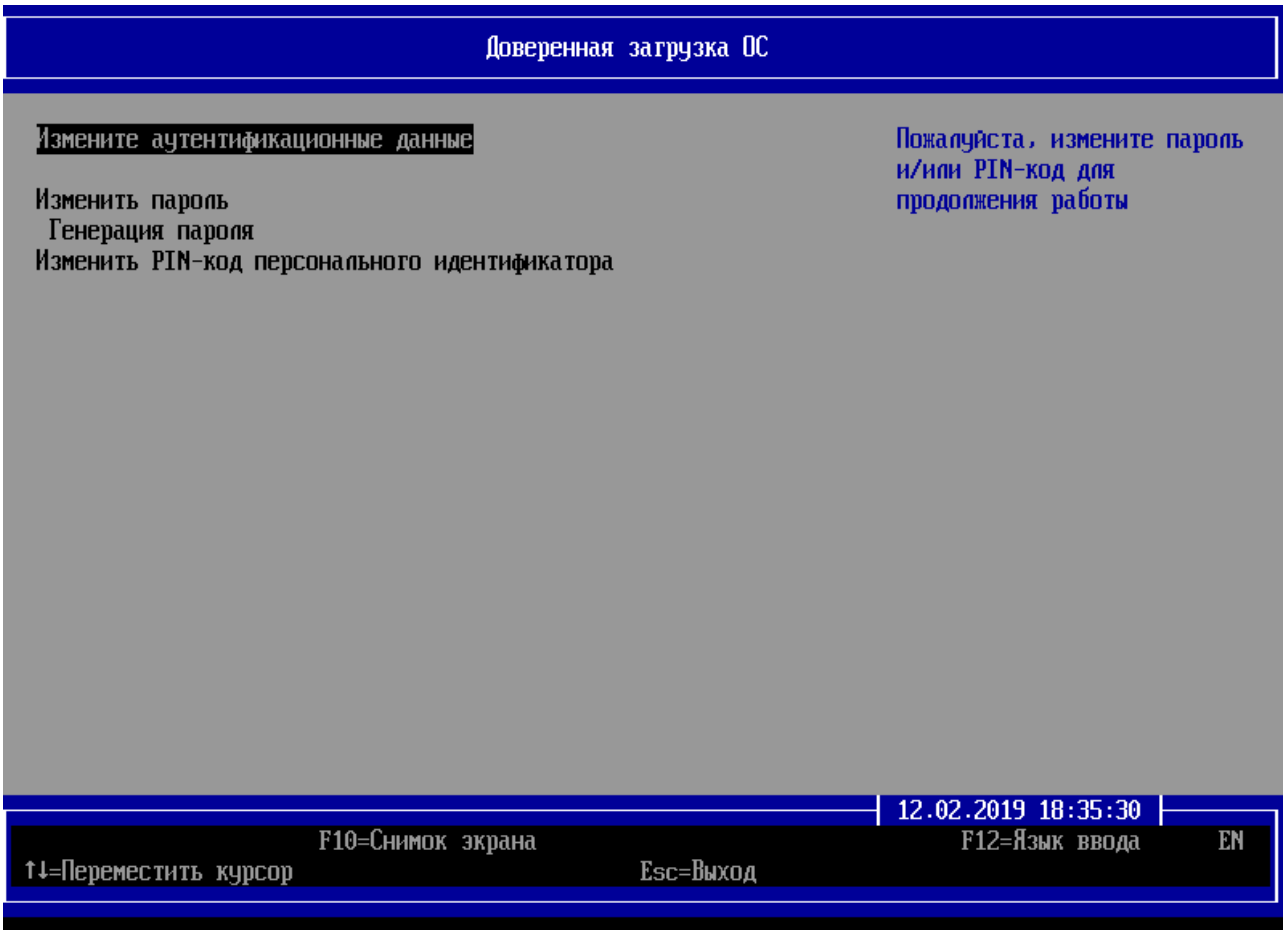


Рисунок 3.7 – Смена пароля и/или PIN-кода пользователем по требованию АБ

3.4.4 Для смены пароля пользователю необходимо перейти в поле ***«Изменить пароль»*** или и в открывшемся диалоговом окне ввести новый пароль (рисунок 3.8).

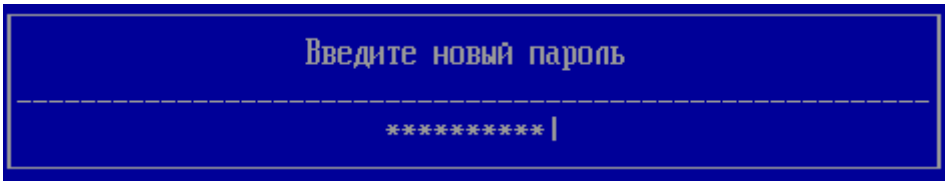


Рисунок 3.8 – Ввод нового пароля

3.4.5 Если введенный пароль соответствует всем требованиям к сложности пароля в заданной политике аутентификации, то на экране ЭВМ появится окно с сообщением ***«Повторите новый пароль»*** для контроля правильного введения символов пароля. После повторного введения пароля, если данные введены безошибочно, пользователю будет выдано сообщение об успешном изменении пароля (рисунок 3.9).

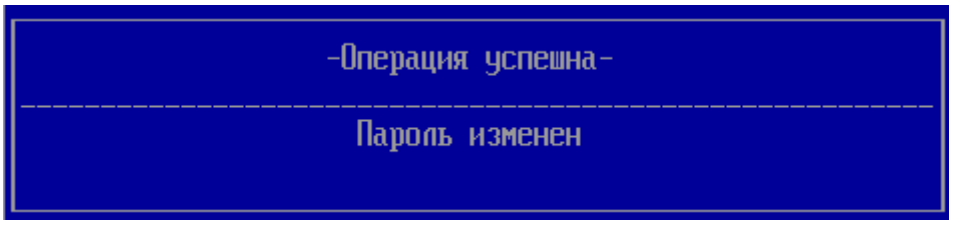


Рисунок 3.9 – Успешная смена пароля

При вводе пароля следует учитывать следующие особенности:

- требования к паролю (длина, сложность) заданы по умолчанию в политике аутентификации ***user policy***;
- ввод подтверждения пароля является обязательным, ПО изделия анализирует введенные значения, не отображая их в явном виде на экране ЭВМ;
- при несовпадении значений пароля и его подтверждения открывается диалоговое окно с сообщением ***«Пароли не совпадают!»***;
- при вводе пароля, не соответствующего требованиям политики аутентификации, на экране ЭВМ появляется диалоговое окно с соответствующим сообщением: ***«Слишком короткий пароль!»*** или ***«Отсутствует заглавная буква»*** (перечень возможных ошибок описан в таблице 7.1).

3.4.6 Для смены PIN-кода персонального идентификатора пользователю необходимо перейти в поле ***«Изменить PIN-код персонального идентификатора»***. В открывшемся диалоговом окне потребуется ввести текущий PIN-код (рисунок 3.10) для подтверждения принадлежности персонального идентификатора пользователю. Далее следует ввести новый PIN-код идентификатора и повторить его в окне с сообщением ***«Введите новый PIN-код»*** для контроля правильного введения символов PIN-кода (рисунок 3.11).

Рисунок 3.10 – Ввод старого PIN-кода

Рисунок 3.11 – Ввод нового PIN-кода

3.4.7 Если данные введены пользователем без ошибок, то на экране ЭВМ появится сообщение об успешном изменении PIN-кода персонального идентификатора.

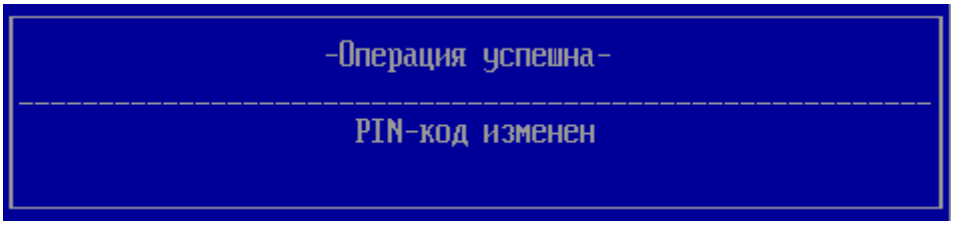


Рисунок 3.12 – Успешная смена PIN-кода

3.4.8 Смена аутентификационных данных самим пользователем возможна по истечению минимального срока действия. После успешного прохождения процедуры аутентификации и идентификации пользователем в окне выбора ОС для доверенной загрузки (рисунок 3.13) станет активным пункт ***«Изменить пароль»*** и/или ***«Изменить PIN-код персонального идентификатора»*** (в зависимости от назначенного АБ типа аутентификации пользователя в политике аутентификации).

3.4.9 Для смены аутентификационных данных пользователю необходимо повторить действия пунктов 3.4.2 – 3.4.6.

3.4.10 После успешной смены пароля и/или PIN-кода идентификатора пользователь может продолжить выбор ОС для доверенной загрузки (рисунок 3.13).

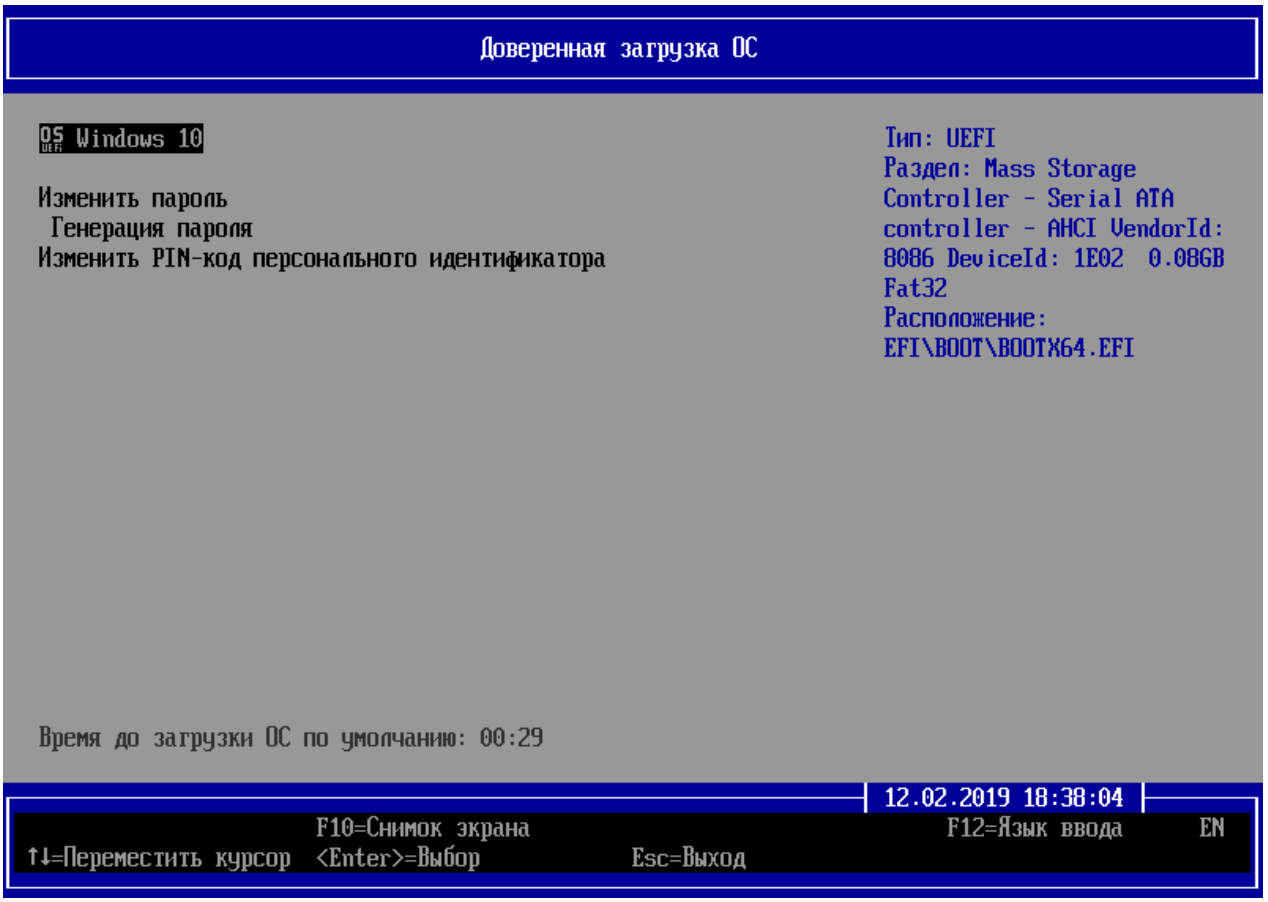


Рисунок 3.13 – Выбор ОС для доверенной загрузки с возможностью изменения пароля пользователя и PIN-кода персонального идентификатора

3.5 Ограничения при аутентификации

3.5.1 В ПО изделия предусмотрены ограничения по времени аутентификации пользователей и количеству попыток входа (рисунок 2.1). Для этого АБ устанавливает индивидуальные и общие ограничения при аутентификации всех пользователей. К общим ограничениям относятся количественные (например, в поле ***«Попытки»*** – 8 попыток) и временные (например, в поле ***«Время входа»*** – 10 минут) ограничения на идентификацию и аутентификацию пользователя в системе.

3.5.2 Индивидуальные ограничения при аутентификации, определенные АБ для конкретного пользователя, будут показаны после осуществления неудачной попытки входа пользователя, при этом счетчик общих попыток входа будет уменьшен на единицу и в диалоговом окне появится сообщение ***«Ошибка аутентификации и идентификации пользователя. Осталось попыток: N»***, где N – оставшееся количество индивидуальных попыток входа пользователя в систему (рисунок 3.14).

Рисунок 3.14 – Индивидуальные ограничения при аутентификации пользователя

3.5.3 При исчерпании всех индивидуальных попыток аутентификации пользователя произойдет блокировка учетной записи пользователя, если данный тип реакции на нарушение указан при создании АБ учетной записи пользователя. В данном случае необходимо обратиться к АБ для разблокировки учетной записи.

3.5.4 При истечении общего времени регистрации на экране ЭВМ появится диалоговое окно с сообщением ***«Блокировка доступа»*** и указанием причины блокировки. Пользователю необходимо в открывшемся диалоговом окне (Рисунок 3.) указать требуемую операцию: перезагрузка или выключение ЭВМ. По умолчанию задана операция ***«Выключение ЭВМ»*** (ей соответствует знак «*X*»).

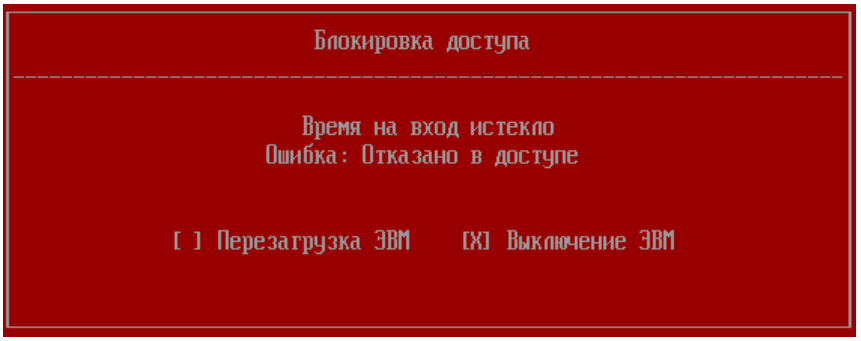


Рисунок 3.15 – Перезагрузка или выключение ЭВМ

4 Выбор ОС для доверенной загрузки

4.1 После выполнения успешной аутентификации и идентификации пользователя изделие выполнит проверку целостности аппаратных и программных объектов ЭВМ. При отсутствии нарушений на экран ЭВМ будет выведено диалоговое окно с разрешением доверенной загрузки ОС (рисунок 4.1).

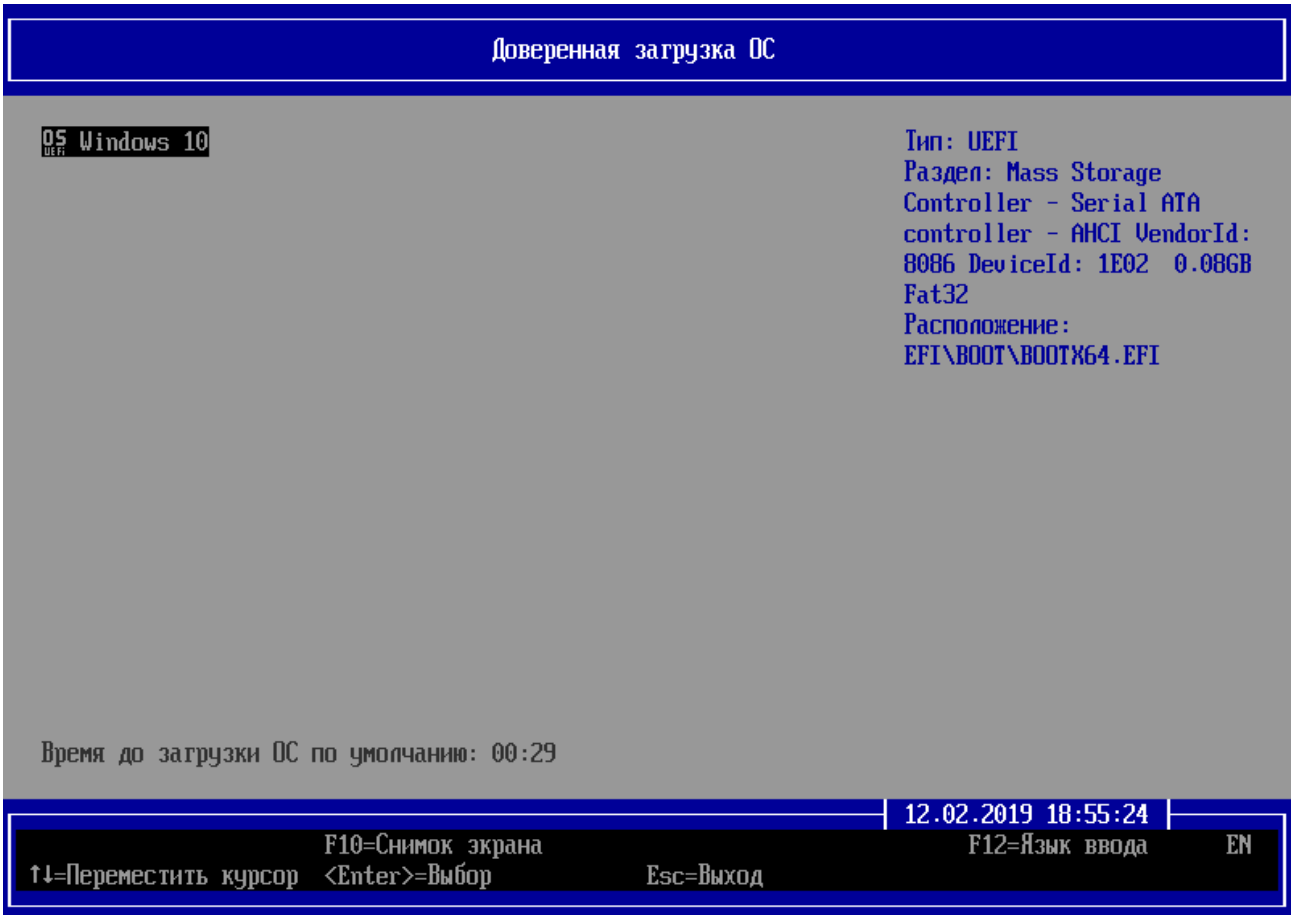


Рисунок 4.1 – Выбор ОС для доверенной загрузки

4.2 Для осуществления доверенной загрузки ОС необходимо выбрать ОС из сформированного списка.

4.3 Если АБ не разрешил для доверенной загрузки пользователю хотя бы одну ОС, то после успешного прохождения идентификации и аутентификации пользователя на экран ЭВМ будет выведено диалоговое окно с сообщением ***«Доступных операционных систем нет»*** (рисунок 4.2).

4.4 В таком случае пользователю необходимо:

- выключить ЭВМ, перейдя в меню действий пользователя (рисунок 6.1) последовательным нажатием клавиши **< *Esc* >** в интерфейсе;

- обратиться к АБ для решения проблемы.

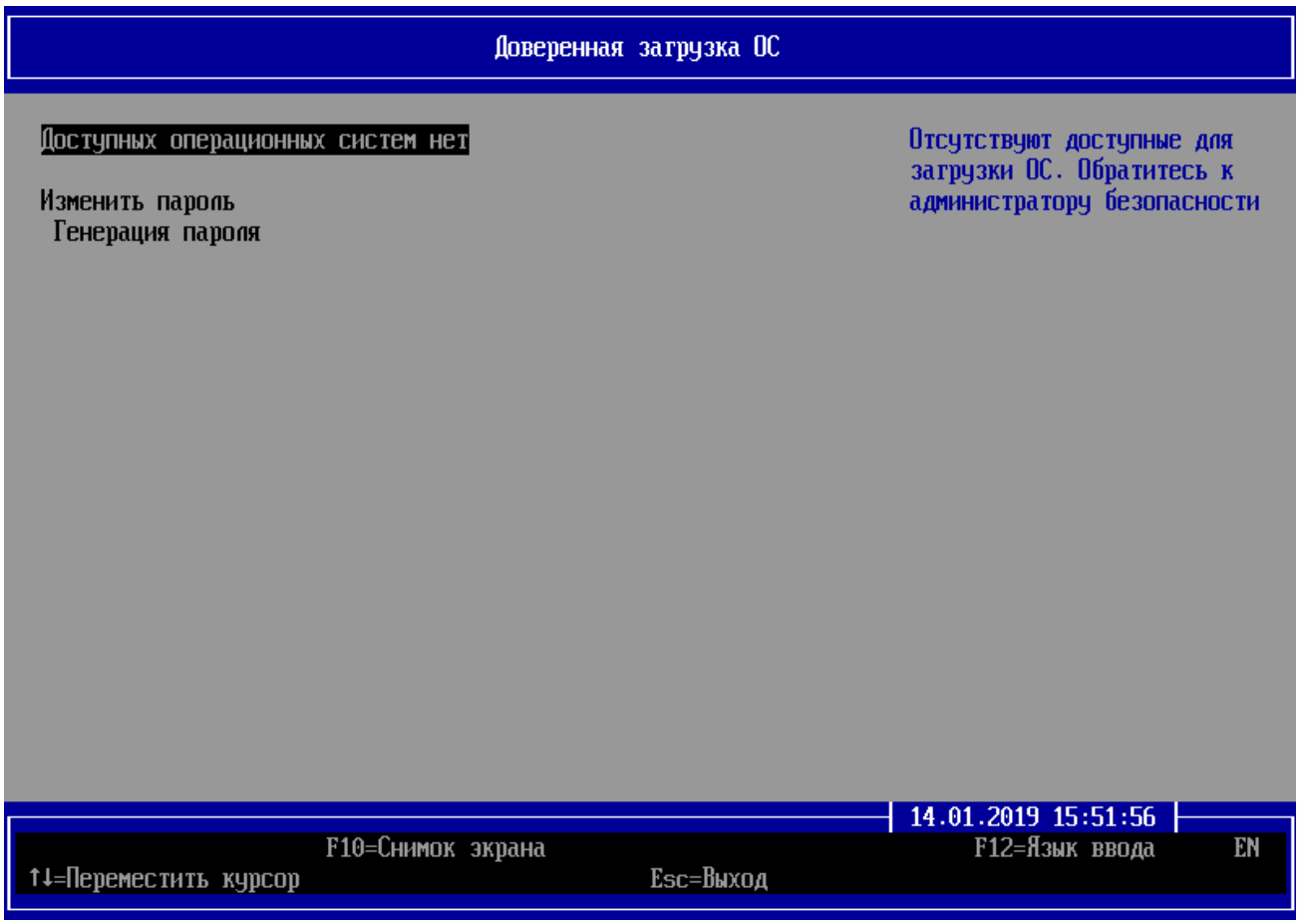


Рисунок 4.2 – Невозможность загрузки ОС пользователю

5 Нарушение политики контроля целостности

5.1 При обнаружении нарушения КЦ в аппаратной и/или программной конфигурации ЭВМ в окне аутентификации и идентификации пользователю будет выведено сообщение ***«Блокировка доступа»*** и пользователь будет заблокирован (рисунок 5.1).

Рисунок 5.1 – Блокировка доступа при обнаружении нарушения КЦ

Если при создании политики КЦ объектов и загрузки ОС был установлен параметр *«Игнорировать»* как реакция при обнаружении нарушения КЦ в аппаратной и/или программной конфигурации ЭВМ, то блокировка учетной записи пользователя осуществлена не будет.

6 Завершение работы с изделием

6.1 Для завершения работы с ПО изделия после загрузки ОС пользователю не требуется производить никаких дополнительных действий.

6.2 При необходимости завершения работы с ПО до загрузки ОС (в этом случае возможен только вариант выключения или перезагрузки ЭВМ), следует перейти в окно ***«Меню действий пользователя»*** (Рисунок 6.1), нажав клавишу **< *Esc* >** после появления окна идентификации и аутентификации пользователя.

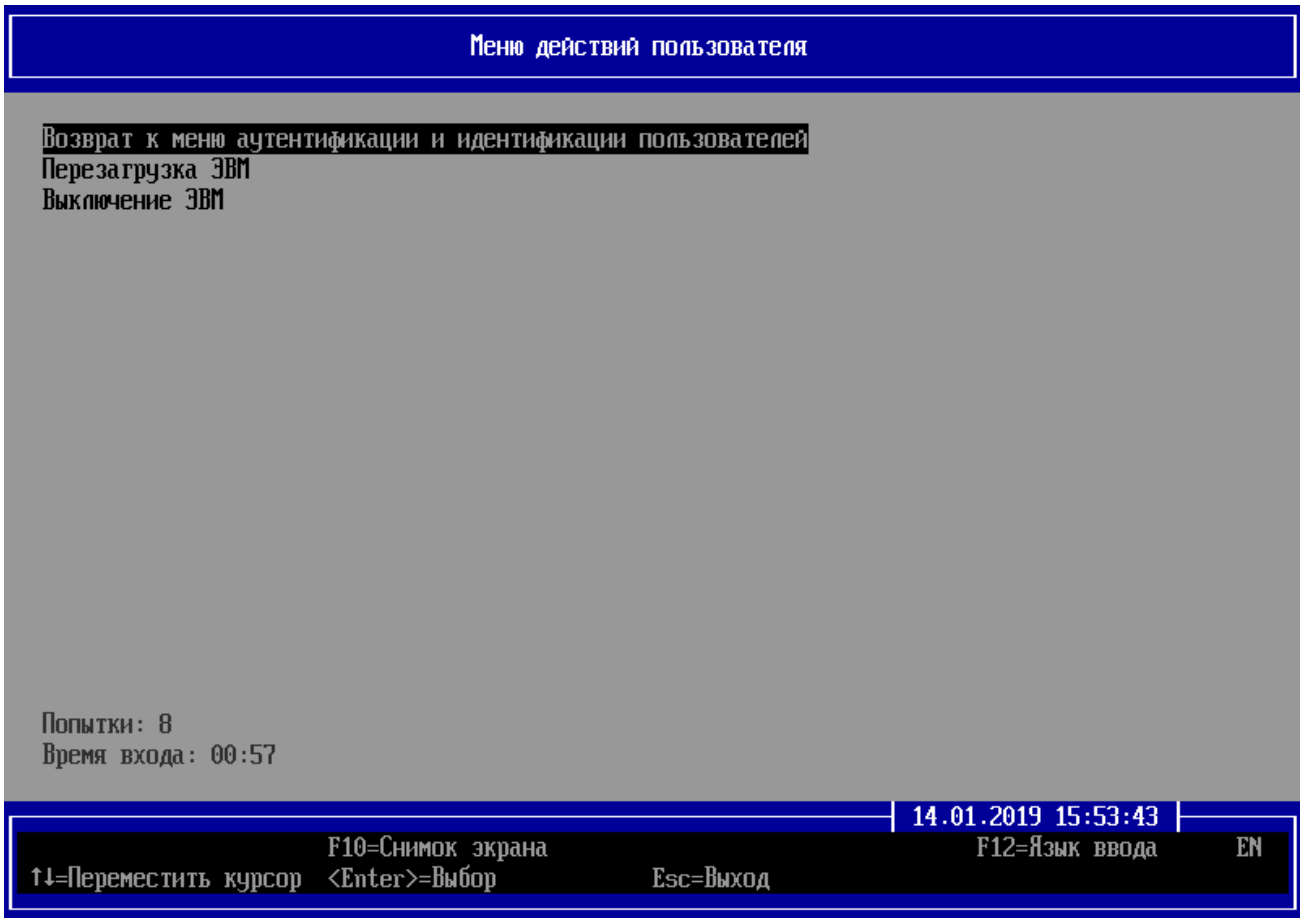


Рисунок 6.1 – Меню действий пользователя

6.3 В окне рисунка 6.1 по умолчанию активным является пункт меню ***««Возврат к меню аутентификации и идентификации пользователей»***, для возврата к меню аутентификации и идентификации пользователей необходимо нажать клавишу **< *Enter* >**.

6.4 Для подтверждения перезагрузки ЭВМ необходимо нажать клавишу **< *Enter* >** и подтвердить действие, выбрав пункт меню ***«Да»*** (рисунок 6.2).

6.5 Для подтверждения выключения ЭВМ необходимо нажать клавишу **< *Enter* >** и подтвердить действие, выбрав пункт меню ***«Да»*** (рисунок 6.3).

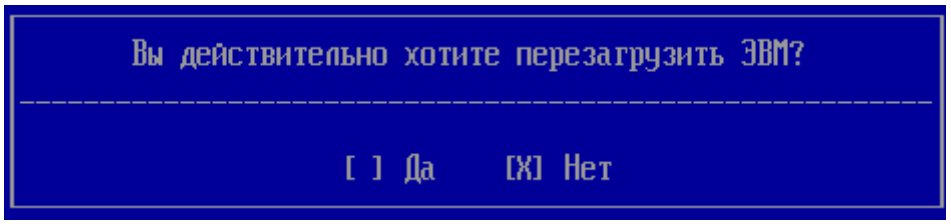


Рисунок 6.2 – Подтверждение действия пользователя для перезагрузки ЭВМ

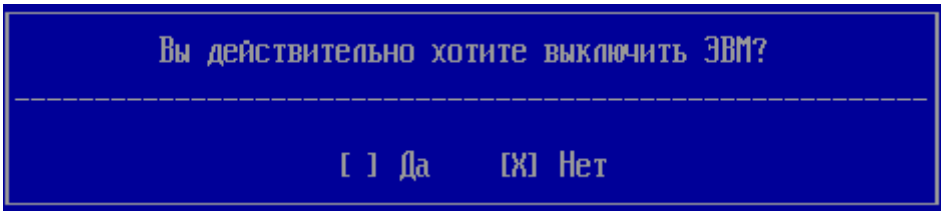


Рисунок 6.3 – Подтверждение действия пользователя для выключения ЭВМ

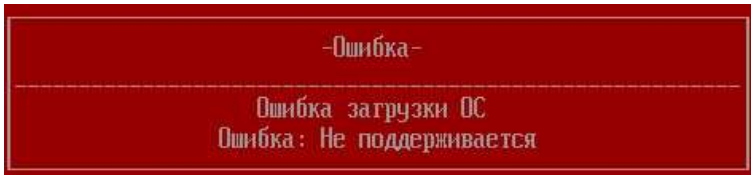
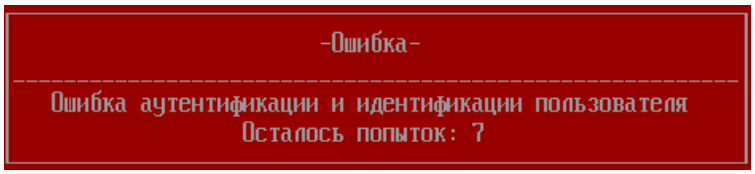
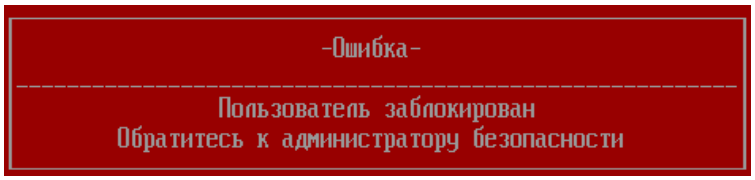
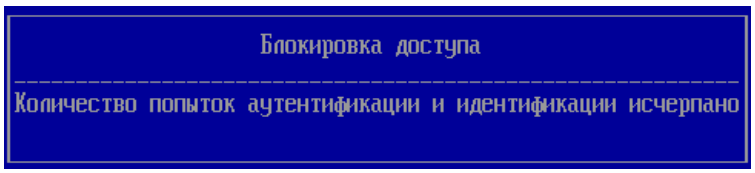
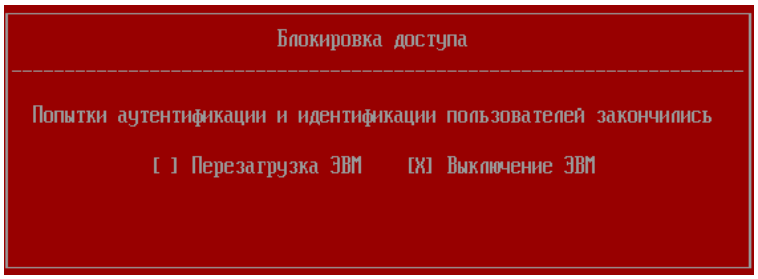
7 Сообщения об ошибках и порядок действий пользователей по их устранению

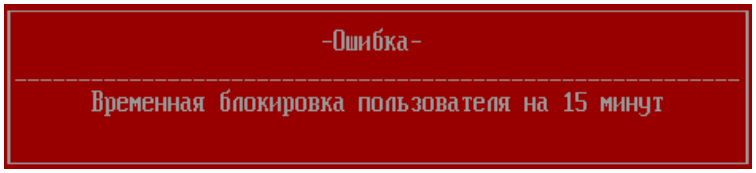
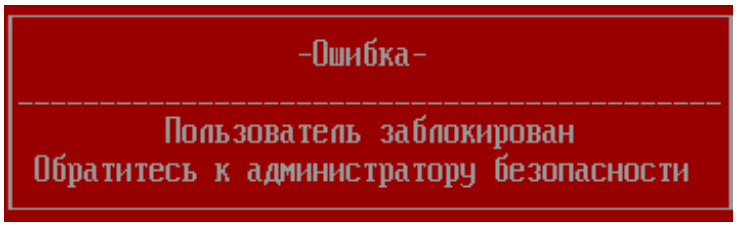
7.1 В процессе работы изделия в составе ЭВМ возможно возникновение ситуаций, при которых пользователям на экран ЭВМ в диалоговых окнах выдаются сообщения об ошибках.

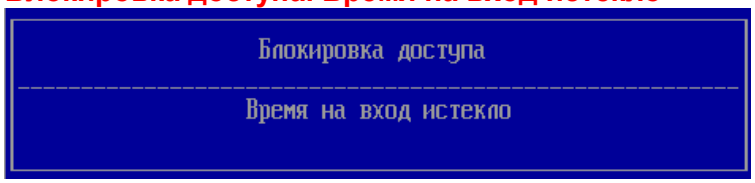
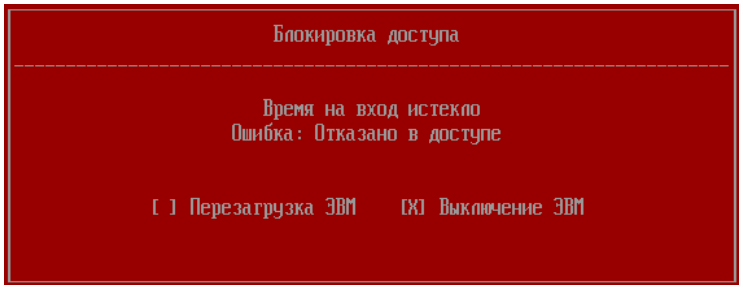
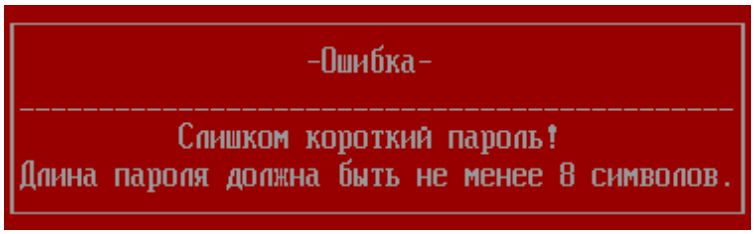
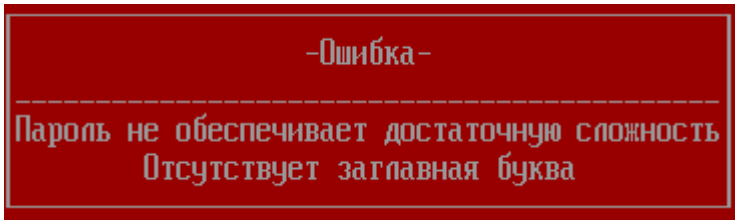
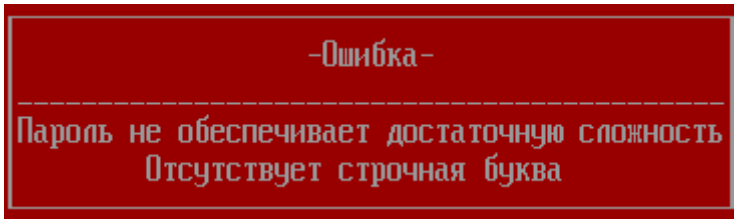
7.2 Перечень сообщений, причины их возникновения и порядок действий пользователей по их устранению приведен в таблице 7.1.

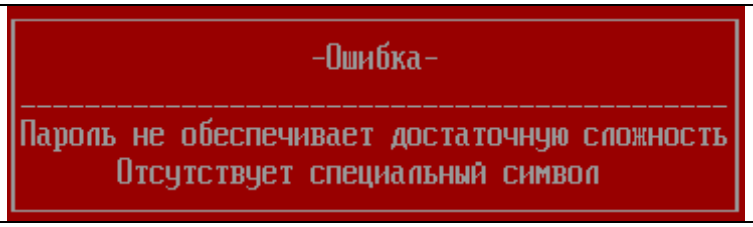
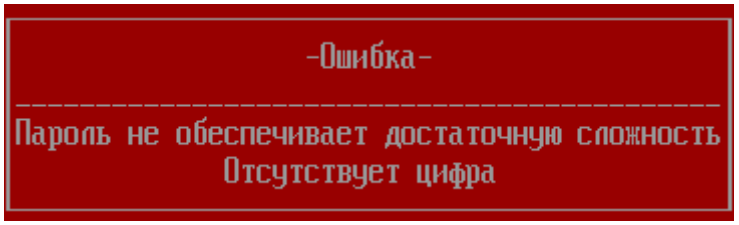
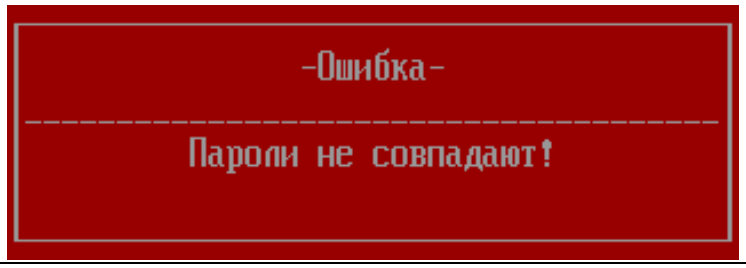
Таблица 7.1 – Перечень сообщений об ошибках при работе с ПО изделия

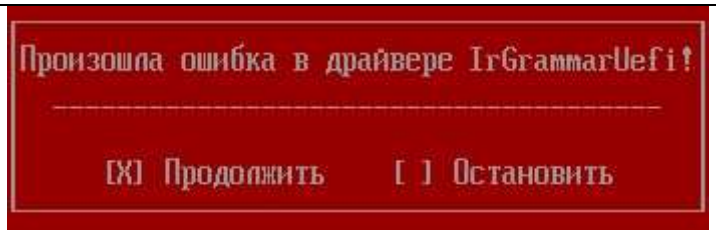
№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий пользователей
1	**Ошибка System blocked!** 	**Причины:** Некорректный ключ базы данных или поврежденная база данных изделия **Порядок действий:** Обратиться к АБ для восстановления изделия
2	**Ошибка System blocked!** 	**Причины:** Несоответствие в проверке электронных подписей модулей ПО **Порядок действий:** Обратиться к АБ для восстановления изделия
3	**Ошибка System blocked!** 	**Причины:** Отсутствие модуля при проверке электронных подписей модулей ПО **Порядок действий:** Обратиться к АБ для восстановления изделия

№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий пользователей
4	**Ошибка загрузки ОС** 	**Причины:** В качестве загрузчика ОС указан неверный файл **Порядок действий:** Указать верный файл загрузчика в пункте меню ***«Контроль загрузки ОС»***
5	**Ошибка аутентификации и идентификации пользователя** 	**Причины:** Указание неверного идентификатора или пароля пользователя **Порядок действий:** Проверить корректность указанных аутентификационных и идентификационных данных пользователя
6	**Блокировка доступа. Количество попыток аутентификации и идентификации исчерпано**   	**Причины:** Возникает при исчерпании всех попыток аутентификации пользователя **Порядок действий:** 1. Выключить ЭВМ или перезагрузить ЭВМ и повторно выполнить процедуру идентификации и аутентификации. 2. При повторении ошибки обратиться к АБ.

№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий пользователей
7	**Временная блокировка пользователя на N минут** 	**Причины:** Достигнуто максимально разрешенное количество индивидуальных попыток аутентификации пользователя **Порядок действий:** Обратиться к АБ
8	**Блокировка доступа. Пользователь заблокирован** 	**Причины:** 1. Нарушение КЦ аппаратной и/или программной конфигурации ЭВМ. У данного пользователя указан тип реакции на нарушении КЦ *«Блокировка пользователя».* 2. Выполнена блокировка учетной записи пользователя, у которого тип реакции на нарушение КЦ указан *«Блокировать всех пользователей».* Учетные записи всех зарегистрированных пользователей блокируются автоматически. 3. При установленной АБ защите от перевода времени, в системе обнаружен перевод времени назад, превышающий допустимый. **Порядок действий:** Обратиться к АБ

№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий пользователей
9	**Блокировка доступа. Время на вход истекло**  	**Причины:** Возникает при истечении общего времени аутентификации пользователей **Порядок действий:** Выключить ЭВМ или перезагрузить ЭВМ и повторно выполнить процедуру идентификации и аутентификации
10	**Слишком короткий пароль!** 	**Причины:** Новый пароль пользователя не удовлетворяет требованиям по минимальной длине пароля **Порядок действий:** Ввести пароль длиной не менее 8 символов
11	**Отсутствует заглавная буква** 	**Причины:** Новый пароль пользователя не удовлетворяет требованиям по сложности **Порядок действий:** Ввести новый пароль, который будет содержать хотя бы одну заглавную букву
12	**Отсутствует строчная буква** 	**Причины:** Новый пароль пользователя не удовлетворяет требованиям по сложности **Порядок действий:** Ввести новый пароль, который будет содержать хотя бы одну строчную букву
13	**Отсутствует специальный символ**	**Причины:** Новый пароль пользователя не удовлетворяет требованиям по сложности

№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий пользователей
		**Порядок действий:** Ввести новый пароль, который будет содержать хотя бы один специальный символ
14	**Отсутствует цифра** 	**Причины:** Новый пароль пользователя не удовлетворяет требованиям по сложности **Порядок действий:** Ввести новый пароль, который будет содержать хотя бы одну цифру
15	**Пароли не совпадают!** 	**Причины:** Несовпадение нового пароля и его подтверждения **Порядок действий:** Ввести верный новый пароль и его подтверждение
16	**Указанный пароль не может быть использован** 	**Причины:** 1. Новый пароль совпадает с паролем, хранимым в базе данных. Размер стека хранимых паролей устанавливается АБ. 2. Новый пароль совпадает с текущим паролем пользователя. **Порядок действий:** 1. Необходимо указать новый пароль пользователя, который не совпадает с предыдущими значениями. 2. Указать новый пароль пользователя, отличный от текущего.
17	**Произошла ошибка в драйвере IrGrammarUefi!**	**Причины:** Ошибка в работе драйвера динамического контроля

№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий пользователей
		исполнения кода изделия **Порядок действий:** Продолжить работу или обратиться к АБ для восстановления системы
18	**Свободное место на файловой системе почти закончилось!** 	**Причины:** Предупреждающее сообщение о заполнении файловой системы на 90%. Возможна аутентификация и идентификация АБ и пользователей **Порядок действий:** Выполнить аутентификацию и идентификацию АБ в системе и сохранить журнал на внешний носитель

Перечень сокращений

ACPI	–	Advanced Configuration and Power Interface (усовершенствованный интерфейс управления конфигурацией и питанием)
BIOS	–	Basic Input Output System (базовая система ввода-вывода)
EXT3, EXT4	–	Extended File System (расширенная файловая система)
GPT	–	GUID Partition Table (таблица разделов GUID, часть спецификации UEFI)
MBR	–	Master Boot Record (главная загрузочная запись)
NTFS	–	New Technology File System (файловая система новой технологии)
PIN	–	Personal Identification Number
PKI	–	Public Key Infrastructure (инфраструктура открытых ключей)
SMBIOS	–	System Management BIOS (системное управление BIOS)
UEFI	–	Unified Extensible Firmware Interface
USB	–	Universal Serial Bus
АБ	–	администратор безопасности
АНП	–	аутентификационный носитель пользователя
ГОСТ	–	государственный стандарт
КИ	–	конфиденциальная информация
КЦ	–	контроль целостности
ОС	–	операционная система
ПО	–	программное обеспечение
С	–	секретно
СДЗ	–	средство доверенной загрузки
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю России
ЭВМ	–	электронно-вычислительная машина
ЭД	–	эксплуатационная документация
ЭЦП	–	электронная цифровая подпись