ГАЗИНФОРМ СЕРВИС

Средство доверенной загрузки «SafeNode System Loader»

Руководство по эксплуатации
Часть 4

Руководство пользователя

Санкт-Петербург, 2024

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

Настройка изделия осуществляется 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 и аутентификация пользователей с помощью учетных записей и соответствующих им паролей с возможностью дополнительной проверки в службе каталогов (AD, FreeIPA, Samba AD DC, ALD Pro[1]);
- аутентификация пользователей с использованием персональных электронных идентификаторов и уникальных PIN-кодов к ним. Поддерживается работа со следующими персональными электронными идентификаторами:
  - JaCarta PKI, JaCarta Pro PKI, JaCarta ГОСТ (USB-носитель и смарт-карта), JaCarta PKI/ГОСТ, JaCarta-2 PKI/ГОСТ, JaCarta-2 ГОСТ (USB-носитель и смарт-карта), JaCarta-2 PRO/ГОСТ (USB-носитель и смарт-карта), JaCarta Flash/PKI, JaCarta SE, JaCarta SF/ГОСТ;
  - Рутокен ЭЦП, Рутокен ЭЦП 2.0 (USB-носитель и смарт-карта), Рутокен ЭЦП 3.0 (USB-носитель и смарт-карта), Рутокен Lite, Рутокен 2151, Рутокен ЭЦП PKI (USB-носитель и смарт-карта), Рутокен ЭЦП 2.0 Flash;
  - eToken Pro Java;

[1] Получение списка пользователей службы каталогов ALD Pro недоступно.

- SafeNet eToken 5100, SafeNet eToken 5105, SafeNet eToken 5200, SafeNet eToken 5205;
- Guardant ID.

В таблице 1.1 приведено соответствие между применяемыми идентификаторами и грифами секретности защищаемой с их помощью информации.

- аутентификация с использованием цифровых сертификатов пользователей. Для хранения сертификата поддерживается работа с персональными электронными идентификаторами, указанными в таблице 1.1;
- аутентификация с использованием цифровых сертификатов пользователей с возможностью дополнительной проверки в службе каталогов (AD, FreeIPA). Для хранения сертификата поддерживается работа с персональными электронными идентификаторами, указанными в таблице 1.1;
- 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;
- контроль целостности: объектов файловой системы, каталогов, объектов реестра ОС семейства Microsoft Windows, аппаратных устройств СВТ, загрузочных секторов устройств хранения данных, переменных и драйверов среды UEFI, таблиц ACPI и SMBIOS, завершенности транзакций журналов файловых систем NTFS, EXT3, EXT4, ресурсов конфигурационного пространства PCI/PCI-E, содержимого энергонезависимой памяти CMOS;
- получение параметров механизмов защиты изделия из средства защиты информации от несанкционированного доступа (СЗИ от НСД) «Блокхост-Сеть 4» и посредством протокола REST API;
- блокировка доверенной загрузки ОС при нарушении пользователями установленных политик безопасности (нарушения политик контроля целостности 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 1.1 – Уровни конфиденциальности информации при использовании персональных электронных идентификаторов

№	Название АНП	Тип носителя	Примечание	Поддерживаемые типы входа	Сведения о сертификате (справочно)	Гриф секретности (справочно)
JaCarta						
1	JaCarta PKI	USB Card		Вход по токену без сертификата	Сертификаты ФСТЭК России № 4446	КИ
2	JaCarta Pro PKI	USB		Вход по токену без сертификата	Сертификаты ФСТЭК России № 4446	КИ
3	JaCarta ГОСТ	USB Card		Вход по токену без сертификата		
4	JaCarta PKI/ГОСТ	USB		Вход по токену без сертификата	Сертификат ФСБ России № СФ/111-2750	КИ
		Card			Сертификаты ФСТЭК России № 4446	КИ
5	JaCarta-2 PKI/ГОСТ	USB		Вход по токену без сертификата	Сертификаты ФСТЭК России № 4446	КИ
		Card		Вход по токену без сертификата	Сертификат ФСБ России № СФ/124-3956	КИ
6	JaCarta-2 ГОСТ	USB		Вход по токену без сертификата	Сертификаты ФСТЭК России № 4446	КИ
		Card			Сертификат ФСБ России № СФ/124-3956	КИ
7	JaCarta-2 PRO/ГОСТ	USB	Вход возможен по апплету PKI	Вход по токену без сертификата	Сертификаты ФСТЭК России № 4446	КИ
		Card			Сертификат ФСБ России № СФ/124-3956	КИ
8	JaCarta Flash/PKI	USB		Вход по токену без сертификата	—	—
9	JaCarta SE	USB		Вход по токену без сертификата	—	—
10	JaCarta SF/ГОСТ	USB		Вход по токену без сертификата	Сертификат ФСБ России № СФ/124-3956	С/СС
Рутокен						

№	Название АНП	Тип носителя	Примечание	Поддерживаемые типы входа	Сведения о сертификате (справочно)	Гриф секретности (справочно)
11	Рутокен ЭЦП	USB		Вход по сертификату в домен Вход по токену без сертификата	—	—
12	Рутокен ЭЦП 2.0	USB (2000)		Вход по сертификату в домен Вход по токену без сертификата	Сертификат ФСТЭК России № 3753	КИ
		USB (2100)			Сертификат ФСБ России № СФ/124-4248 (Рутокен ЭЦП 2.0 2100)	КИ
		Card (2100)			Сертификат ФСБ России № СФ/124-3990 (Рутокен ЭЦП 2.0)	КИ
					Сертификат ФСБ России № СФ/124-4129 (смарт-карта Рутокен ЭЦП 2.0 2100)	КИ
13	Рутокен ЭЦП 3.0	USB (3100 NFC, 3100, 3200, 3220)		Вход по сертификату в домен Вход по токену без сертификата	Сертификат ФСТЭК России № 4582	КИ
					Сертификат ФСБ России № СФ/124-4398 (Рутокен ЭЦП 3.0)	КИ
					Сертификат ФСБ России № СФ/124-4307 (Рутокен ЭЦП 3.0)	КИ
14	Рутокен ЭЦП 3.0 NFS	Card (3100)		Вход по сертификату в домен Вход по токену без сертификата	—	—
15	Рутокен Lite	USB (1000)		Вход по токену без сертификата	Сертификат ФСТЭК России № 3753	КИ
16	Рутокен 2151	USB		Вход по сертификату в домен Вход по токену без сертификата	—	—
17	Рутокен ЭЦП PKI	USB		Вход по сертификату в домен Вход по токену без сертификата	Сертификат ФСТЭК России № 3753	КИ
		Card (1800)				

№	Название АНП	Тип носителя	Примечание	Поддерживаемые типы входа	Сведения о сертификате (справочно)	Гриф секретности (справочно)
18	Рутокен ЭЦП 2.0 Flash	USB (4500)		Вход по сертификату в домен Вход по токену без сертификата	Сертификат ФСБ России № СФ/124-4075 Сертификат ФСТЭК России № 3753	
eToken						
19	eToken Pro Java	USB Card		Вход по токену без сертификата	—	—
20	SafeNet eToken 5100	USB		Вход по токену без сертификата		
21	SafeNet eToken 5105	USB		Вход по токену без сертификата		
22	SafeNet eToken 5200	USB		Вход по токену без сертификата		
23	SafeNet eToken 5205[1)]	USB		Вход по токену без сертификата		
Guardant						
24	Guardant ID	USB		Вход по сертификату в домен Вход по токену без сертификата	Сертификат ФСТЭК России № 4515	СС

Примечание:

[1)] не поддерживается идентификация и аутентификация пользователей с использованием персональных электронных идентификаторов SafeNet 5200 и SafeNet 5205 в виртуальной среде vmware.

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 настоящим документом;
- 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 При успешной загрузке изделия ПО изделия на экране появится окно графического интерфейса изделия с приглашением к аутентификации и идентификации пользователя (рисунок 2.1).

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

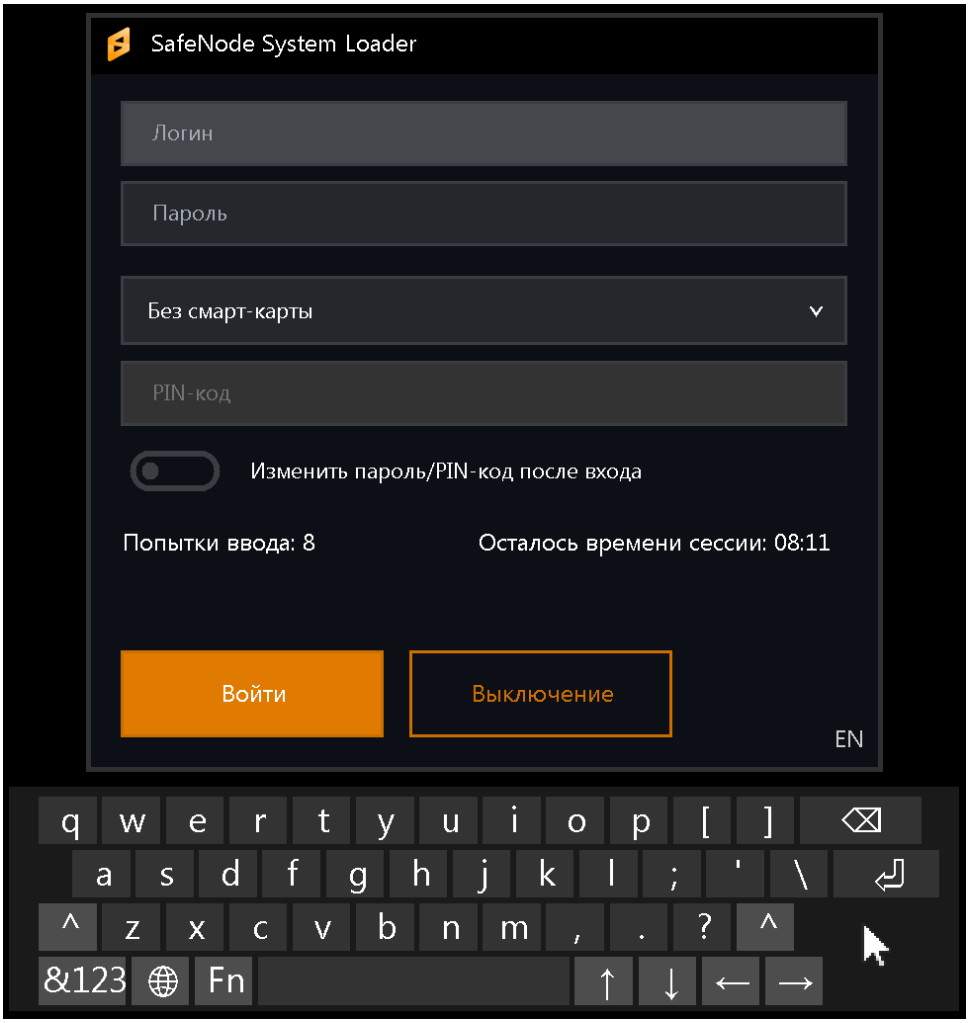


Рисунок 2.1 – Приглашение к идентификации и аутентификации пользователя

При вводе аутентификационных данных поддерживается работа виртуальной клавиатуры и манипулятора «мышь».

Если во время загрузки модулей изделия нажать клавишу ***«О»***, то появится окно для выбора варианта загружаемой консоли (рисунок 2.2):

- псевдографическая консоль СДЗ **(Old style UI)**;
- графической аварийной консоли СДЗ **(New style GUI).**

Рисунок 2.2 – Выбор варианта консоли

После выбора варианта консоли, опция сохраняется и предлагается в дальнейшем по умолчанию. Для смены варианта загрузки консоли необходимо снова во время загрузки модулей изделия нажать клавишу ***«О»*** и выбрать другой вариант консоли.

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

2.1.4 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 2.3).

Рисунок 2.3 – 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:

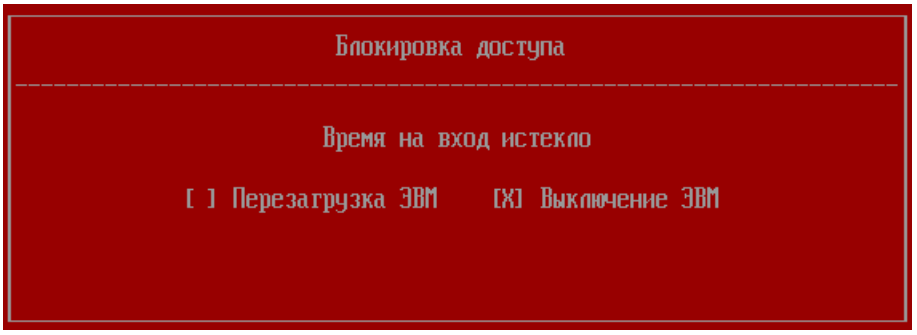
- **на ЭВМ с AMI BIOS запрещается переподключение АНП после старта ПО изделия;**

- **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.**

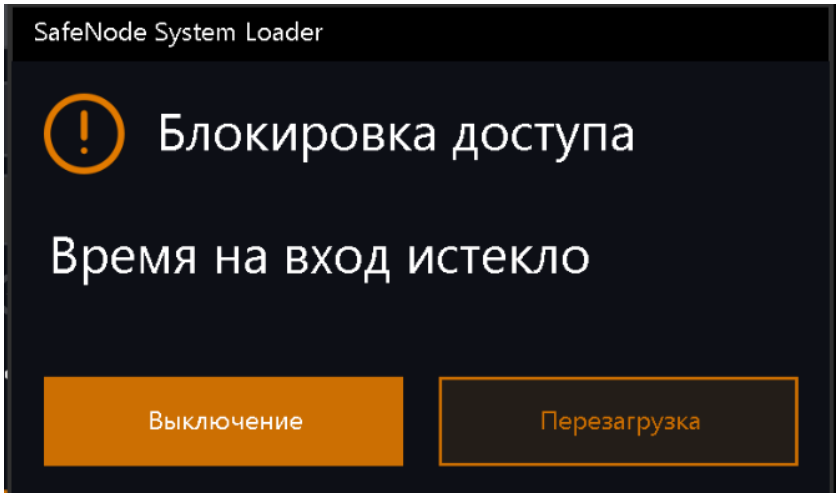
2.2.3 Запуск ПО изделия осуществляется автоматически при каждом включении ЭВМ. При успешной загрузке ПО изделия на экране появится окно с приглашением к идентификации и аутентификации пользователя (рисунок 2.1, 2.2).

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, 2.3). При истечении общего времени аутентификации или количества попыток экран ЭВМ будет автоматически заблокирован и пользователям будет доступна только перезагрузка или выключение ЭВМ (рисунки 2.4 и 2.5 соответственно).

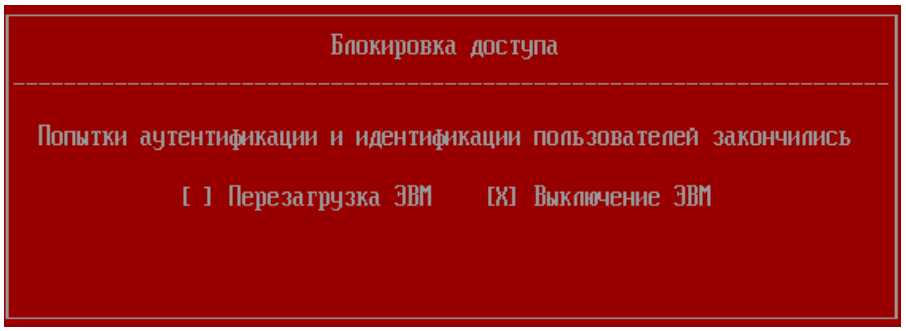


а) Псевдографический интерфейс

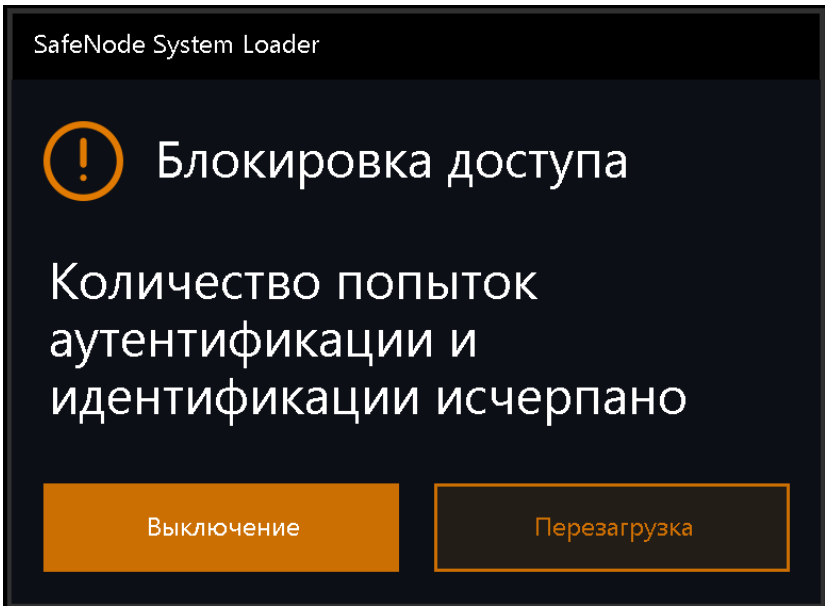


б) Графический интерфейс

Рисунок 2.4 – Блокировка доступа при истечении времени на аутентификацию пользователей



а) Псевдографический интерфейс



б) Графический интерфейс

Рисунок 2.5 – 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 2.6).

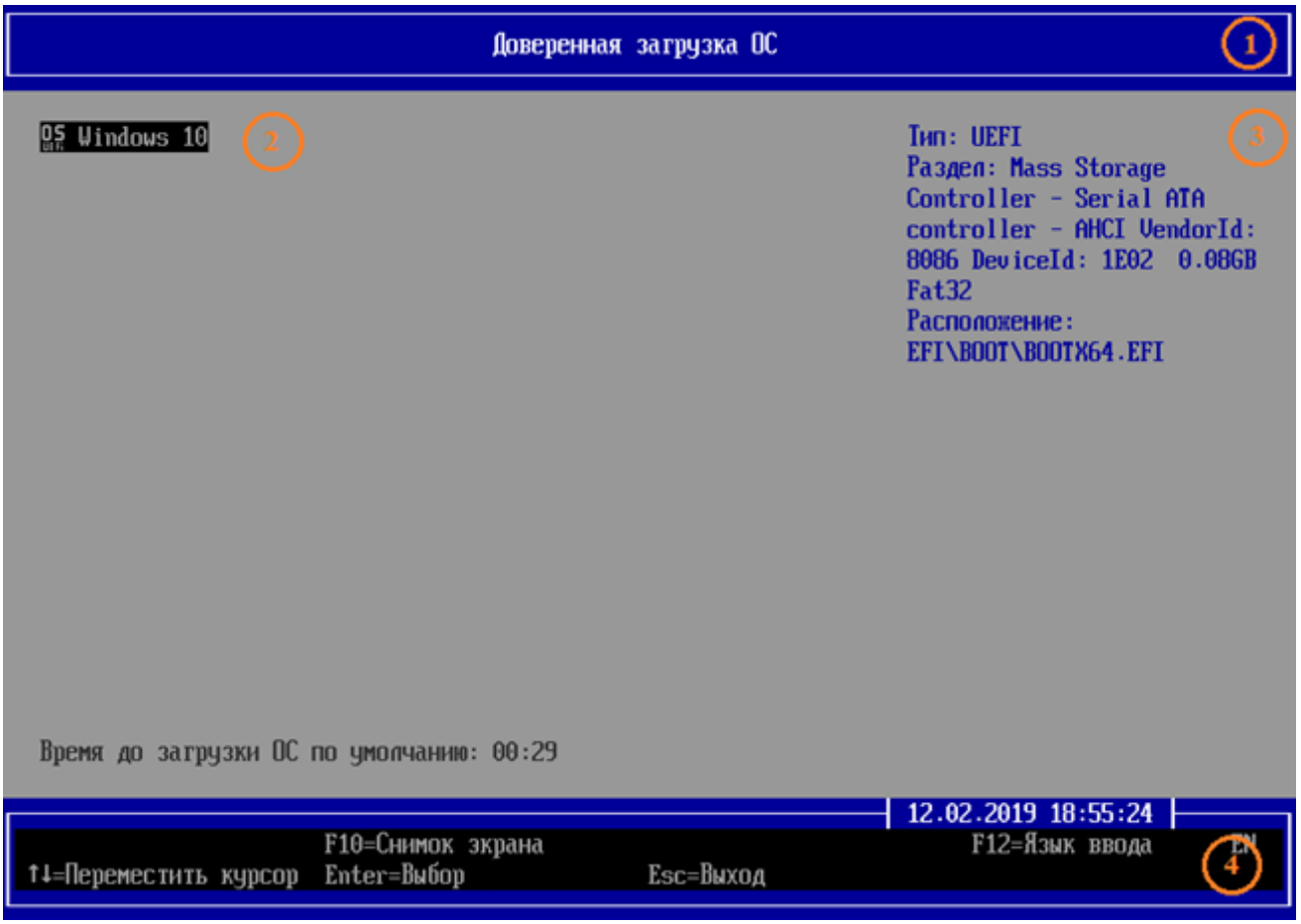


Рисунок 2.6 – Псевдографический интерфейс окон изделия

2.3.2 На рисунке 2.6 цифрами в кругах обозначены:

- поле 1 – заголовок;
- поле 2 – список доступных для просмотра 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 2.5).

2.3.5 Для выхода из основного окна псевдографического интерфейса (рисунок 2.6) к основному окну идентификации и аутентификации пользователей (рисунок 2.3) 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 в графическом интерфейсе

3.1 Идентификация и аутентификация с использованием пароля

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

- в поле ***«Логин»*** ввести имя пользователя;
- в поле «Пароль» ввести имя пользователя и нажать кнопку **< *Войти* >**.

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 « * ».

4.1.4 При правильном вводе имени учетной записи пользователя и его пароля, ПО изделия выполнит проверку целостности аппаратных и программных объектов ЭВМ. При отсутствии нарушений на экран ЭВМ будет выведено диалоговое окно с разрешением доверенной загрузки ОС (рисунок 3.5).

4.1.5 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

№	Наименование	Допустимые символы	Количество символов, шт.
		# $ % ^ & * ( ) _	
Итого:			139

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

3.2.1 Если в политике аутентификации назначен тип аутентификации пользователя с использованием персонального идентификатора и PIN-кода, в окне с приглашением к идентификации и аутентификации необходимо указать в поле для АНП, назначенный АНП пользователю и указать PIN-код (рисунок 2.1).

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

- подключить идентификатор пользователя к ЭВМ;
- выбрать из выпадающего списка соответствующий АНП (рисунок 3.1);
- ввести PIN-код персонального идентификатора в поле ***«PIN-код»*** (рисунок 3.2).

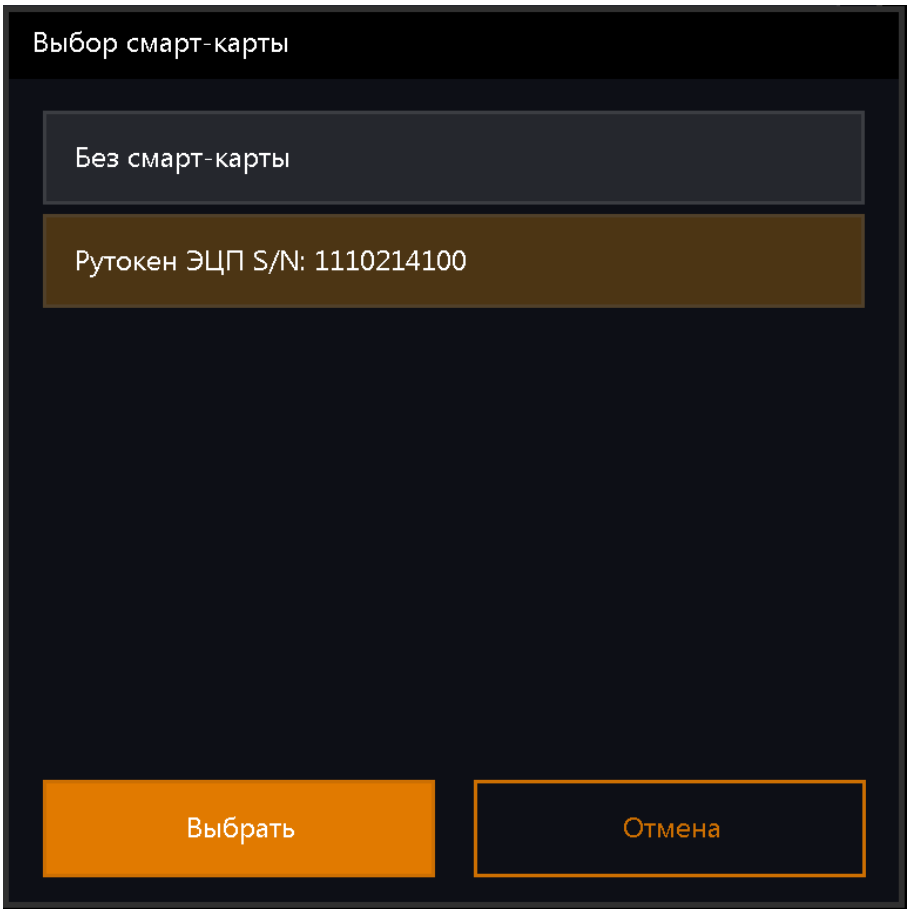


Рисунок 3.1 – Выбор персонального идентификатора

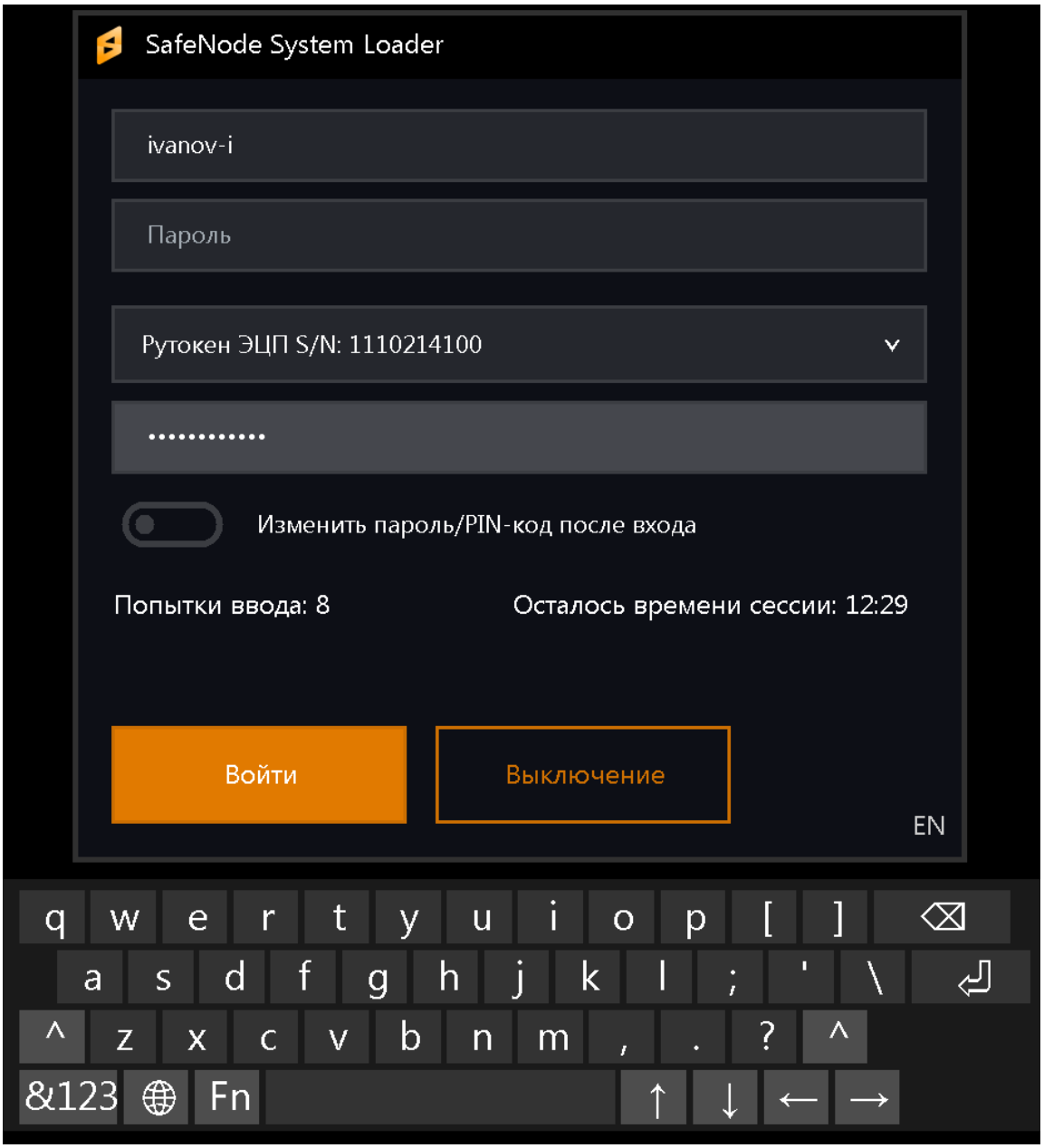


Рисунок 3.2 – Указание данных для аутентификации пользователя

В случае неверно указанного PIN-кода на экран ЭВМ будет выведено сообщение об ошибке: **«Неверная- комбинация имени пользователя и пароля/PIN-кода. Осталось попыток пользователя: N»**.

3.2.3 После выполнения успешной аутентификации и идентификации пользователя ПО изделия выполнит проверку целостности аппаратных и программных объектов ЭВМ. При отсутствии нарушений на экран ЭВМ будет выведено диалоговое окно с разрешением доверенной загрузки ОС (рисунок 3.5).

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 необходимо заполнить соответствующие поля (рисунок 3.3).

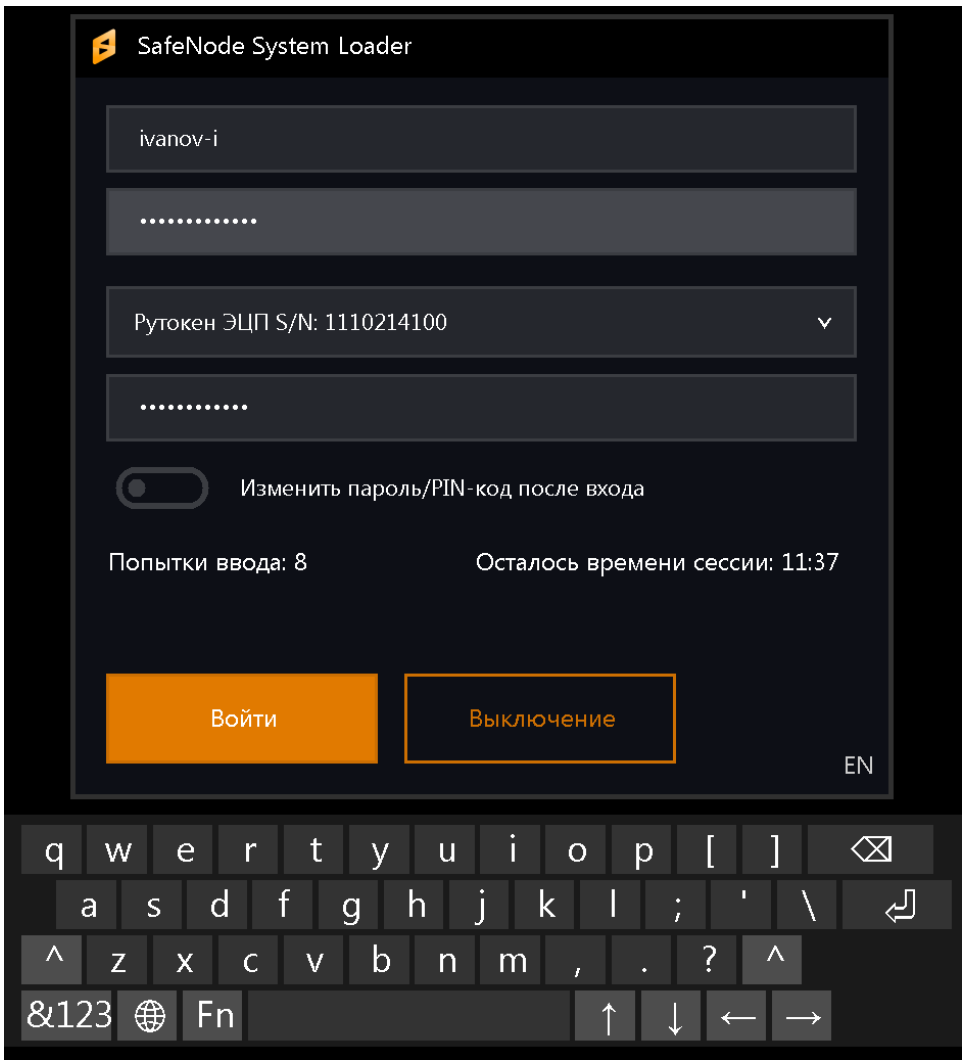


Рисунок 3.3 – Аутентификация пользователя с использованием пароля, персонального идентификатора и PIN-кода

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 ПО изделия выполнит проверку целостности аппаратных и программных объектов

ЭВМ. При отсутствии нарушений на экран ЭВМ будет выведено диалоговое окно с разрешением доверенной загрузки ОС (рисунок 3.5).

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.

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 первой успешной аутентификации (принудительная смена) (рисунок 3.4);
- 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 3.4).

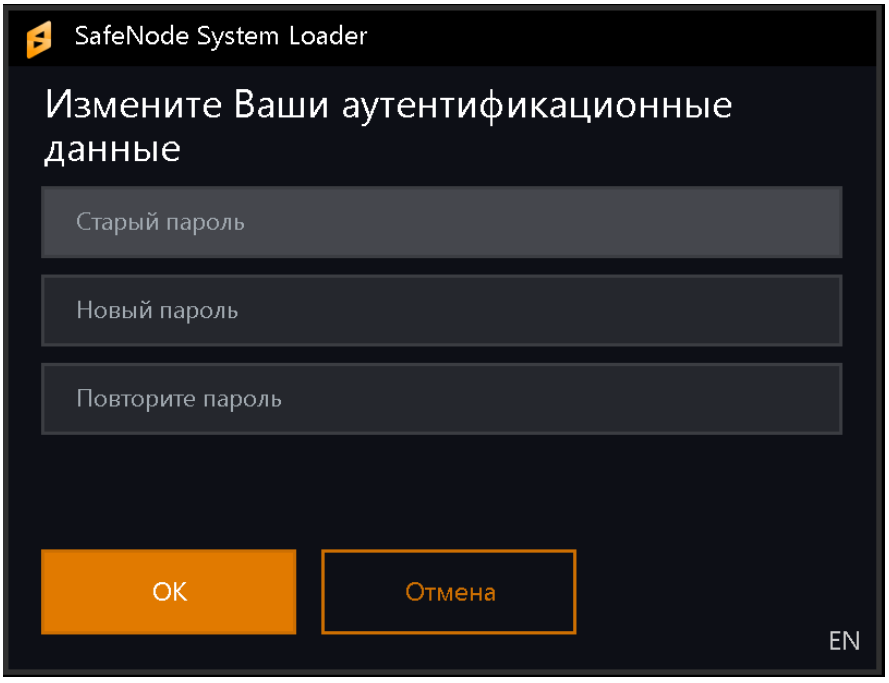


Рисунок 3.4 – Смена пароля пользователем по требованию АБ

3.4.4 Для смены пароля пользователю необходимо указать старое значение пароля, новый пароль, подтвердить значение нового пароля и нажать ***< ОК >***.

3.4.5 Если введенный пароль соответствует всем требованиям к сложности пароля в заданной политике аутентификации, то на экране ЭВМ появится окно для выбора загрузки ОС (рисунок 3.5).

Рисунок 3.5 – Выбор ОС для загрузки

При вводе пароля следует учитывать следующие особенности:

- 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 отображается 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! Длина пароля должна быть не менее 10 символов»*** или ***«Отсутствует заглавная буква»*** (перечень возможных ошибок описан в таблице 9.1).

3.4.6 Для смены PIN-кода персонального идентификатора пользователю необходимо перейти в открывшемся диалоговом окне указать текущий PIN-код (рисунок 3.6) для подтверждения принадлежности персонального идентификатора пользователю. Далее следует ввести новый PIN-код идентификатора и повторить его для контроля правильного введения символов PIN-кода.

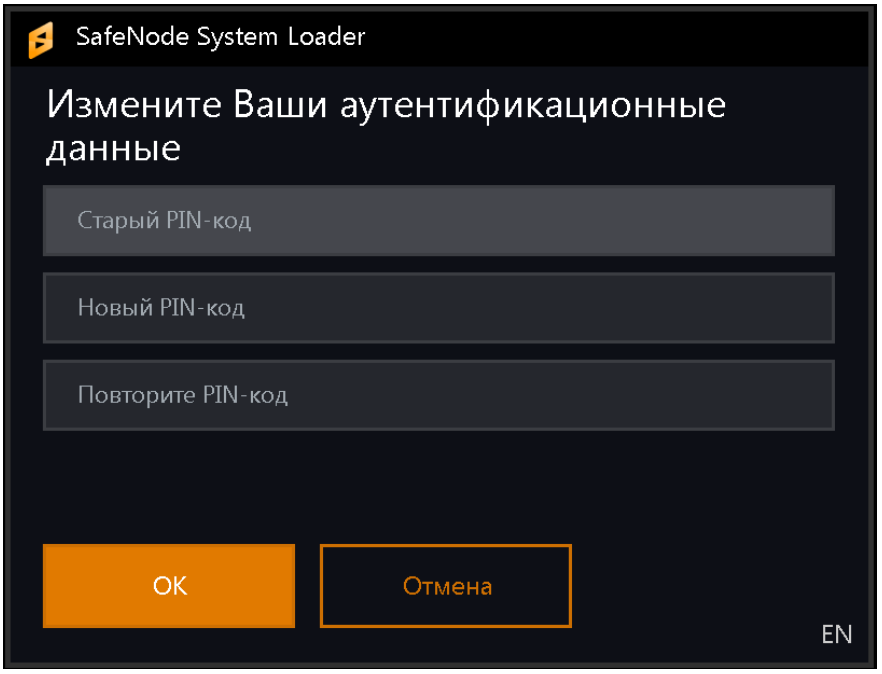


Рисунок 3.6 – Ввод нового PIN-кода

3.4.7 Если данные введены пользователем без ошибок, то на экране ЭВМ появится диалоговое окно с выбором ОС для загрузки (рисунок 3.5).

3.4.8 Смена аутентификационных данных самим пользователем возможна по истечению минимального срока действия. Для этого в окне идентификации и аутентификации пользователя необходимо активировать пункт ***«Изменить пароль/PIN-код после входа»*** (рисунок 3.3). В зависимости от назначенного АБ типа аутентификации пользователя в политике аутентификации появится окно смены пароля и /или PIN-кода носителя.

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 3.6).

3.5 Ограничения при аутентификации

3.5.1 В ПО изделия предусмотрены ограничения по времени аутентификации пользователей и количеству ее попыток (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, отображаются после осуществления неудачной попытки входа пользователя, при этом счетчик общих попыток входа будет уменьшен на единицу и в диалоговом окне появится сообщение **«Неверная комбинация имени пользователя и пароля/PIN-кода. Осталось попыток пользователя: N»**, где N – оставшееся количество индивидуальных попыток входа пользователя в систему (рисунок 3.7).

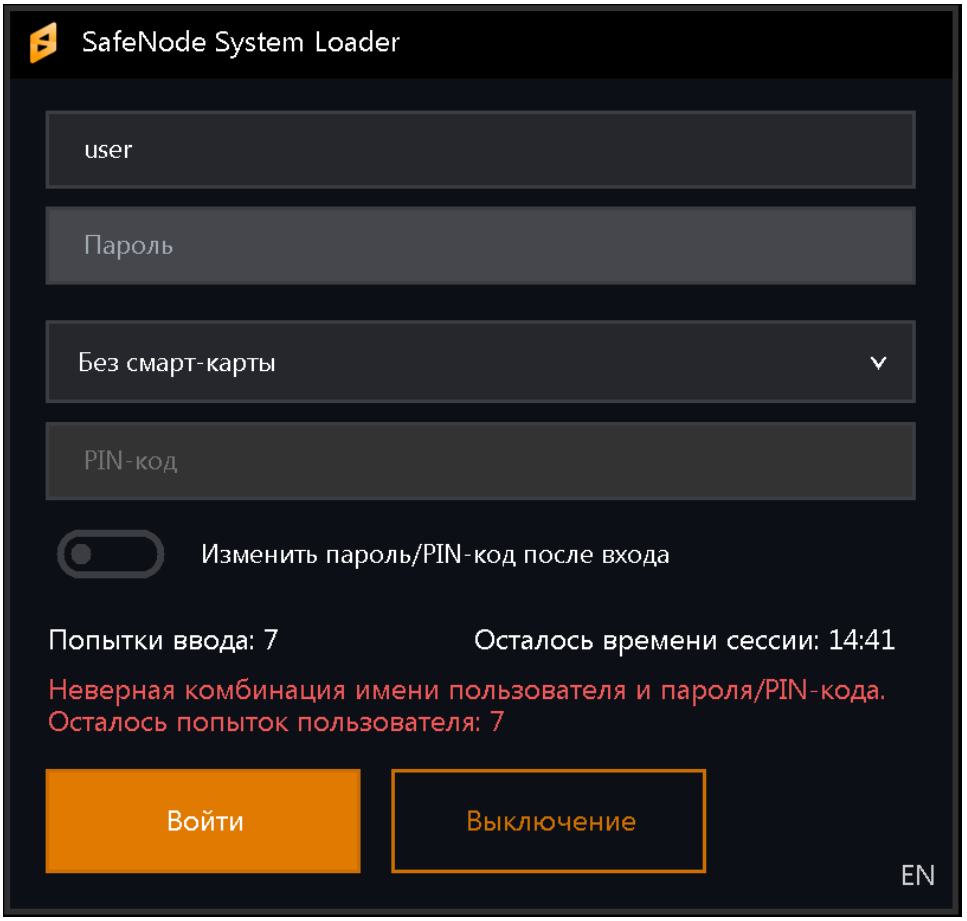


Рисунок 3.7 – Индивидуальные ограничения при аутентификации пользователя

3.5.3 При исчерпании всех индивидуальных попыток аутентификации пользователя произойдет блокировка 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 в открывшемся диалоговом окне (рисунок 3.8) необходимо указать требуемую операцию: перезагрузка или выключение ЭВМ.

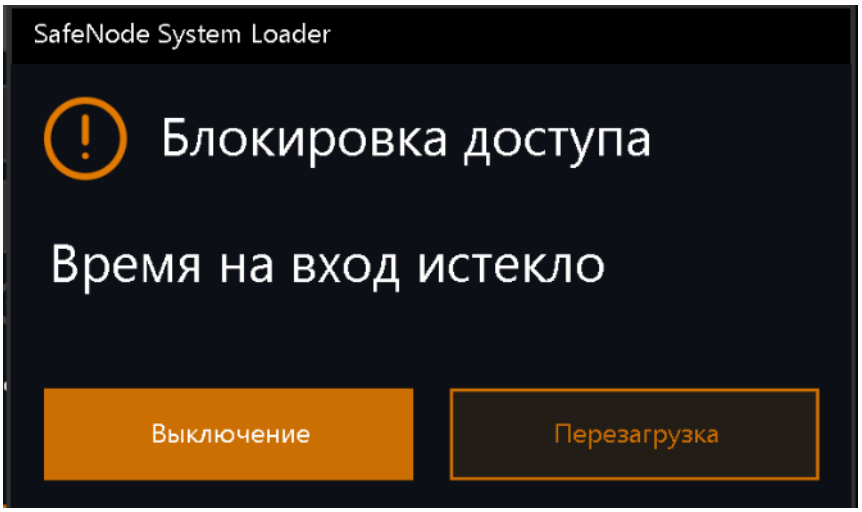


Рисунок 3.8 – Блокировка доступа

4 Аутентификация и идентификация пользователя в псевдографическом интерфейсе

В псевдографическом интерфейсе СДЗ не поддерживается аутентификация доменных пользователей.

4.1 Идентификация и аутентификация с использованием пароля

4.1.1 Для прохождения аутентификации с использованием пароля пользователю необходимо в окне идентификации и аутентификации (рисунок 2.3):

- в поле ***«Имя пользователя»*** ввести имя пользователя и нажать клавишу ***< Enter >*** (рисунок 4.1);
- в поле ***«Пароль»*** ввести имя пользователя и нажать клавишу ***< Enter >*** (рисунок 4.2).

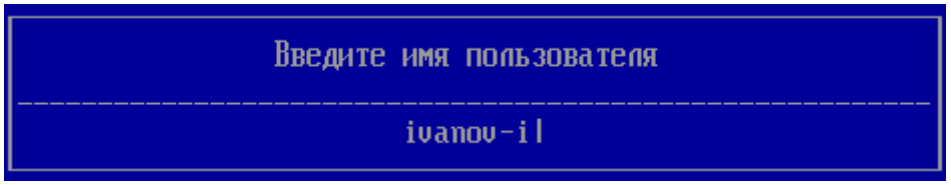


Рисунок 4.1 – Ввод имени пользователя

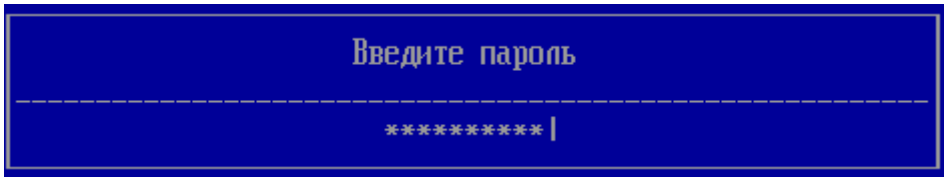


Рисунок 4.2 – Ввод пароля

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 « * ».

4.1.2 При правильном вводе имени учетной записи пользователя и его пароля, ПО изделия выполнит проверку целостности аппаратных и программных объектов ЭВМ. При отсутствии нарушений на экран ЭВМ будет выведено диалоговое окно с разрешением доверенной загрузки ОС (рисунок 4.13).

4.1.3 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 4.1.

Таблица 4.1 – 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**

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

4.2.1 Если в политике аутентификации АБ назначен тип аутентификации пользователя с использованием персонального идентификатора и PIN-кода, в окне с приглашением идентификации и аутентификации после заполнения имени пользователя станут доступны для заполнения поля ***«Персональный идентификатор»*** и ***«PIN-код»*** (рисунки 4.3 – 4.5).

Рисунок 4.3 – Выбор персонального идентификатора

4.2.2 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 4.3) и в новом диалоговом окне (рисунок 4.4) выбрать требуемый персональный идентификатор из списка нажатием клавиши **< *Enter* >**;
- выбранный персональный идентификатор будет выделен < угловыми скобками >;
- нажать клавишу | ***OK*** | (рисунок 4.4), перейти курсором в поле ***«PIN-код»*** (рисунок 4.5) и нажать клавишу **< *Enter* >**;
- ввести PIN-код персонального идентификатора (рисунок 4.5).

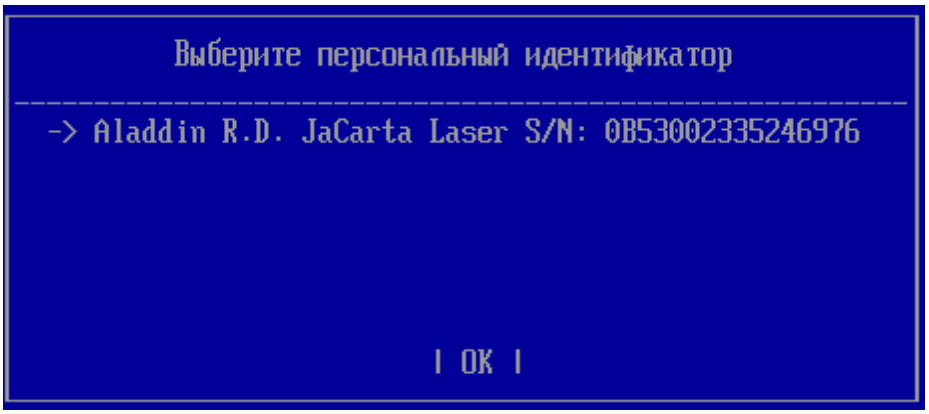


Рисунок 4.4 – Выбор персонального идентификатора пользователя

Рисунок 4.5 – 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»***.

4.2.3 После выполнения успешной аутентификации и идентификации пользователя ПО изделия выполнит проверку целостности аппаратных и программных объектов ЭВМ. При отсутствии нарушений на экран ЭВМ будет выведено диалоговое окно с разрешением доверенной загрузки ОС (рисунок 4.13).

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

4.3.1 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 4.6 – Аутентификация пользователя с использованием пароля, персонального идентификатора и PIN-кода

4.3.2 Правила заполнения полей ввода пароля, персонального идентификатора и PIN-кода описаны в подразделах 4.1 и 4.2.

4.3.3 После выполнения успешной аутентификации и идентификации пользователя ПО изделия выполнит проверку целостности аппаратных и программных объектов

ЭВМ. При отсутствии нарушений на экран ЭВМ будет выведено диалоговое окно с разрешением доверенной загрузки ОС (рисунок 4.13).

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

4.4.1 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.

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

- АБ при конфигурации учетной записи пользователя установлено требование об изменении аутентификационных данных после первой успешной аутентификации (принудительная смена) (рисунок 4.7);
- при истечении максимального срока действия пароля и/или PIN-кода (равносильно истечению срока действия политики аутентификации).

4.4.3 При возникновении ситуации п. 4.4.2 после успешного прохождения процедуры аутентификации и идентификации на экран ЭВМ будет выведено диалоговое окно, в котором принудительно требуется сменить аутентификационные данные (рисунок 4.7).

Рисунок 4.7 – Смена пароля и/или PIN-кода пользователем по требованию АБ

4.4.4 Для смены пароля пользователю необходимо перейти в поле ***«Изменить пароль»*** или и в открывшемся диалоговом окне ввести новый пароль (рисунок 4.8).

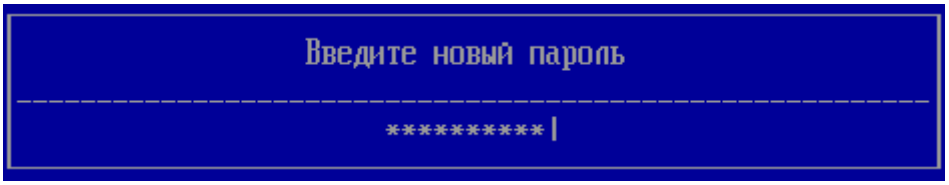


Рисунок 4.8 – Ввод нового пароля

4.4.5 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 4.9).

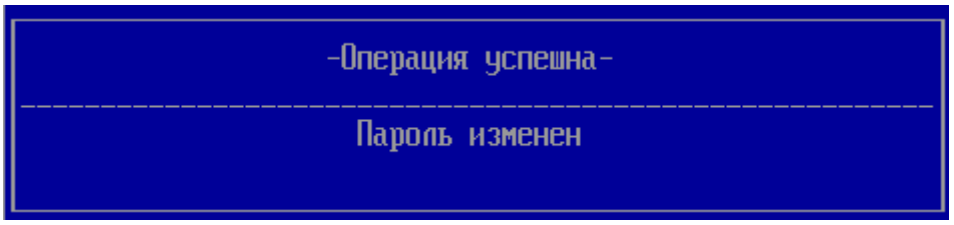


Рисунок 4.9 – Успешная смена пароля

При вводе пароля следует учитывать следующие особенности:

- 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 отображается 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 9.1).

4.4.6 Для смены PIN-кода персонального идентификатора пользователю необходимо перейти в поле ***«Изменить PIN-код персонального идентификатора»***. В открывшемся диалоговом окне необходимо ввести текущий PIN-код (рисунок 4.10) 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 4.11).

Рисунок 4.10 – Ввод старого PIN-кода

Рисунок 4.11 – Ввод нового PIN-кода

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

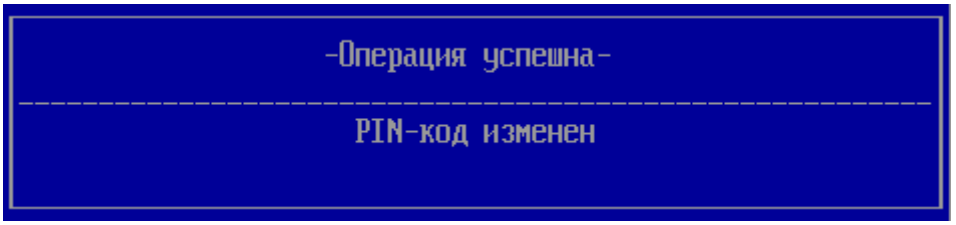


Рисунок 4.12 – Успешная смена PIN-кода

4.4.8 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 4.13) станет активным пункт ***«Изменить пароль»*** и/или ***«Изменить PIN-код персонального идентификатора»*** (в зависимости от назначенного АБ типа аутентификации пользователя в политике аутентификации).

4.4.9 Для смены аутентификационных данных пользователю необходимо повторить действия пунктов 4.4.2 – 4.4.6.

4.4.10 После успешной смены пароля и (или) PIN-кода идентификатора пользователь может продолжить выбор ОС для доверенной загрузки (рисунок 4.13).

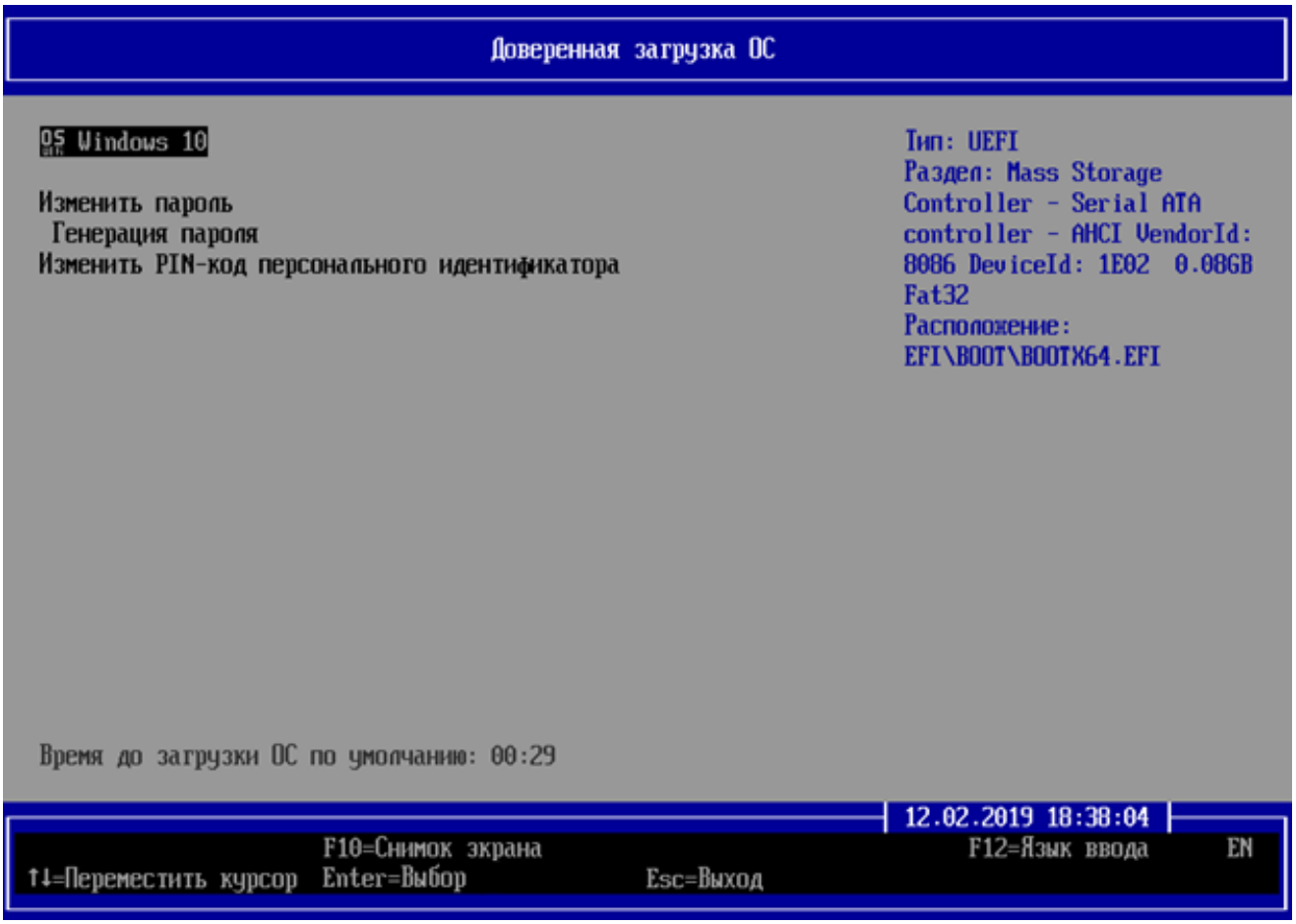


Рисунок 4.13 – Выбор ОС для доверенной загрузки с возможностью изменения пароля пользователя и PIN-кода персонального идентификатора

4.5 Ограничения при аутентификации

4.5.1 В ПО изделия предусмотрены ограничения по времени аутентификации пользователей и количеству ее попыток (рисунок 2.3). 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.

4.5.2 Индивидуальные ограничения при аутентификации, определенные АБ для конкретного пользователя, отображаются 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 4.14).

Рисунок 4.14 – Индивидуальные ограничения при аутентификации пользователя

4.5.3 При исчерпании всех индивидуальных попыток аутентификации пользователя произойдет блокировка учетной записи пользователя. В данном случае необходимо обратиться к АБ для разблокировки учетной записи.

4.5.4 При истечении общего времени регистрации на экране ЭВМ появится диалоговое окно с сообщением ***«Блокировка доступа»*** и указанием причины блокировки. Пользователю в открывшемся диалоговом окне (рисунок 4.15) необходимо указать требуемую операцию: перезагрузка или выключение ЭВМ. По умолчанию задана операция ***«Выключение ЭВМ»*** (ей соответствует знак «*X*»).

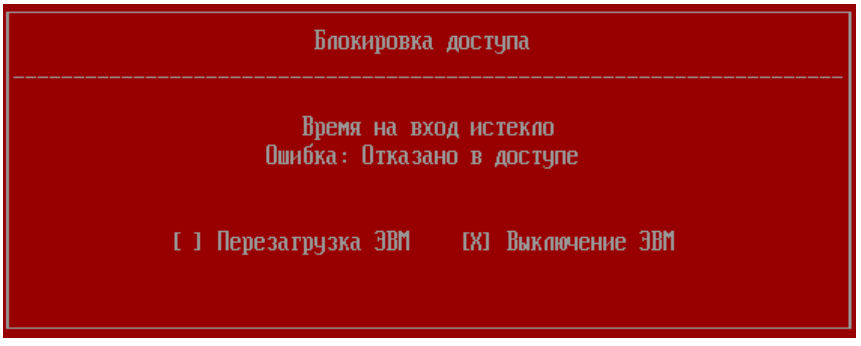
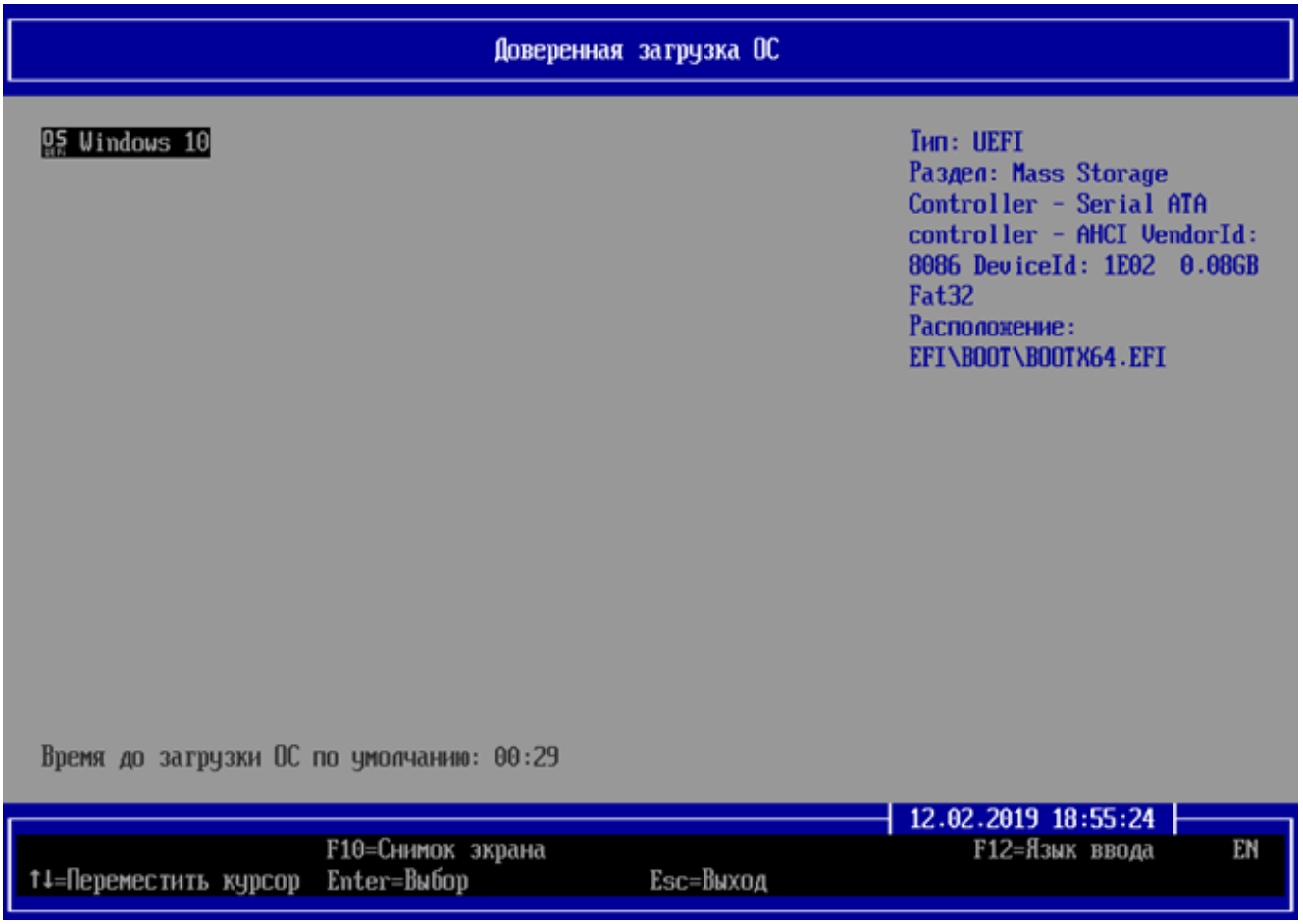


Рисунок 4.15 – Перезагрузка или выключение ЭВМ

5 Выбор ОС для доверенной загрузки

5.1 После выполнения успешной аутентификации и идентификации пользователя ПО изделия выполнит проверку целостности аппаратных и программных объектов ЭВМ. При отсутствии нарушений на экран ЭВМ будет выведено диалоговое окно с разрешением доверенной загрузки ОС (рисунок 5.1).



а) Псевдографическая интерфейс

б) Графический интерфейс

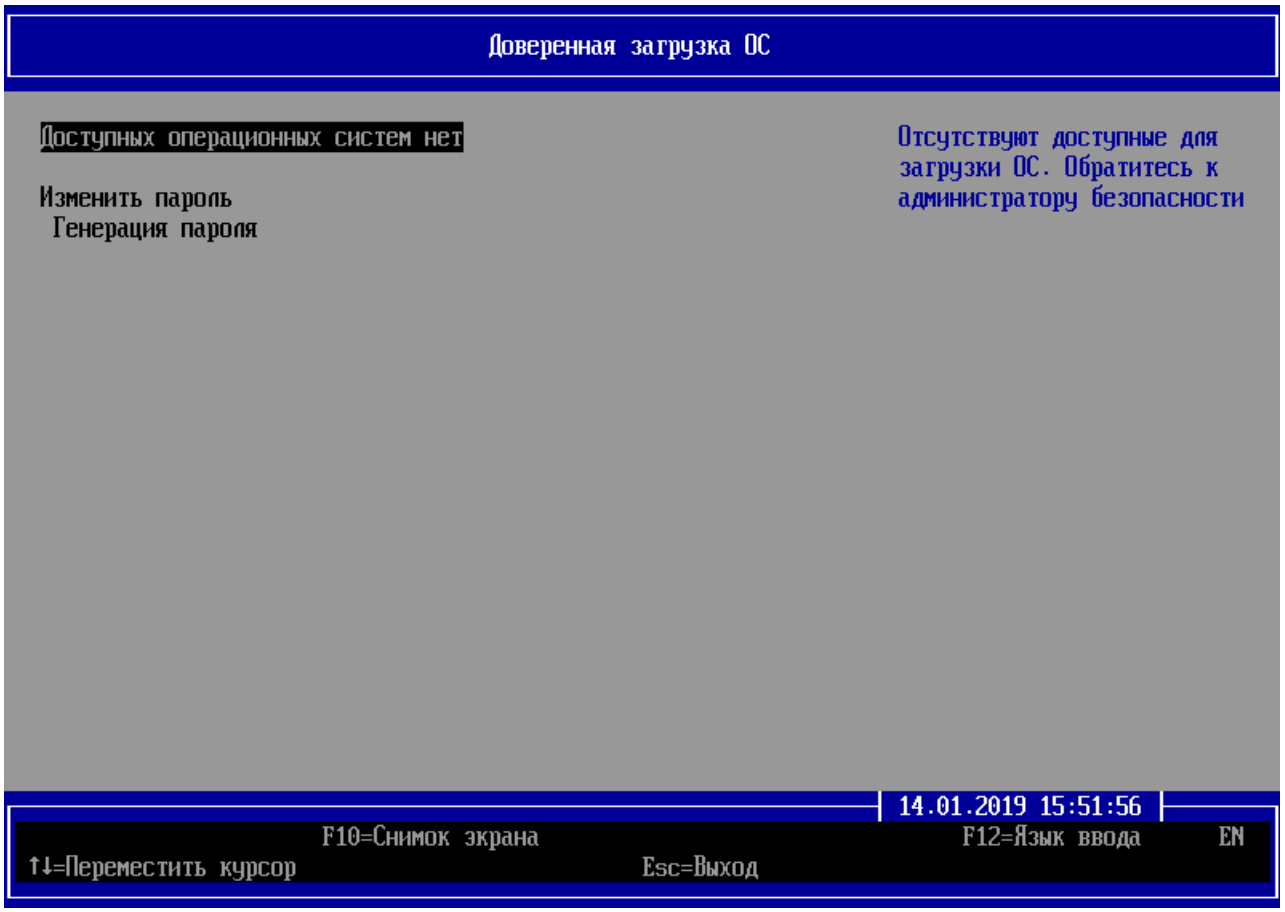
Рисунок 5.1 – Выбор ОС для доверенной загрузки

5.2 Для осуществления доверенной загрузки ОС необходимо выбрать ОС из сформированного АБ списка.

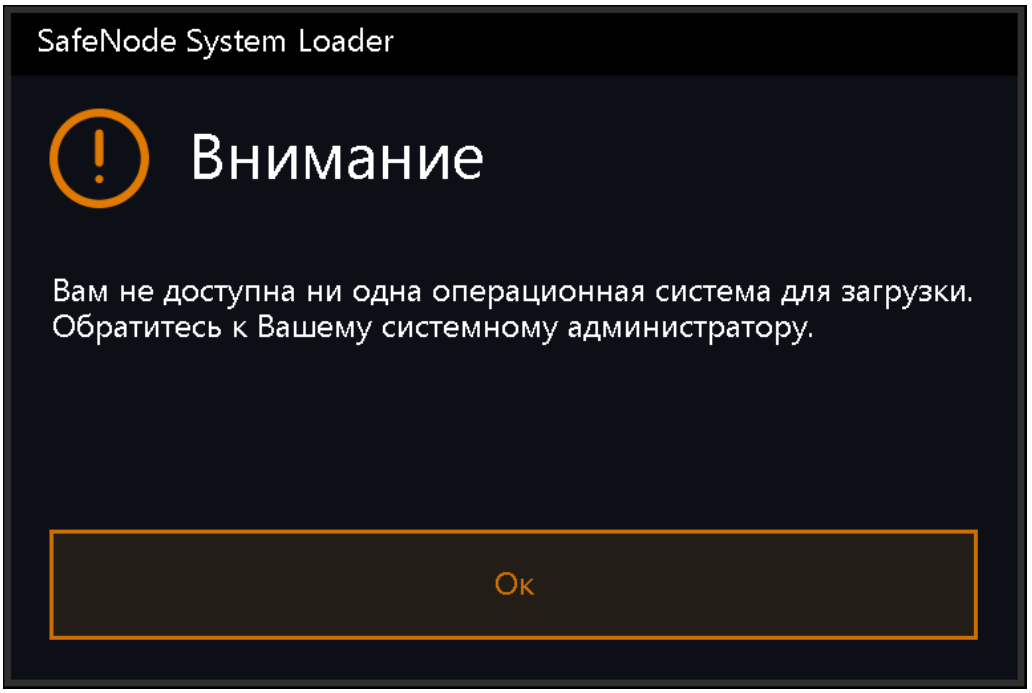
5.3 Если АБ не разрешил для доверенной загрузки пользователю хотя бы одну ОС, то после успешного прохождения идентификации и аутентификации пользователя на экран ЭВМ будет выведено диалоговое окно с сообщением ***«Доступных операционных систем нет»*** (рисунок 5.2).

5.4 В таком случае пользователю необходимо:

- выключить ЭВМ, перейдя в меню действий пользователя (рисунок 8.1) последовательным нажатием клавиши **< *Esc* >** в интерфейсе;
- обратиться к АБ для решения проблемы.



а) Псевдографический интерфейс



а) Графический интерфейс

Рисунок 5.2 – Невозможность загрузки ОС пользователю

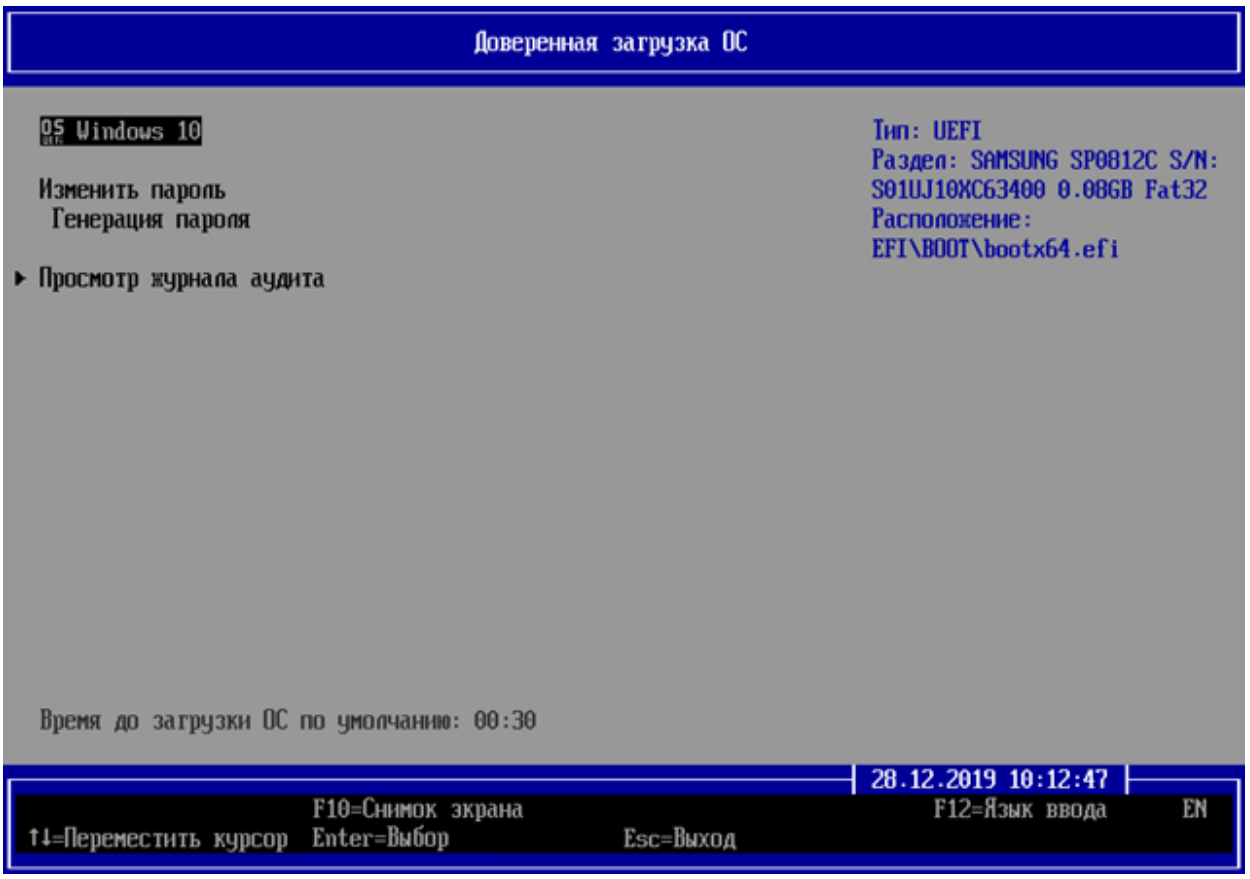
6 Журнал аудита

6.1 Предоставление пользователю доступа к работе с журналом аудита

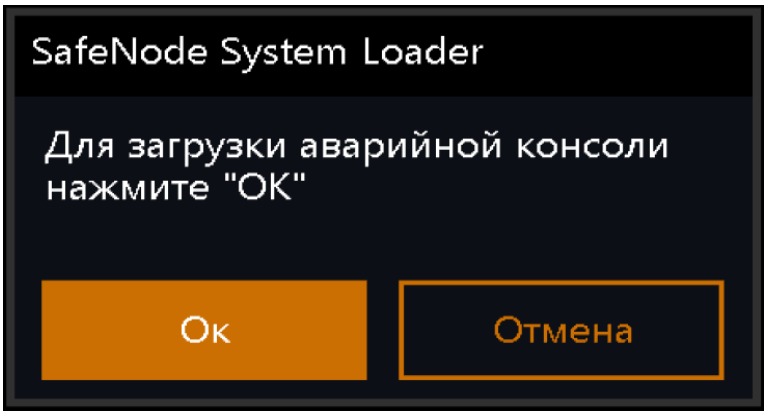
6.1.1 Пользователям с ролью аудитора (далее по тексту – аудитор), предоставляется возможность работы с журналами аудита изделия. Журналы предназначены для мониторинга всех действий АБ и пользователей, происходящих до доверенной загрузки ОС.

6.1.2 Доступ пользователя к журналам аудита предоставляется АБ путем соответствующей конфигурации учетной записи пользователя.

6.1.3 В этом случае, после выполнения успешной аутентификации и идентификации пользователя изделие выполнит проверку целостности аппаратных и программных объектов ЭВМ и при отсутствии нарушений на экран ЭВМ будет выведено диалоговое окно с разрешением доверенной загрузки ОС и возможностью работы с журналами аудита (рисунок 6.1 а) в псевдографической консоли. В графической консоли после успешной аутентификации и идентификации пользователя будет предложено загрузить аварийную консоль (рисунок 6.1 б).



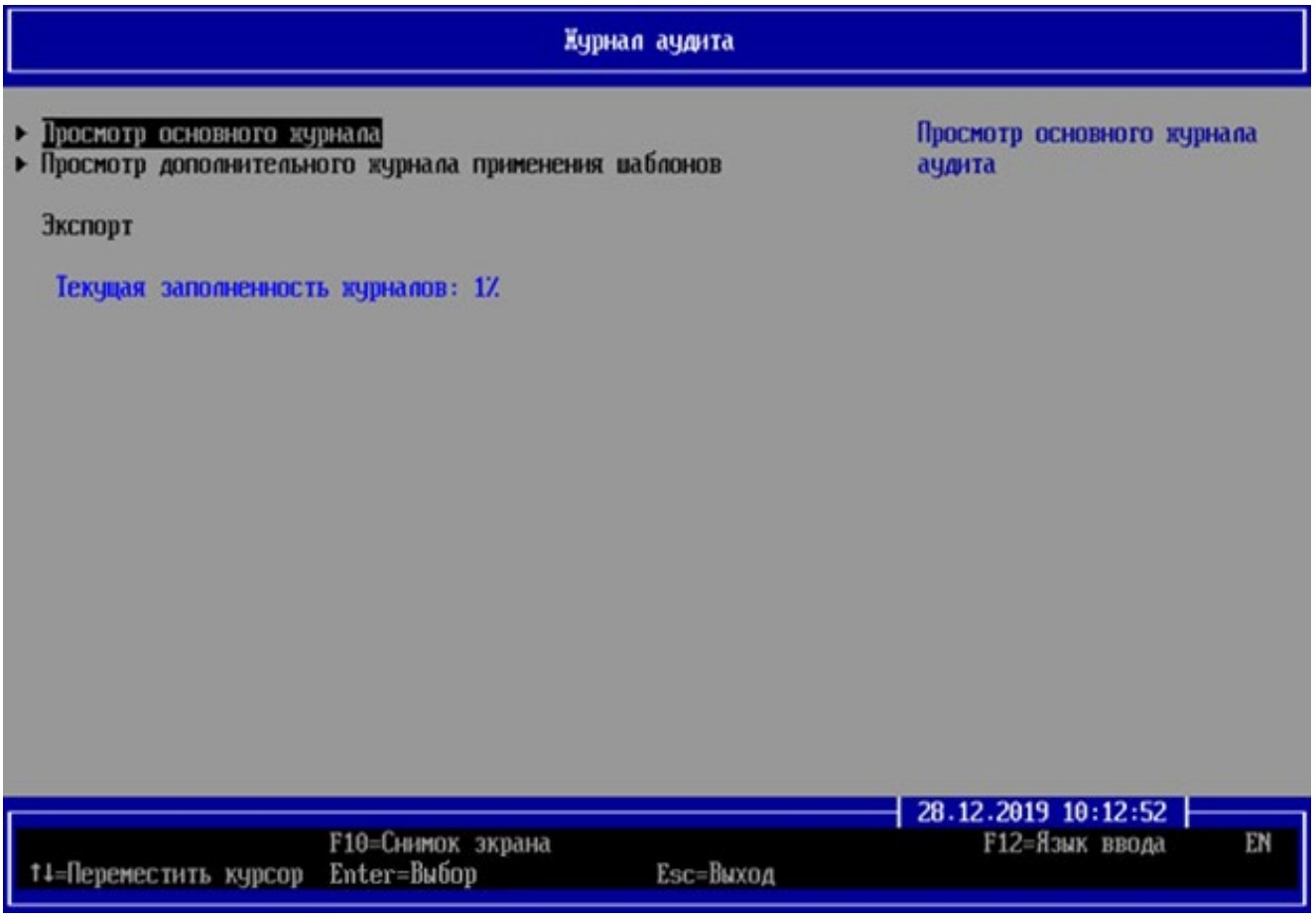
а) Псевдографический интерфейс



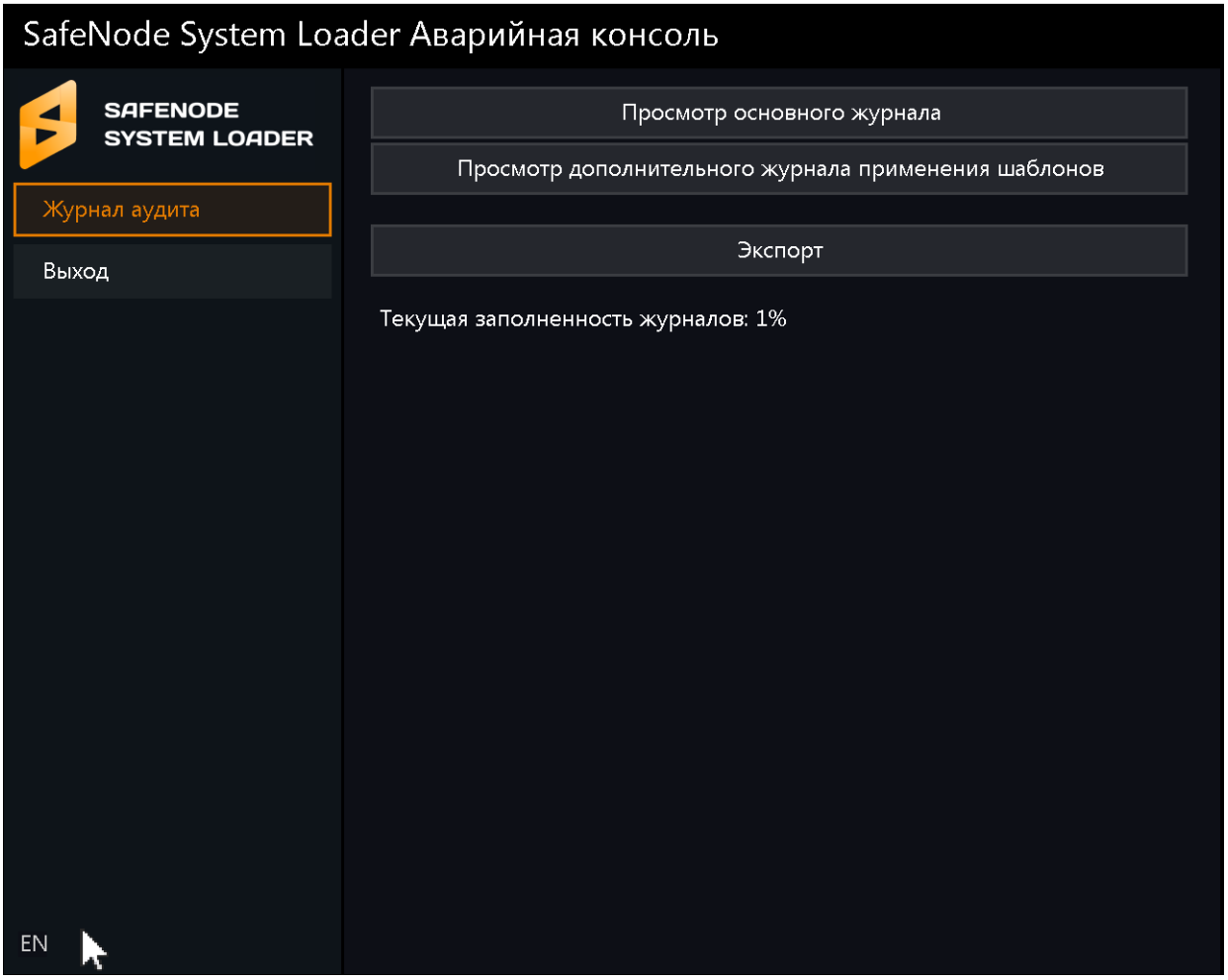
а) Графический интерфейс

Рисунок 6.1 – Доверенная загрузка ОС с возможностью просмотра журнала аудита

6.1.4 Для работы с журналами аудита пользователю необходимо перейти в строку ***«Просмотр журнала аудита»*** и нажать клавишу **< *Enter* >** (рисунок 6.2 а), в графическом интерфейсе необходимо выбрать «Просмотр основного журнала» (рисунок 6.2 б).



а) Псевдографический интерфейс



б) Графический интерфейс

Рисунок 6.2 – Журнал аудита

6.1.5 Аудитор имеет возможность:

- просмотра основного журнала зарегистрированных событий;
- просмотра дополнительного журнала применения шаблонов;
- экспорта журналов на внешнее устройство хранения данных без их очистки.

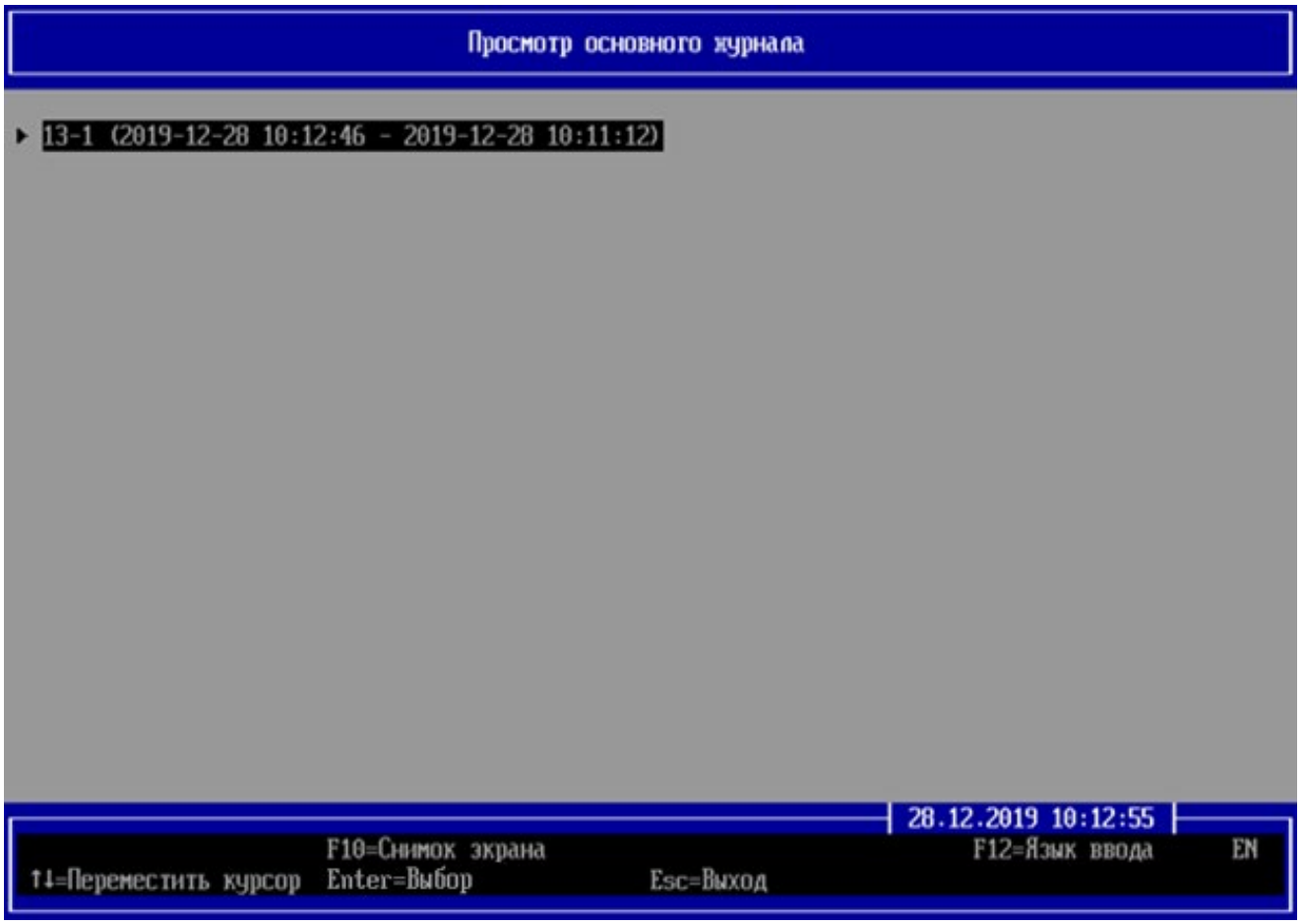
6.1.6 В строке ***«Текущая заполненность журналов»*** отображается информация о процентном заполнении специально выделенной области для хранения данных аудита.

6.2 Просмотр основного журнала аудита

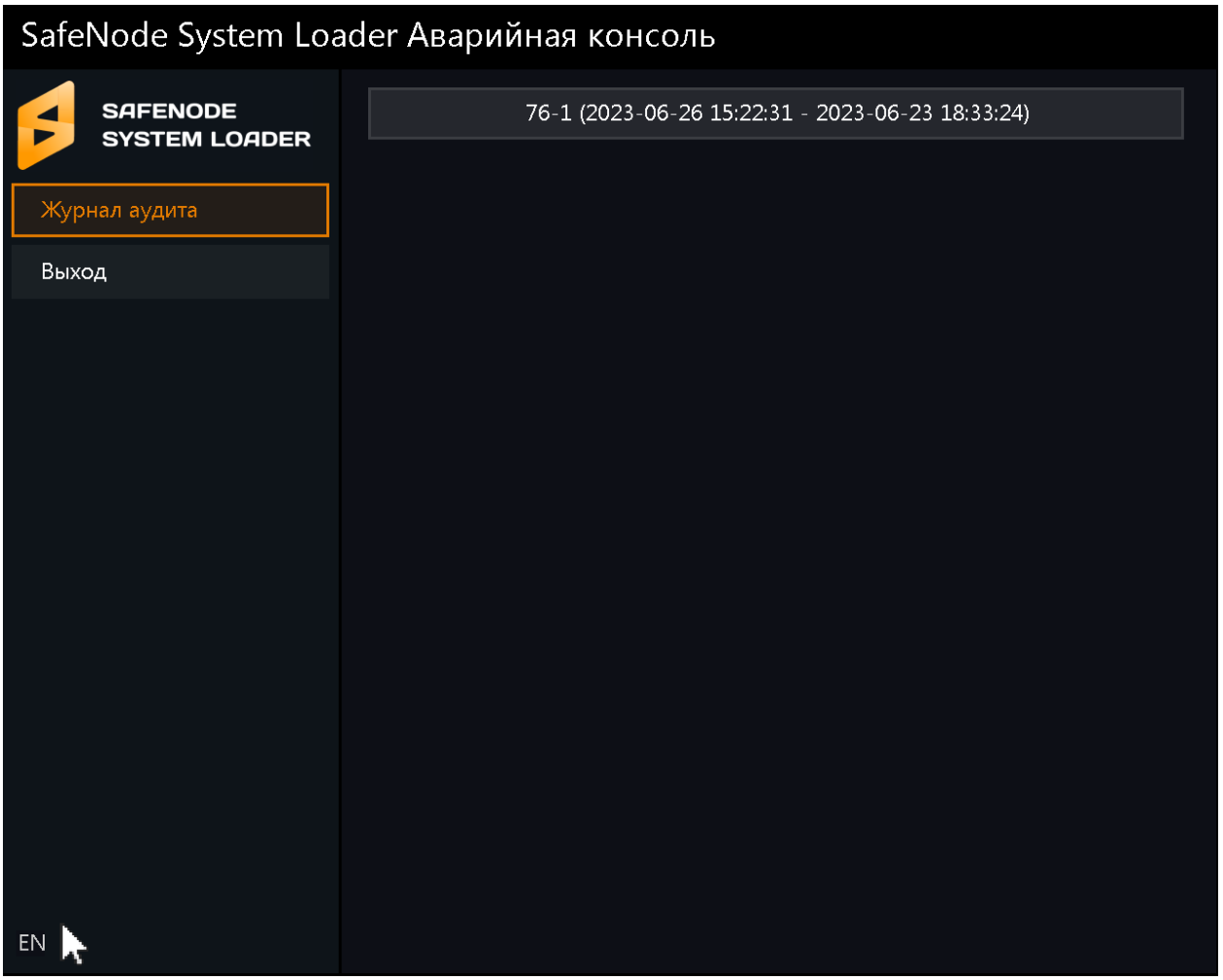
6.2.1 В основном журнале аудита регистрируются все действия АБ и пользователей, а также сообщения при срабатывании механизмов КЦ объектов.

6.2.2 Для просмотра основного журнала аудита необходимо перейти в строку «Просмотр основного журнала» и нажать клавишу < ***Enter*** > (рисунок 6.2).

6.2.3 В появившемся диалоговом окне ***«Просмотр основного журнала»*** все события, регистрируемые в основном журнале аудита, разделены построчно (рисунок 6.3).



а) Псевдографический интерфейс

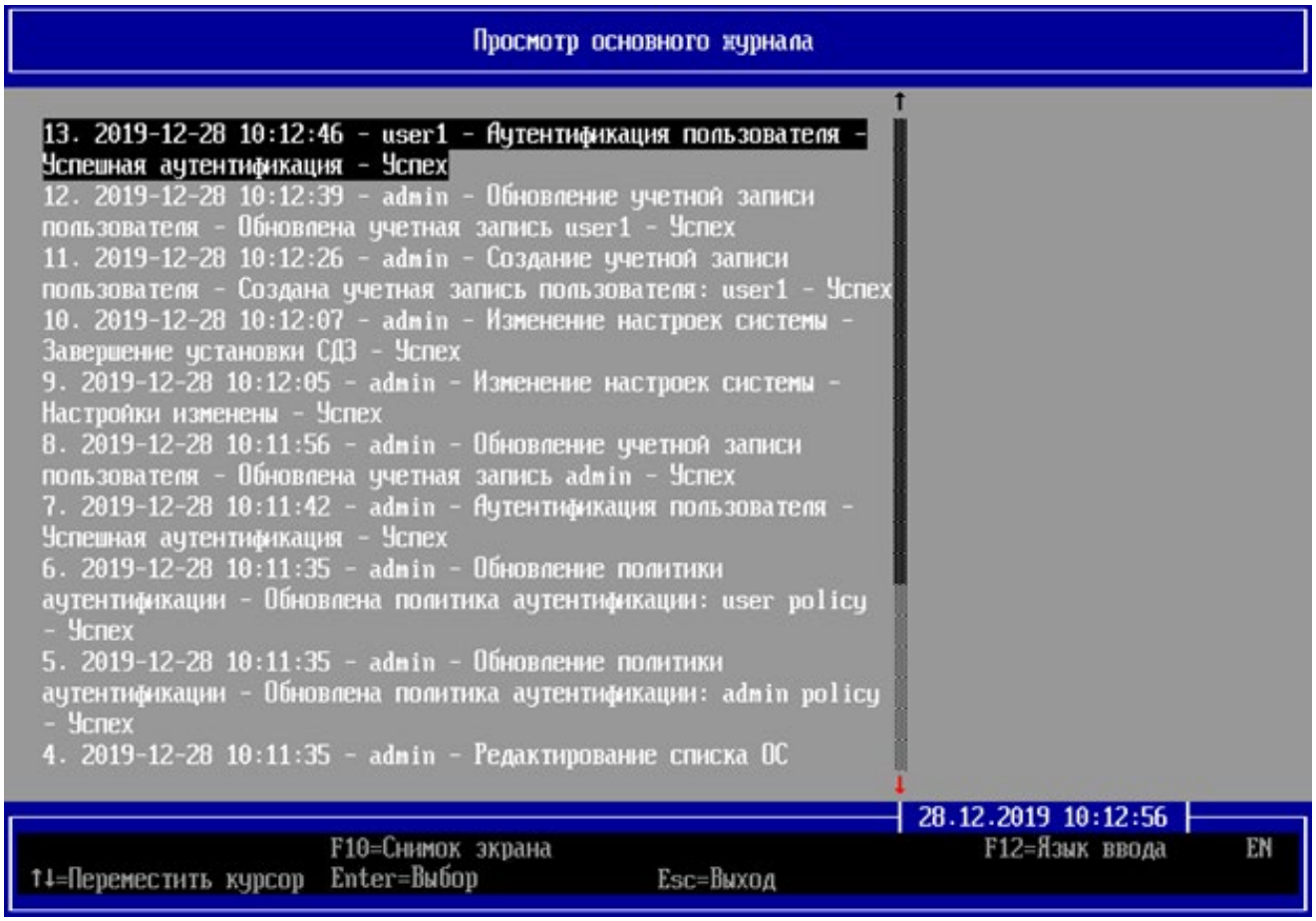


б) Графический интерфейс

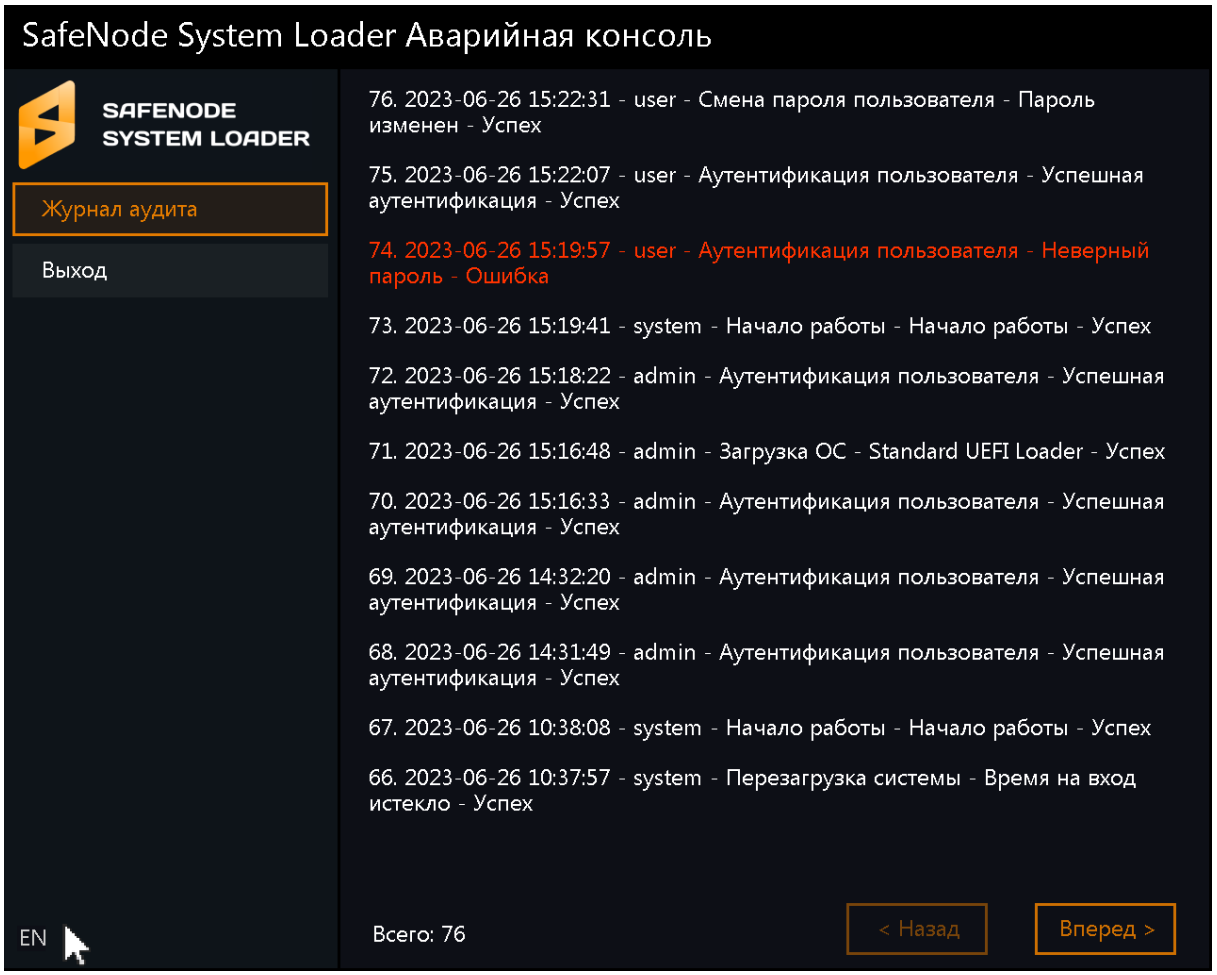
Рисунок 6.3 – Список периодов событий основного журнала аудита

6.2.4 Для просмотра аудитору необходимо перейти в строку, соответствующую периоду времени, за которое требуется просмотреть события, и нажать клавишу < ***Enter*** > (рисунок 6.3).

6.2.5 Список событий, регистрируемых в основном журнале аудита (рисунок 6.4), приведен в таблице 6.1.



а) Псевдографический интерфейс



б) Графический интерфейс

Рисунок 6.4 – Просмотр основного журнала аудита

6.2.6 Каждому событию присваивается порядковый номер и указывается:

- дата и время события;
- пользователь-инициатор события;
- описание события (выполняемая операция) и комментарии к нему;
- результат: успешное завершение операции или ошибка.

6.2.7 Строки с сообщениями об ошибках выделены красным цветом.

Таблица 6.1 – Список событий, регистрируемых в основном журнале аудита

№	Событие	Успех/Ошибка	Комментарий
Общесистемные события			
1	Загрузка ОС	Успех	Название операционной системы
		Ошибка	Отсутствуют доступные для загрузки ОС
2	Восстановление настроек по	Успех	Заводские настройки восстановлены

№	Событие	Успех/Ошибка	Комментарий
	умолчанию		
3	Изменение настроек системы	Успех	Настройки изменены
			Автовход разрешен для пользователя: <имя пользователя>
4	Выключение системы	Успех	Выключение ЭВМ
5	Обновление системного ПО	Успех	Системное ПО обновлено
6	Начало работы	Успех	Начало работы
7	Перезагрузка системы	Успех	Перезагрузка ЭВМ
События идентификации и аутентификации пользователей			
8	Аутентификация пользователя	Ошибка	Журнал заполнен
			Максимальное время неактивности истекло
			Неверный пароль
			Неверный PIN-код
			Персональный идентификатор не подключен к ЭВМ
			Неверный персональный идентификатор
			Попытка аутентификации заблокированного пользователя
			Попытка аутентификации незарегистрированного пользователя
			Неверная хэш-сумма на персональном идентификаторе
			Сертификат на персональном идентификаторе некорректен, не найден или просрочен
		Успех	Успешная аутентификация
События при действиях АБ			
Работа с журналом аудита			
9	Работа с журналом	Успех	Журналы сохранены в файлы с именами sdzlog.csv и sdzlogT.csv
			Журналы аудита очищены
Работа с шаблонами			
10	Работа с шаблонами	Успех	Применено объектов шаблона <количество>
Работа с учетными записями пользователей			
11	Создание учетной записи пользователя	Успех	Создана учетная запись пользователя: <имя пользователя>
12	Обновление учетной записи пользователя	Успех	Обновлена учетная запись <имя пользователя>
13	Удаление учетной записи пользователя	Успех	Удалена учетная запись пользователя: <имя пользователя>

№	Событие	Успех/Ошибка	Комментарий
Работа с политиками аутентификации пользователей			
14	Создание политики аутентификации	Успех	Создана политика аутентификации: <имя политики>
15	Обновление политики аутентификации	Успех	Обновлена политика аутентификации: <имя политики>
16	Удаление политики аутентификации	Успех	Удалена политика аутентификации: <имя политики>
Работа с политиками контроля целостности объектов и загрузки ОС			
17	Создание политики контроля целостности объектов и загрузки ОС	Успех	Создана политика контроля целостности объектов и загрузки ОС: <имя политики>
18	Обновление политики контроля целостности объектов и загрузки ОС	Успех	Обновлена политика контроля целостности объектов и загрузки ОС: <имя политики>
19	Удаление политики контроля целостности объектов и загрузки ОС	Успех	Удалена политика контроля целостности объектов и загрузки ОС: <имя политики>
События при действиях пользователя			
20	Смена PIN-кода устройства	Успех	Изменен PIN-код персонального идентификатора <имя идентификатора>
21	Смена пароля пользователя	Успех	Пароль изменен
События подсистемы контроля целостности			
Контроль целостности файлов			
22	Редактирование списка контролируемых объектов ФС	Успех	Политика <имя политики> Добавление <имя объекта>
			Политика <имя политики> Удаление <имя объекта>
23	Проверка объектов ФС	Ошибка	Проверка целостности файлов
			Политика <имя политики> <имя объекта> Содержимое объекта изменено
			Политика <имя политики> <имя объекта> Объект не найден
		Успех	Проверка целостности файлов
Контроль целостности объектов реестра ОС			
24	Редактирование списка контролируемых объектов реестра	Успех	Политика <имя политики> Добавление <имя объекта>
			Политика <имя политики> Удаление <имя объекта>
25	Проверка объектов	Ошибка	Проверка целостности объектов реестра

№	Событие	Успех/Ошибка	Комментарий
	реестра		Политика <имя политики> <имя объекта> Содержимое объекта изменено
			Политика <имя политики> <имя объекта> Объект не найден
		Успех	Проверка целостности объектов реестра
Контроль устройств			
26	Редактирование списка контролируемых устройств	Успех	Политика <имя политики> Добавление <имя объекта>
			Политика <имя политики> Удаление <имя объекта>
27	Проверка устройств	Ошибка	Проверка целостности аппаратных устройств
			Политика <имя политики> <имя объекта> Содержимое объекта изменено
			Политика <имя политики> <имя объекта> Объект не найден
		Успех	Проверка целостности аппаратных устройств
Управление загрузкой ОС			
28	Редактирование списка ОС пользователей	Успех	Политика <имя политики> Добавление <наименование ОС>
			Политика <имя политики> Удаление <наименование ОС>
Контроль загрузочных секторов			
29	Редактирование списка контролируемых загрузочных областей	Успех	Политика <имя политики> Добавление <имя объекта>
			Политика <имя политики> Удаление <имя объекта>
30	Проверка загрузочных секторов	Ошибка	Проверка целостности загрузочных секторов
			Политика <имя политики> <имя объекта> Содержимое объекта изменено
			Политика <имя политики> <имя объекта> Объект не найден
		Успех	Проверка целостности загрузочных секторов
Контроль целостности среды UEFI			
31	Редактирование списка целостности среды UEFI	Успех	Политика <имя политики> Добавление <имя объекта>
			Политика <имя политики> Удаление <имя объекта>
32	Проверка параметров среды UEFI	Ошибка	Проверка целостности среды UEFI
			Политика <имя политики> <имя объекта> Содержимое объекта изменено
			Политика <имя политики> <имя объекта> Объект не найден
		Успех	Проверка целостности среды UEFI
Контроль целостности журналов транзакций файловых систем			
33	Редактирование списка журналов	Успех	Политика <имя политики> Добавление <имя объекта>
			Политика <имя политики> Удаление <имя объекта>

№	Событие	Успех/Ошибка	Комментарий
	файловых систем		
34	Проверка журналов файловых систем	Успех	Проверка целостности транзакций журналов файловых систем
			Разрешение однократного входа для восстановления файловой системы <имя объекта>
		Ошибка	Проверка завершенности транзакций журналов файловых систем
			Политика <имя политики> <имя объекта> Содержимое объекта изменено
			Политика <имя политики> <имя объекта> Объект не найден
Блокирование и разблокирование учетной записи пользователя			
35	Редактирование статуса пользователей	Успех	Блокировка пользователя на n минут
			Блокировка пользователя
			<имя пользователя> был заблокирован администратором
			<имя пользователя> был разблокирован администратором
			Блокировка пользователя по истечению времени неактивности

6.3 Просмотр дополнительного журнала применения шаблонов

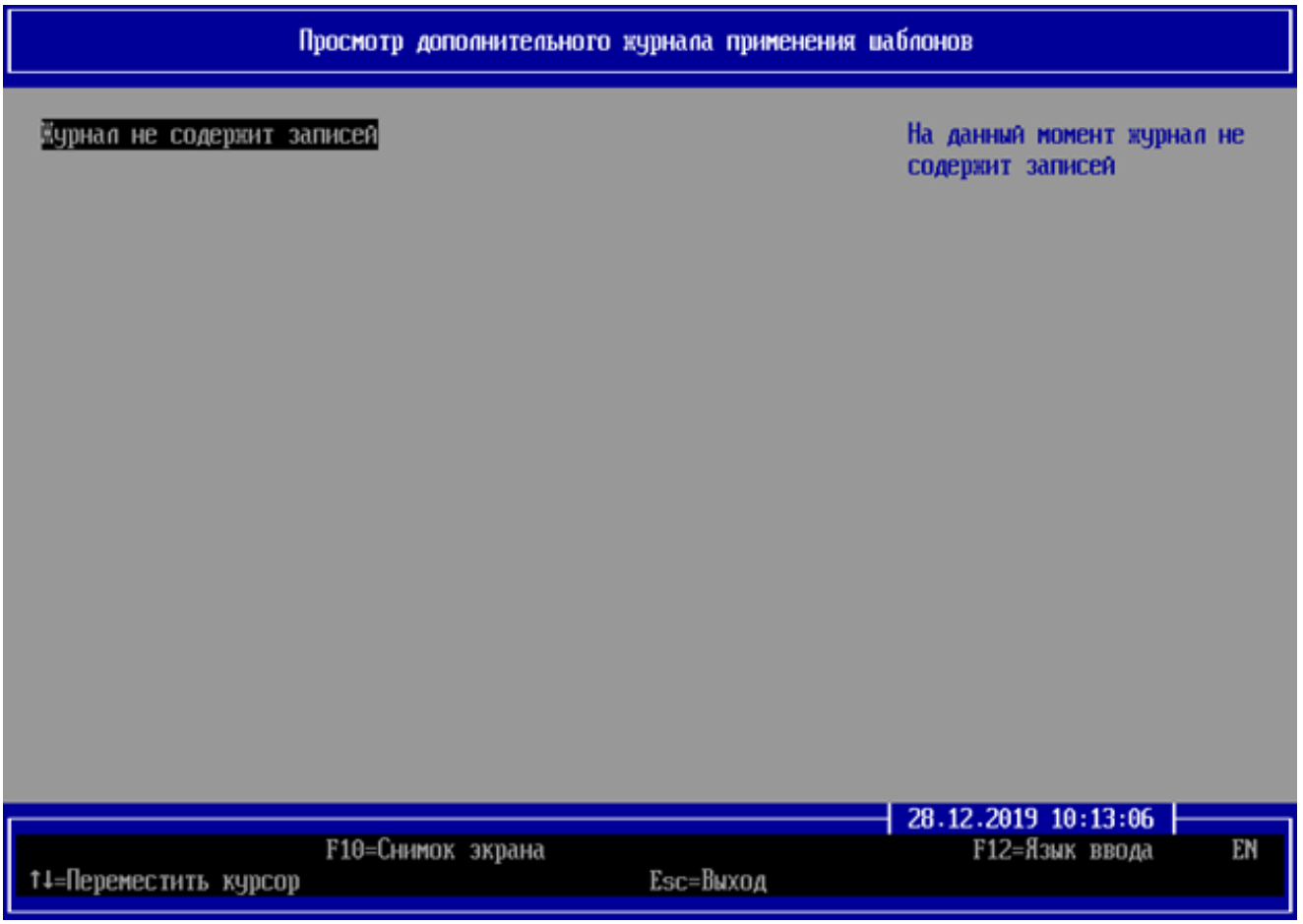
6.3.1 В дополнительном журнале применения шаблонов регистрируются действия АБ по применению шаблонов к политикам аутентификации и КЦ.

6.3.2 Для просмотра дополнительного журнала применения шаблонов необходимо перейти в строку ***«Просмотр дополнительного журнала применения шаблонов»*** и нажать клавишу < ***Enter*** > (рисунок 6.2).

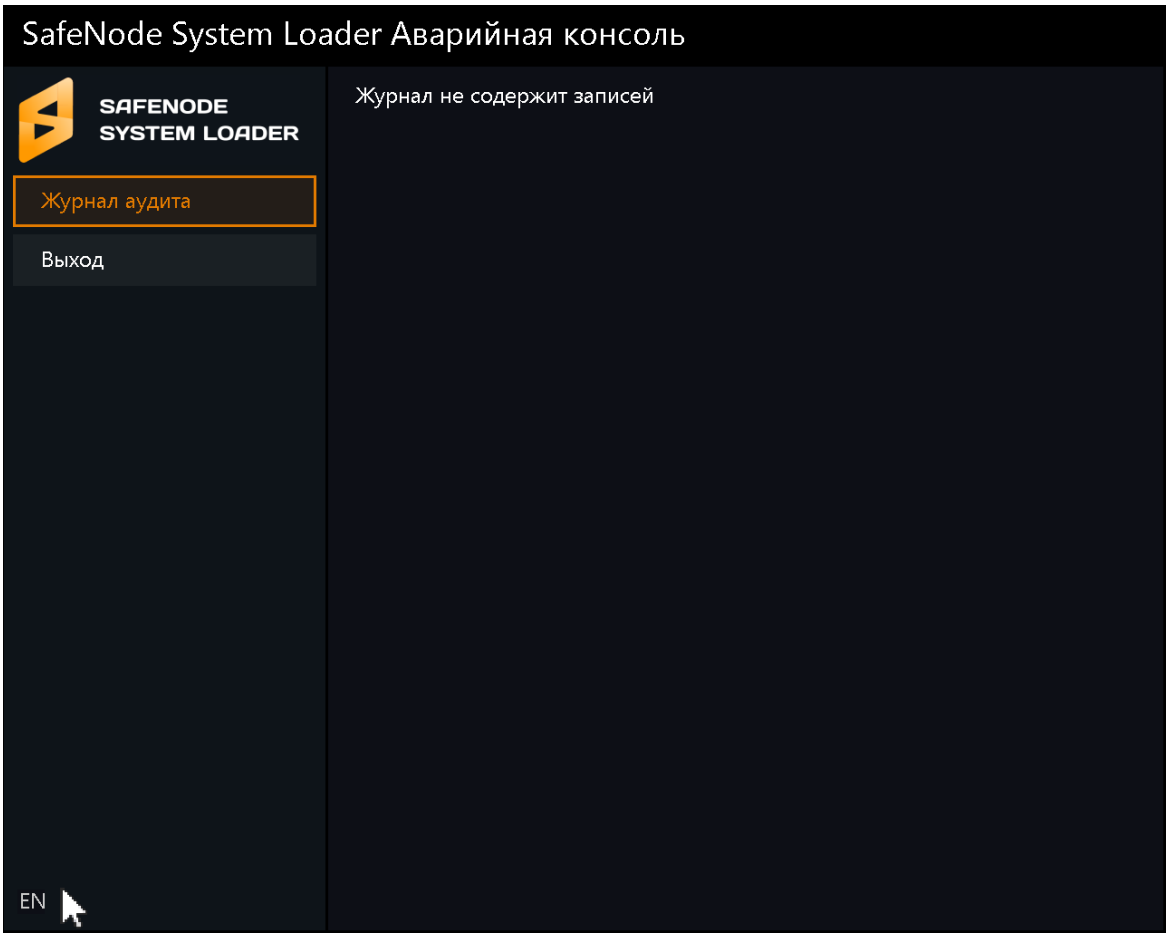
6.3.3 В появившемся диалоговом окне ***«Просмотр дополнительного журнала применения шаблонов»***, все события, регистрируемые в основном журнале, разделены построчно.

6.3.4 Аудитору необходимо перейти в строку, соответствующую периоду времени, за которое требуется просмотреть события, регистрируемые в дополнительном журнале применения шаблонов, и нажать клавишу < ***Enter*** >.

6.3.5 В появившемся диалоговом окне ***«Просмотр дополнительного журнала применения шаблонов»*** аудитору предоставляется возможность просмотра всех действий, по применению шаблонов к политикам (рисунок 6.5).



а) Псевдографический интерфейс



б) Графический интерфейс

Рисунок 6.5 – Просмотр дополнительного журнала применения шаблонов

6.3.6 Каждому событию присваивается порядковый номер и указываются данные п. 6.2.6.

6.3.7 Строки с сообщениями об ошибках выделены красным цветом.

Таблица 6.2 – Список событий, регистрируемых в дополнительном журнале применения шаблонов

№	Событие	Успех/Ошибка	Комментарий
Общесистемные события			
1	Изменение настроек системы	Успех	Настройки системы изменены
События подсистемы контроля целостности			
Контроль целостности файлов			
2	Редактирование списка контролируемых объектов ФС	Успех	Политика <имя политики> Добавление <имя объекта>
		Ошибка	
Контроль целостности объектов реестра ОС			
3	Редактирование списка контролируемых объектов реестра	Успех	Политика <имя политики> Добавление <имя объекта>
		Ошибка	

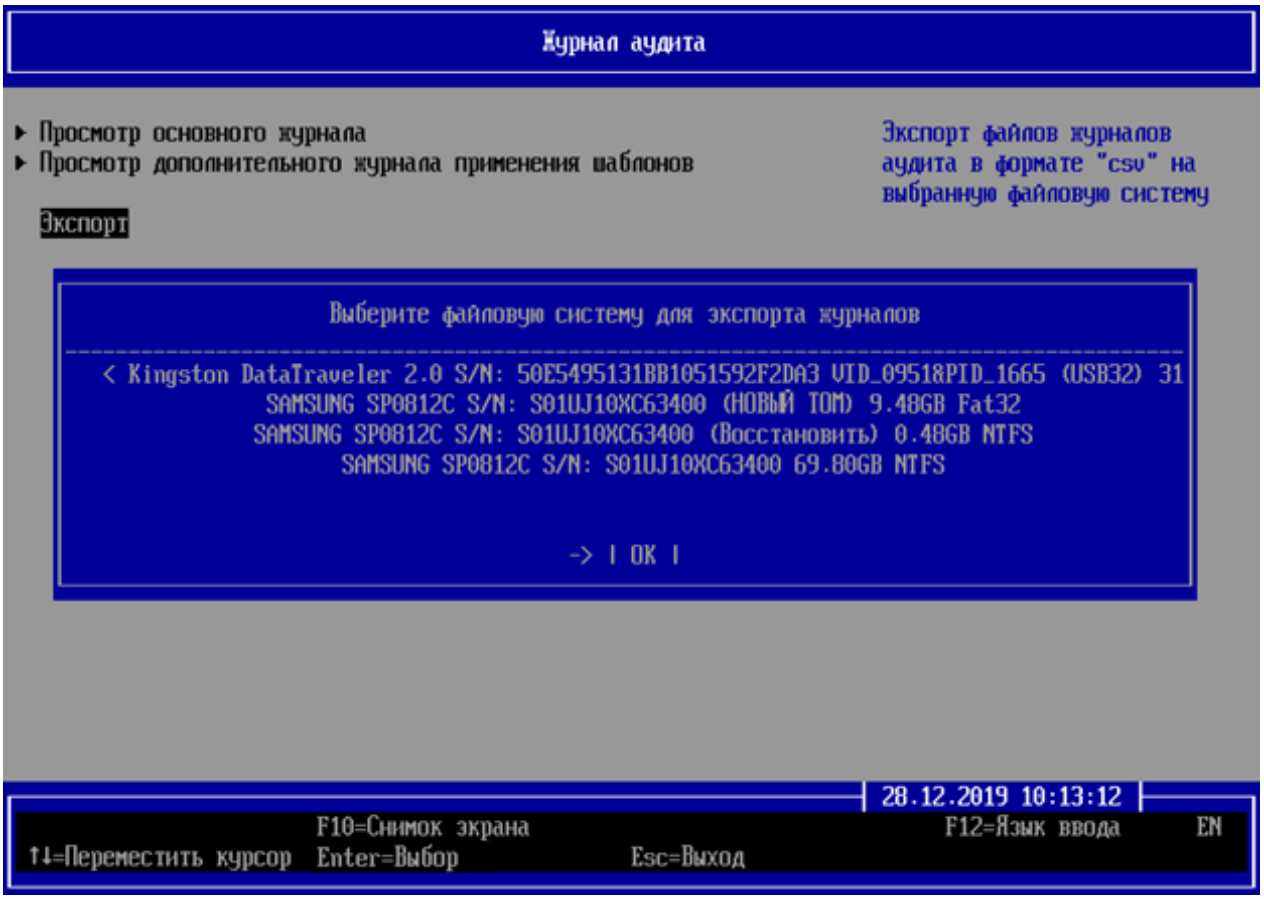
№	Событие	Успех/Ошибка	Комментарий
Контроль устройств			
4	Редактирование списка контролируемых устройств	Успех	Политика <имя политики> Добавление <имя объекта>
		Ошибка	
Управление загрузкой ОС			
5	Редактирование списка ОС пользователя	Успех	Политика <имя политики> Добавление <наименование ОС>
		Ошибка	
Управление дисками			
6	Редактирование списка контролируемых загрузочных областей	Успех	Политика <имя политики> Добавление <имя объекта>
		Ошибка	
Контроль целостности среды UEFI			
7	Редактирование списка целостности среды UEFI	Успех	Политика <имя политики> Добавление <имя объекта>
		Ошибка	
Работа с учетными записями пользователей			
8	Создание учетной записи пользователя	Успех	Добавление <имя пользователя>
9	Обновление учетной записи пользователя	Успех	Редактирование <имя пользователя>
Работа с политиками аутентификации пользователей			
10	Создание политики аутентификации	Успех	Добавление <имя политики>
11	Обновление политики аутентификации	Успех	Редактирование <имя политики>
Работа с политиками контроля целостности объектов и загрузки ОС			
12	Создание политики контроля целостности объектов и загрузки ОС	Успех	Добавление <имя политики>
13	Обновление политики контроля целостности объектов и загрузки ОС	Успех	Редактирование <имя политики>

6.4 Экспорт журналов аудита

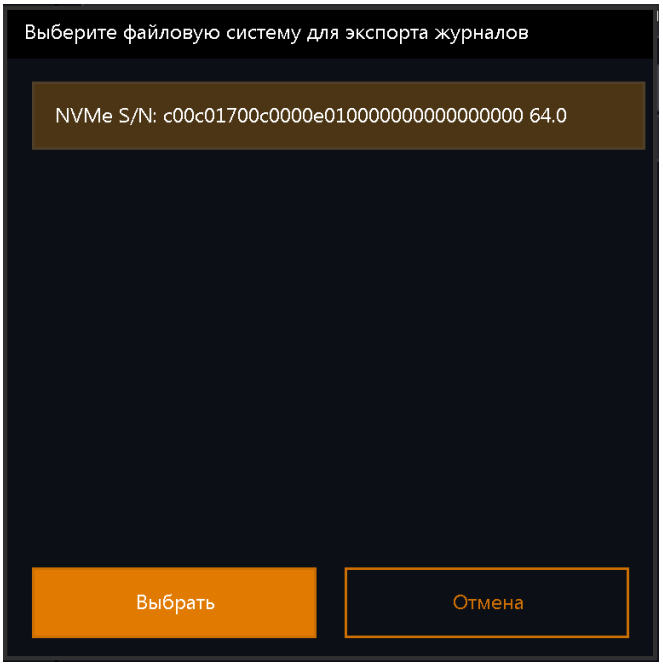
6.4.1 Аудитор имеет возможность экспортировать журналы аудита на внешнее устройство хранения данных. Для этого необходимо:

- подключить устройство хранения данных к ЭВМ;
- перейти курсором в строку «***Экспорт***» (рисунок 6.2) и нажать клавишу < ***Enter*** >;
- в новом диалоговом окне выбрать устройство хранения данных и нажать кнопку | ***OK*** | (рисунок 6.6);
- при успешном экспорте журналов на экран ЭВМ будет выведено сообщение (рисунок 6.7).

6.4.2 Журналы аудита сохраняются в корневой раздел выбранного устройства хранения данных с именами файлов **sdzlog.csv** и **sdzlogT.csv** (рисунок 6.7).

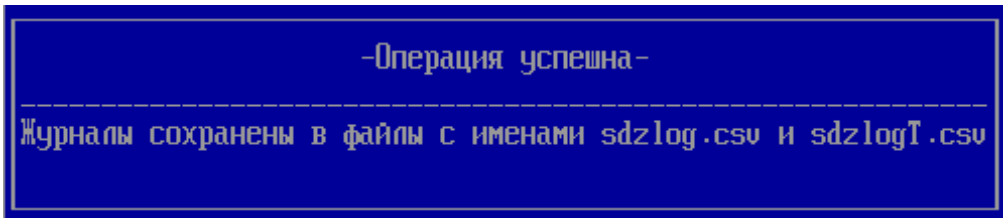


а) Псевдографический интерфейс

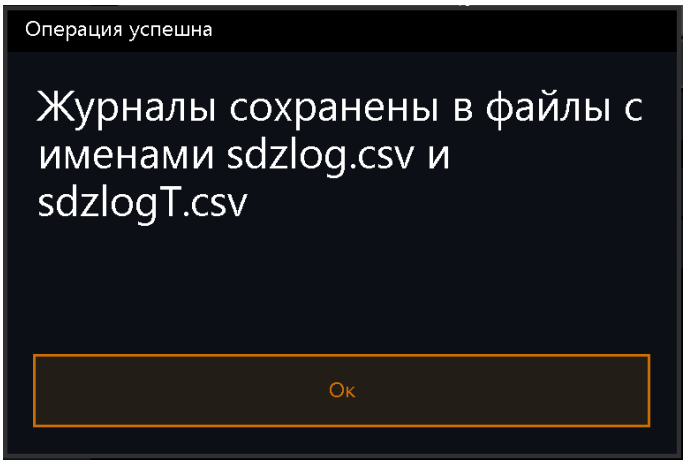


б) Графический интерфейс

Рисунок 6.6 – Выбор устройства хранения данных для экспорта журналов аудита



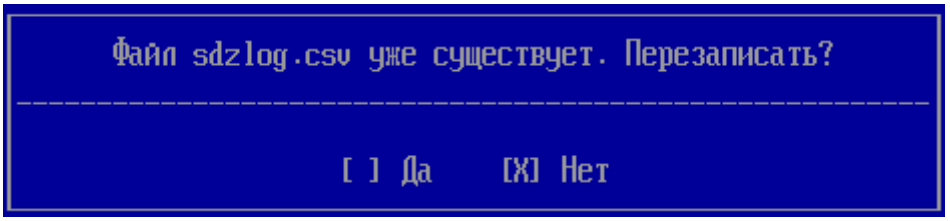
а) Псевдографический интерфейс

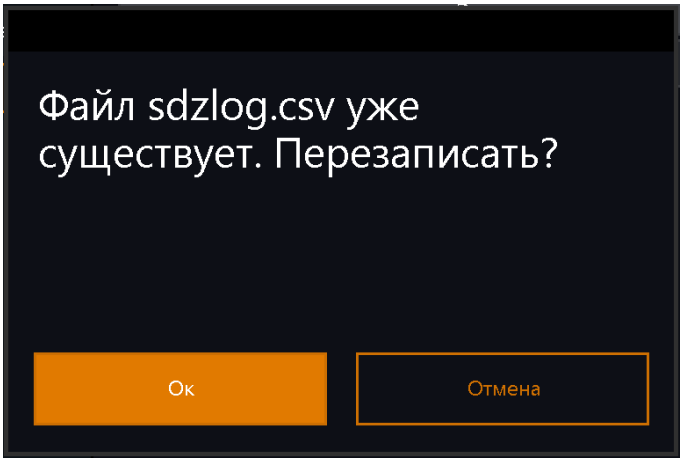


б) Графический интерфейс

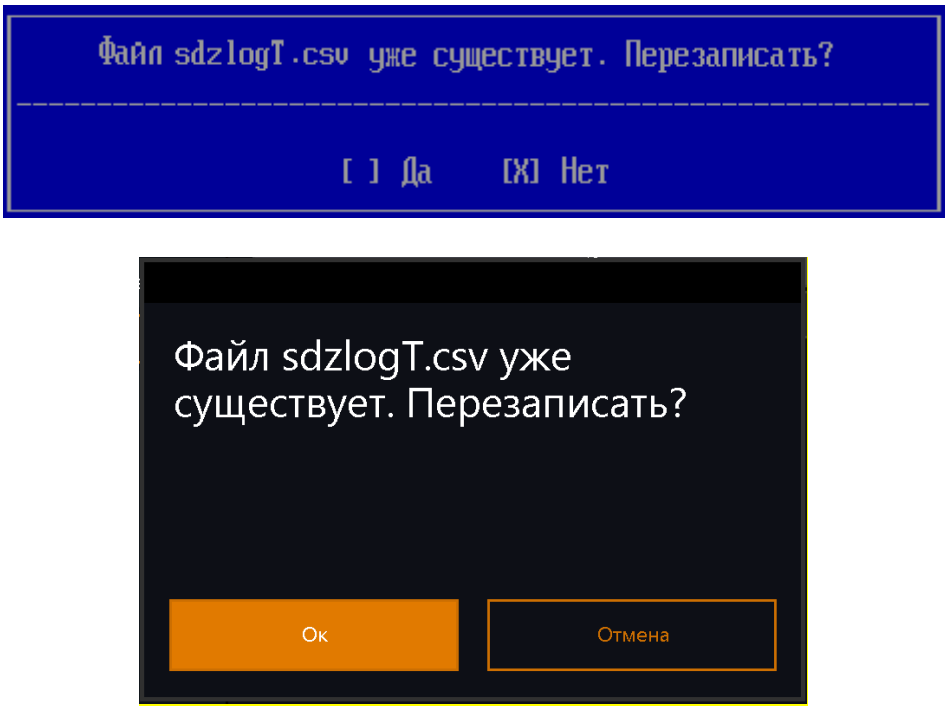
Рисунок 6.7 – Успешный экспорт журналов аудита

6.4.3 В случае существования на выбранном устройстве хранения данных файла с таким именем аудитору на экран ЭВМ будет выведено предупреждение (рисунок 6.8 а, б).





а)



б)

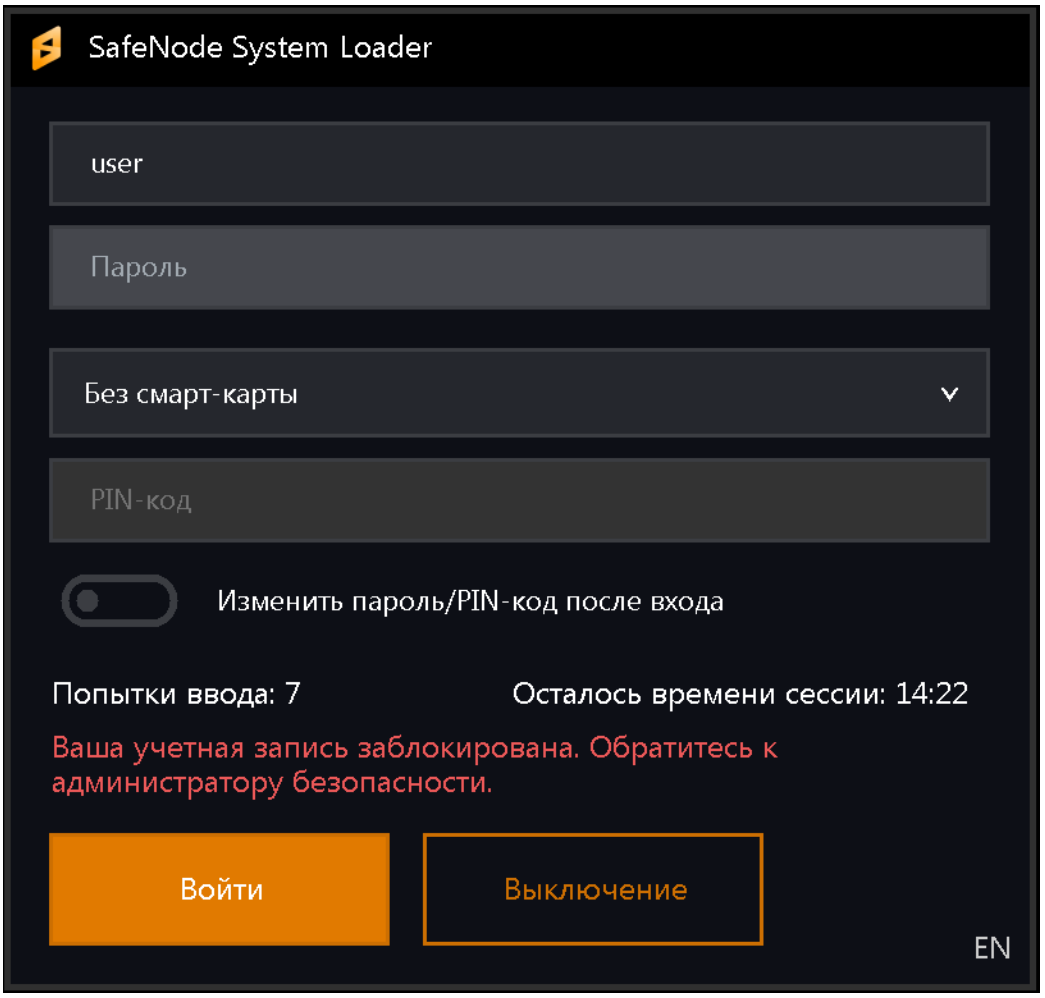
Рисунок 6.8 – Перезапись файлов журналов аудита

Рекомендуется периодически осуществлять экспорт журналов на внешнее устройство хранения данных.

7 Нарушение политики контроля целостности

7.1 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 7.1).

а) Псевдографический интерфейс



б) Графический интерфейс

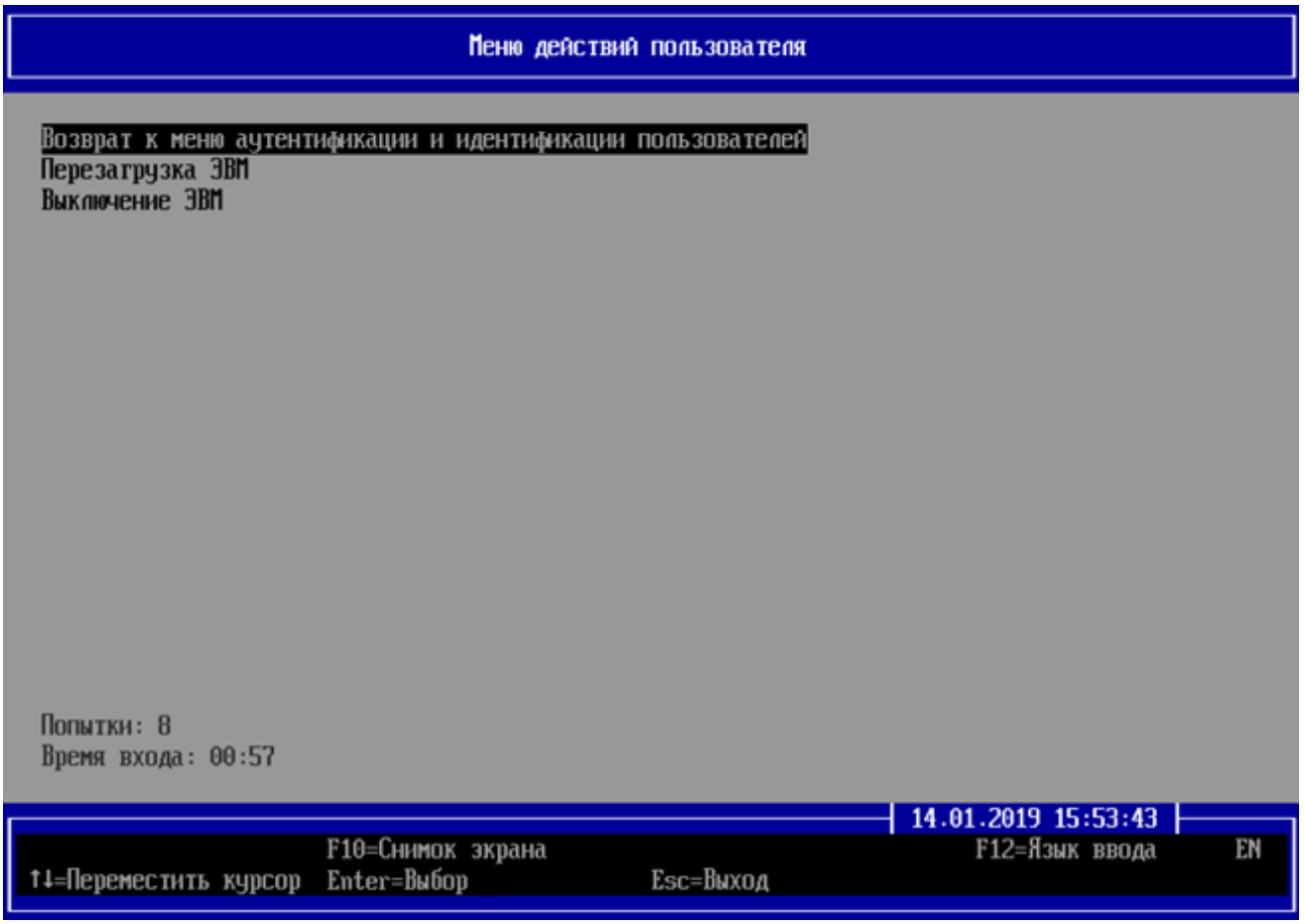
Рисунок 7.1 – Блокировка доступа при обнаружении нарушения КЦ

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

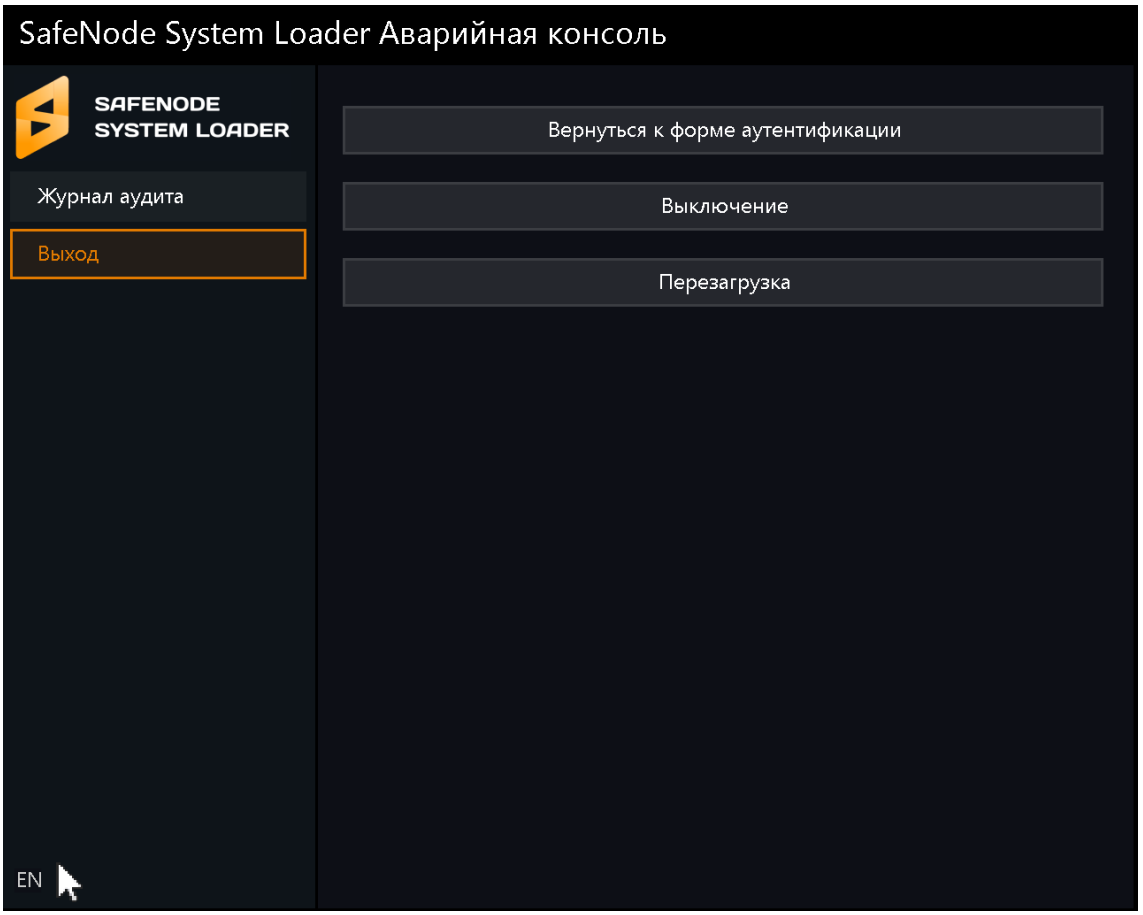
8 Завершение работы с изделием

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

8.2 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 8.1), нажав клавишу **< *Esc* >** после появления окна идентификации и аутентификации пользователя.



а) Псевдографический интерфейс



а) Графический интерфейс

Рисунок 8.1 – Меню действий пользователя

8.3 В окне рисунка 8.1 а) 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 >***.

8.4 Для подтверждения перезагрузки ЭВМ необходимо нажать клавишу ***< Enter >*** и подтвердить действие, выбрав пункт меню ***«Да»*** (рисунок 8.2).

8.5 Для подтверждения выключения ЭВМ необходимо нажать клавишу ***< Enter >*** и подтвердить действие, выбрав пункт меню ***«Да»*** (рисунок 8.3).

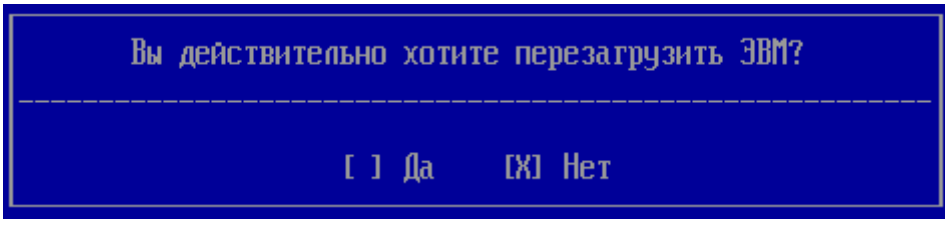


Рисунок 8.2 – Подтверждение действия пользователя для перезагрузки ЭВМ

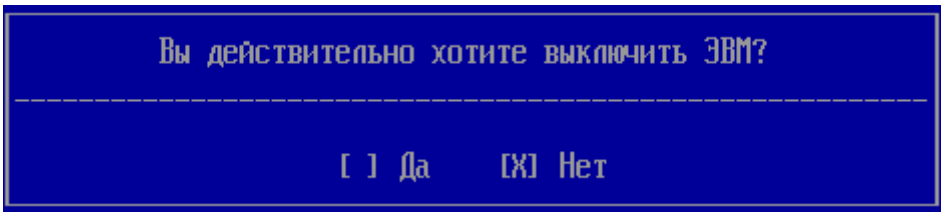


Рисунок 8.3 – Подтверждение действия пользователя для выключения ЭВМ

В графическом интерфейсе при выборе перезагрузки или выключения ЭВМ действия осуществляются без подтверждения сразу после выбора соответствующего пункта меню.

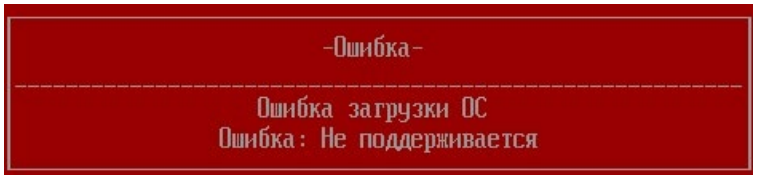
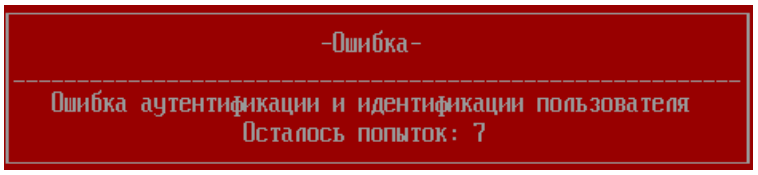
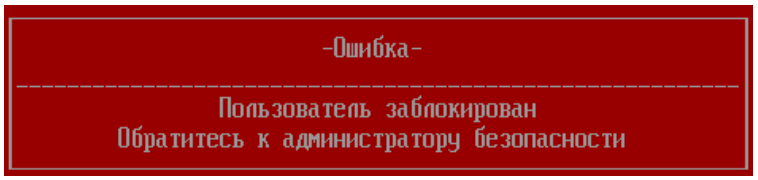
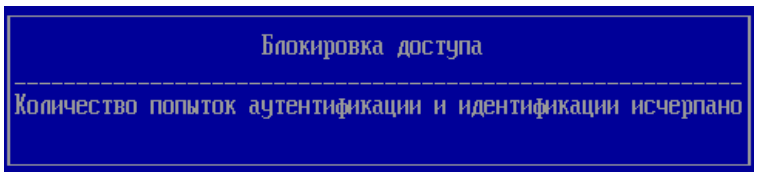
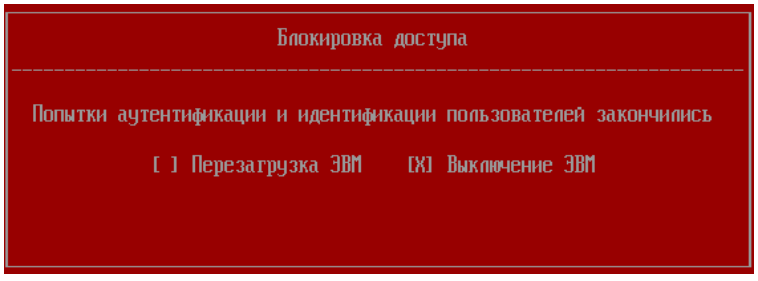
9 Сообщения об ошибках и порядок действий пользователей по их устранению

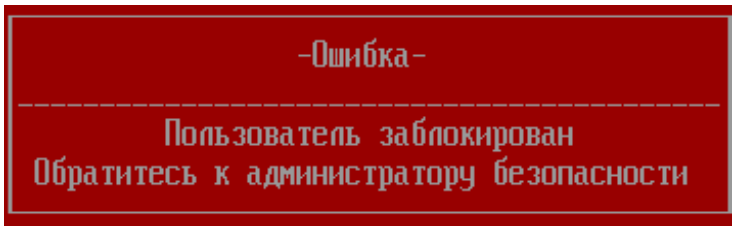
9.1 В процессе работы изделия в составе ЭВМ возможно возникновение ситуаций, при которых пользователям на экран ЭВМ в диалоговых окнах выдаются сообщения об ошибках.

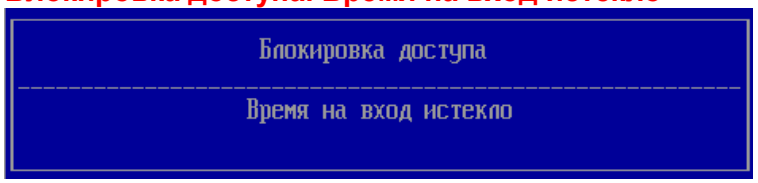
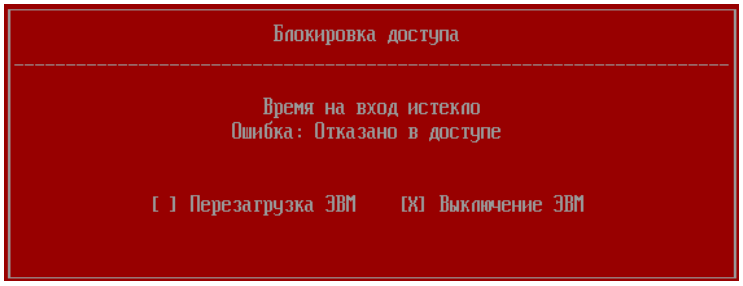
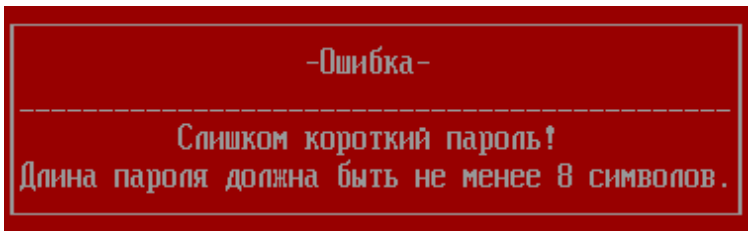
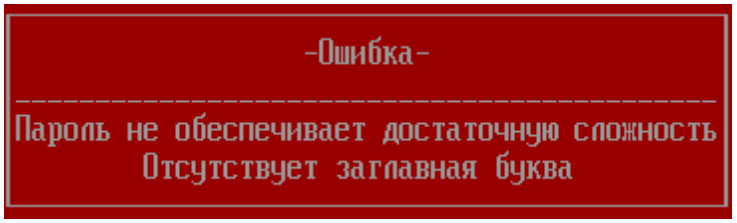
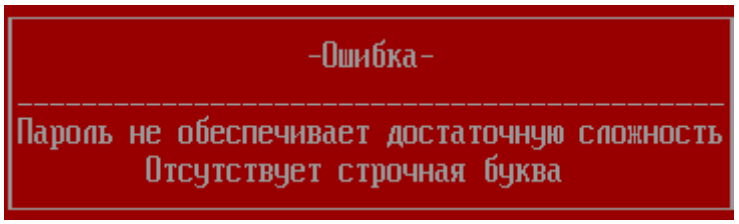
9.2 Перечень сообщений, причины их возникновения и порядок действий пользователей по их устранению приведен в таблице 9.1.

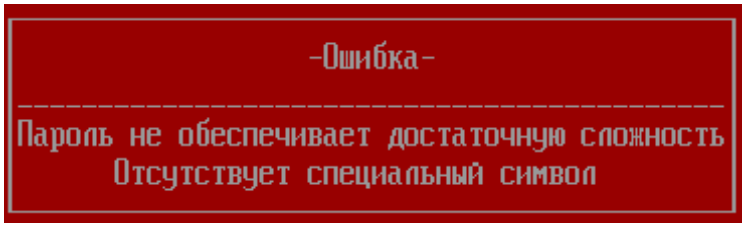
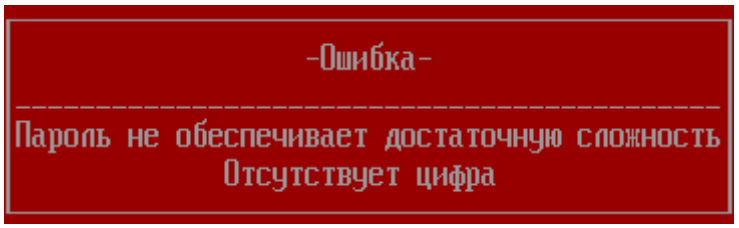
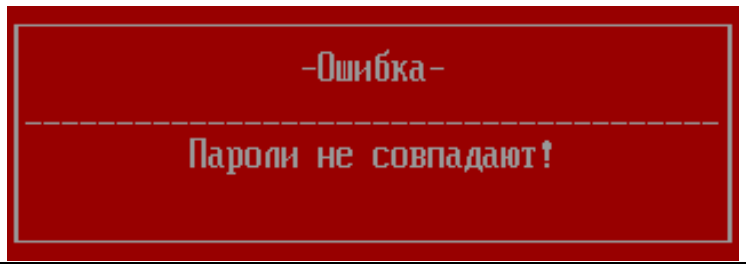
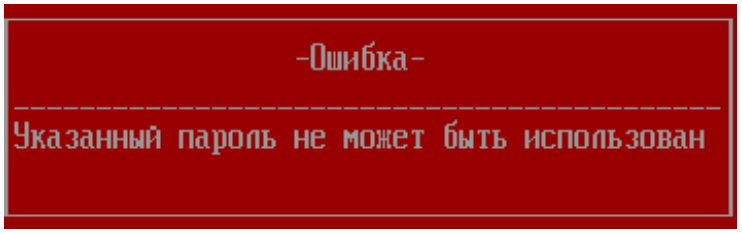
Таблица 9.1 – Перечень сообщений об ошибках при работе с ПО изделия

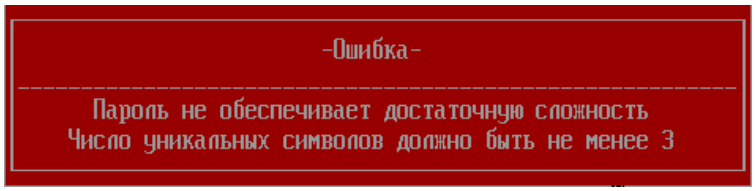
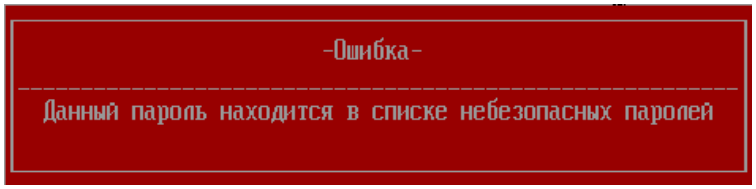
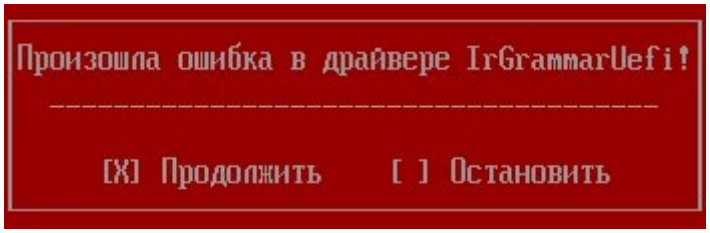
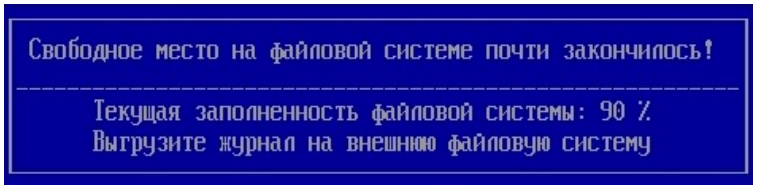
№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий пользователей
1	**Ошибка System blocked!** 	**Причины:** Некорректный ключ базы данных или поврежденная база данных изделия **Порядок действий:** Обратиться к АБ для восстановления изделия
2	**Ошибка System blocked!** 	**Причины:** 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

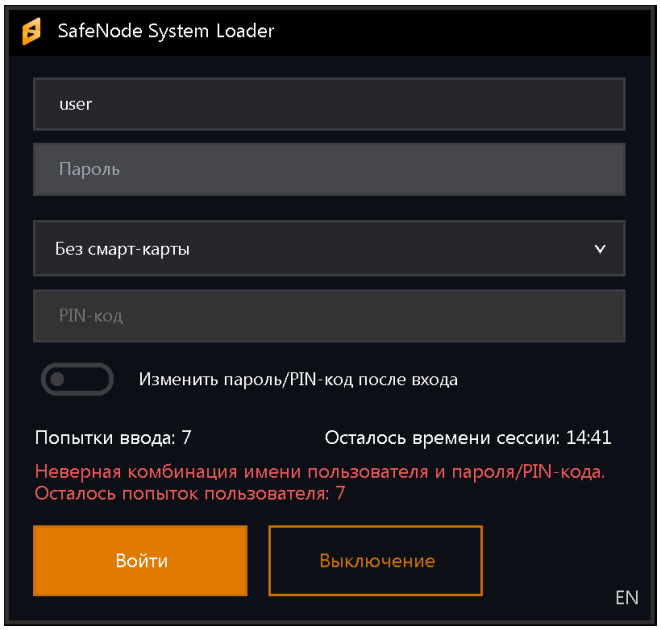
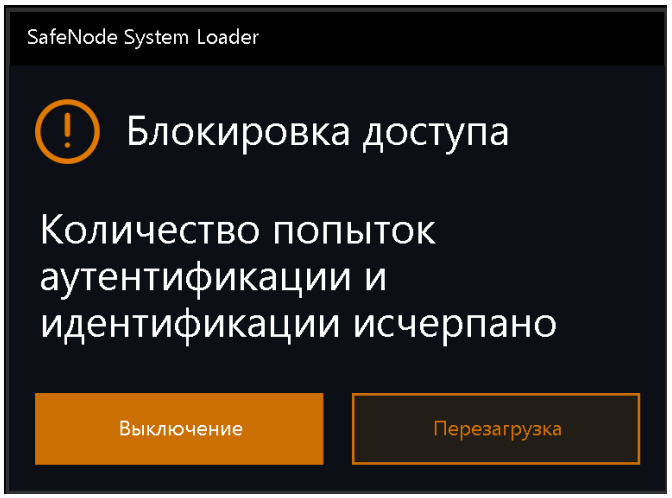
№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий пользователей
4	**Ошибка загрузки ОС** 	**Причины:** В качестве загрузчика ОС указан неверный файл **Порядок действий:** Указать верный файл загрузчика в пункте меню ***«Контроль загрузки ОС»***
5	**Ошибка аутентификации и идентификации 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.

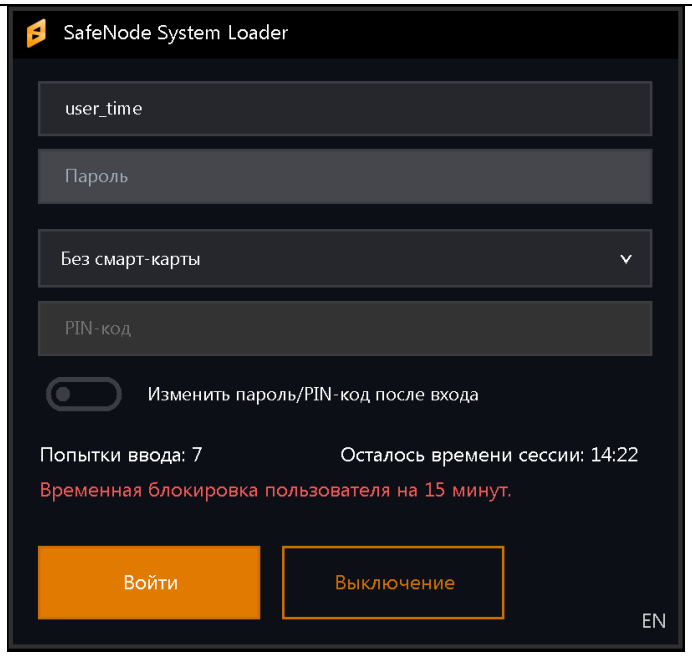
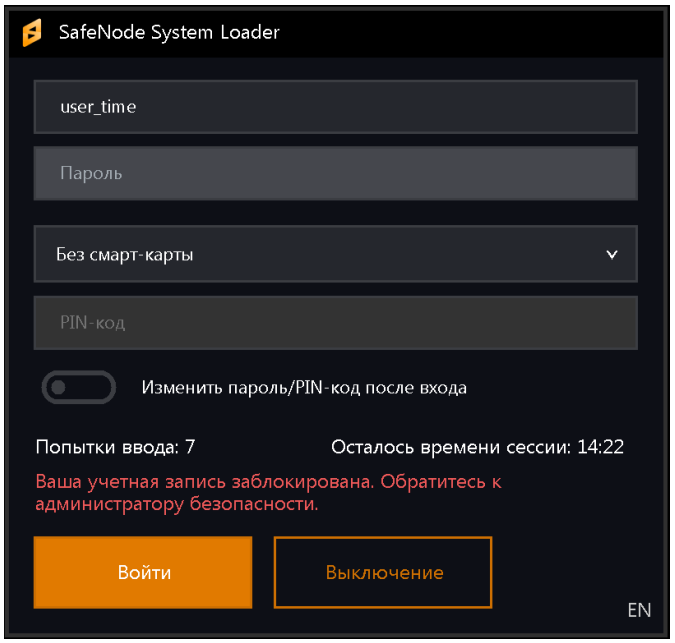
№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий пользователей
7	**Временная блокировка пользователя на N минут** 	**Причины:** Достигнуто максимально разрешенное количество индивидуальных попыток аутентификации пользователя **Порядок действий:** Обратиться к АБ
8	**Блокировка 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

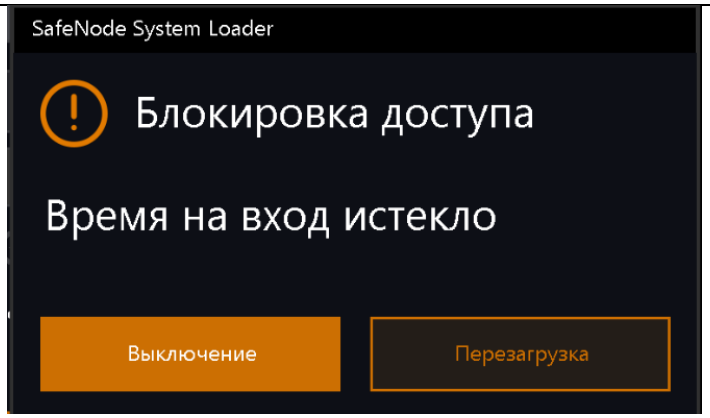
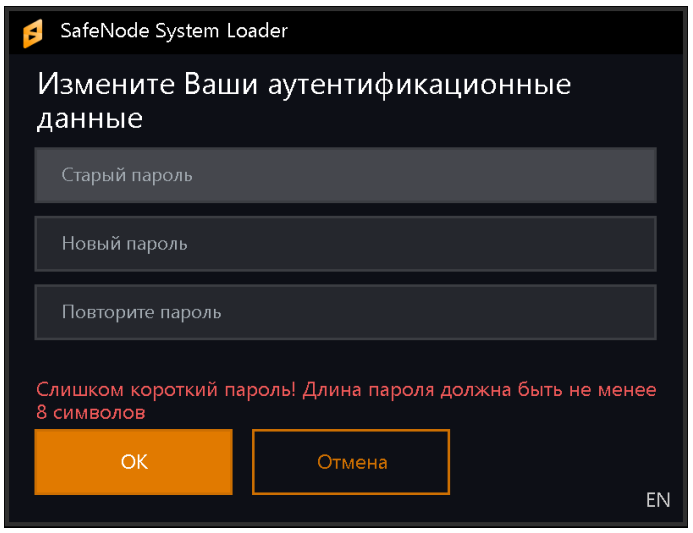
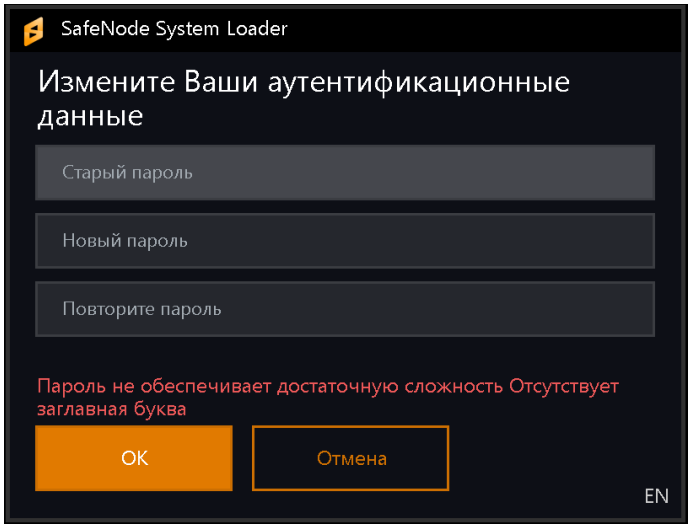
№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий пользователей
9	**Блокировка доступа. Время на вход истекло**  	**Причины:** Возникает при истечении общего времени аутентификации пользователей **Порядок действий:** Выключить ЭВМ или перезагрузить ЭВМ и повторно выполнить процедуру 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

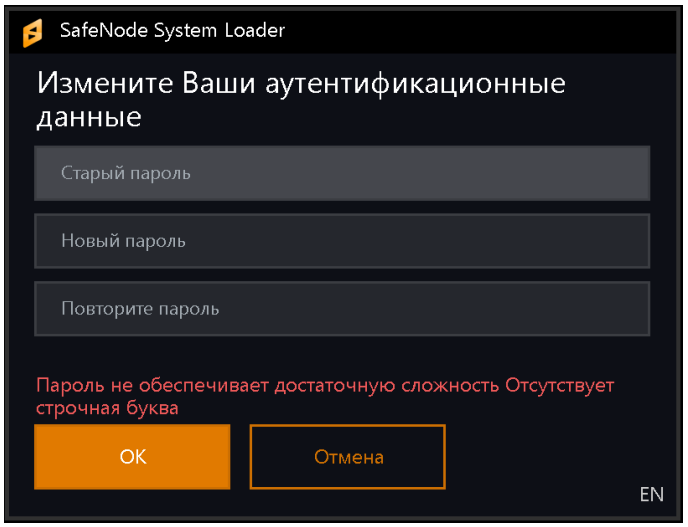
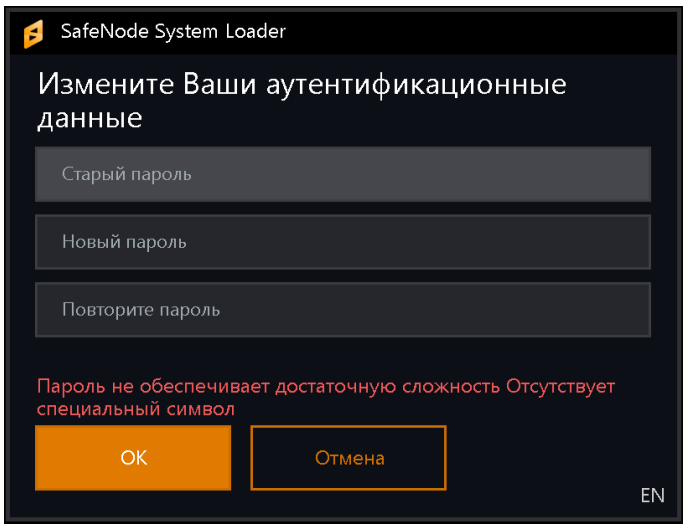
№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий пользователей
13	**Отсутствует специальный символ** 	**Причины:** Новый пароль пользователя не удовлетворяет требованиям по сложности **Порядок действий:** Ввести новый пароль, который будет содержать хотя бы один специальный символ
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.

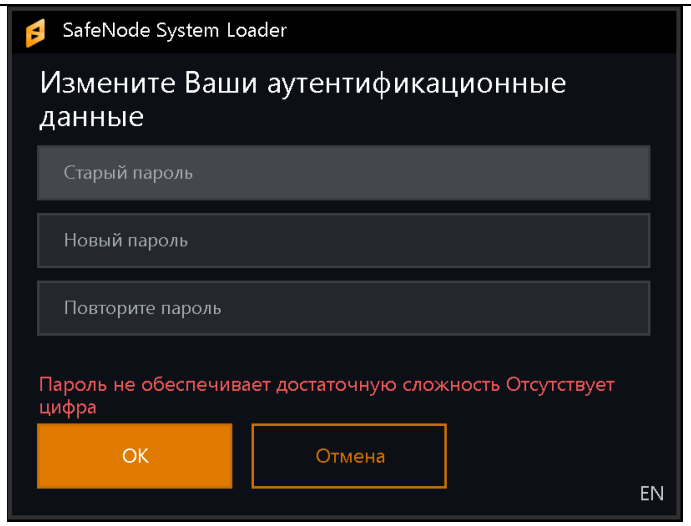
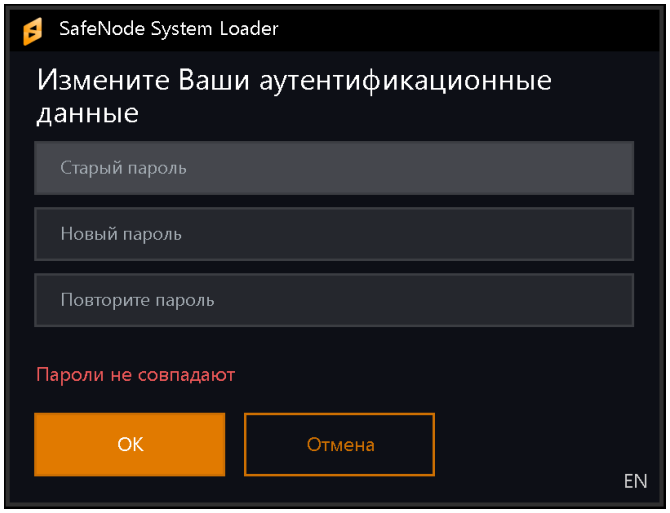
№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий пользователей
17	**Пароль не обеспечивает достаточную сложность. Число уникальных символов должно быть не менее N** 	**Причины:** Новый пароль содержит меньшее количество уникальных символов. **Порядок действий:** Необходимо указать новый пароль пользователя, который содержит необходимое количество уникальных символов согласно политике аутентификации.
18	**Данный пароль находится в списке небезопасных паролей** 	**Причины:** Новый пароль совпадает с паролем из перечня небезопасных паролей. **Порядок действий:** Необходимо указать новый пароль пользователя, который удовлетворяет требованиям согласно политике аутентификации.
19	**Произошла ошибка в драйвере IrGrammarUefi!** 	**Причины:** Ошибка в работе драйвера динамического контроля исполнения кода изделия **Порядок действий:** Продолжить работу или обратиться к АБ для восстановления системы
20	**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

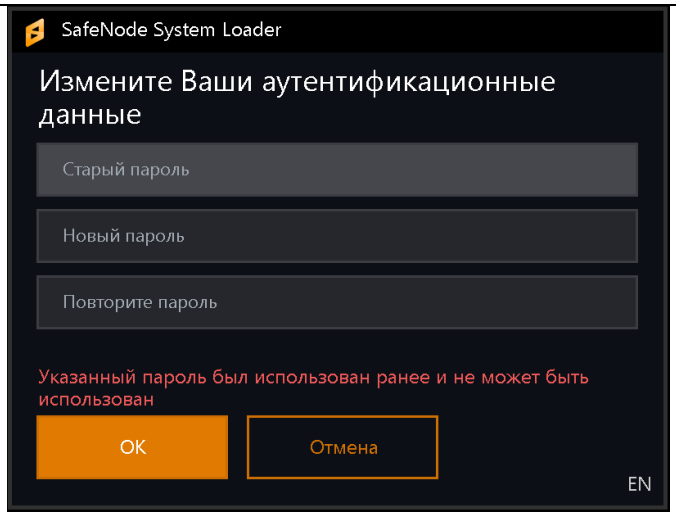
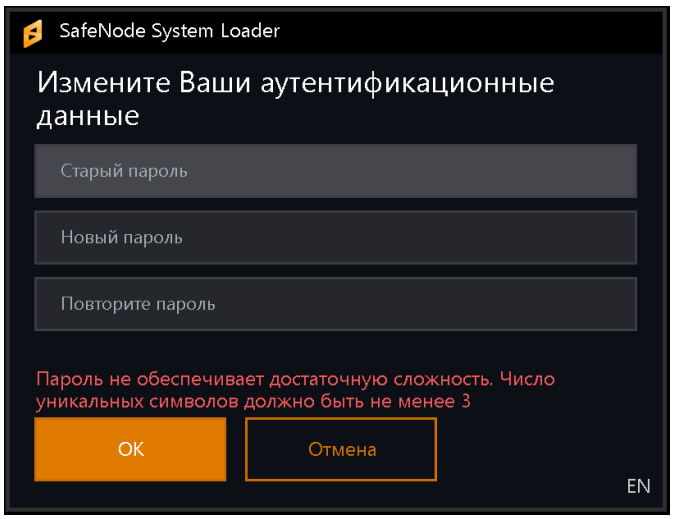
№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий пользователей
21	**Неверная комбинация имени пользователя и пароля/PIN-кода. Осталось попыток пользователя: N** 	**Причины:** Указание неверного идентификатора или пароля пользователя **Порядок действий:** Проверить корректность указанных аутентификационных и идентификационных данных пользователя
22	**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.
23	**Временная блокировка пользователя на N минут**	**Причины:** Достигнуто максимально разрешенное количество индивидуальных попыток аутентификации пользователя **Порядок действий:** Обратиться к АБ

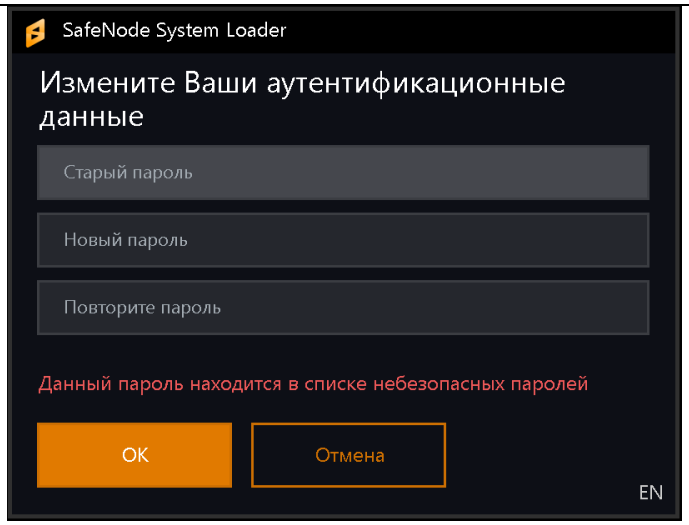
№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий пользователей
		
24	**Ваша учетная запись заблокирована. Обратитесь к администратору безопасности.** 	**Причины:** 1. Нарушение КЦ аппаратной и/или программной конфигурации ЭВМ. У данного пользователя указан тип реакции на нарушении 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
25	**Блокировка доступа. Время на вход истекло**	**Причины:** Возникает при истечении общего времени

№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий пользователей
		аутентификации пользователей **Порядок действий:** Выключить ЭВМ или перезагрузить ЭВМ и повторно выполнить процедуру идентификации и аутентификации
26	**Слишком короткий пароль!** 	**Причины:** Новый пароль пользователя не удовлетворяет требованиям по минимальной длине пароля **Порядок действий:** Ввести пароль длиной не менее 8 символов
27	**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

№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий пользователей
28	**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
29	**Отсутствует специальный символ** 	**Причины:** Новый пароль пользователя не удовлетворяет требованиям по сложности **Порядок действий:** Ввести новый пароль, который будет содержать хотя бы один специальный символ
30	**Отсутствует цифра**	**Причины:** Новый пароль пользователя не удовлетворяет требованиям по сложности **Порядок действий:** Ввести новый пароль, который будет содержать хотя бы одну цифру

№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий пользователей
		
31	**Пароли не совпадают!** 	**Причины:** Несовпадение нового пароля и его подтверждения **Порядок действий:** Ввести верный новый пароль и его подтверждение
32	**Указанный пароль был использован ранее и 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

№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий пользователей
		пользователя, отличный от текущего.
33	**Пароль не обеспечивает достаточную сложность. Число уникальных символов должно быть не менее N** 	**Причины:** Новый пароль содержит меньшее количество уникальных символов. **Порядок действий:** Необходимо указать новый пароль пользователя, который содержит необходимое количество уникальных символов согласно политике аутентификации.
34	**Данный пароль находится в списке небезопасных паролей**	**Причины:** Новый пароль совпадает с паролем из перечня небезопасных паролей. **Порядок действий:** Необходимо указать новый пароль пользователя, который удовлетворяет требованиям согласно политике аутентификации.

№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий пользователей
		

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