ГАЗИНФОРМ СЕРВИС

Средство доверенной загрузки «SafeNode System Loader»

Руководство по эксплуатации
Часть 2

Руководство администратора

Санкт-Петербург, 2024

Содержание

Введение

Настоящее руководство администратора безопасности средства доверенной загрузки (СДЗ) «SafeNode System Loader» (далее по тексту – изделие) является эксплуатационным документом (ЭД), содержащим информацию о действиях администратора безопасности (АБ) по управлению параметрами изделия, а также по созданию, редактированию и удалению учетных записей пользователей и политик безопасности.

Информация о назначении изделия, а также условиях его применения и решаемой задаче приведены в документе «Средство доверенной загрузки «SafeNode System Loader». Описание применения. 72410666.00060-04 31 01».

Установка изделия осуществляется согласно рекомендациям документа «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 1. Руководство по установке. ГМТК.468269.060РЭ1».

Описание управления параметрами изделия из консоли АБ Linux/Windows приведено в документе «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 3. Руководство администратора Linux/Windows. ГМТК.468269.060РЭ3».

Правила по работе пользователей приведены в документе «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 4. Руководство пользователя. ГМТК.468269.060РЭ4».

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.

1.1.2 Программное обеспечение (ПО) изделия поддерживает работу с загрузчиками ОС и файловыми системами, указанными в таблице 1.1.

Таблица 1.1 – Список поддерживаемых загрузчиков и файловых систем в изделии

Семейство ОС	Тип загрузчика ОС	Файл загрузчика ОС	Тип файловой системы
Windows	Windows Boot Manager	Master Boot Record (MBR) …\EFI\BOOT\BOOTX64.EFI …\EFI\Microsoft\Boot\bootmgfw.efi	FAT32, NTFS
Unix	LInux LOader (LILO)	MBR	Ext2, Ext3, Ext4, FAT32, UDF
	Grand Unified Bootloader (GRUB)	…\EFI\BOOT\BOOTX64.EFI	
Linux	LILO	MBR …\EFI\BOOT\BOOTX64.EFI	Ext2, Ext3, Ext4, FAT32, UDF
	GRUB	…\EFI\BOOT\BOOTX64.EFI …\EFI\BOOT\FBX64.EFI …\EFI\BOOT\grubx64.efi …\EFI\CENTOS\GRUBX64.EFI	

Семейство ОС	Тип загрузчика ОС	Файл загрузчика ОС	Тип файловой системы
		…\EFI\CENTOS\SHIM.EFI …\EFI\CENTOS\SHIMX64.EFI …\EFI\CENTOS\shimx64-centos.efi …\EFI\redhat\grubx64.efi …\EFI\redhat\shim.efi …\EFI\redhat\shimx64.efi …\EFI\redhat\shimx64-redhat.efi …\EFI\ubuntu\grubx64.efi …\EFI\ubuntu\shimx64.efi	
VMware ESX, VMware ESXi	LILO	MBR …\EFI\BOOT\BOOTX64.EFI	Ext2, Ext3, Ext4, FAT32, UDF
	GRUB	MBR …\EFI\BOOT\BOOTX64.EFI	Ext2, Ext3, Ext4, FAT32, UDF

Для поддержки необходимого уровня защищенности ЭВМ и ее информационных ресурсов, эксплуатации и эффективного применения изделия требуется обязательное выполнение следующих организационно-технических мероприятий:

- установка изделия осуществляется уполномоченным лицом, ответственным за безопасность и эксплуатацию изделия на местах пользователей;
- перед началом использования необходимо ознакомиться с эксплуатационной документацией, входящей в комплект поставки изделия;
- установка изделия на ЭВМ должна осуществляться в соответствии с документом «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 1. Руководство по установке. ГМТК.468269.060РЭ1»;
- 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;
- настройка параметров изделия должна осуществляться в соответствии с документами «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 2. Руководство администратора. ГМТК.468269.060РЭ2» и «Средство доверенной загрузки «SafeNode System Loader». Руководство по

эксплуатации. Часть 3. Руководство администратора Linux/Windows. ГМТК.468269.060РЭ3»;

- работа пользователей должна осуществляться в соответствии с документом «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 4. Руководство пользователя. ГМТК.468269.060РЭ4»;
- восстановление работоспособности изделия после сбоев должно осуществляться в соответствии с документом «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 5. Руководство по безопасному восстановлению. ГМТК.468269.060РЭ5»;
- для обеспечения надежной эксплуатации ЭВМ должна иметь минимальный состав технических и программных средств и должна быть произведена первоначальная настройка параметров BIOS Setup;
- при создании автоматизированных рабочих мест (АРМ) с использованием изделия обязательна проверка его совместимости и ЭВМ, в составе которой предполагается использование изделия;
- установка изделия должна осуществляться на ЭВМ защищаемой локальной вычислительной сети, расположенной в контролируемой зоне;
- КЦ исполняемых программных модулей на эксплуатируемой ЭВМ во время сеанса работы пользователя, их надежное восстановление из резервных копий и очистка оперативной памяти ЭВМ после завершения процессов должны обеспечиваться сертифицированными средствами защиты информации от несанкционированного доступа;
- АБ должен периодически проверять наличие обновлений ОС на официальном сайте разработчика и устанавливать их на эксплуатируемую ЭВМ;
- после завершения установки и настройки изделия должны быть приняты организационно-технические меры, исключающие бесконтрольный доступ к изделию и техническим средствам ЭВМ;
- после установки изделия на ЭВМ АБ должен установить пароль для входа в BIOS Setup;
- АБ запрещается обновлять (модифицировать) ПО UEFI BIOS ЭВМ после установки изделия;
- запрещается использование режимов энергопотребления ЭВМ «Standby» и «Hibernate» при эксплуатации изделия;
- обеспечение физической сохранности (целостности) ЭВМ, наличие физической охраны помещения, в котором эксплуатируется ЭВМ и исключение возможности несанкционированного доступа к ЭВМ посторонних лиц;
- хранение в секрете идентификаторов (имен), паролей (кодов), а также PIN-кодов аутентификационных носителей пользователей (АНП) и АБ;

- периодическая смена паролей и PIN-кодов АНП пользователей и АБ.

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

  В таблице 1.2 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 персональным электронным идентификатором, указанными в таблице 1.2;
- аутентификация с использованием цифровых сертификатов пользователей с возможностью дополнительной проверки в службе каталогов (AD, FreeIPA). Для хранения сертификата поддерживается работа с персональным электронным идентификатором, указанными в таблице 1.2;
- блокировка загрузки пользователями нештатных копий ОС;
- блокировка возможности обхода процесса доверенной загрузки с помощью внешних органов управления;

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

- 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 CBT, 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» 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 АБ;
- диагностика программных средств изделия.

Таблица 1.2 – 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		

№	Название АНП	Тип носителя	Примечание	Поддерживаемые типы входа	Сведения о сертификате (справочно)	Гриф секретности (справочно)
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						
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	КИ

№	Название АНП	Тип носителя	Примечание	Поддерживаемые типы входа	Сведения о сертификате (справочно)	Гриф секретности (справочно)
					Рутокен ЭЦП 2.0 2100)	
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)				
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		Вход по токену без сертификата	—	—
		Card				
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	Сертификат ФСТЭК России № 4515	СС

№	Название АНП	Тип носителя	Примечание	Поддерживаемые типы входа	Сведения о сертификате (справочно)	Гриф секретности (справочно)
				Вход по токену без сертификата		

Примечание:

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

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.**

1.3 Состав изделия

1.3.1 Изделие состоит из аппаратных и программных компонент.

1.3.2 К аппаратным компонентам изделия относятся применяемые АНП.

1.3.3 Перечень и количество средств аутентификации и идентификации пользователей (АНП) определяется договором поставки изделия и обязательно указывается в разделе ***«Комплектность»*** документа «Средство доверенной загрузки «SafeNode System Loader». Формуляр. 72410666.00060-04 30 01»:

- ГМТК.685001.060 – АНП JaCarta;
- ГМТК.685002.060 – АНП Рутокен ЭЦП (Rutoken ECP) и Рутокен Lite;
- ГМТК.685003.060 – АНП eToken;
- ГМТК.685004.060 – АНП SafeNet eToken;
- ГМТК.685005.060 – АНП Guardant ID.

1.3.4 **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».

1.3.5 После установки изделия и его первичной настройки согласно руководству по установке АБ доступны три варианта исполнения консоли управления параметрами СДЗ:

- **псевдографическая консоль СДЗ** (рисунок 1.1), исполняемая в среде **UEFI BIOS** и запускаемая по требованию АБ (**консоль АБ**). Доступна АБ только после успешного прохождения их процедуры аутентификации и идентификации после включения питания ЭВМ и старте ПО изделия. Дополнительно доступна загрузка **графической аварийной консоли СДЗ (аварийная консоль АБ)** (рисунок 1.2);
- **графическая консоль СДЗ Linux (консоль АБ Linux,** рисунок 1.3), запускаемая по требованию АБ из среды ОС Linux. Для работы требуется предварительно установить дополнительные компоненты из архива **snsl.tar.gz** (входит в состав дистрибутива изделия). Для запуска консоли и управления параметрами СДЗ требуется обязательная аутентификация и идентификация АБ;
- **графическая консоль СДЗ Windows (консоль АБ Windows)**, запускаемая по требованию АБ из среды ОС **Windows** (рисунок 1.4). Требуется дополнительная установка компонент с помощью инсталлятора ***SafeNodeSystemLoader.exe*** (входит в состав дистрибутива изделия). Для запуска консоли и управления параметрами СДЗ требуется обязательная аутентификация и идентификация АБ.

Рисунок 1.1 – Интерфейс консоли АБ

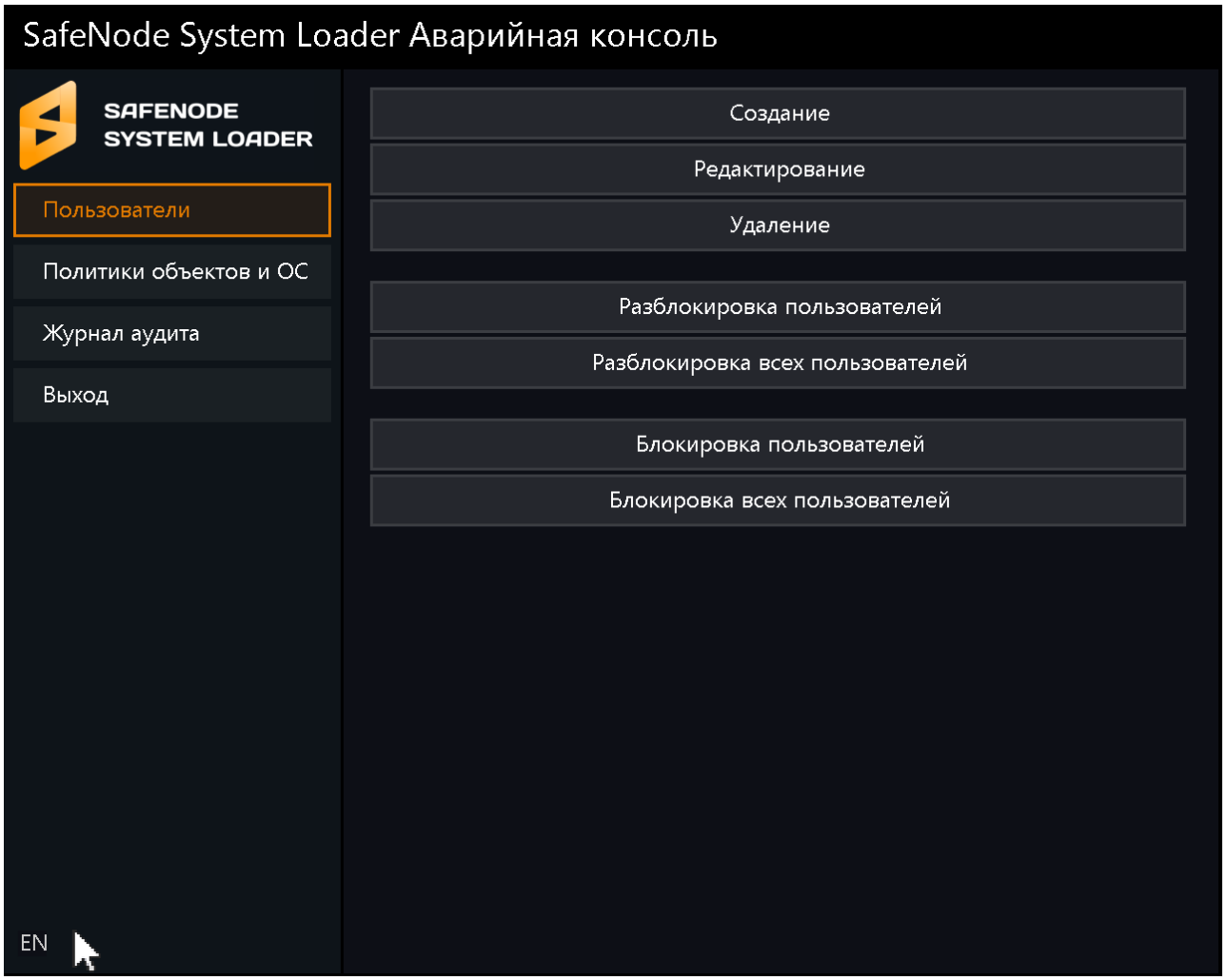


Рисунок 1.2 – Аварийная консоль АБ

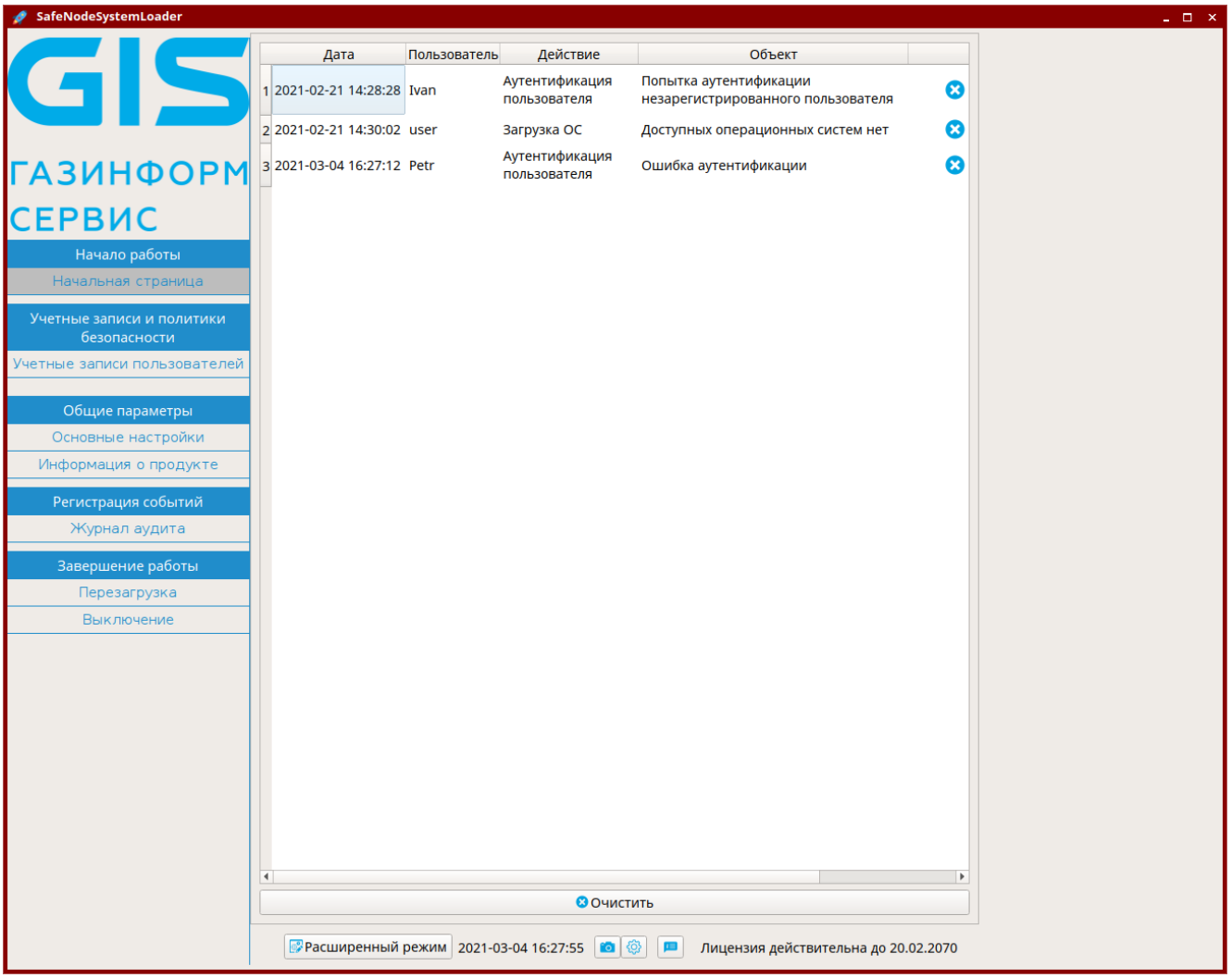


Рисунок 1.3 – Интерфейс консоли АБ Linux

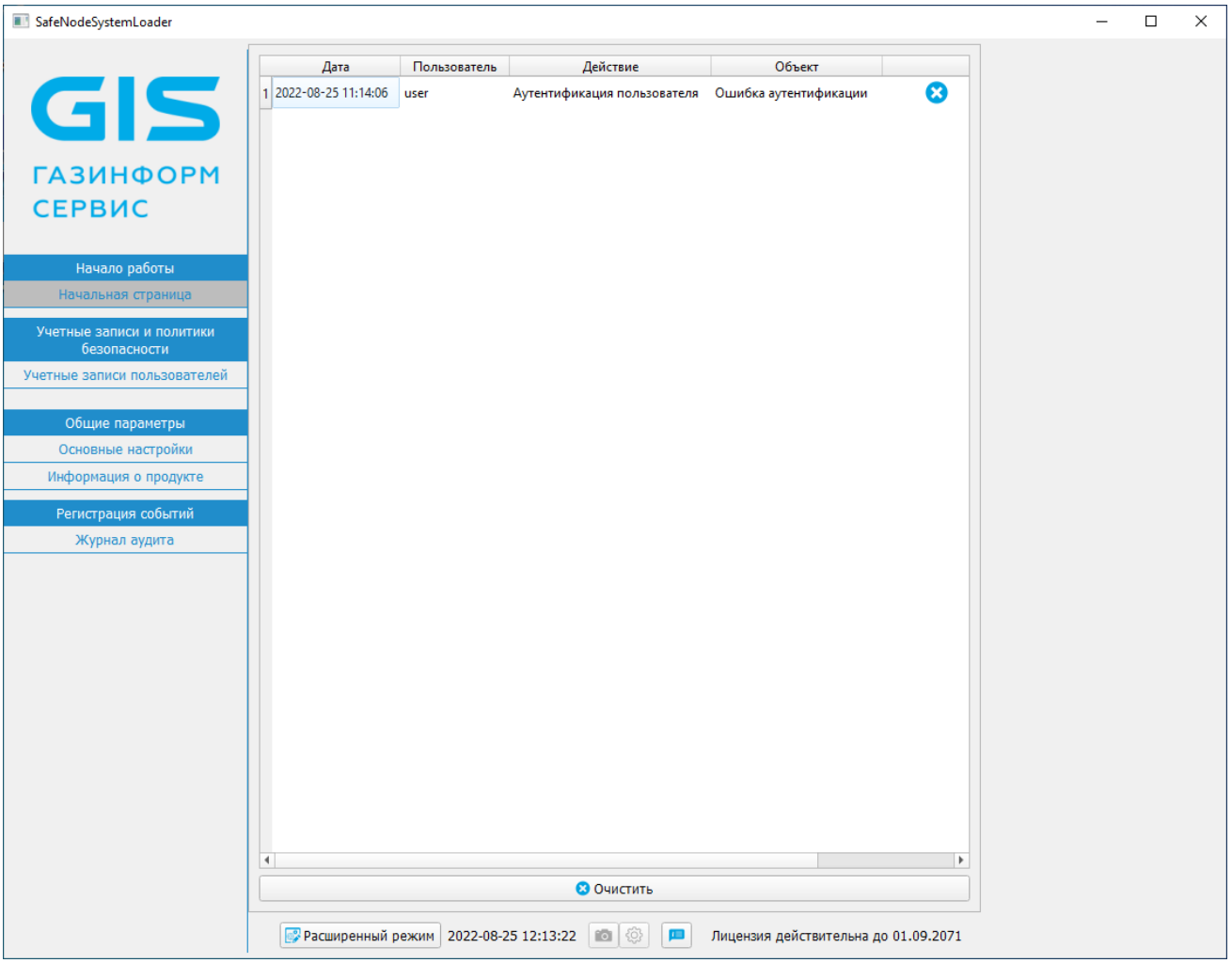


Рисунок 1.4 – Интерфейс консоли АБ Windows

1.3.6 База данных (БД) изделия является единой для всех консолей АБ.

1.4 Приемка изделия

1.4.1 Изделие поставляется на компакт-диске вместе с сопроводительным документом «Средство доверенной загрузки «SafeNode System Loader». Формуляр. 72410666.00060-04 30 01».

1.4.2 Комплектность поставки определяется в соответствии с разделом 4 формуляра.

1.4.3 Изделие закрепляется за ответственным за эксплуатацию (администратором безопасности) и данные фиксируются в таблице 8 формуляра.

1.4.4 При первичном закреплении изделия проводится контроль основных характеристик, необходимо произвести расчет контрольных сумм изделия и зафиксировать данные в таблице 5 формуляра.

2 Общая схема и порядок действий администратора безопасности по настройке и управлению параметрами изделия

2.1 На рисунке 2.1 приведена общая схема и порядок действий АБ по первоначальной установке, настройке и управлению параметрами изделия.

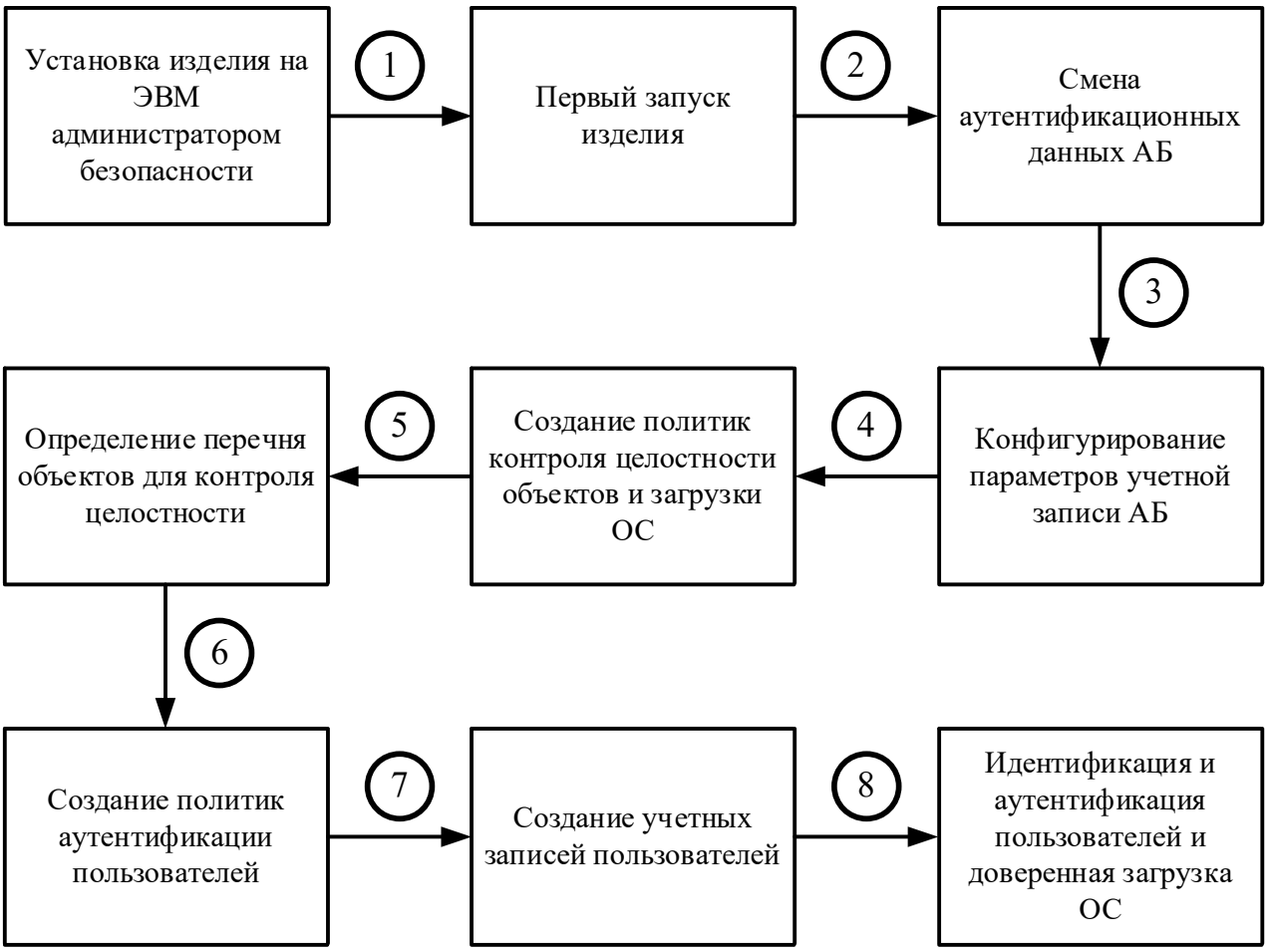


Рисунок 2.1 – Общая последовательность действий АБ при настройке изделия

2.2 Перед установкой на ЭВМ необходимо убедиться, что соблюдены все меры по реализации функций безопасности среды функционирования изделия согласно п 1.1 документа.

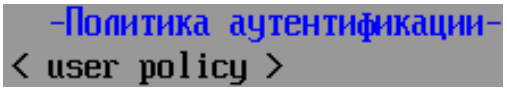
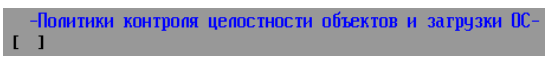
2.3 При работе с консолью АБ изменение параметров возможно путем ввода или выбора значений из известного списка **только с помощью клавиатуры** (рисунок 4.1).

При работе с 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 >***;
- поля с возможностью выбора **только одного значения параметра** обозначаются в интерфейсе в **< треугольных скобках >**;
- поля с возможностью выбора **множественных значений параметра** обозначаются в интерфейсе в **[квадратных скобках]**.

2.4 В таблице 2.1 приведено описание внешнего вида полей диалоговых окон интерфейса консоли АБ.

Таблица 2.1 – Внешний вид полей диалоговых окон интерфейса консоли АБ

Тип поля	**Внешний вид**	
	пустого поля	**заполненного поля**
Поле ввода значения		
Поле одиночного выбора		
Поле множественного выбора		

3 Первый запуск изделия

3.1 Загрузка изделия

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».

3.1.1 После успешной установки изделия потребуется перезагрузка ЭВМ для вступления в силу изменений, внесенных ПО изделия. В случае успешной контрольной проверки цифровых подписей модулей изделия загрузится графический интерфейс аварийной консоли изделия (рисунок 3.1).

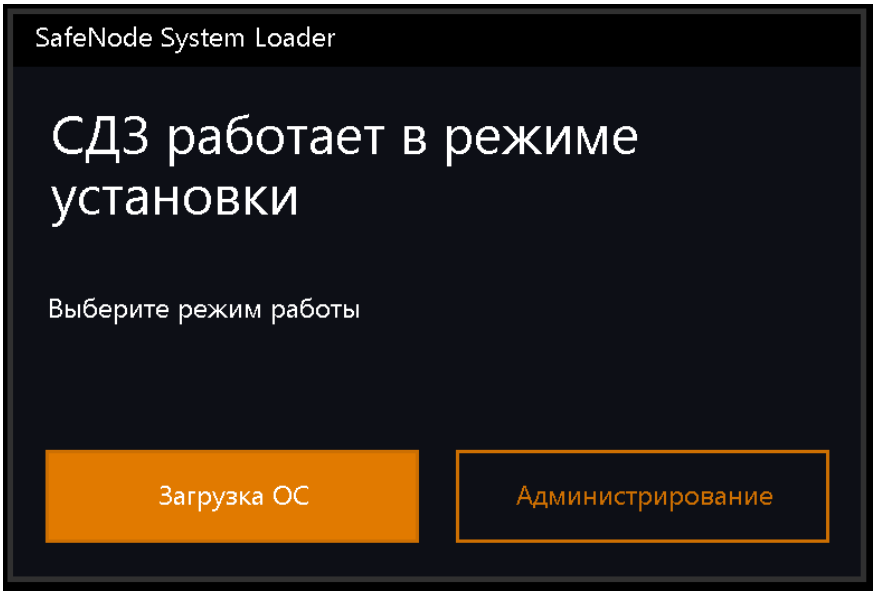


Рисунок 3.1 – Выбор дальнейшего режима работы

Если во время загрузки модулей изделия нажать клавишу ***«О»***, то появится окно для выбора варианта загружаемой консоли (рисунок 3.2):

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

Рисунок 3.2 – 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 ***«O»*** и выбрать другой вариант консоли.

3.1.2 Для начала работы с изделием АБ необходимо выбрать ***«Администрирование»*** (рисунок 3.1).

3.1.3 При первой аутентификации АБ в окне с приглашением к идентификации и аутентификации пользователя (рисунок 3.3) следует ввести имя пользователя ***«admin»*** и установленный по умолчанию пароль ***«12345678»***.

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

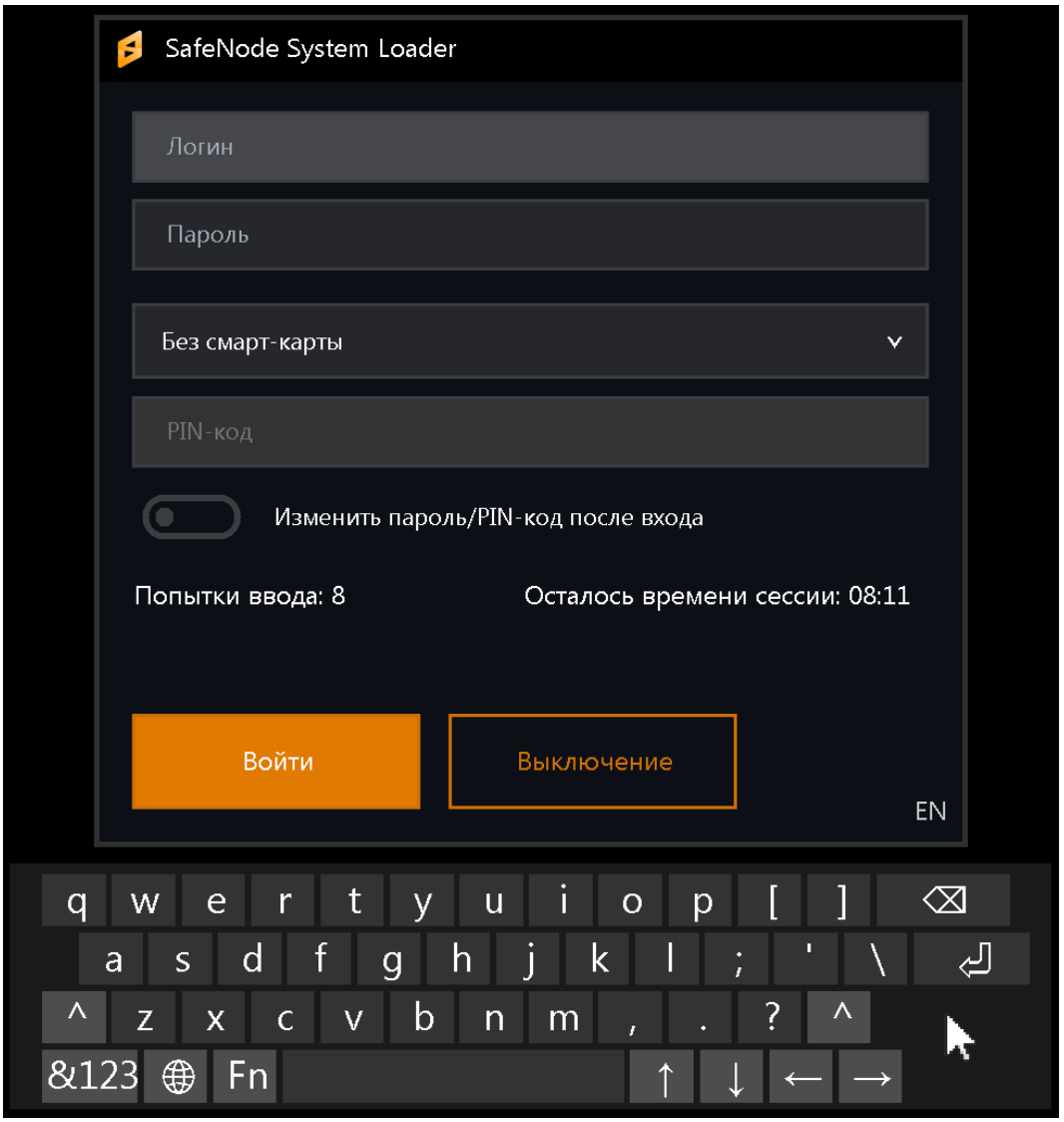


Рисунок 3.3 – Ввод предустановленных аутентификационных данных АБ

3.1.4 После успешной процедуры аутентификации и идентификации АБ появится диалоговое окно для смены аутентификационных данных АБ (рисунок 3.4).

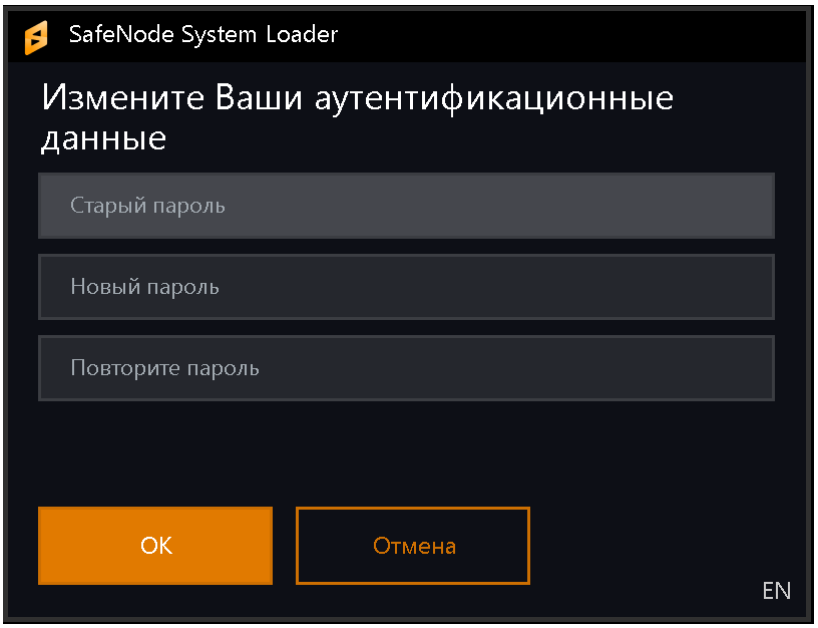


Рисунок 3.4 – Диалоговое окно для смены аутентификационных данных АБ

3.1.5 Для выполнения дальнейших действий необходимо сменить пароль АБ и нажать клавишу ***«ОК»***. В случае успешной смены аутентификационных данных появится информационное сообщение с предложением загрузить аварийную консоль (рисунок 3.5).

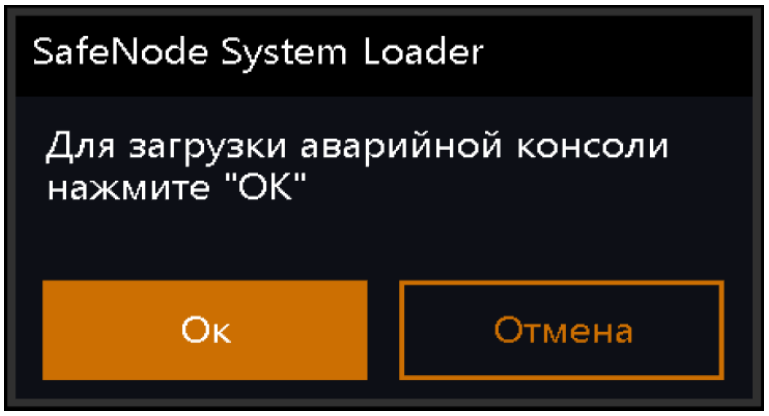


Рисунок 3.5 – Информационное сообщение

3.1.6 Для загрузки аварийной консоли необходимо нажать ***«ОК»***. Если загрузка данной консоли не выбрана, загрузится псевдографическая консоль СДЗ и дальнейшая работа будет осуществляться в ней.

Подробнее работа аварийной консоли рассмотрена в разделе 15 документа.

3.2 Псевдографическая консоль СДЗ. Аутентификация администратора безопасности

Для загрузки псевдографической консоли СДЗ во время загрузки изделия необходимо нажать ***«O»*** и выбрать опцию ***«Old style UI»*** (см. рис. 3.2).

В псевдографическом интерфейсе СДЗ не поддерживается аутентификация доменных пользователей.

3.2.1 Модуль псевдографического интерфейса СДЗ поддерживает автономную (локальную) модель управления работой изделия, до начала работы требуется предварительная установка изделия на ЭВМ.

3.2.2 После успешной установки изделия потребуется перезагрузка ЭВМ для вступления в силу изменений, внесенных ПО изделия. При каждом запуске осуществляется контрольная проверка цифровых подписей модулей изделия (рисунок 3.6).

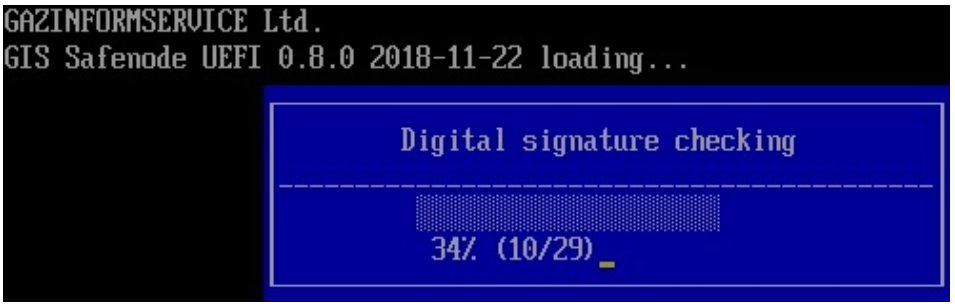


Рисунок 3.6 – Проверка цифровых подписей моделей изделия

3.2.3 При обнаружении несоответствия цифровых подписей загружаемых модулей изделия запуск ПО изделия не осуществляется и на экран ЭВМ выводится ошибка (рисунок 3.7).

Рисунок 3.7 – Ошибка при проверке цифровых подписей модулей

3.2.4 Для восстановления работоспособности изделия необходимо обратиться к документу «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 5. Руководство по восстановлению. ГМТК.468269.060РЭ5».

3.2.5 При успешной проверке цифровых подписей модулей изделия на экране ЭВМ появится окно псевдографического интерфейса изделия, в котором АБ сообщается о работе СДЗ в режиме установки и предлагается приступить к администрированию СДЗ или по умолчанию загрузить ОС (рисунок 3.8).

3.2.6 Для начала работы с изделием АБ необходимо выбрать ***«Администрирование СДЗ»*** и нажать клавишу ***< Enter >***.

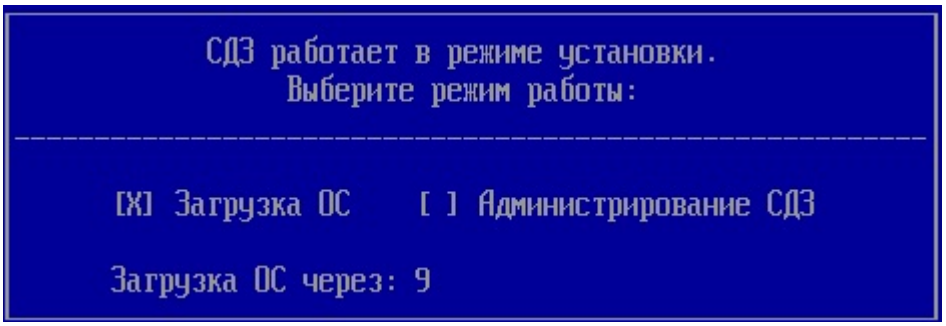


Рисунок 3.8 – Выбор дальнейшего режима работы

3.2.7 При первой аутентификации АБ в окне с приглашением к идентификации и аутентификации пользователя (рисунок 3.9) следует ввести имя пользователя ***«admin»*** и установленный по умолчанию пароль ***«12345678»***.

Рисунок 3.9 – Ввод предустановленных аутентификационных данных АБ

В целях обеспечения безопасности после первой аутентификации АБ предусмотрена принудительная смена пароля, используемого по умолчанию (рисунок 3.10).

При необходимости АБ следует назначить АНП и PIN-код к нему, предварительно выполнив необходимые настройки в параметрах политики аутентификации АБ и учетной записи, указанные в разделе 5.

Если был выбран параметр «Загрузка ОС» без проведения первичной настройки (рисунок 3.8), то при запуске консоли АБ Windows в ОС потребуется принудительная смена аутентификационных данных АБ после первой успешной идентификации и аутентификации АБ.

3.2.8 После успешной процедуры аутентификации и идентификации АБ появится диалоговое окно, сообщающее о необходимости смены аутентификационных данных АБ (рисунок 3.10).

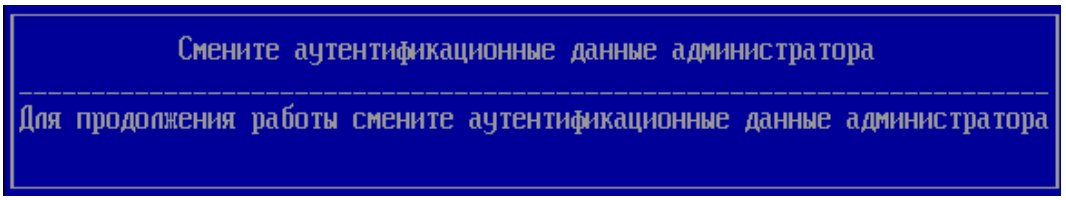


Рисунок 3.10 – Необходимость смены аутентификационных данных АБ

3.2.9 Для выполнения дальнейших действий необходимо нажать любую клавишу и в новом окне (рисунок 3.8) приступить к смене пароля АБ.

3.3 Смена аутентификационных данных АБ

Принудительная смена аутентификационных данных администратора при первом входе осуществляется в любой из консолей АБ.

3.3.1 После успешной аутентификации АБ по предустановленному паролю появится окно для принудительной смены его аутентификационных данных (рисунок 3.11).

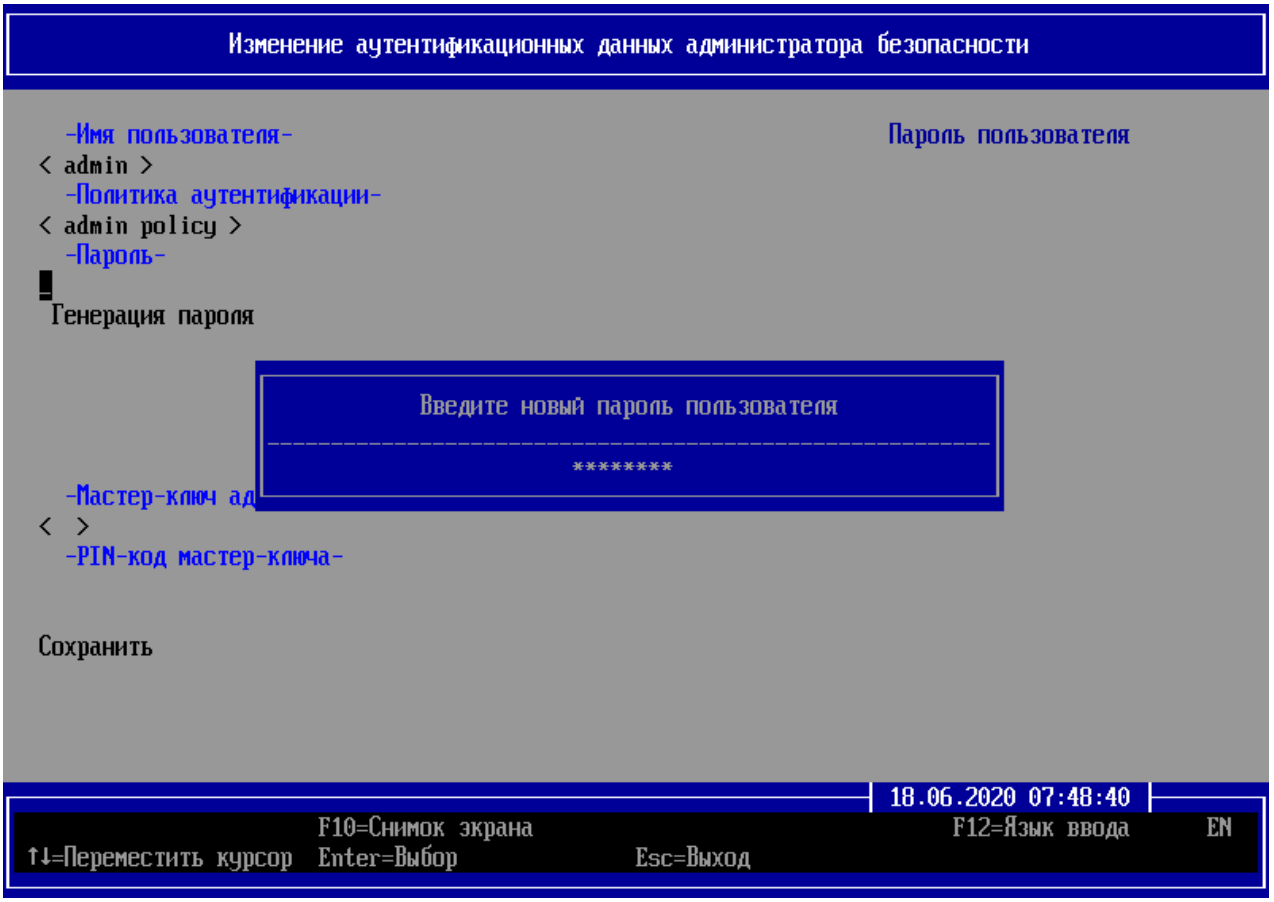
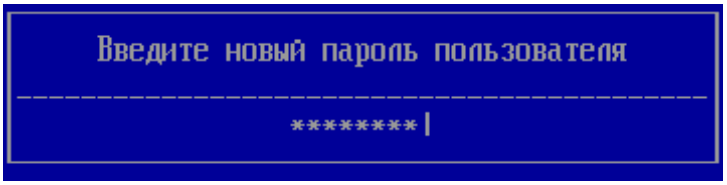
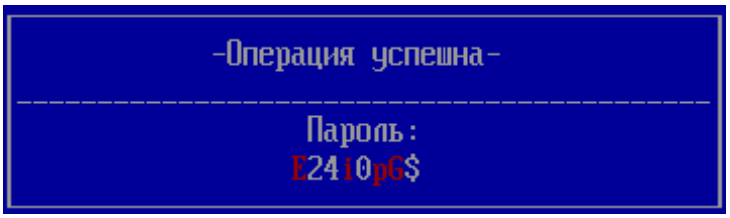
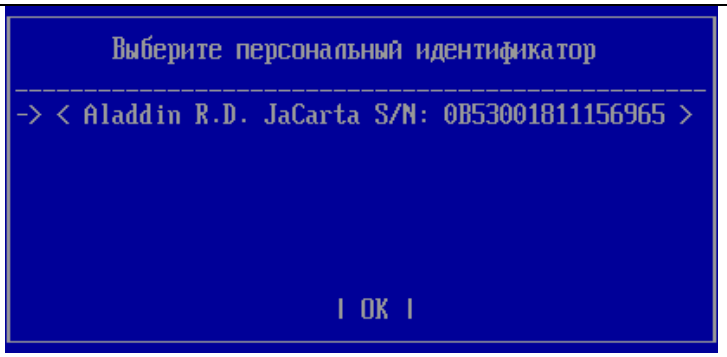
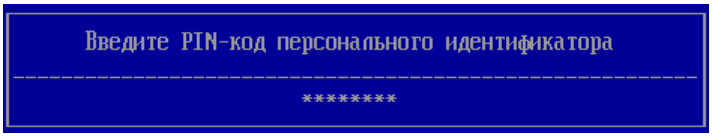


Рисунок 3.11 – Изменение аутентификационных данных АБ

3.3.2 В таблице 3.1 приведены названия полей рисунка 3.11 и их возможные значения.

Таблица 3.1 – Возможные значения полей при смене аутентификационных данных АБ

№	Наименование поля	Значения поля	Примечание
1	Имя пользователя	**admin**	Зарезервированное название учетной записи пользователя. Недоступно для изменения
2	Политика аутентификации	**admin policy**	Зарезервированное название политики аутентификации АБ. Недоступно для изменения
3	Пароль	Значение пароля	Поле предназначено для установки пароля АБ. Активируется при нажатии клавиши **< *Enter* >**  
4	Генерация пароля	Значение пароля	Поле предназначено для генерации пароля с помощью программного датчика случайных чисел (ДСЧ). Активируется при нажатии клавиши **< *Enter* >**. 
5	Мастер-ключ администратора	Присвоенный персональный мастер-ключ администратора	Поле предназначено для ввода мастер-ключа администратора. Активируется при нажатии клавиши **< *Enter* >**.

№	Наименование поля	Значения поля	Примечание
			
6	PIN-код мастер-ключа	Значение PIN-кода мастер-ключа	Поле предназначено для ввода PIN-кода мастер-ключа администратора. Активируется при нажатии клавиши **< *Enter* >**. 

3.3.3 Требования к использованию допустимых символов в пароле АБ приведены в таблице 5.2.

3.3.4 Генерация паролей осуществляется с помощью программного ДСЧ. Для генерации пароля необходимо перейти в строку ***«Генерация пароля»*** и нажать клавишу **< *Enter* >** (рисунок 3.11). На экран ЭВМ будет выведено сгенерированное значение случайного пароля (рисунок 3.12), при этом **красным цветом** отображаются буквы английского алфавита, **желтым цветом** – русского алфавита.

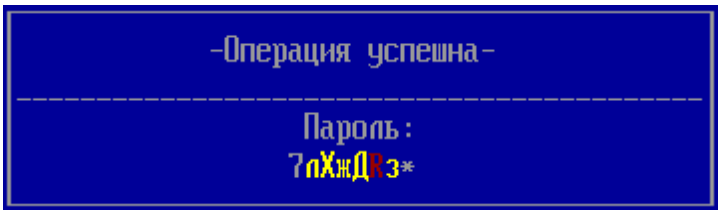


Рисунок 3.12 – Значение сгенерированного случайного пароля АБ

3.3.5 При необходимости в окне смены аутентификационных данных АБ (рисунок 3.11) возможно указать **мастер-ключ** администратора, используемый **для сброса аутентификационных данных АБ до значений по умолчанию в случае утраты** пароля, PIN-кода администратора АНП или потери АНП. Для установки мастер-ключа администратора необходимо выбрать требуемый мастер-ключ и ввести PIN-код к нему в соответствующих диалоговых окнах, приведенных в таблице 3.1.

4 Описание основного окна консоли АБ

4.1 Интерфейс основного окна консоли АБ

4.1.1 Консоль АБ имеет интерфейс, похожий на интерфейс базовой системы ввода-вывода UEFI BIOS. Изменение значений параметров в данном интерфейсе осуществляется только при помощи выбора или ввода их значений с клавиатуры (рисунок 4.1).

Рисунок 4.1 – Основное окно интерфейса консоли АБ

4.1.2 На рисунке 4.1 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.

4.1.3 Функциональная клавиша **< *F9* >** предназначена для переключения между расширенным и сокращенным режимом отображения элементов в основном меню.

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

4.1.5 Переключение языков ввода (английский, русский) осуществляется при помощи функциональной клавиши **< *F12* >**. В правом нижнем углу интерфейса отображается текущий язык ввода (рисунок 4.1).

4.1.6 Для выхода из основного окна консоли АБ (рисунок 4.1) к основному окну идентификации и аутентификации пользователей (рисунок 12.1) необходимо нажать клавишу **< *Esc* >**.

4.2 Режимы функционирования основного окна консоли АБ

4.2.1 Основное окно консоли АБ имеет два режима отображения элементов в основном меню для удобства пользования: сокращенный и расширенный режим.

4.2.2 По умолчанию доступен сокращенный режим отображения элементов в основном меню (рисунок 4.1).

4.2.3 Переключение между сокращенным и расширенным режимом отображения основного меню осуществляется при помощи функциональной клавиши **< *F9* >**.

4.2.4 Расширенный режим отображения основного меню консоли АБ изображен на рисунке 4.2.

Рисунок 4.2 – Расширенный режим отображения меню консоли АБ

4.2.5 Расширенный режим отображения основного меню консоли АБ используется для первоначальной и последующей настройки параметров изделия. АБ может настроить отображение элементов основного меню консоли АБ при расширенном режиме функционирования в подразделе **«Основные настройки»** (подраздел 10.5).

4.2.6 Сокращенный режим отображения основного меню используется в процессе работы с изделием для:

- контроля за ошибками в политиках КЦ объектов и загрузки ОС;
- проведения диагностики изделия;
- просмотра журнала аудита;
- разблокировки учетных записей пользователей.

4.3 Основные параметры консоли АБ

4.3.1 Основная консоль АБ выполнена в виде единого псевдографического интерфейса (рисунок 4.1) и доступна АБ только после успешного прохождения им процедуры аутентификации и идентификации.

4.3.2 Основными функциями консоли АБ являются:

- управление учетными записями пользователей: создание, редактирование, удаление, блокировка, разблокировка (раздел 9);
- управление политиками идентификации и аутентификации пользователей и АБ: создание, их редактирование или удаление (раздел 8);
- управление политиками КЦ объектов и загрузки ОС: создание, их редактирование и удаление (раздел 6);
- применение шаблонов политик безопасности (раздел 6.9);
- настройка политик КЦ объектов и загрузки ОС (раздел 7):
  - файлов;
  - журналов транзакций файловых систем;
  - объектов реестра ОС для ОС семейства Windows;
  - параметров среды UEFI;
  - загрузочных секторов диска;
  - устройств ЭВМ;
- управление загружаемыми ОС;
- устранение нарушений КЦ объектов (подраздел 6.8);
- управление общими настройками аутентификации и идентификации пользователей и КЦ объектов (подраздел 10.1);
- восстановление заводских настроек изделия (подраздел 10.7);
- обновление ПО изделия (подраздел 10.8);
- проведение диагностики изделия (подраздел 10.12);
- просмотр информации о продукте (подраздел 10.13);
- работа с журналами аудита и применения шаблонов: просмотр сообщений о действиях АБ и пользователей, экспорт журнала на внешнее устройство хранения данных, очистка журнала (раздел 11).

4.3.3 В таблице 4.1 приведено описание разделов консоли АБ при расширенном режиме функционирования (рисунок 4.2).

Таблица 4.1 – Перечень разделов, подразделов консоли АБ расширенного режима функционирования и их назначение

Раздел	Подраздел	Назначение
Учетные записи и политики безопасности	Учетные записи пользователей	Управление учетными записями пользователей: добавление, редактирование, удаление, блокировка, разблокировка
	Политики аутентификации пользователей	Управление политиками аутентификации пользователей: добавление, редактирование, удаление
	Политики контроля целостности объектов и загрузки ОС	Управление политиками КЦ объектов и загрузки ОС: добавление, редактирование, удаление
	Шаблоны политик	Использование созданных шаблонов с настроенными параметрами политик аутентификации пользователей и КЦ объектов и загрузки ОС
Контроль целостности объектов	Файлы	Настройка механизма КЦ соответствующих компонентов аппаратной и программной конфигурации ЭВМ
	Журналы транзакций файловых систем	
	Реестр ОС Windows	
	Параметры среды UEFI	
	Загрузочные сектора	
	Устройства	
Управление загрузкой ОС	Контроль загрузки ОС	Настройка ОС для доверенной загрузки пользователями
Общие параметры	Основные настройки	Настройка общих параметров для аутентификации и идентификации пользователей и КЦ объектов, восстановление заводских настроек изделия и иные настройки
	Диагностика	Запуск диагностики изделия и просмотр ее результатов
	Информация о продукте	Просмотр информации о продукте
Регистрация событий	Журнал аудита	Просмотр основного журнала действий АБ и пользователей, журнала применения шаблонов, экспорт журналов на внешнее устройство хранения данных, очистка журналов

5 Конфигурирование параметров учетной записи АБ

5.1 Управление параметрами политики аутентификации АБ

5.1.1 АБ по умолчанию назначена собственная зарезервированная политика аутентификации **admin policy**.

5.1.2 Для редактирования политики аутентификации АБ необходимо выбрать в главном окне расширенного меню (рисунок 4.2) подраздел ***«Политики аутентификации пользователей»*** и в появившемся диалоговом окне перейти в строку ***«Редактирование»***, нажать клавишу **< *Enter* >** (рисунок 5.1).

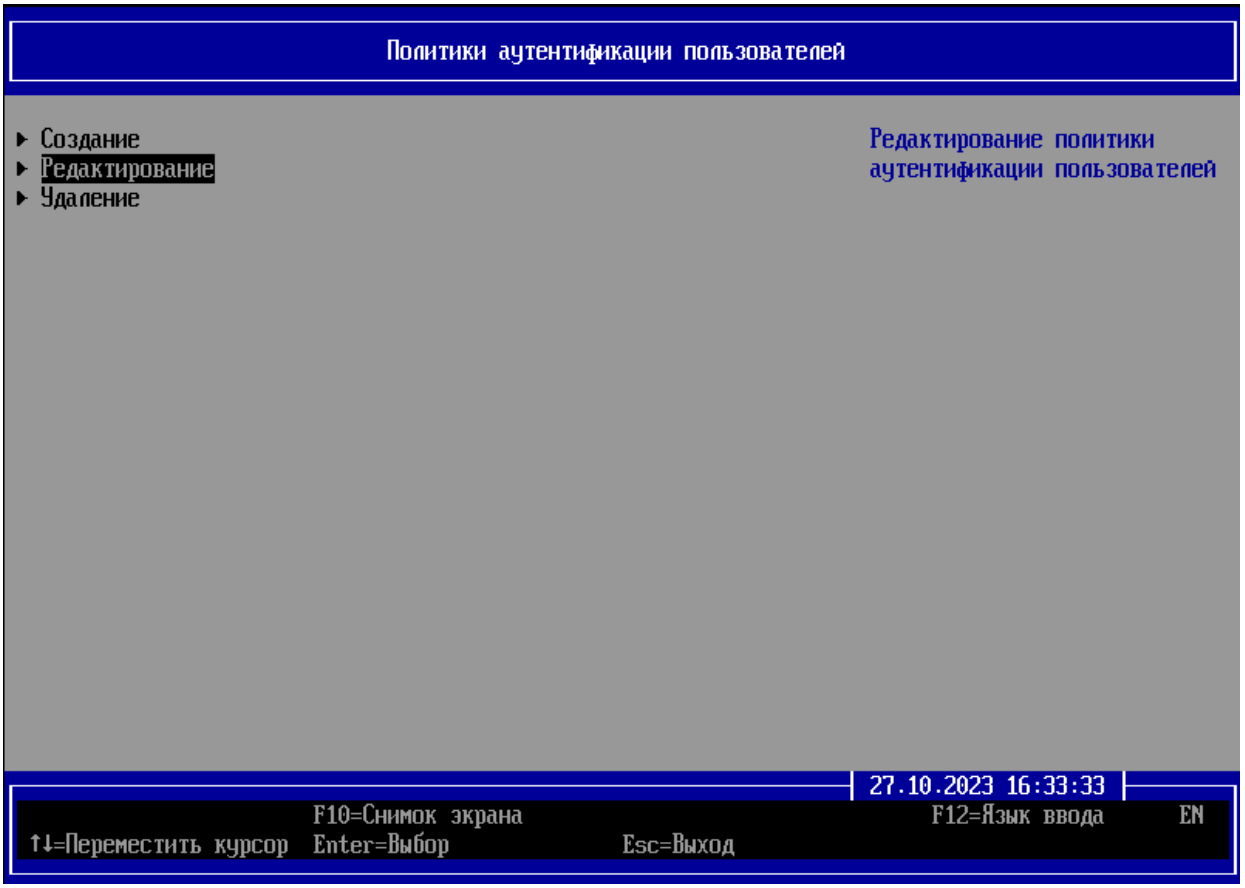


Рисунок 5.1 – Редактирование политики аутентификации АБ

5.1.3 В новом диалоговом окне ***«Редактирование политики аутентификации пользователей»*** (рисунок 5.2) необходимо выбрать имя редактируемой политики аутентификации в поле ***«Имя»*** и нажать кнопку **| *ОК* |** (рисунок 5.3).

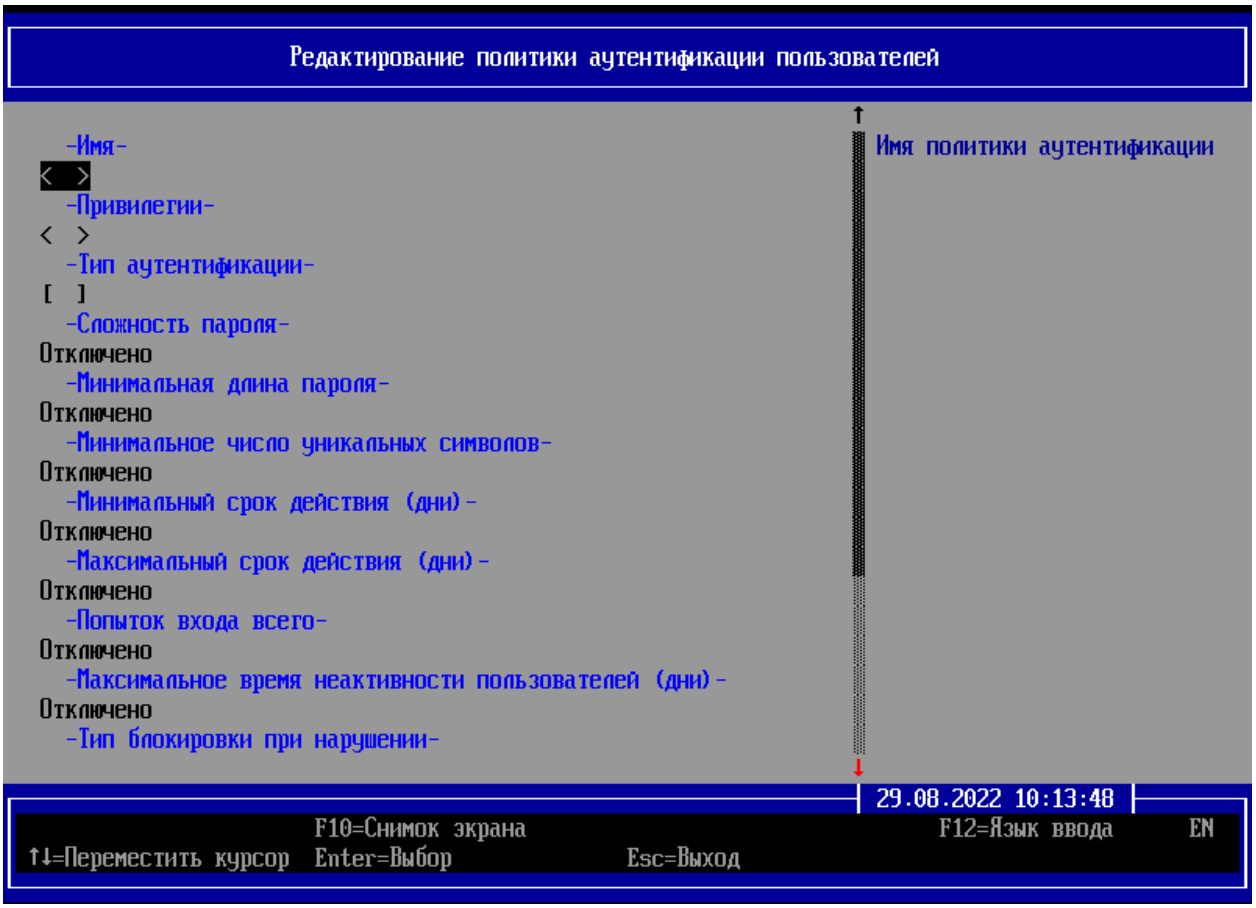


Рисунок 5.2 – Редактирование политики аутентификации пользователей

Рисунок 5.3 – Выбор политики аутентификации для редактирования

5.1.4 В таблице 5.1 приведены доступные для редактирования параметры политики аутентификации АБ, их возможные принимаемые значения и примечания к ним (рисунок 5.4).

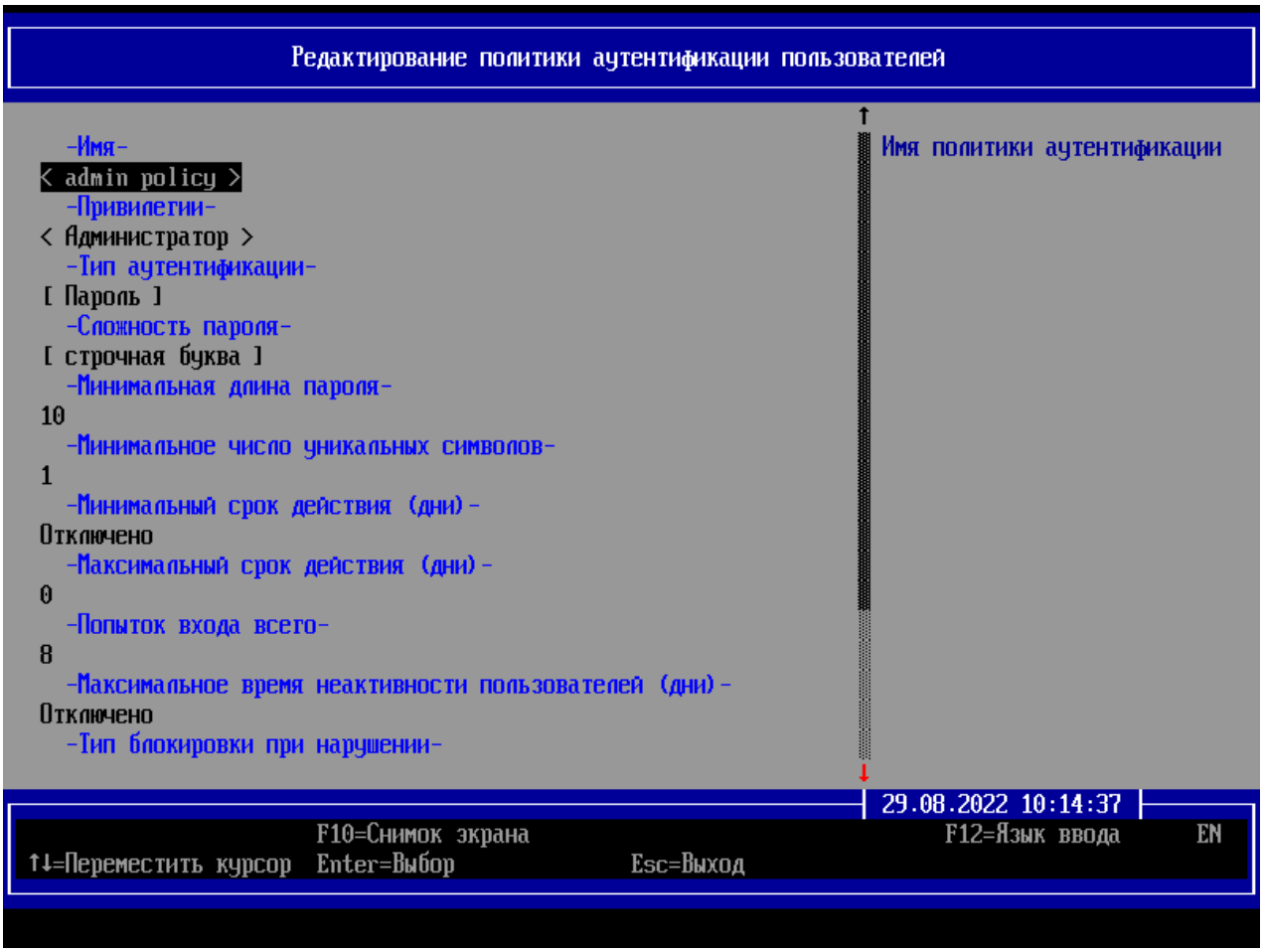


Рисунок 5.4 – Редактируемые поля политики аутентификации АБ

Таблица 5.1 – Возможные значения полей при изменении политики аутентификации АБ

№	Наименование поля	Возможные значения поля [по умолчанию]	Минимальное … максимальное значения	Примечание
1	Имя	**admin policy**		Зарезервированное название политики аутентификации АБ. Недоступно для изменения
2	Привилегии	Администратор		
3	Тип аутентификации	[Пароль] Персональный идентификатор Пароль и персональный идентификатор		
4	Сложность пароля	[строчная буква] заглавная буква		Поле предназначено для установки сложности пароля.

№	Наименование поля	Возможные значения поля [по умолчанию]	Минимальное … максимальное значения	Примечание
		цифра специальный символ		Активируется при нажатии клавиши ***< Enter >***
5	Минимальная длина пароля	10	8…32	
6	Минимальное число уникальных символов	1	1…8	Минимальное число уникальных символов в пароле
7	Минимальный срок действия (дни)	–	–	Недоступно для изменения
8	Максимальный срок действия (дни)	0	1…45	Для политики аутентификации АБ значение «0» означает бесконечное время действия политики
9	Попыток входа всего	8	1…8	
10	Максимальное время неактивности пользователя (дни)	–	–	Недоступно для изменения
11	Тип блокировки при нарушении	Запись в журнал	–	Недоступно для изменения
12	Блокирование общеизвестных паролей	[Отключено] Включено		Блокирование общеизвестных паролей

Параметры политики аутентификации АБ ***«Сложность пароля», «Минимальная длина пароля», «Минимальное число уникальных символов», «Максимальный срок действия (дни)», «Попыток входа всего»*** возможно полностью отключить. При этом в политике аутентификации АБ снимаются все ограничения, заданные в данных параметрах.

5.1.5 Сложность пароля или PIN-кода АНП АБ и пользователей определяется путем использования в нем сочетания заглавных букв, строчных букв, цифр и специальных символов из определенного разработчиком алфавита пароля, указанного в таблице 5.2. Ограничения по применению символов в именах учетных записей пользователей и паролях приведены в таблице 5.3.

Таблица 5.2 – Алфавит пароля и PIN-кодов АБ и 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

№	Наименование	Допустимые символы	Количество символов, шт.
4	Специальные символы	! @ # $ % ^ & * ( ) _	11
Итого:			**139**

5.1.6 Для сохранения изменений редактируемой политики аутентификации АБ необходимо перейти в строку ***«Сохранить»*** и нажать клавишу **< *Enter* >**. При этом в новом диалоговом окне будет выведено сообщение об успешном редактировании политики аутентификации АБ (рисунок 5.5).

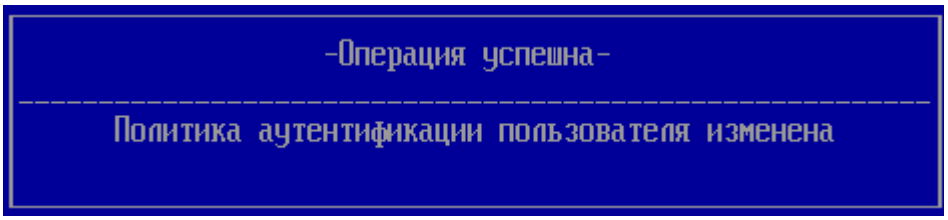


Рисунок 5.5 – Успешное изменение политики аутентификации АБ

5.2 Управление параметрами учетной записи АБ

5.2.1 Управление параметрами учетной записи АБ осуществляется в подразделе ***«Учетные записи пользователей»*** основного окна консоли АБ.

5.2.2 Для редактирования учетной записи АБ необходимо выбрать в главном окне (рисунок 4.1) подраздел ***«Учетные записи пользователей»***. В появившемся диалоговом окне перейти в строку ***«Редактирование»*** и нажать клавишу **< *Enter* >** (рисунок 5.6).

Рисунок 5.6 – Редактирование учетной записи АБ

5.2.3 В новом диалоговом окне ***«Редактирование учетной записи пользователя»*** необходимо выбрать имя редактируемой учетной записи АБ в поле ***«Имя пользователя»*** и нажать кнопку **| *ОК* |** (рисунок 5.7).

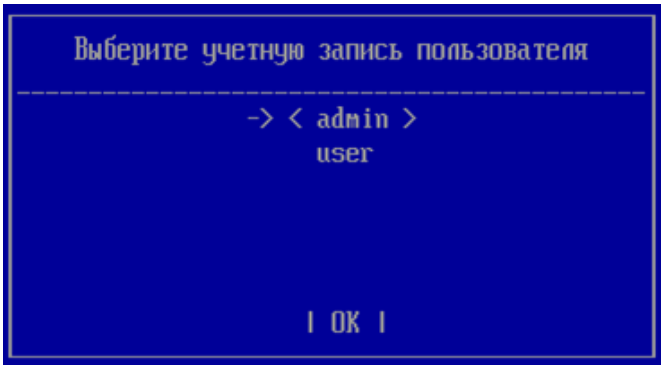


Рисунок 5.7 – Выбор учетной записи АБ для редактирования

5.2.4 Доступные для редактирования параметры учетной записи АБ (рисунок 5.8) и их значения приведены в таблице 5.3.

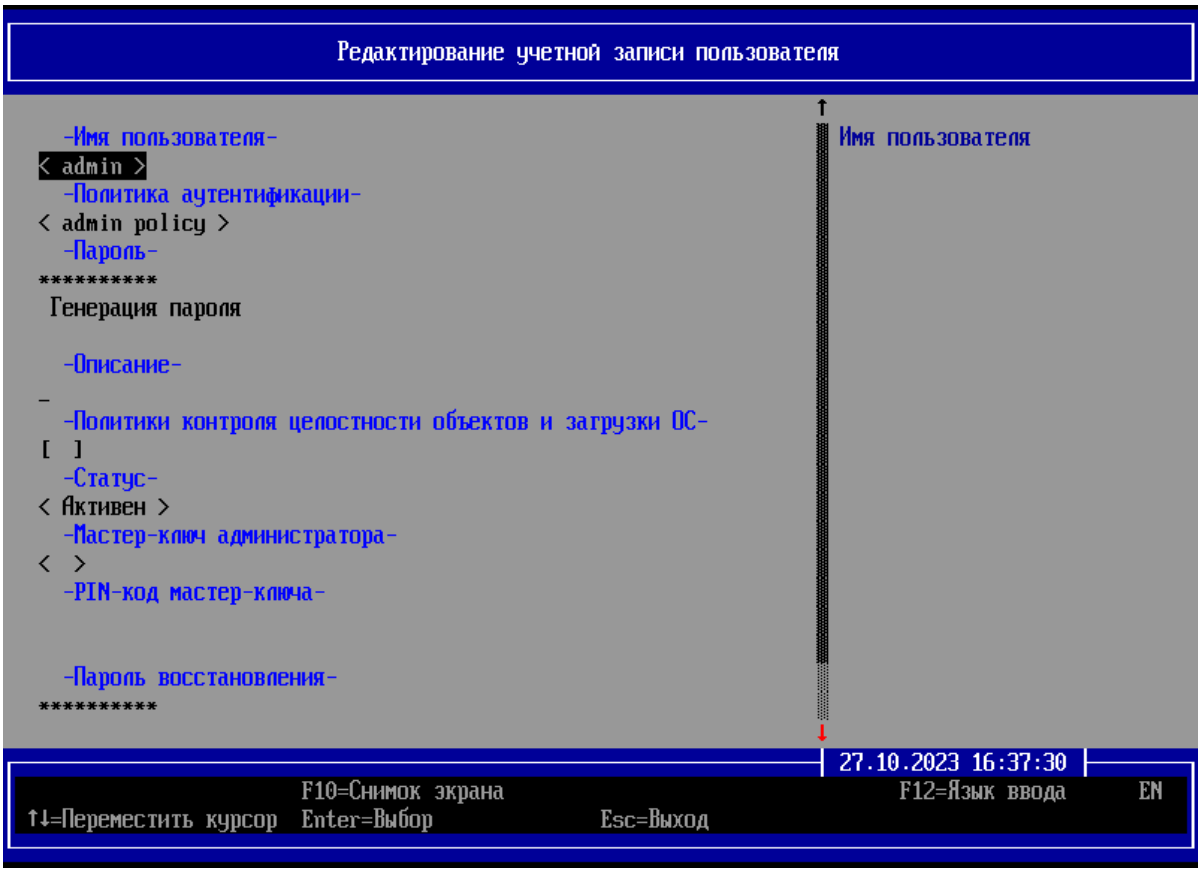
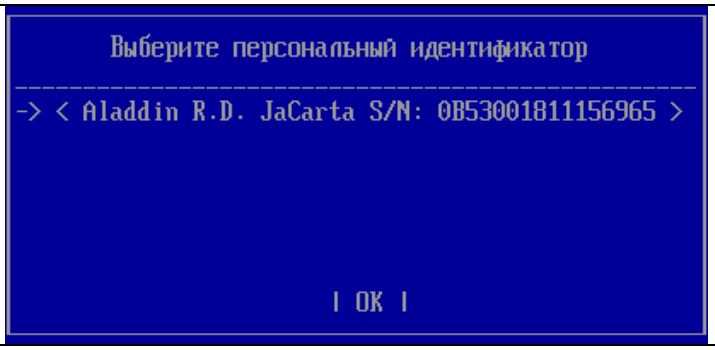
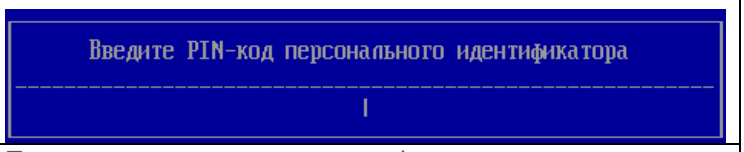
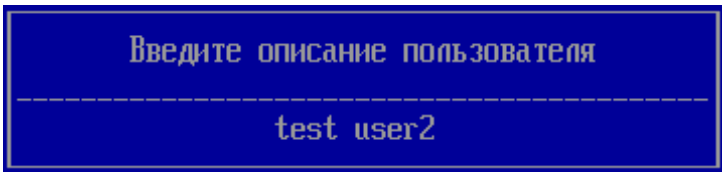


Рисунок 5.8 – Редактирование учетной записи АБ

Таблица 5.3 – Возможные значения полей при редактировании учетной записи АБ

№	Наименование поля	Значения поля	Примечание
1	Имя пользователя	**admin**	Зарезервированное название учетной записи пользователя. Недоступно для изменения
2	Политика аутентификации	**admin policy**	Зарезервированное название политики аутентификации АБ. Недоступно для изменения
3	Пароль	Значение пароля	Поле предназначено для установки пароля АБ. **Допускается использование символов из таблицы 5.2.** Активируется при нажатии клавиши **< *Enter* >**
4	Генерация пароля	Значение пароля	Поле предназначено для генерации пароля с помощью программного ДСЧ. Активируется при нажатии клавиши **< *Enter* >**.
5	Персональный идентификатор	Присвоенный персональный идентификатор	Поле предназначено для выбора и установки персонального идентификатора. Активируется при нажатии клавиши **< *Enter* >**.

№	Наименование поля	Значения поля	Примечание
			
6	PIN-код	Значение PIN-кода	Поле предназначено для ввода PIN-кода персонального идентификатора. **Допускается использование символов из таблицы 5.2.** Активируется при нажатии клавиши **< *Enter* >**. 
7	Описание	Произвольная текстовая строка	Поле предназначено для формирования описания учетной записи АБ Максимальная длина поля – 48 символов. Активируется при нажатии клавиши **< *Enter* >**. 
8	Политики контроля целостности объектов и загрузки ОС	Введенное значение	Указание названия политики КЦ и загрузки ОС, по правилам которой будет обрабатываться учетная запись АБ
9	Статус	Активен	Недоступно для изменения
10	Мастер-ключ администратора	Присвоенный персональный мастер-ключ администратора	Поле предназначено для ввода мастер-ключа администратора. Активируется при нажатии клавиши **< *Enter* >**.
11	PIN-код мастер-ключа	Значение PIN-кода мастер-ключа	Поле предназначено для ввода PIN-кода мастер-ключа администратора. Активируется при нажатии клавиши **< *Enter* >**.
12	Пароль восстановления	Значение пароля восстановления	Поле предназначено для смены пароля восстановления. Активируется при нажатии клавиши **< *Enter* >.**

5.2.5 Для сохранения изменений редактируемой учетной записи АБ необходимо перейти в строку ***«Сохранить»*** (рисунок 5.8) и нажать клавишу **< *Enter* >**. При этом в новом диалоговом окне будет выведено сообщение об успешном редактировании учетной записи пользователя (рисунок 5.9).

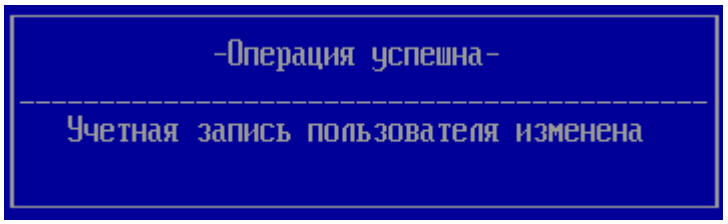


Рисунок 5.9 – Успешное редактирование учетной записи АБ

5.2.6 Перечень ошибок, возникающих при конфигурировании параметров политики аутентификации АБ и его учетной записи, а также действия по их устранению указаны в разделе 15.

5.3 Назначение АНП администратору безопасности

5.3.1 АБ может назначить АНП и использовать его в качестве средства аутентификации. При этом в параметре политики аутентификации ***«Тип аутентификации»*** должно быть установлено значение ***«Персональный идентификатор»*** (рисунок 5.4).

5.3.2 Для установки АНП в качестве средства аутентификации АБ необходимо:

- подключить АНП АБ к ЭВМ;
- перейти курсором в строку ***«Персональный идентификатор»*** (рисунок 5.10), нажать клавишу **< *Enter* >** и в новом диалоговом окне (рисунок 5.11) выбрать требуемый персональный идентификатор из списка поддерживаемых в изделии нажатием клавиши **< *Enter* >**;
- выбранный персональный идентификатор будет выделен < угловыми скобками >;
- нажать клавишу | ***OK*** | (рисунок 5.11), перейти курсором в поле ***«PIN-код»*** (рисунок 5.10) и нажать клавишу **< *Enter* >**;
- ввести PIN-код персонального идентификатора (рисунок 5.12).

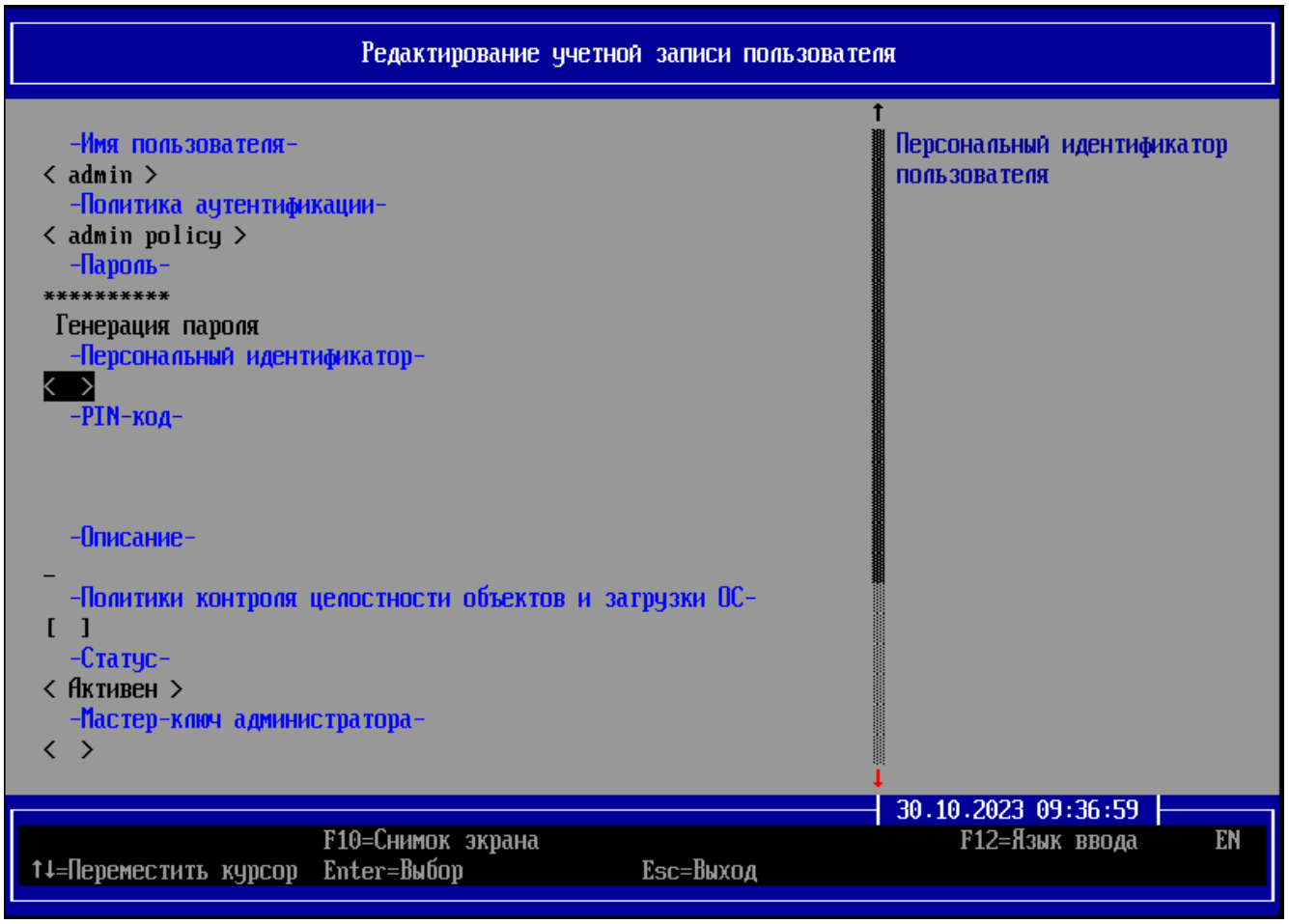


Рисунок 5.10 – Назначение персонального идентификатора АБ

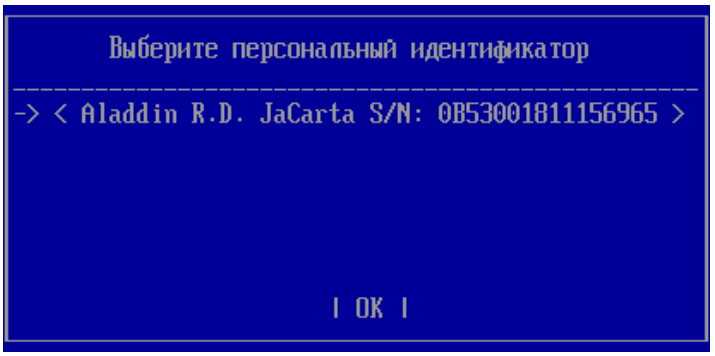


Рисунок 5.11 – Выбор персонального идентификатора АБ

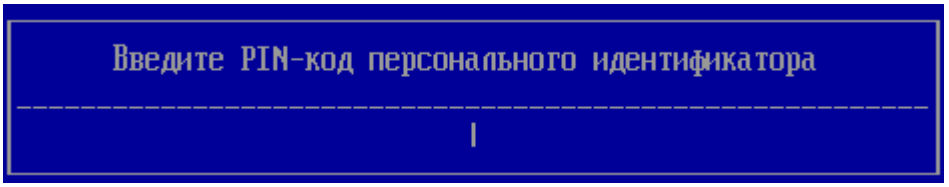


Рисунок 5.12 – Ввод PIN-кода персонального идентификатора АБ

5.3.3 Для поддерживаемых в изделии АНП PIN-код пользователя задается с помощью специального ПО (PKI Client), поставляемого производителем совместно с идентификатором. При этом для смены PIN-кода пользователя из специального ПО необходимо знать PIN-код администратора АНП.

Для назначения в качестве АНП Guardant ID необходимо предварительно произвести его инициализацию с помощью специализированной утилиты[2].

В процессе инициализации все данные по работе с другими СЗИ будут уничтожены, АНП будет полностью сконфигурирован для работы с СДЗ «SafeNode System Loader»

5.3.4 В таблице 5.4 приведен список PIN-кодов администраторов АНП, установленных разработчиками (производителями) по умолчанию.

Таблица 5.4 – Список используемых по умолчанию паролей администраторов АНП для разных типов АНП

№ п/п	Наименование АНП	PIN-код пользователя АНП по умолчанию	PIN-код администратора АНП по умолчанию
1	eToken PRO (Java) 72K, SafeNet eToken 5100/5110/5200/5205	1234567890	Не задан
2	JaCarta PKI	11111111	00000000
3	JaCarta ГОСТ	Не задан	1234567890
4	Рутокен ЭЦП 3.0/ЭЦП 2.0/ЭЦП/2151/Lite	12345678	87654321
5	Guardant ID[3]	12345678	12345678

5.3.5 Для корректного функционирования АНП с изделием необходима установка соответствующих драйверов в ОС Windows, указанных в таблице 5.5. Установка специализированного ПО для АНП производится согласно документации разработчика (производителя).

Таблица 5.5 – Перечень PKI клиентов

№ п/п	Наименование PKI Клиента	Версия	Ссылка
1	Драйверы Рутокен	4.7.0.0	https://www.rutoken.ru/support/download/drivers-for-windows/

[2] В комплект поставки не входит, предоставляется производителем СДЗ «SafeNode System Loader» по запросу.
[3] Установка значений по умолчанию для данного АНП осуществляется при инициализации с помощью специализированной утилиты.

№ п/п	Наименование PKI Клиента	Версия	Ссылка
2	Единый Клиент Jacarta	2.12.0 Сборка 2008(бета)	https://www.aladdin-rd.ru/support/downloads/jacarta
3	SafeNet Authentication Client	10.4.26.0	ПО доступно после регистрации и запроса у разработчика. https://safenet.gemalto.com/multi-factor-authentication/security-applications/authentication-client-token-management/

5.3.6 Проверка PIN-кода при использовании АНП осуществляется внутренними механизмами защиты этих идентификаторов (собственным программным кодом).

В случае неверно указанного PIN-кода на экран ЭВМ будет выведено сообщение ***«Неверный PIN-код!»*** (рисунок 5.13).

Рисунок 5.13 – Ошибка при вводе неверного PIN-кода персонального идентификатора

Допускается использование одного АНП для нескольких пользователей.

Но в качестве АНП для входа АБ (пользователя) не может быть назначен носитель, который используется в качестве мастер-ключа АБ для сброса данных.

5.4 Использование мастер-ключа администратора безопасности

5.4.1 Мастер-ключ используется для сброса аутентификационных данных АБ до значений по умолчанию в случае утраты пароля АБ, PIN-кода администратора АНП или потери АНП. При исчерпании количества попыток аутентификации и идентификации АБ на экран ЭВМ будет выведено сообщение о блокировке с предложением восстановить доступ с помощью мастер-ключа (рисунок 5.14).

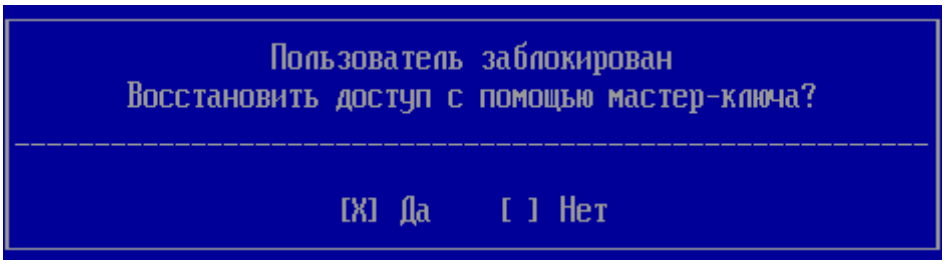


Рисунок 5.14 – Подтверждение восстановления доступа АБ с помощью мастер-ключа

5.4.2 Для восстановления доступа с помощью мастер-ключа необходимо:

- подключить мастер-ключ АБ к ЭВМ;
- в появившемся окне «***Сброс аутентификационных данных администратора***» (рисунок 5.15) перейти курсором в строку ***«Мастер-ключ администратора»***, нажать клавишу **< *Enter* >** и в новом диалоговом окне (рисунок 5.16) выбрать требуемый мастер-ключ нажатием клавиши **< *Enter* >**;
- выбранный мастер-ключ будет выделен < угловыми скобками >;
- нажать клавишу | ***ОК*** | (рисунок 5.16), перейти курсором в поле ***«PIN-код мастер-ключа»*** (рисунок 5.15) и нажать клавишу **< *Enter* >**;
- ввести PIN-код мастер-ключа (рисунок 5.17);
- перейти курсором в строку «***Сбросить***» и нажать клавишу **< *Enter* >** (рисунок 5.15).

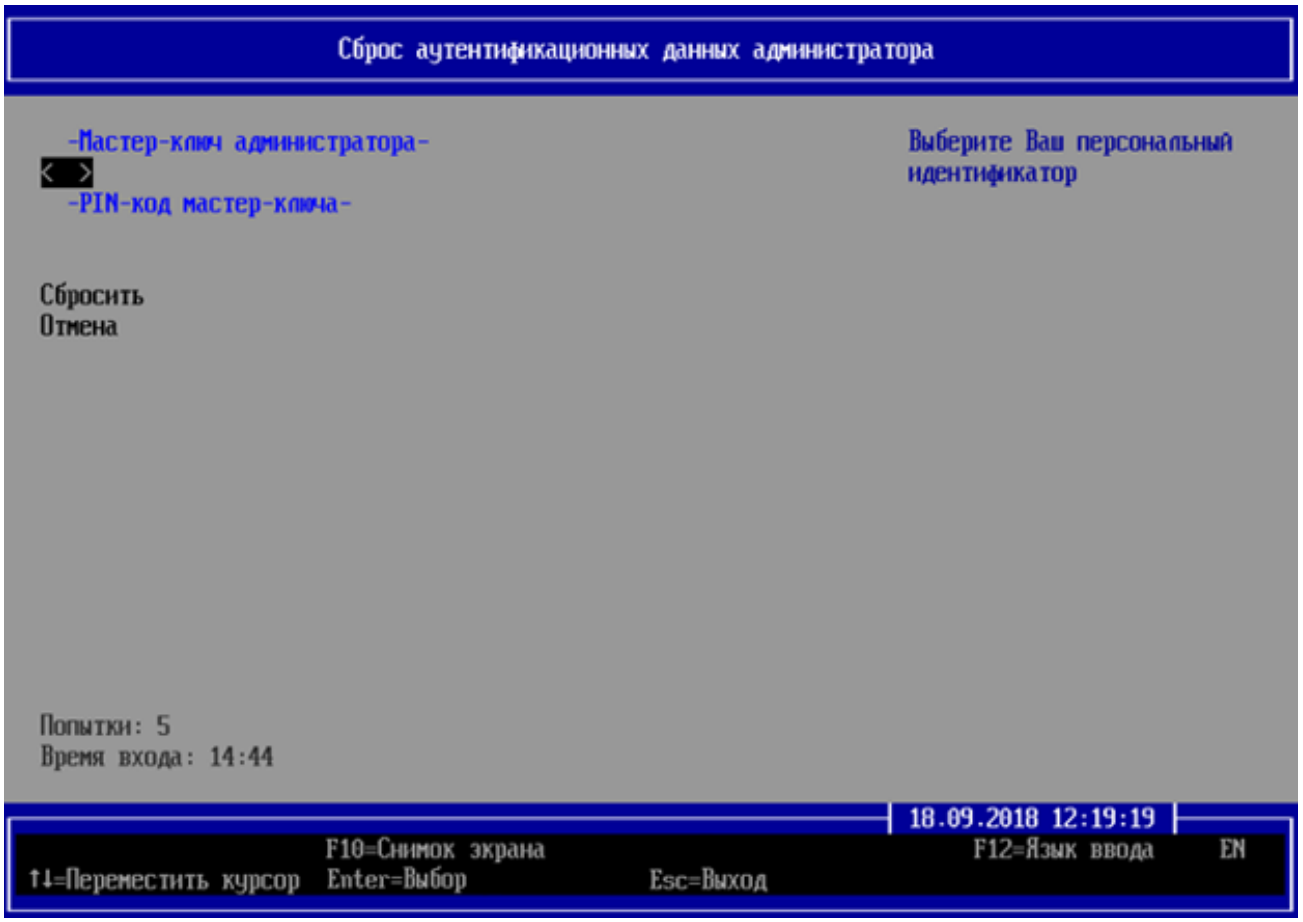


Рисунок 5.15 – Сброс аутентификационных данных

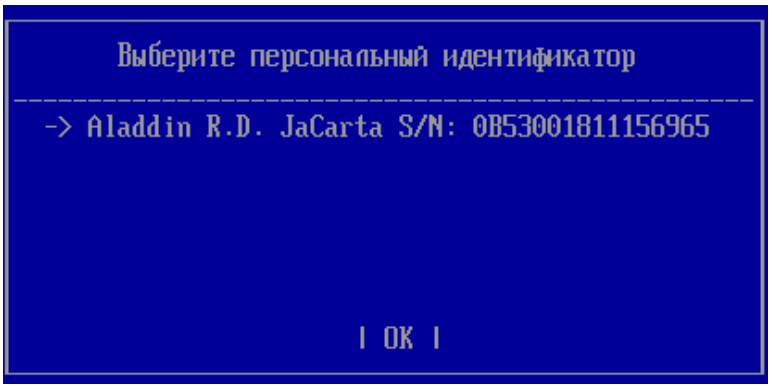


Рисунок 5.16 – Выбор мастер-ключа АБ

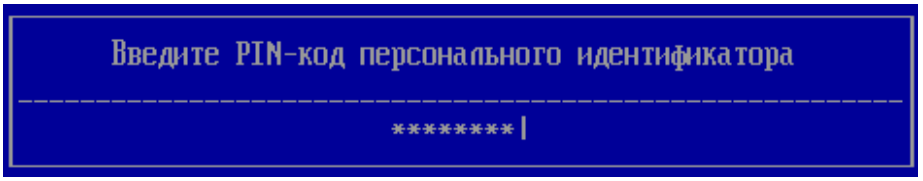


Рисунок 5.17 – Ввод PIN-кода мастер-ключа АБ

5.4.3 При успешном сбросе аутентификационных данных АБ будет выведено сообщение (рисунок 5.18), содержащее новый пароль АБ, установленный по умолчанию.

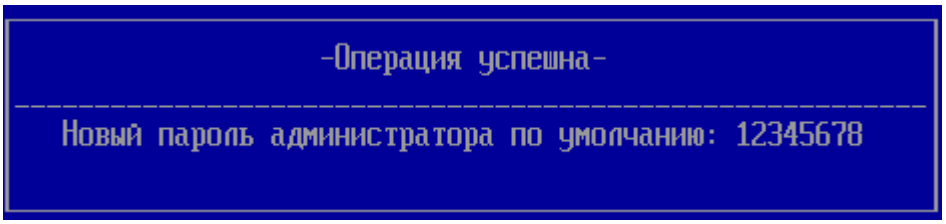


Рисунок 5.18 – Успешный сброс аутентификационных данных АБ

Мастер-ключ и персональный носитель, назначенный в качестве АНП для прохождения аутентификации АБ (пользователя), не могут совпадать!

В случае, если в качестве мастер-ключа выбран носитель, который назначен как АНП для входа АБ (пользователя), будет выведено сообщение с ошибкой (рисунок 5.19).

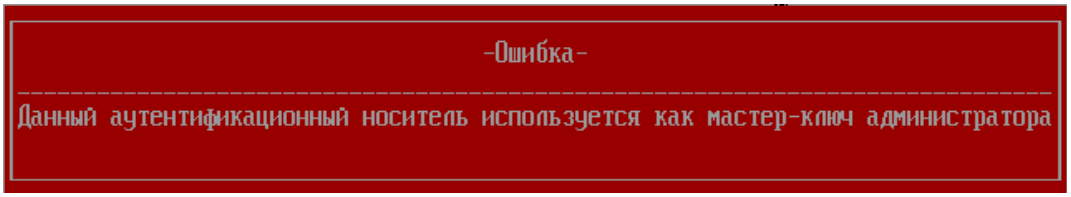


Рисунок 5.19 – Ошибка выбора носителя для назначения в качестве мастер-ключа

5.5 Смена пароля восстановления

5.5.1 При первом выходе из мягкого режима необходимо сменить пароль восстановления, который будет использоваться для безопасного восстановления ПО в случае сбоев и отказов.

В целях обеспечения безопасности при первом выходе из мягкого режима осуществляется принудительная смена пароля восстановления, используемого по умолчанию.

По умолчанию паролю восстановления присвоено значение ***12345678***.

Подробнее процесс безопасного восстановления «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 5. Руководство по восстановлению. ГМТК.468269.060РЭ5»

5.5.2 Для смены пароля восстановления необходимо:

- перейти в раздел ***Учетные записи → Учетные записи пользователей → Редактирование***;
- выбрать пользователя ***admin***;
- перейти в поле «Пароль восстановления» и нажать клавишу **< *Enter* >** (рисунок 5.20);

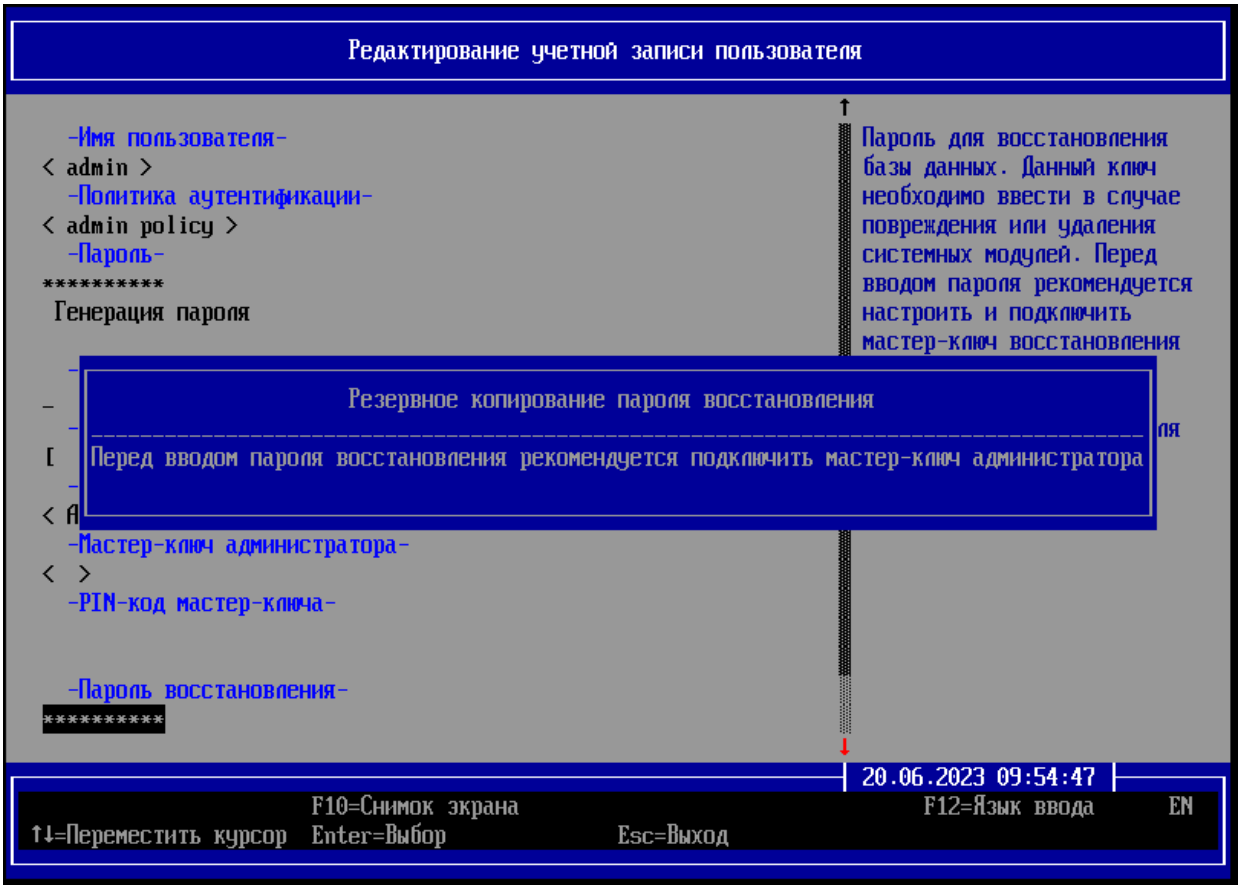


Рисунок 5.20 – Смена пароля восстановления

- появится информационное сообщение с предложением подключить мастер-ключ АБ.

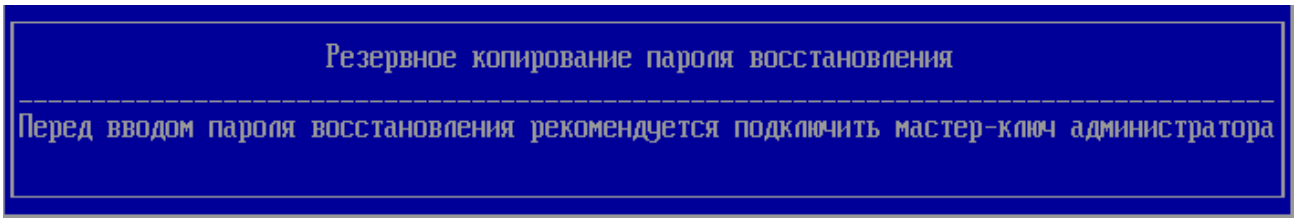


Рисунок 5.21 – Информационное сообщение

Рекомендуется для резервного копирования значения пароля восстановления сначала подключить мастер-ключ АБ.

В качестве идентификатора для сохранения пароля восстановления поддерживается только назначенный мастер-ключ АБ.

5.5.3 Для смены значения пароля восстановления без резервного копирования на мастер ключ администратора необходимо в диалоговом окне (рисунок 5.20) нажать **< *Enter*>**. Появится окно для ввода нового значения пароля восстановления (рисунок 5.22).

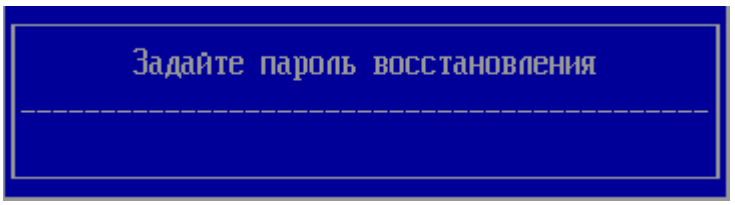


Рисунок 5.22 – Ввод пароля восстановления

Требования к паролю восстановления:

- минимальная длина пароля должна составлять не менее 4 символов;
- максимальная длина пароля – 32 символа;
- заглавные/строчные буквы латинского алфавита A…Z\a…z;
- цифры 0…9.

5.5.4 Следует указать новое значение пароля восстановления и нажать **< *Enter*>**, в следующем окне повторить ввод пароля (рисунок 5.23).

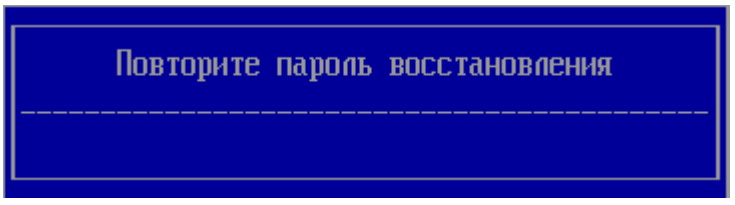


Рисунок 5.23 – Повторение ввода пароля

5.5.5 При успешной установке ключа восстановления будет выведено сообщение (рисунок 5.24).

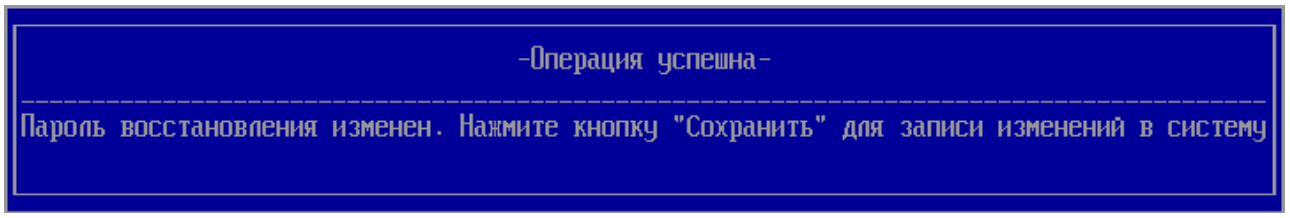


Рисунок 5.24 – Успешная установка пароля восстановления

В диалоговом окне редактирования учетной записи обязательно нажать «Сохранить» для применения нового значения пароля восстановления.

5.5.6 Для сохранения пароля восстановления на мастер-ключ АБ, необходимо предварительно подключить носитель, выбрать его в поле «Мастер-ключ администратора» (рисунок 5.20) и повторить действия по установке пароля восстановления, приведенные выше. После информационного сообщения (рисунок 5.21) будет предложено указать PIN-код персонального идентификатора, а затем указать пароль восстановления.

5.5.7 В случае, если пароль восстановления не задан, то при выходе из мягкого режима будет выведено сообщение (рисунок 5.25).

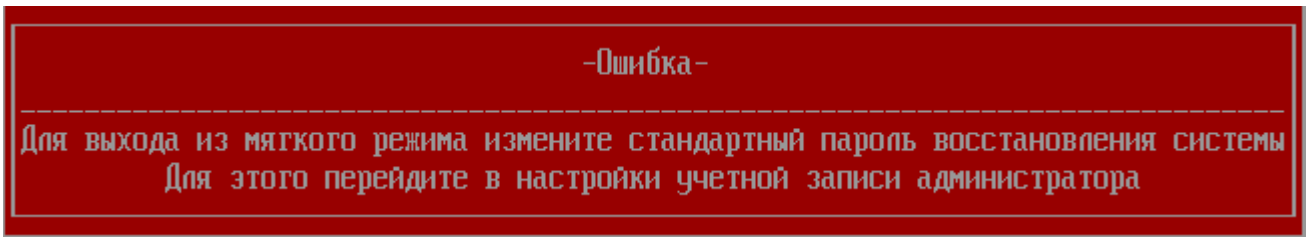


Рисунок 5.25 – Сообщение о необходимости сменить пароль восстановления

6 Управление политиками КЦ объектов и загрузки ОС

6.1 Управление параметрами учетных записей пользователей

6.1.1 Процесс управления параметрами учетных записей пользователей состоит из следующих 4 основных этапов (рисунок 2.1):

1) Создание политики КЦ объектов и загрузки ОС и выбор для контроля:

- файлов и/или каталогов;
- журнала завершенности транзакций файловой системы;
- объектов реестра ОС Windows;
- файлов и параметров среды UEFI;
- загрузочных секторов устройств хранения данных;
- аппаратных устройств ЭВМ.

2) Создание механизма контроля загрузки ОС:

- определение ОС, разрешенных к доверенной загрузке пользователям.

3) Создание политики аутентификации и идентификации пользователя:

- выбор типа аутентификации пользователей;
- определение требований к длине и сложности пароля;
- определение параметров политики: срок действия и количество попыток;
- определение типа блокировки.

4) Определение параметров учетной записи пользователя: имя, политика аутентификации, политика КЦ и загрузки ОС, описание, текущий статус.

Для одной учетной записи пользователя возможно назначение нескольких политик КЦ и загрузки ОС. В случае обнаружения нарушения целостности при нескольких назначенных политиках применяются правила наиболее строгого типа блокировки пользователя.

6.1.2 Перед созданием учетной записи пользователя АБ необходимо (рисунок 2.1):

- предварительно создать политику КЦ объектов и загрузки ОС;
- настроить КЦ аппаратной и/или программной конфигурации ЭВМ;

- настроить механизм контроля доверенной загрузки ОС.

6.1.3 При настройке КЦ объектов для каждой политики доступны следующие варианты:

- **контроль файлов** – КЦ файлов и (или) каталогов загружаемой ОС, а также файлов и (или) каталогов пользователя;
- **контроль журналов транзакций файловых систем** – контроль завершенности транзакций журналов файловых систем NTFS, EXT3, EXT4;
- **контроль реестра ОС Windows** – КЦ объектов реестра ОС семейства Windows;
- **контроль параметров среды UEFI** – КЦ переменных, драйверов и таблиц среды UEFI;
- **контроль загрузочных секторов** – КЦ загрузочных секторов устройств хранения данных;
- **контроль устройств** – контроль аппаратных устройств (аппаратной конфигурации) ЭВМ.

6.1.4 При настройке контроля загрузки ОС для каждой политики доступна процедура **контроля загрузки ОС** – назначение одной или нескольких ОС для доверенной загрузки пользователю.

6.1.5 Реакция при нарушении КЦ объектов является одинаковой для всех объектов контроля и устанавливается при создании политики КЦ объектов и загрузки ОС (подраздел 6.2).

6.2 Создание политики КЦ объектов и загрузки ОС

В БД изделия по умолчанию присутствует встроенная политика контроля ***«All users»***. Для этой политики изначально не настроены механизмы КЦ и контроля загрузки ОС.

6.2.1 Для создания новой политики КЦ и загрузки ОС необходимо выбрать в расширенном меню главного окна консоли АБ подраздел ***«Политики контроля целостности объектов и загрузки ОС»*** (рисунок 4.2). В появившемся диалоговом окне необходимо перейти в строку ***«Создание»*** и нажать клавишу **< *Enter* >** (рисунок 6.1).

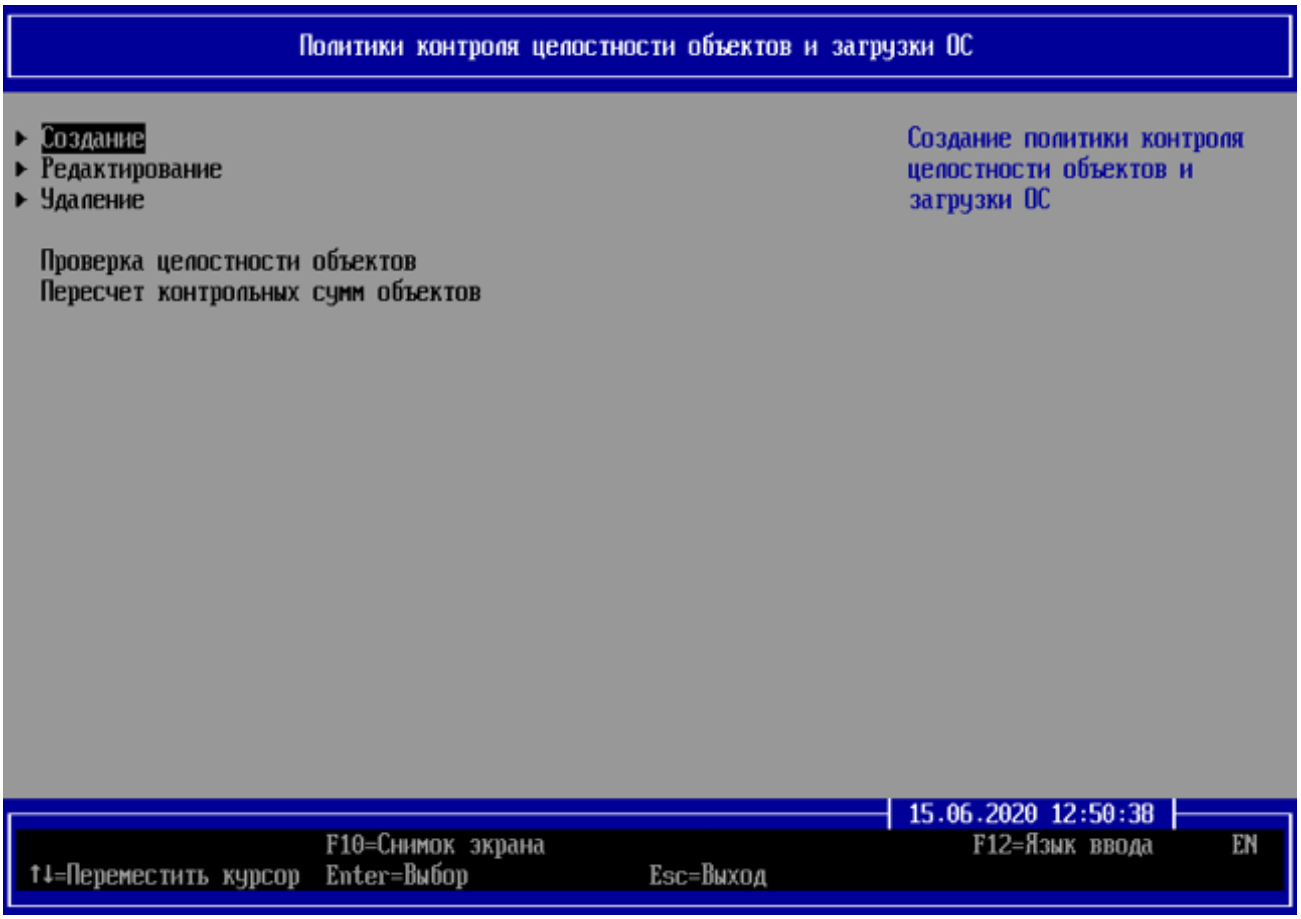


Рисунок 6.1 – Создание политики КЦ объектов и загрузки ОС

6.2.2 В новом диалоговом окне ***«Создание политики контроля целостности объектов и загрузки ОС»*** (рисунок 6.2) необходимо заполнить поле ***«Имя»*** (рисунок 6.3), установить значение параметра ***«Тип блокировки при нарушении»*** (рисунок 6.4) и выбрать какие объекты будут устанавливаться на контроль в создаваемой политике (рисунок 6.5).

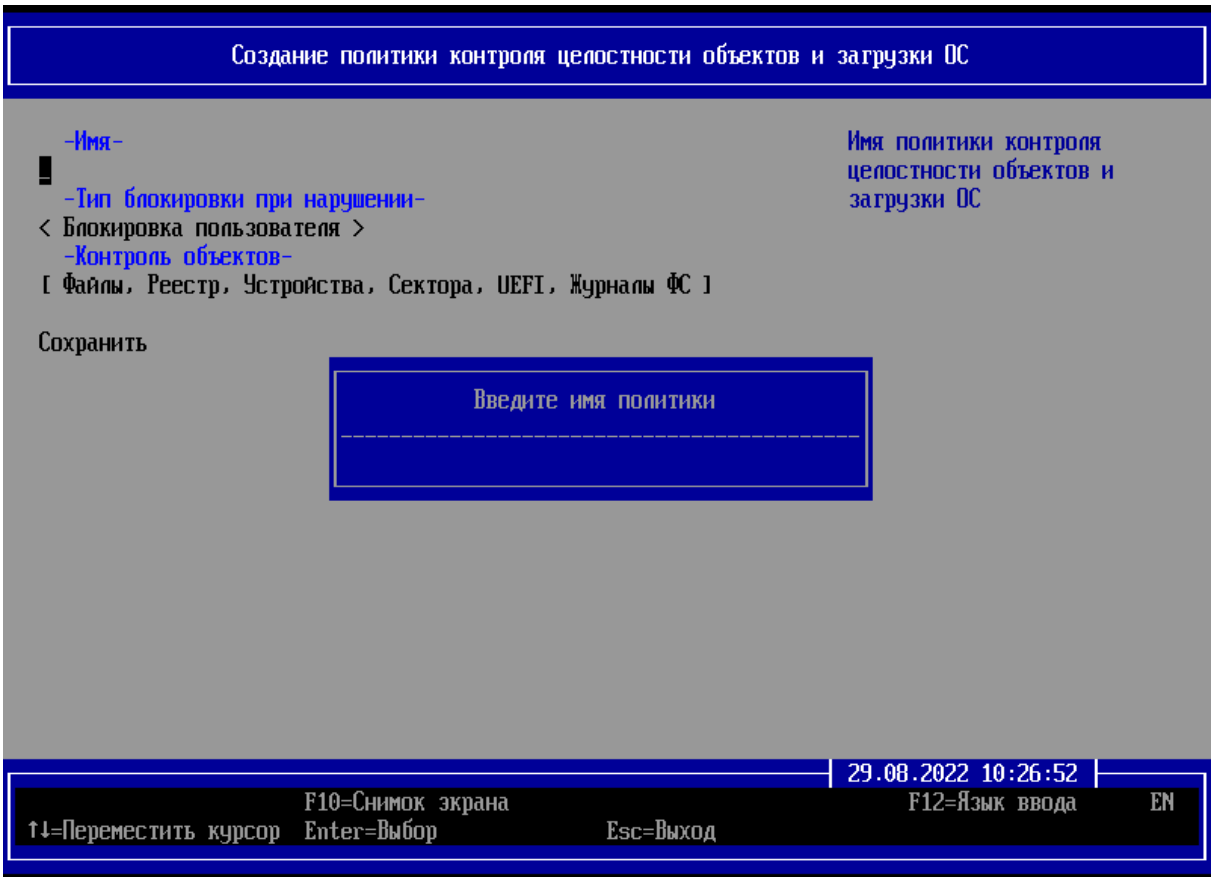


Рисунок 6.2 – Управление параметрами политики КЦ объектов и загрузки ОС

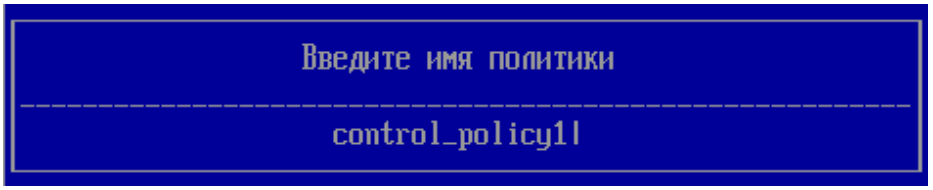


Рисунок 6.3 – Ввод имени политики КЦ объектов и загрузки ОС

6.2.3 Выбранный тип блокировки выделяется угловыми скобками (рисунок 6.4).

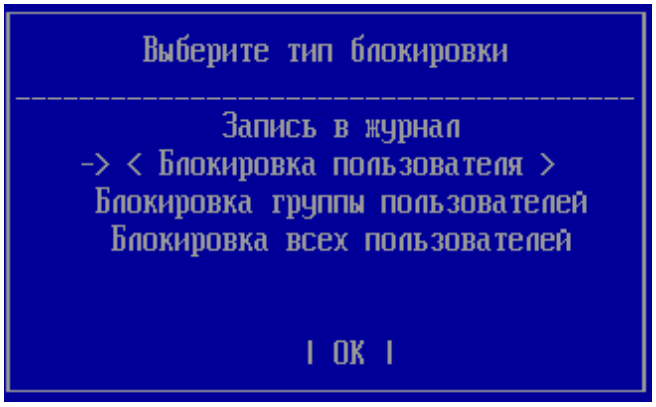


Рисунок 6.4 – Выбор типа блокировки пользователей

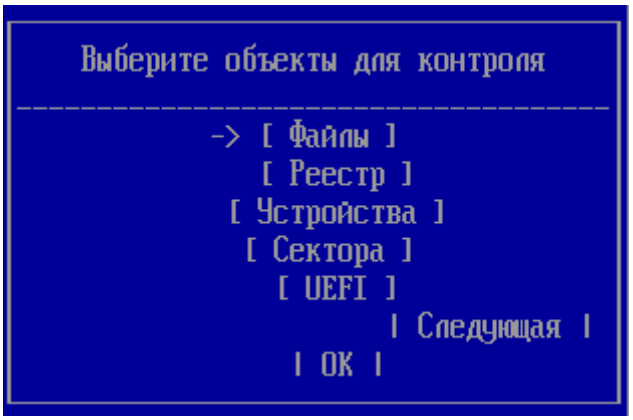


Рисунок 6.5 – Выбор объектов для контроля

Имя политики КЦ объектов и загрузки ОС является уникальным и не может быть дублировано.

КЦ объектов осуществляется в зависимости от значения установленного параметра *«Основные настройки. Контроль целостности. Осуществление контроля целостности»*:

1) до аутентификации пользователя;

2) после аутентификации пользователя.

Если в параметрах хотя бы одной политики КЦ объектов и загрузки ОС установлен параметр *«Блокировка всех пользователей»*, то при обнаружении ошибок КЦ для текущего пользователя, доступ к системе всех пользователей, за исключением АБ, будет блокирован.

6.2.4 Для сохранения сформированной политики необходимо перейти в строку ***«Сохранить»*** и нажать клавишу **< *Enter* >**, при этом на экране ЭВМ появится новое диалоговое окно об успешном создании политики (рисунок 6.6).

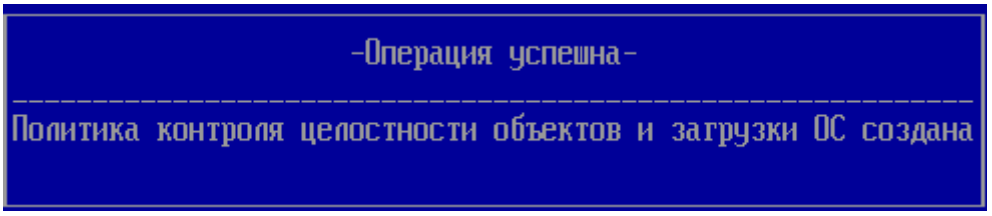


Рисунок 6.6 – Успешное создание политики КЦ и загрузки ОС

В ПО изделия установлено ограничение на создание политик КЦ объектов и загрузки ОС.

Допускается создавать не более 20 политик.

При превышении установленного максимального количества политик КЦ объектов и загрузки ОС, будет выведено сообщение *«Достигнут лимит создания политик»* и операция сохранения политики осуществлена не будет (рисунок 6.7).

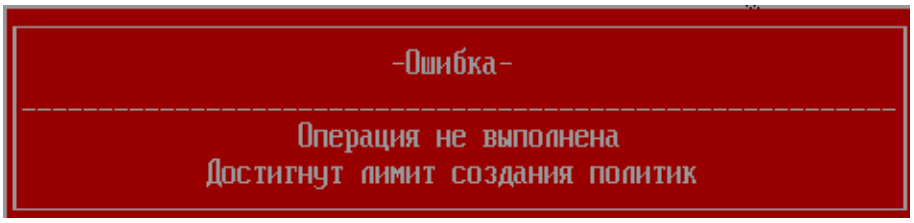


Рисунок 6.7 – Ошибка при создании политики КЦ и загрузки ОС

6.3 Выбор политик КЦ объектов и загрузки ОС для формирования объектов контроля

6.3.1 Объекты контроля для каждой политики назначаются индивидуально, при этом одни и те же объекты КЦ могут быть включены в разные политики КЦ и загрузки ОС.

6.3.2 Для управления объектами КЦ АБ необходимо предварительно указать настраиваемую политику, для этого:

1) В разделе ***«Контроль целостности объектов»*** (рисунок 4.2) перейти в требуемый подраздел КЦ и нажать клавишу **< *Enter* >**.

2) В появившемся диалоговом окне (рисунок 6.8) указать политику контроля, для которой будет осуществляться настройка и нажать кнопку | ***OK*** |.

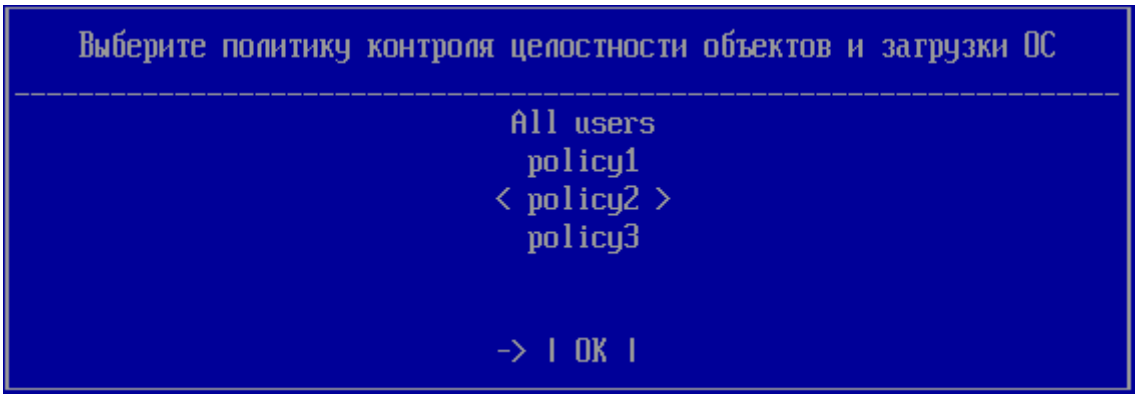


Рисунок 6.8 – Выбор политики КЦ и загрузки ОС для редактирования списка объектов КЦ

6.4 Редактирование политики КЦ и загрузки ОС

6.4.1 Для редактирования существующей политики КЦ и загрузки ОС необходимо выбрать в главном окне консоли АБ подраздел «***Политики контроля целостности объектов и загрузки ОС»*** (рисунок 4.2). В появившемся диалоговом окне необходимо перейти в строку ***«Редактирование»*** и нажать клавишу **< *Enter* >** (рисунок 6.9).

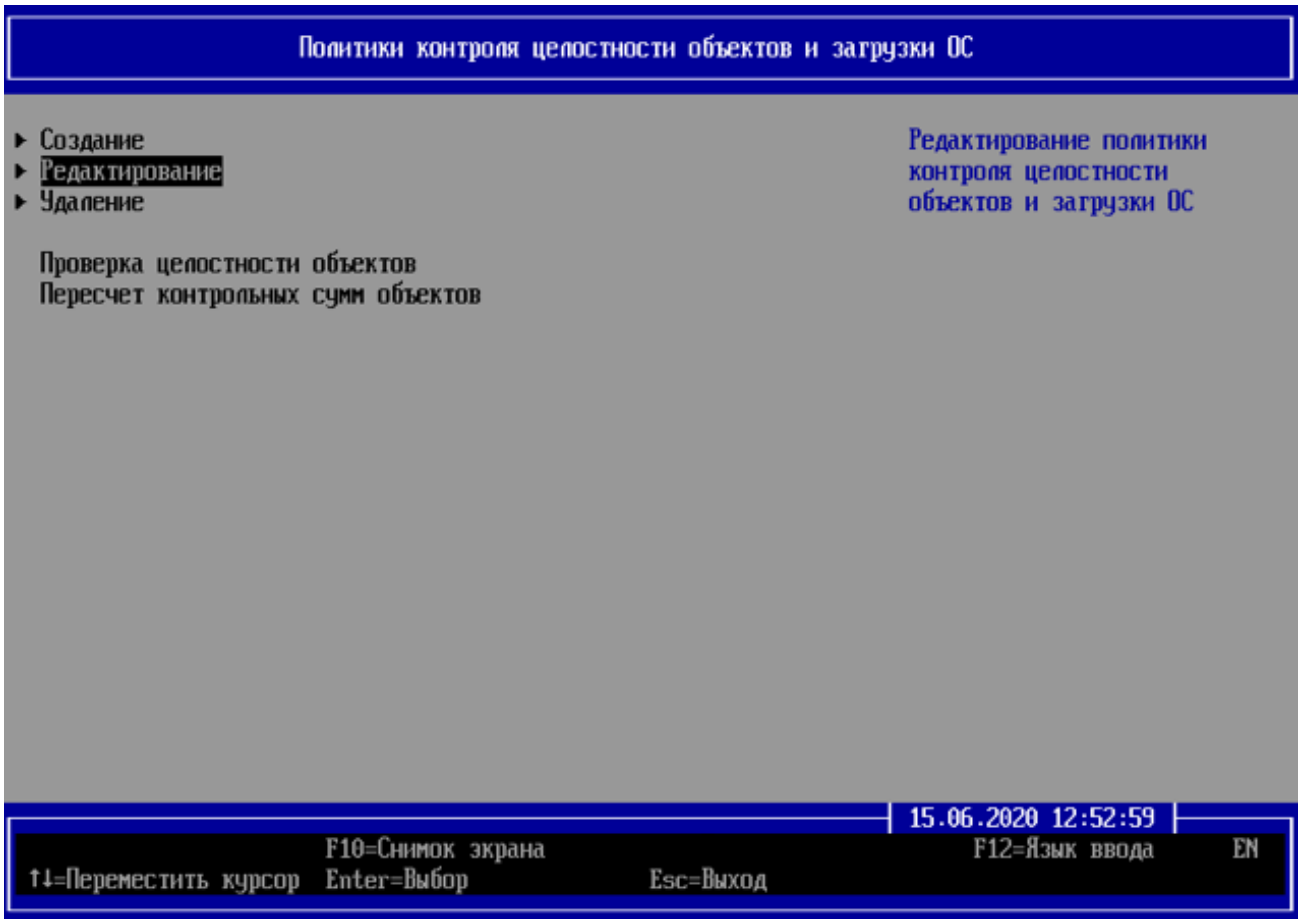


Рисунок 6.9 – Редактирование политики КЦ и загрузки ОС

6.4.2 В новом диалоговом окне ***«Редактирование политики контроля целостности объектов и загрузки ОС»*** (рисунок 6.10) необходимо выбрать имя редактируемой политики КЦ и загрузки ОС в поле ***«Имя»*** и нажать кнопку | ***ОК*** | (рисунок 6.11).

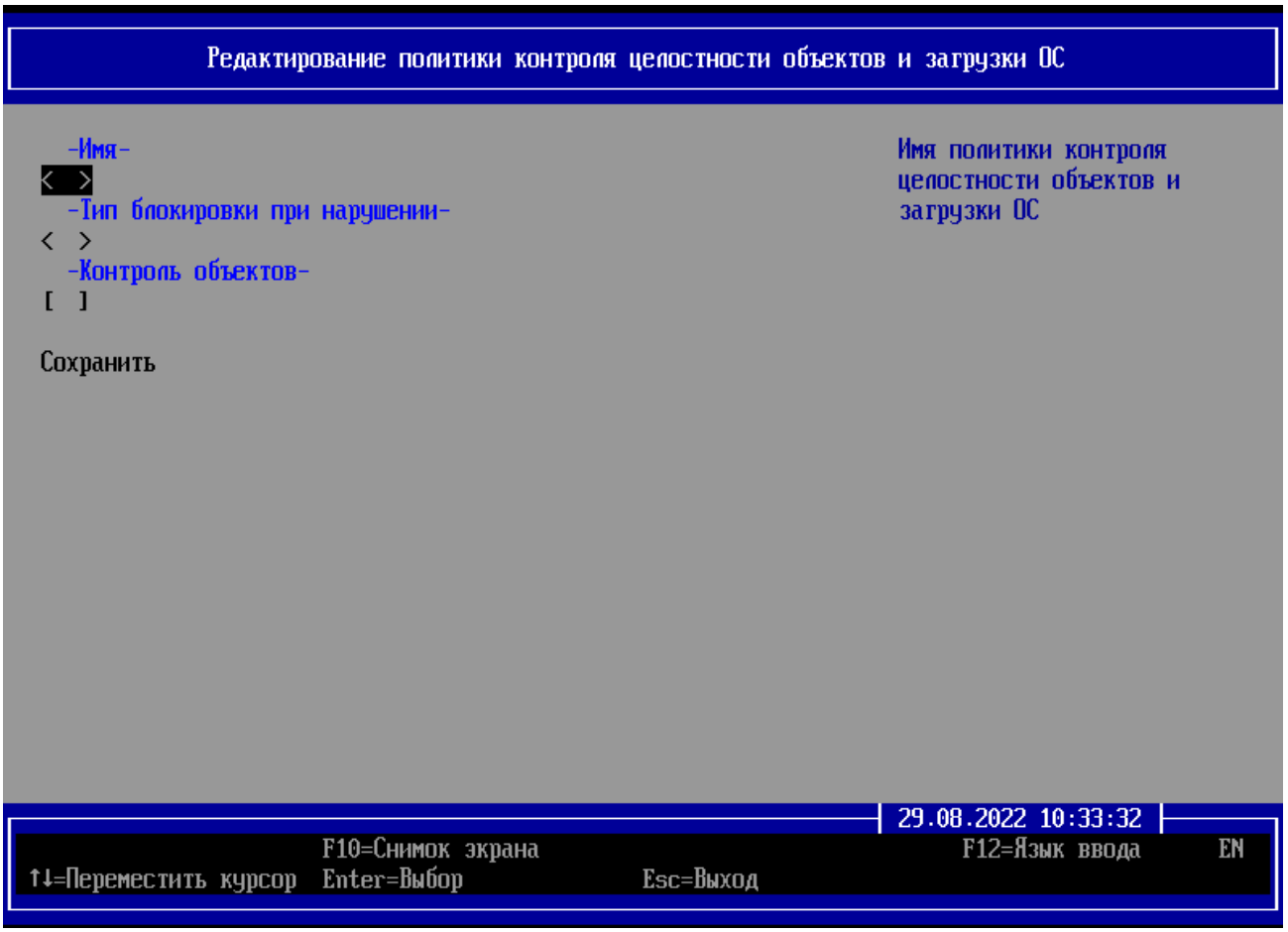


Рисунок 6.10 – Редактирование политики КЦ и загрузки ОС

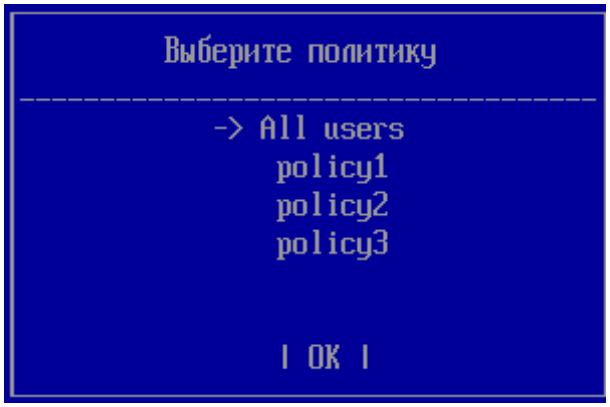


Рисунок 6.11 – Выбор политики КЦ и загрузки ОС

6.4.3 Доступные для установки параметры политики КЦ и загрузки ОС приведены на рисунке 6.12.

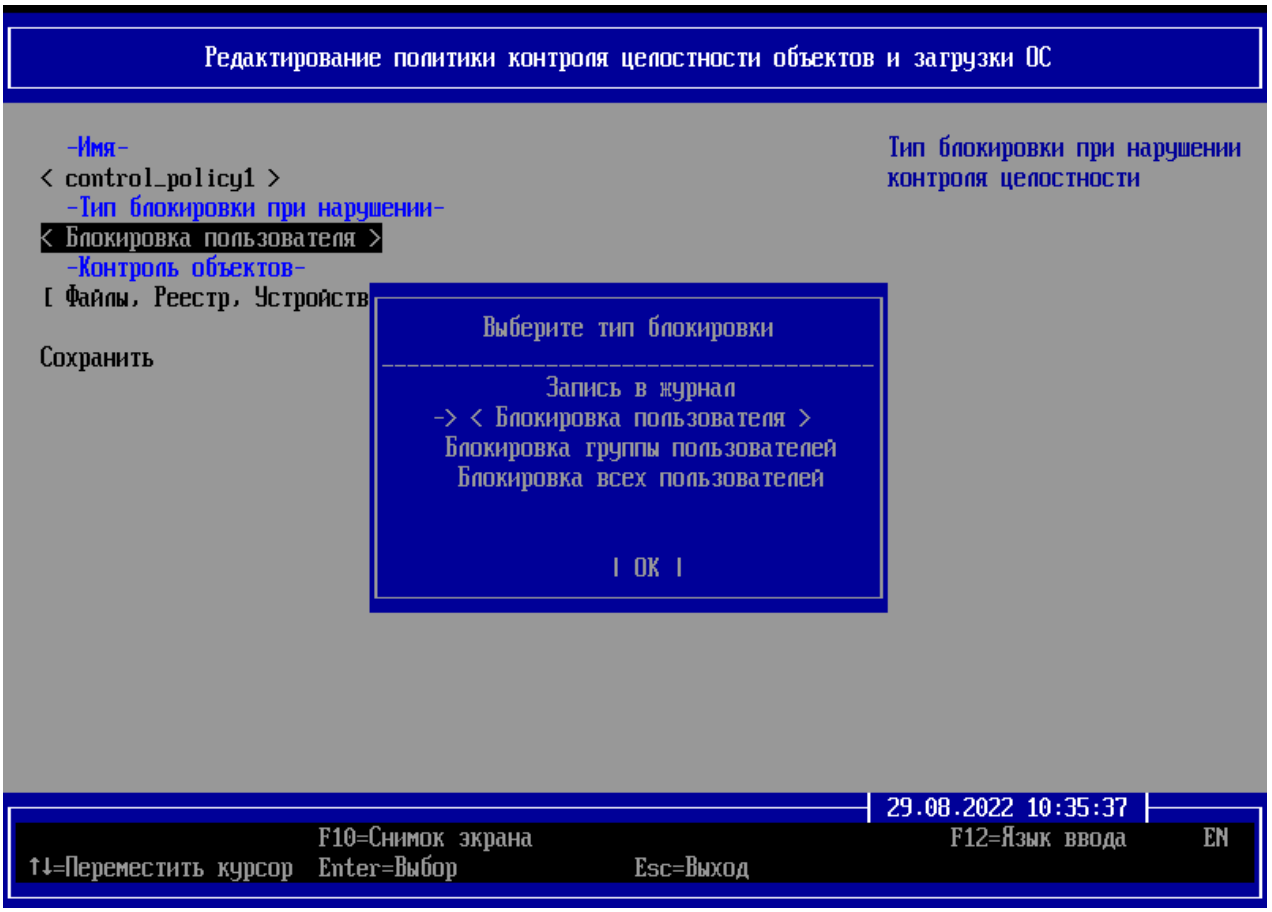


Рисунок 6.12 – Редактируемые параметры политики КЦ и загрузки ОС

6.4.4 Для сохранения изменений редактируемой политики КЦ и загрузки ОС необходимо перейти в строку ***«Сохранить»*** (рисунок 6.12) и нажать клавишу ***< Enter >***. При этом в новом диалоговом окне будет выведено сообщение об успешном редактировании политики КЦ и загрузки ОС (рисунок 6.13).

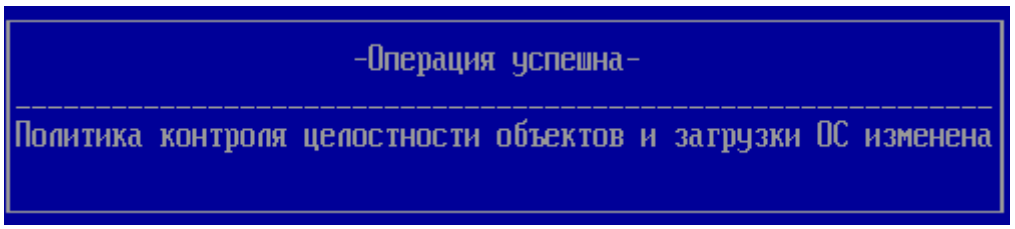


Рисунок 6.13 – Успешное редактирование политики КЦ и загрузки ОС

6.5 Удаление политики КЦ и загрузки ОС

6.5.1 Для удаления существующей политики КЦ и загрузки ОС необходимо выбрать в главном окне консоли АБ подраздел «***Политики контроля целостности объектов и загрузки ОС»*** (рисунок 4.2). В появившемся диалоговом окне необходимо перейти в строку ***«Удаление»*** и нажать клавишу **< *Enter* >** (рисунок 6.1).

6.5.2 В новом диалоговом окне ***«Удаление политики контроля целостности объектов и загрузки ОС»*** (рисунок 6.14) необходимо выбрать имя удаляемой политики КЦ и загрузки ОС в поле ***«Имя»*** и нажать кнопку **| *ОК* |** (рисунок 6.15).

Рисунок 6.14 – Удаление политики КЦ и загрузки ОС

Рисунок 6.15 – Выбор удаляемой политики КЦ и загрузки ОС

Удаление групповых политик производится поочередно.

Групповая политика ***«All users»*** недоступна для удаления.

6.5.3 Для удаления выбранной политики необходимо перейти в строку ***«Удалить»*** и нажать клавишу **< *Enter* >**, при этом на экране ЭВМ появится сообщение об успешном удалении политики КЦ и загрузки ОС (рисунок 6.16).

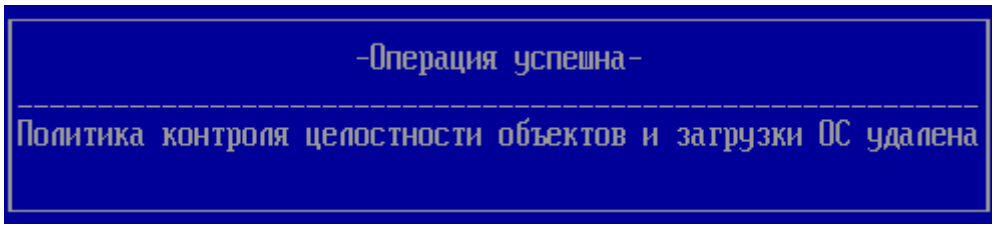


Рисунок 6.16 – Успешное удаление политики КЦ и загрузки ОС

Если политика КЦ объектов и загрузки ОС назначена хотя бы для одной учетной записи пользователя, удаление выполнено не будет и на экран ЭВМ будет выведено сообщение ***«Операция не выполнена. На данную политику ссылаются учетные записи пользователей»*** (рисунок 6.17).

При этом АБ представляется возможность:

- записать данные о выбранной политике в файл – создается файл *.txt с именем политики, содержащий учетные записи пользователей, которым назначена данная политика, и объекты, установленные на контроль;
- отобразить элементы политики – на экран ЭВМ выводятся учетные записи пользователей, которым назначена данная политика (рисунок 6.18).

Для удаления данной политики необходимо поочередно перейти в учетные записи пользователей, которым назначена данная политика, и отредактировать учетные записи путем назначения им другой политики КЦ и загрузки ОС.

Затем действия по удалению политики необходимо повторить.

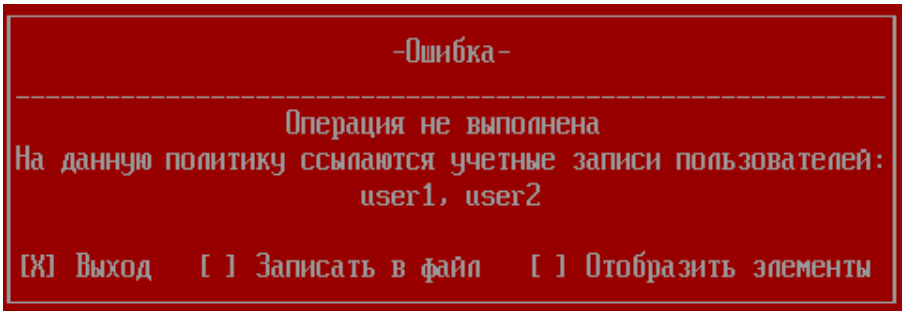


Рисунок 6.17 – Ошибка удаления политики КЦ и загрузки ОС

Рисунок 6.18 – Список объектов в политике КЦ и загрузки ОС

6.6 Проверка нарушений целостности объектов

6.6.1 Для проверки нарушений целостности объектов необходимо в главном окне консоли АБ выбрать подраздел ***«Политики контроля целостности объектов и загрузки ОС»*** (рисунок 4.2). В появившемся диалоговом окне необходимо перейти в строку ***«Проверка целостности объектов»*** и нажать клавишу < ***Enter*** > (рисунок 6.1).

6.6.2 Информация о выполнении процесса проверки нарушений целостности объектов отображается на экране ЭВМ при помощи индикатора (рисунок 6.19).

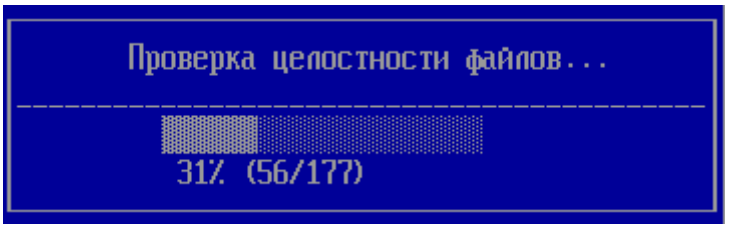


Рисунок 6.19 – Индикатор процесса проверки целостности объектов

6.6.3 При отсутствии нарушений на экран ЭВМ будет выведено сообщение об успешности операции проверки целостности объектов (рисунок 6.20).

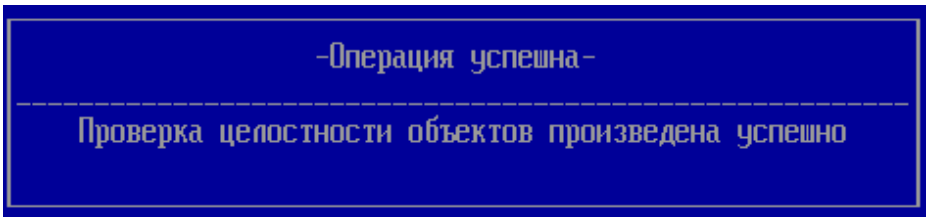


Рисунок 6.20 – Сообщение об успешной проверке целостности объектов

6.6.4 При обнаружении нарушения целостности объектов на экран ЭВМ будет выведено сообщение о выявленном нарушении и указана политика КЦ, в которой обнаружено данное нарушение (рисунок 6.21).

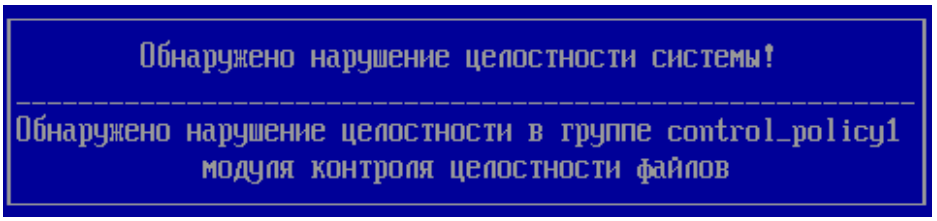


Рисунок 6.21 – Сообщение о нарушении КЦ для АБ

6.6.5 При обнаружении нарушения целостности объектов учетная запись пользователя (за исключением учетной записи АБ) будет заблокирована и на экран ЭВМ будет выведено сообщение о блокировке доступа (рисунок 6.22).

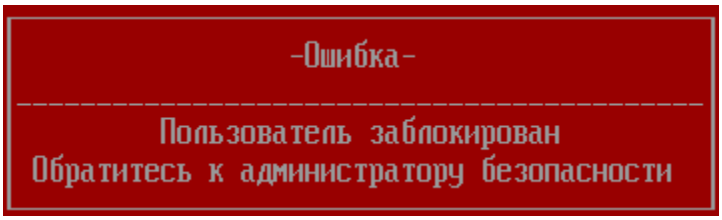


Рисунок 6.22 – Сообщение о блокировке пользователя

6.6.6 Детальное описание выявленного нарушения КЦ указано в журнале аудита (раздел 11).

6.6.7 Порядок действий АБ по устранению выявленных нарушений КЦ объектов описан в подразделе 6.8.

6.7 Отображение ошибок КЦ объектов

6.7.1 При обнаружении нарушения целостности объектов в процессе выполнения проверки (подраздел 6.6) на экран ЭВМ будет выведено сообщение о выявленном нарушении и указана политика КЦ и загрузки ОС, в которой обнаружено данное нарушение (рисунок 6.21).

6.7.2 Для просмотра объектов с нарушением КЦ необходимо перейти в соответствующий раздел ***«Контроль целостности объектов»*** (рисунок 4.2) и выбрать политику КЦ с выявленным нарушением целостности (рисунок 6.21).

6.7.3 В новом диалоговом окне **красным цветом** будет отображаться устройство хранения данных (каталог), в котором выявлено нарушение целостности (рисунок 6.23).

6.7.4 Далее АБ необходимо перейти в строку каталога с нарушением целостности и нажать клавишу < ***Enter*** > (рисунок 6.24).

6.7.5 Объекты с нарушением КЦ отображаются красным цветом (рисунок 6.25).

6.7.6 В ПО изделия реализована следующая индикация объектов КЦ, для которых выявлены нарушения (рисунок 6.25):

-  – объект удален;
-  – объект изменен (модифицирован), в контролируемый каталог добавлен новый объект, в контролируемом каталоге удален объект.

При добавлении объекта в контролируемый каталог данный объект будет отображаться белым цветом (рисунок 6.25).

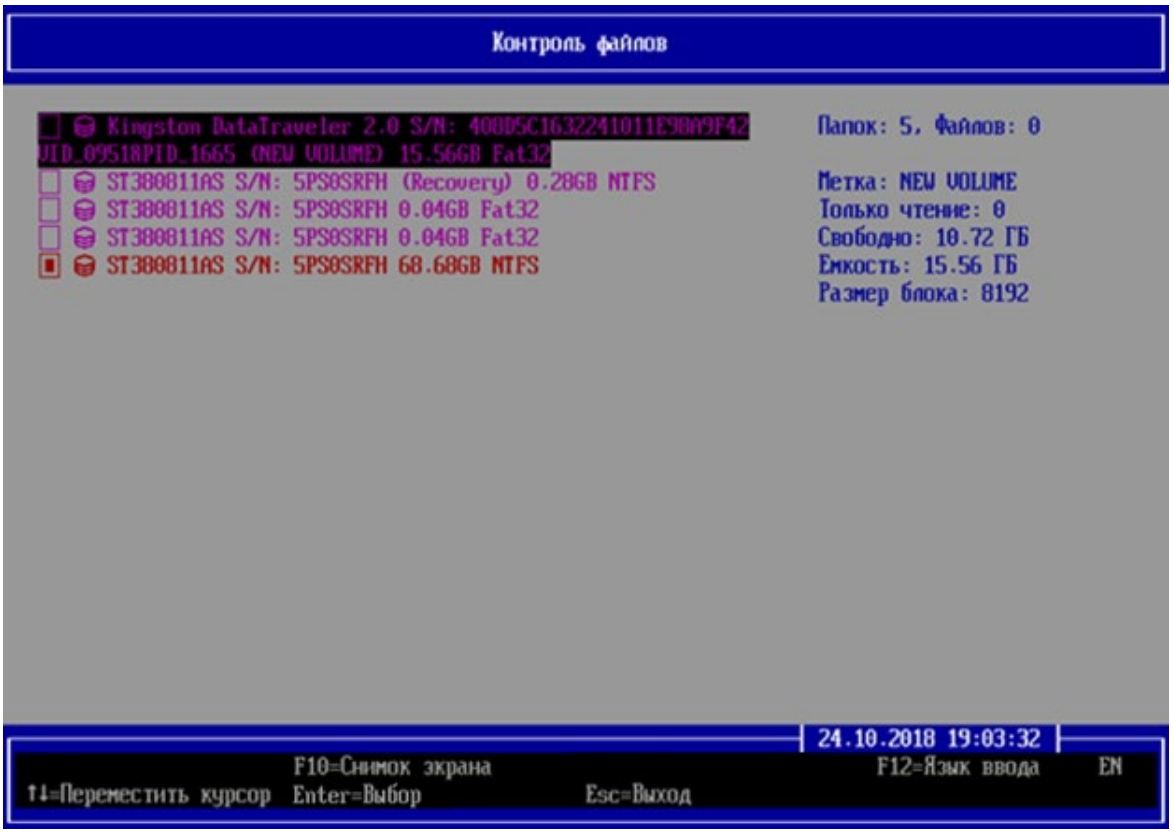


Рисунок 6.23 – Устройство хранения данных с нарушением целостности

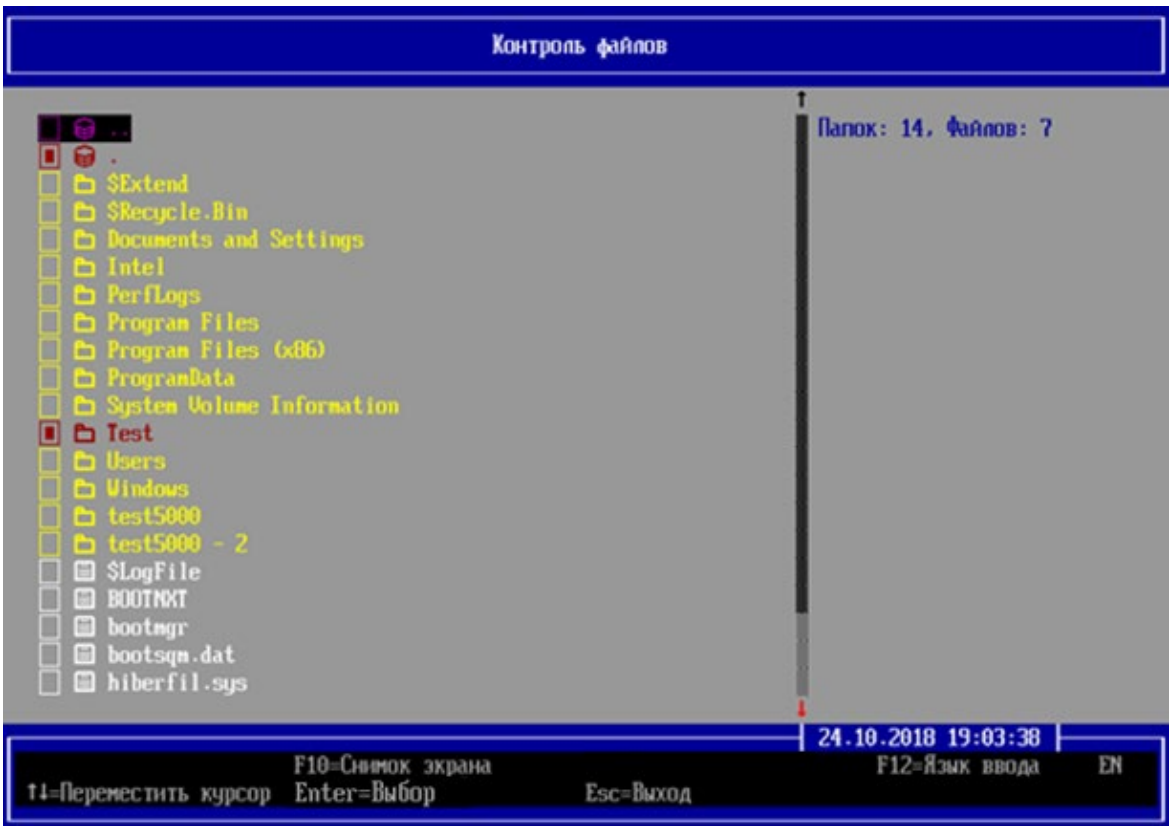


Рисунок 6.24 – Объект с нарушением целостности

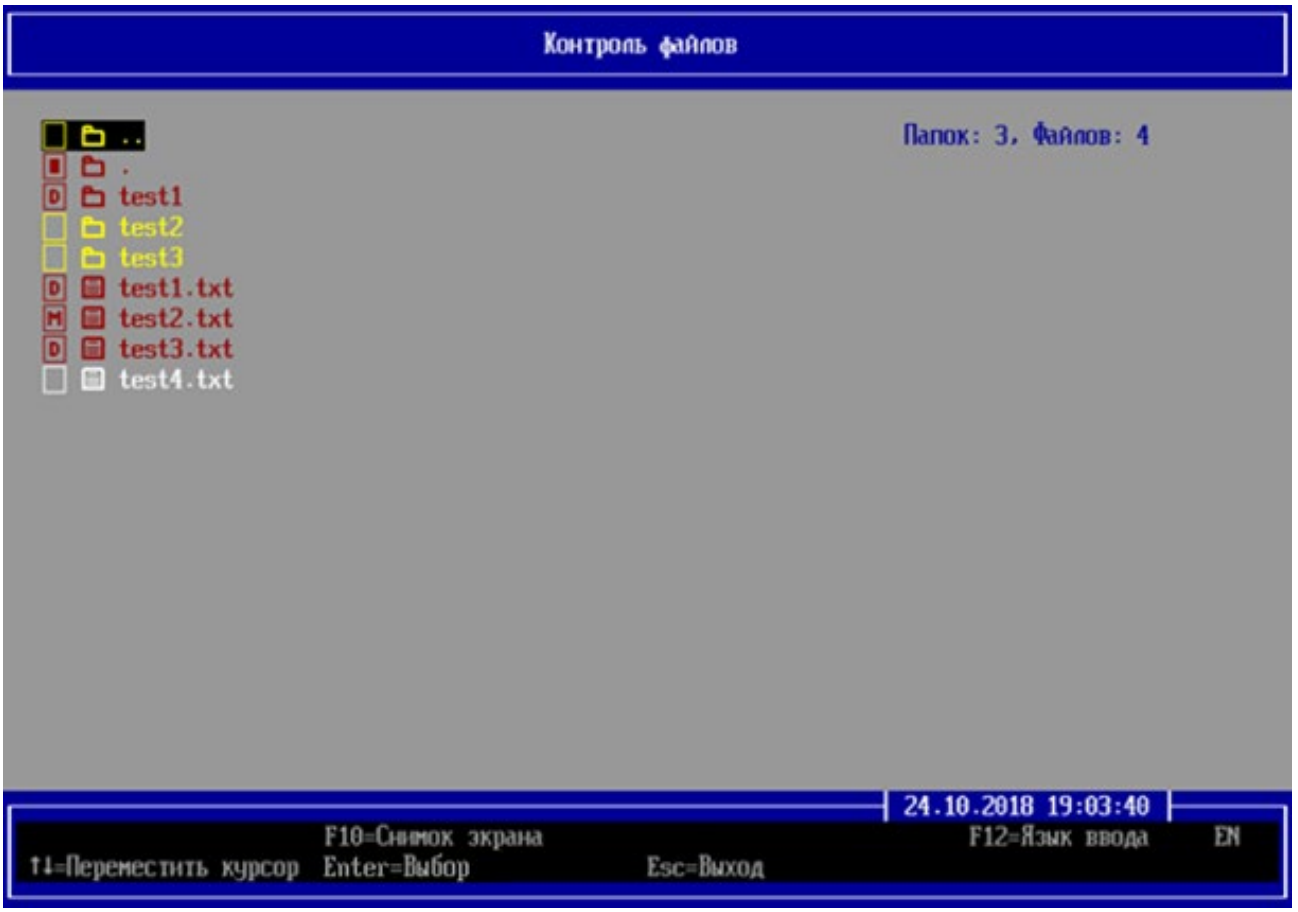


Рисунок 6.25 – Отображение добавленных и удаленных объектов, поставленных на КЦ

6.8 Устранение ошибок КЦ объектов

6.8.1 Для пересчета значений контрольных сумм всех объектов в БД изделия необходимо выбрать в главном окне консоли АБ подраздел ***«Политики контроля целостности объектов и загрузки ОС»*** (рисунок 4.2). В появившемся диалоговом окне необходимо перейти в строку ***«Пересчет контрольных сумм объектов»*** и нажать клавишу < ***Enter*** > (рисунок 6.1).

6.8.2 Информация о выполнении процесса пересчета значений контрольных сумм объектов в БД изделия отображается при помощи индикатора.

6.8.3 По окончанию процесса пересчета значений контрольных сумм объектов в БД изделия на экран ЭВМ будет выведено сообщение об успешности пересчета контрольных сумм объектов (рисунок 6.26).

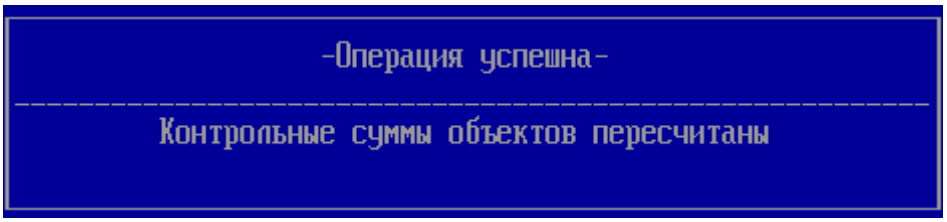


Рисунок 6.26 – Сообщение об успешности пересчета контрольных сумм объектов

6.8.4 Для удаления объекта с КЦ его необходимо выделить его курсором и нажать клавишу < ***Enter*** > (рисунок 6.25).

6.8.5 Для удаления каталога с КЦ его необходимо выделить курсором и нажать клавишу < ***Enter*** >, затем в новом диалоговом окне выделить строку  и нажать клавишу < ***Enter*** > (рисунок 6.24).

Удаленные с КЦ объекты изменят цвет: файлы будут отображаться белым цветом, каталоги – желтым цветом (рисунок 6.25).

6.8.6 После устранения нарушения КЦ объектов необходимо выполнить разблокировку учетных записей пользователей (подраздел 9.4).

6.9 Применение шаблонов политик

6.9.1 Создание шаблонов политик безопасности осуществляется из консоли АБ Linux/Windows. Порядок действий АБ по созданию шаблонов приведен в документе «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 3. Руководство администратора Linux/Windows. ГМТК.468269.060РЭ3».

6.9.2 Использование шаблонов политик безопасности позволяет тиражировать настройки, выполненные АБ для политик аутентификации пользователей и КЦ объектов и загрузки ОС, на АРМ пользователей с установленным изделием.

6.9.3 Для применения шаблона политик безопасности необходимо выбрать в главном окне консоли АБ подраздел ***«Шаблоны политик»*** (рисунок 4.2). В появившемся диалоговом окне в строке ***«Применить шаблон»*** следует нажать клавишу < ***Enter*** > (рисунок 6.27), при этом на экран ЭВМ будет выведено диалоговое окно с выбором устройства хранения данных, содержащим файл шаблона **sdztpl.xml**.

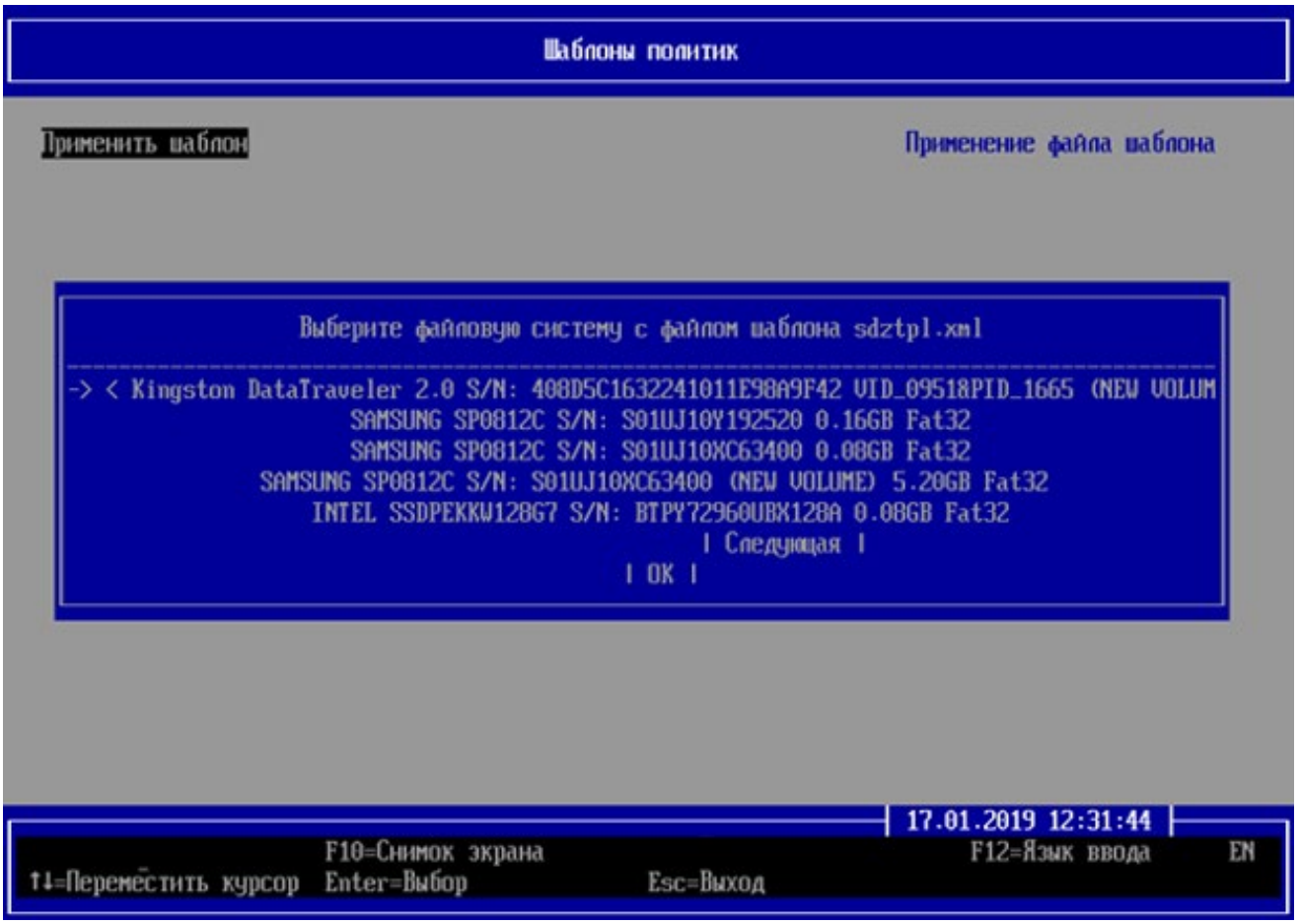
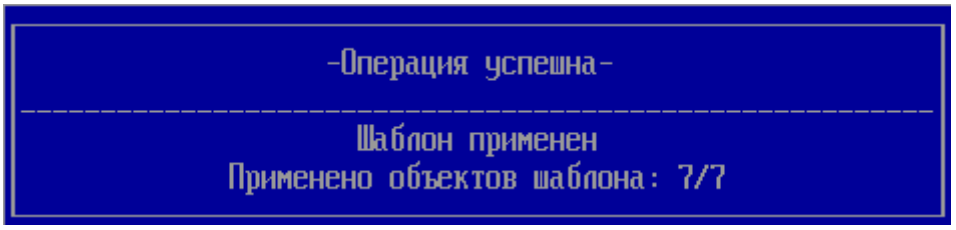
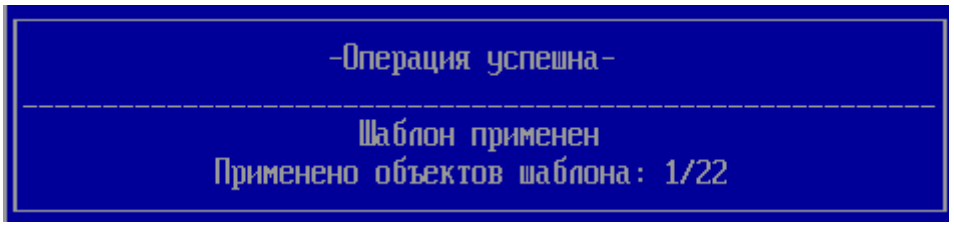


Рисунок 6.27 – Выбор шаблона политик безопасности

6.9.4 В случае успешного применения шаблона в диалоговом окне будет выведено сообщение об успешном применении шаблона и количестве примененных объектов шаблона (рисунок 6.28 а). При отсутствии на АРМ пользователя объектов, в отношении которых применяются настройки шаблона, возможно частичное применение шаблона (рисунок 6.28 б).



а)



б)

Рисунок 6.28 – Успешное применение шаблона

При повреждении файла шаблона политик он применен не будет. В новом диалоговом окне АБ будет выведено сообщение о некорректности файла (рисунок 6.29).

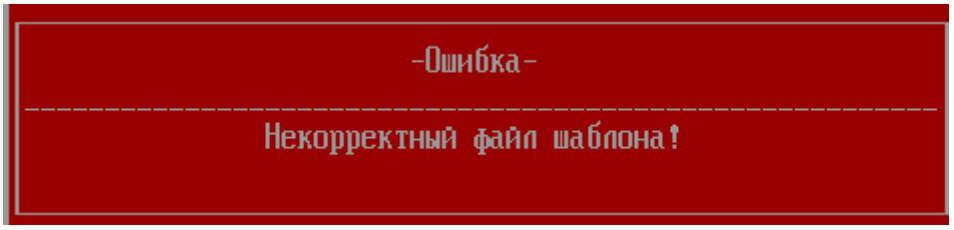


Рисунок 6.29 – Некорректный файл шаблона

6.9.5 При успешном применении шаблона политик безопасности из файла шаблона они будут перенесены в БД изделия.

7 Контроль целостности объектов

7.1 КЦ файлов

7.1.1 При выборе в разделе ***«Контроль целостности»*** подраздела ***«Файлы»*** (рисунок 4.2), последующем выборе редактируемой политики КЦ и загрузки ОС (рисунок 6.7) на экране ЭВМ появится диалоговое окно (рисунок 7.1), содержащее список подключенных к ЭВМ устройств хранения данных и краткое описание их известных свойств. Наименования устройств хранения данных отображаются на экране ЭВМ фиолетовым цветом (рисунок 7.1).

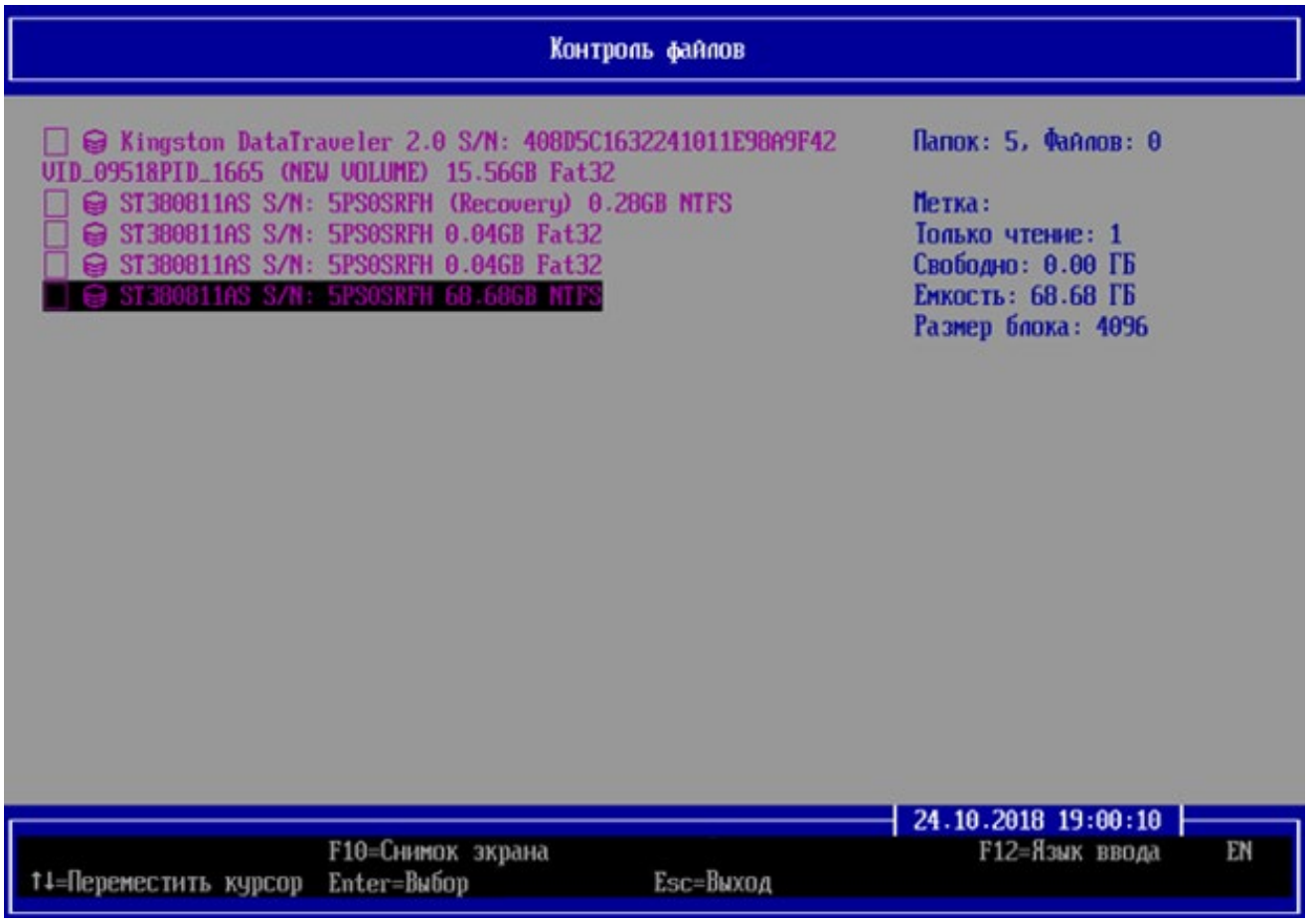


Рисунок 7.1 – Устройства хранения данных и их свойства

7.1.2 Для выбора и установки на КЦ файлов необходимо выбрать требуемое устройство хранения данных (рисунок 7.1) и нажать клавишу **< *Enter* >**, при этом на экране ЭВМ появится новое диалоговое окно (рисунок 7.2).

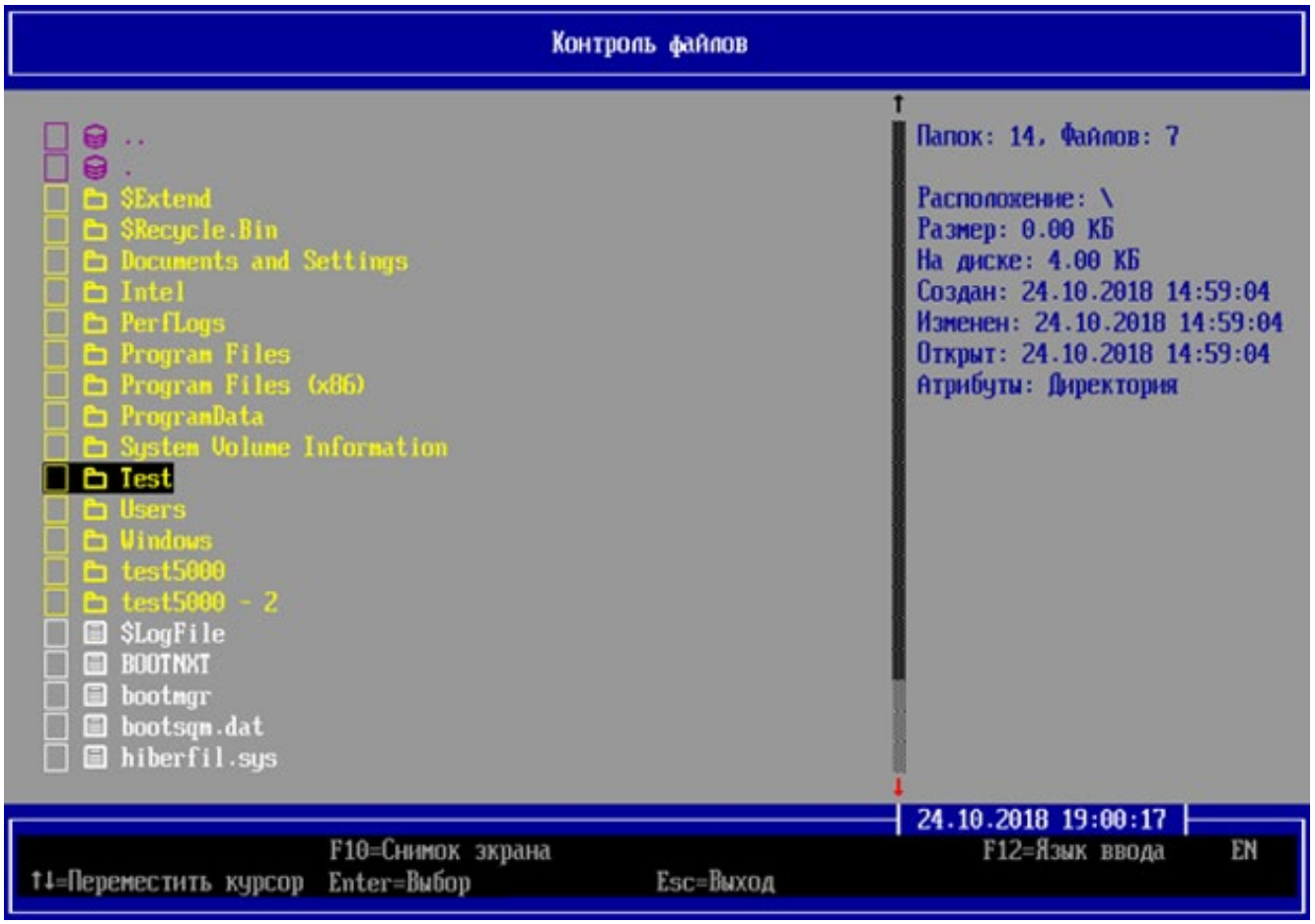


Рисунок 7.2 – Структура каталогов и файлов устройства хранения данных

7.1.3 В левой части окна (рисунок 7.2) отображаются структура каталогов и файлов, доступных для установки на КЦ. Наименования каталогов верхнего (..) и текущего (.) уровней выделены фиолетовым цветом, имена каталогов отображаются желтым цветом ( ), файлов – белым цветом ( ).

7.1.4 В правом верхнем углу окна (рисунок 7.2) расположено поле с информационными данными о выделенном курсором объекте.

7.1.5 Для возврата в каталог верхнего уровня (устройства хранения данных) необходимо перейти в поле .. (рисунок 7.2) и нажать клавишу **< *Enter* >**.

7.1.6 Для установки на КЦ **файла в текущем каталоге** его необходимо выделить курсором (рисунок 7.2) и нажать клавишу **< *Enter* >**.

7.1.7 Для установки на КЦ **каталога** его необходимо выделить курсором, перейдя на соответствующую строку . (рисунок 7.2), и нажать клавишу **< *Enter* >**. При нажатии клавиши осуществится переход в выбранный каталог и отобразится его содержимое. Для установки файла в выбранном каталоге на КЦ необходимо применить

правило из п. 7.1.6, для установки на КЦ всего содержимого каталога необходимо применить правило 7.1.8.

7.1.8 Для установки на КЦ (удаления с КЦ) **всех каталогов и файлов**, содержащихся на данном устройстве хранения данных или выбранном каталоге необходимо перейти в поле  и нажать клавишу **< *Enter* >**.

Перечень файлов ОС семейства Windows и Linux, рекомендуемых к установке на КЦ, приведен в Приложениях А и Б.

7.1.9 Информация о выполнении процесса добавления объектов (каталогов и файлов) на КЦ отображается на экране ЭВМ при помощи индикатора (рисунок 7.3).

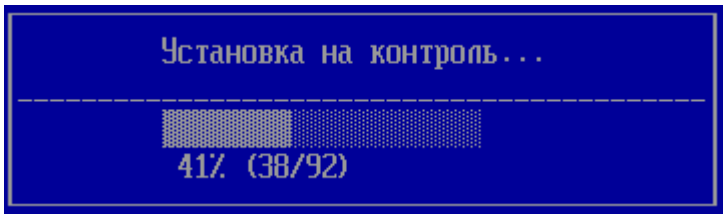


Рисунок 7.3 – Индикатор процесса установки объектов на КЦ

7.1.10 Для **удаления объекта с КЦ** его необходимо выделить курсором и нажать клавишу **< *Enter* >**. Для **пересчета контрольной суммы** объекта его необходимо выделить курсором и дважды нажать клавишу **< *Enter* >**, при этом пересчет и сохранение контрольных сумм объекта происходит автоматически.

7.1.11 Установленные на КЦ объекты отображаются зеленым цветом (рисунок 7.4).

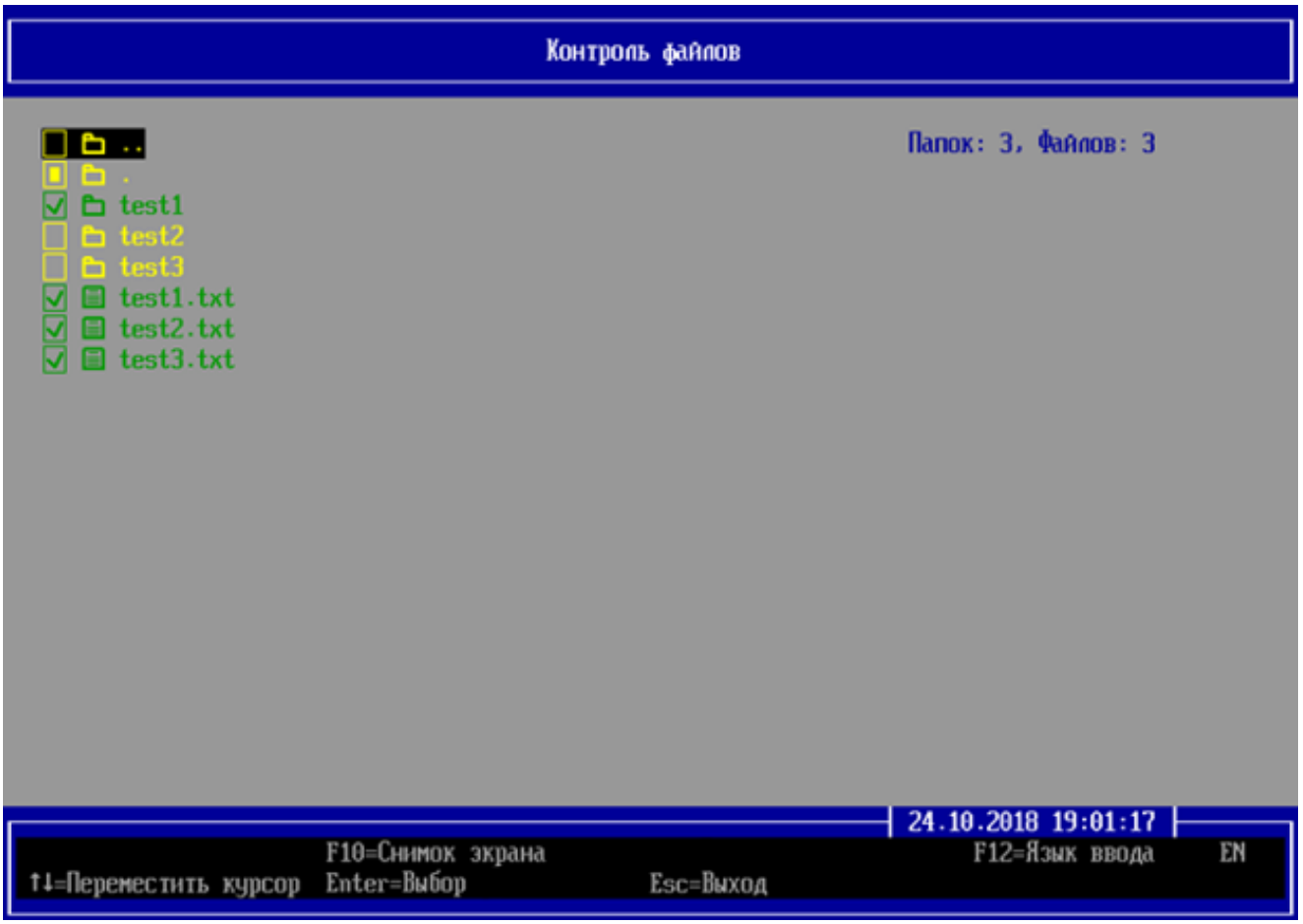


Рисунок 7.4 – Установленные на КЦ объекты

Установка на КЦ большого количества объектов (или объектов большого размера) приведет к значительному увеличению времени аутентификации пользователей в связи с расчетом контрольных сумм объектов и сверкой их со значениями из БД изделия.

Рекомендуется устанавливать на КЦ не более 1000 файлов!

Указание максимального количества контролируемых объектов осуществляется в разделе *«Основные настройки»* (подраздел 10.1).

При превышении установленного максимального количества будет выведено сообщение *«Превышен лимит установки файлов на контроль!»* и установка объектов на КЦ выполнена не будет (рисунок 7.5).

Рисунок 7.5 – Ошибка установки файлов на КЦ

7.1.12 Информация о выполнении процесса удаления объектов (каталогов и файлов) с КЦ отображается на экране ЭВМ при помощи индикатора (рисунок 7.6).

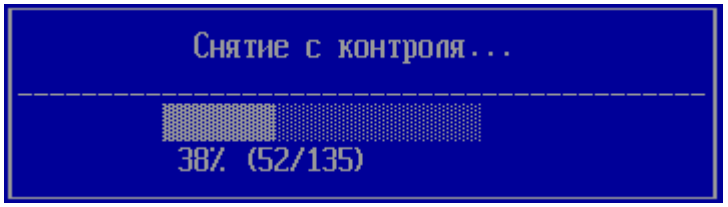


Рисунок 7.6 – Индикатор процесса удаления объектов с КЦ

7.1.13 Процедура просмотра нарушений КЦ и исправления ошибок приведена в подразделе 6.8.

7.2 Контроль завершенности транзакций журналов файловых систем

7.2.1 При выборе в разделе ***«Контроль целостности»*** подраздела ***«Журналы транзакций файловых систем»*** (рисунок 4.2) и последующем выборе редактируемой политики КЦ и загрузки ОС (рисунок 6.7) на экране ЭВМ появится диалоговое окно (рисунок 7.7), содержащее список подключенных к ЭВМ устройств хранения данных и краткое описание их известных свойств. Наименования устройств хранения данных отображаются фиолетовым цветом (рисунок 7.7).

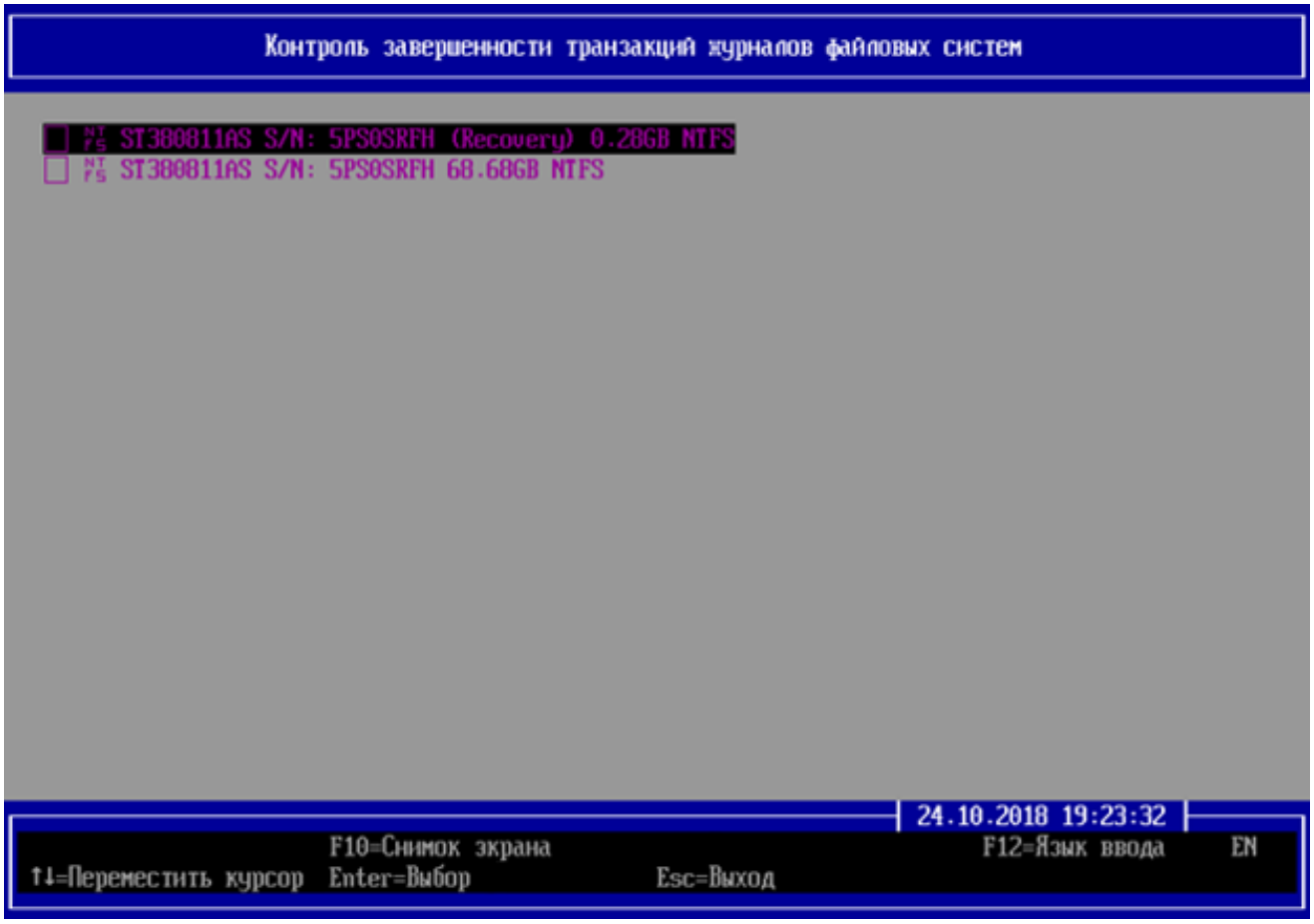


Рисунок 7.7 – Настройка КЦ журналов файловых систем

7.2.2 Для установки на КЦ журналов транзакций файловых систем необходимо курсором перейти в строку с требуемым именем устройства хранения данных и нажать клавишу **< *Enter* >**.

7.2.3 Установленные на КЦ объекты отображаются зеленым цветом (рисунок 7.8).

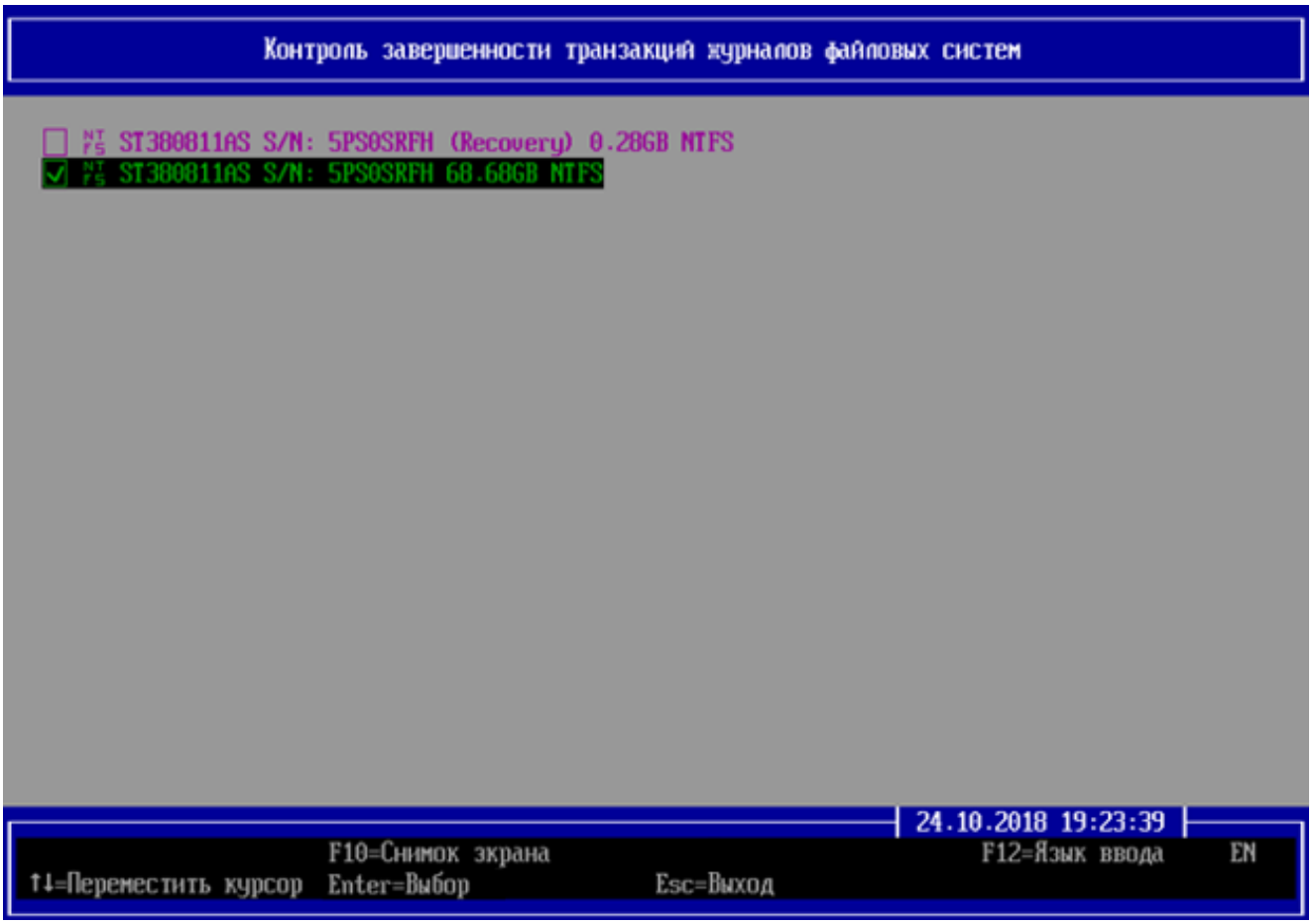


Рисунок 7.8 – Установленные на КЦ журналы файловых систем

7.2.4 Установка на КЦ журналов транзакций файловых систем и их удаление с КЦ осуществляется по правилам, указанным в подразделе 7.1.

7.2.5 В случае установки на КЦ журналов файловых систем, содержащих ошибки или при удалении журналов с контроля после выявленного нарушения, АБ на экран ЭВМ будет выведено диалоговое окно с предложением выбора дальнейшего действия (рисунок 7.9).

7.2.6 Для устранения ошибок программой **CHKDSK** во время последующей загрузки ОС Windows необходимо выбрать пункт ***«Разрешить однократный вход пользователю для восстановления»***, для удаления объекта с КЦ – ***«Удалить объект с контроля»*** (рисунок 7.9).

7.2.7 Для файловых систем, журналирование которых было отключено, АБ в диалоговом окне на экран ЭВМ выводится уведомление ***«Журналирование отключено»***.

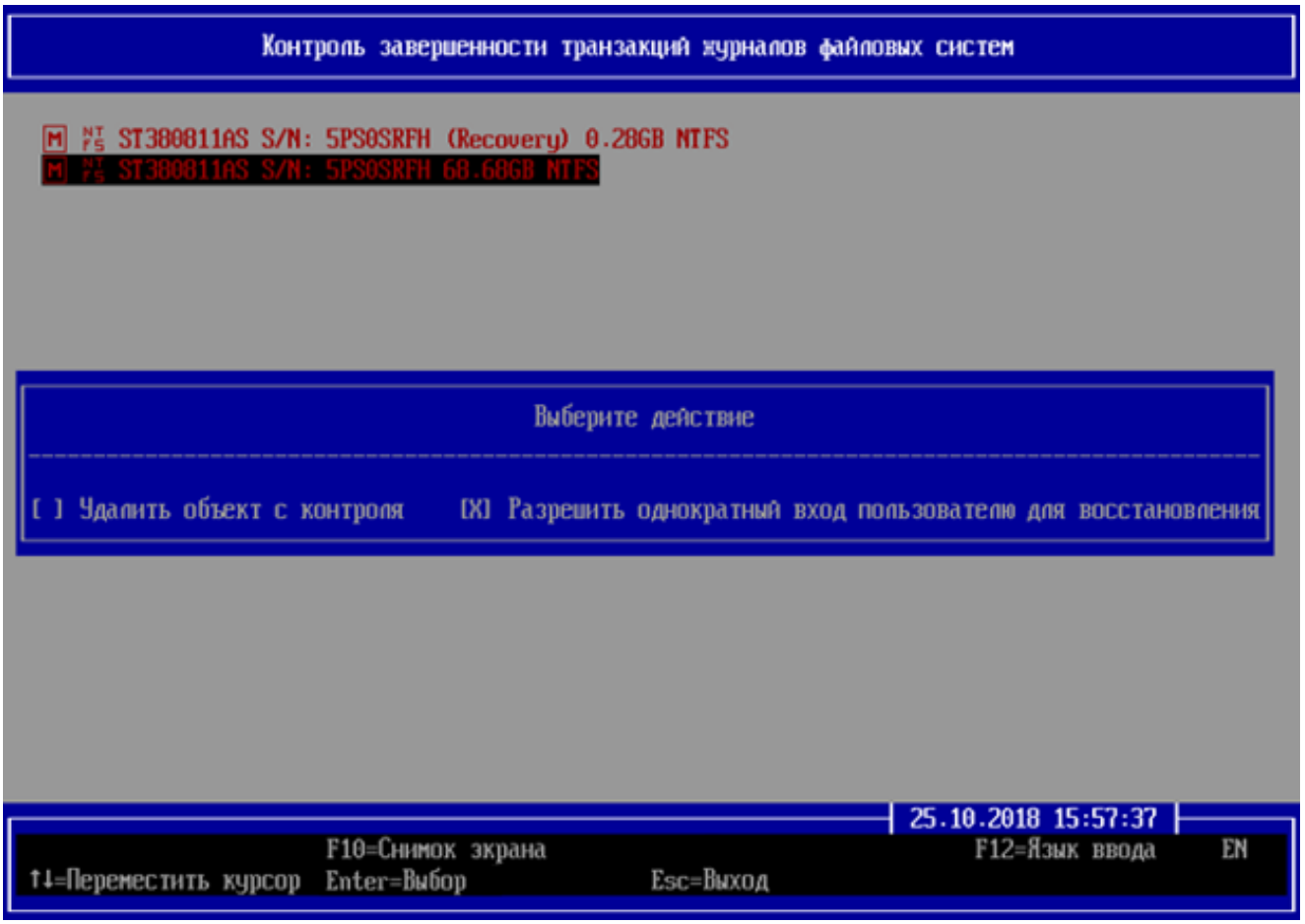


Рисунок 7.9 – Однократный вход пользователя для восстановления журнала транзакций

7.2.8 Процедура просмотра нарушений КЦ объектов и исправления ошибок приведена в подразделе 6.8.

7.3 КЦ объектов реестра ОС семейства Microsoft Windows

7.3.1 При выборе в разделе ***«Контроль целостности»*** подраздела ***«Реестр ОС Windows»*** (рисунок 4.2) и последующем выборе редактируемой политики КЦ и загрузки ОС (рисунок 6.7) на экране ЭВМ появится диалоговое окно (рисунок 7.10), содержащее список объектов реестра ОС Windows. Наименования объектов реестра ОС Windows отображаются фиолетовым цветом (рисунок 7.10).

7.3.2 Установка на КЦ объектов реестра ОС Windows и их удаление с КЦ осуществляется по правилам, указанным в подразделе 7.1.

7.3.3 Установленные на КЦ объекты отображаются зеленым цветом (рисунок 7.11).

7.3.4 Процедура просмотра нарушений КЦ и исправления ошибок приведена в подразделе 6.8.

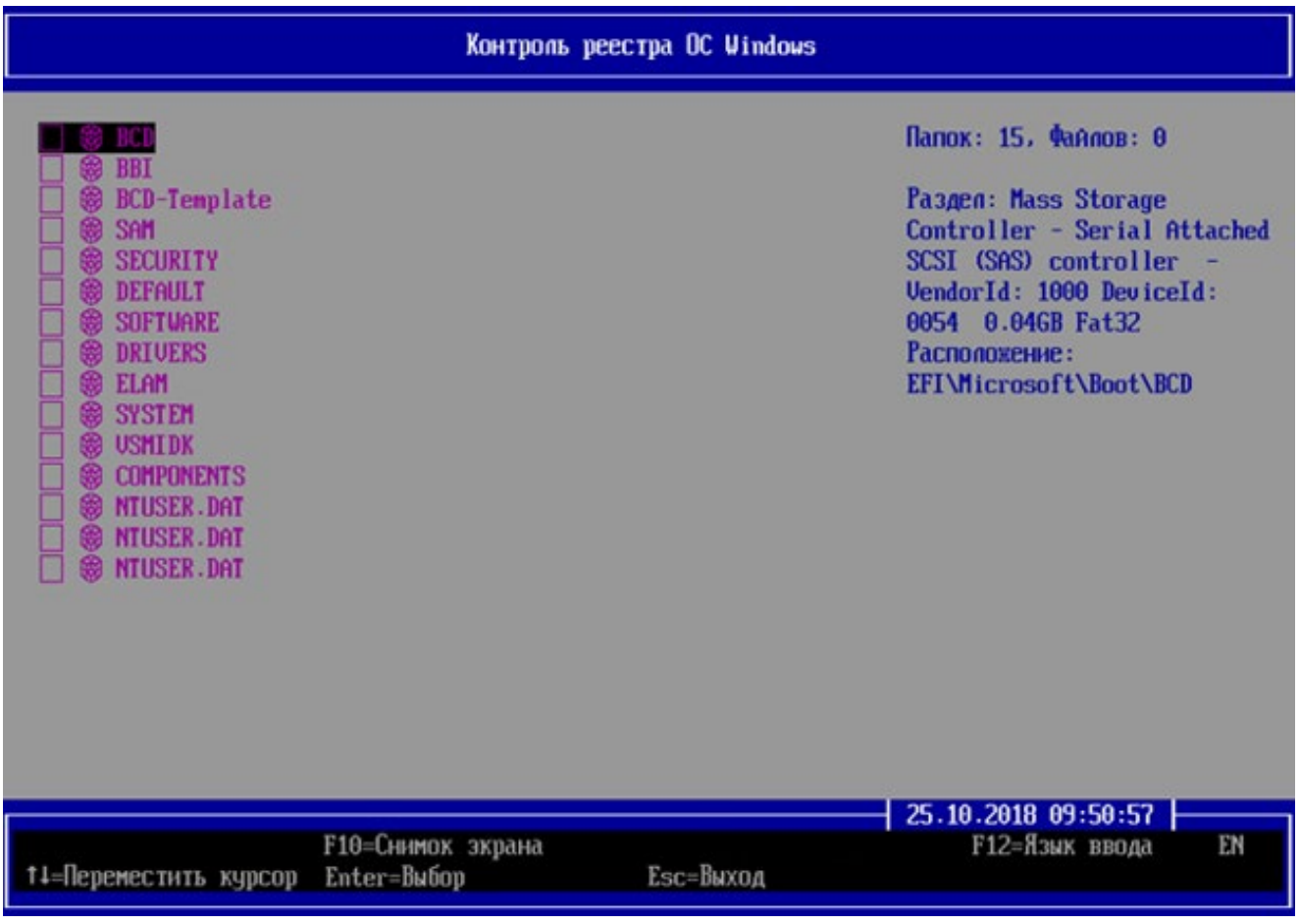


Рисунок 7.10 – Структура объектов реестра ОС Windows

7.3.5 Информация о выполнении процесса добавления объектов (каталогов и файлов) на КЦ отображается на экране ЭВМ при помощи индикатора (рисунок 7.3).

Рисунок 7.11 – Установленные на КЦ объекты реестра ОС Windows

Установка на КЦ большого количества объектов реестра ОС Windows (либо всего реестра ОС) приведет к значительному увеличению времени при аутентификации пользователей в связи с расчетом контрольных сумм объектов реестра и сверкой их со значениями из БД изделия.

Рекомендуется устанавливать на КЦ не более 1000 объектов реестра ОС Windows!

Задание максимального количества контролируемых объектов реестра осуществляется в разделе *«Основные настройки»* основного окна консоли АБ (подраздел 10.1). При превышении установленного максимального количества, АБ будет выведено сообщение *«Превышен лимит установки объектов реестра на контроль!»* и установка объектов реестра на КЦ не будет выполнена (рисунок 7.12).

Рисунок 7.12 – Ошибка установки объектов реестра на КЦ

В связи с особенностями хранения реестра ОС Windows в файлах на устройствах хранения данных (разделы реестра HKEY_CLASSES_ROOT, HKEY_CURRENT_USER HKEY_CURRENT_CONFIG создаются при запуске ОС) для КЦ доступны объекты реестра, существующие до старта ОС семейства Windows.

Подробная информация о структуре реестра ОС Windows приведена на официальном сайте компании Microsoft по следующим ссылкам: http://support.microsoft.com/kb/256986/ru или https://msdn.microsoft.com/ru-ru/library/windows/desktop/ms724877%28v=vs.85%29.aspx

7.3.6 В таблице 7.1 приведено соответствие между названиями основных ветвей реестра ОС Windows (рисунок 7.10) и названиями ветвей реестра, отображаемыми в редакторе реестра **regedit**.

Таблица 7.1 – Соответствие названий разделов реестра в консоли АБ и редакторе реестра **regedit**

№	Название объектов реестра в консоли АБ (имя файла)	Название объектов реестра в редакторе regedit
<Имя устройства хранения данных>:\Windows\System32\config		
1	BBI	
2	BCD-Template	HKEY_LOCAL_MACHINE\BCD00000000
3	COMPONENTS	
4	DEFAULT	HKEY_USERS\.DEFAULT
5	DRIVERS	HKEY_LOCAL_MACHINE\DRIVERS
6	ELAM	
7	SAM	HKEY_LOCAL_MACHINE\SAM
8	SECURITY	HKEY_LOCAL_MACHINE\SECURITY
9	SOFTWARE	HKEY_LOCAL_MACHINE\SOFTWARE
10	SYSTEM	HKEY_LOCAL_MACHINE\SYSTEM

№	Название объектов реестра в консоли АБ (имя файла)	Название объектов реестра в редакторе regedit
<Имя устройства хранения данных>:\Boot		
11	BCD	HKEY_LOCAL_MACHINE\BCD00000000
<Имя устройства хранения данных>:\<Пользователи>\<Имя пользователя>		
12	NTUSER.DAT	HKEY_CURRENT_USER

7.4 КЦ параметров среды UEFI

7.4.1 При выборе в разделе ***«Контроль целостности»*** подраздела ***«Параметры среды UEFI»*** (рисунок 4.2) и последующем выборе редактируемой политики КЦ и загрузки ОС (рисунок 6.7) на экране ЭВМ появится диалоговое окно (рисунок 7.13), содержащее список переменных, драйверов, системных таблиц среды и карты памяти UEFI. Наименования объектов отображаются фиолетовым цветом (рисунок 7.13).

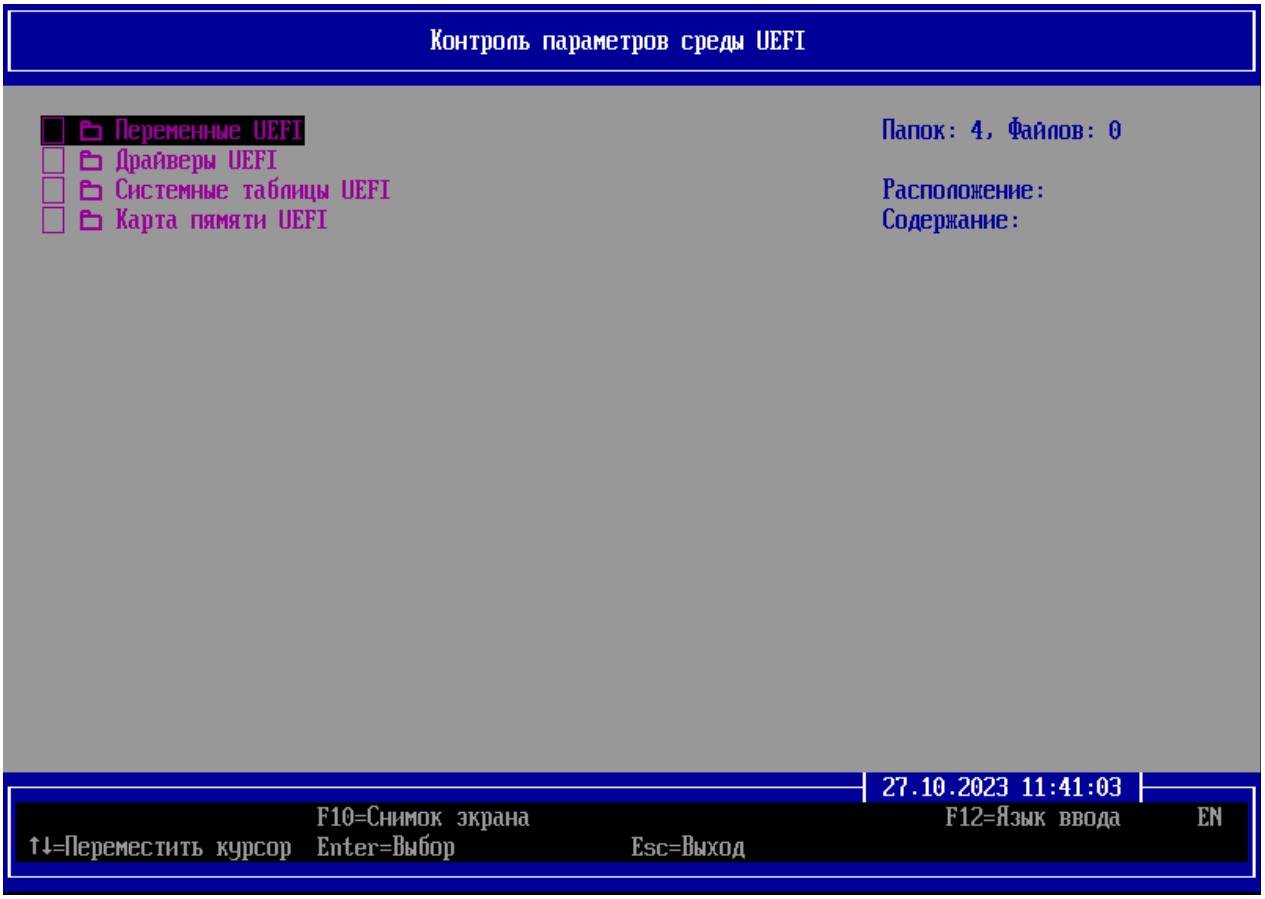


Рисунок 7.13 – Настройка КЦ параметров среды UEFI

7.4.2 Установка на КЦ объектов среды UEFI и их удаление осуществляется по правилам, указанным в подразделе 7.1.

7.4.3 Установленные на КЦ объекты отображаются зеленым цветом (рисунки 7.14 – 7.17).

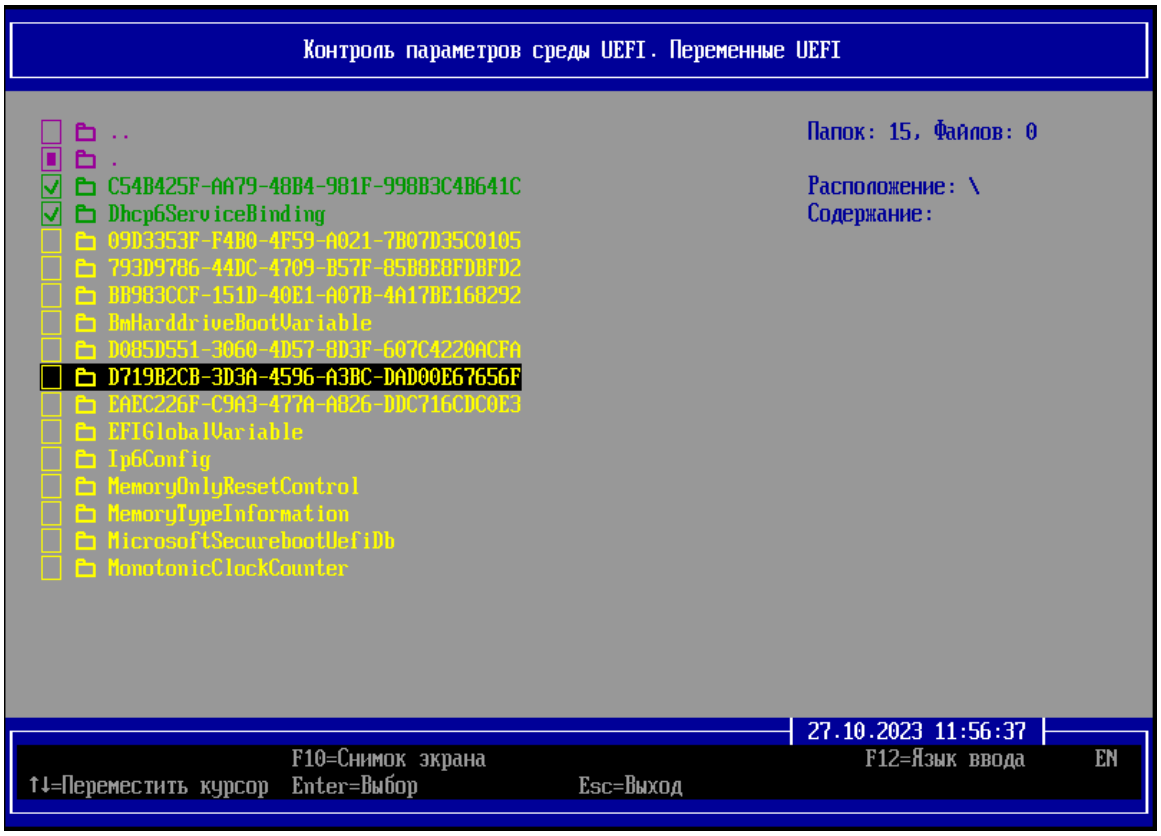


Рисунок 7.14 – Установленные на КЦ переменные UEFI

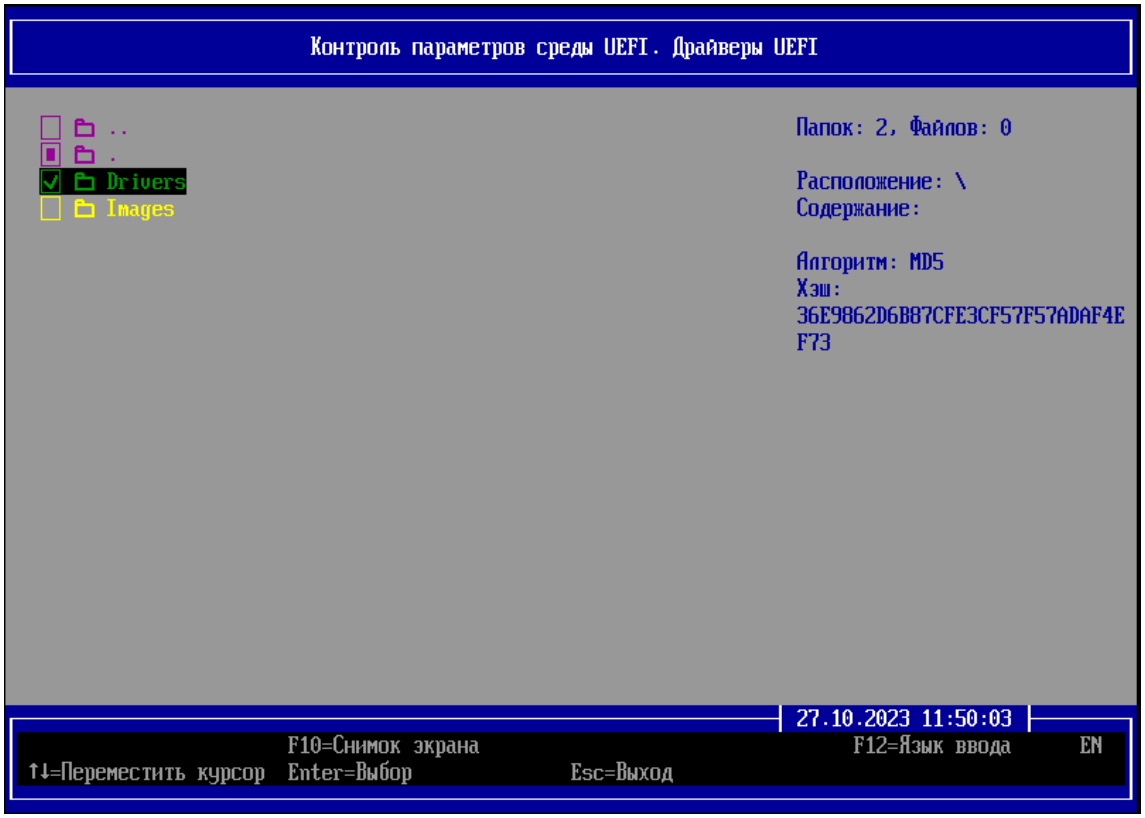


Рисунок 7.15 – Установленные на КЦ драйверы UEFI

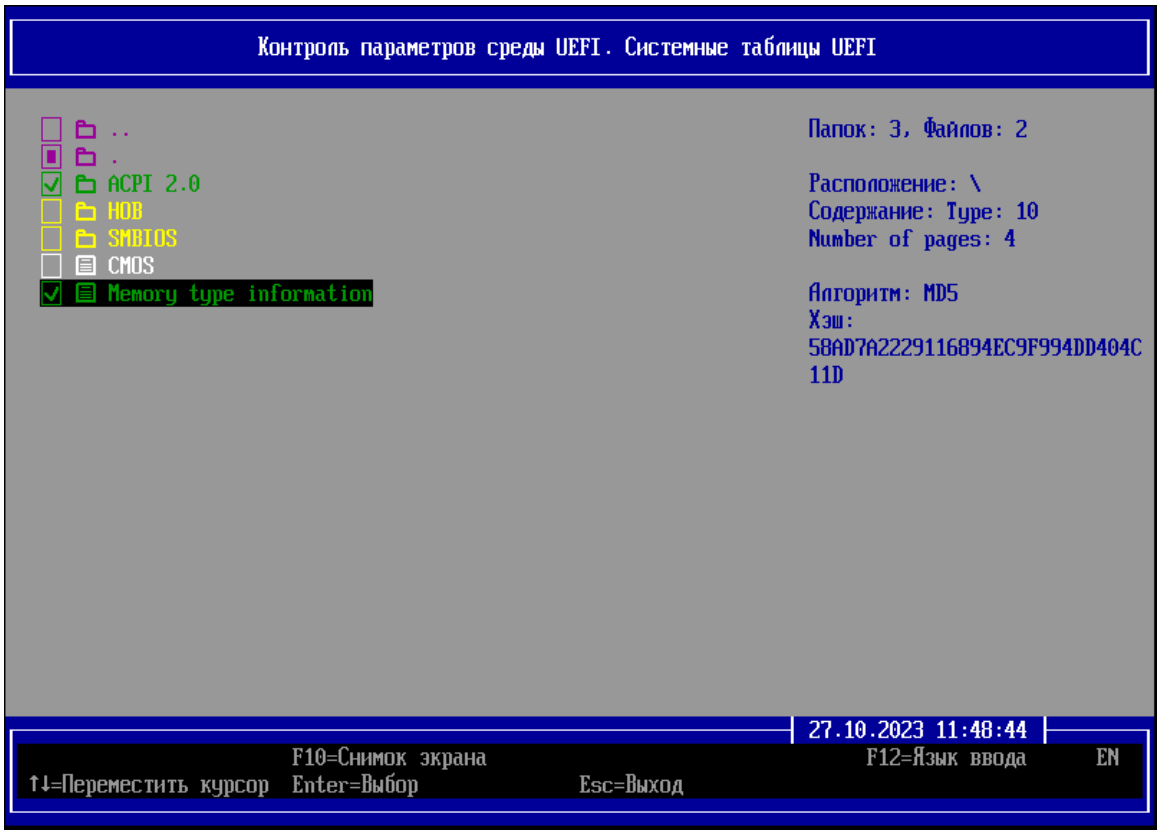


Рисунок 7.16 – Установленные на КЦ системные таблицы UEFI

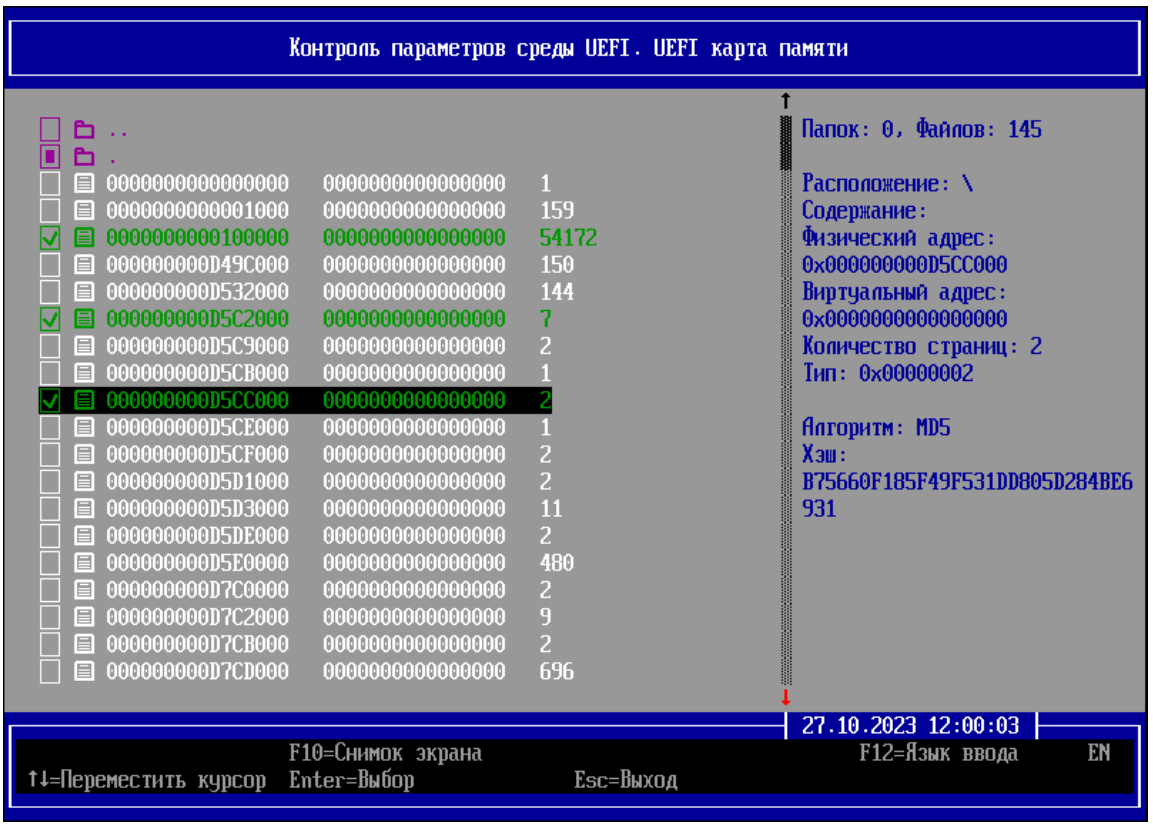


Рисунок 7.17 – Установленная на КЦ карта памяти UEFI

7.4.4 Установленные на КЦ объекты среды UEFI в окне ***«Контроль параметров среды UEFI»*** будут отображаться как  (рисунок 7.18).

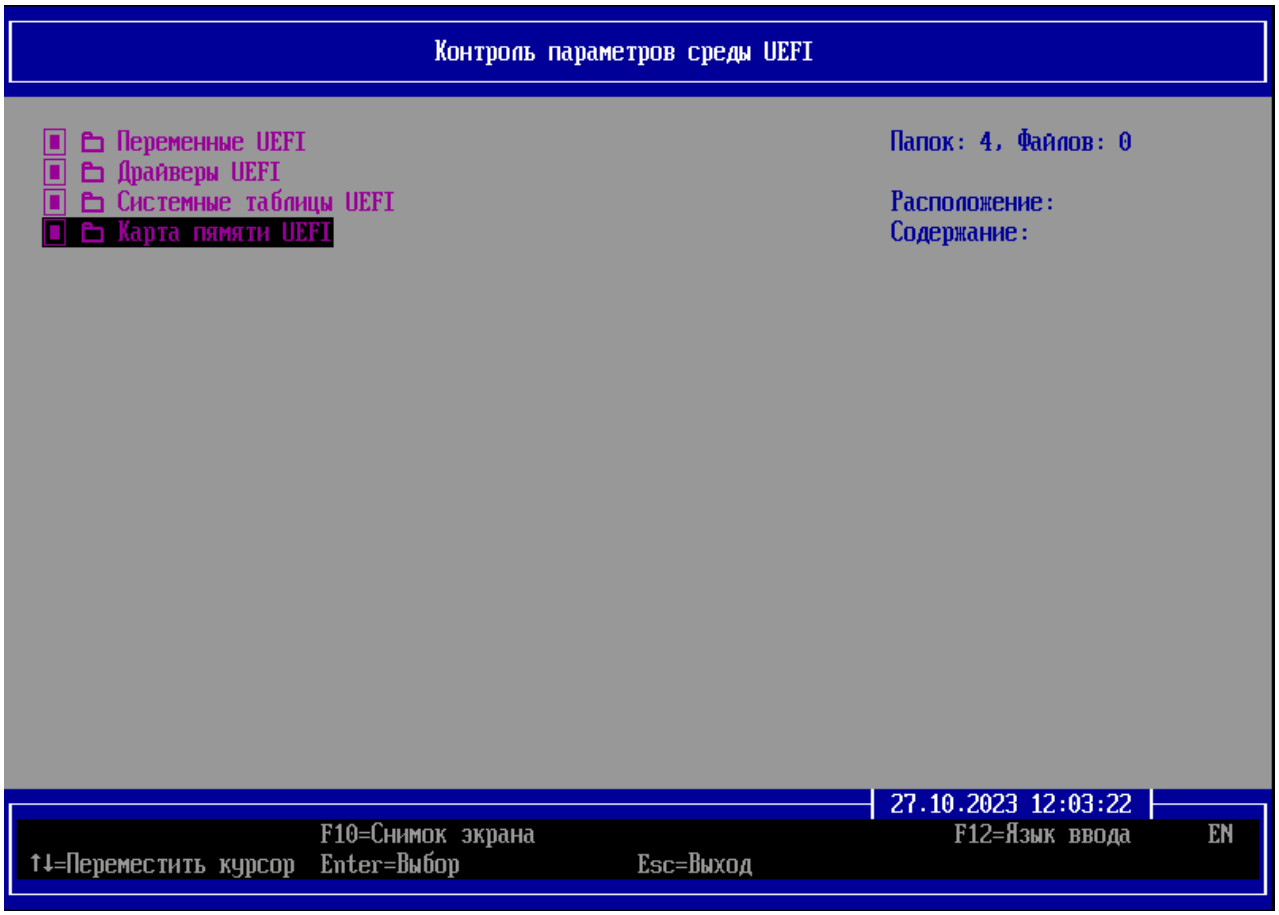


Рисунок 7.18 – Отображение контролируемых объектов среды UEFI

7.4.5 Процедура просмотра нарушений КЦ и исправления ошибок приведена в подразделе 6.8.

7.5 КЦ загрузочных секторов устройств хранения данных

7.5.1 При выборе в разделе ***«Контроль целостности»*** подраздела ***«Загрузочные сектора»*** (рисунок 4.2) и последующем выборе редактируемой политики КЦ и загрузки ОС (рисунок 6.7) на экране ЭВМ появится диалоговое окно (рисунок 7.19), содержащее список подключенных к ЭВМ устройств хранения данных и краткое описание их известных свойств. Наименования устройств хранения данных отображаются фиолетовым цветом (рисунок 7.19).

7.5.2 Установка на КЦ загрузочных секторов и их удаление с КЦ осуществляется по правилам, указанным в подразделе 7.1.

7.5.3 Установленные на КЦ объекты отображаются зеленым цветом (рисунок 7.20).

7.5.4 Процедура просмотра нарушений КЦ и исправления ошибок приведена в подразделе 6.8.

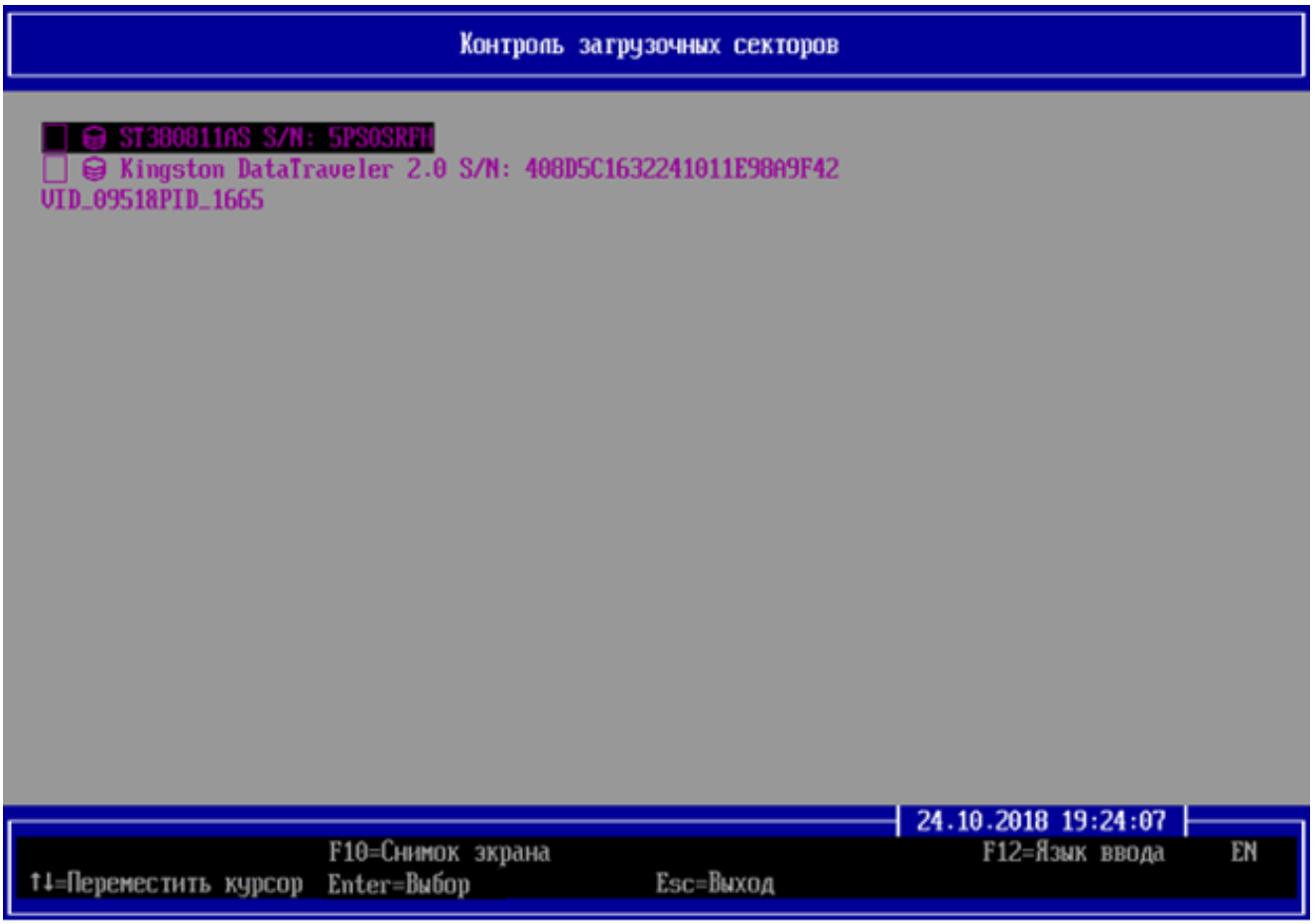


Рисунок 7.19 – Настройка КЦ загрузочных секторов

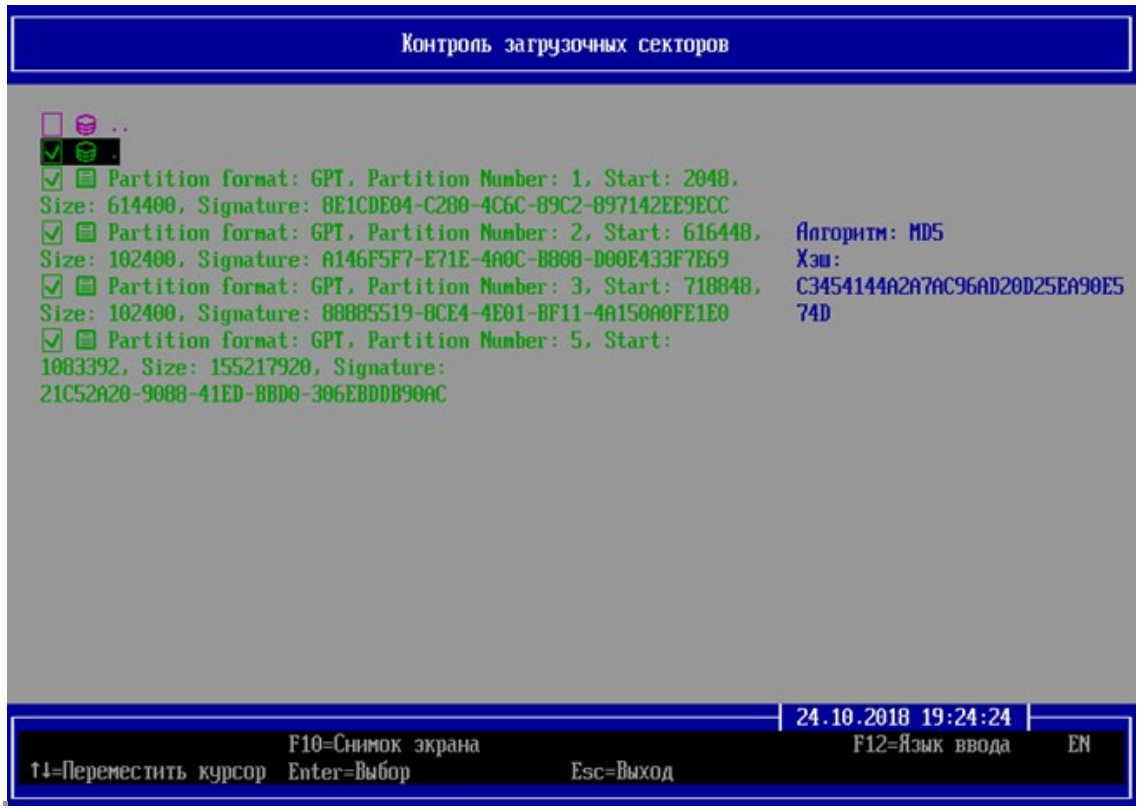


Рисунок 7.20 – Установленные на КЦ загрузочные сектора

Невозможна установка на КЦ устройства CD/DVD-ROM, не содержащего подключенный носитель CD/DVD.

При попытке установки на контроль такого устройства АБ на экран ЭВМ будет выведено сообщение об ошибке (рисунок 7.21).

Рисунок 7.21 – Ошибка установки на КЦ

7.6 КЦ аппаратных устройств ЭВМ

7.6.1 При выборе в разделе ***«Контроль целостности»*** раздела ***«Устройства»*** (рисунок 4.2) и последующем выборе редактируемой политики КЦ и загрузки ОС (рисунок 6.7) на экране ЭВМ появится диалоговое окно (рисунок 7.22), содержащее список аппаратных устройств ЭВМ. Наименования устройств отображаются фиолетовым цветом (рисунок 7.22).

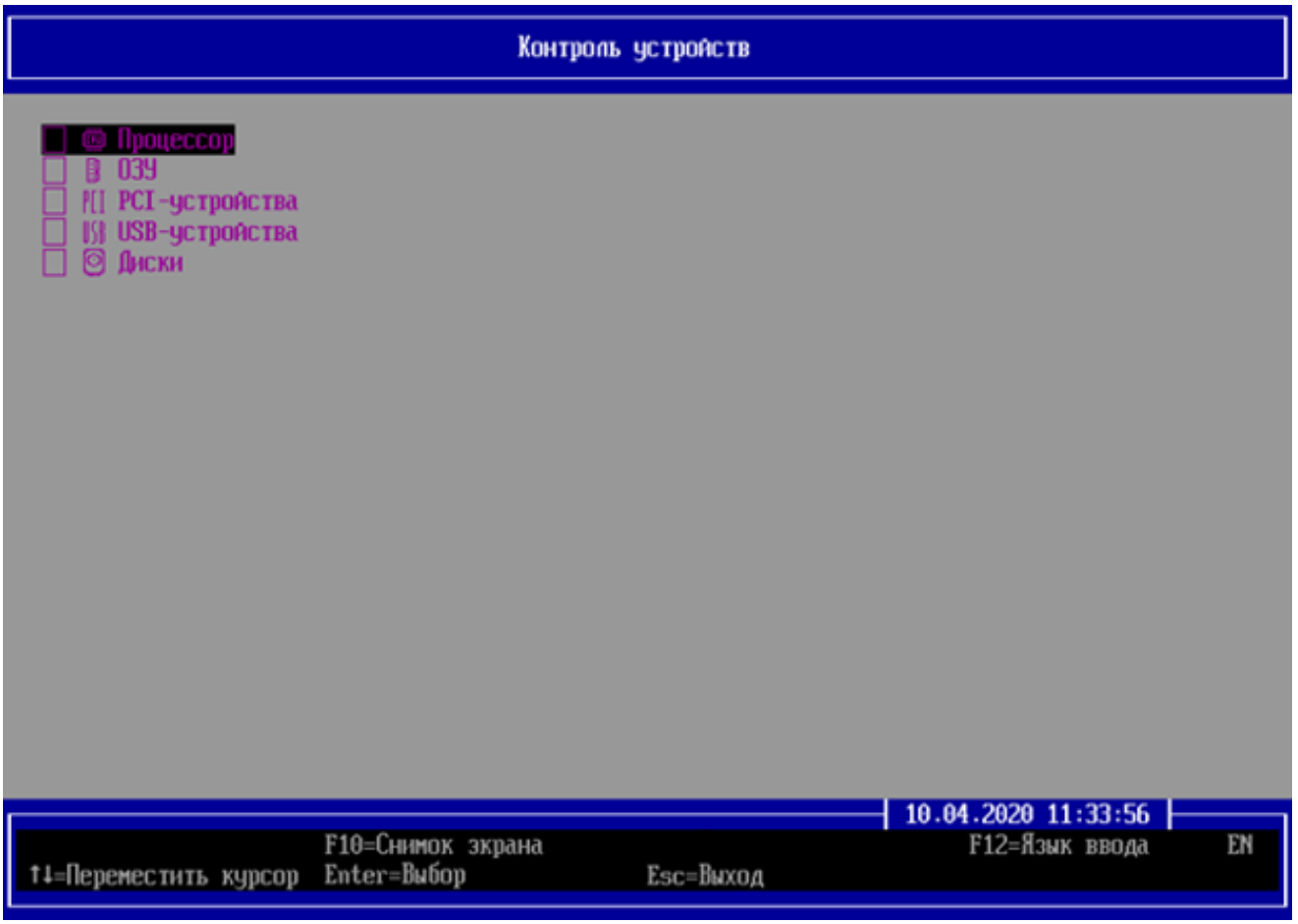


Рисунок 7.22 – Настройка КЦ устройств

7.6.2 Установка на КЦ устройств и их удаление с КЦ осуществляется по правилам, указанным в подразделе 7.1.

7.6.3 Установленные на КЦ объекты отображаются зеленым цветом (рисунок 7.23).

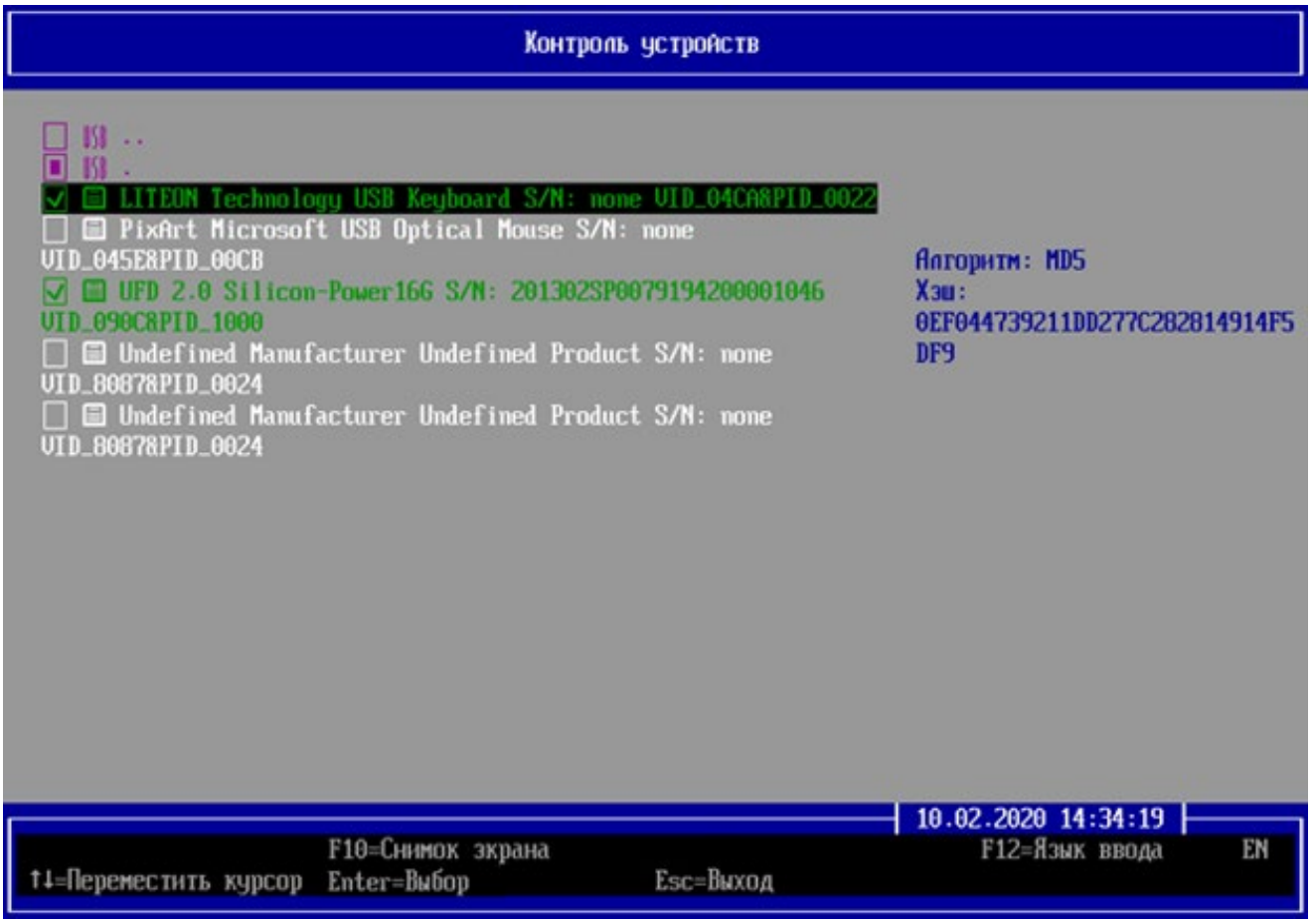


Рисунок 7.23 – Установленные на КЦ USB-устройства

7.6.4 В окне ***«Контроль устройств»*** полностью установленный на контроль каталог со всеми устройствами будет отображаться как ☑. Если в каталоге установлены на контроль выборочные устройства из списка, каталог будет отображаться как ■ (рисунок 7.24).

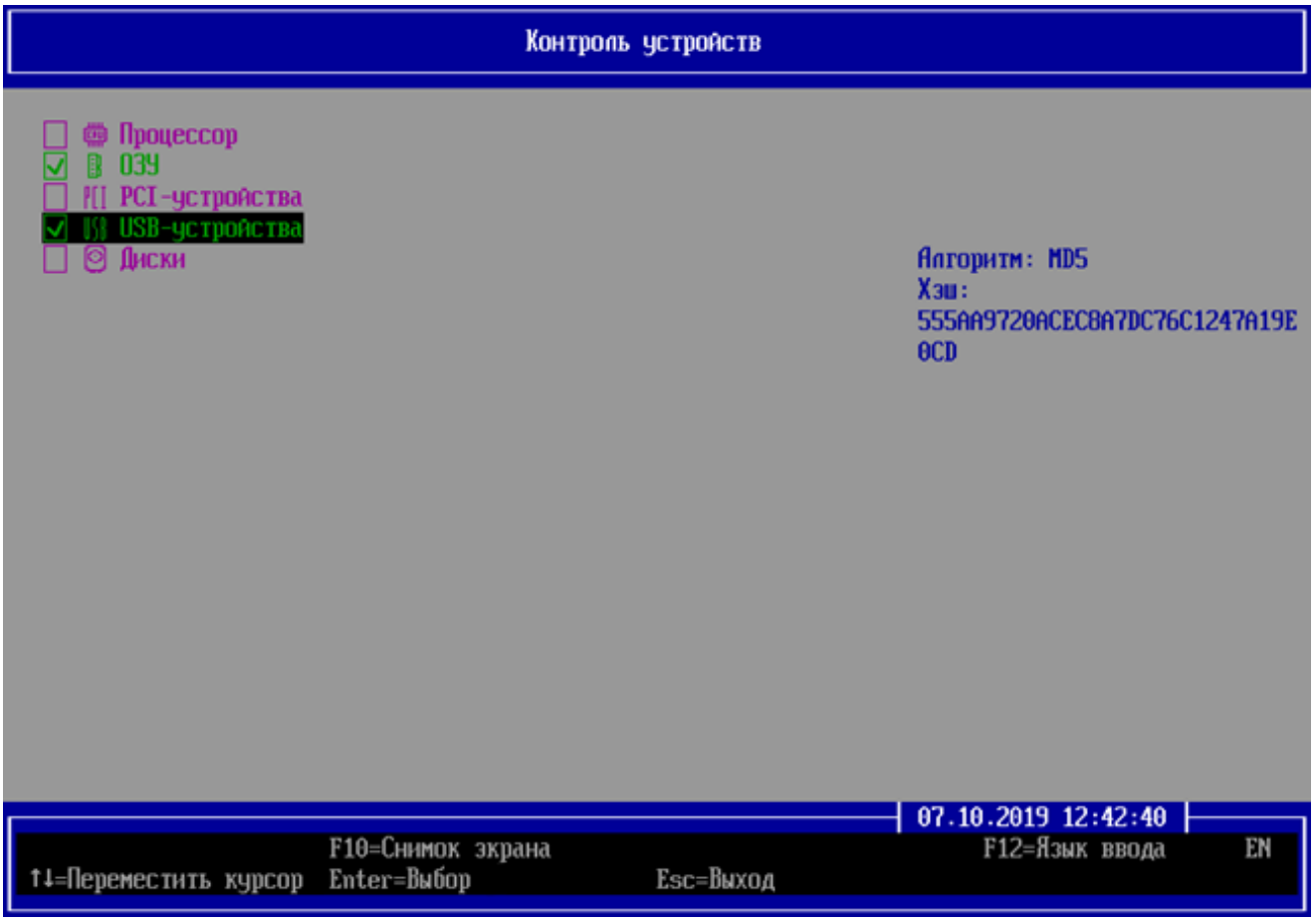


Рисунок 7.24 – Отображение контролируемых устройств

7.6.5 Процедура просмотра нарушений КЦ и исправления ошибок приведена в подразделе 6.8.

Добавленное на КЦ USB-устройство будет недоступно пользователю только во время доверенной загрузки ОС!

После загрузки ОС пользователем устройство будет доступно пользователю из среды ОС. Для ограничения доступа пользователей к устройствам во время их работы с ОС следует использовать средства защиты информации от несанкционированного доступа.

При эксплуатации изделия на некоторых ЭВМ (например, Acer Veriton N4660G) необходимо изменить значение параметра ***«Режим SATA»*** в BIOS Setup с значения «RST with Optane» на ***«AHCI»***.

7.7 Контроль загрузки ОС

7.7.1 При выборе в разделе ***«Управление загрузкой ОС»*** подраздела ***«Контроль загрузки ОС»*** (рисунок 4.2) и последующем выборе редактируемой политики КЦ и загрузки ОС (рисунок 6.7) на экране ЭВМ появится диалоговое окно (рисунок 7.25), содержащее список установленных ОС на данной ЭВМ.

7.7.2 Установленные на ЭВМ ОС для режима загрузки **UEFI** отображаются на экране голубым цветом, для режима загрузки **Legacy Boot** – фиолетовым цветом (рисунок 7.25).

7.7.3 Для установки ОС в качестве доверенной для загрузки пользователем необходимо выделить ее курсором и нажать клавишу **< *Enter* >**. Установленные для доверенной загрузки пользователям ОС отображаются зеленым цветом (рисунок 7.25).

7.7.4 ПО изделия осуществляет доверенную загрузку:

- 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;
- ОС на ЭВМ со стандартным Legacy/PnP BIOS (в режиме «Legacy Boot», спецификация PnP BIOS версии 1.0A);
- ОС на ЭВМ с интерфейсами EFI/UEFI (спецификация UEFI версии не ниже 2.0);
- ОС с MBR и GPT-разделов.

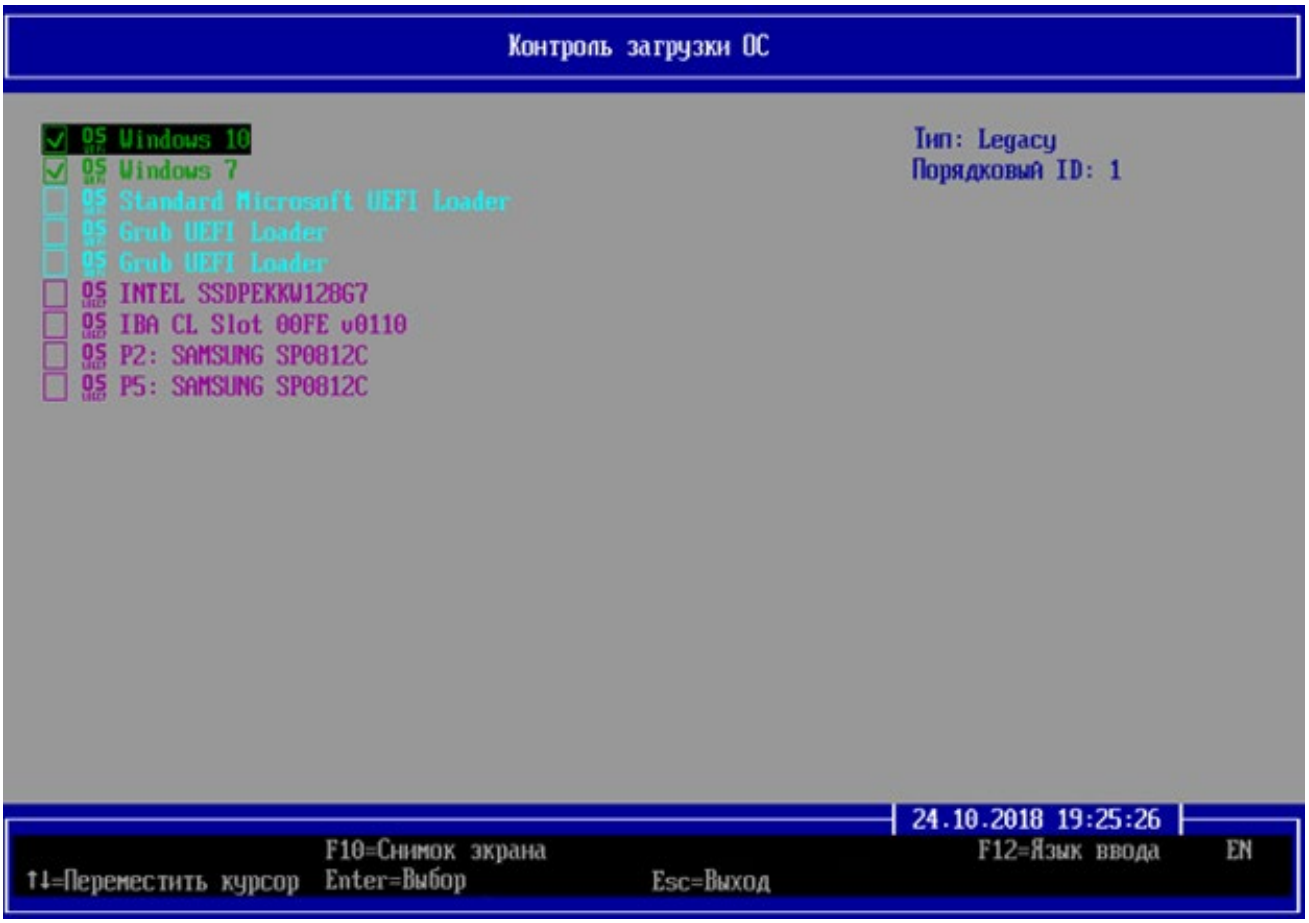


Рисунок 7.25 – Выбор ОС для доверенной загрузки пользователям

Установка нескольких ОС на единый MBR раздел устройства хранения данных повлечет за собой невозможность разграничить доступ пользователя к загрузке этих ОС.

В списке операционных систем для доверенной загрузки будет отображаться только загрузчик ОС.

При этом разграничить список ОС для доверенной загрузки пользователю будет невозможно.

7.7.5 Появление в списке отсутствующей ОС, отмеченной символом D (рисунок 7.26), означает, что ОС, определенная для доверенной загрузки, удалена с ЭВМ. При снятии данной отметки ОС удаляется из списка.

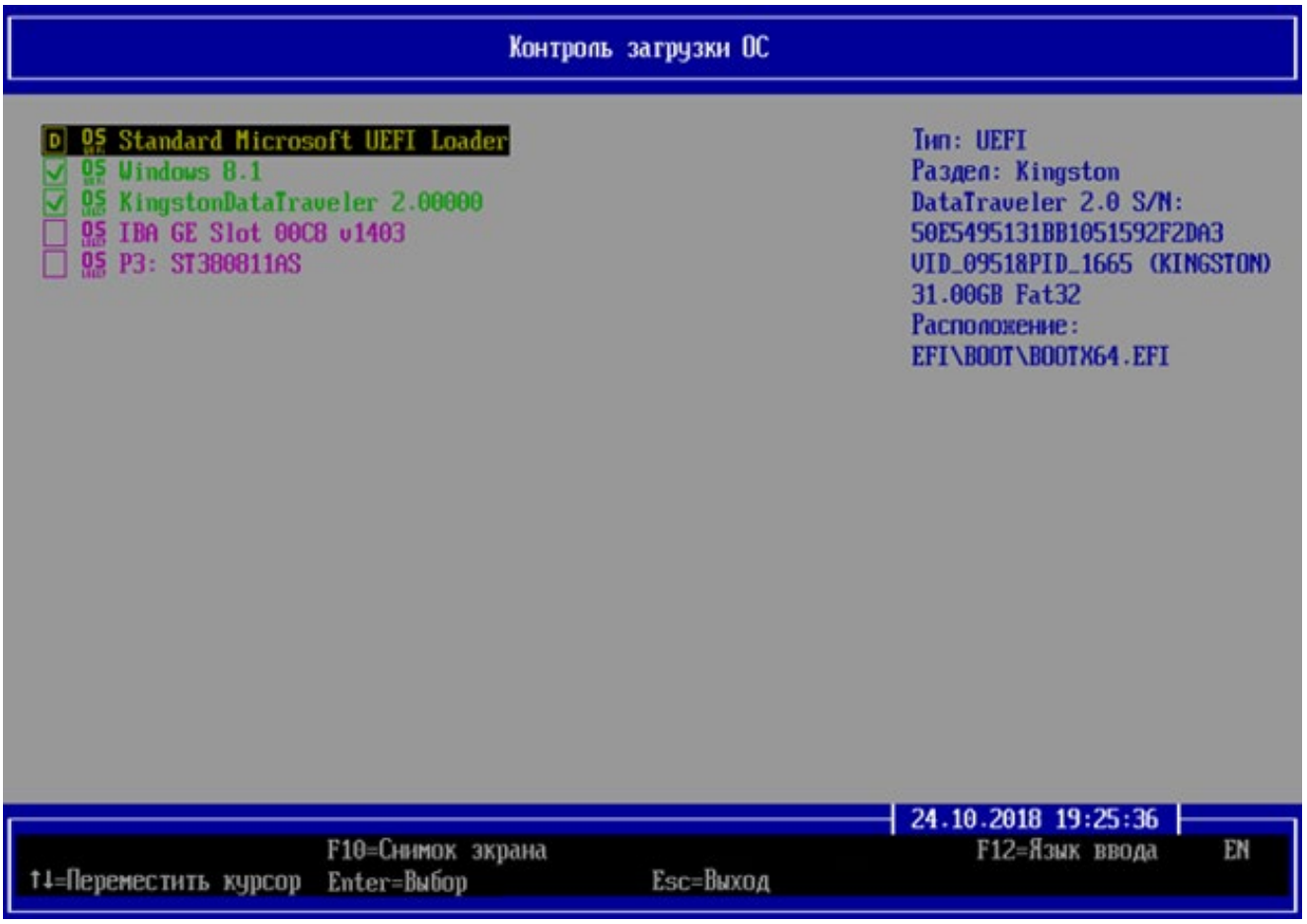


Рисунок 7.26 – Отображение удаленных ОС

8 Управление политиками аутентификации пользователей

8.1 Создание политики аутентификации пользователей

8.1.1 Для создания новой политики аутентификации пользователей АБ необходимо в главном окне консоли АБ (рисунок 4.2) выбрать подраздел «***Политики аутентификации пользователей»***. В появившемся диалоговом окне необходимо перейти в строку ***«Создание»*** и нажать клавишу **< *Enter* >** (рисунок 8.1).

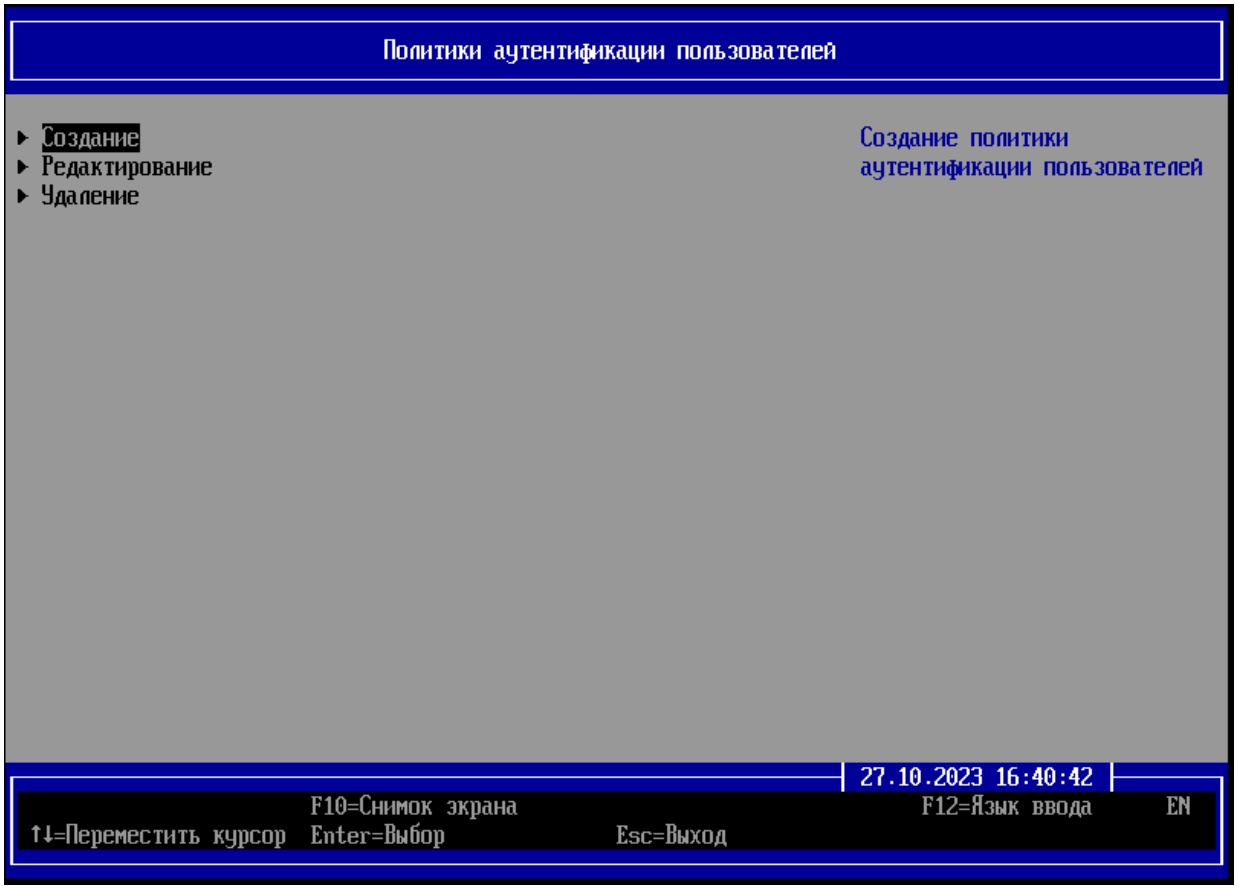


Рисунок 8.1 – Создание политики аутентификации пользователей

8.1.2 В новом диалоговом окне ***«Создание политики аутентификации пользователей»*** (рисунок 8.4) необходимо ввести имя создаваемой политики аутентификации пользователей в поле ***«Имя»*** (рисунок 8.2).

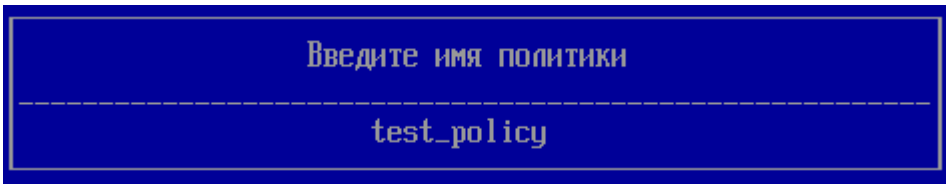


Рисунок 8.2 – Ввод имени политики аутентификации пользователей

Имя политики аутентификации пользователей является уникальным и не может быть дублировано. Если новое имя совпадает с уже имеющимся в БД, будет выведено предупреждающее сообщение ***«Политика с указанным именем уже существует»*** (рисунок 8.3).

Рисунок 8.3 – Ошибка при создании политики аутентификации пользователей

8.1.3 В таблице 8.1 приведены поля и их возможные значения при создании политики аутентификации пользователя (рисунок 8.4).

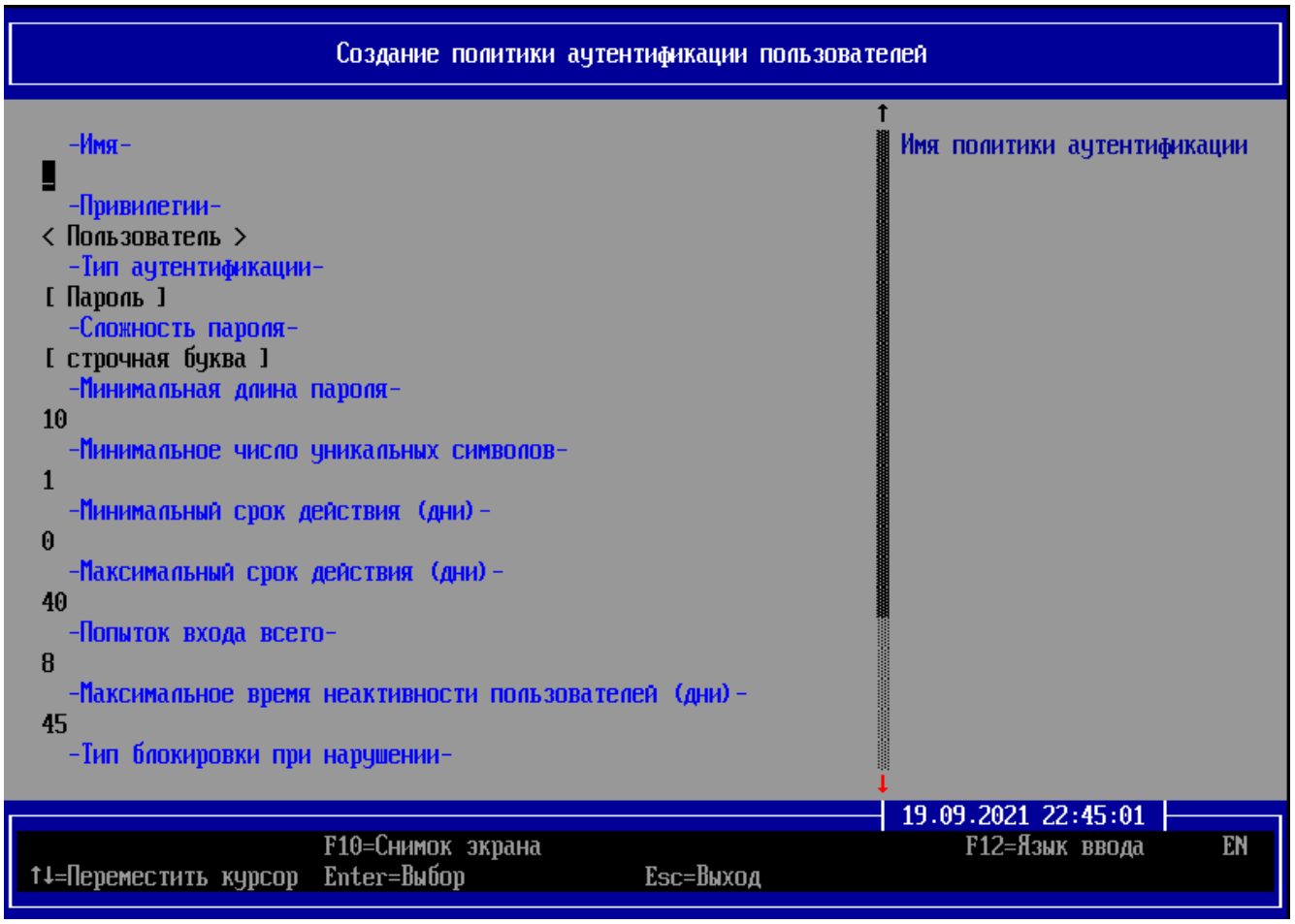


Рисунок 8.4 – Создание политики аутентификации пользователей

Таблица 8.1 – Возможные значения полей при создании политики аутентификации пользователя

№	Наименование поля	Возможные значения поля [по умолчанию]	Минимальное … максимальное значения	Примечание
1	Имя	Введенное значение		Уникальное название, не может быть дублировано
2	Привилегии	Пользователь		
3	Тип аутентификации	[Пароль] Персональный идентификатор Пароль и персональный идентификатор		
4	Сложность пароля	[строчная буква]		Поле предназначено для установки сложности

№	Наименование поля	Возможные значения поля [по умолчанию]	Минимальное … максимальное значения	Примечание
		заглавная буква цифра специальный символ		пароля. Активируется при нажатии клавиши **< *Enter* >**
5	Минимальная длина пароля	10	8…32	
6	Минимальное число уникальных символов	1	1…10	Минимальное число уникальных символов в пароле
7	Минимальный срок действия (дни)	0	0…45	Меньше или равно максимальному сроку действия. При установке значения параметра «0» смена пароля возможна с текущей даты
8	Максимальный срок действия (дни)	40	1…45	
9	Попыток входа всего	8	1…8	
10	Максимальное время неактивности пользователя (дни)	45	1…45	
11	Тип блокировки при нарушении	Временная блокировка пользователя [Блокировка пользователя] Блокировка группы пользователя Блокировка всех пользователей		
12	Время блокировки (минуты)	15	1…60	
13	Блокирование общеизвестных паролей	[Отключено] Включено		При активации данного поля добавляется список популярных паролей, запрещенных к использованию. При необходимости, можно выделить требуемые пароли и исключить их из

№	Наименование поля	Возможные значения поля [по умолчанию]	Минимальное … максимальное значения	Примечание
				перечня с помощью кнопки «Удалить выделенные»

Параметры политики аутентификации пользователя ***«Сложность пароля», «Минимальная длина пароля», «Минимальное число уникальных символов», «Минимальный срок действия (дни)», «Максимальный срок действия (дни)», «Попыток входа всего», «Максимальное время неактивности пользователей (дни)»*** возможно полностью отключить. При этом в политике аутентификации пользователей снимаются все ограничения, заданные в данных параметрах.

8.1.4 После установки полей для сохранения изменений в создаваемой политике аутентификации необходимо перейти в строку ***«Сохранить»*** (рисунок 8.4) и нажать клавишу **< *Enter* >**. При этом в новом диалоговом окне будет выведено сообщение об успешном создании политики аутентификации пользователя (рисунок 8.5).

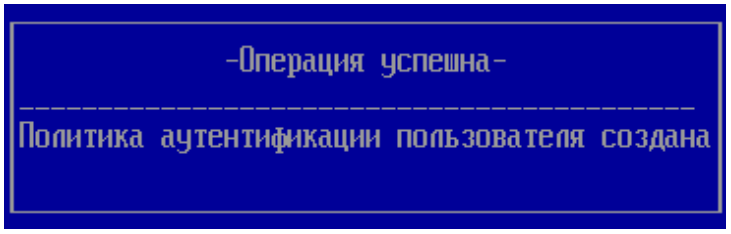


Рисунок 8.5 – Успешное создание политики аутентификации пользователей

В ПО изделия установлено ограничение на создание политик аутентификации.

Установлено ограничение на количество создаваемых политик аутентификации – не более 20 политик аутентификации.

При превышении установленного максимального количества политик аутентификации, будет выведено сообщение *«Достигнут лимит создания политик»* и операция сохранения политики выполнена не будет (рисунок 6.7).

Пользователям предоставлена возможность смены паролей без привлечения АБ. По истечении минимального срока действия политики пользователь может изменить его на основе правил, заданных АБ (минимальная длина, сложность, минимальный и максимальный сроки действия). Принудительная смена пароля обеспечивается по истечении максимального срока действия пароля.

В графической консоли СДЗ, запускаемой в среде Windows или Linux, реализована возможность редактирования списка популярных паролей, запрещенных к использованию, после активации поля ***«Блокирование общеизвестных паролей»*** при создании политики аутентификации (см. подробнее «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 3. руководство администратора Linux/Windows» раздел 8 «Управление политиками аутентификации пользователей»). В случае, если политика аутентификации была создана с помощью данных консолей, то правила смены пароля будут распространяться на псевдографическую консоль СДЗ.

8.2 Редактирование политики аутентификации пользователей

8.2.1 Для редактирования существующей политики аутентификации пользователей необходимо выбрать в главном окне (рисунок 4.2) подраздел «***Политики аутентификации пользователей»***. В появившемся диалоговом окне необходимо перейти в строку ***«Редактирование»*** и нажать клавишу **< *Enter* >** (рисунок 8.6).

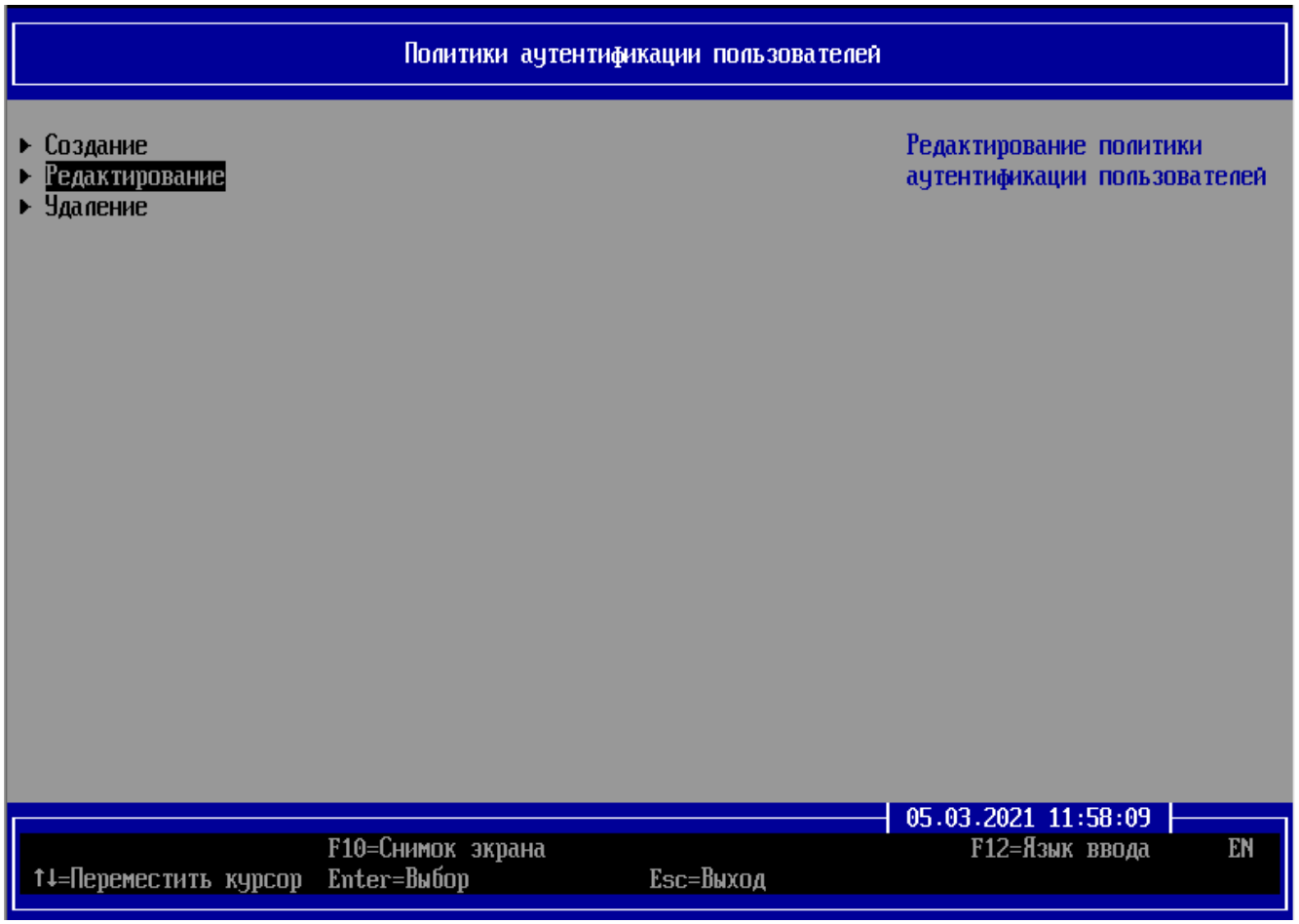


Рисунок 8.6 – Конфигурирование политики аутентификации пользователей

8.2.2 В новом диалоговом окне ***«Редактирование политики аутентификации пользователей»*** (рисунок 8.7) необходимо выбрать имя редактируемой политики аутентификации пользователей в поле ***«Имя»*** и нажать кнопку **| *ОК* |** (рисунок 8.8).

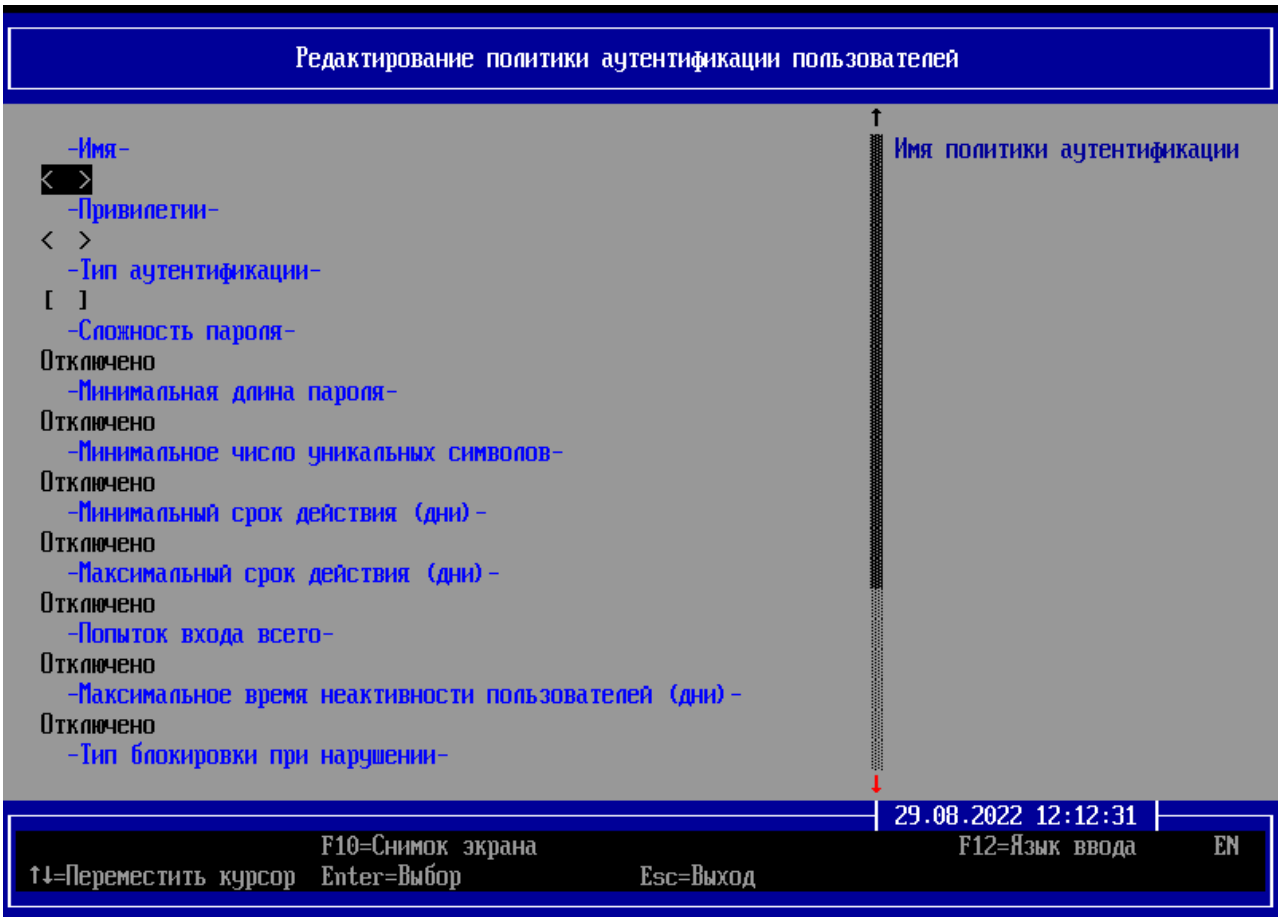


Рисунок 8.7 – Редактирование политики аутентификации пользователей

Рисунок 8.8 – Выбор политики аутентификации пользователей для редактирования

8.2.3 Доступные для редактирования параметры политики аутентификации пользователя (рисунок 8.9) и их значения приведены в таблице 8.1.

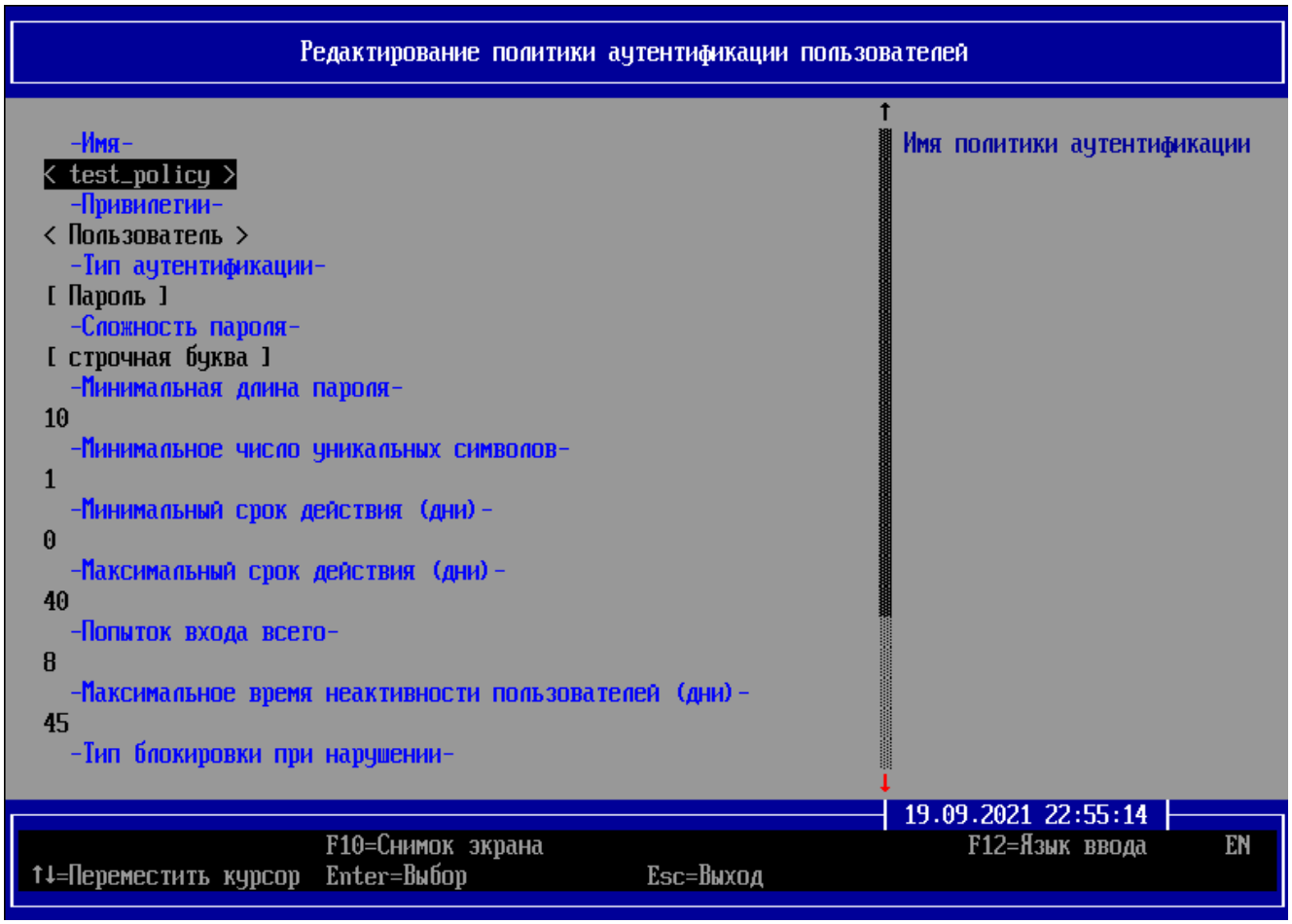


Рисунок 8.9 – Редактируемые поля политики аутентификации пользователей

8.2.4 Для сохранения изменений редактируемой политики аутентификации необходимо перейти в строку ***«Сохранить»*** (рисунок 8.9) и нажать клавишу ***< Enter >***. При этом в новом диалоговом окне будет выведено сообщение об успешном редактировании политики аутентификации пользователя (рисунок 8.10).

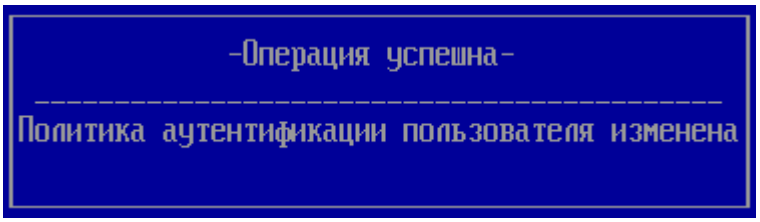


Рисунок 8.10 – Успешное редактирование политики аутентификации пользователей

8.3 Удаление политики аутентификации пользователей

8.3.1 Для удаления существующей политики аутентификации пользователей необходимо выбрать в главном окне (рисунок 4.2) подраздел «***Политики аутентификации пользователей»***. В появившемся диалоговом окне необходимо перейти в строку ***«Удаление»*** и нажать клавишу **< *Enter* >** (рисунок 8.11).

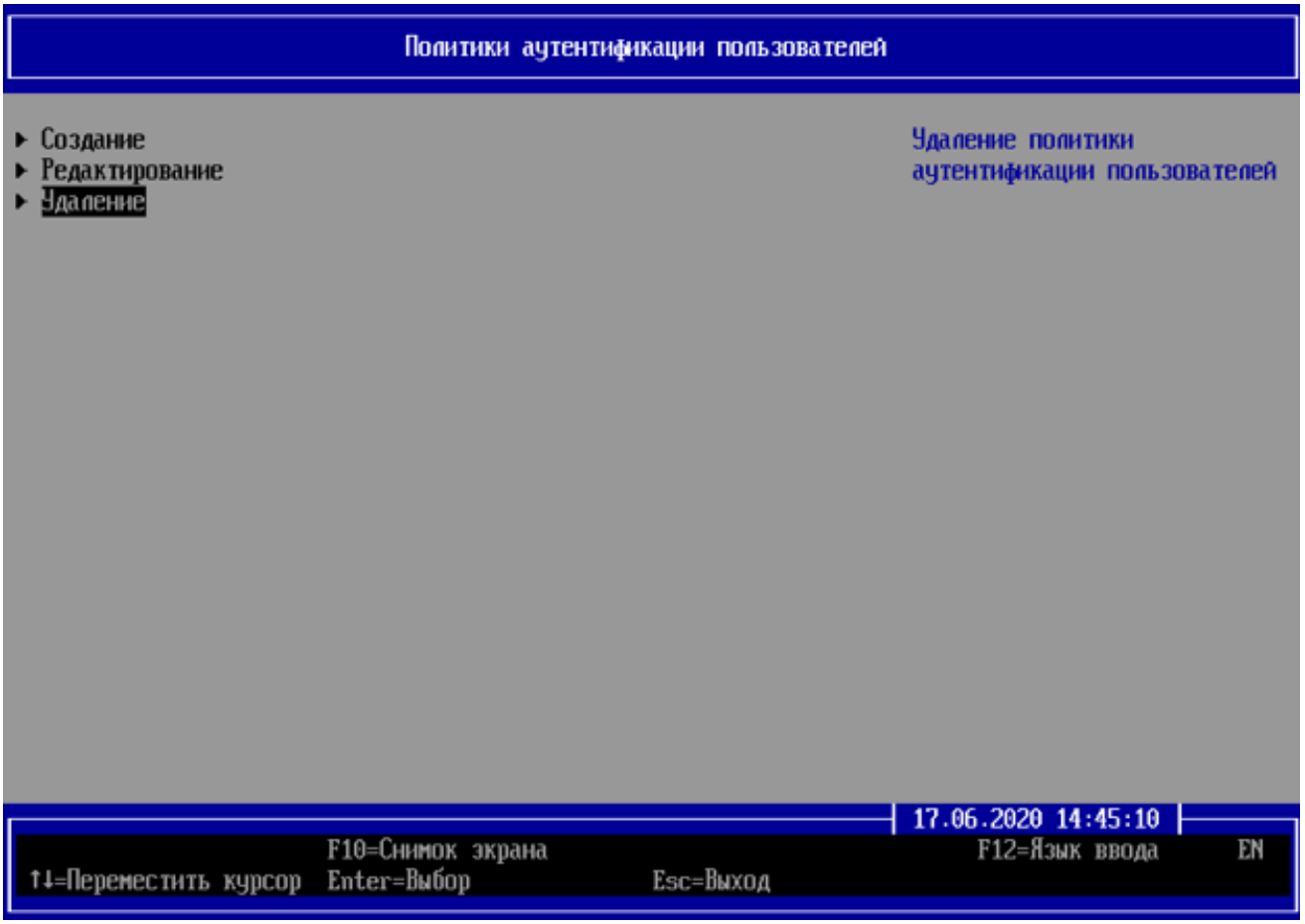


Рисунок 8.11 – Удаление политики аутентификации пользователей

8.3.2 В новом диалоговом окне ***«Удаление политики аутентификации пользователей»*** (рисунок 812) необходимо выбрать имя удаляемой политики аутентификации пользователей в поле ***«Имя»*** и нажать кнопку **| *ОК* |** (рисунок 8.13).

Рисунок 8.12 – Выбор для удаления политики аутентификации пользователей

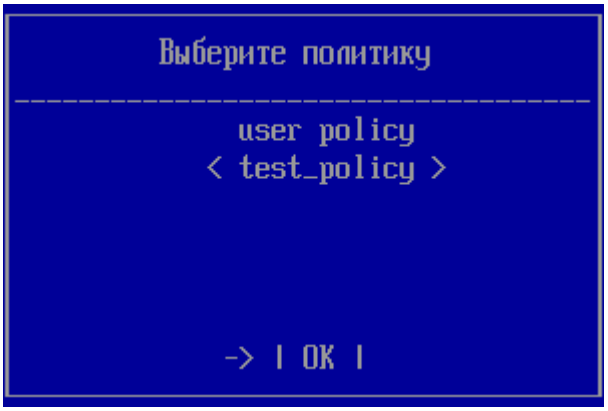


Рисунок 8.13 – Выбор для удаления политики аутентификации пользователей

8.3.3 Для удаления выбранной политики необходимо перейти в строку ***«Удалить»*** (рисунок 8.14) и нажать клавишу **< *Enter* >**. При этом в новом диалоговом окне будет выведено сообщение об успешном удалении политики аутентификации пользователей (рисунок 8.15).

Удаление политик аутентификации осуществляется поочередно.

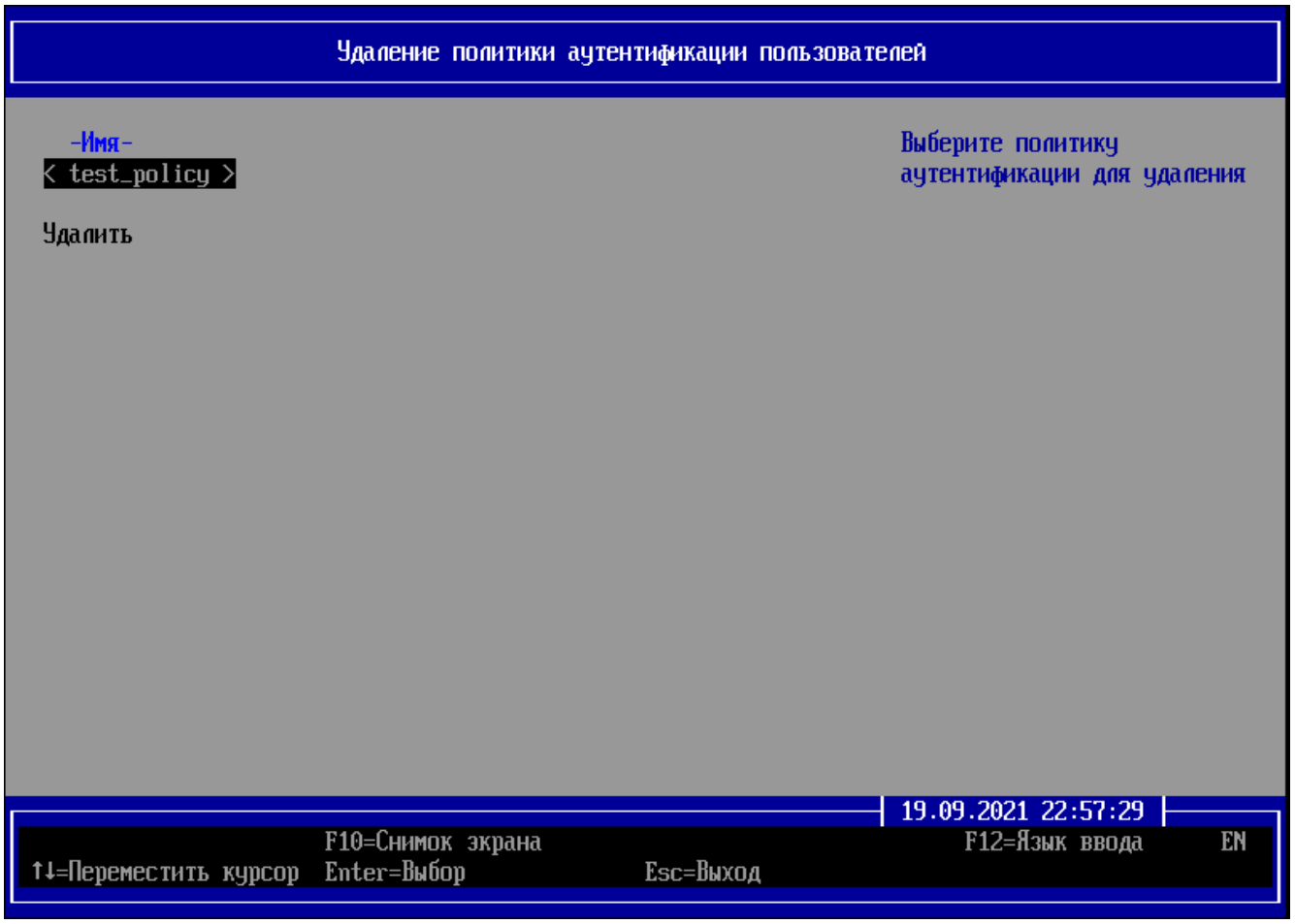


Рисунок 8.14 –Удаление политики аутентификации пользователей

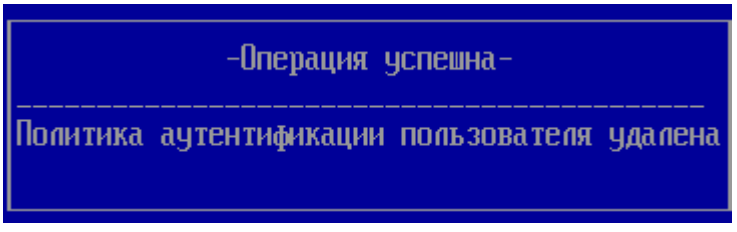


Рисунок 8.15 – Успешное удаление политики аутентификации пользователей

Если политика аутентификации назначена хотя бы одной учетной записи пользователя, удаление выполнено не будет и на экран ЭВМ будет выведено сообщение ***«Операция не выполнена. На данную политику ссылаются учетные записи пользователей»*** (рисунок 8.16).

Для удаления данной политики необходимо поочередно перейти в учетные записи пользователей, которым назначена данная политика, и отредактировать учетные записи путем назначения им другой политики аутентификации.

Затем действия по удалению политики необходимо повторить.

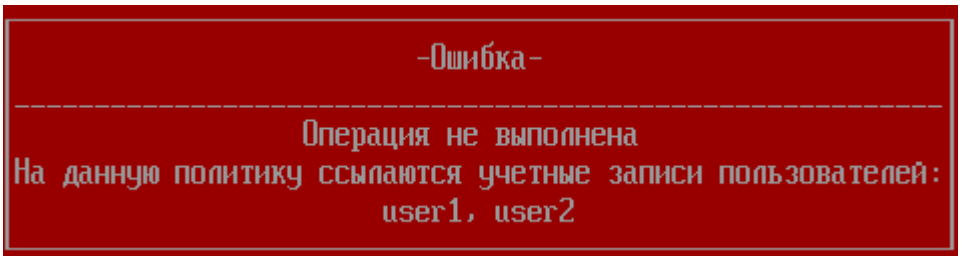


Рисунок 8.16 – Ошибка при удалении политики аутентификации пользователей

8.4 Автовход пользователей

8.4.1 В ПО изделия для созданных учетных записей пользователей доступна функция автовхода (за исключением учетной записи АБ).

8.4.2 При установке режима автовхода пользователь выполняет процедуру аутентификации и идентификации в автоматическом режиме с последующей доверенной загрузкой ОС. Режим автовхода доступен только с использованием персонального идентификатора.

8.4.3 Для включения режима автовхода пользователю АБ необходимо назначить учетной записи пользователя политику аутентификации пользователя с типом аутентификации по персональному идентификатору. Далее необходимо перейти в подраздел ***«Основные настройки»*** основного окна консоли АБ и указать в пункте ***«Автовход»*** имя необходимой учетной записи (рисунок 8.17).

8.4.4 При установленном режиме автовхода, наличии подключенного АНП и отсутствии ошибок аутентификации и идентификации и КЦ, будет осуществлена доверенная загрузка ОС, назначенной в политике КЦ объектов и загрузке ОС в учетной записи пользователя.

8.4.5 В случае отсутствия подключенного АНП автовход в систему выполнен не будет и на экране ЭВМ будет выведено диалоговое окно с приглашением аутентификации и идентификации пользователя (рисунок 12.1).

8.4.6 При обнаружении нарушения целостности объектов, автовход в систему выполнен не будет, учетная запись пользователя будет заблокирована и на экран ЭВМ будет выведено сообщение о блокировке доступа (рисунок 6.22).

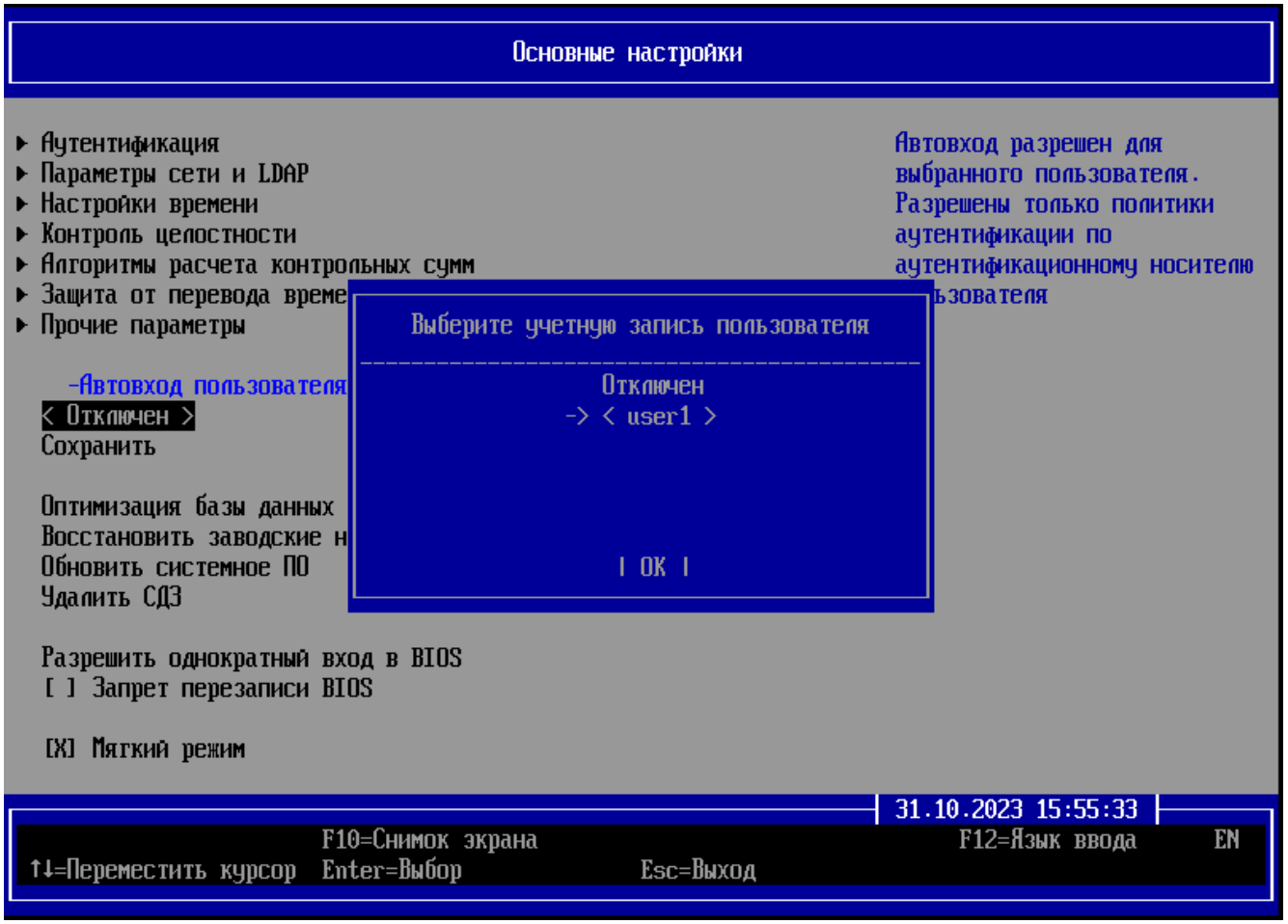


Рисунок 8.17 – Настройка автовхода для учетной записи пользователя

Функция автовхода доступна только одной зарегистрированной учетной записи пользователя. Если в политике КЦ объектов и загрузки ОС, назначенной пользователю, добавлено несколько ОС как доверенных к загрузке, будет выбрана первая ОС из списка.

9 Управление учетными записями пользователей

9.1 Создание учетной записи пользователя

В изделии добавлен предустановленный пользователь ***user*** для возможности загрузки ОС администратором без регистрации нового пользователя. Пользователю установлен пароль по умолчанию ***12345678*** и предустановленные политики – политика контроля целостности и загрузки ОС ***all users*** и политика аутентификации ***user policy***. Пароль пользователя необходимо сменить до первого выхода из мягкого режима иначе пользователь будет заблокирован.

9.1.1 Для создания новой учетной записи пользователя необходимо выбрать в главном окне консоли АБ (рисунок 4.2) подраздел «***Учетные записи пользователей»***. В появившемся диалоговом окне необходимо перейти в строку ***«Создание»*** и нажать клавишу **< *Enter* >** (рисунок 9.1).

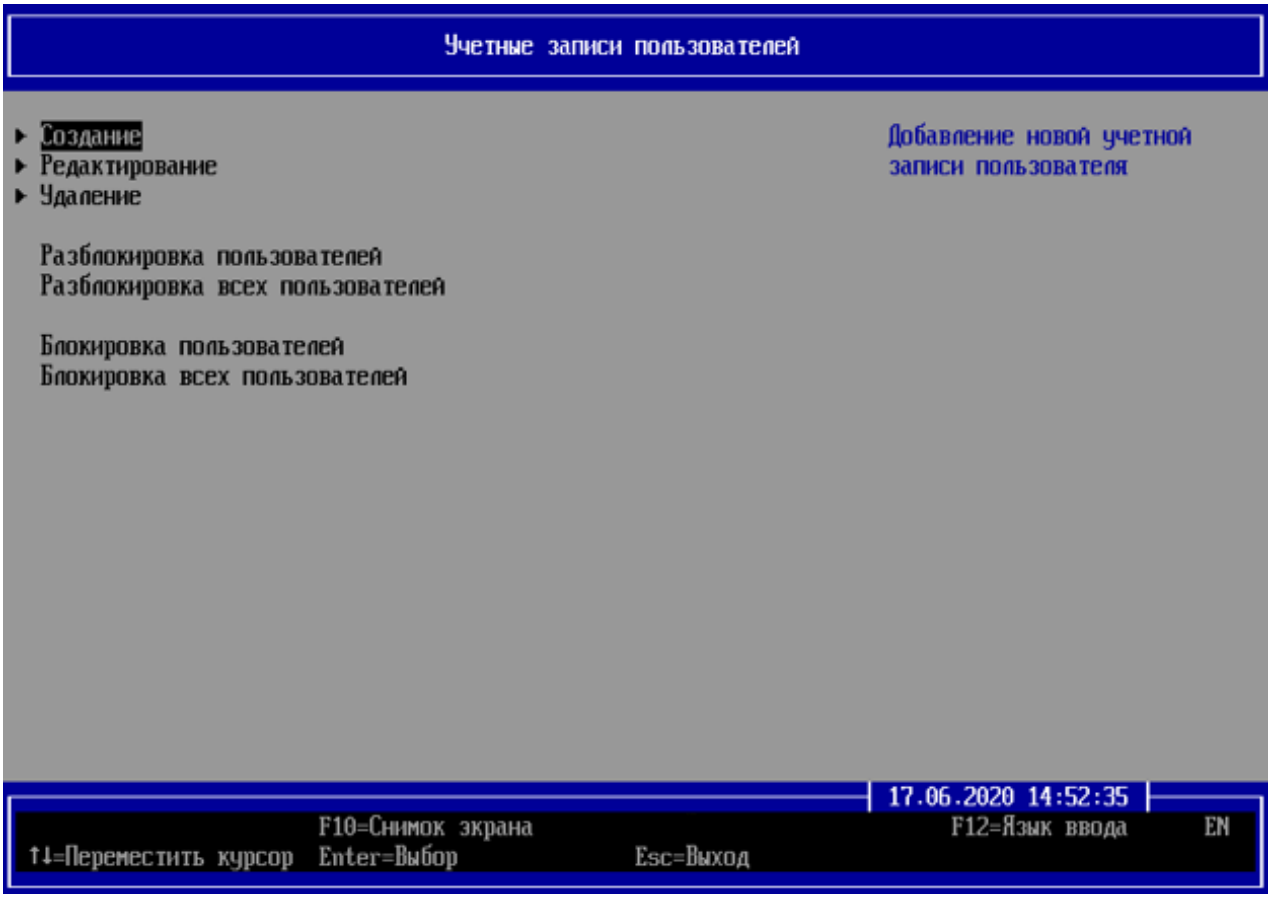


Рисунок 9.1 – Конфигурирование учетной записи пользователя

9.1.2 В новом диалоговом окне ***«Создание учетной записи пользователя»*** (рисунок 9.2) в поле ***«Имя пользователя»*** ввести имя создаваемой учетной записи (рисунок 9.3).

9.1.3 Диалоговое окно ***«Создание учетной записи пользователя»*** после ввода имени пользователя примет вид (рисунок 9.4).

9.1.4 В таблице 9.1 приведены поля и их возможные значения при создании учетной записи пользователя (рисунок 9.2).

Сложность пароля или PIN-кода персональных идентификаторов пользователей определяется путем использования в нем сочетания заглавных букв, строчных букв, цифр и специальных символов из определенного разработчиком алфавита пароля, приведенного в таблице 5.2.

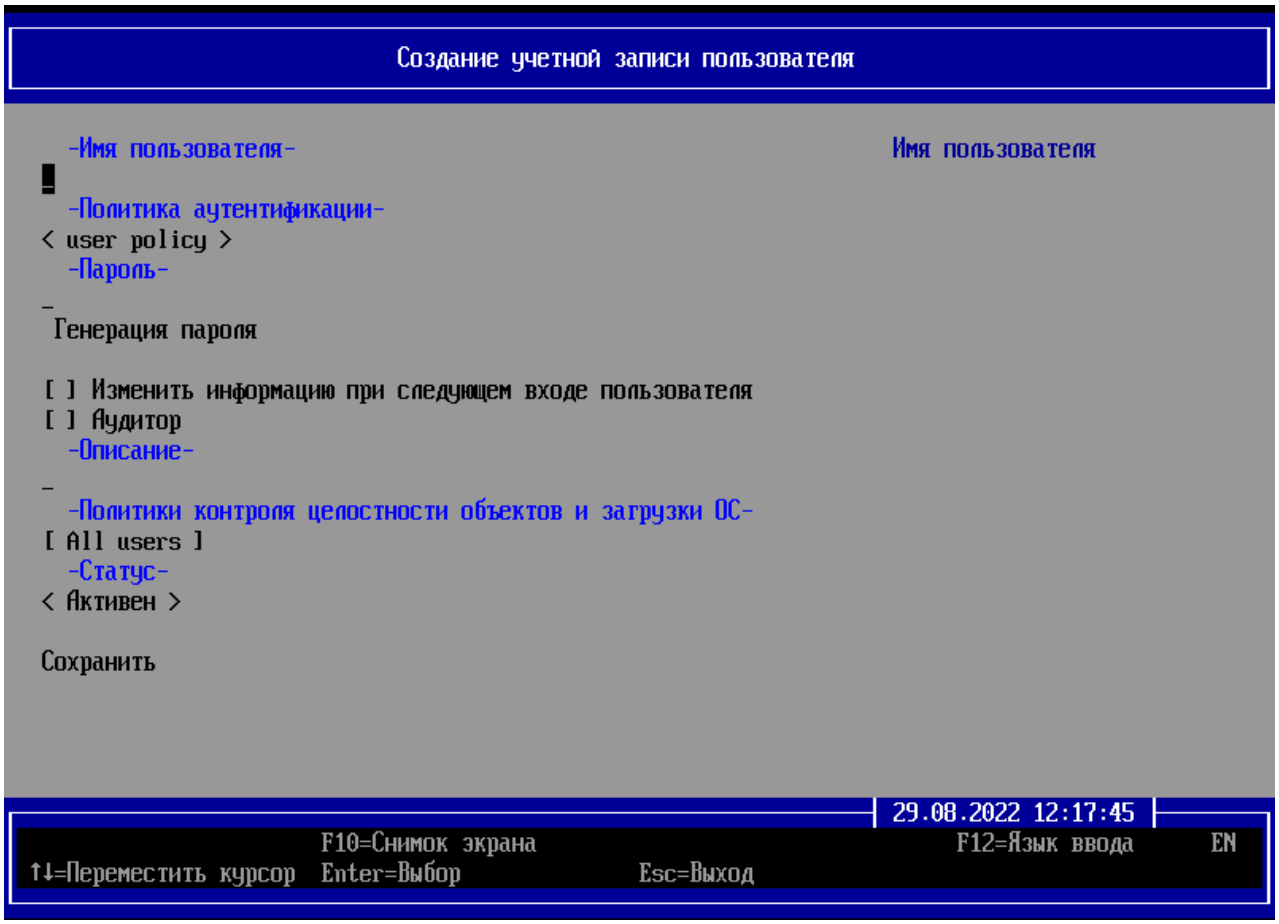


Рисунок 9.2 – Создание учетной записи пользователя

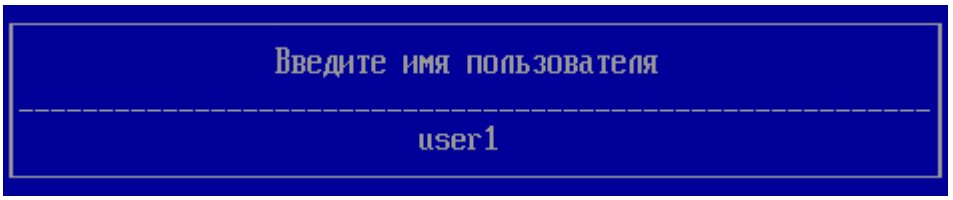


Рисунок 9.3 – Ввод имени учетной записи пользователя

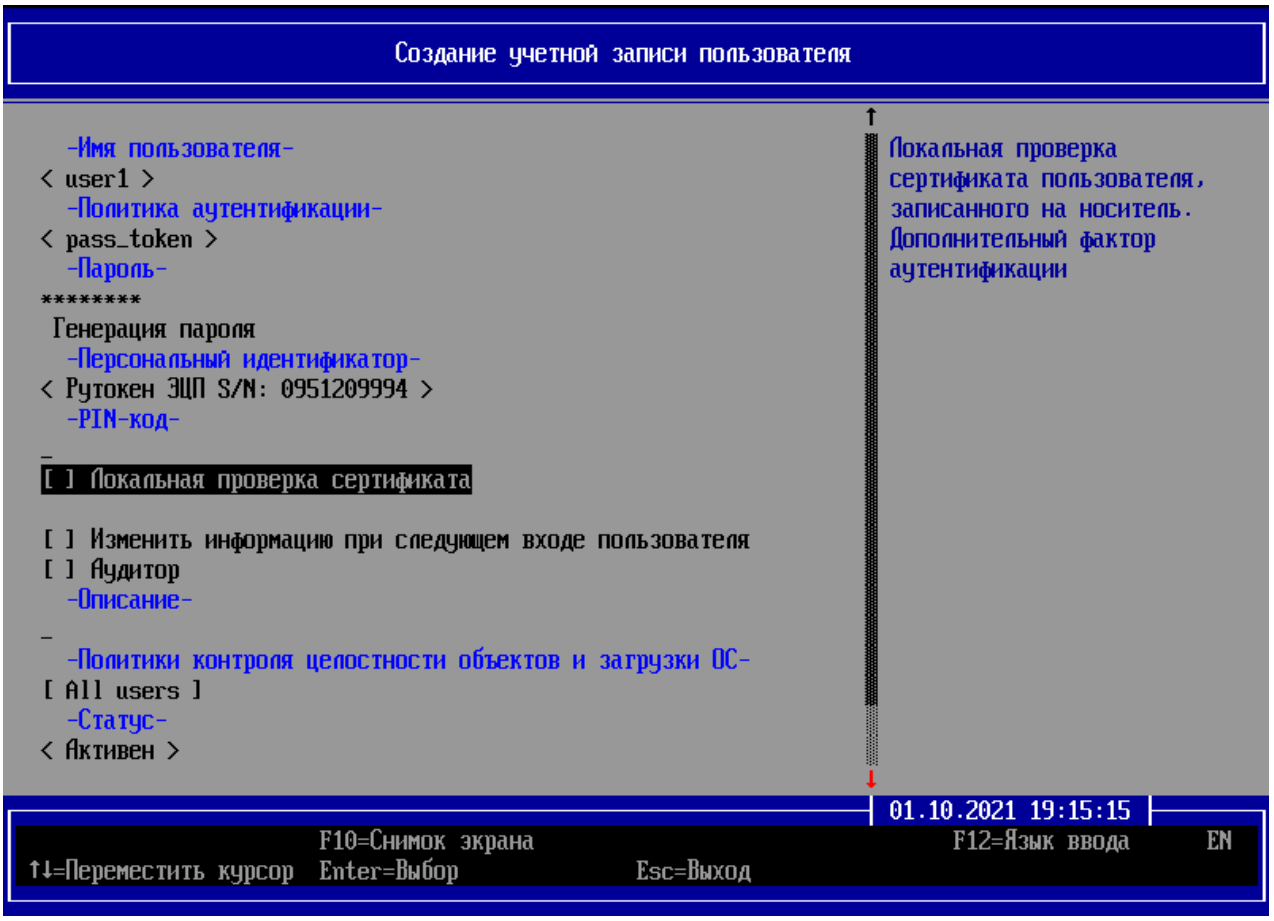


Рисунок 9.4 – Ввод параметров учетной записи пользователя

Таблица 9.1 – Поля и их возможные значения при создании учетной записи пользователя

№	Наименование поля	Возможные значения поля [по умолчанию]	Примечание
1	Имя пользователя	Введенное значение	Уникальное название, не может быть дублировано. Максимальная длина имени учетной записи пользователя – 256 символов. В имени учетной записи пользователя нельзя использовать: 1) первый символ не должен быть специальным символом или цифрой;

№	Наименование поля	Возможные значения поля [по умолчанию]	Примечание
			2) остальные символы не могут специальными символами
2	Политика аутентификации	Введенное значение	Указание названия политики аутентификации, по правилам которой будет обрабатываться данная учетная запись пользователя
3	Пароль	Значение пароля	Поле предназначено для установки пароля. **Допускается использование символов из таблицы 5.2.** Активируется при нажатии клавиши **< *Enter* >**
4	Генерация пароля	Значение пароля	Поле предназначено для генерации пароля с использованием программного ДСЧ. Активируется при нажатии клавиши **< *Enter* >**
5	Персональный идентификатор	Присвоенный персональный идентификатор	Поле предназначено для выбора и установки персонального идентификатора. Активируется при нажатии клавиши **< *Enter* >**
6	PIN-код	Значение PIN-кода	Поле предназначено для установки PIN-кода персонального идентификатора. **Допускается использование символов из таблицы 5.2.** Активируется при нажатии клавиши **< *Enter* >**
7	Изменить информацию при следующем входе пользователя	[Включено] Отключено	Принудительное изменение аутентификационных данных пользователя при его первой успешной аутентификации
8	Локальная проверка сертификата	[Отключено] Включено	С помощью данного параметра осуществляется аутентификация учетной записи пользователя с использованием сертификата для входа (имеют признак «Вход по смарт-карте»). Проверка сертификата осуществляется локально СДЗ. Дополнительный фактор аутентификации можно назначить как локальному, так и доменному пользователю. При выборе доменного пользователя, политика аутентификации СДЗ должна совпадать с доменной политикой. Внимание:

№	Наименование поля	Возможные значения поля [по умолчанию]	Примечание
			При изменении сертификата для входа на АНП необходимо повторно назначить носитель пользователю!
9	Аудитор	Включено [Отключено]	При назначении прав аудитора пользователю предоставляется дополнительная возможность просмотра и экспорта журнала аудита без его очистки
10	Описание	Произвольная текстовая строка	Поле предназначено для формирования описания учетной записи пользователя. Максимальная длина поля – 48 символов. Активируется при нажатии клавиши **< *Enter* >**
11	Политики контроля целостности и загрузки ОС	Введенное значение [All users]	Выбор названия политики КЦ и загрузки ОС, по правилам которой будет обрабатываться данная учетная запись пользователя
12	Статус	[Активен] Заблокирован	С помощью данного параметра осуществляется блокировка и разблокировка учетных записей пользователей, за исключением учетной записи АБ

9.1.5 В поле ***«Политика аутентификации»*** (рисунок 9.4) необходимо выбрать имя ранее созданной политики аутентификации пользователей (рисунок 9.5). Выбранная политика аутентификации выделена < треугольными скобками > (рисунок 9.5).

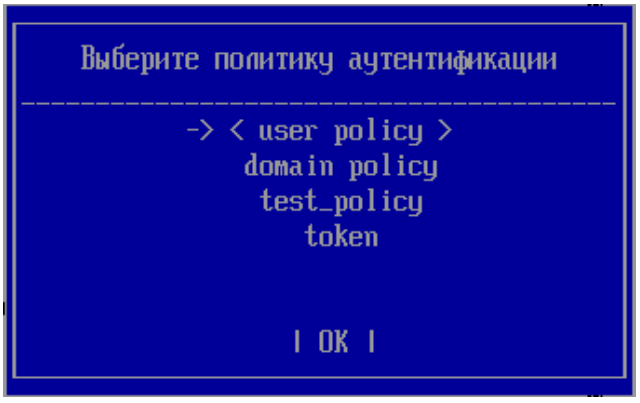


Рисунок 9.5 – Выбор политики аутентификации пользователей

9.1.6 В случае выбора политики аутентификации для входа с АНП, в качестве дополнительного фактора поддерживается использование сертификата пользователя. Необходимо подключить носитель, выбрать соответствующую политику, затем указать АНП и поле «Локальная проверка сертификата» (рисунок 9.4). Сертификат с признаком «Вход по смарт-карте» должен быть выпущен и записан на АНП заранее, для этого необходимо воспользоваться соответствующим PKI-клиентом или сервером СЗИ от НСД «Блокхост-Сеть 4».

Для входа по сертификату на токене поддерживается работа только с АНП Рутокен ЭЦП 2.0.

9.1.7 В случае, если сертификат на АНП стал некорректным (просрочен, изменен или перезаписан на носителе после назначения его пользователю в изделии) необходимо отредактировать соответствующую учетную запись пользователя и назначить ему АНП снова.[4]

9.1.8 В поле ***«Политики контроля целостности и загрузки ОС»*** (рисунок 9.4) необходимо выбрать имя ранее созданной политики КЦ объектов и загрузки ОС. Выбранные АБ политики будут [квадратными скобками] (рисунок 9.6).

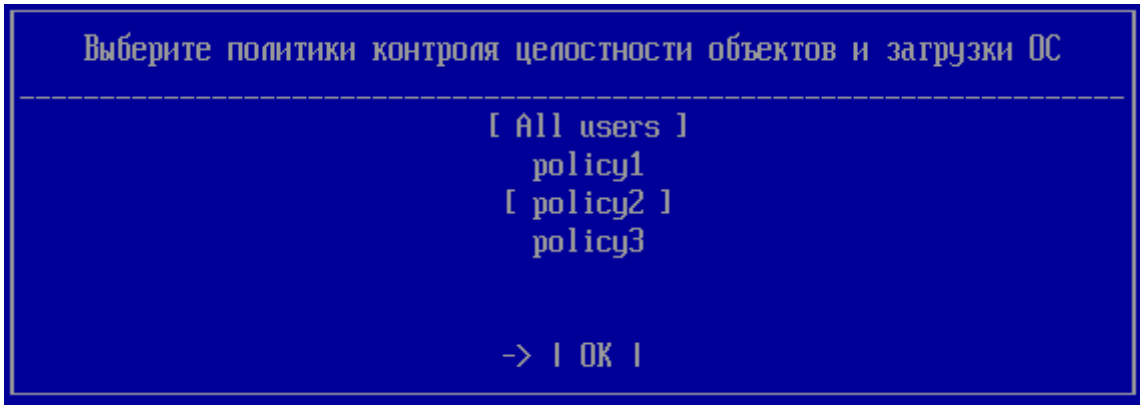


Рисунок 9.6 – Выбор политики КЦ и загрузки ОС

9.1.9 После установки полей для сохранения изменений в создаваемой учетной записи пользователя АБ необходимо перейти в строку ***«Сохранить»*** (рисунок 9.4) и нажать клавишу **< *Enter* >**. При этом в новом диалоговом окне будет выведено сообщение об успешном создании учетной записи пользователя (рисунок 9.7).

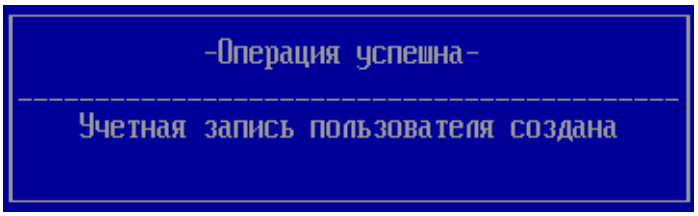


Рисунок 9.7 – Успешное создание учетной записи пользователя

[4] Переназначение носителя необходимо только при активированном режиме «Локальная проверка сертификата», когда проверка сертификата на носителе осуществляется изделием. В случае, если доменному пользователю на сервере будет назначен другой сертификат, то при аутентификации такого пользователя в изделии будет осуществляться проверка серверного сертификата доменом.

9.1.10 В случае если какое-либо из обязательных полей не было заполнено, на экран ЭВМ будет выведено сообщение об ошибке (рисунок 9.8).

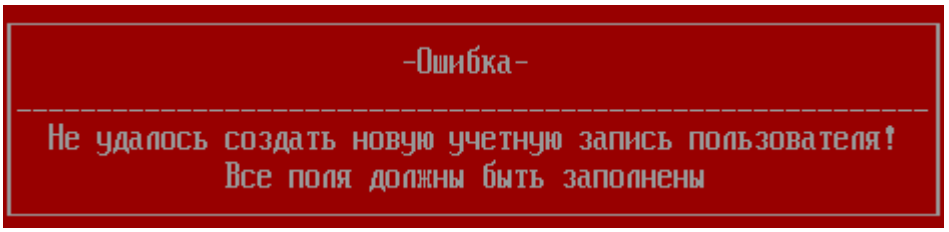


Рисунок 9.8 – Ошибка при создании учетной записи пользователя

9.2 Редактирование учетной записи пользователя

9.2.1 Для редактирования существующей учетной записи пользователя необходимо выбрать в главном окне (рисунок 4.2) подраздел ***«Учетные записи пользователей»***. В появившемся диалоговом окне АБ необходимо перейти в строку ***«Редактирование»*** и нажать клавишу **< *Enter* >** (рисунок 9.1).

9.2.2 В новом диалоговом окне «***Редактирование учетной записи пользователя»*** АБ необходимо выбрать имя редактируемой учетной записи пользователя в поле ***«Имя пользователя»*** и нажать кнопку | ***ОК*** | (рисунок 9.9).

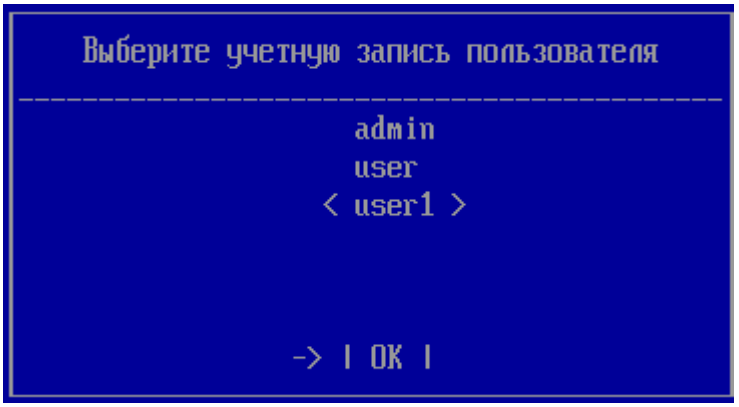


Рисунок 9.9 – Выбор учетной записи пользователя для редактирования

9.2.3 Доступные для редактирования параметры учетной записи пользователя (рисунок 9.10) и их значения приведены в таблице 9.1.

Поле «Имя пользователя» заполняется при создании учетной записи пользователя и в дальнейшем недоступно для редактирования.

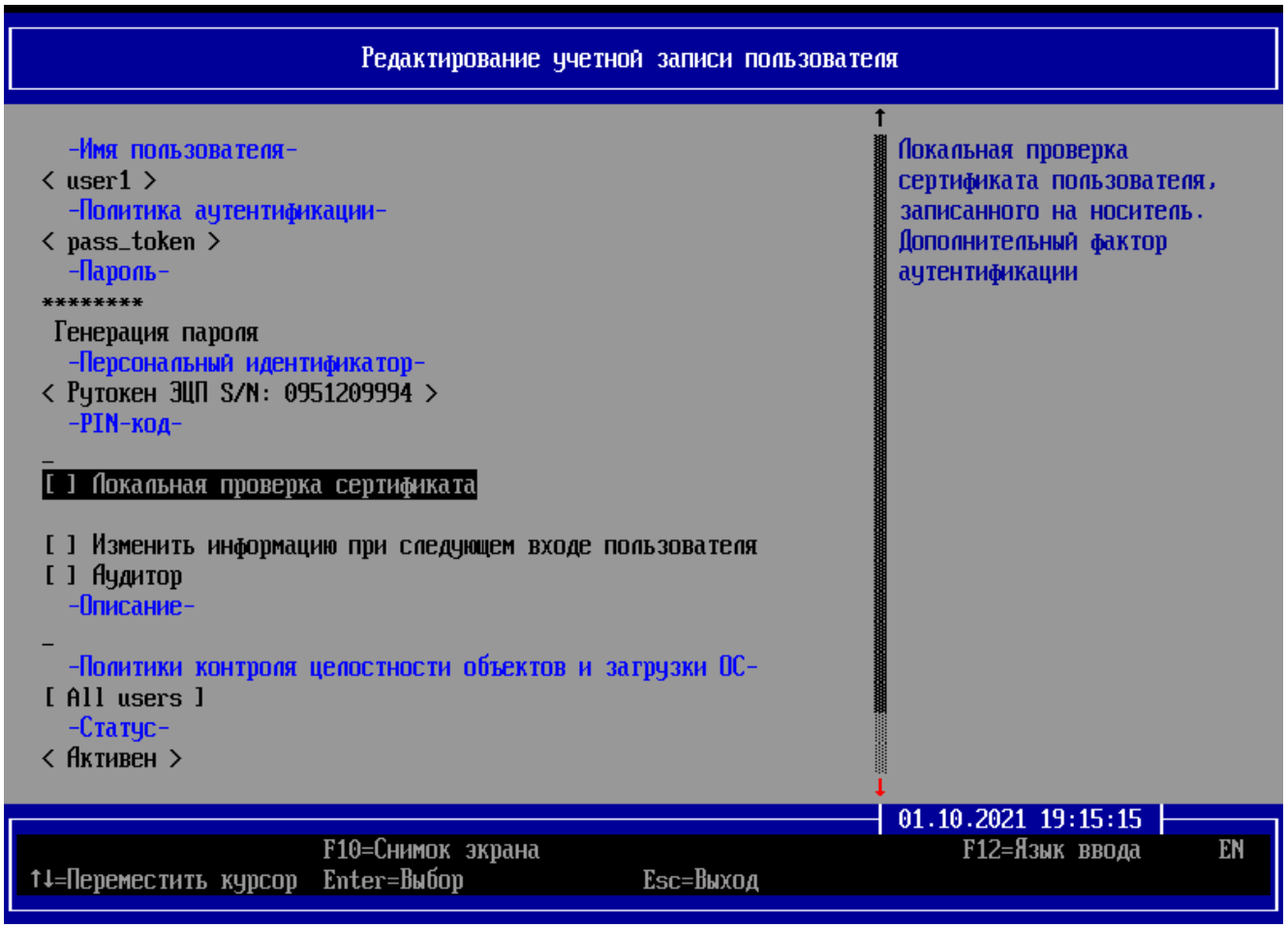


Рисунок 9.10 – Редактируемые поля учетной записи пользователя

9.2.4 Для сохранения изменений редактируемой учетной записи пользователя необходимо перейти в строку ***«Сохранить»*** (рисунок 9.10) и нажать клавишу ***< Enter >***. При этом в новом диалоговом окне будет выведено сообщение об успешном редактировании учетной записи пользователя (рисунок 9.11).

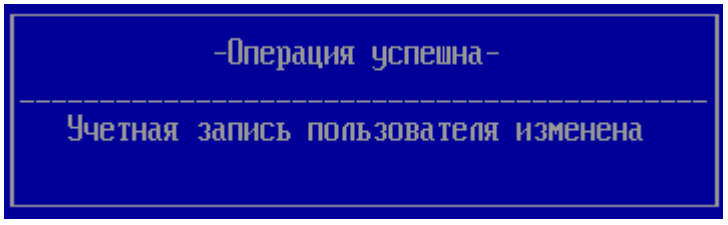


Рисунок 9.11 – Успешное изменение учетной записи пользователя

9.3 Удаление учетной записи пользователя

9.3.1 Для удаления существующей учетной записи пользователя АБ необходимо выбрать в главном окне (рисунок 4.2) подраздел «***Учетные записи пользователей»***. В появившемся диалоговом окне АБ необходимо перейти в строку ***«Удаление»*** и нажать клавишу **< *Enter* >** (рисунок 9.1).

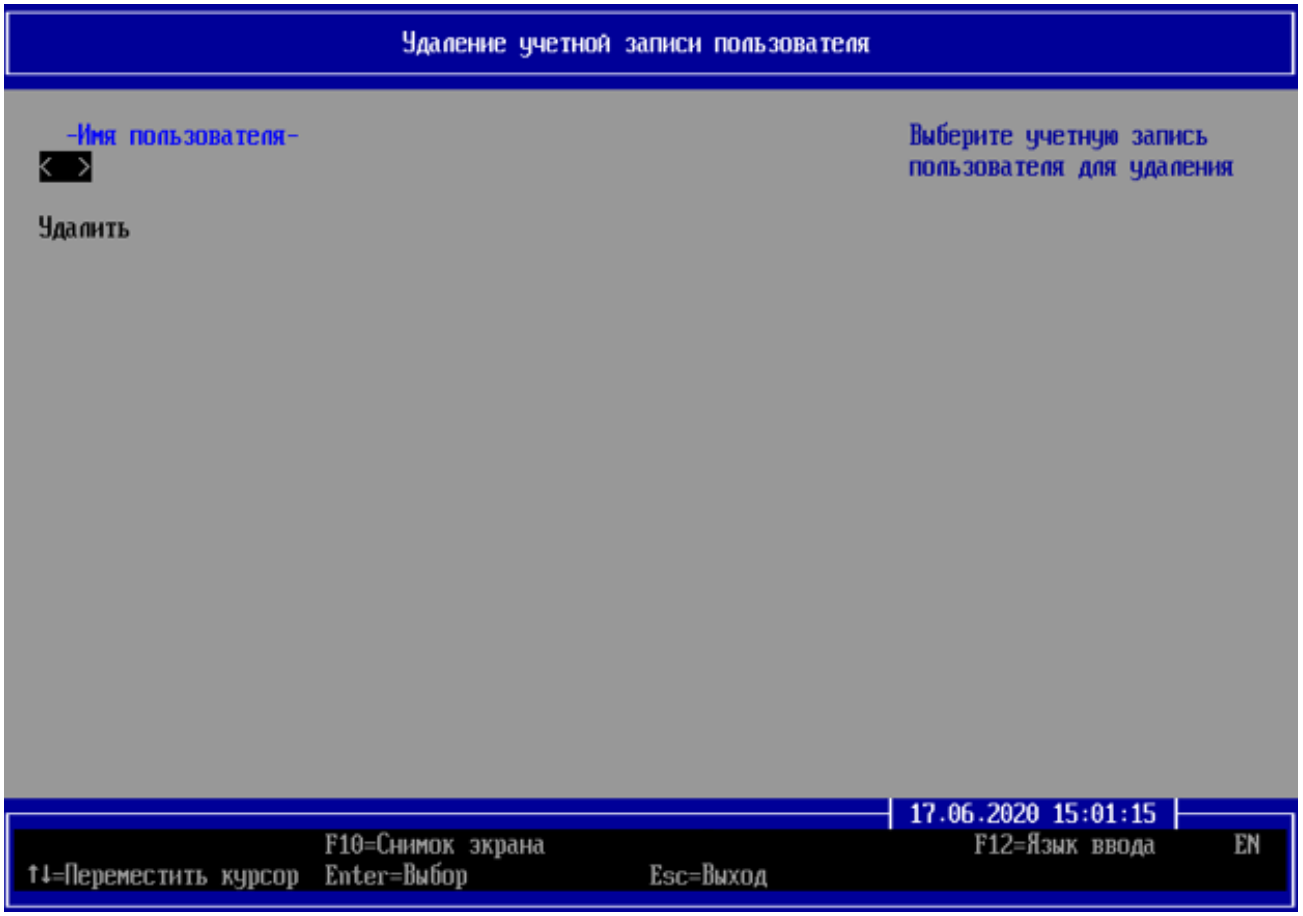


Рисунок 9.12 – Удаление учетной записи пользователя

9.3.2 В новом диалоговом окне ***«Удаление учетной записи пользователя»*** (рисунок 9.12) необходимо выбрать имя удаляемой учетной записи пользователя в поле ***«Имя пользователя»*** и нажать кнопку **| *ОК* |** (рисунок 9.9).

9.3.3 Для удаления выбранной учетной записи пользователя АБ необходимо перейти в строку ***«Удалить»*** (рисунок 9.12) и нажать клавишу **< *Enter* >**. При этом в новом диалоговом окне будет выведено сообщение об успешном удалении учетной записи пользователя (рисунок 9.13).

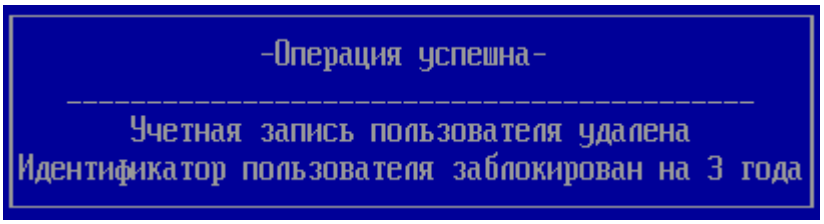


Рисунок 9.13 – Успешное удаление учетной записи пользователя

Удаление учетных записей пользователей производится поочередно.

После удаления учетной записи пользователя из БД изделия исключено его повторное использование в течение трех лет в соответствии с требованиями меры безопасности ИАФ.3 «Методический документ. Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014).

При восстановлении параметров изделия к заводским удаленная учетная запись пользователя станет доступной для использования.

9.4 Разблокировка пользователей

9.4.1 Для разблокировки пользователей после выявления и устранения нарушений КЦ или при ошибках в процессе идентификации и аутентификации пользователей необходимо выбрать в главном окне (рисунок 4.2) подраздел «***Учетные записи пользователей»***.

9.4.2 Для разблокировки всех пользователей АБ необходимо в появившемся диалоговом окне (рисунок 9.1) перейти в строку ***«Разблокировка всех пользователей»*** и нажать клавишу ***< Enter >***. При этом в новом диалоговом окне будет выведено сообщение об успешной разблокировке пользователей (рисунок 9.14).

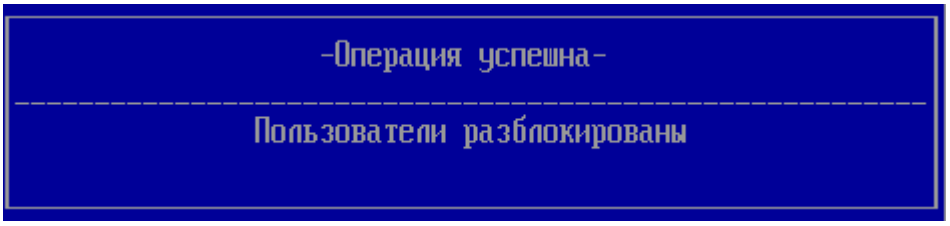


Рисунок 9.14 – Успешная разблокировка всех пользователей

9.4.3 Для разблокировки выборочных учетных записей пользователей АБ необходимо в появившемся диалоговом окне (рисунок 9.1) перейти в строку ***«Разблокировка пользователей»*** и нажать клавишу ***< Enter >***.

9.4.4 В новом диалоговом окне АБ необходимо выбрать учетные записи пользователей для разблокировки и нажать кнопку **|** ***OK*** **|** (рисунок 9.15). При этом в новом диалоговом окне будет выведено сообщение об успешной разблокировке выбранных учетных записей пользователей (рисунок 9.14).

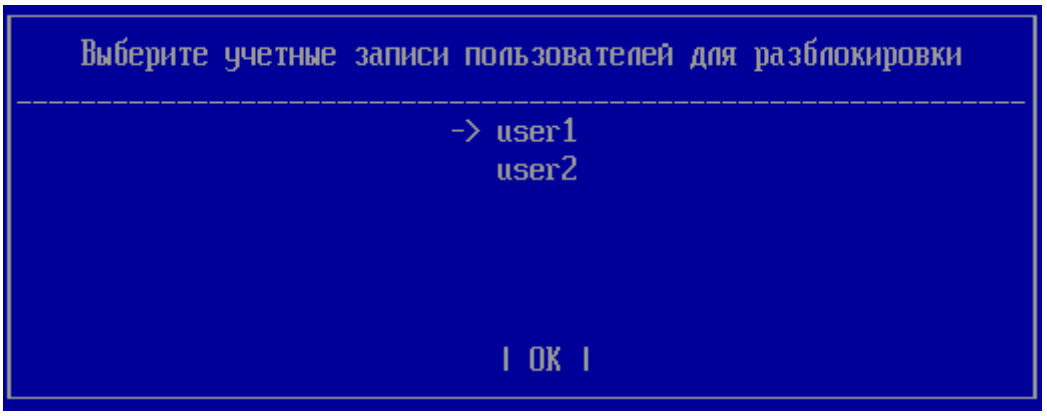


Рисунок 9.15 – Выбор учетных записей для разблокировки

9.5 Блокировка пользователей

9.5.1 Для блокировки пользователей после выявления и устранения нарушений КЦ или при ошибках в процессе идентификации и аутентификации пользователей необходимо выбрать в главном окне (рисунок 4.2) подраздел «***Учетные записи пользователей»***.

9.5.2 Для блокировки всех пользователей АБ необходимо в появившемся диалоговом окне (рисунок 9.1) перейти в строку «***Блокировка всех пользователей***» и нажать клавишу < ***Enter*** >. При этом в новом диалоговом окне будет выведено сообщение об успешной блокировке пользователей (рисунок 9.16).

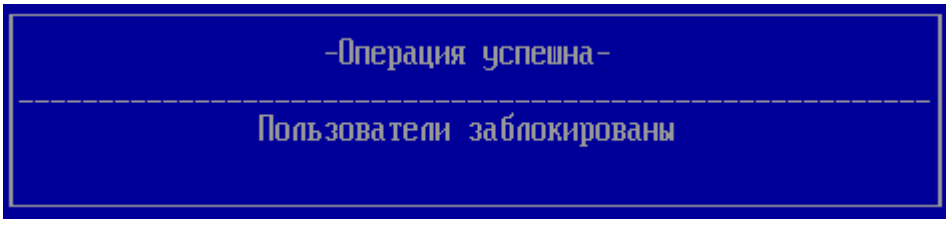


Рисунок 9.16 – Успешная блокировка всех пользователей

9.5.3 Для блокировки выборочных учетных записей пользователей необходимо в появившемся диалоговом окне (рисунок 9.1) перейти в строку «***Блокировка пользователей***» и нажать клавишу < ***Enter*** >.

9.5.4 В новом диалоговом окне АБ необходимо выбрать учетные записи пользователей для блокировки и нажать кнопку | ***ОК*** | (рисунок 9.17). При этом в новом диалоговом окне будет выведено сообщение об успешной блокировке выбранных учетных записей пользователей (рисунок 9.16).

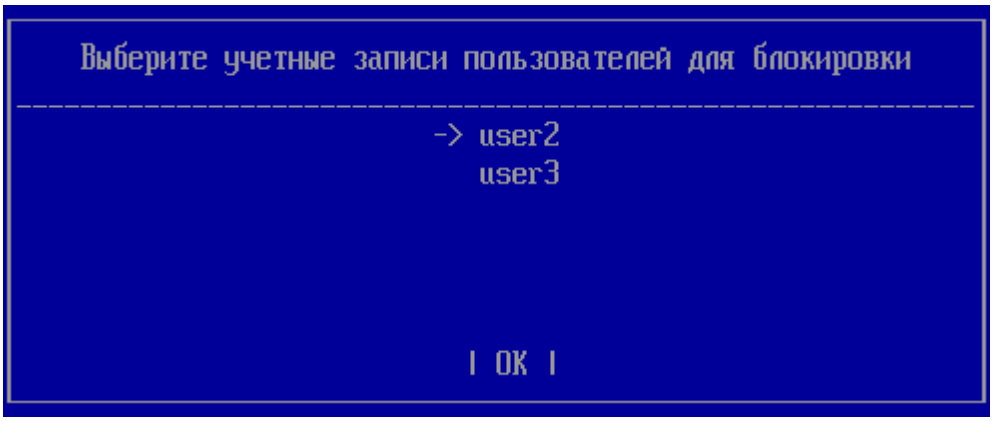


Рисунок 9.17 – Выбор учетных записей для блокировки

10 Общие параметры

Раздел ***«Общие параметры»*** в главном окне консоли АБ (рисунок 4.2) предназначен для настройки общих параметров изделия, диагностики изделия, сброса параметров к заводским настройкам и обновления ПО изделия.

10.1 Основные настройки: аутентификация, параметры сети и LDAP, настройки времени, контроль целостности, алгоритмы расчета контрольных сумм, защита от перевода времени, прочие параметры

10.1.1 Содержимое подраздела ***«Основные настройки»*** приведено на рисунке 10.1.

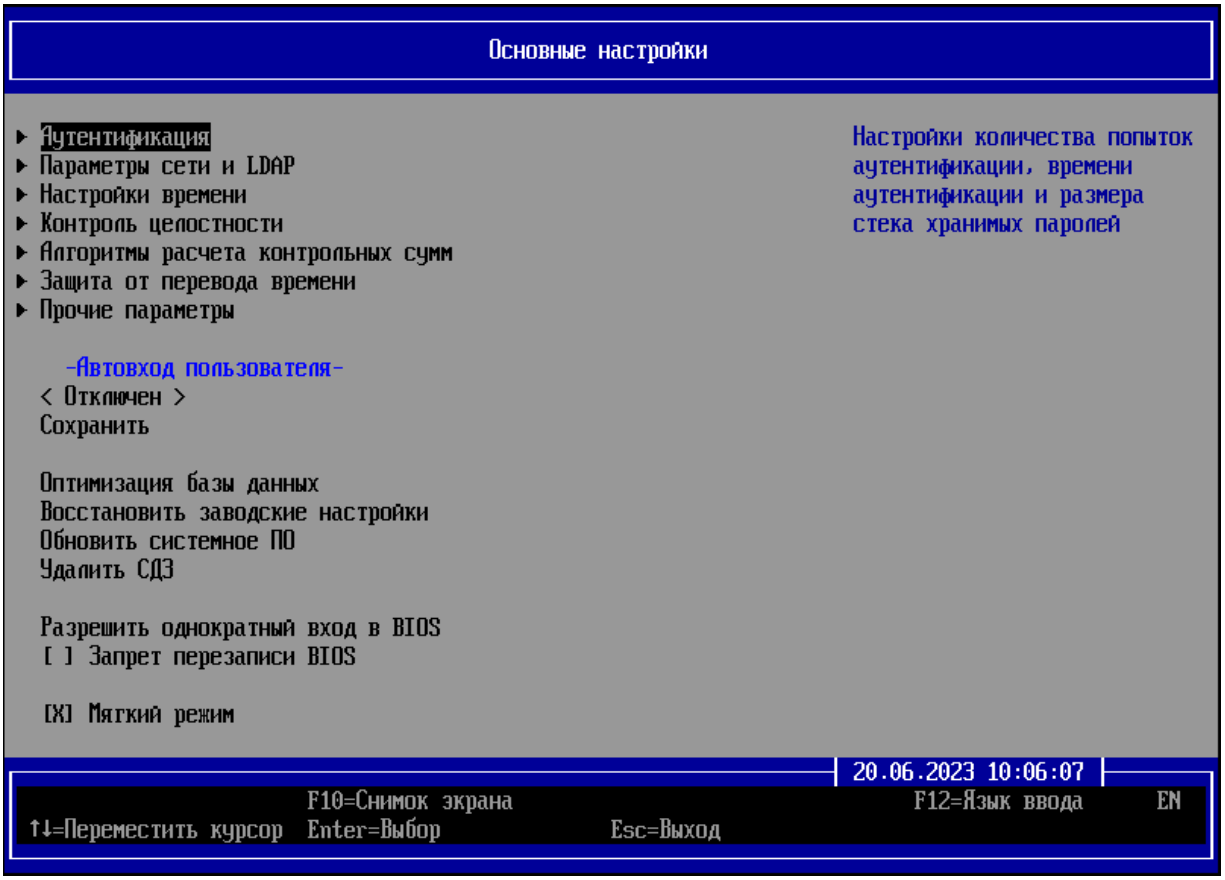


Рисунок 10.1 – Содержимое пунктов подраздела «Основные настройки»

10.1.2 В таблице 10.1 приведено содержимое полей всех пунктов подраздела (рисунок 10.1) и их возможные значения.

Таблица 10.1 – Возможные значения полей пунктов подраздела «Основные настройки»

№	Наименование поля	Возможные значения поля [по умолчанию]	Минимальное … максимальное значения	Примечание
Пункт «Аутентификация»				
1	Количество попыток аутентификации пользователей	8	1…8	
2	Время аутентификации пользователей (минуты)	15	1…30	
3	Размер стека хранимых паролей	10	1…100	
Пункт «Параметры сети и LDAP. Сетевые настройки»				
4	Сетевая подсистема	[Выключена] Включена		Включение или выключение сетевой подсистемы
5	Сетевой интерфейс	[eth0]		Количество сетевых интерфейсов зависит от количества установленных сетевых карт
6	MAC	Текущее значение параметра		MAC-адрес сетевой карты ЭВМ
7	Параметры IP-адреса	[Статический] Динамический		
8	IP-адрес	[0.0.0.0]	0.0.0.0 … 255.255.255.255	
9	Маска подсети	[0.0.0.0]	0.0.0.0 … 255.255.255.255	
10	Шлюз по умолчанию	[0.0.0.0]	0.0.0.0 … 255.255.255.255	
Пункт «Параметры сети и LDAP. LDAP»				
11	Аутентификация LDAP	[Отключена] Включена		Включить или выключить аутентификацию LDAP
12	Файлы конфигураций OpenLdap и Kerberos	hosts krb5.conf ldap.conf		Загрузить файлы конфигураций в систему
13	Проверить доступность сервера LDAP или Kerberos			Проверка доступности сервера LDAP или Kerberos путем отправки запроса на IP-адрес сервера
14	Префикс и суффикс пользователей			Уникальное имя учетной записи пользователя

№	Наименование поля	Возможные значения поля [по умолчанию]	Минимальное … максимальное значения	Примечание
15	Использование Kerberos	[Выключено] Включено		Использование преобразования Kerberos
16	Редактирование списка доменных пользователей			Добавление или удаление доменных пользователей в систему и формирование белого списка доменных пользователей
Пункт «Контроль целостности»				
17	Дата			Установка даты в формате ДД.ММ.ГГГГ
18	Время			Установка времени в формате ЧЧ:ММ:ГГГГ
19	Часовой пояс			Выбор часового пояса из списка
20	Адрес NTP сервера			Позволяет указать один или более NTP серверов в формате строки
21	Синхронизировать время с сервером			Позволяет получить текущее время с NTP сервера и установить его
22	Синхронизировать время автоматически	[Выключено] Включено		Выполнение автоматической синхронизации времени с NTP сервером при старте ЭВМ
Пункт «Контроль целостности»				
23	Осуществление контроля целостности	До аутентификации пользователей [После аутентификации пользователей]		
24	Максимальное количество контролируемых объектов файловой системы	5000	1…9 999 999	
25	Максимальное количество контролируемых объектов реестра ОС Windows	5000	1…9 999 999	
Пункт «Алгоритмы расчета контрольных сумм»				
26	Алгоритм расчета	MD4		

№	Наименование поля	Возможные значения поля [по умолчанию]	Минимальное … максимальное значения	Примечание
	контрольных сумм аутентификации	[MD5] SHA1 SHA256 SHA384 SHA512		
27	Алгоритм расчета контрольных сумм контроля целостности	MD4 [MD5] SHA1 SHA256 SHA384 SHA512		
28	Алгоритм проверки цифровой подписи	RSA 2048 бит		
29	Алгоритм шифрования	AES 256 бит		
Пункт «Защита от перевода времени»				
30	Защита от перевода времени	[Выключена] Включена		Включение/выключение защиты от перевода пользователем времени назад
31	Допустимый сдвиг (часы)	1	1…24	Максимально допустимый сдвиг по времени в часах в пределах которого нарушение не регистрируется
32	Тип блокировки	[Блокировка пользователя] Запись в журнал Блокировка группы пользователя Блокировка всех пользователей		

№	Наименование поля	Возможные значения поля [по умолчанию]	Минимальное … максимальное значения	Примечание
		Пункт «Прочие параметры»		
33	Количество записей в журнале для отображения	200	10…4000	
34	Количество циклов очистки памяти	1	1…5	Количество циклов перезаписи при очистке памяти СДЗ
35	Язык меню	[ru-RU] en-US		Язык отображения меню
36	Режим отображение основного меню	Расширенный [Сокращенный]		Выбор режима отображения меню по умолчанию
37	Максимальное время бездействия администратора (минуты)	[0]	0…30	
38	Интерфейс командной строки	Выключен [Включен]		УКАЗАНИЕ параметра для работы с командной строкой
39	Настройка основного меню	–	–	Выбор элементов меню, отображаемых при расширенном режиме функционирования
		Пункт «Автовход»		
40	Автовход	[Отключен] Введенное значение		Возможность указать учетной записи пользователя автоматическую аутентификацию с АНП
		Иные параметры		
41	Оптимизация базы данных	–		Возможность уменьшить размер БД и ускорить работу с ней
42	Восстановить заводские настройки	–		Все данные системы, кроме записей журнала аудита, будут полностью удалены, ЭВМ перезагружена
43	Обновить системное ПО	–		При обновлении потребуется указать раздел, содержащий файл обновления
44	Удалить СДЗ	–		Удаление СДЗ с ЭВМ. Подробнее данный пункт рассмотрен в

№	Наименование поля	Возможные значения поля [по умолчанию]	Минимальное … максимальное значения	Примечание
				документе «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 1. Руководство по установке. ГМТК.468269.060РЭ1»
45	Разрешить однократный вход в BIOS	–		Разрешение однократного входа в BIOS с использованием стандартных клавиш входа сразу после перезагрузки ЭВМ. **После включения параметра потребуется перезагрузка ЭВМ**
46	Запрет перезаписи BIOS	Включено [Отключено]	–	Установка запрета перезаписи UEFI BIOS ЭВМ в обход изделия
47	Мягкий режим	–		Позволяет активировать режим с возможностью загрузки ОС без настроенных механизмов защиты

10.1.3 После внесения изменений в пункты ***«Алгоритмы расчета контрольных сумм»***, ***«Контроль целостности»***, ***«Аутентификация»***, ***«Защита от перевода времени», «Прочие параметры»*** и ***«Автовход»*** для сохранения выбранных значений необходимо перейти в строку ***«Сохранить»*** (рисунок 10.2) и нажать клавишу ***< Enter >***. При этом в новом диалоговом окне будет выведено сообщение об успешном изменении настроек (рисунок 10.3).

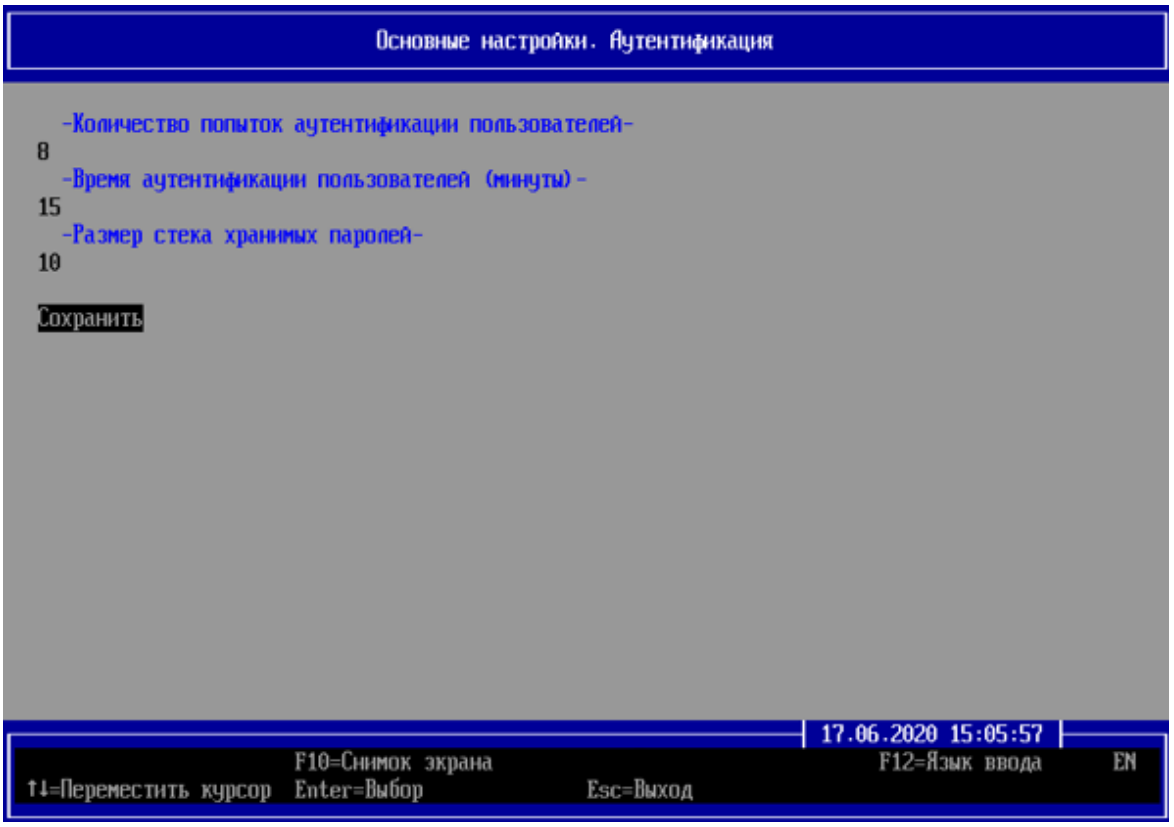


Рисунок 10.2 – Сохранение результатов изменений

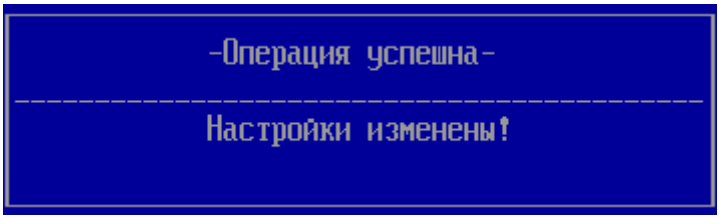


Рисунок 10.3 – Успешное изменение настроек

10.1.4 При попытке выхода из меню при помощи клавиши ***<Esc>*** без нажатия кнопки ***«Сохранить»*** на экран ЭВМ будет выведено сообщение с предложением сохранения настроек (рисунок 10.4).

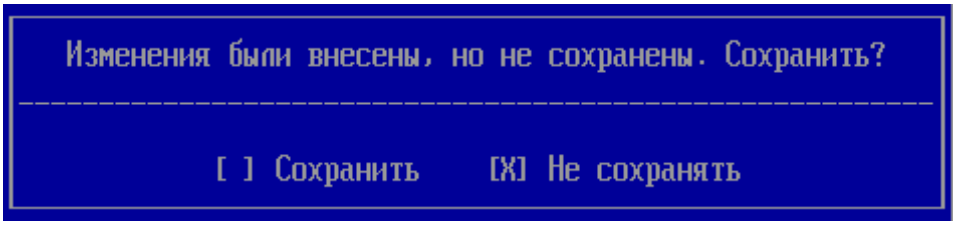


Рисунок 10.4 – Подтверждение выхода из меню без сохранения изменений

При изменении параметров *«Алгоритм расчета контрольных сумм аутентификации»* и *«Алгоритм расчета контрольных сумм контроля целостности»* ранее установленные объекты КЦ будут проверяться по предыдущим установленным алгоритмам расчета, новые объекты – по новым (измененным) алгоритмам расчета.

10.2 Параметры сети и LDAP

Пункт ***«Параметры сети и LDAP»*** предназначен для установки сетевых настроек ЭВМ, на которой установлено изделие, и настройки параметров сервера LDAP для аутентификации пользователей, зарегистрированных на сервере LDAP.

Для подключения LDAP аутентификации необходимо предварительно выполнить следующие действия:

- **в BIOS ЭВМ установить необходимые параметры сетевой подсистемы ЭВМ (указаны в документе «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 1. Руководство по установке. ГМТК.468269.060РЭ1»);**
- **установить параметры LDAP сервера и создать учетные записи пользователей;**
- **на сервере аутентификации LDAP указать необходимость активации преобразования TLS или аутентификации по протоколу Kerberos.**

10.2.1 Для настройки параметров сети на ЭВМ необходимо в разделе ***«Основные настройки»*** (рисунок 10.1) выбрать пункт ***«Параметры сети и LDAP»***. При этом на экране ЭВМ появится диалоговое окно, представленное на рисунке 10.5.

10.2.2 В новом диалоговом окне ***«Основные настройки. Сетевые настройки»*** (рисунок 10.6) осуществляется настройка сетевых параметров ЭВМ, на которой установлено изделие. Установка параметра «Сетевая подсистема» в состояние «Включена» позволяет включить взаимодействие изделия и сервера LDAP по сети.

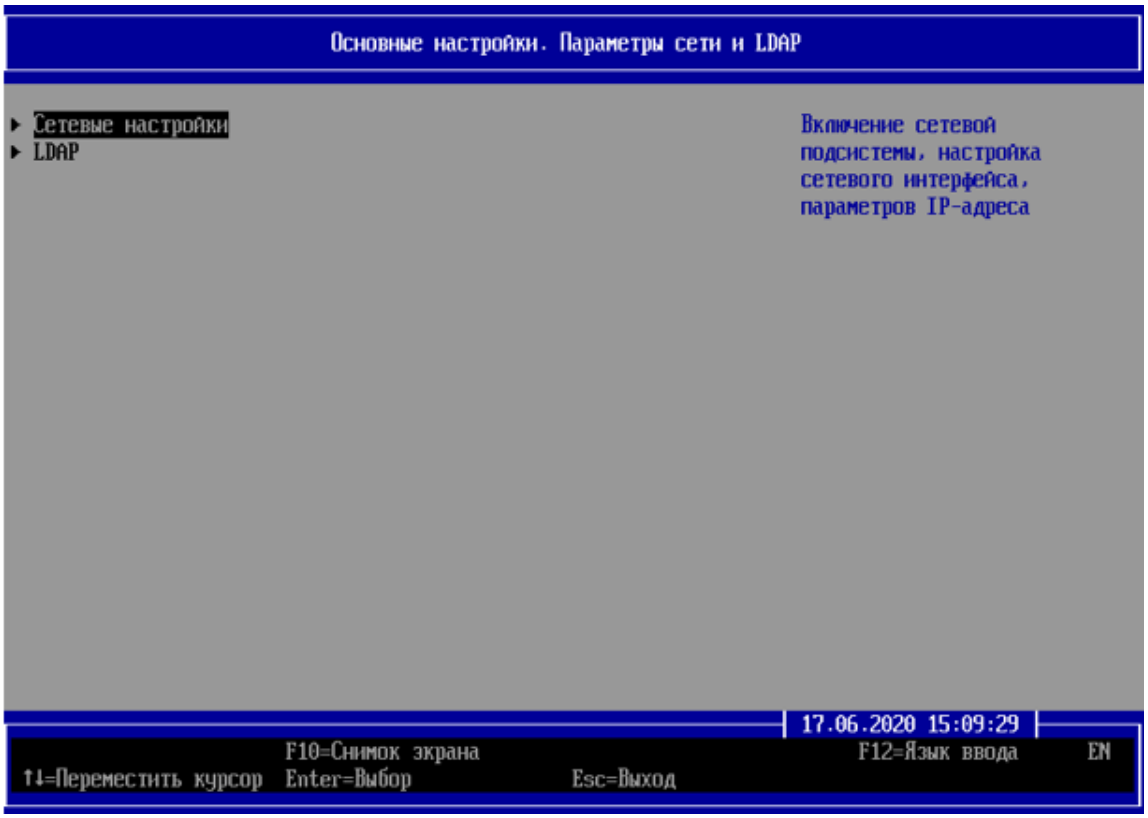


Рисунок 10.5 – Настройка параметров сети и LDAP

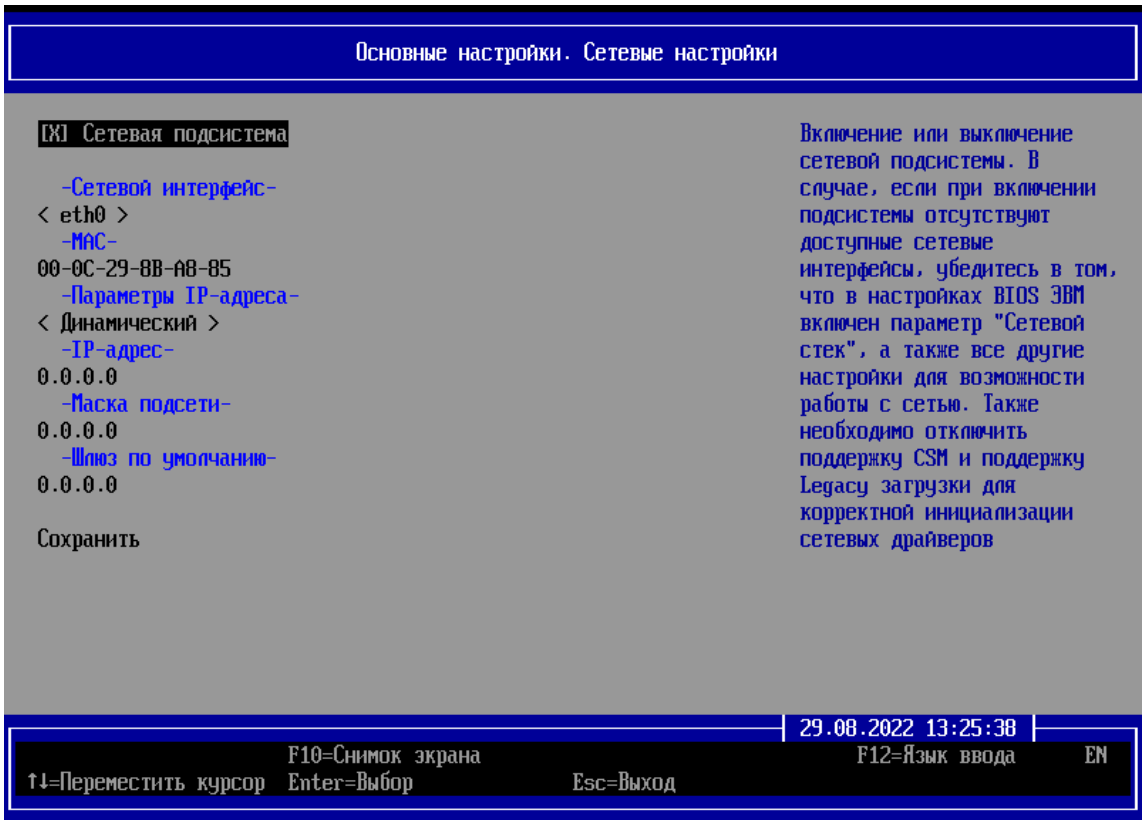


Рисунок 10.6 – Сетевые настройки

10.2.3 Для настройки параметров сетевого взаимодействия необходимо указать сетевой интерфейс ЭВМ в поле ***«Сетевой интерфейс»***. Количество сетевых интерфейсов зависит от количества установленных сетевых карт на ЭВМ.

10.2.4 После выбора сетевого интерфейса автоматически будет определен MAC-адрес сетевой карты в поле ***«MAC»***, при этом данный параметр не подлежит изменению АБ.

10.2.5 В поле ***«Параметры IP-адреса»*** необходимо указать способ получения сетевых настроек – статический или динамический. При выборе параметра ***«Динамический»***, поля ***«IP-адрес»***, ***«Маска подсети»*** и ***«Шлюз по умолчанию»*** заполнятся автоматически. При выборе параметра ***«Статический»*** данные поля необходимо заполнять самостоятельно.

10.2.6 После установки параметров необходимо перейти в поле ***«Сохранить»*** и нажать клавишу **< *Enter* >**. В случае успешного применения параметров сетевого подключения появится сообщение (рисунок 10.7).

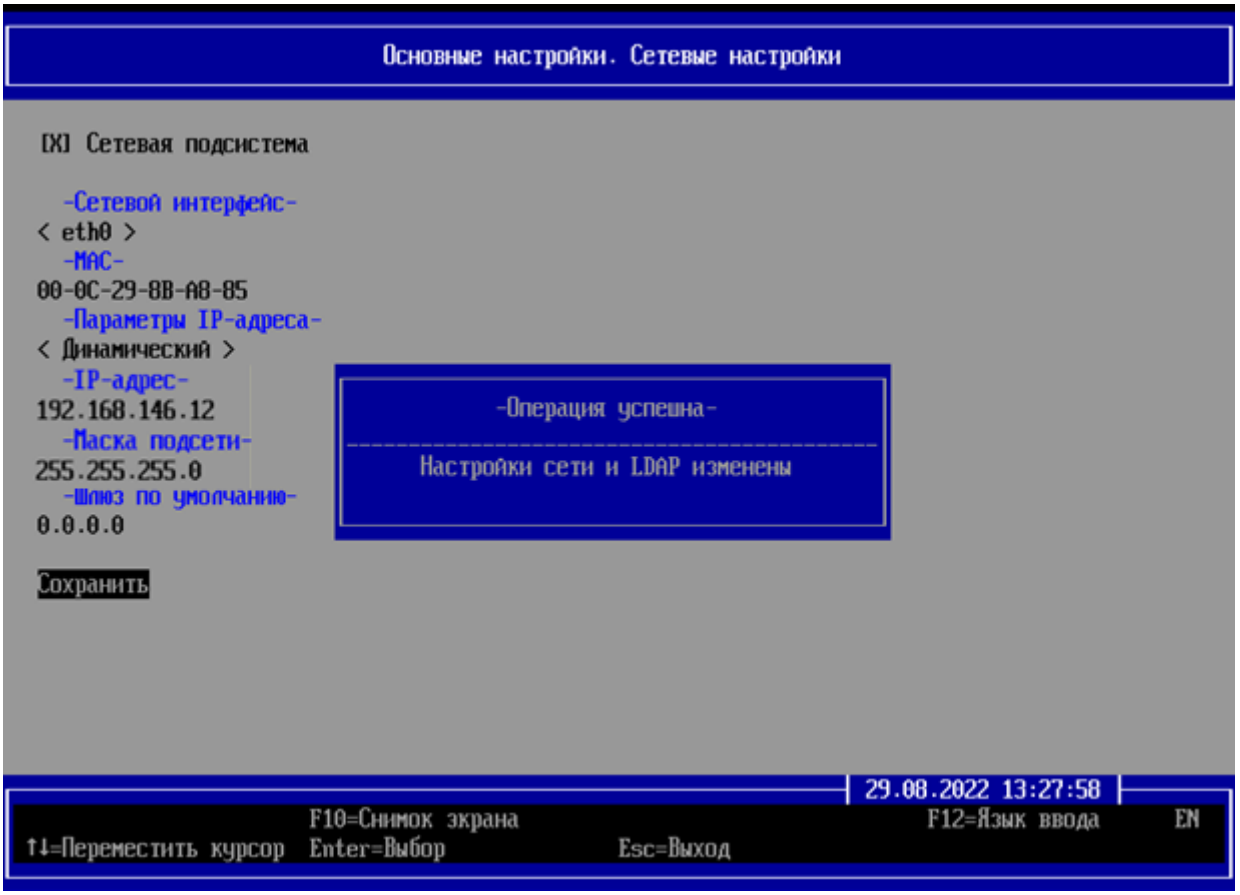


Рисунок 10.7 – Успешное изменение сетевых настроек

10.2.7 После конфигурирования сетевых настроек ЭВМ необходимо указать настройки LDAP сервера, для этого в диалоговом окне ***«Основные настройки.***

Параметры сети и LDAP» (рисунок 10.8) выбрать параметр «LDAP» и нажать клавишу < Enter >.

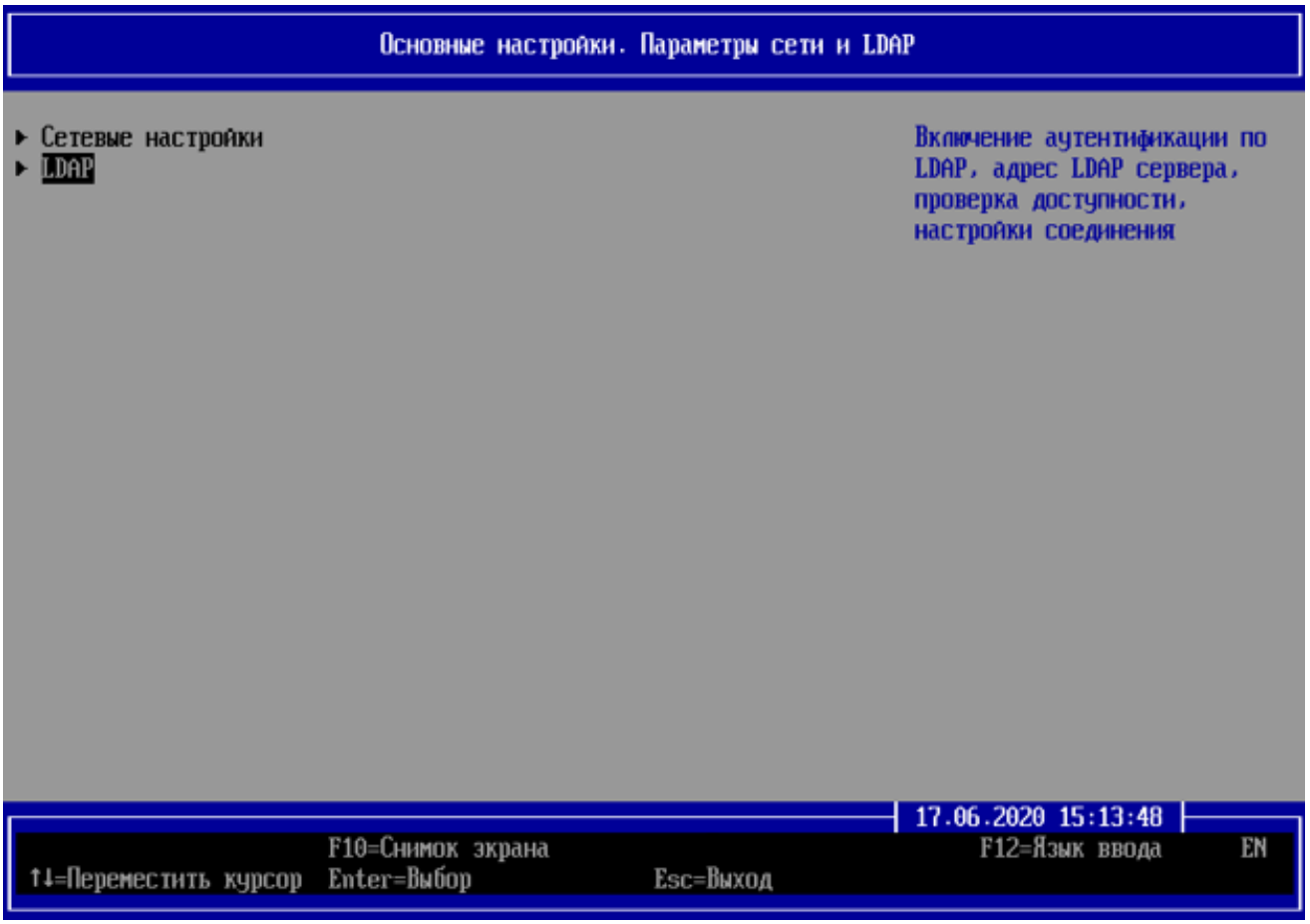


Рисунок 10.8 – Выбор пункта меню «LDAP» для настройки

10.2.8 Для включения аутентификации LDAP необходимо в окне ***«Основные настройки. LDAP»*** перейти в строку ***«Аутентификация LDAP»*** (рисунок 10.9) и нажать клавишу ***< Enter >***.

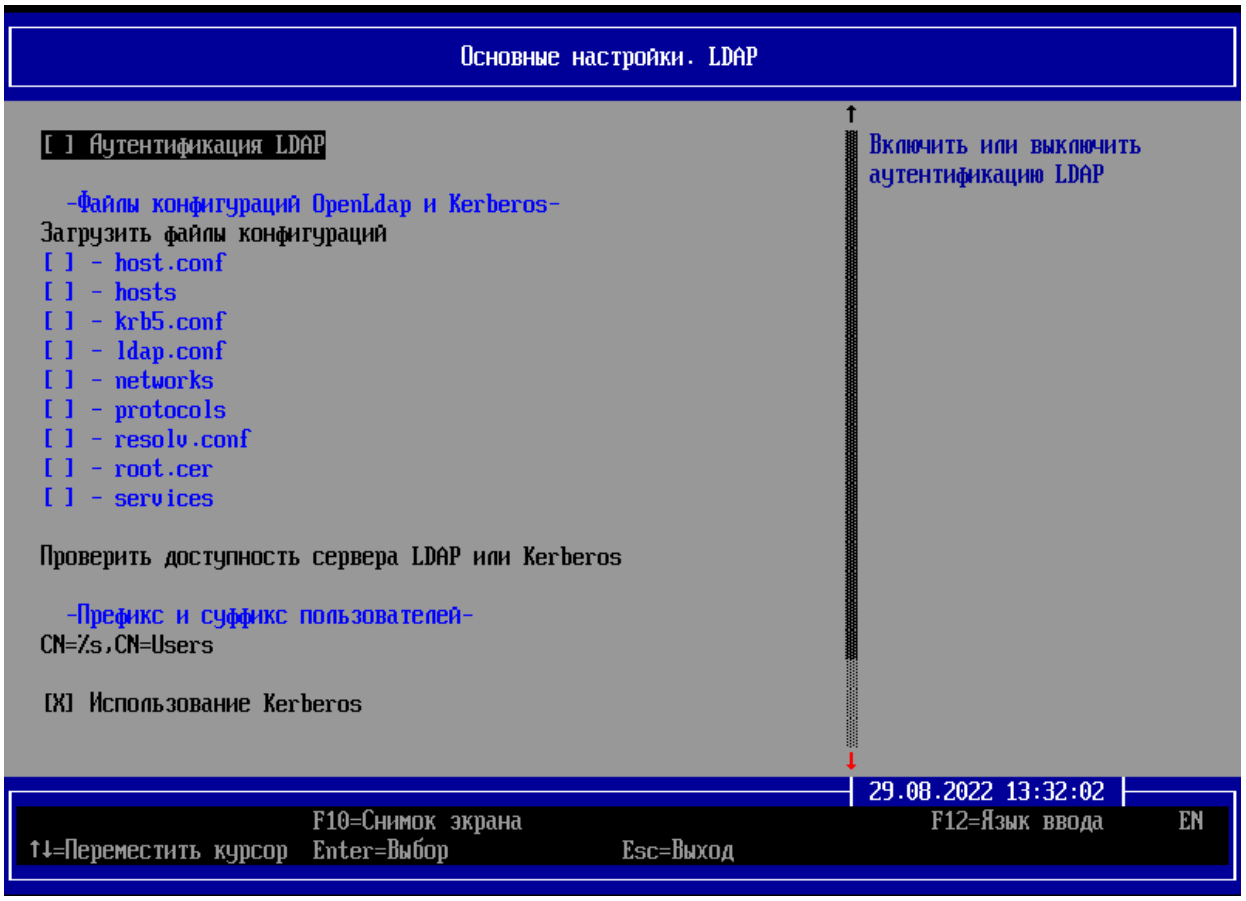


Рисунок 10.9 – Настройка аутентификации LDAP

10.2.9 Для включения параметра ***«Аутентификация LDAP»*** в состояние ***«Включена»*** необходимо перейти в строку параметра и нажать клавишу **< *Enter* >**.

10.2.10 После включения параметра ***«Аутентификация LDAP»*** необходимо загрузить подготовленные ранее файлы конфигураций (рисунок 10.10). Подробная информация о подготовке файлов конфигураций приведена в разделе 10.2 документа «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 3. Руководство администратора Linux/Windows. ГМТК.468269.060РЭ3».

10.2.11 Для загрузки файлов конфигураций необходимо перейти в поле ***«Загрузить файлы конфигураций»*** и нажать клавишу **< *Enter* >** (рисунок 10.10). В появившемся диалоговом окне следует выбрать файловую систему устройства хранения данных, в корне которой располагаются файлы конфигураций ***hosts***, ***krb5.conf*** и ***ldap.conf*** и выбрать кнопку **| *OK* |**.

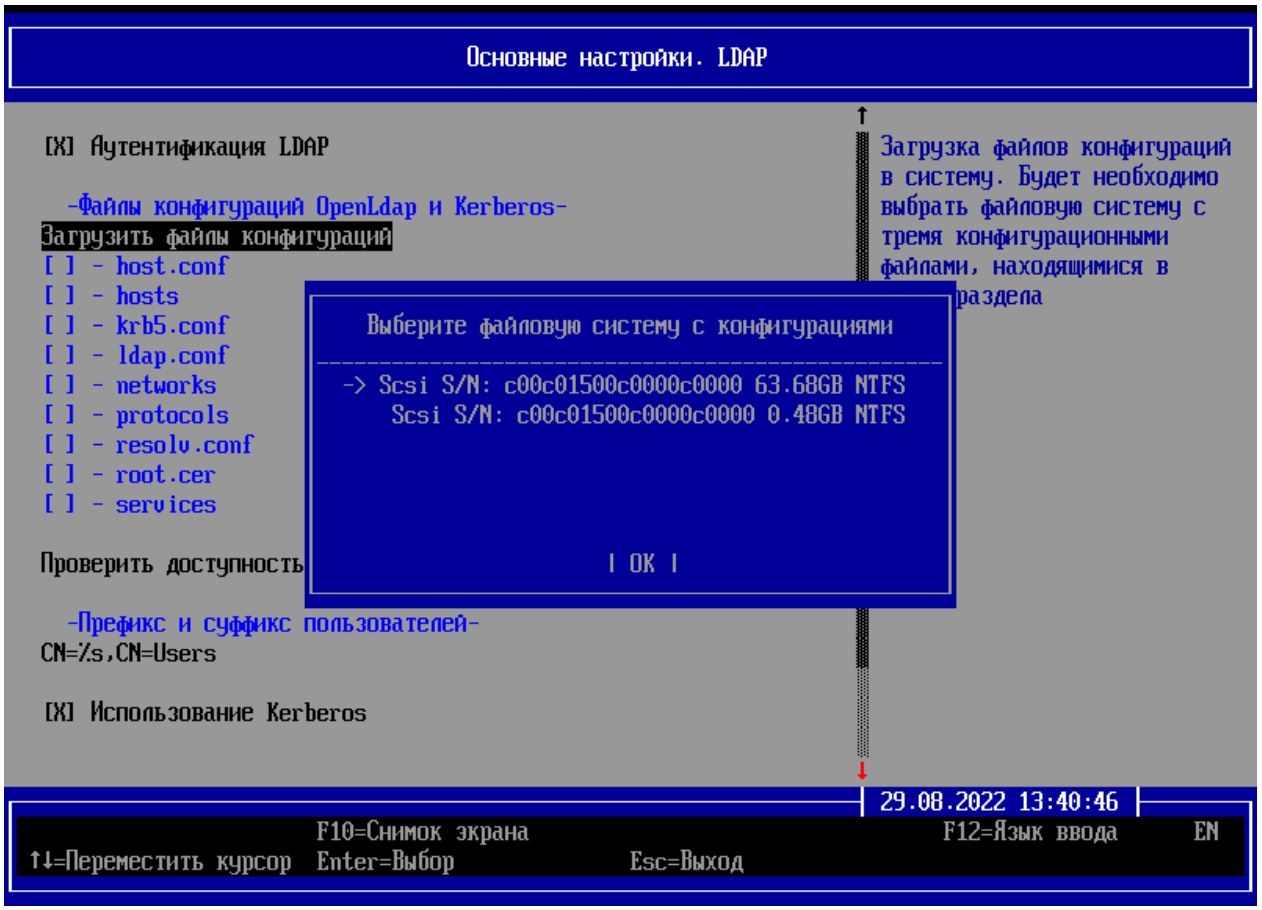


Рисунок 10.10 – Выбор файловой системы с файлами конфигураций

10.2.12 В случае удачного применения файлов конфигурации на экране ЭВМ появится информационное сообщение (рисунок 10.11).

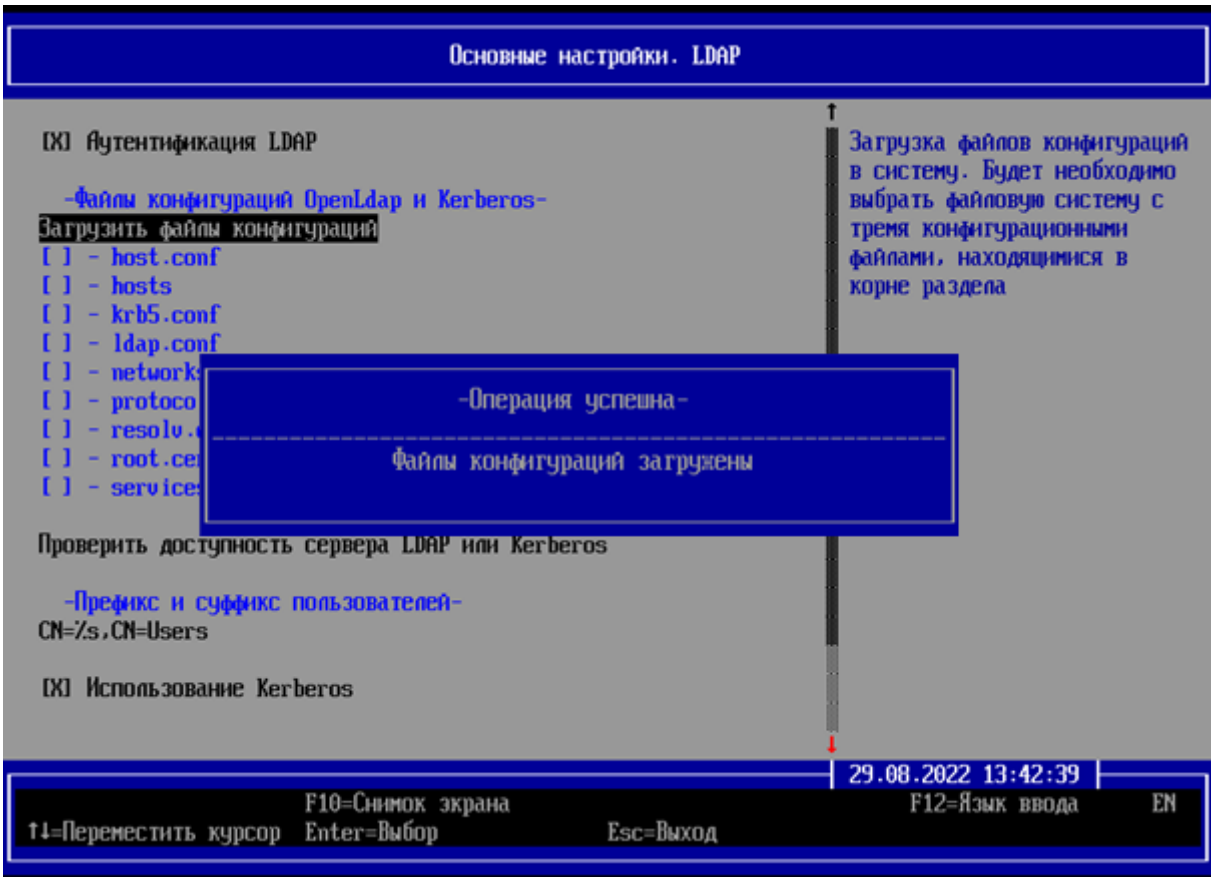


Рисунок 10.11 – Выбор файловой системы с файлами конфигураций

10.2.13 Для сохранения параметров настроек необходимо перейти в поле ***«Сохранить»*** и нажать клавишу ***< Enter >***, при успешном сохранении настроек появится сообщение (рисунок 10.12).

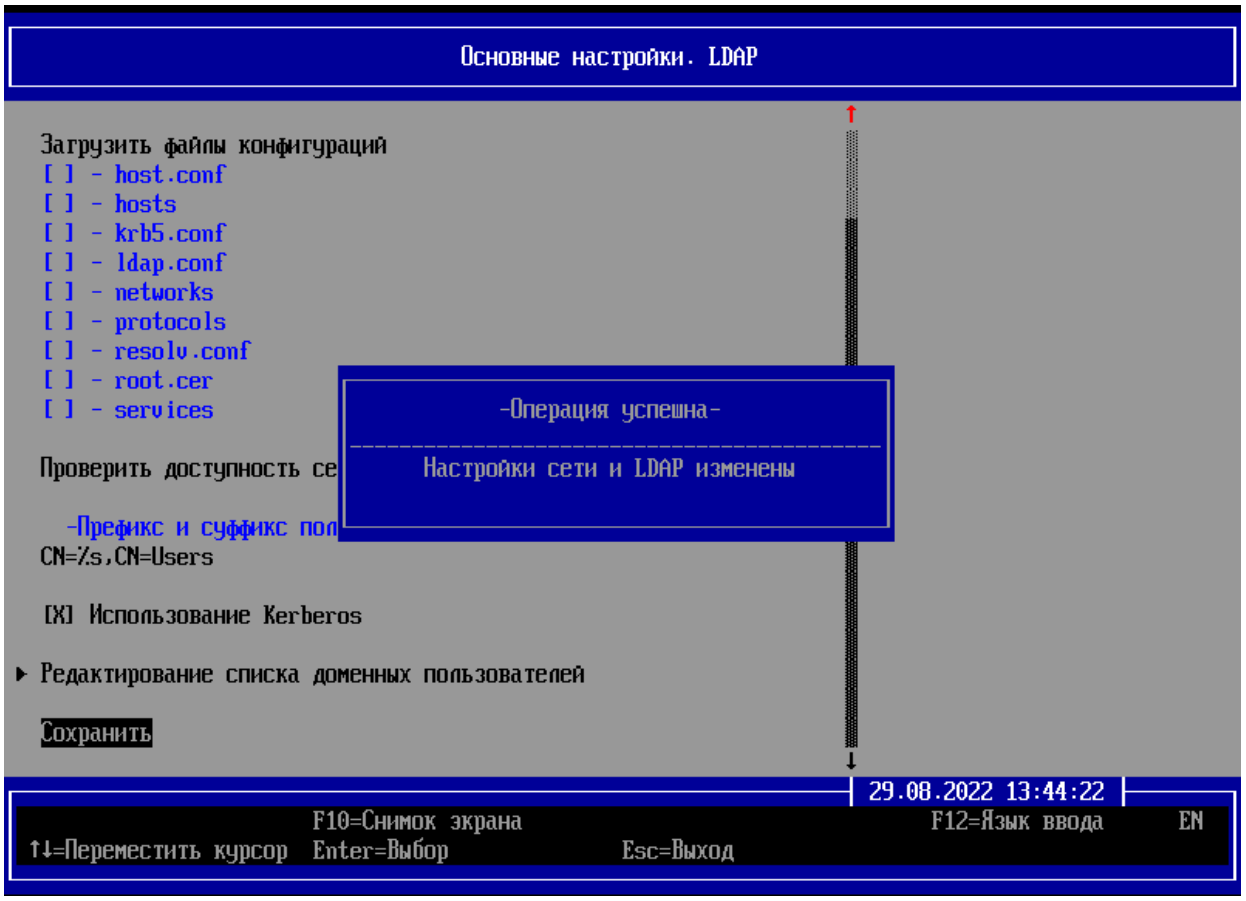


Рисунок 10.12 – Сохранение параметров аутентификации

10.2.14 Для проверки связи с сервером аутентификации LDAP необходимо перейти в поле ***«Проверить доступность сервера LDAP или Kerberos»*** и нажать клавишу ***< Enter >***, при этом осуществится отправка запроса на IP-адрес сервера LDAP.

10.2.15 В случае некорректно указанных настроек на экране ЭВМ появится сообщение ***«Ошибка. Указанный адрес недоступен»*** (рисунок 10.13), в случае наличия связи с сервером аутентификации – сообщение (рисунок 10.14).

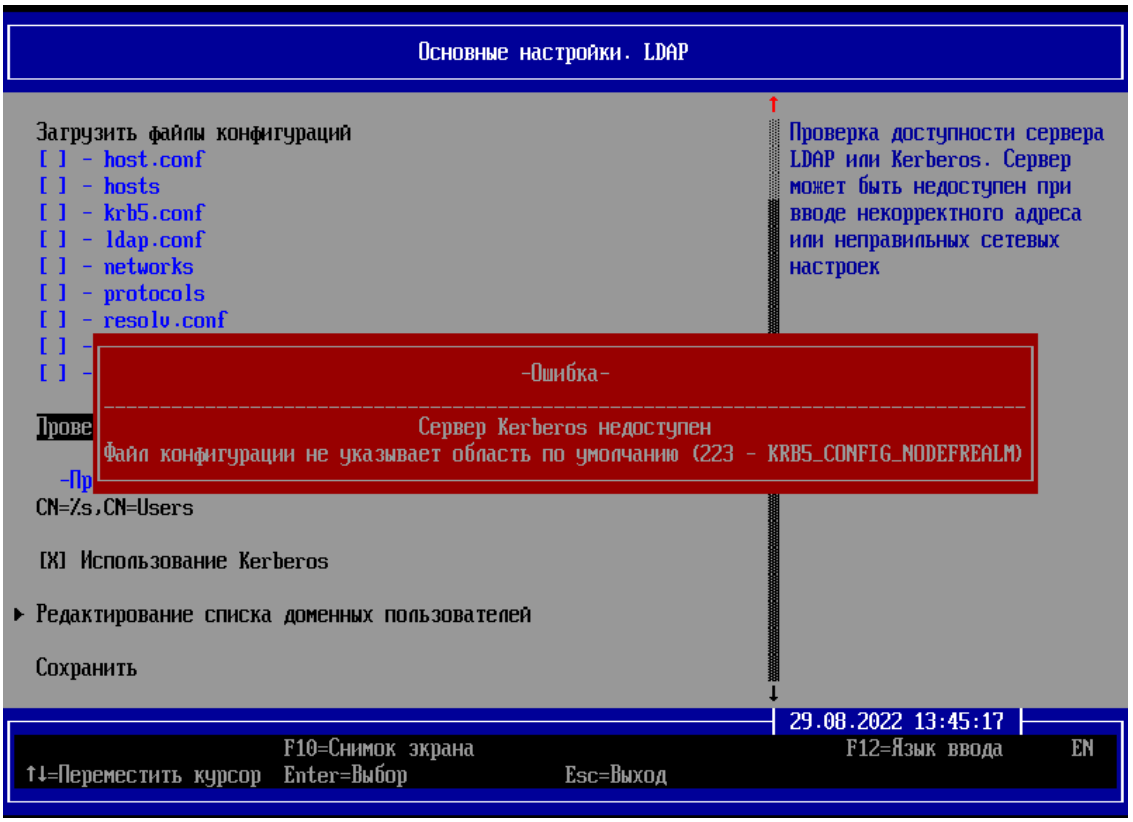


Рисунок 10.13 – Отсутствие связи с сервером LDAP

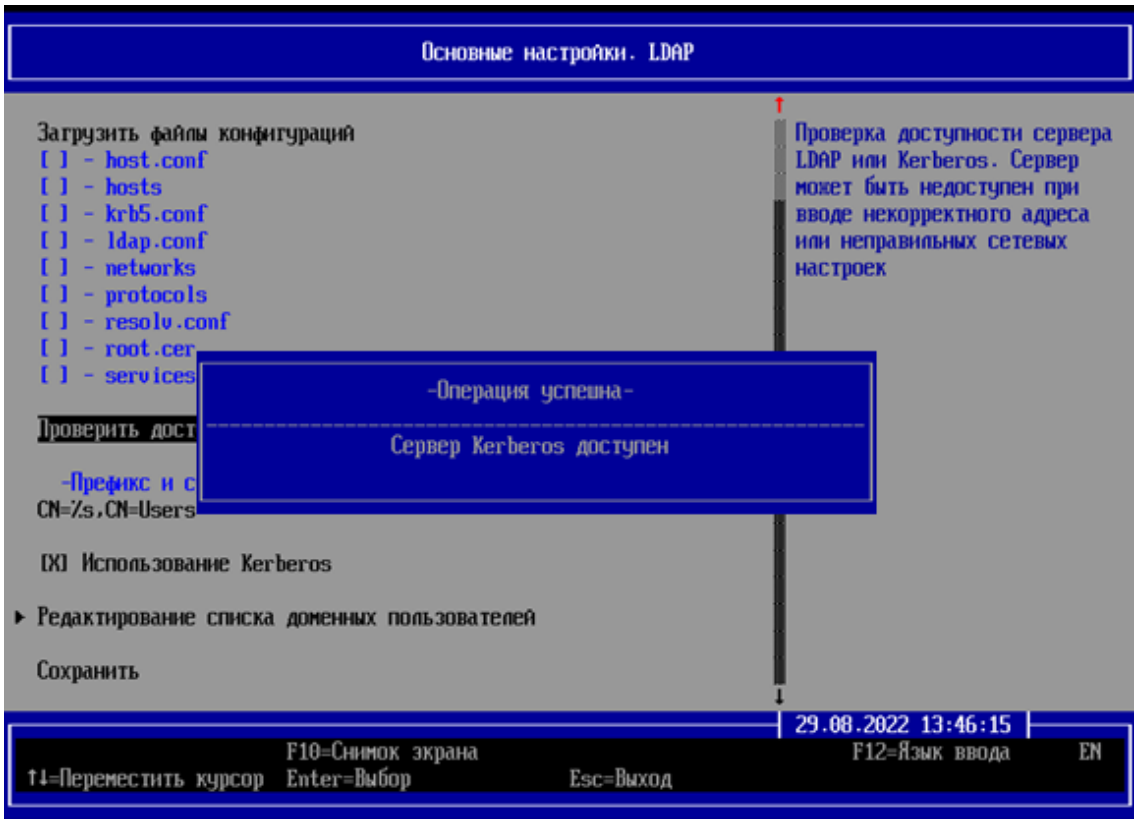


Рисунок 10.14 – Связь с сервером аутентификации LDAP

10.2.16 Поле ***«Префикс и суффикс пользователей»*** (рисунок 10.9) предназначено для установки уникального имени (DN) учетной записи пользователя, состоящего из префикса и суффикса и определяющего имя и домен для аутентификации пользователей. Для редактирования поля следует нажать клавишу **< *Enter* >** и задать параметры в соответствии с форматом, представленным на рисунке 10.15.

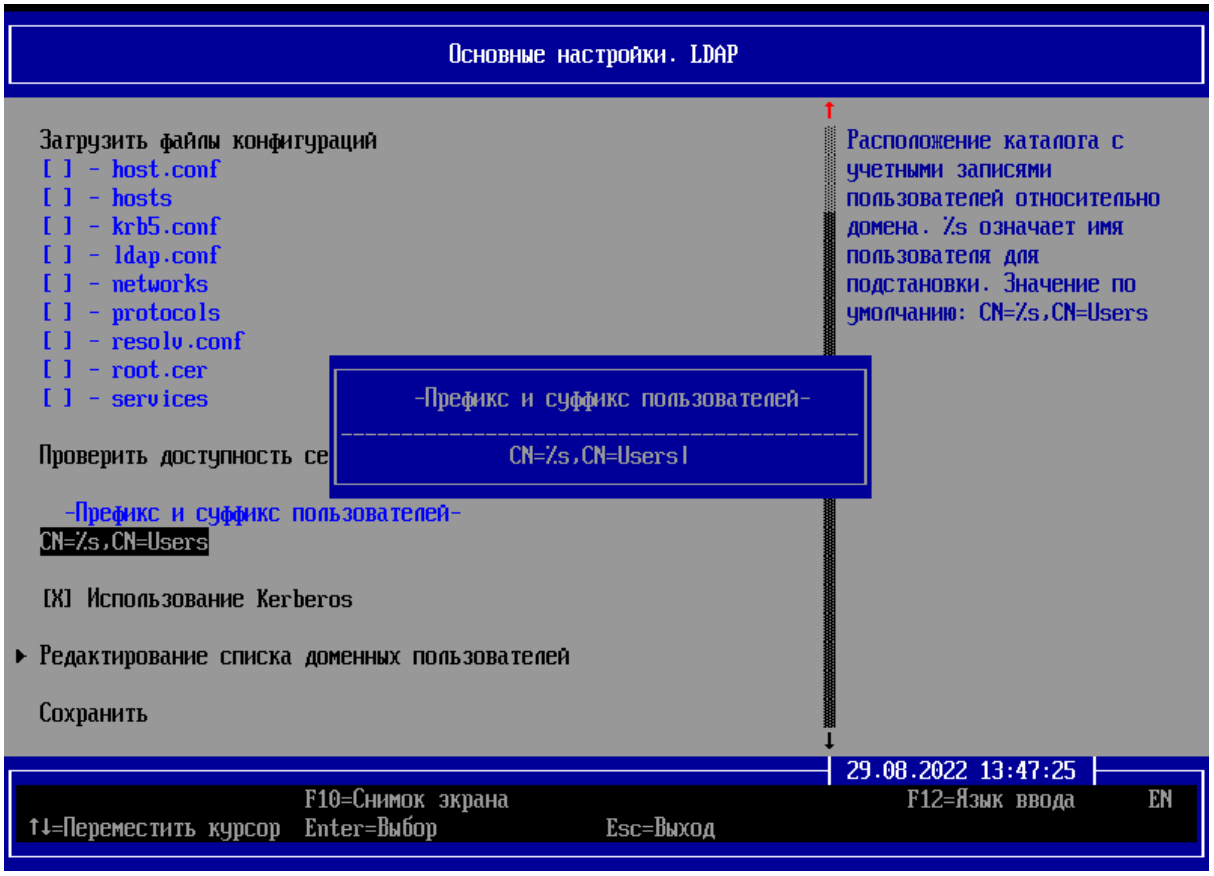


Рисунок 10.15 – Установка префикса и суффикса доменного имени пользователя

10.2.17 При включении аутентификации LDAP устанавливается полное доверие LDAP серверу[5]: при успешной аутентификации пользователя в изделии с учетной записью, сохраненной на LDAP сервере, автоматически создается учетная запись в БД изделия. Пользователю назначается политика аутентификации ***domain policy*** и политика контроля целостности и ОС ***All users***.

[5] Для формирования белого списка доменных учетных записей необходимо перейти в раздел ***«Основной раздел. LDAP»*** → ***«Редактирование списка доменных пользователей».***

В случае отсутствия сетевого соединения при указанных параметрах аутентификации LDAP работа изделия осуществляется в автономном режиме.

Если аутентификация учетной записи пользователя, зарегистрированной на сервере LDAP, была осуществлена ранее, вход будет выполнен по последнему паролю, введенному при наличии сетевого подключения и сохраненному в БД изделия.

10.2.18 Для аутентификации пользователей с сервером LDAP по протоколу Kerberos следует перейти в поле ***«Использование Kerberos»*** и нажать клавишу **< *Enter* >** (рисунок 10.16).

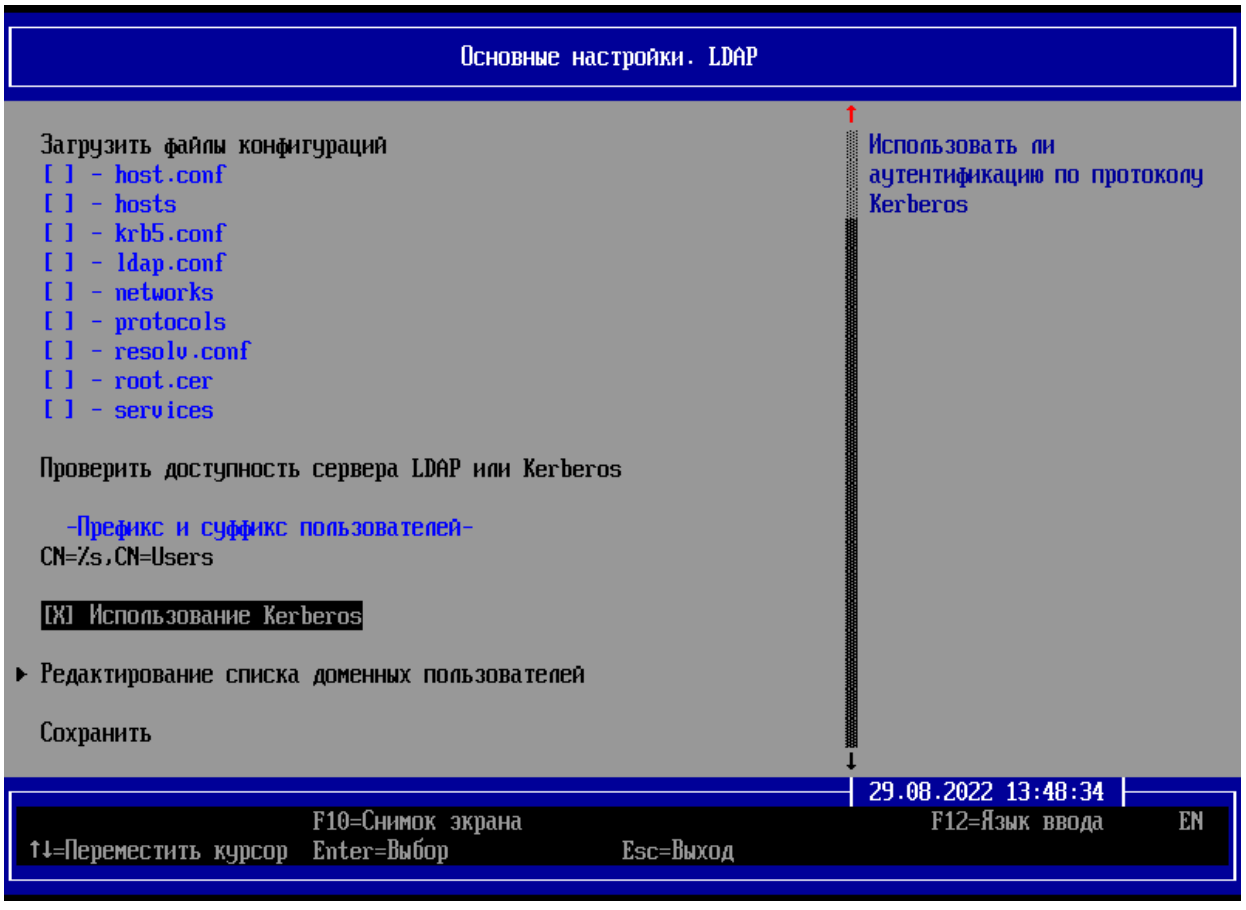


Рисунок 10.16 – Выбор параметра «Использование Kerberos» для изменения

10.2.19 После настройки параметров необходимо сохранить изменения, для этого следует перейти в поле ***«Сохранить»*** нажать клавишу **< *Enter* >** (рисунок 10.17).

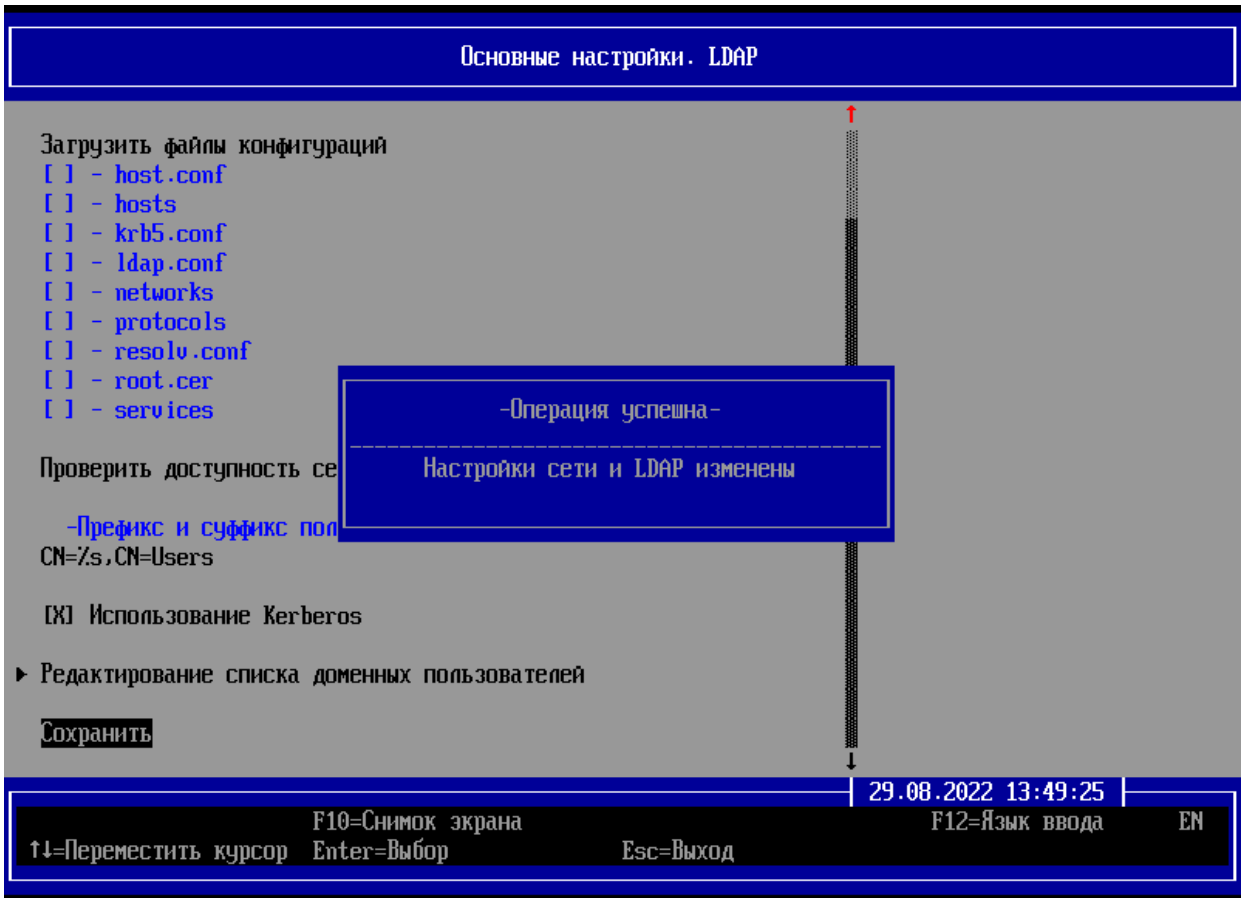


Рисунок 10.17 – Сохранение настроек сети и LDAP

10.2.20 Для работы со списком пользователей и формирования белого списка доменных пользователей необходимо перейти в строку ***«Редактирование списка доменных пользователей»*** и нажать клавишу **< *Enter* >** (рисунок 10.18).

Рисунок 10.18 – Редактирование списка доменных пользователей

10.2.21 Для получения списка пользователей, зарегистрированных на сервере LDAP, необходимо предварительно осуществить настройки параметров сетевого взаимодействия (см. ***«Основные настройки. Сетевые настройки»***). Затем выбрать ***«Открыть список»*** в области ***«Список пользователей на сервере LDAP»*** нажать клавишу **< *Enter* >** (рисунок 10.19).

10.2.22 После указания имени администратора, необходимо ввести пароль к данной учетной записи (рисунок 10.20).

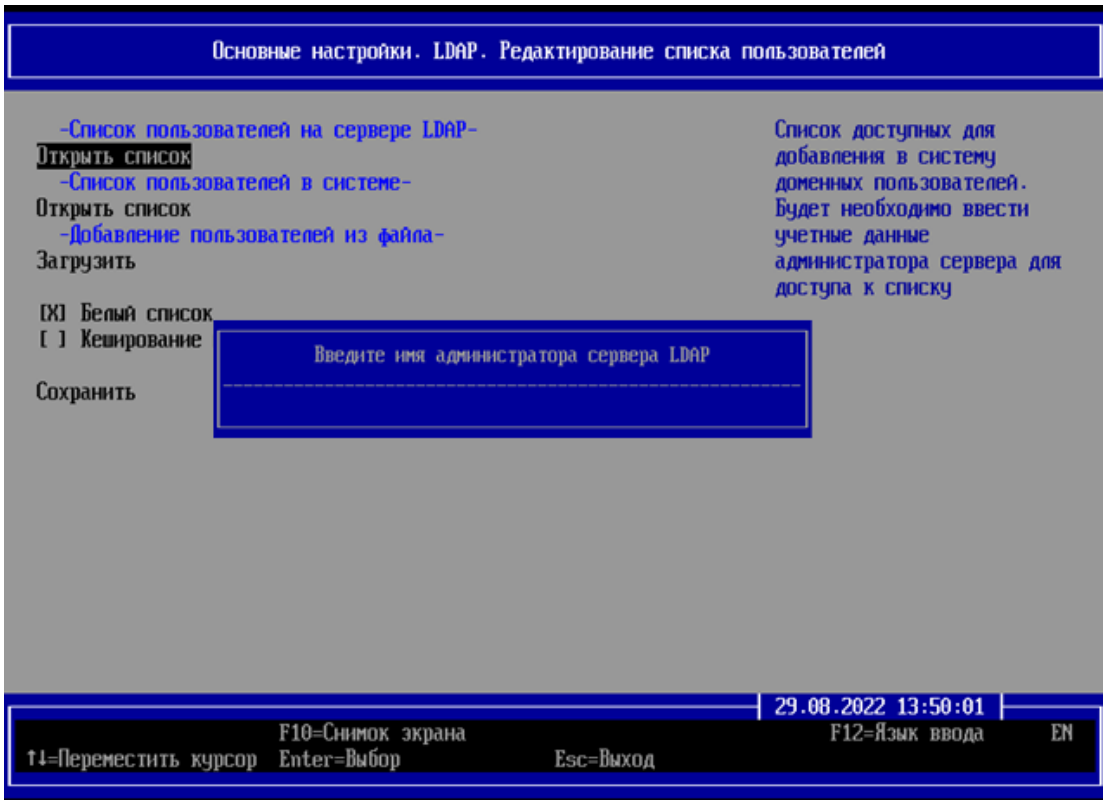


Рисунок 10.19 – Ввод аутентификационных данных администратора сервера LDAP

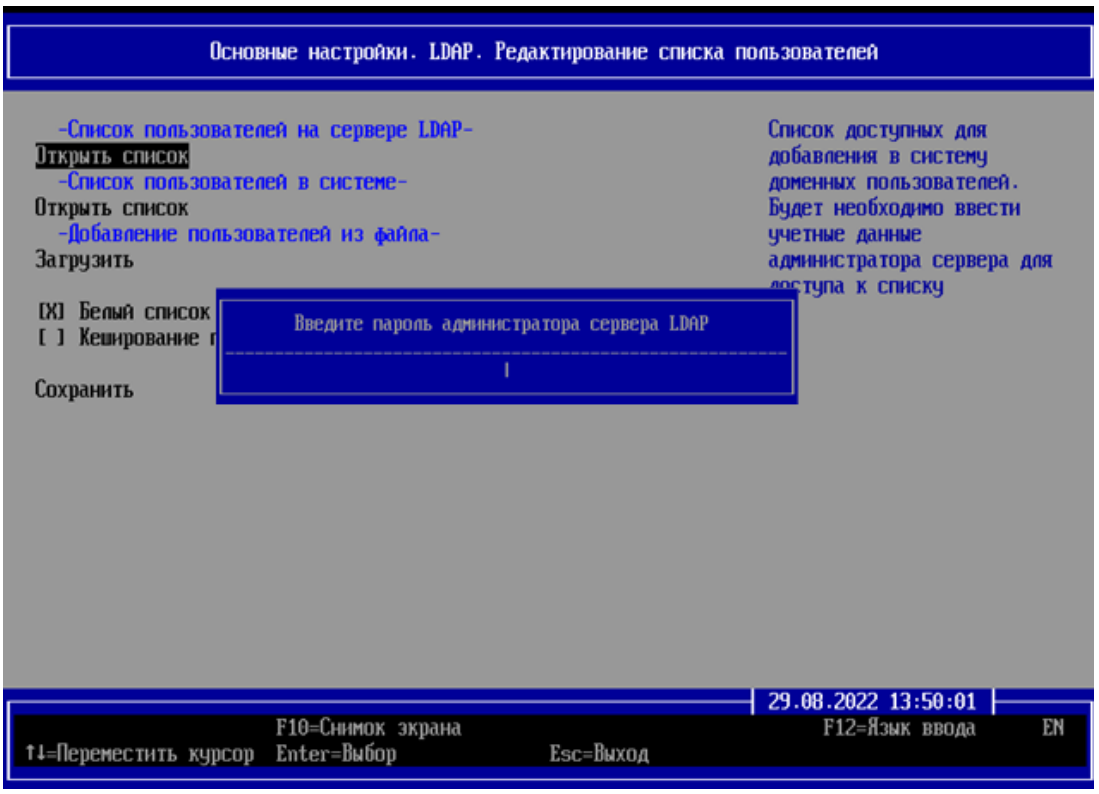


Рисунок 10.20 – Указание пароля администратора сервера LDAP

10.2.23 При верном вводе аутентификационных данных администратора сервера LDAP, появится перечень зарегистрированных пользователей данного сервера (рисунок 10.21) [6].

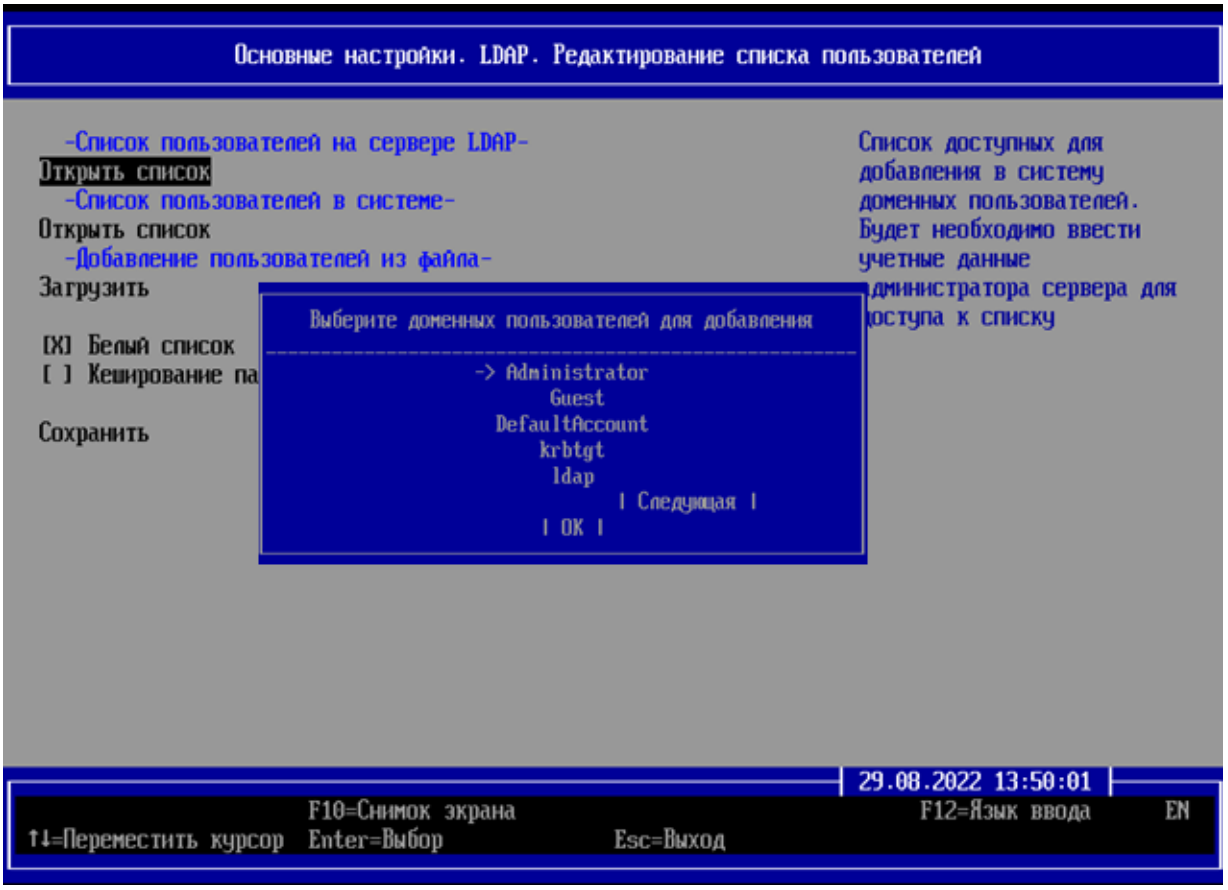


Рисунок 10.21 – Доменные пользователи для добавления

10.2.24 Из указанного перечня необходимо выбрать доменные учетные записи пользователей, которым будет разрешен вход.

Необходимо последовательно выбирать учетные записи пользователей с помощью клавиши **< *Enter* >** (рисунок 10.21).

10.2.25 Выбранные учетные будут добавлены в систему. Для просмотра добавленного списка доменных пользователей необходимо выбрать ***«Открыть список»*** в области ***«Список пользователей в системе»*** нажать клавишу **< *Enter* >** (рисунок 10.22). При необходимости, из данного перечня можно исключить учетную запись пользователя, путем снятия выделения и нажатия кнопки **| *OK* |**.

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

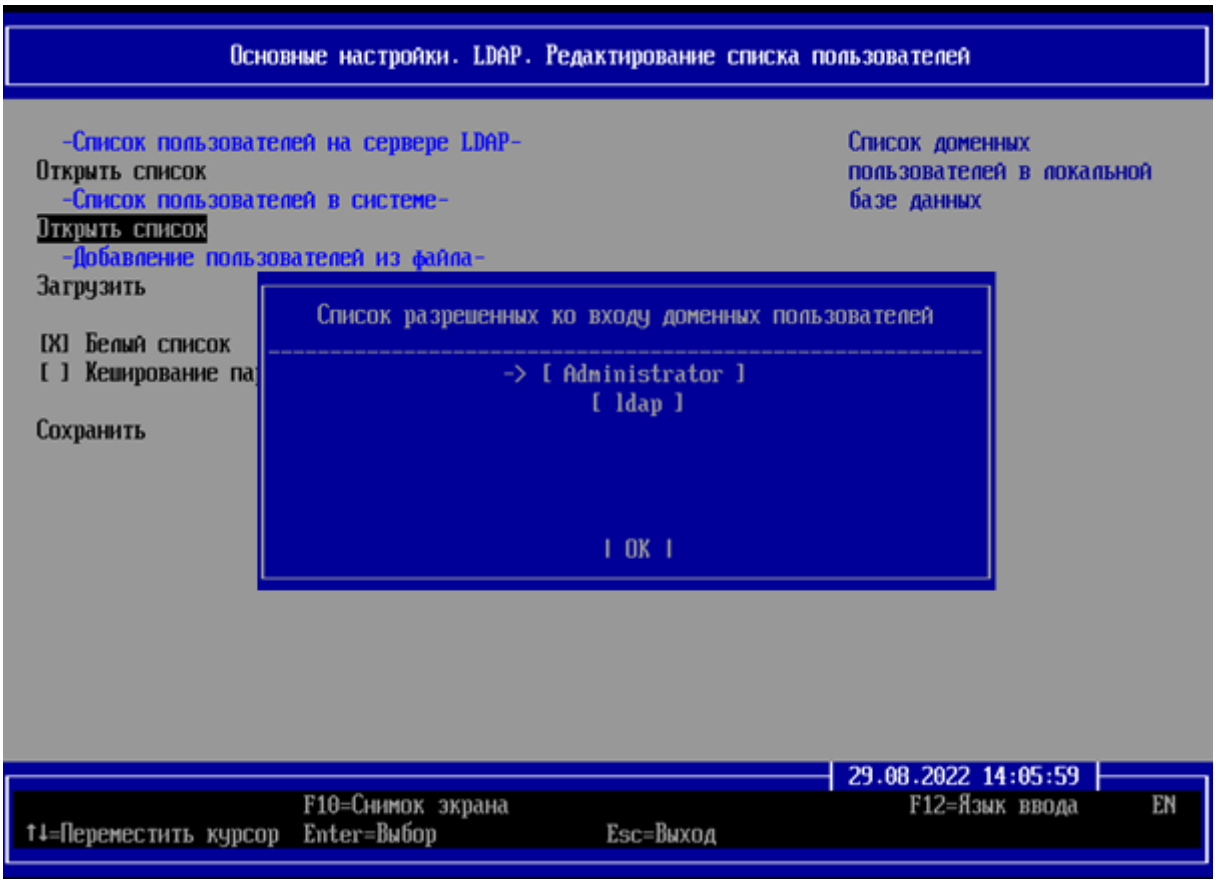


Рисунок 10.22 – Добавленные доменные пользователи

10.2.26 В системе реализована возможность загрузки заранее сформированного перечня доменных пользователей с помощью файла.

Файл ***userlist.tx***t должен размещаться в корне раздела. Каждая доменная учетная запись пользователя должна размещаться на отдельной строке.

10.2.27 Для загрузки пользователей с помощью списка необходимо перейти в область ***«Добавление пользователей из файла»***, выбрать ***«Загрузить»*** и нажать клавишу ***< Enter >*** (рисунок 10.23).

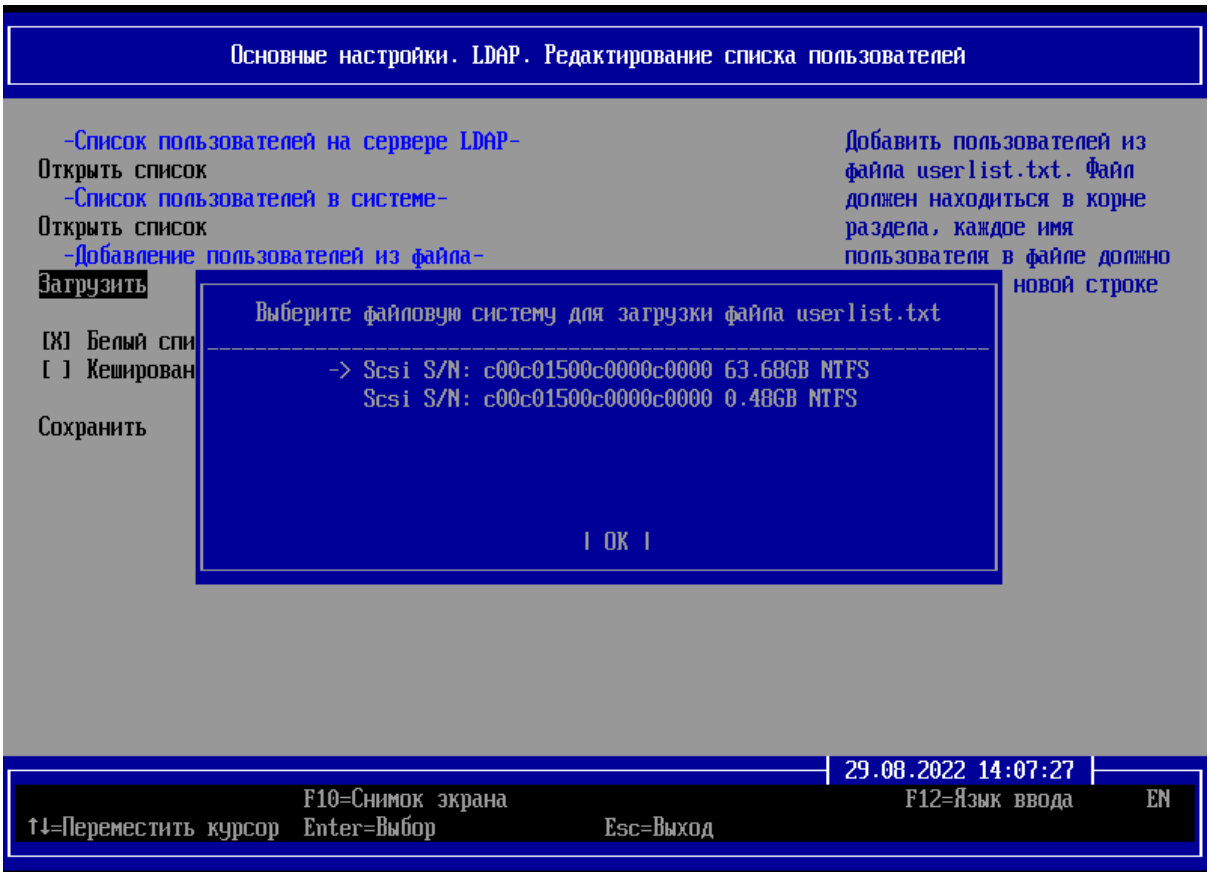


Рисунок 10.23 – Выбор файловой системы для загрузки

10.2.28 В случае успешной загрузки списка пользователей из файла ***userlist.txt*** на экране ЭВМ появится диалоговое окно рисунка 10.24, неуспешной попытке загрузки рисунок 10.25.

При сформированном списке доменных пользователей в системе, пользователи из файла ***userlist.txt*** добавляются к существующему перечню.

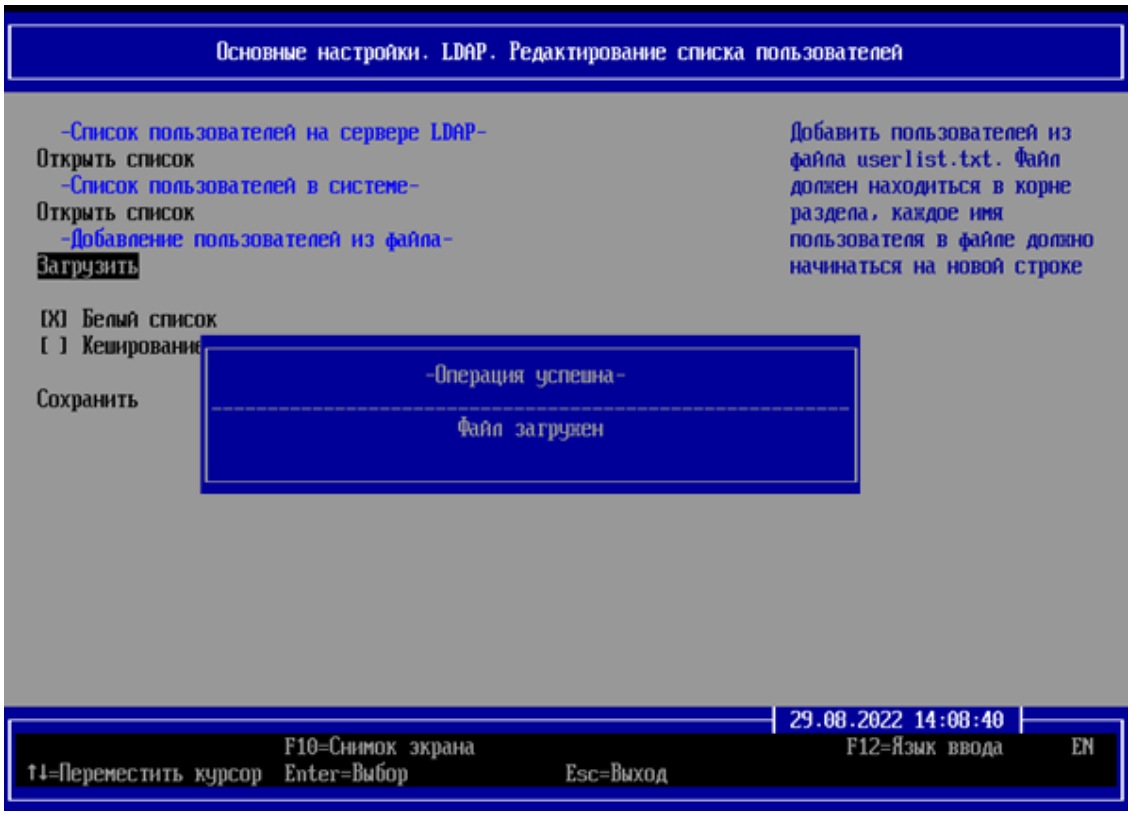


Рисунок 10.24 – Успешная загрузка списка пользователей

Рисунок 10.25 – Ошибка при загрузке списка пользователей

10.2.29 Для применения данного списка пользователей как разрешенного для прохождения аутентификации, необходимо перейти в поле ***«Белый список»*** и нажать клавишу **< *Enter* >** [7] (рисунок 10.26).

Рисунок 10.26 – Включение белого списка

10.2.30 После установки параметров необходимо перейти в поле ***«Сохранить»*** и нажать клавишу **< *Enter* >**. В случае успешного применения появится сообщение (рисунок 10.27).

[7] Активация данного режима означает, что при прохождении процедуры аутентификации устанавливается полное доверие домену. Включать данный режим можно только при использовании сертифицированного домена.

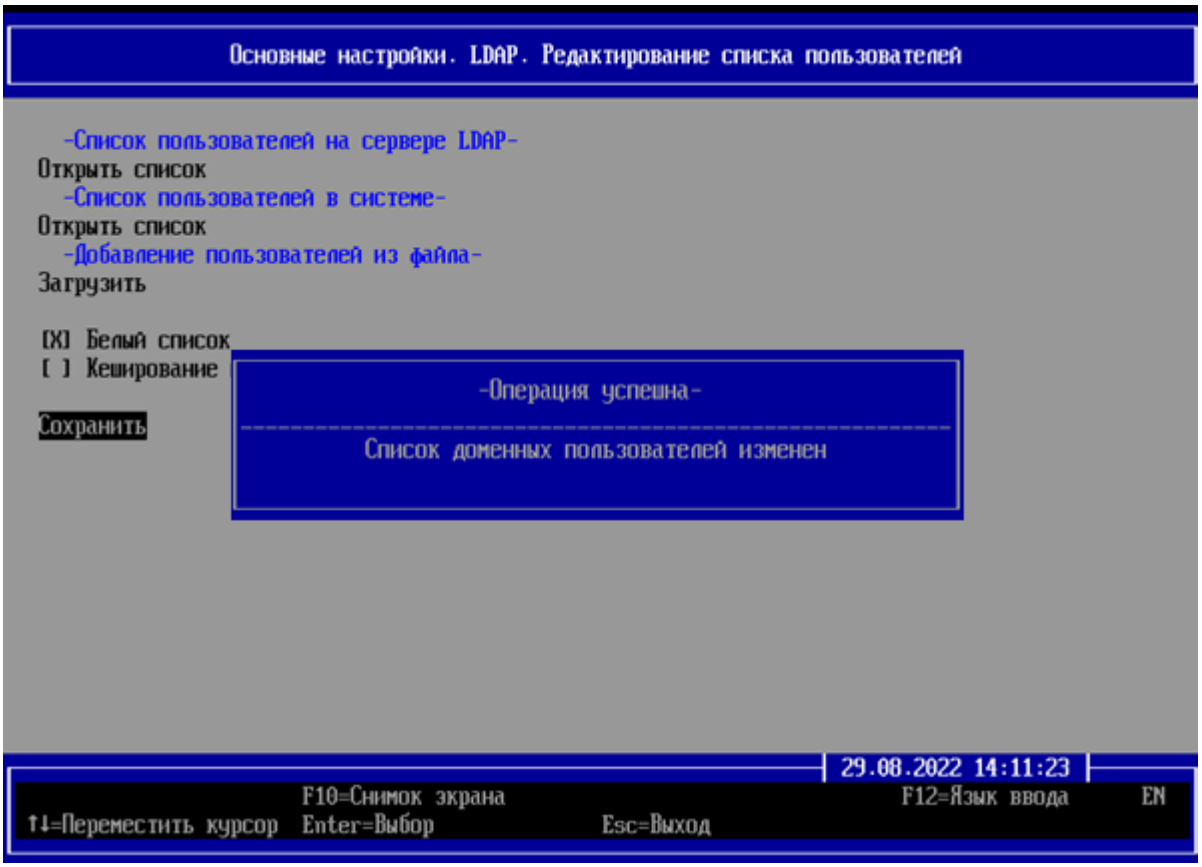


Рисунок 10.27 – Сохранение списка доменных пользователей

10.3 Настройки времени

10.3.1 В ПО изделия присутствует возможность синхронизации времени с указанным в настройках NTP сервером. Настройка времени позволяет избежать ошибок аутентификации доменных пользователей в изделии, так как если системное время компьютеров пользователей будет отличаться от времени на контроллере домена, пользователи не смогут успешно пройти процедуру аутентификации.

10.3.2 Для настройки времени необходимо в окне ***«Основные настройки»*** перейти в строку ***«Настройки времени»*** (рисунок 10.28) и нажать клавишу ***< Enter >***.

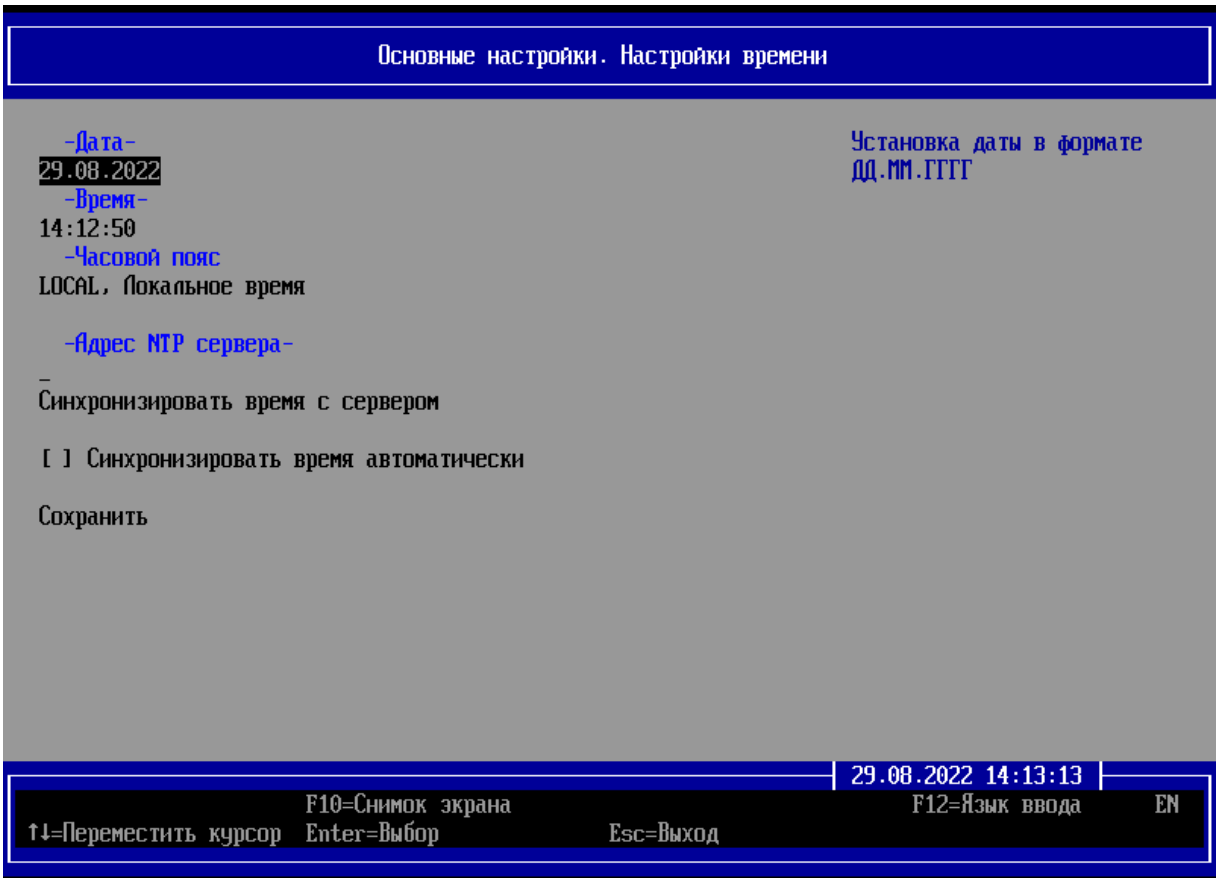


Рисунок 10.28 – Настройка времени

10.3.3 В появившемся диалоговом окне (рисунок 10.28) доступны для изменения следующие параметры (принимаемые параметрами значения и их описание приведены в таблице 10.1):

- ***«Дата»*** – позволяет в ручном режиме установить дату в формате ДД.ММ.ГГ;
- ***«Время»*** – позволяет в ручном режиме установить время в формате ЧЧ.ММ.СС;
- ***«Часовой пояс»*** – установка требуемого часового пояса из списка;
- ***«Адрес NTP сервера»*** – указание адреса NTP сервера.

10.3.4 После заполнения требуемых полей, для принудительной синхронизации времени с NTP сервером необходимо выбрать поле ***«Синхронизировать время с сервером»*** (рисунок 10.28). В случае, если сетевые параметры были указаны некорректно, появится сообщение об ошибке (рисунок 10.29).

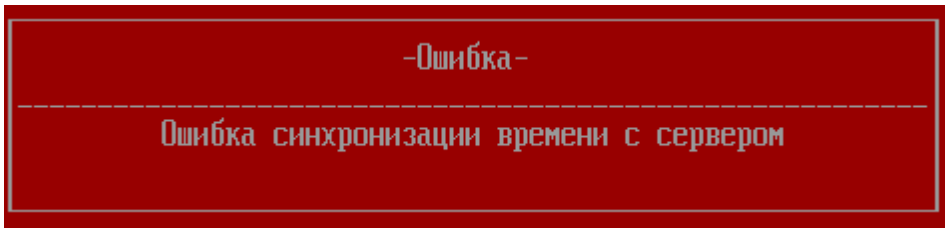


Рисунок 10.29 – Сообщение об ошибке при синхронизации с NTP сервером

10.3.5 Для автоматической синхронизации с сервером NTP при старте ЭВМ необходимо установить поле ***«Синхронизировать время автоматически»*** в состояние **< *Включено* >** и нажать ***Сохранить*** для сохранения текущих настроек.

10.4 Защита от перевода времени назад

10.4.1 В ПО изделия присутствует возможность установки защиты от перевода назад времени, установленного в настройках системы UEFI BIOS. Данная функция изделия позволяет нейтрализовать угрозу, связанную с попытками подбора паролей пользователей при переводе времени назад.

10.4.2 Для включения защиты от перевода времени назад необходимо в окне ***«Основные настройки»*** перейти в строку ***«Защита от перевода времени»*** (рисунок 10.30) и нажать клавишу **< *Enter* >**.

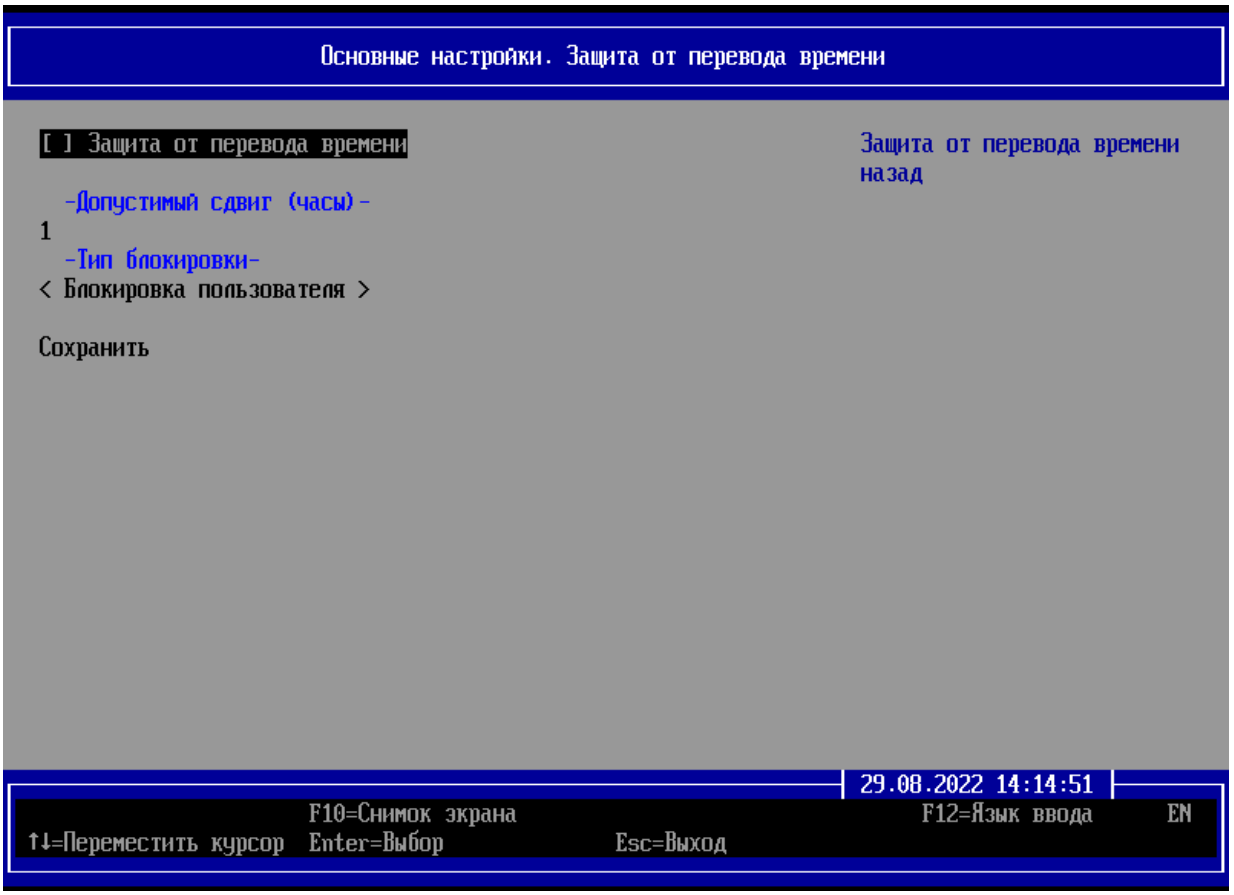


Рисунок 10.30 – Настройка защиты от перевода времени назад

10.4.3 В появившемся диалоговом окне (рисунок 10.30) доступны для изменения следующие параметры (принимаемые параметрами значения и их описание приведены в таблице 10.1):

- ***«Защита от перевода времени»*** – включение (выключение) параметра защиты от перевода пользователем времени назад;
- ***«Допустимый сдвиг (часы)»*** – установка допустимого значения перевода времени, при котором блокировка пользователя не будет осуществлена;
- ***«Тип блокировки»*** – установка типа блокировки пользователя при превышении допустимого сдвига времени.

10.4.4 При превышении допустимого перевода времени, установленного в параметре ***«Допустимый сдвиг (часы)»***, вход пользователя в систему выполнен не будет, учетная запись пользователя блокируется и на экран ЭВМ выводится сообщение о блокировке доступа (рисунок 6.22).

10.4.5 При первой аутентификации АБ после выявленного нарушения на экране появится сообщение об обнаружении ошибок в журнале аудита (рисунок 11.5), содержащее запись об обнаружении перевода времени (рисунок 10.31).

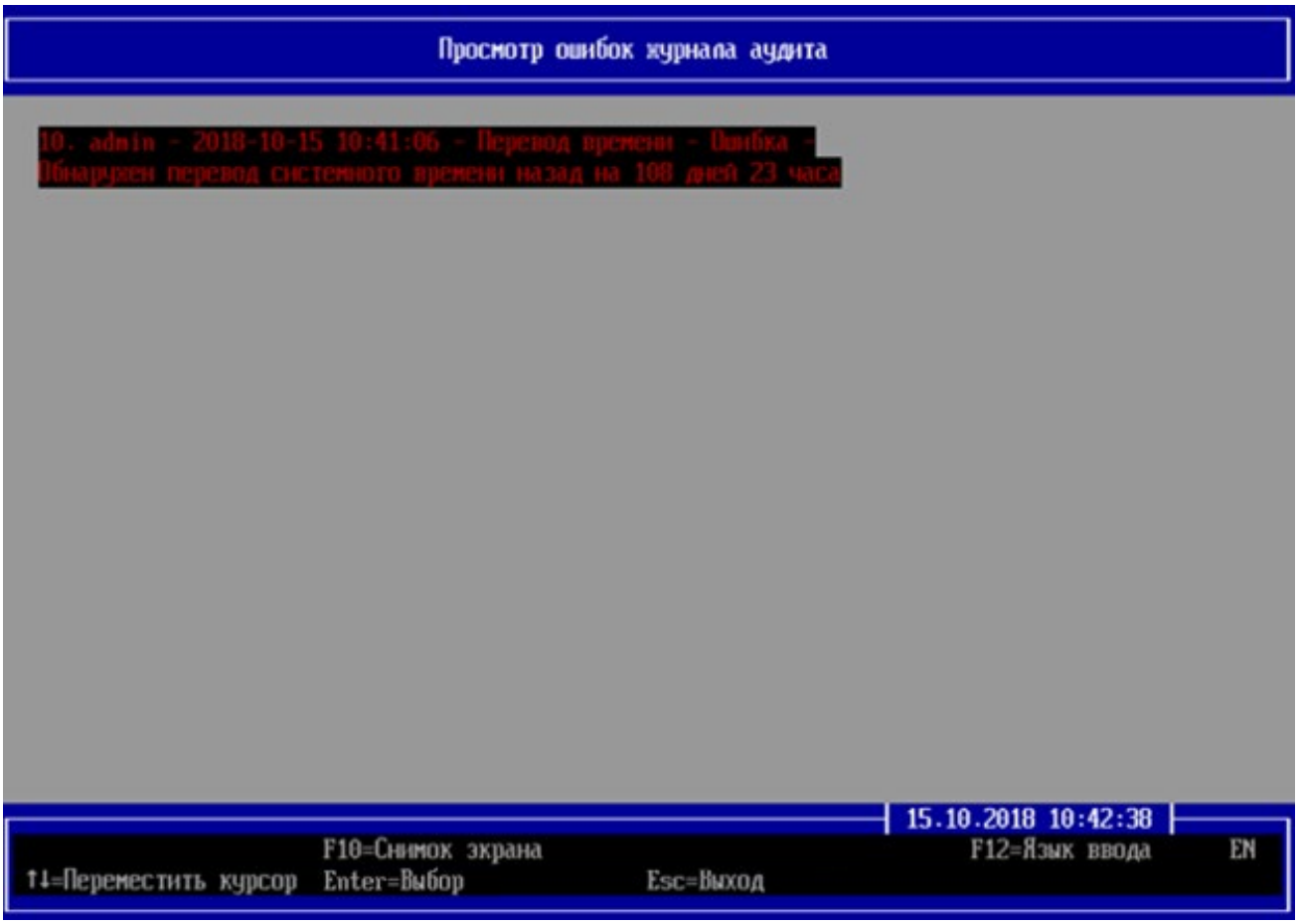


Рисунок 10.31 – Ошибка в журнале аудита о переводе времени назад

При переводе времени **вперед** защита не блокирует пользователей и сообщений о переводе времени АБ не поступает.

10.5 Настройка основного меню

10.5.1 Для настройки отображения элементов меню основной консоли АБ при расширенном режиме функционирования необходимо в окне ***«Основные настройки»*** перейти в строку ***«Прочие параметры»*** (рисунок 10.1) и нажать клавишу ***< Enter >***.

10.5.2 В появившемся диалоговом окне необходимо перейти в строку ***«Настройка основного меню»*** и нажать клавишу ***< Enter >***.

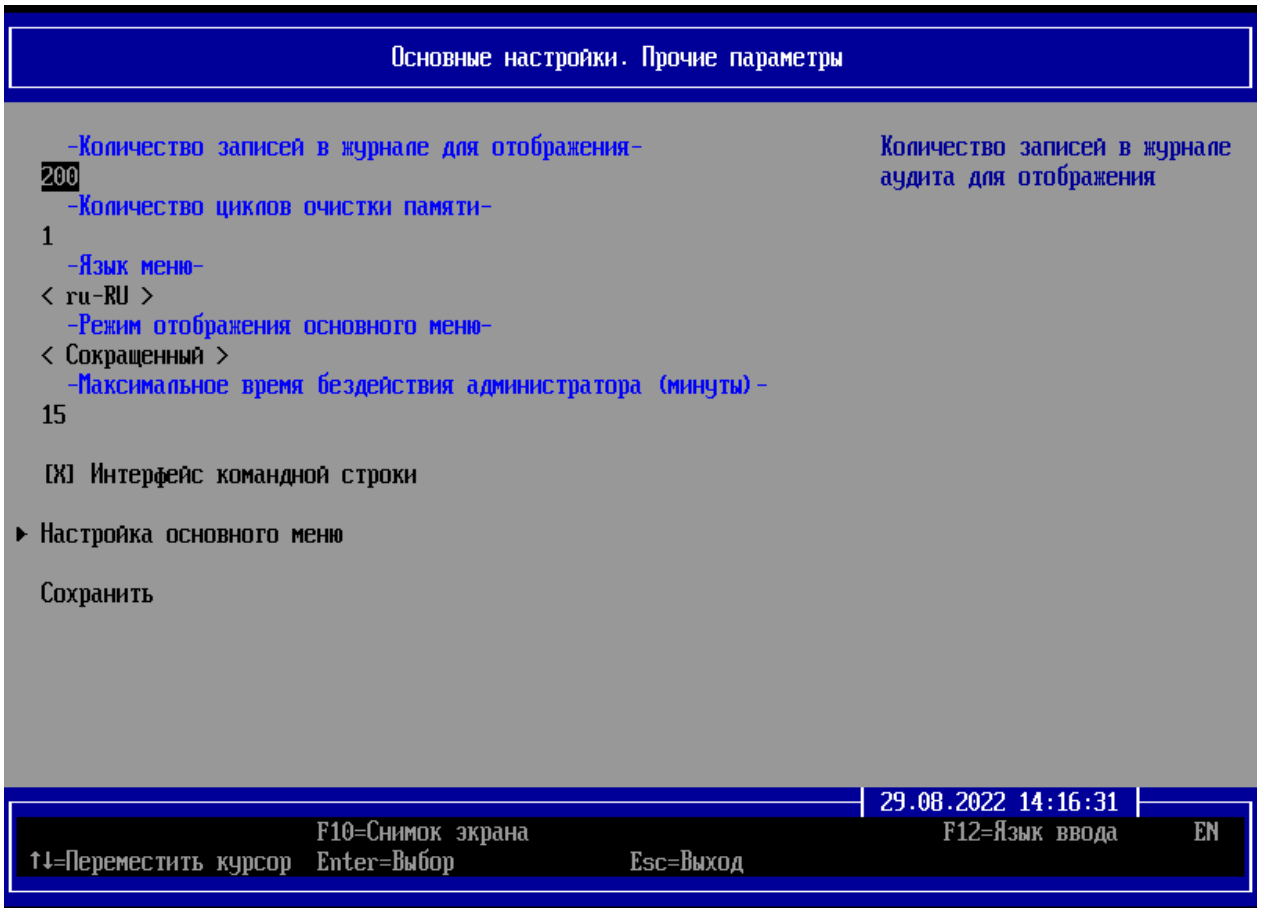


Рисунок 10.32 – Содержимое пункта ***«Прочие параметры»***

10.5.3 В появившемся диалоговом окне АБ необходимо выбрать элементы меню, которые будут отображены при расширенном режиме функционирования (рисунок 10.32).

10.5.4 Для сохранения введенных значений необходимо перейти в строку ***«Сохранить»*** (рисунок 10.33) и нажать клавишу **< *Enter* >**. При этом в новом диалоговом окне будет выведено сообщение об успешном изменении настроек (рисунок 10.3).

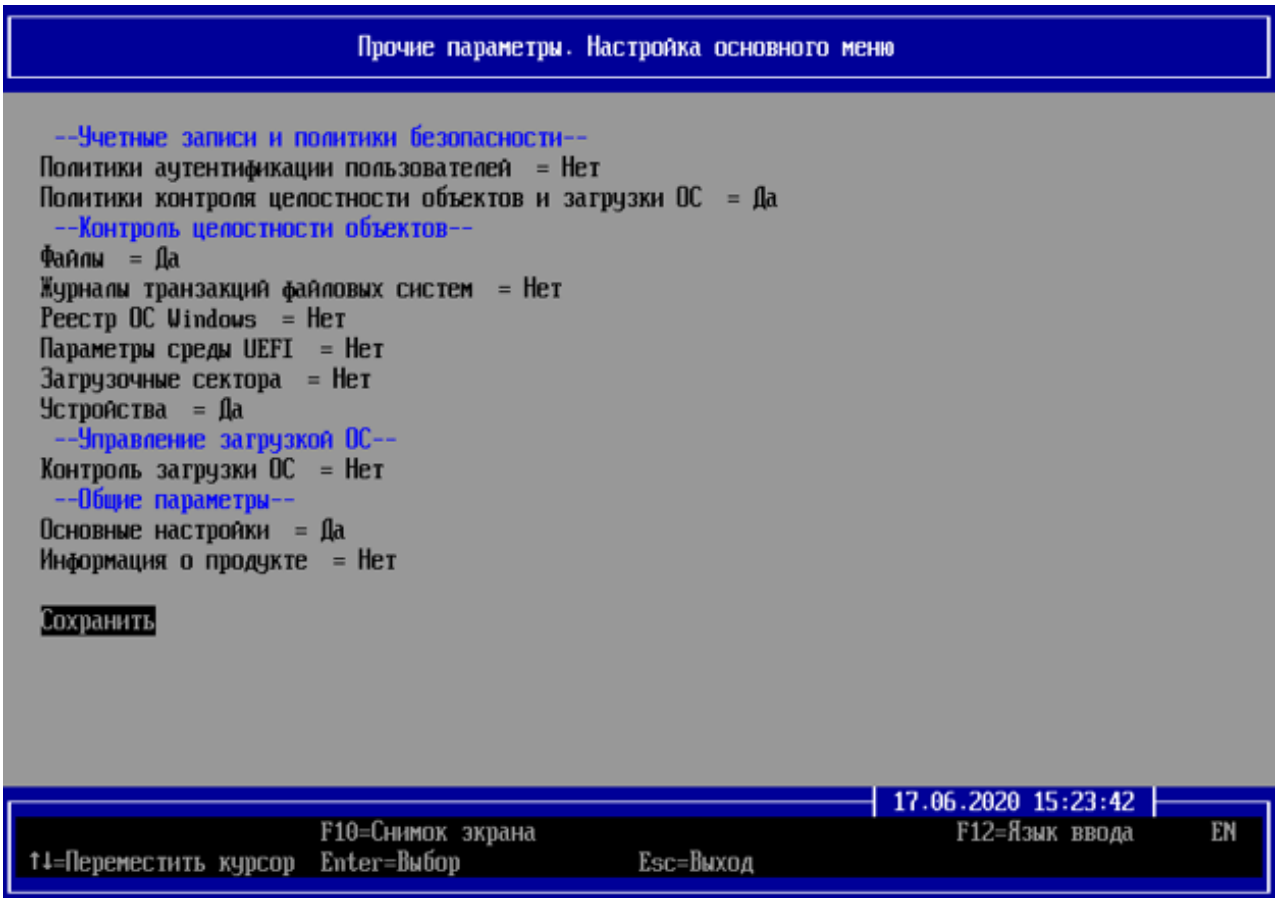


Рисунок 10.33 – Выбор элементов меню для отображения при расширенном режиме функционирования

10.5.5 Для смены языка отображения интерфейса необходимо в окне ***«Основные настройки. Прочие параметры»*** (рисунок 10.32) выбрать пункт ***«Язык меню»***, нажать клавишу ***< Enter >*** и выбрать необходимый язык отображения. Изменения вступят в силу после перезагрузки системы (рисунок 10.34).

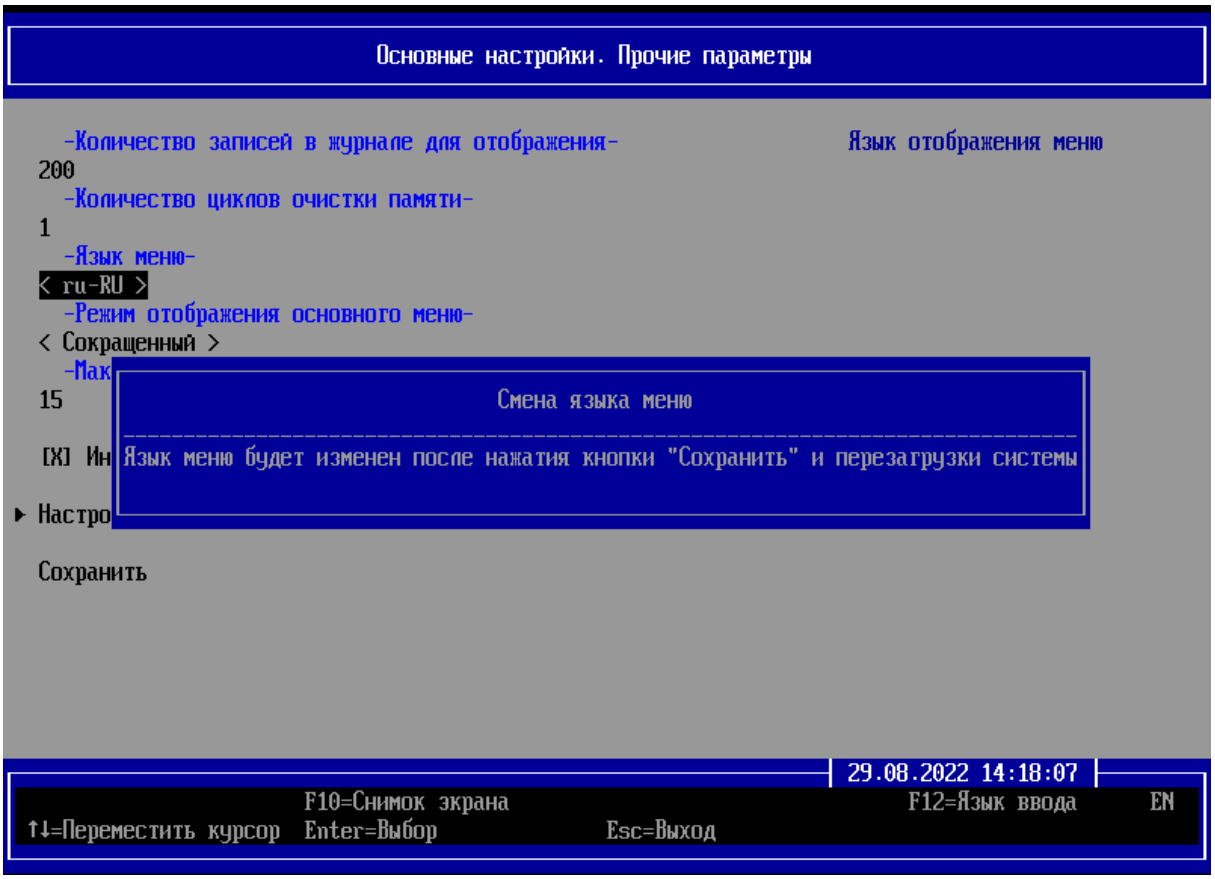


Рисунок 10.34 – Изменение языка отображения меню

10.5.6 Для включения поддержки режима командной строки необходимо перейти в соответствующее поле ***«Интерфейс командной строки»*** в диалоговом окне ***«Основные настройки. Прочие параметры»*** (рисунок 10.32) и нажать клавишу ***< Enter >*** (рисунок 10.35).

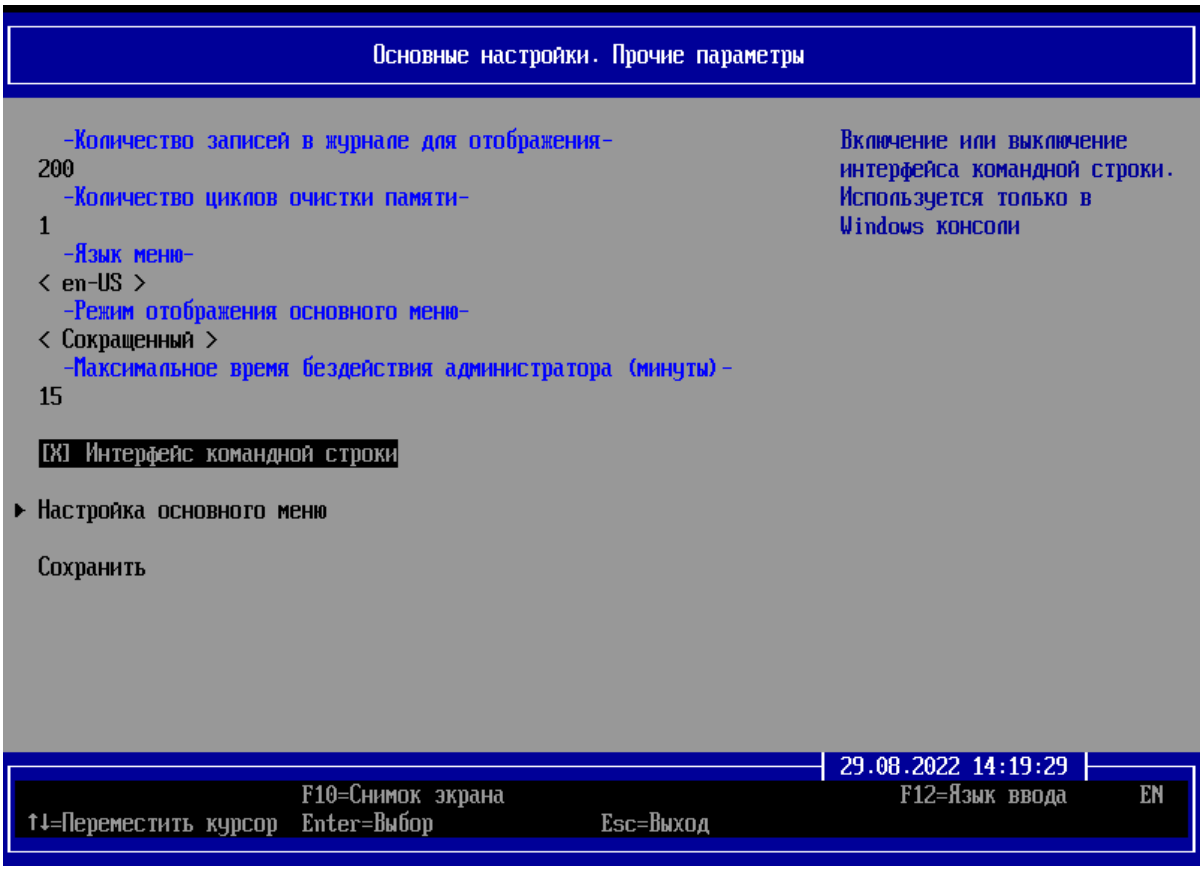


Рисунок 10.35 – Включение параметра «Интерфейс командной строки»

10.5.7 Описание работы с интерфейсом командной строки приведено в разделе 12 документа «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 3. Руководство администратора Linux/Windows. ГМТК.468269.060РЭ3».

10.5.8 Для установки максимального значения времени бездействия АБ при работе с консолью необходимо в диалоговом окне ***«Основные настройки. Прочие параметры»*** (рисунок 10.32) перейти в поле ***«Максимальное время бездействия администратора (минуты)»*** и нажать клавишу ***< Enter >***.

10.5.9 В появившемся диалоговом окне (рисунок 10.36) следует указать необходимое значение в пределах допустимых параметров и нажать клавишу ***< Enter >***.

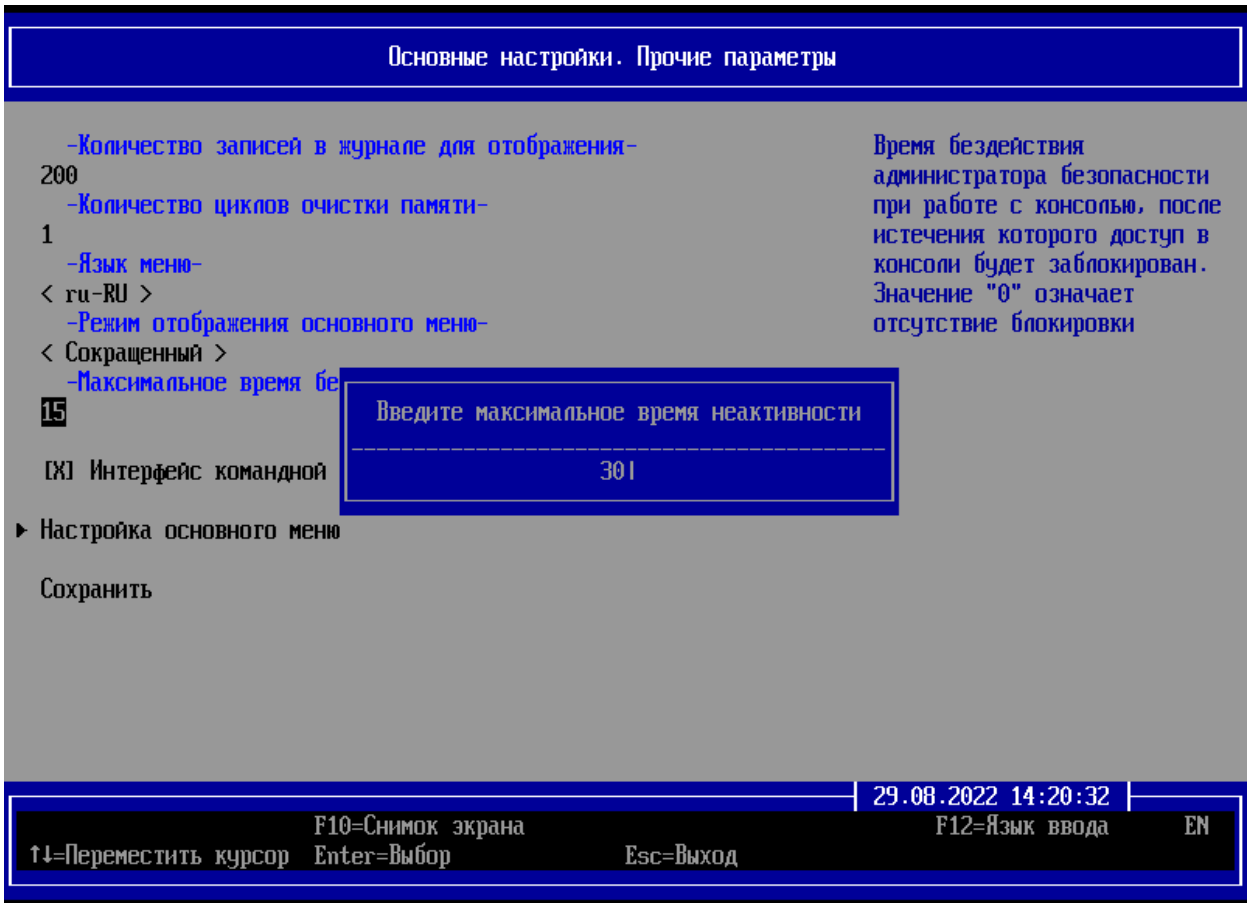


Рисунок 10.36 – Определение максимального времени неактивности АБ

10.5.10 При достижении максимального времени бездействия АБ при работе с консолью появится соответствующее информационное сообщение и осуществится блокировка доступа.

10.5.11 При входе в консоль после перезагрузки ЭВМ на экране появится сообщение об обнаружении ошибок в журнале аудита (рисунок 11.5), содержащее запись об обнаружении истечения максимального времени неактивности АБ (рисунок 10.37).

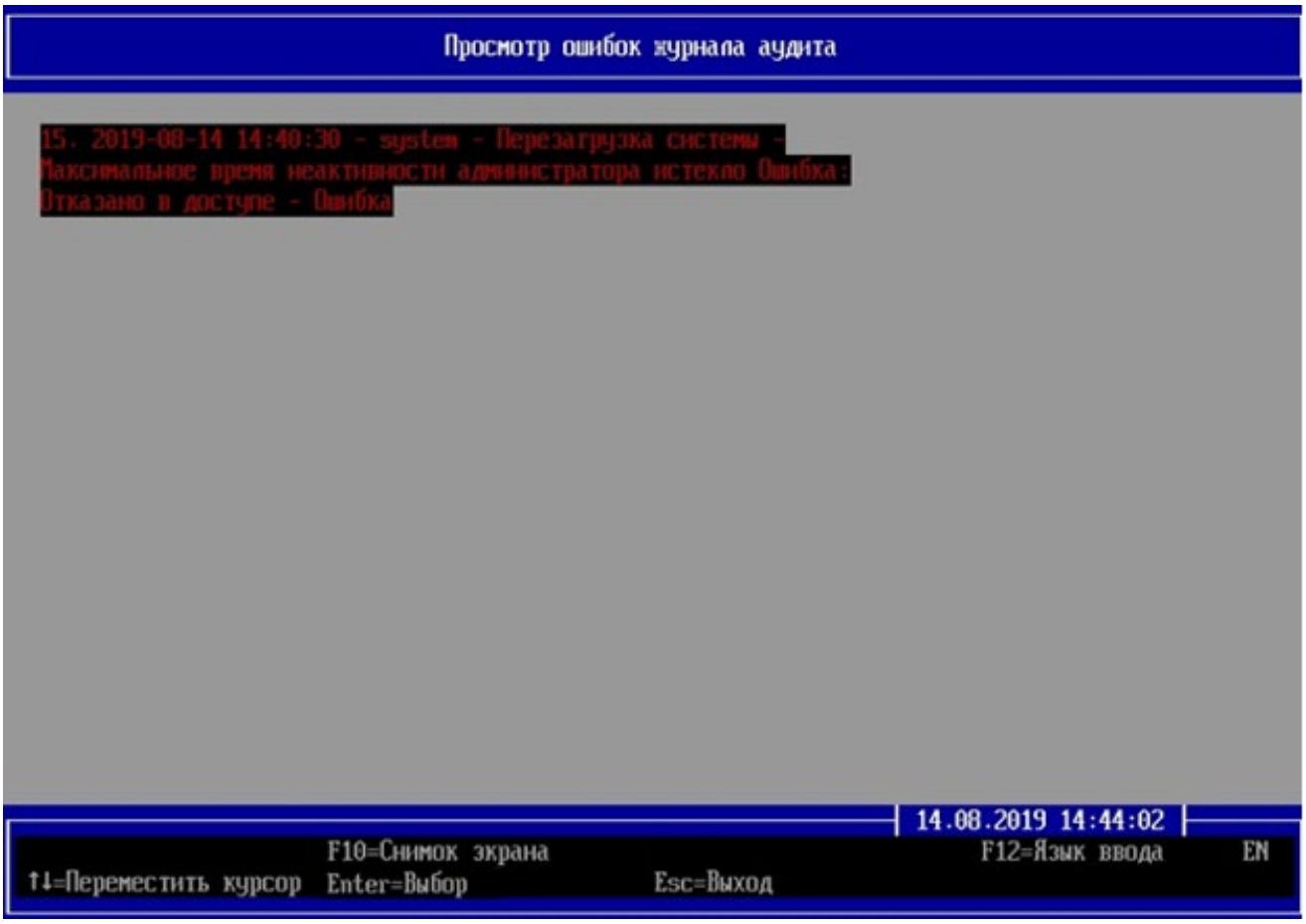


Рисунок 10.37 – Ошибка в журнале аудита об истечении максимального времени неактивности администратора

10.6 Оптимизация базы данных

10.6.1 Для оптимизации работы БД изделия (уменьшение размера) в окне ***«Основные настройки»*** необходимо перейти в строку ***«Оптимизация базы данных»*** (рисунок 10.1) и нажать клавишу ***< Enter >.***

10.6.2 В случае успешной оптимизации БД АБ в диалоговом окне будет выведено сообщение об успешной оптимизации БД (рисунок 10.38).

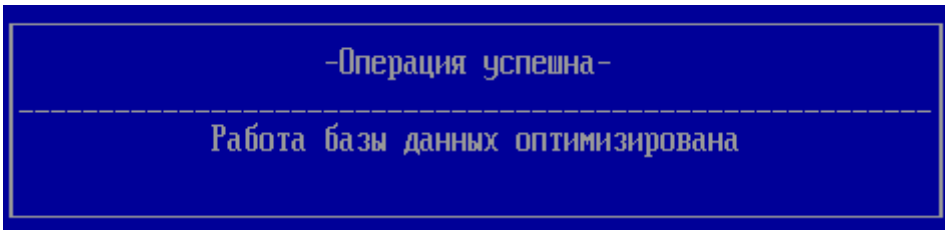


Рисунок 10.38 –Успешная оптимизация работы БД изделия

10.7 Восстановление заводских настроек

10.7.1 Для восстановления параметров изделия к стандартным заводским настройкам в окне ***«Основные настройки»*** необходимо перейти в строку ***«Восстановить заводские настройки»*** (рисунок 10.1) и нажать клавишу ***< Enter >***, при этом на экран ЭВМ будет выведено диалоговое окно (рисунок 10.39).

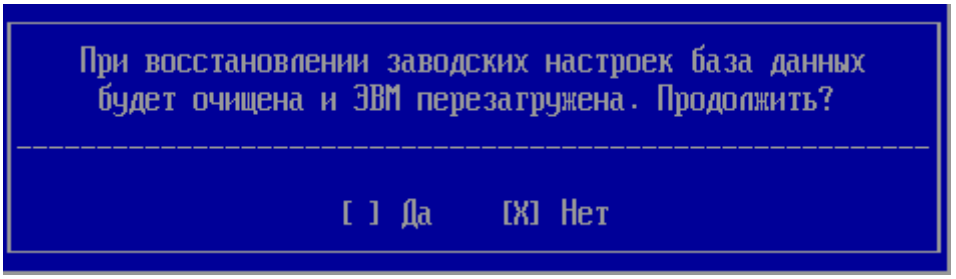


Рисунок 10.39 – Восстановление заводских настроек изделия

При восстановлении заводских настроек изделия вся информация из БД изделия будет удалена и ЭВМ будет перезагружена.

Защита от входа в BIOS Setup при восстановлении настроек изделия к заводским параметрам отключается до момента завершения установки СДЗ.

10.8 Обновление ПО

10.8.1 Для обновления системного ПО изделия АБ необходимо в окне ***«Основные настройки»*** перейти в строку ***«Обновить системное ПО»*** (рисунок 10.1) и нажать клавишу ***< Enter >***, при этом на экран ЭВМ будет выведено диалоговое окно с выбором устройства хранения данных с обновленного ПО (рисунок 10.40).

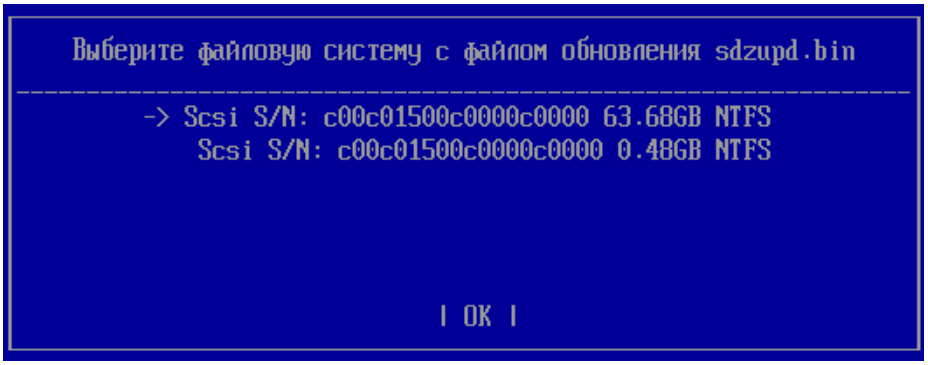


Рисунок 10.40 – Обновление системного ПО изделия

10.8.2 После выбора устройства хранения данных с обновлением ПО на экран ЭВМ будет выведено диалоговое окно с предложением очистки текущей БД изделия (рисунок 10.41). При подтверждении очистки вся информация из БД изделия удаляется. Отказ от очистки БД сохраняет всю информацию в неизменном виде.

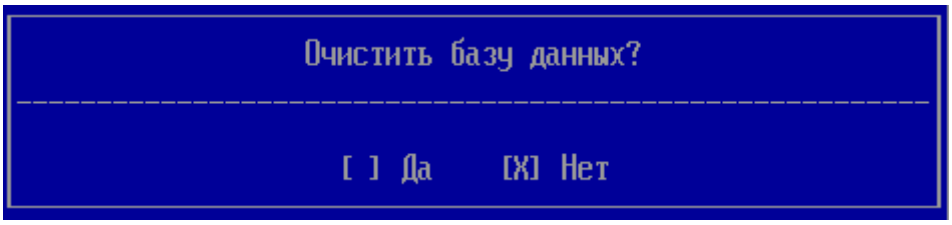


Рисунок 10.41 – Подтверждение очистки БД изделия

10.8.3 В случае успешной установки обновления ПО в диалоговом окне будет выведено сообщение об успешном обновлении (рисунок 10.42) и будет выполнена перезагрузка ЭВМ для вступления в силу установленных обновлений.

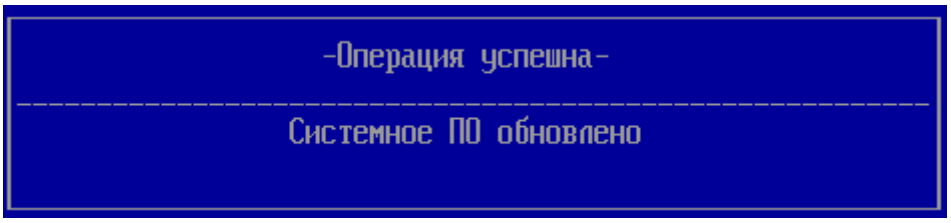


Рисунок 10.42 – Успешное обновление ПО изделия

10.9 Однократный вход в BIOS

10.9.1 Для разрешения однократного входа в BIOS АБ необходимо в окне ***«Основные настройки»*** перейти в строку ***«Разрешить однократный вход в BIOS»*** (Рисунок) и нажать клавишу < ***Enter*** >, при этом на экран ЭВМ будет выведено диалоговое окно с требованием перезагрузки ЭВМ (рисунок 10.43).

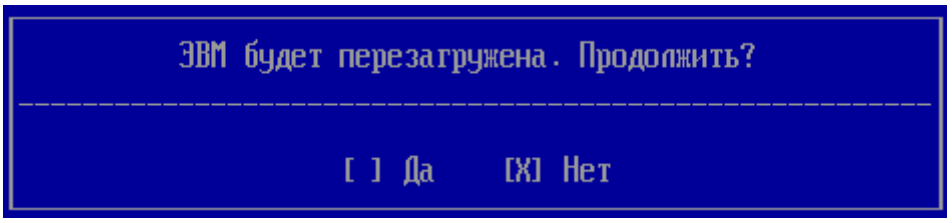


Рисунок 10.43 – Подтверждение перезагрузки ЭВМ для входа в BIOS

10.9.2 При подтверждении перезагрузки ЭВМ, АБ будет доступен однократный вход в BIOS с использованием стандартных клавиш входа сразу после перезагрузки.

10.10 Запрет перезаписи BIOS

10.10.1 Для запрета перезаписи UEFI BIOS ЭВМ АБ необходимо в окне ***«Основные настройки»*** перейти в строку ***«Запрет перезаписи BIOS»*** (рисунок 10.1) и нажать клавишу **< *Enter* >**, при этом на экран ЭВМ будет выведено диалоговое окно с сообщением об успешности установки запрета перезаписи UEFI BIOS ЭВМ (рисунок 10.44).

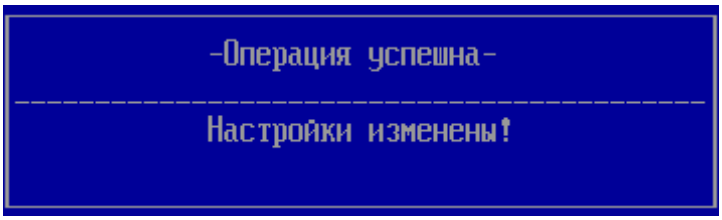


Рисунок 10.44 – Успешная установка запрета перезаписи BIOS

ВНИМАНИЕ!

Установка параметра «Защита перезаписи BIOS» не поддерживается на некоторых типах материнских плат ЭВМ и может привести к блокировке загрузки ЭВМ.

10.11 Мягкий режим

10.11.1 Мягкий режим СДЗ позволяет выполнять загрузку ОС без настроенных механизмов защиты. Отключение мягкого режима необходимо для запрета загрузки ОС пользователем сразу после включения ЭВМ и запуска процесса аутентификации пользователя.

10.11.2 Отключение и включение мягкого режима осуществляется по требованию АБ, после первого отключения мягкого режима осуществляется принудительная смена пароля восстановления (см. п. 5.5 руководства).

10.11.3 Для выхода из мягкого режима необходимо в окне ***«Основные настройки»*** перейти в строку «***Мягкий режим***» (рисунок 10.1), нажать клавишу **< *Enter* >** и в новом диалоговом окне подтвердить выключение режима (рисунок 10.45).

Рисунок 10.45 – Подтверждение выхода из мягкого режима

10.11.4 После успешного выхода их мягкого режима в диалоговом окне будет выведено сообщение об успешности операции и вступлении произведенных изменений в силу после перезагрузки ЭВМ (рисунок 10.46).

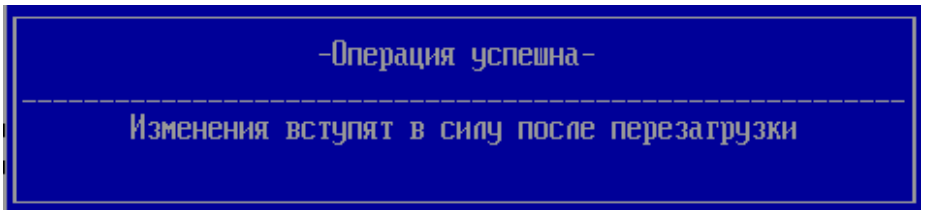


Рисунок 10.46 – Успешное завершение операции

10.11.5 Включение мягкого режима осуществляется аналогичным образом. Необходимо перейти в окно ***«Основные настройки»***, затем в строку ***«Мягкий режим»*** (рисунок 10.1), нажать клавишу **< *Enter* >** и в новом диалоговом окне будет выведено сообщение об успешности операции и вступлении произведенных изменений в силу после перезагрузки ЭВМ (рисунок 10.46).

10.12 Диагностика

10.12.1 Для диагностики работы изделия АБ в главном окне (рисунок 4.2) необходимо выбрать подраздел «***Диагностика»*** и нажать клавишу **< *Enter* >**, при этом на экран ЭВМ будет выведено новое диалоговое окно (рисунок 10.47).

Рисунок 10.47 – Диагностика изделия

10.12.2 В ПО изделия присутствует возможность диагностики с отслеживанием исполнения кода (пункт «***Контроль исполнения кода***») в определенном порядке в соответствии с установленными правилами с целью предотвратить несанкционированный доступ к ЭВМ.

10.12.3 По умолчанию параметр «***Контроль исполнения кода***» выключен. Для включения данного параметра АБ необходимо перейти в строку «***Контроль исполнения кода***» и в появившемся диалоговом окне выбрать требуемый вариант (рисунок 10.48).

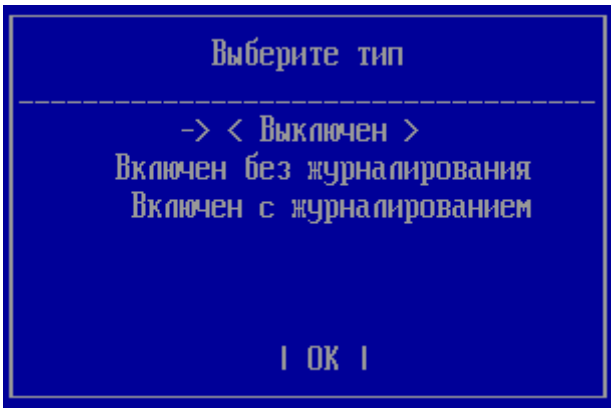


Рисунок 10.48 – Выбор типа контроля исполнения кода

В ПО изделия предусмотрены следующие варианты установки параметра ***«Контроль исполнения кода»***:

- ***«Выключен»*** (по умолчанию) – динамический контроль исполнения кода не осуществляется;
- ***«Включен без журналирования»*** – динамический контроль исполнения кода осуществляется в соответствии с заданными правилами, при этом результаты диагностики не записываются в журналы диагностики;
- ***«Включен с журналированием»*** – то же, результаты записываются в журналы диагностики.

10.12.4 После изменения значения параметра «***Контроль исполнения кода***» в диалоговом окне АБ будет выведено сообщение об успешности операции, при этом изменения вступят в силу после перезагрузки ЭВМ (рисунок 10.49).

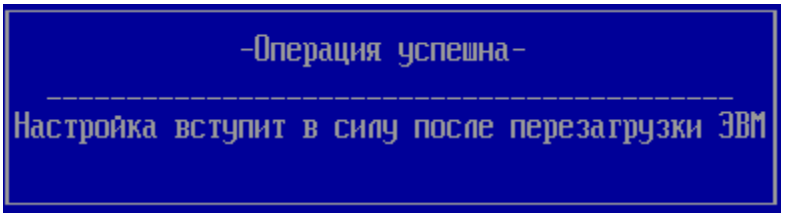


Рисунок 10.49 – Успешное изменение типа контроля исполнения кода

10.12.5 При выборе в параметре ***«Контроль исполнения кода»*** значения ***«Включен с журналированием»*** возможен экспорт журнала контроля исполнения кода. Для осуществления экспорта необходимо перейти в строку «***Экспортировать журналы контроля исполнения кода***» (рисунок 10.47) и в появившемся диалоговом окне выбрать устройство хранения данных (рисунок 10.50).

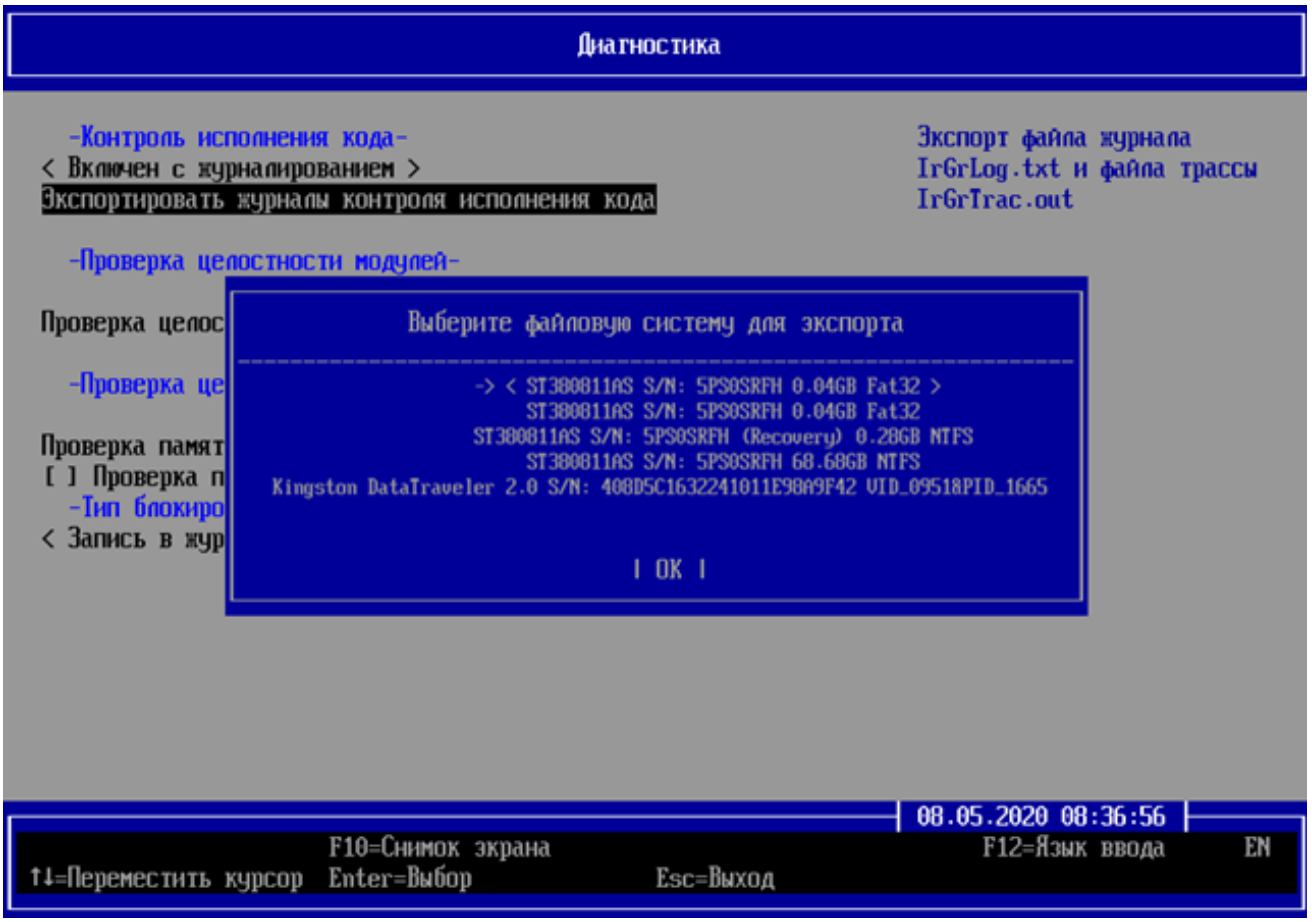


Рисунок 10.50 – Выбор файловой системы для экспорта

10.12.6 Диагностика изделия заключается в проверке целостностей модулей. Для запуска диагностики работы изделия необходимо перейти в строку ***«Проверка целостности»*** пункта ***«Проверка целостности модулей»*** (рисунок 10.47) и нажать клавишу **< *Enter* >**.

10.12.7 Показателем исправной работы изделия является успешная проверка целостности модулей, отображаемая в окне диагностики (рисунок 10.51).

Рисунок 10.51 – Успешная диагностика изделия

10.12.8 При выявлении ошибок диагностики изделия АБ необходимо обратиться в службу технической поддержки предприятия-изготовителя для устранения неполадок.

10.12.9 В изделии реализован механизм проверки оперативной памяти ЭВМ после старта изделия – для определения сбойных участков (рисунок 10.47). Проверка может быть запущена по требованию АБ или автоматически после старта изделия.

Алгоритм проверки основан на циклах последовательной записи и чтения страниц оперативной памяти ЭВМ.

Для проверки по требованию АБ необходимо нажать кнопку ***«Проверка памяти»***, при этом на экране ЭВМ появится индикатор проверки (рисунок 10.52).

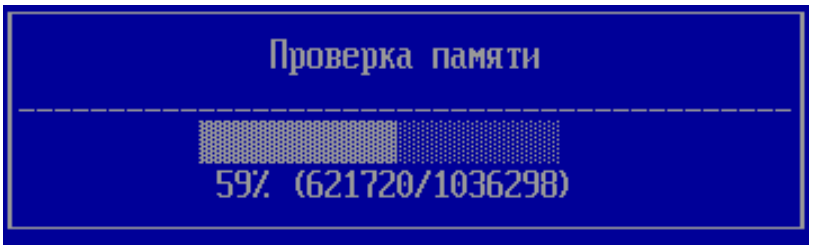


Рисунок 10.52 – Индикатор процесса проверки оперативной памяти ЭВМ

По завершении проверки на экран ЭВМ будет выведен результат проверки оперативной памяти (рисунок 10.53).

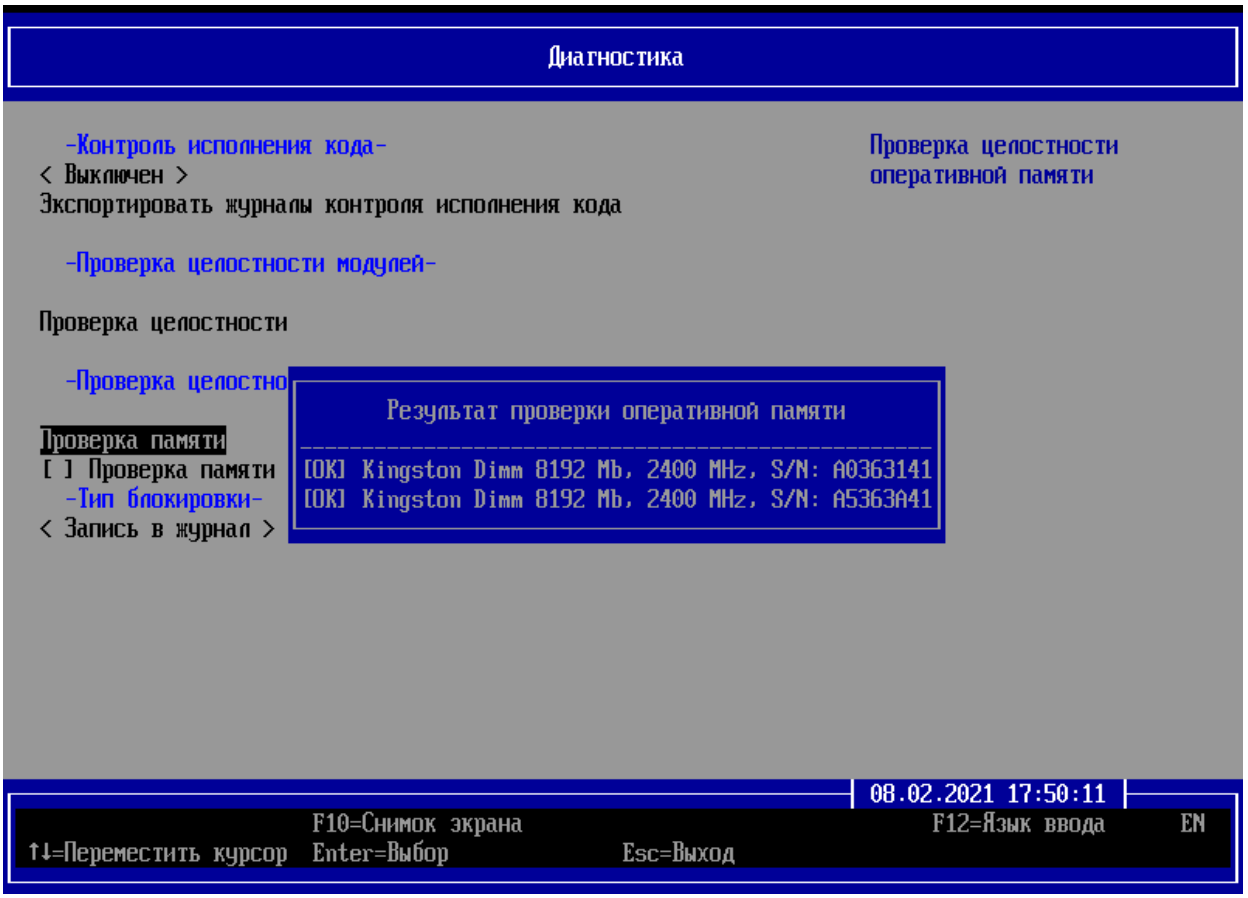


Рисунок 10.53 – Результаты проверки оперативной памяти ЭВМ

По результатам диагностики отображается информация по каждому слоту оперативной памяти, в случае успеха выводится ***[OK]***, при обнаружении ошибки ***[FAIL]*** (рисунок 10.53). Для закрытия окна необходимо нажать клавишу **< *Esc* >**. Если проверки по всем томам оперативной памяти пройдены успешно, появится соответствующая надпись (рисунок 10.54).

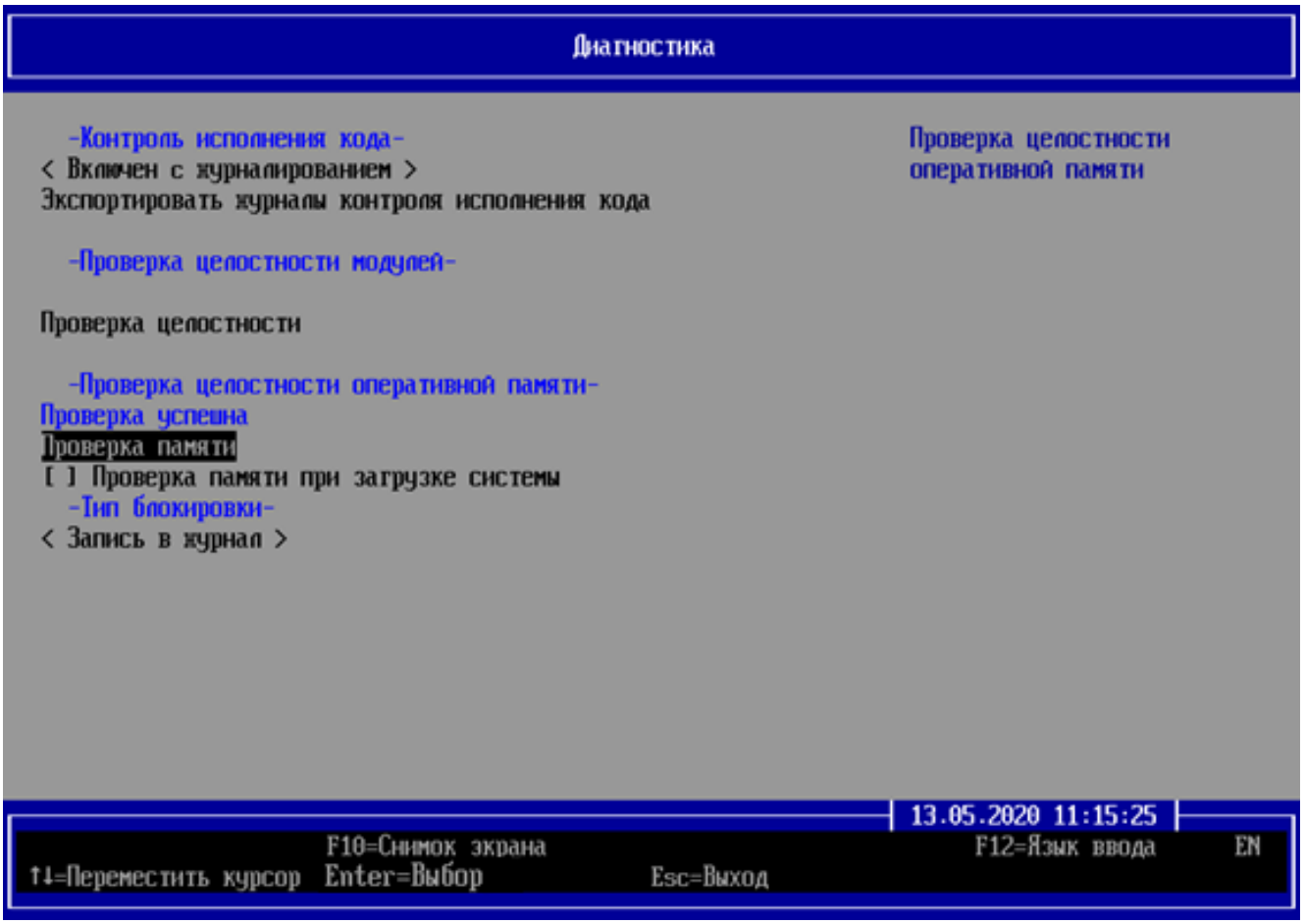


Рисунок 10.54 – Появление надписи об успешно пройденной проверке

Результаты проверки оперативной памяти сохраняются в журнале аудита изделия (рисунок 10.55).

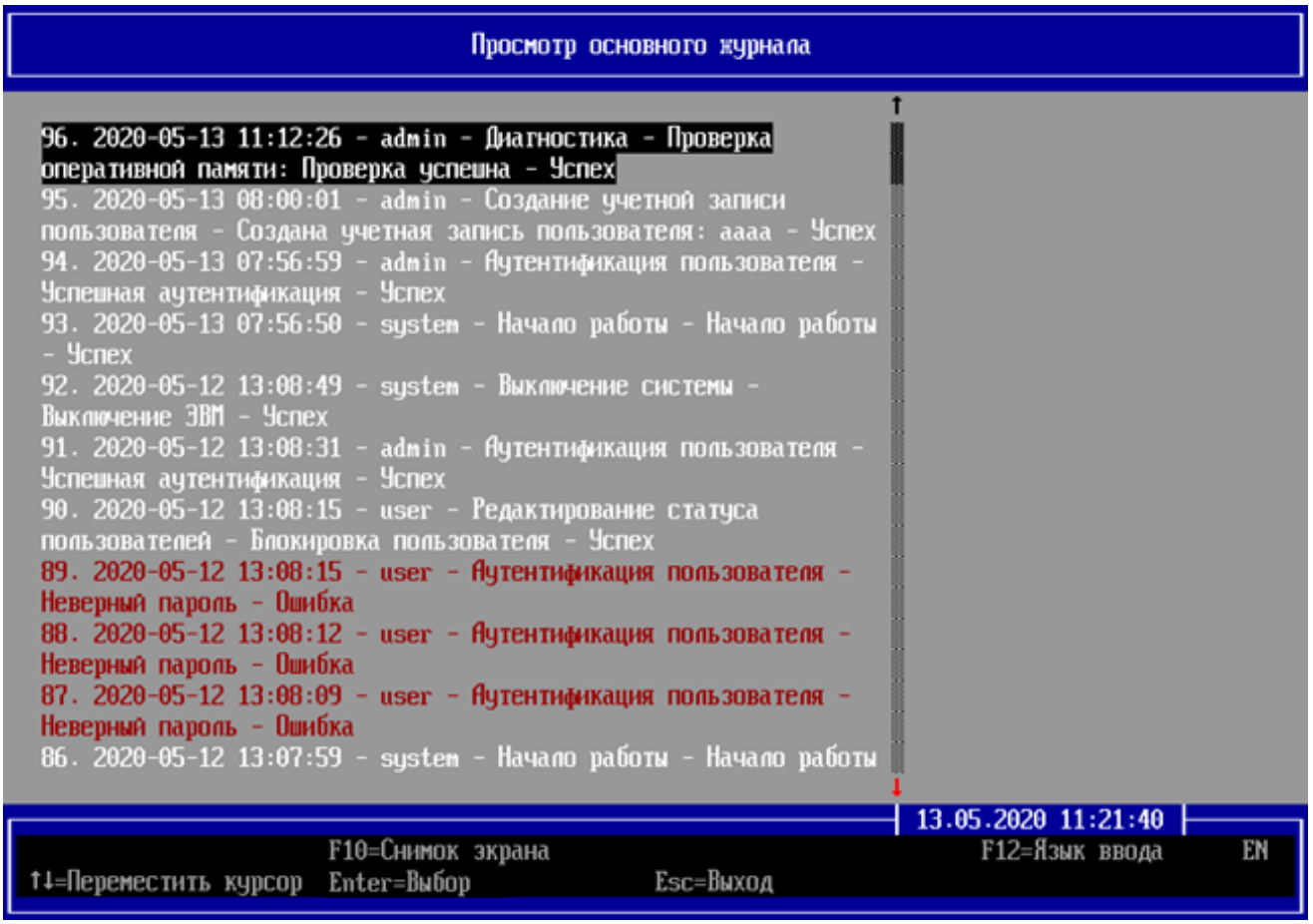


Рисунок 10.55 – Результаты проверки оперативной памяти ЭВМ

Для автоматической проверки оперативной памяти при старте системы необходимо перейти в поле ***«Проверка памяти при загрузке системы»*** и нажать клавишу ***< Enter >*** (рисунок 10.47). Кроме того, необходимо установить тип блокировки при обнаружении сбойных участков оперативной памяти ЭВМ (рисунок 10.56).

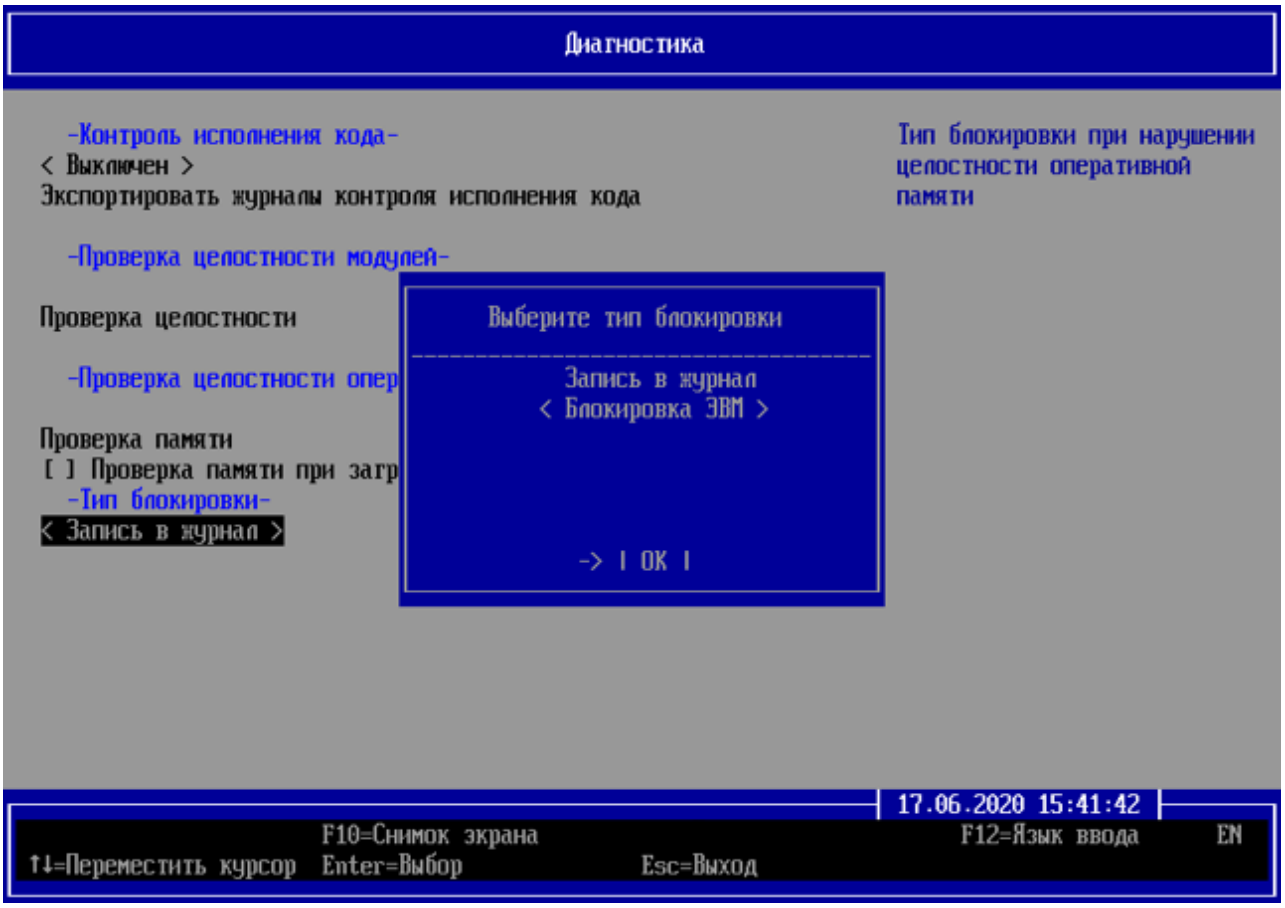


Рисунок 10.56 – Тип блокировки при обнаружении сбойных участков оперативной памяти

10.13 Информация о продукте

10.13.1 Подраздел ***«Информация о продукте»*** раздела ***«Основные настройки»*** содержит сведения о предприятии-изготовителе изделия и сведения о версии ПО (рисунок 10.57).

10.13.2 Пункт «***Контрольные суммы ПО***» содержит общую контрольную сумму всех модулей и сведения о контрольных суммах и версиях для каждого модуля ПО (рисунок 10.58).

10.13.3 Для экспорта информации о контрольных суммах и версиях модулей ПО необходимо перейти в строку «***Экспорт версии ПО в файл***» (рисунок 10.57) и нажать клавишу < ***Enter*** >, при этом на экран ЭВМ будет выведено новое диалоговое окно выбора устройства хранения данных (рисунок 10.59). После выбора устройства хранения данных АБ необходимо нажать кнопку | ***ОК*** | (рисунок 10.60).

10.13.4 Информация о версии ПО будет сохранена в корневой раздел выбранного устройства хранения данных в файл **sdzinfo.txt** (рисунок 10.60).

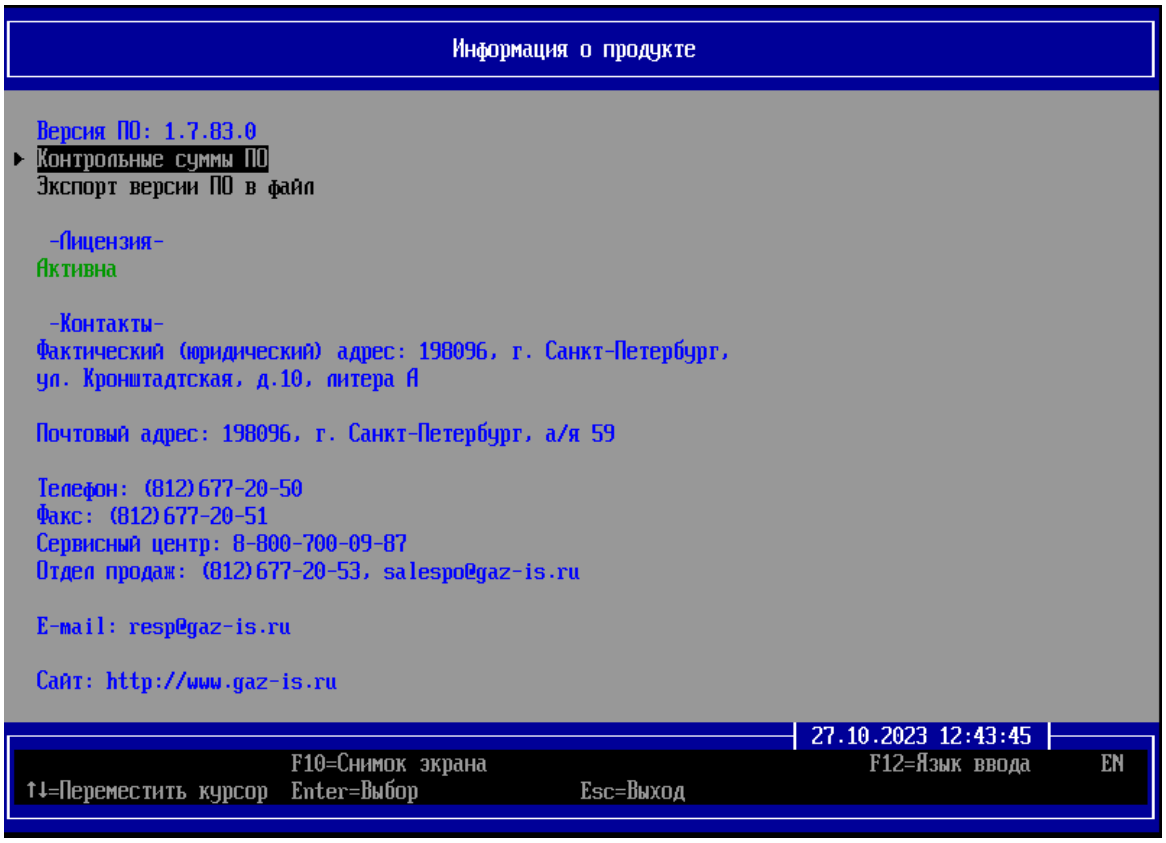


Рисунок 10.57 – Общая информация об изделии

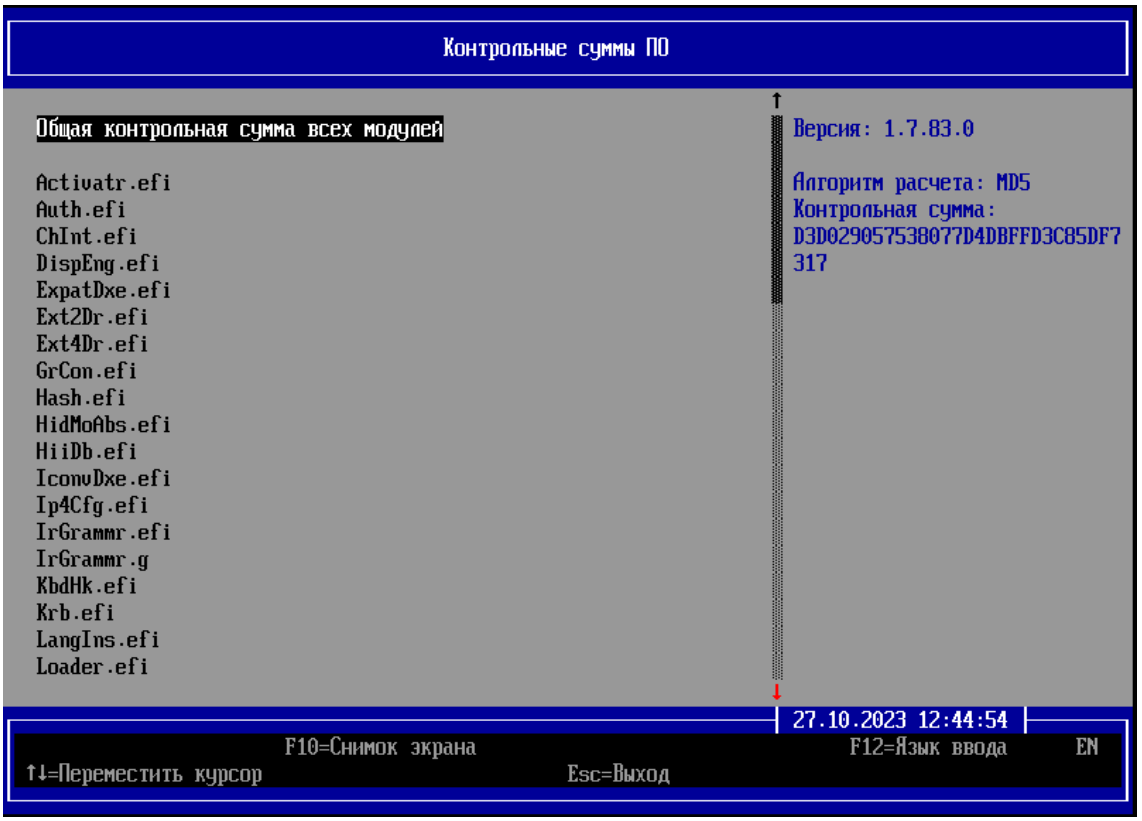


Рисунок 10.58 – Контрольные суммы ПО

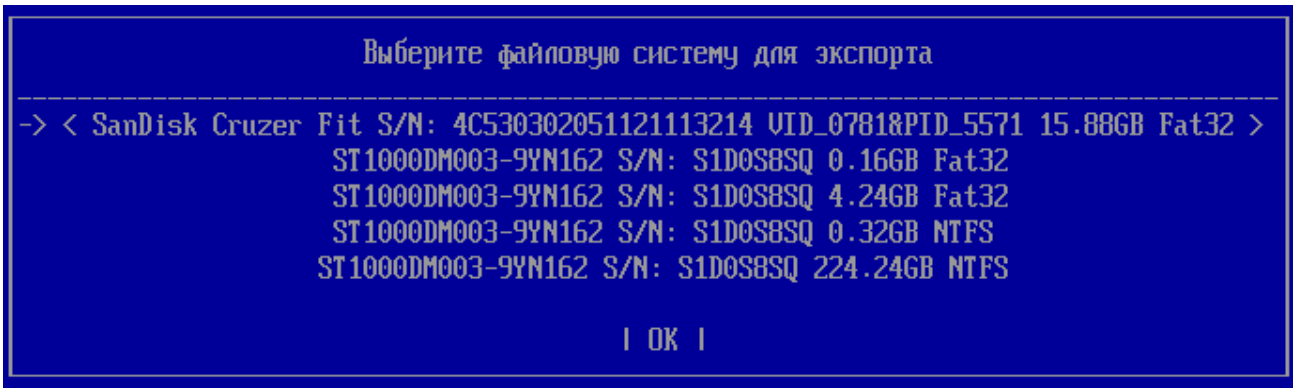


Рисунок 10.59 – Выбор устройства хранения данных для экспорта версии ПО в файл

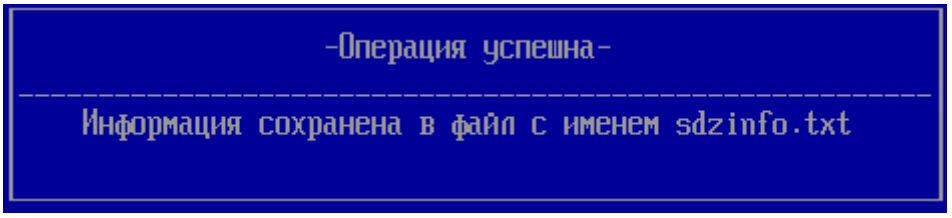


Рисунок 10.60 – Успешный экспорт версии ПО в файл

10.13.5 В случае существования на выбранном устройстве хранения данных файла с таким именем, АБ на экран ЭВМ будет выведено предупреждение (рисунок 10.61).

Рисунок 10.61 – Перезапись файла с версией ПО

11 Регистрация событий. Журнал аудита

Подраздел ***«Журнал аудита»*** предназначен для мониторинга АБ всех событий, происходящих до доверенной загрузки ОС. В журнале аудита регистрируются действия АБ и пользователей.

Для работы с журналом аудита АБ необходимо выбрать в главном окне консоли АБ (рисунок 4.2) подраздел «***Журнал аудита»*** и нажать клавишу **< *Enter* >** (рисунок 11.1).

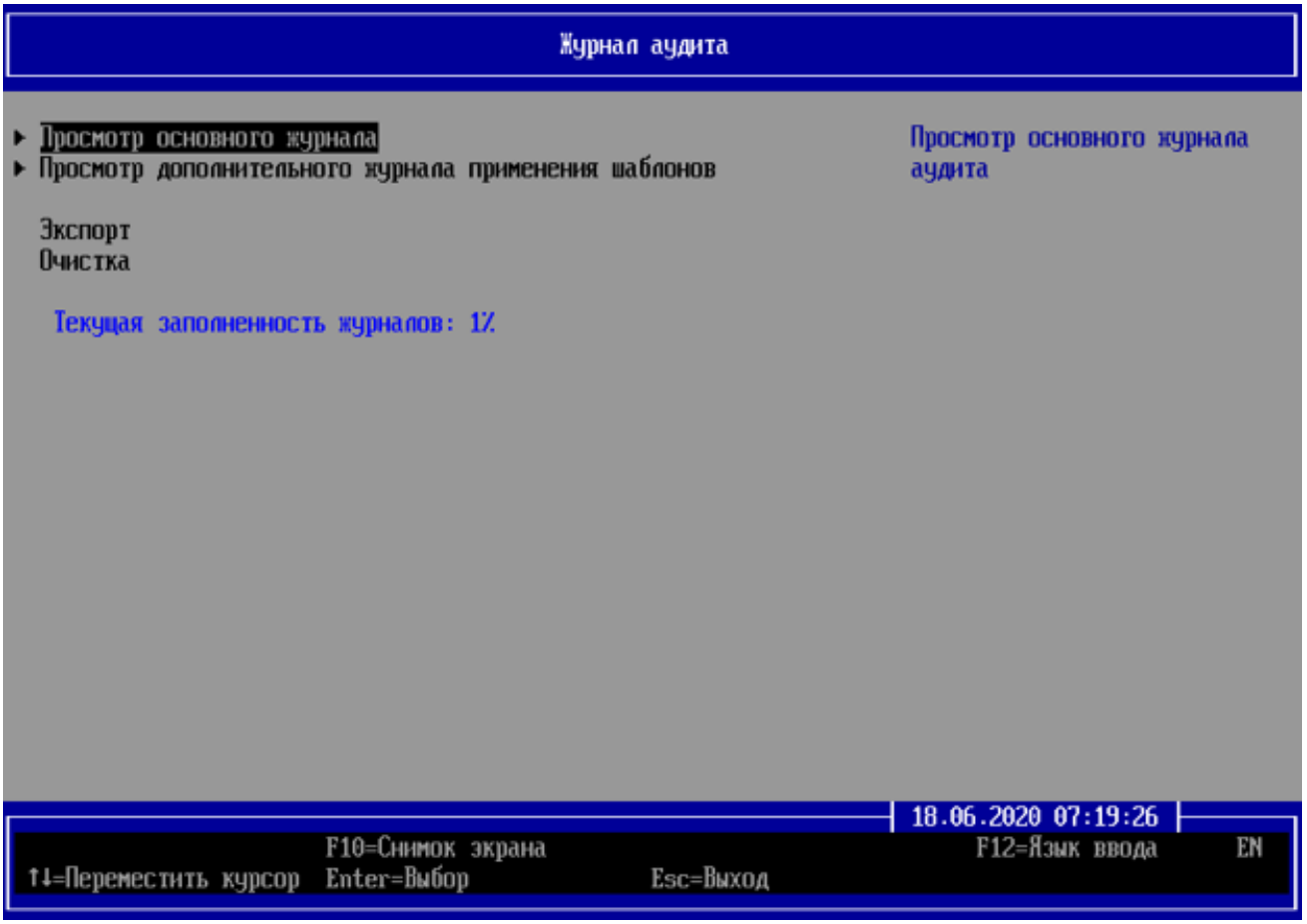


Рисунок 11.1 – Журнал аудита

АБ имеет возможность:

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

Возможность просмотра основного и дополнительного журналов аудита, экспорта журналов аудита на внешнее устройство хранения данных (без их удаления) доступна также пользователям с назначенной ролью аудитора.

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

11.1 Просмотр основного журнала аудита

11.1.1 В основном журнале аудита регистрируются все действия АБ (изменение общих настроек изделия, изменения настроек политик аутентификации и КЦ, действия с учетными записями пользователей) и действия пользователей.

Также в основной журнал аудита регистрируются сообщения при срабатывании механизмов КЦ объектов.

11.1.2 Для просмотра основного журнала аудита необходимо перейти в строку ***«Просмотр основного журнала»*** и нажать клавишу **< *Enter* >** (рисунок 11.1).

11.1.3 В появившемся диалоговом окне ***«Просмотр основного журнала»*** все события, регистрируемые в основном журнале аудита, разделены построчно (рисунок 11.2) в соответствии со значением параметра ***«Количество записей в журнале для отображения»***, установленного в подразделе ***«Основные настройки»*** (возможные значения параметра приведены в таблице 10.1).

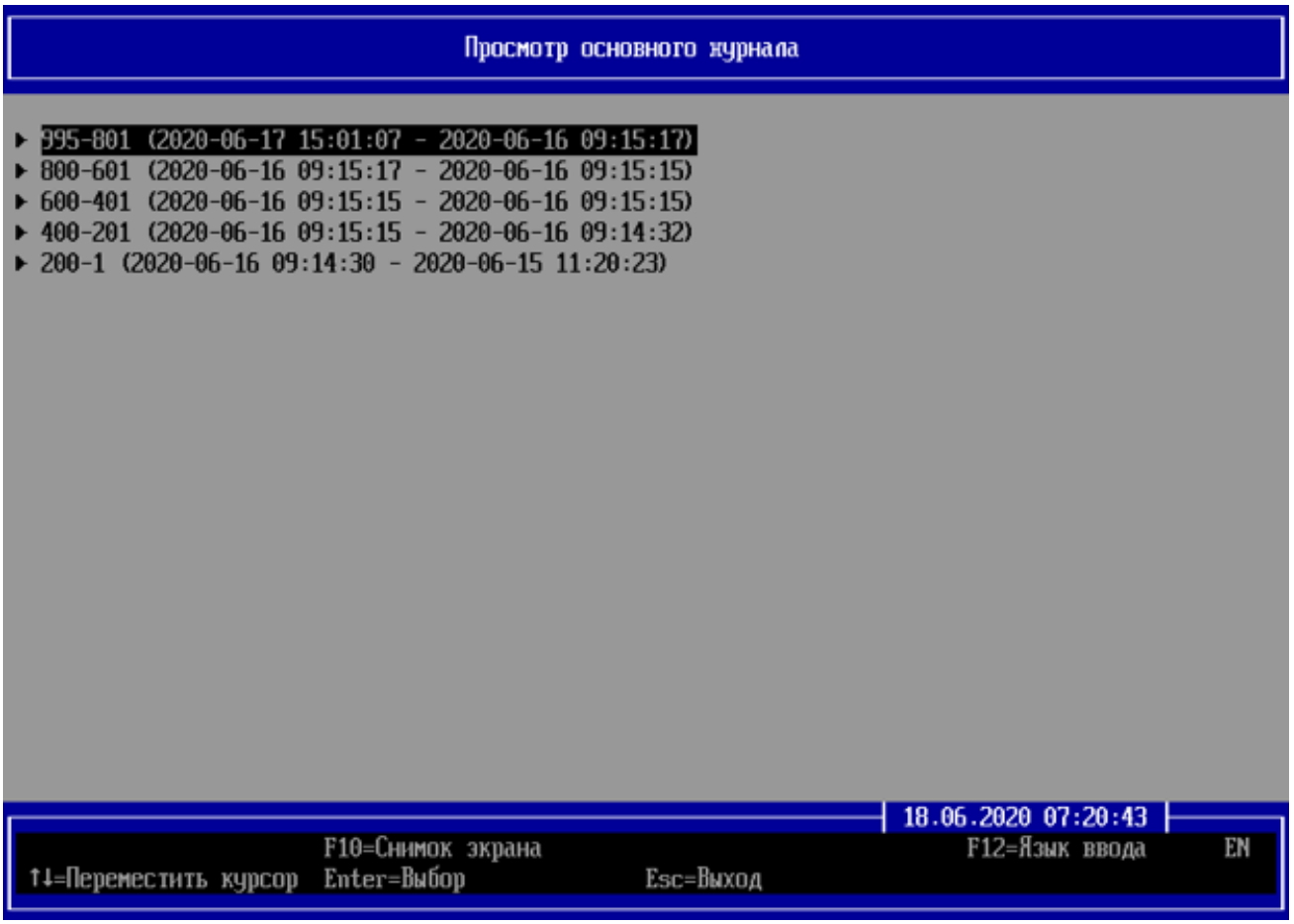


Рисунок 11.2 – Список периодов событий основного журнала аудита

11.1.4 Для просмотра АБ необходимо перейти в строку, соответствующую выбранному периоду времени, за которое требуется просмотреть события, регистрируемые в основном журнале и нажать клавишу **< *Enter* >** (рисунок 11.2).

11.1.5 Список событий, регистрируемых в основном журнале аудита (рисунок 11.3), приведен в таблице 11.1.

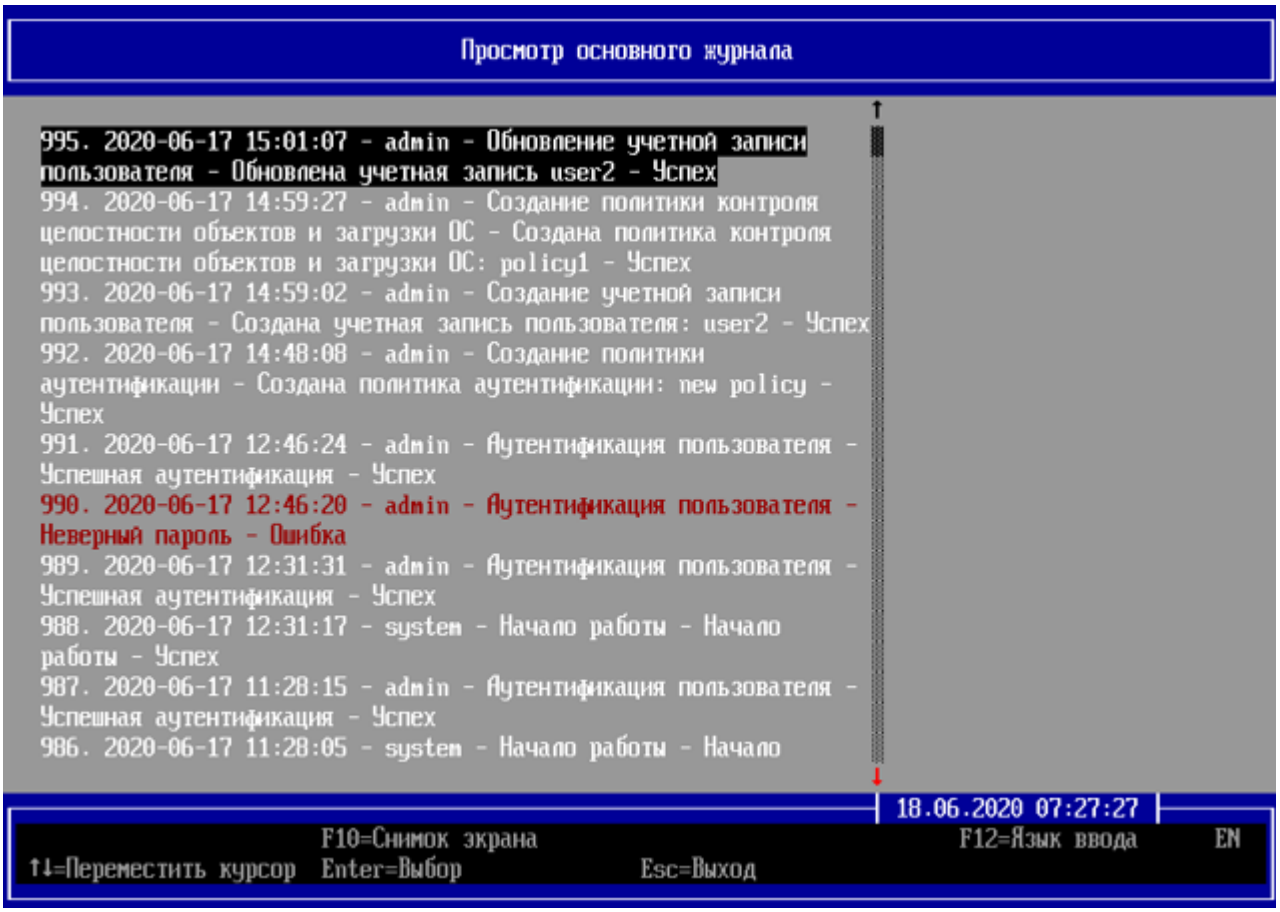


Рисунок 11.3 – Просмотр основного журнала аудита

11.1.6 Каждому событию присваивается порядковый номер и указывается:

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

11.1.7 Строки с сообщениями об ошибках выделены красным цветом (рисунок 11.3).

Таблица 11.1 – 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 умолчанию	Успех	Заводские настройки восстановлены
3	Изменение настроек системы	Успех	Настройки изменены
			Автовход разрешен для пользователя: <имя пользователя>
4	Выключение системы	Успех	Выключение ЭВМ

№	Событие	Успех /Ошибка	Комментарий
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>
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>

№	Событие	Успех /Ошибка	Комментарий
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 реестра	Ошибка	Проверка целостности объектов 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>

№	Событие	Успех /Ошибка	Комментарий
			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 файловых систем	Успех	Политика <имя политики> Добавление <имя объекта>
			Политика <имя политики> Удаление <имя объекта>
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

№	Событие	Успех /Ошибка	Комментарий
			Блокировка пользователя
			<имя пользователя> был заблокирован администратором
			<имя пользователя> был разблокирован администратором
			Блокировка пользователя по истечению времени неактивности

11.2 Просмотр дополнительного журнала применения шаблонов

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

11.2.2 Для просмотра дополнительного журнала применения шаблонов необходимо перейти в строку ***«Просмотр дополнительного журнала применения шаблонов»*** и нажать клавишу **< *Enter* >** (рисунок 11.1).

11.2.3 В появившемся диалоговом окне ***«Просмотр дополнительного журнала применения шаблонов»*** все события, регистрируемые в основном журнале, разделены построчно в соответствии со значением параметра ***«Количество записей в журнале для отображения»***, установленного в подразделе ***«Основные настройки»***.

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

11.2.5 В появившемся диалоговом окне ***«Просмотр дополнительного журнала применения шаблонов»*** АБ предоставляется возможность просмотра всех действий, по применению шаблонов к политикам (рисунок 11.4).

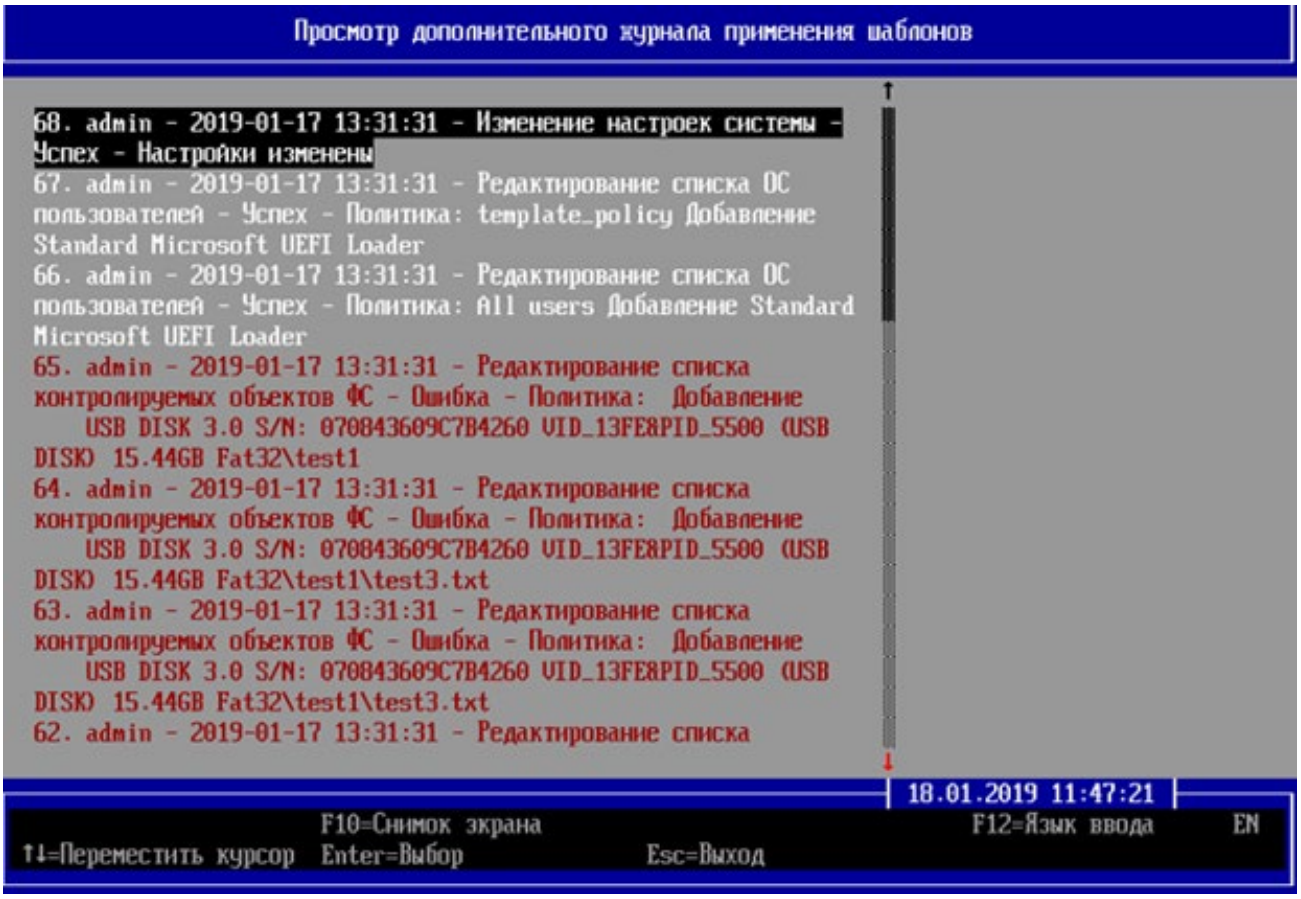


Рисунок 11.4– Просмотр дополнительного журнала применения шаблонов

11.2.6 Каждому событию присваивается порядковый номер и указывается:

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

11.2.7 Строки с сообщениями об ошибках выделены красным цветом (рисунок 11.4).

Таблица 11.2 – 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			

№	Событие	Успех/Ошибка	Комментарий
3	Редактирование списка контролируемых объектов реестра	Успех Ошибка	Политика <имя политики> Добавление <имя объекта>
Контроль устройств			
4	Редактирование списка контролируемых устройств	Успех Ошибка	Политика <имя политики> Добавление <имя объекта>
Управление загрузкой ОС			
5	Редактирование списка ОС пользователя	Успех Ошибка	Политика <имя политики> Добавление <наименование ОС>
Управление дисками			
6	Редактирование списка контролируемых загрузочных областей	Успех Ошибка	Политика <имя политики> Добавление <имя объекта>
Контроль целостности среды UEFI			
7	Редактирование списка целостности среды UEFI	Успех Ошибка	Политика <имя политики> Добавление <имя объекта>
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>

11.3 Оповещение об ошибках в журнале аудита

11.3.1 Фиксация в журнале аудита ошибочных действий пользователя при работе с изделием сопровождается оповещением АБ о выявлении ошибок в журнале.

11.3.2 После аутентификации и (или) идентификации АБ на экран ЭВМ выводится сообщение об обнаружении ошибок в журнале аудита (рисунок 11.5).

Рисунок 11.5 – Оповещение об ошибках в журнале аудита

11.3.3 При выборе пункта ***«Нет»*** и нажатии клавиши **< *Enter* >** будет осуществлен переход к основному окну консоли АБ. При этом не просмотренные события, зафиксированные в журнале аудита, будут храниться в БД как события, на которые АБ не отреагировал, и сообщение об обнаружении ошибок в журнале аудита (рисунок 11.5) будет выводиться АБ при каждой аутентификации и (или) идентификации.

11.3.4 При выборе пункта ***«Да»*** и нажатии клавиши **< *Enter* >** будет осуществлен переход к окну просмотра ошибок журнала аудита, содержащему список ошибок, выявленных при работе пользователя с изделием (рисунок 11.6). При этом события, зафиксированные в журнале аудита, будут помечены как события, на которые АБ отреагировал, и сообщение об обнаружении ошибок в журнале аудита (рисунок 11.5) выводиться не будет.

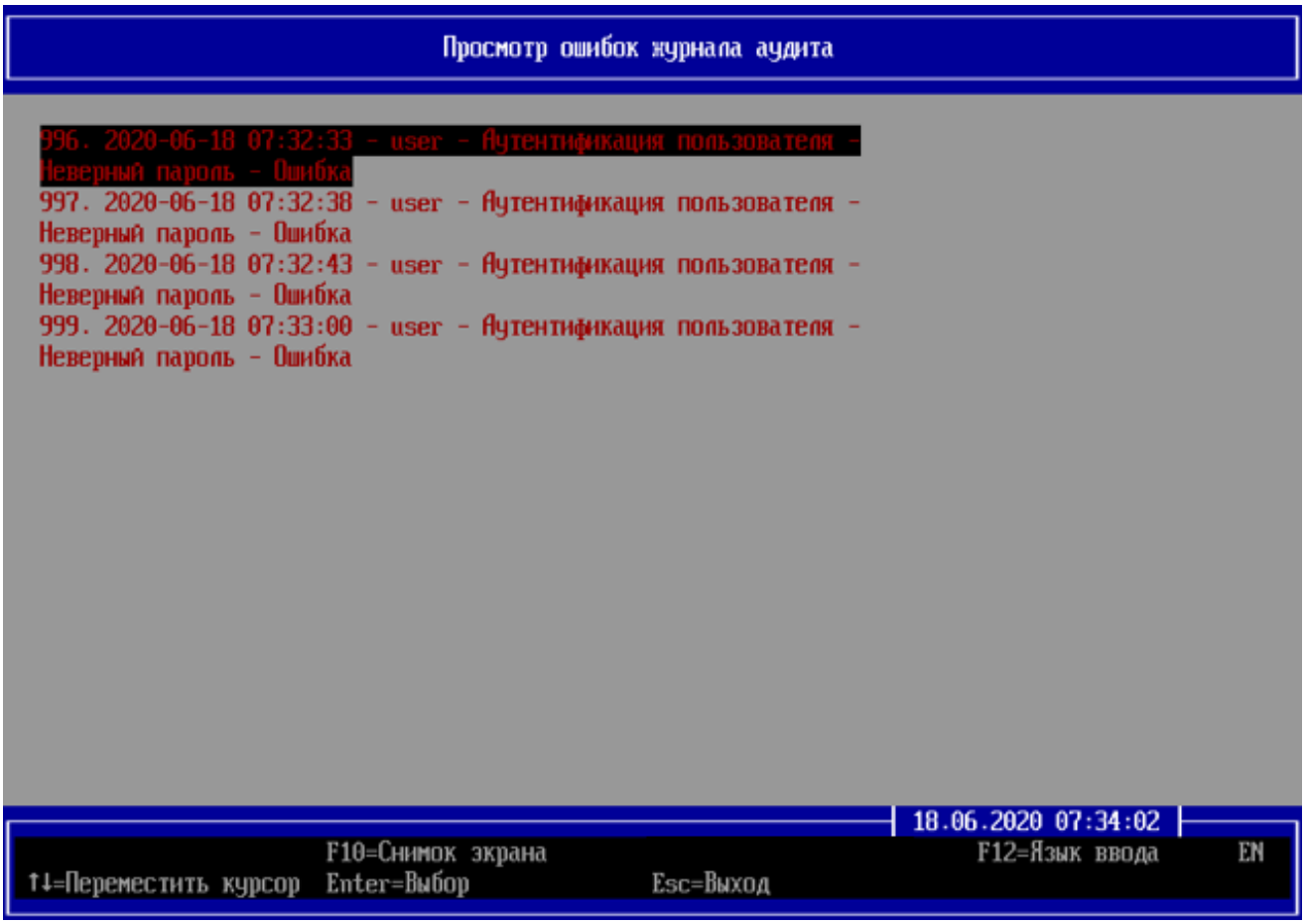


Рисунок 11.6 – Просмотр дополнительного журнала применения шаблонов

11.3.5 Для дальнейшей работы и возврата в основное окно консоли АБ необходимо нажать клавишу **< *Esc* >**.

11.4 Экспорт журналов аудита

11.4.1 АБ 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 11.1) и нажать клавишу ***< Enter >***;
- в новом диалоговом окне выбрать устройство хранения данных и нажать кнопку | ***OK*** | (рисунок 11.7);
- при успешном экспорте журналов на экран ЭВМ будет выведено сообщение (рисунок 11.8).

11.4.2 Журналы аудита будут сохранены в корневой раздел выбранного устройства хранения данных в файлы **sdzlog.csv** и **sdzlogT.csv** (рисунок 11.8).

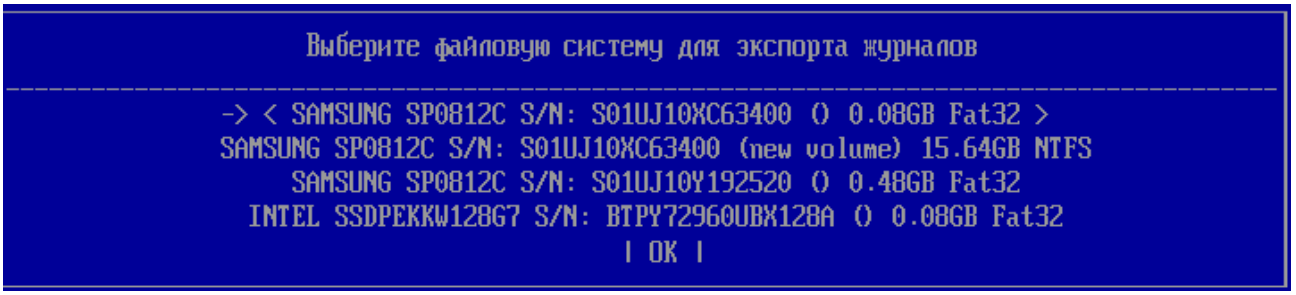


Рисунок 11.7 – Выбор устройства хранения данных для экспорта журналов аудита

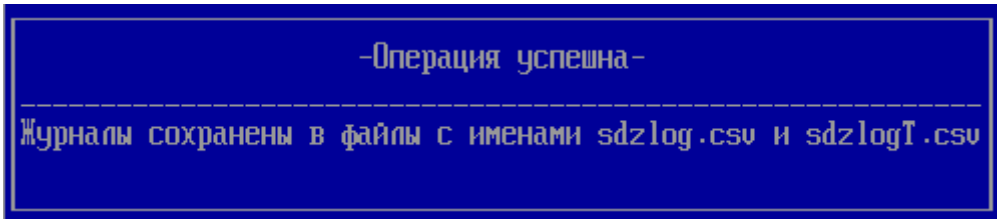
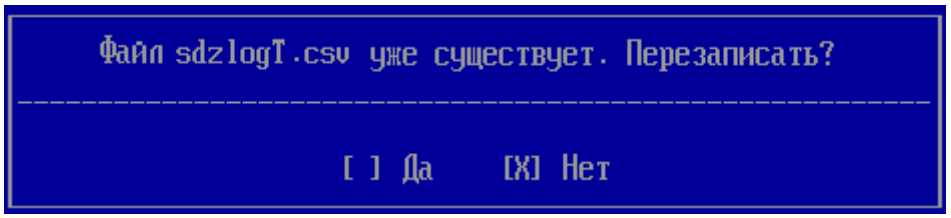


Рисунок 11.8 – Успешный экспорт журналов аудита

11.4.3 В случае существования на выбранном устройстве хранения данных файла с таким именем АБ на экран ЭВМ будет выведено предупреждение (рисунок 11.9 а, б).

а)



б)

Рисунок 11.9 – Перезапись файлов журналов аудита

Рекомендуется периодически осуществлять экспорт журналов на внешнее устройство хранения данных.

11.5 Очистка журналов аудита

11.5.1 АБ имеет возможность удалить записи журналов аудита без их экспорта.

11.5.2 Для очистки журналов АБ необходимо перейти в строку ***«Очистка»*** (рисунок 11.1), нажать клавишу ***< Enter >*** и в новом диалоговом окне подтвердить очистку журналов (рисунок 11.10).

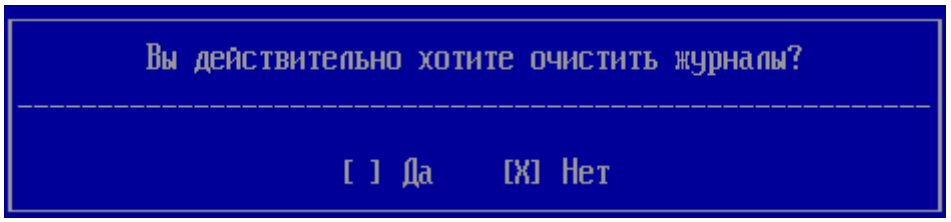


Рисунок 11.10 – Очистка журналов аудита

11.5.3 После завершения выполнения операции АБ будет выведено сообщение ***«Журналы аудита очищены»*** (рисунок 11.11) и в системном журнале добавится запись о произведенной операции.

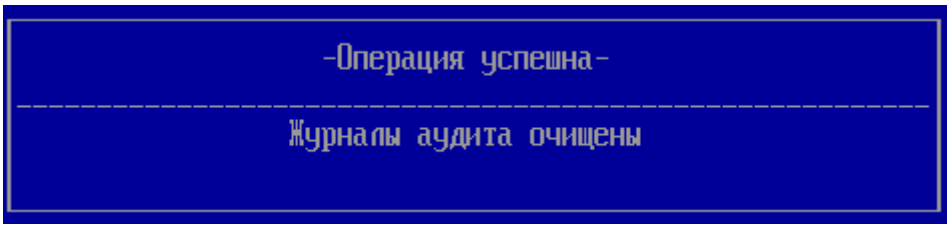


Рисунок 11.11 – Успешная очистка журналов

12 Описание старта изделия

12.1 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 12.1).

Рисунок 12.1 – Приглашение к идентификации и аутентификации пользователей

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

12.3 По умолчанию всем пользователям установлены общие количественные (8 попыток) и временные ограничения (15 минут) на идентификацию и аутентификацию (рисунок 12.1). При истечении общего времени аутентификации или количества попыток экран ЭВМ будет автоматически заблокирован и пользователям будет доступна только перезагрузка или выключение ЭВМ (рисунки 12.2 и 12.3 соответственно).

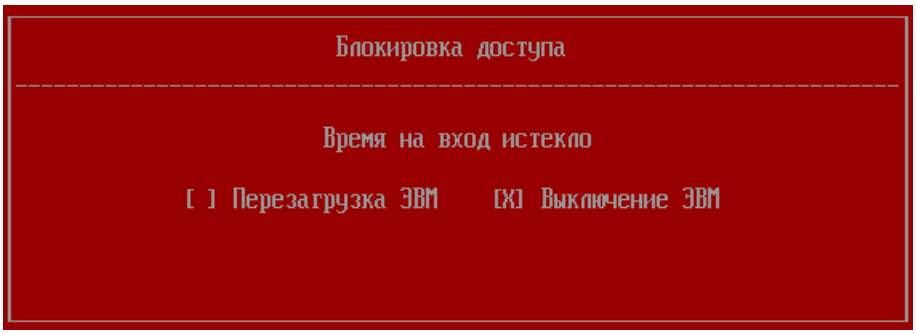


Рисунок 12.2 – Блокировка доступа при истечении времени на аутентификацию пользователей

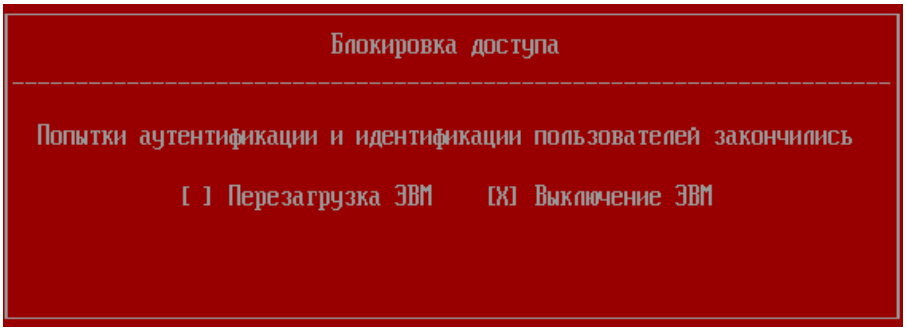


Рисунок 12.3 – Блокировка доступа при исчерпании количества попыток аутентификации пользователей

12.4 **Процедура проверки правильности старта ПО СДЗ** заключается в возможности идентификации и аутентификации АБ для настройки параметров изделия или пользователей для доверенной загрузки ОС и описана в разделе 2.

13 Завершение работы

13.1 Для выхода из консоли АБ необходимо в главном окне (рисунок 4.1) нажать клавишу **< *Esc* >**, при этом на экране ЭВМ появится диалоговое окно, в котором необходимо подтвердить или отказаться от выхода из консоли АБ (рисунок 13.1).

Рисунок 13.1 – Подтверждение или отказ от выхода из консоли АБ

13.2 По умолчанию курсор установлен на пункте ***«Нет»***, при нажатии клавиши **< *Enter* >** будет осуществлен возврат в консоль АБ.

13.3 Для выхода из консоли АБ необходимо установить курсор на пункт ***«Да»*** и нажать клавишу **< *Enter* >**.

13.4 При этом будет осуществлен переход к окну аутентификации и идентификации пользователей (рисунок 12.1).

13.5 При повторном нажатии клавиши **< *Esc* >** на экране ЭВМ появится окно ***«Меню действий пользователя»*** с выбором дальнейшего действия АБ (рисунок 13.2).

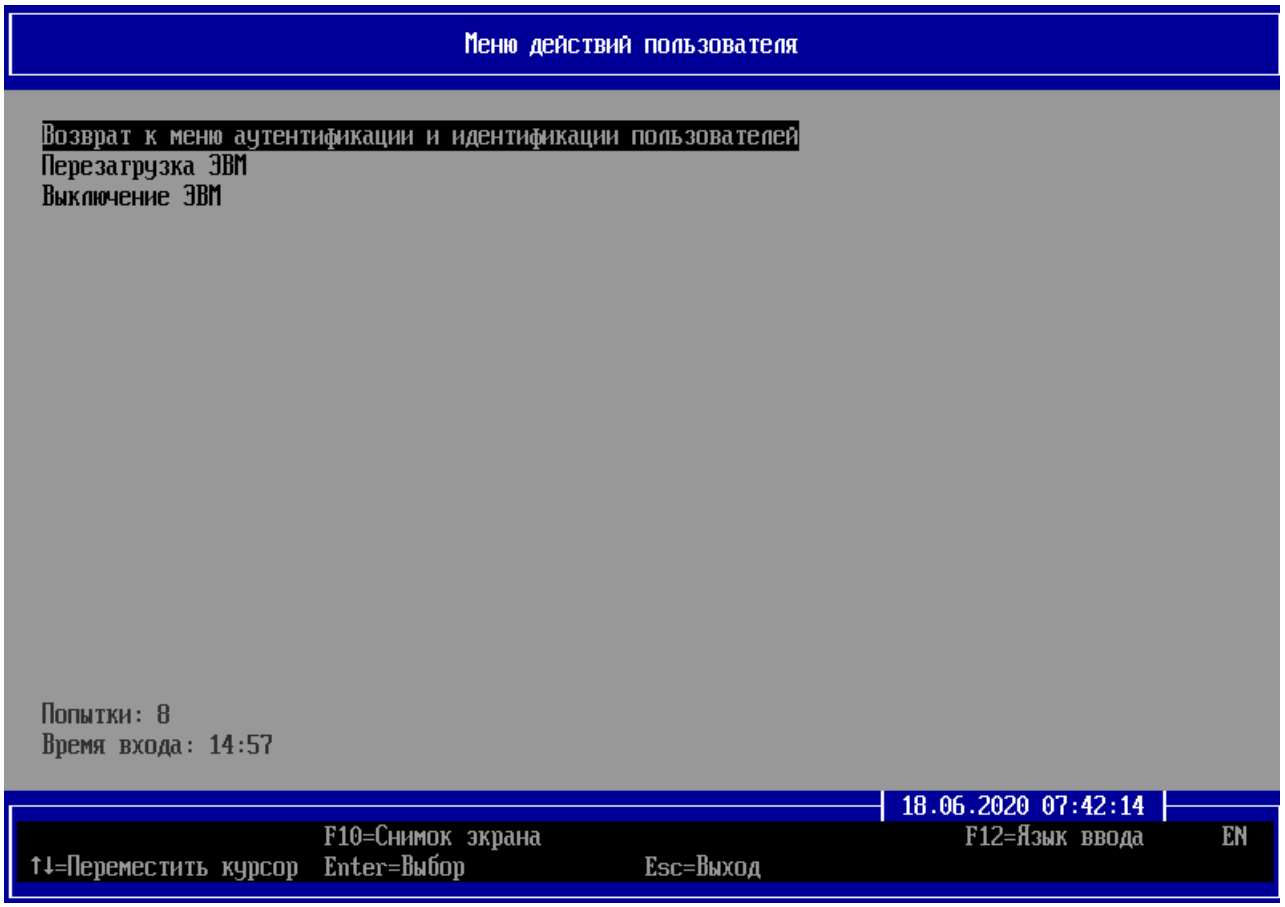


Рисунок 13.2 – Меню действий пользователя

13.6 По умолчанию выбор установлен на пункте ***«Возврат к меню аутентификации и идентификации пользователей»***.

13.7 При нажатии клавиши **< *Enter* >** будет выполнен переход к предыдущему окну (рисунок 12.1).

13.8 Для перезагрузки ЭВМ необходимо выбрать пункт ***«Перезагрузка ЭВМ»*** (рисунок 13.2).

13.9 Для выключения ЭВМ необходимо выбрать пункт ***«Выключение ЭВМ»*** (рисунок 13.2).

14 Централизованное управление СДЗ «SafeNode System Loader»

14.1 Управление СДЗ «SafeNode System Loader» сторонними приложениями с помощью командной строки

14.1.1 Управление СДЗ «SafeNode System Loader» сторонними приложениями предполагает возможность изменения настроек рабочих станций под управлением ОС семейств Windows, Linux с установленным СДЗ «SafeNode System Loader» через интерфейс командной строки на уровне операционных систем.

14.1.2 Опции и команды СДЗ «SafeNode System Loader», доступные для управления сторонними приложениями из командной строки, приведены в разделе 12 «Интерфейс командной строки изделия» документа «СДЗ «SafeNode System Loader». Руководство по эксплуатации. Часть 3. Руководство администратора Linux/Windows».

14.2 Управление СДЗ «SafeNode System Loader» сторонними приложениями посредством протокола REST API

14.2.1 Управление СДЗ «SafeNode System Loader» сторонними приложениями предполагает возможность изменения настроек рабочих станций под управлением ОС семейств Windows, Linux с установленным СДЗ «SafeNode System Loader» посредством протокола REST API.

14.2.2 Подробнее управление изделием посредством REST API приведено в документе «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 6. Описание REST API. ГМТК.468269.060РЭ6».

14.3 Управление СДЗ «SafeNode System Loader» с помощью политик СЗИ от НСД «Блокхост-Сеть 4»

14.3.1 Управление СДЗ «SafeNode System Loader» с помощью СЗИ от НСД «Блокхост-Сеть 4» предполагает возможность дистанционного изменения настроек клиентских рабочих станций под управлением ОС семейств Windows, Linux с установленным СДЗ «SafeNode System Loader» в консоли управления СЗИ от НСД «Блокхост-Сеть 4» при помощи политик.

14.3.2 Возможность взятия под управление клиентской рабочей станции с установленным СДЗ «SafeNode System Loader» с помощью СЗИ от НСД «Блокхост-Сеть 4» доступна только на уровне операционных систем. Клиентская рабочая станция должна функционировать под управлением ОС семейств Windows, Linux.

14.3.3 Если клиентская рабочая станция взята под управление СЗИ от НСД «Блокхост-Сеть 4», получение параметров механизмов защиты СДЗ из СЗИ от НСД «Блокхост-Сеть» доступно и на уровне операционных систем, и на уровне EFI. При этом во время запуска изделия выполняется подключение к серверу, и настройки, установленные в политиках СЗИ от НСД «Блокхост-Сеть 4», передаются клиентской рабочей станции.

14.3.4 Подробная информация об управлении СДЗ «SafeNode System Loader» с помощью политик СЗИ от НСД «Блокхост-Сеть 4» приведена в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора. Часть 1. Управлением политиками».

14.3.5 Для возможности управления настройками СДЗ с помощью политик СЗИ от НСД «Блокхост-Сеть 4» необходимо взять под управление клиентскую рабочую станцию с установленным СДЗ «SafeNode System Loader».

14.3.6 Создание задачи на взятие под управление модуля доверенной загрузки «SafeNode System Loader» доступно администратору в консоли управления в подсистеме развертывания СЗИ от НСД «Блокхост-Сеть 4». Подробная информация приведена в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора. Часть 2. Развертывание и аудит».

14.3.7 В процессе создания задачи на взятие под управление модуля доверенной загрузки «SafeNode System Loader» администратор формирует список клиентских рабочих станций, на которых планируется взять под управление СДЗ «SafeNode System Loader», добавляет пароли локальных администраторов для подтверждения прав на управление СДЗ «SafeNode System Loader» и устанавливает режим для времени запуска задачи.

Необходимо учитывать, что взять под управление возможно только рабочие станции с установленным СДЗ «SafeNode System Loader» версии 1.4 и выше.

14.3.8 На рабочих станциях с установленным СДЗ «SafeNode System Loader», взятых под управление СЗИ от НСД «Блокхост-Сеть 4», параметры и настройки политик СДЗ будут недоступны для редактирования на локальной машине локальному администратору.

14.3.9 В локальной консоли администрирования (BIOS) СДЗ «SafeNode System Loader» будет отображена информация о том, что он взят под управление (рисунок 14.1).

Рисунок 14.1 – Консоль взята под управление СЗИ от НСД «Блокхост-Сеть 4»

14.3.10 Вывод СДЗ «SafeNode System Loader» из-под управления СЗИ от НСД «Блокхост-Сеть 4» доступен администратору после аутентификации на локальной машине в локальной консоли администрирования (BIOS) СДЗ «SafeNode System Loader» (рисунок 14.2).

14.3.11 После вывода из-под управления СЗИ от НСД «Блокхост-Сеть 4», СДЗ «SafeNode System Loader» отправляет информацию о разрыве подчинения в СЗИ от НСД «Блокхост-Сеть 4» и управление настройками СДЗ посредством политик становится невозможным. Управление настройками СДЗ «SafeNode System Loader» передается локальному администратору на локальной машине.

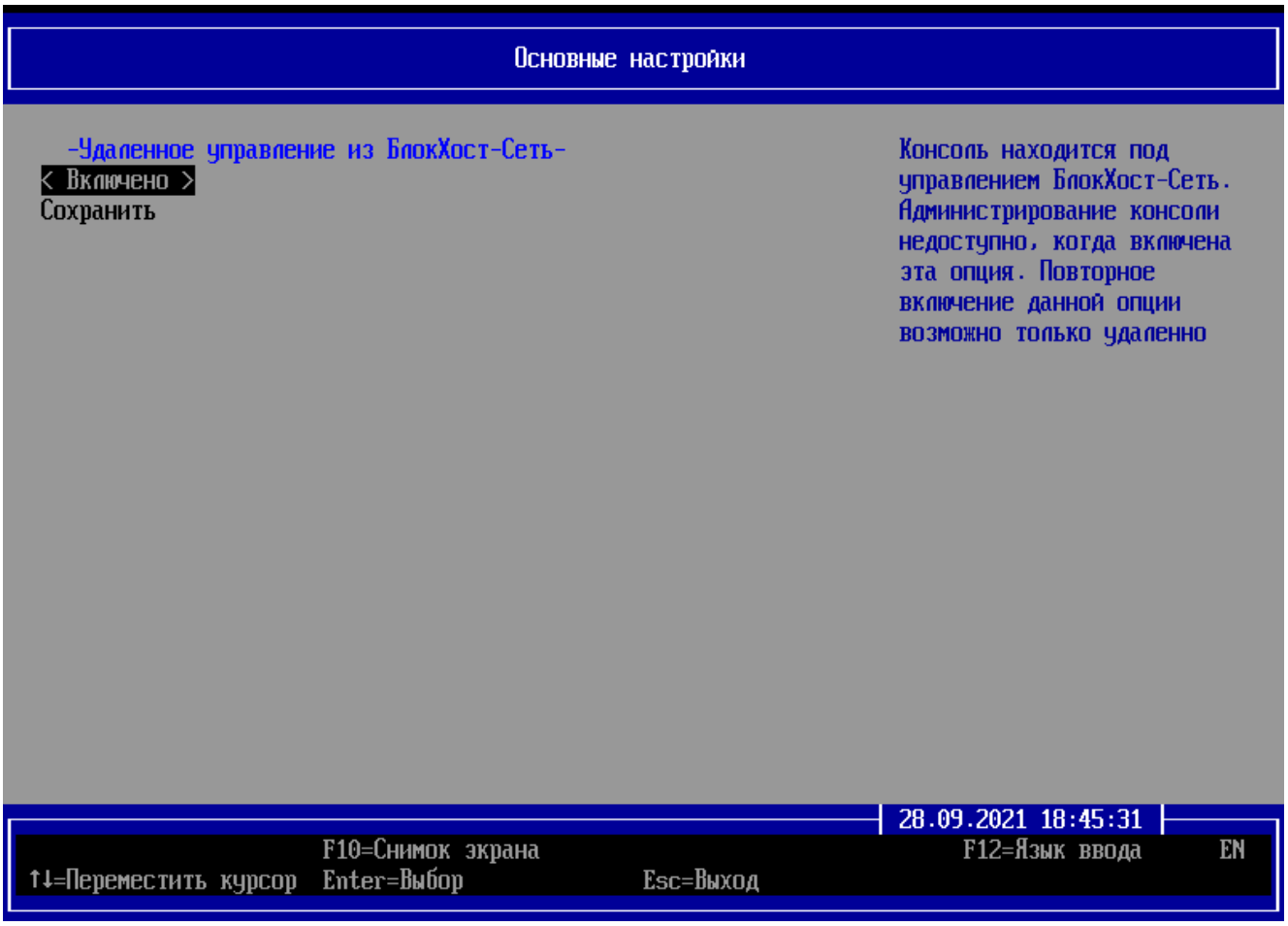


Рисунок 14.2 – Вывод консоли из-под управления СЗИ от НСД «Блокхост-Сеть 4»

14.3.12 Управление СДЗ «SafeNode System Loader» с помощью СЗИ от НСД «Блокхост-Сеть 4» осуществляется в консоли управления СЗИ от НСД «Блокхост-Сеть 4» при помощи политики, передающейся от сервера безопасности клиентам.

14.3.13 Политика, в которой задаются настройки СДЗ «SafeNode System Loader», позволяет управлять следующими механизмами:

- **механизм управления входом** – выбор дополнительного средства аутентификации пользователей до загрузки ОС при входе на клиентские рабочие станции с помощью СДЗ «SafeNode System Loader». При установке данного механизма при входе пользователя на клиентские рабочие станции аутентификация будет осуществляться в два этапа:
  - на этапе до загрузки ОС средствами СДЗ «SafeNode System Loader»;
  - на этапе после загрузки ОС средствами СЗИ от НСД «Блокхост-Сеть 4»;
- **механизм управления аутентификацией** – управление параметрами аутентификации пользователей до загрузки ОС при входе на клиентские рабочие станции если в механизме управления входом установлено дополнительное средство аутентификации СДЗ «SafeNode System Loader»;

- **механизм управления сложностью паролей** – управление ограничениями при задании пароля пользователя и администратора для входа на клиентские рабочие станции под управлением СДЗ «SafeNode System Loader», блокировка при неудачных попытках авторизации в ОС и установка запрета на использование заданного количества последних паролей;
- **контроль целостности** – управление параметрами КЦ аппаратной и программной конфигурации рабочей станции. При настройке механизма КЦ администратору доступно управление параметрами контроля целостности следующих компонентов контролируемой рабочей станции:
  - контроль целостности файловой системы (КЦ файлов и (или) каталогов загружаемой ОС, а также файлов и (или) каталогов пользователя);
  - контроль реестра (КЦ объектов реестра ОС семейства Windows);
  - контроль целостности загрузочных секторов (КЦ загрузочных секторов устройств хранения данных);
  - контроль параметров UEFI (КЦ переменных, драйверов и таблиц среды UEFI);
  - контроль изменения аппаратной среды (контроль аппаратных устройств (аппаратной конфигурации) ЭВМ);
  - установка алгоритма расчета контрольных сумм объектов, установленных на контроль целостности;
- **механизм настройки подключения к домену** – настройка параметров сервера LDAP через файлы конфигураций hosts, krb5.conf и ldap.conf для аутентификации пользователей, зарегистрированных на сервере LDAP;
- **механизм настройки сетевого адаптера UEFI** – установка способа получения сетевых настроек на клиентских рабочих станциях под управлением СДЗ «SafeNode System Loader» для взаимодействия клиента и сервера LDAP;
- **механизм включения мягкого режима** – установка режима работы на клиентских рабочих станциях, при котором СДЗ «SafeNode System Loader» работает в мягком режиме – пользователям разрешается загрузка ОС без настроенных механизмов защиты с фиксацией доступа в журнале аудита.

14.3.14 Управление блокировкой/разблокировкой учетных записей пользователей СДЗ «SafeNode System Loader» с помощью СЗИ от НСД «Блокхост-Сеть 4» осуществляется в консоли управления СЗИ от НСД «Блокхост-Сеть 4» при помощи настроек рабочей станции, которые передаются от сервера безопасности на клиентскую рабочую станцию.

14.3.15 Настройки рабочей станции с установленным СДЗ «SafeNode System Loader» позволяют удаленно, с помощью СЗИ от НСД «Блокхост-Сеть 4», управлять разблокировкой пользователей, заблокированных после выявления и устранения

нарушений КЦ или при ошибках в процессе идентификации и аутентификации пользователей.

14.3.16 Подробная информация об управлении настройками рабочей станции с установленным СДЗ «SafeNode System Loader» с помощью СЗИ от НСД «Блокхост-Сеть 4» приведена в разделе «Настройки клиента» документа «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора. Часть 1. Управление политиками».

14.3.17 При взятии СДЗ «SafeNode System Loader» под управление с помощью СЗИ от НСД «Блокхост-Сеть 4» учетные записи пользователей, сохраненные в локальной базе данных СДЗ, будут переданы на сервер СЗИ от НСД. Для дальнейшей аутентификации локальными пользователями СДЗ необходимо добавить данных пользователей в политику модуля SafeNode System Loader «Управление аутентификацией».

14.3.18 Активация механизма **«Пользователи с разрешением на вход в ОС»** в СЗИ от НСД позволяет настроить белый список пользователей (локальных и доменных) для входа на клиентскую рабочую станцию со взятым под управление СДЗ «SafeNode System Loader». По умолчанию, после активации механизма, всем пользователям разрешен вход в ОС (добавлен псевдоним ***Все пользователи***).

14.3.19 Подробная информация настройке белого списка пользователей с помощью СЗИ от НСД «Блокхост-Сеть 4» приведена в разделе «Пользователи с разрешением на вход в ОС» документа «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора. Часть 1. Управление политиками».

14.3.20 Для всех учетных записей пользователей, добавленных в СДЗ с помощью политики СЗИ от НСД «Блокхост-Сеть 4», присваивается политика аутентификации ***BHS domain policy*** и политика контроля целостности объектов и загрузки ОС ***All users***. При этом способ аутентификации у пользователей может отличаться в рамках данной политики: пароль, персональный идентификатор или сочетание данных способов.

Рисунок 14.3 – Добавление политики аутентификации BHS domain policy

15 Аварийная консоль АБ

Аварийная консоль предназначена для решения возникающих проблем в условия отсутствия клавиатуры, для выполнения основных функциональных возможностей по администрированию изделия следует использовать основную консоль АБ.

Для загрузки аварийной консоли необходимо пройти процесс аутентификации АБ и в диалоговом окне выбора загрузки аварийной консоли выбрать ***«ОК»*** (рисунок 3.4).

Аварийная консоль АБ выполнена в виде графического интерфейса и представляет собой сокращенную по функциональности консоль для выполнения основных функций по администрированию до загрузки ОС. Ввод данных осуществляется с помощью виртуальной клавиатуры, переключение между вкладками и полями осуществляется при помощи мыши (рисунок 15.1).

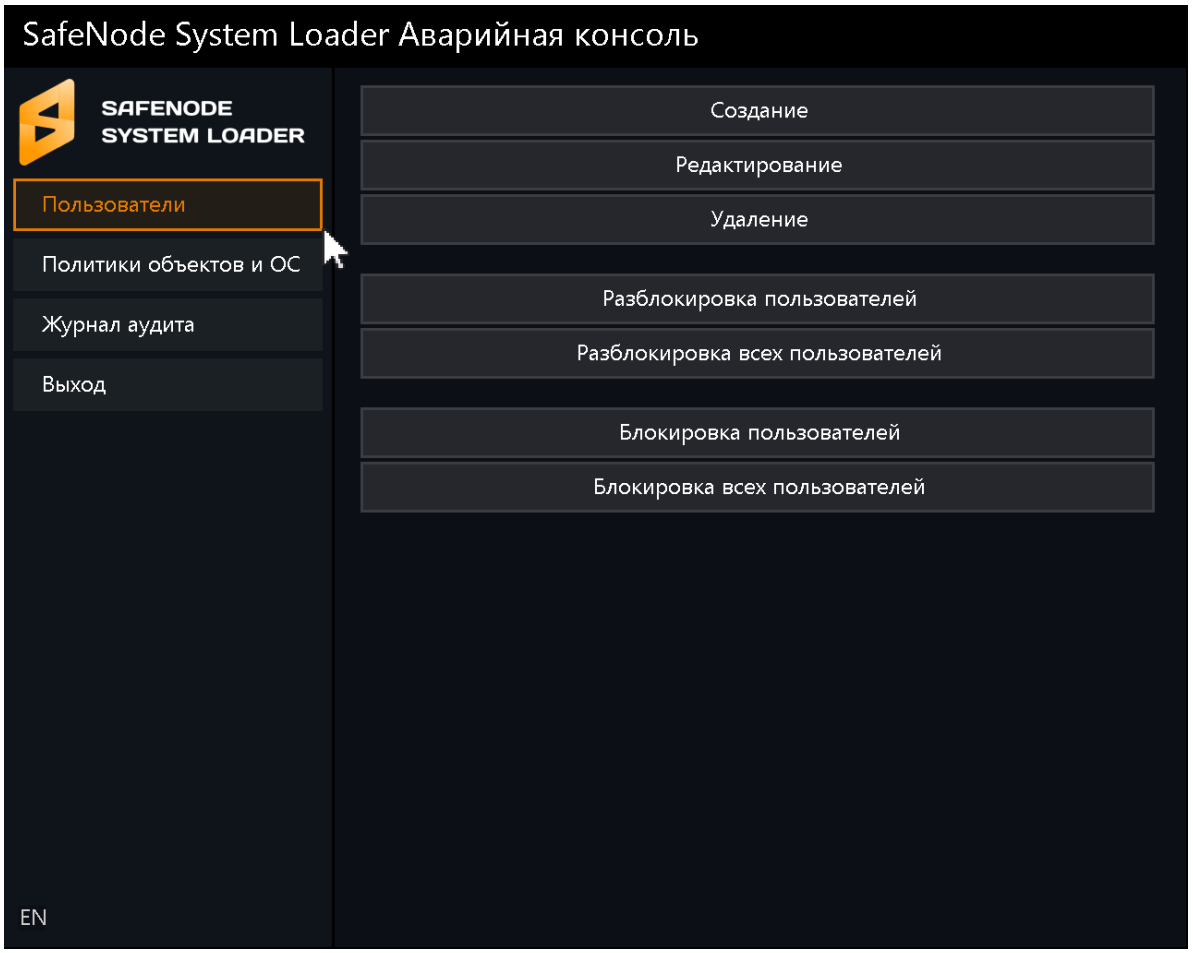


Рисунок 15.1 – Аварийная консоль АБ

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

Основными функциями аварийной консоли являются:

- управление учетными записями пользователей: создание, редактирование, удаление, блокировка, разблокировка (подраздел 15.1);
- пересчет контрольных сумм в политиках контроля и ОС (подраздел 15.2);
- работа с журналами аудита: просмотр сообщений о действиях АБ и пользователей, экспорт журнала на внешнее устройство хранения данных, очистка журнала (подраздел 15.3).

15.1 Управление учетными записями пользователей

В данной консоли не поддерживается создание политик КЦ объектов и загрузки ОС. Данные политики должны быть заведены предварительно с помощью других консолей изделия.

15.1.1 Для создания новой учетной записи пользователя необходимо выбрать в аварийной консоли АБ (рисунок 15.1) подраздел «***Пользователи»→ «Создание»*** (рисунок 15.2).

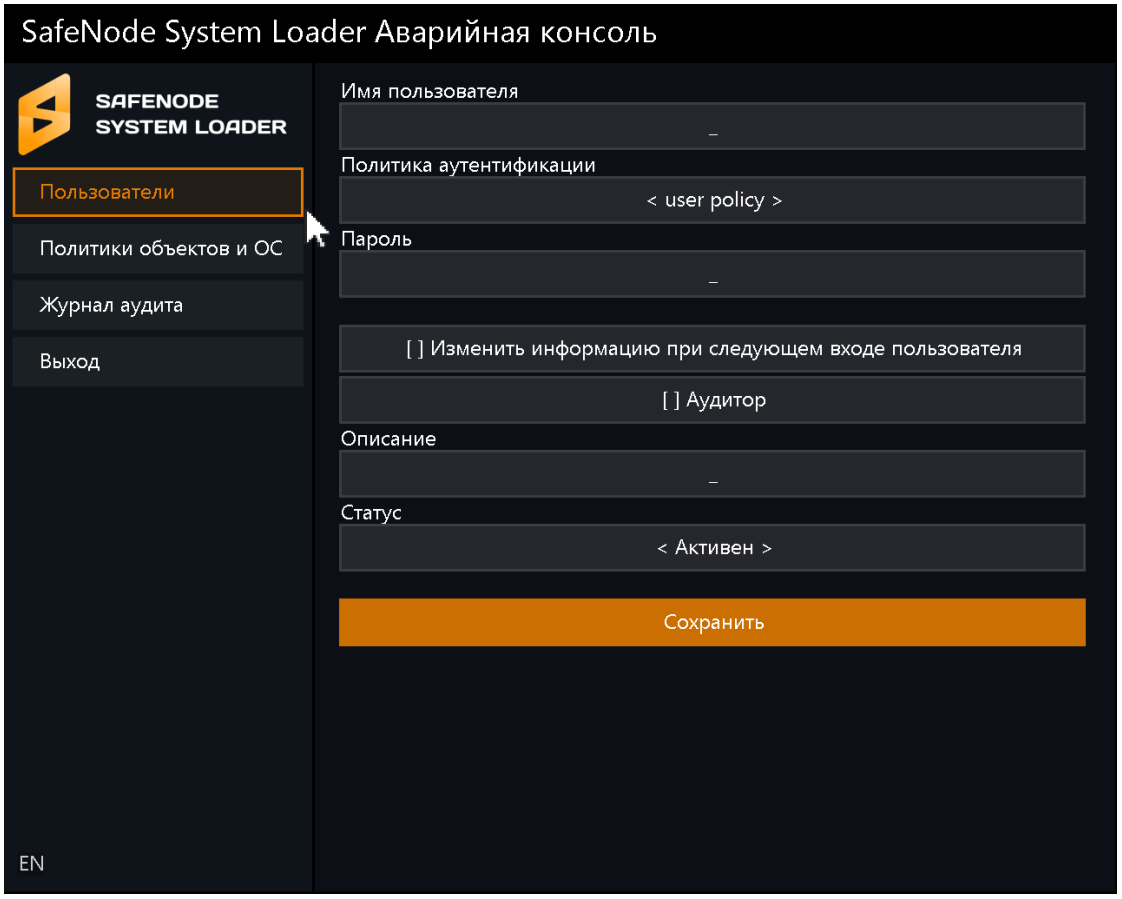


Рисунок 15.2 – Подраздел создания учетной записи пользователя

15.1.2 В таблице 15.1 приведены поля и их возможные значения при создании учетной записи пользователя.

Сложность пароля или PIN-кода персональных идентификаторов пользователей определяется путем использования в нем сочетания заглавных букв, строчных букв, цифр и специальных символов из определенного разработчиком алфавита пароля, приведенного в таблице 5.2.

Таблица 15.1 – Поля и их возможные значения при создании учетной записи пользователя

№	Наименование поля	Возможные значения поля [по умолчанию]	Примечание
1	Имя пользователя	Введенное значение	Уникальное название, не может быть дублировано. Максимальная длина имени учетной записи пользователя – 32 символа. В имени учетной записи пользователя нельзя использовать: 1) первый символ не должен быть специальным символом или цифрой; 2) остальные символы не могут специальными символами
2	Политика аутентификации	Введенное значение	Указание названия политики аутентификации, по правилам которой будет обрабатываться данная учетная запись пользователя
3	Пароль	Значение пароля	Поле предназначено для установки пароля. **Допускается использование символов из таблицы 5.2.**
4	Персональный идентификатор	Присвоенный персональный идентификатор	Поле предназначено для выбора и установки персонального идентификатора.
5	PIN-код	Значение PIN-кода	Поле предназначено для установки PIN-кода персонального идентификатора. **Допускается использование символов из таблицы 5.2.**
6	Изменить информацию при следующем входе пользователя	Включено [Отключено]	Принудительное изменение аутентификационных данных пользователя при его первой успешной аутентификации

№	Наименование поля	Возможные значения поля [по умолчанию]	Примечание
7	Аудитор	Включено [Отключено]	При назначении прав аудитора пользователю предоставляется дополнительная возможность просмотра и экспорта журнала аудита без его очистки
8	Описание	Произвольная текстовая строка	Поле предназначено для формирования описания учетной записи пользователя. Максимальная длина поля – 48 символов.
9	Статус	[Активен] Заблокирован	С помощью данного параметра осуществляется блокировка и разблокировка учетных записей пользователей, за исключением учетной записи АБ

15.1.3 Для заполнения необходимо выбрать требуемое поле и ввести информацию в появившемся окне. После установки полей для сохранения изменений в создаваемой учетной записи пользователя необходимо выбрать ***«Сохранить»*** (рисунок 15.2). При этом в новом диалоговом окне будет выведено сообщение об успешном создании учетной записи пользователя (рисунок 15.3).

При заведении учетных записей пользователей в аварийной консоли нельзя выбрать политику КЦ объектов и загрузки ОС, пользователям назначается встроенная политика контроля ***«All users»***.

Для назначения политики КЦ объектов и загрузки ОС необходимо воспользоваться другой консолью СДЗ.

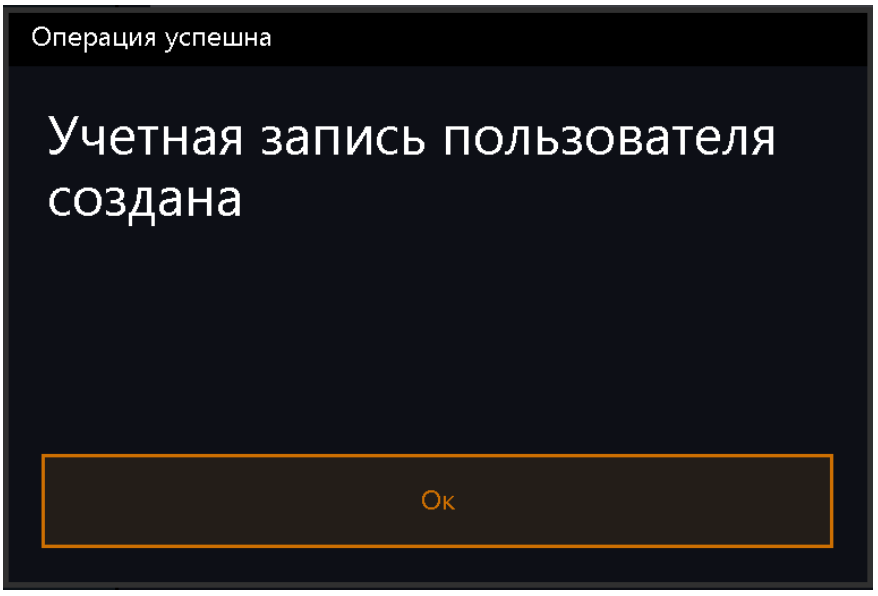


Рисунок 15.3 – Успешное создание учетной записи пользователя

15.1.4 В случае если какое-либо из обязательных полей не было заполнено, на экран ЭВМ будет выведено сообщение об ошибке (рисунок 15.4).

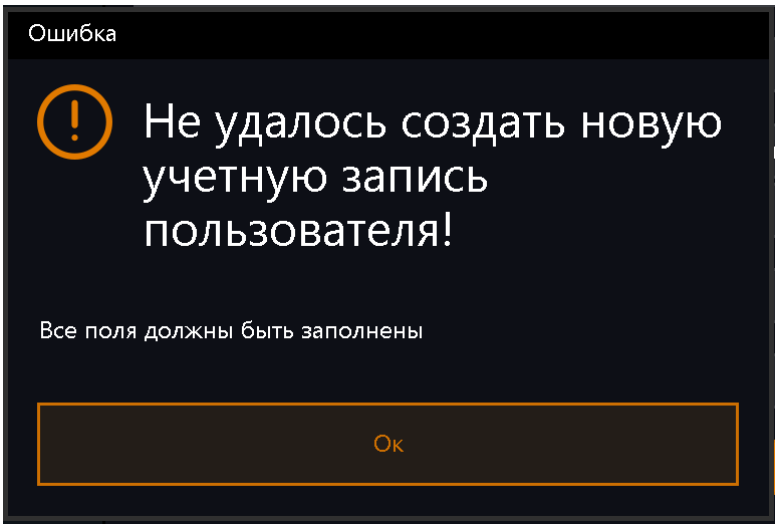


Рисунок 15.4 – Ошибка при создании учетной записи пользователя

15.1.5 Для редактирования существующей учетной записи пользователя необходимо выбрать в главном окне (рисунок 15.1) подраздел ***«Пользователи»→ «Редактирование»*** (рисунок 15.5).

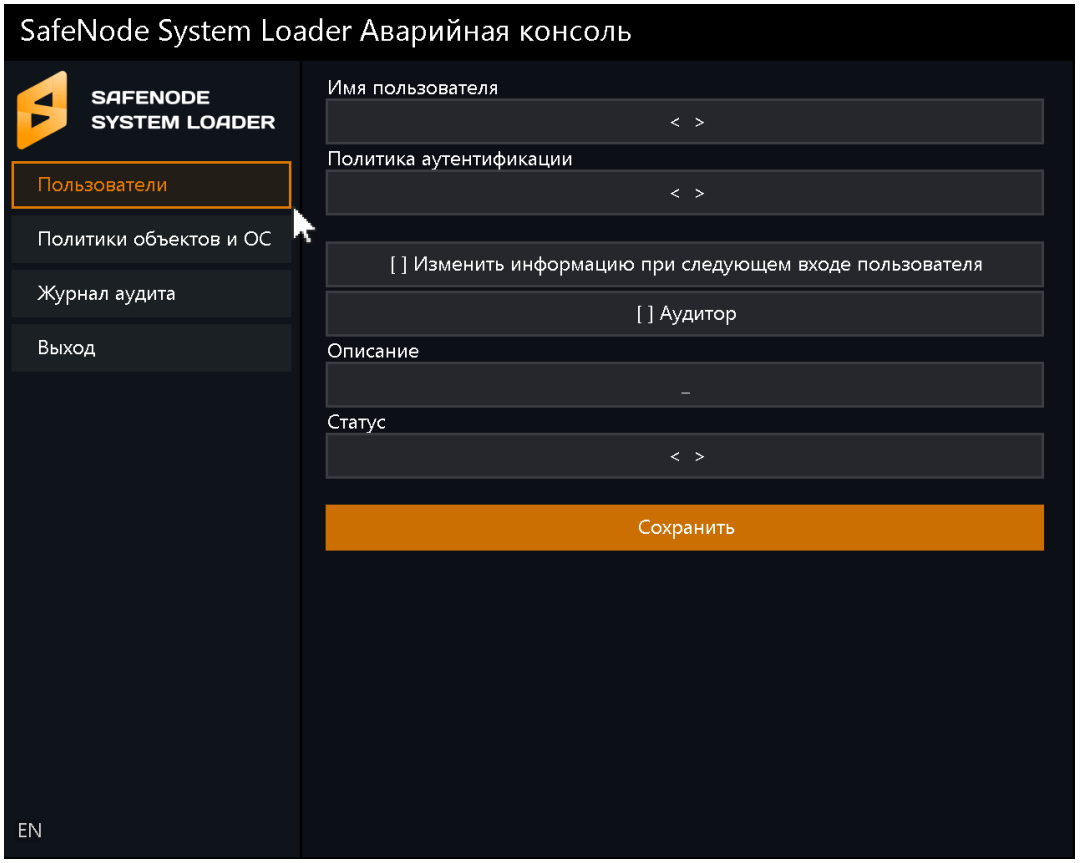


Рисунок 15.5 – Окно редактирования учетной записи пользователя

15.1.6 В новом диалоговом окне редактирования учетной записи пользователя необходимо выбрать имя редактируемой учетной записи пользователя в поле ***«Имя пользователя»*** и нажать кнопку **| *Выбрать* |** (рисунок 15.6).

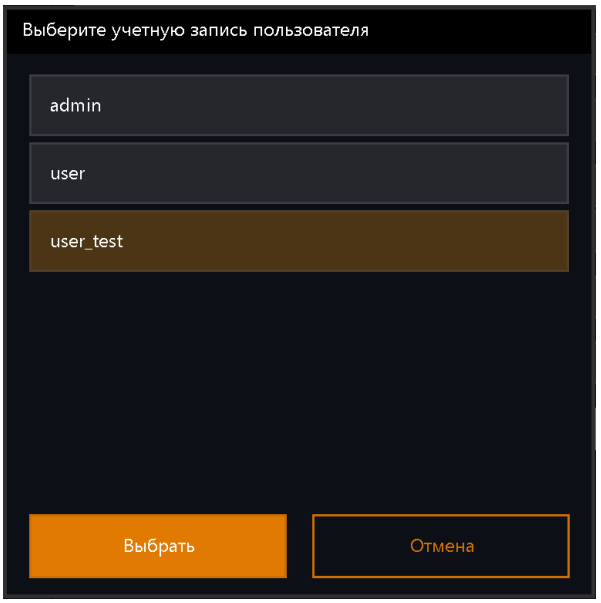


Рисунок 15.6 – Выбор учетной записи пользователя для редактирования

15.1.7 Доступные для редактирования параметры учетной записи пользователя (рисунок 15.7) и их значения приведены в таблице 15.1.

Поле «Имя пользователя» заполняется при создании учетной записи пользователя и в дальнейшем недоступно для редактирования.

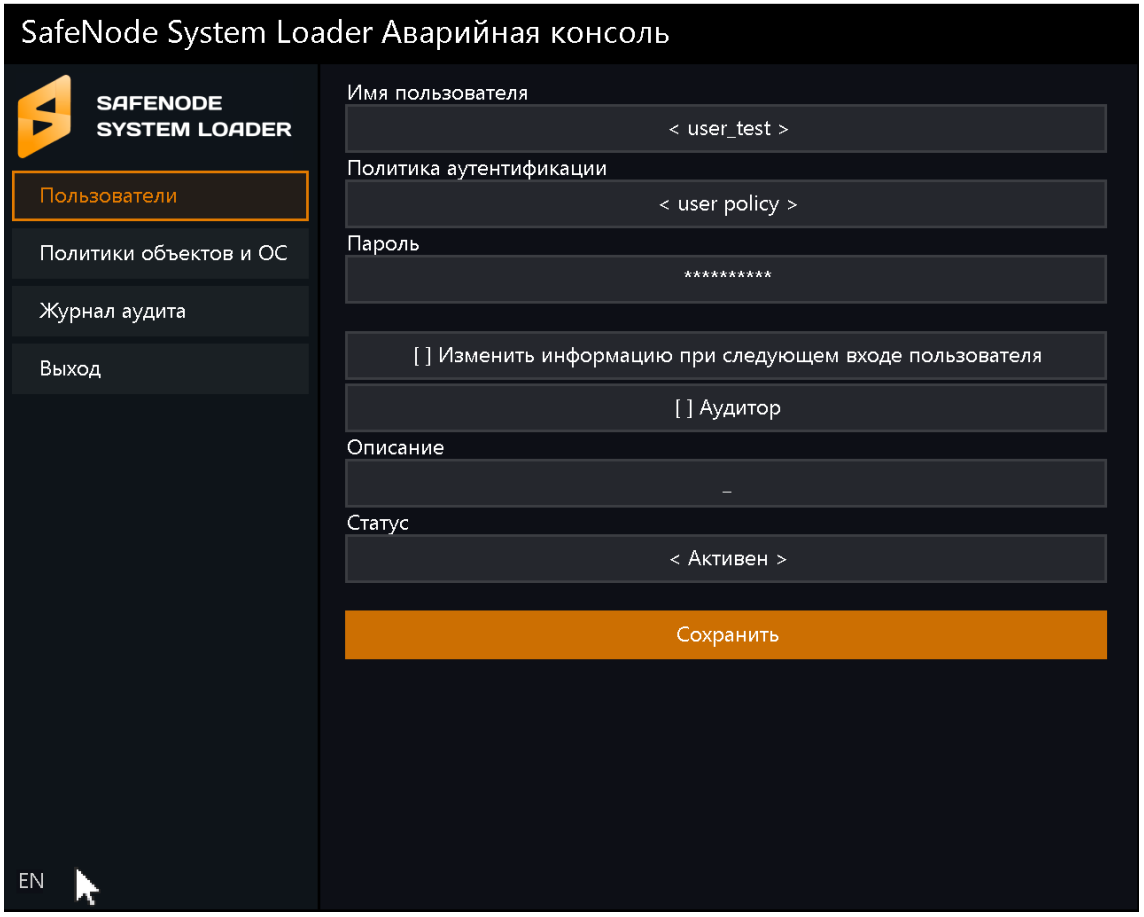


Рисунок 15.7 – Редактируемые поля учетной записи пользователя

15.1.8 Для сохранения изменений редактируемой учетной записи пользователя необходимо нажать кнопку | ***Сохранить*** | (рисунок 15.7). При этом в новом диалоговом окне будет выведено сообщение об успешном редактировании учетной записи пользователя (рисунок 15.8).

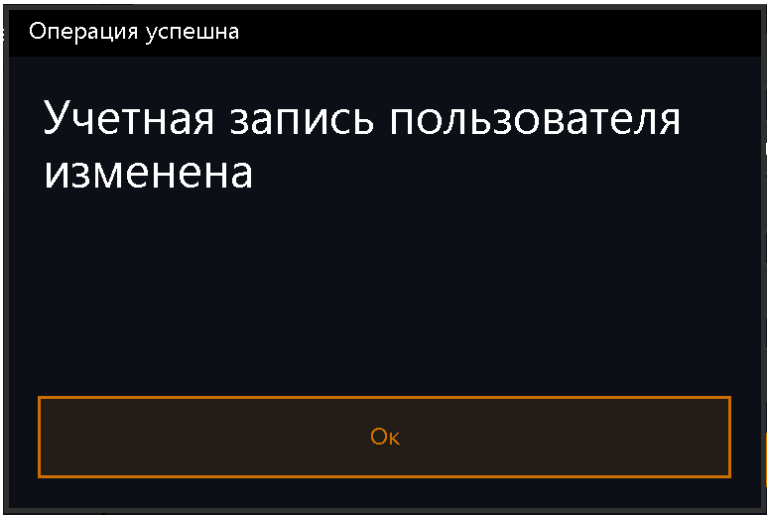


Рисунок 15.8 – Успешное изменение учетной записи пользователя

15.1.9 Для удаления существующей учетной записи пользователя необходимо выбрать в главном окне (рисунок 15.1) подраздел ***«Пользователи»*** → ***«Удаление»*** (рисунок 15.5).

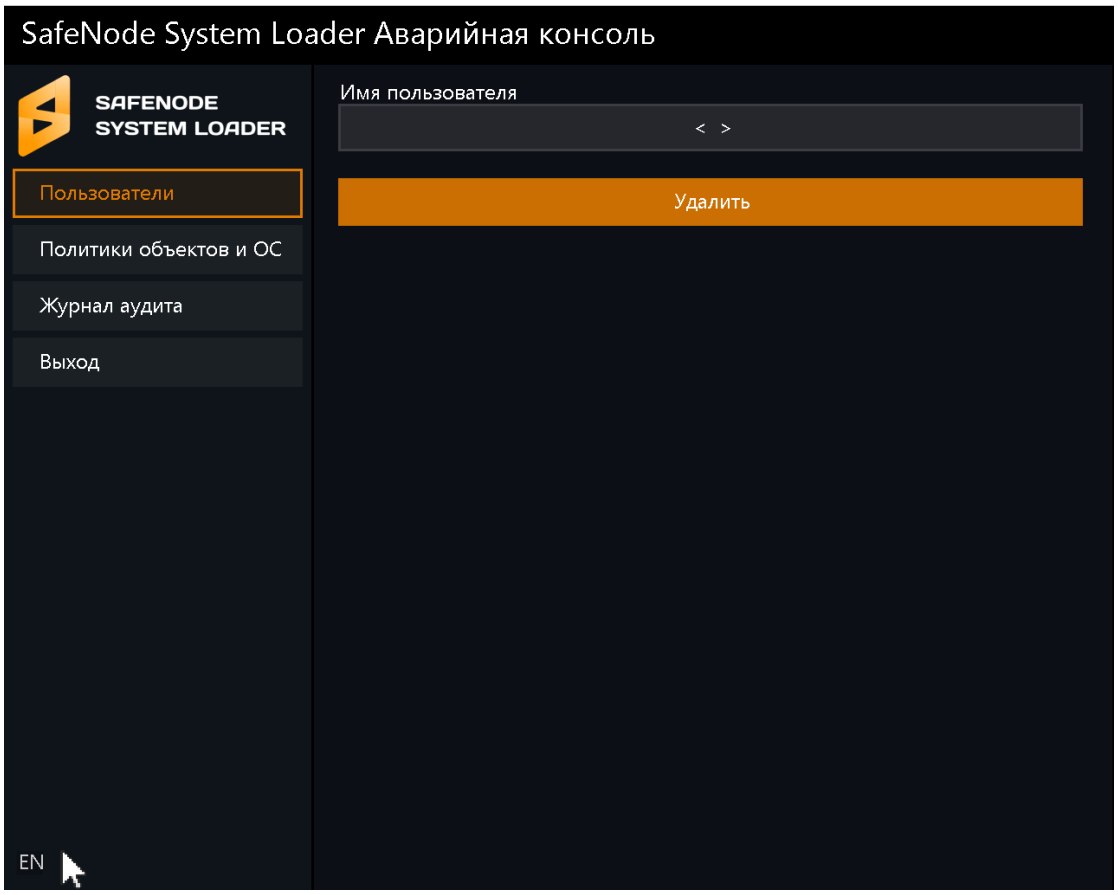


Рисунок 15.9 – Удаление учетной записи пользователя

15.1.10 В новом диалоговом окне удаления учетной записи пользователя (рисунок 15.9) необходимо выбрать имя удаляемой учетной записи пользователя в поле ***«Имя пользователя»*** и нажать кнопку | ***Выбрать*** |.

15.1.11 Для удаления выбранной учетной записи пользователя АБ необходимо и нажать кнопку | ***Удалить*** | (рисунок 15.9). При этом в новом диалоговом окне будет выведено сообщение об успешном удалении учетной записи пользователя (рисунок 15.10).

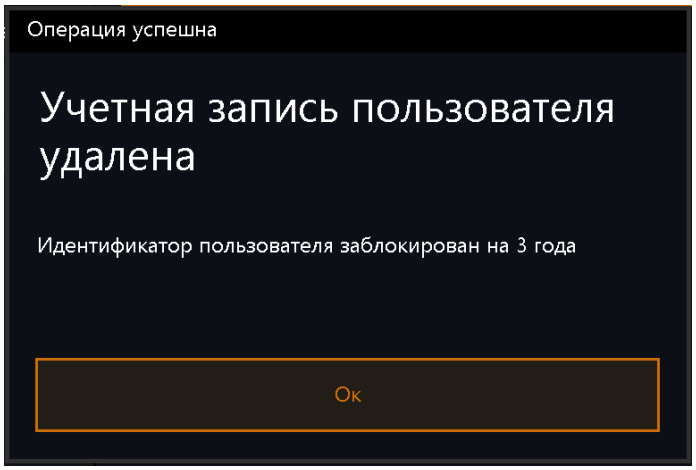


Рисунок 15.10 – Успешное удаление учетной записи пользователя

Удаление учетных записей пользователей производится поочередно.

После удаления учетной записи пользователя из БД изделия исключено его повторное использование в течение трех лет в соответствии с требованиями меры безопасности ИАФ.3 «Методический документ. Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014).

При восстановлении параметров изделия к заводским удаленная учетная запись пользователя станет доступной для использования.

15.1.12 Для разблокировки пользователей после выявления и устранения нарушений КЦ или при ошибках в процессе идентификации и аутентификации пользователей необходимо выбрать в главном окне (рисунок 15.1) подраздел ***«Пользователи»***.

15.1.13 Для разблокировки всех пользователей АБ необходимо в появившемся диалоговом окне (рисунок 15.1) нажать кнопку ***«Разблокировка всех пользователей»***. При этом в новом диалоговом окне будет выведено сообщение об успешной разблокировке пользователей (рисунок 15.11).

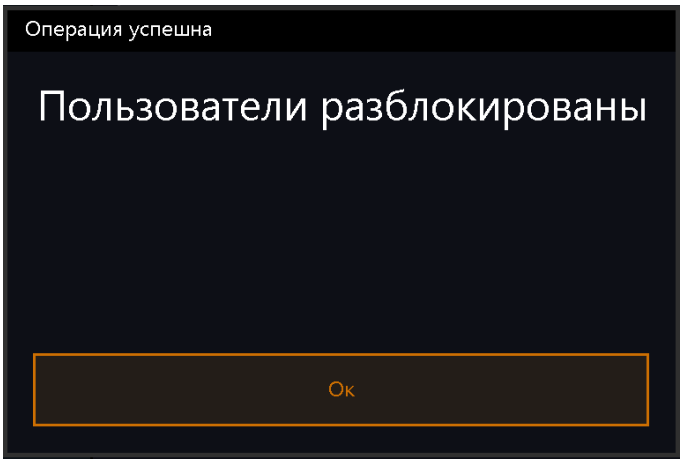


Рисунок 15.11 – Успешная разблокировка всех пользователей

15.1.14 Для разблокировки выборочных учетных записей пользователей АБ необходимо в появившемся диалоговом окне (рисунок 15.1) нажать кнопку **| *Разблокировка пользователей* |**.

15.1.15 В новом диалоговом окне АБ необходимо выбрать учетные записи пользователей для разблокировки и нажать кнопку **| *Выбрать* |** (рисунок 15.12). При этом в новом диалоговом окне будет выведено сообщение об успешной разблокировке выбранных учетных записей пользователей (рисунок 5.11).

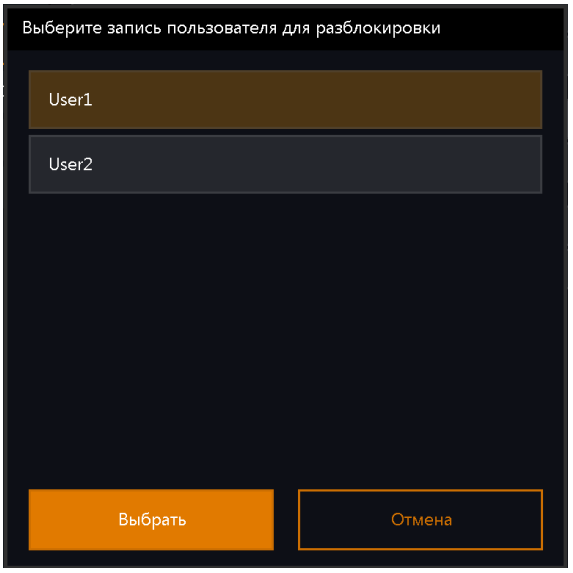


Рисунок 15.12 – Выбор учетных записей для разблокировки

15.1.16 Для блокировки пользователей после выявления и устранения нарушений КЦ или при ошибках в процессе идентификации и аутентификации пользователей необходимо выбрать в главном окне (рисунок 15.1) подраздел ***«Пользователи»***.

15.1.17 Для блокировки всех пользователей АБ необходимо в появившемся диалоговом окне (рисунок 15.1) нажать кнопку | ***Блокировка всех пользователей*** |. При этом в новом диалоговом окне будет выведено сообщение об успешной блокировке пользователей (рисунок 15.13).

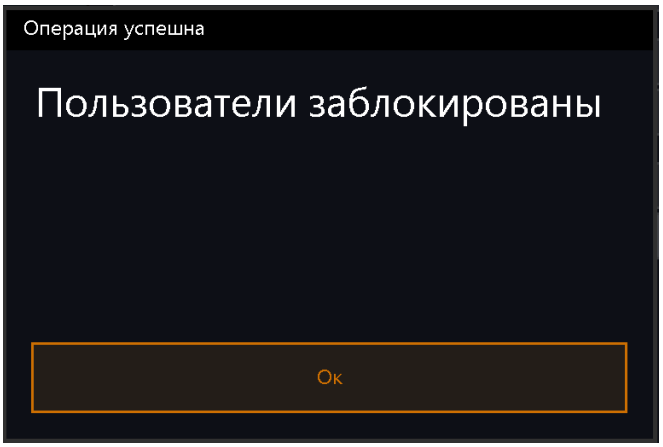


Рисунок 15.13 – Успешная блокировка всех пользователей

15.1.18 Для блокировки выборочных учетных записей пользователей необходимо в появившемся диалоговом окне (рисунок 15.1) нажать кнопку | ***Блокировка пользователей*** |.

15.1.19 В новом диалоговом окне АБ необходимо выбрать учетные записи пользователей для блокировки и нажать кнопку | ***Выбрать*** | (рисунок 15.14). При этом в новом диалоговом окне будет выведено сообщение об успешной блокировке выбранных учетных записей пользователей (рисунок 15.13).

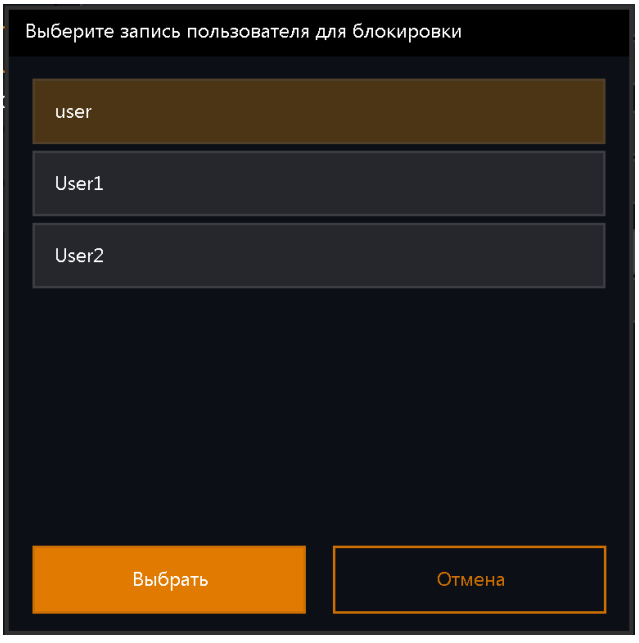


Рисунок 15.14 – Выбор учетных записей для блокировки

15.2 Политики объектов и ОС

15.2.1 Для пересчета значений контрольных сумм всех объектов в БД изделия необходимо выбрать в главном окне аварийной консоли АБ подраздел ***«Политики объектов и ОС»*** (рисунок 15.1). В появившемся диалоговом окне необходимо нажать кнопку **| *Пересчет контрольных сумм объектов* |** (рисунок 15.5).

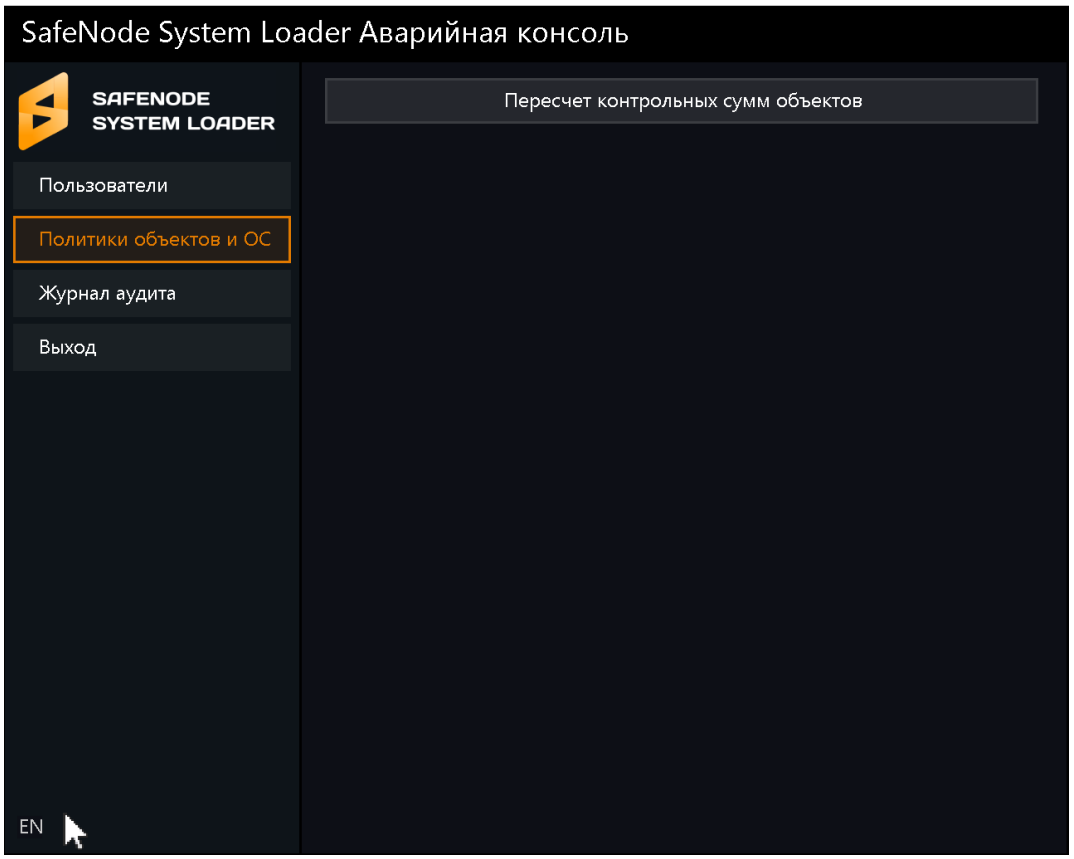


Рисунок 15.15 – Раздел «Политики объектов и ОС»

15.2.2 По окончанию процесса пересчета значений контрольных сумм объектов в БД изделия на экран ЭВМ будет выведено сообщение об успешности пересчета контрольных сумм объектов (рисунок 15.16).

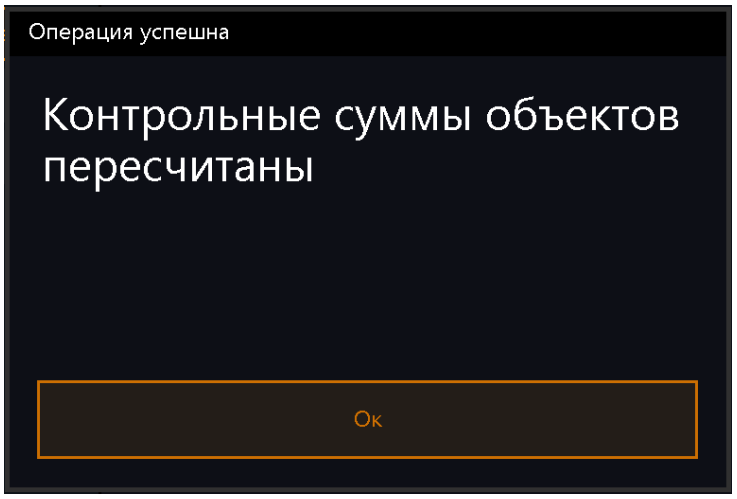


Рисунок 15.16 – Сообщение об успешности пересчета контрольных сумм объектов

15.3 Журнал аудита

15.3.1 Подраздел ***«Журнал аудита»*** предназначен для мониторинга АБ всех событий, происходящих до доверенной загрузки ОС. В журнале аудита регистрируются действия АБ и пользователей.

Для работы с журналом аудита АБ необходимо выбрать в главном окне аварийной консоли АБ (рисунок 15.1) подраздел ***«Журнал аудита»*** (рисунок 15.7).

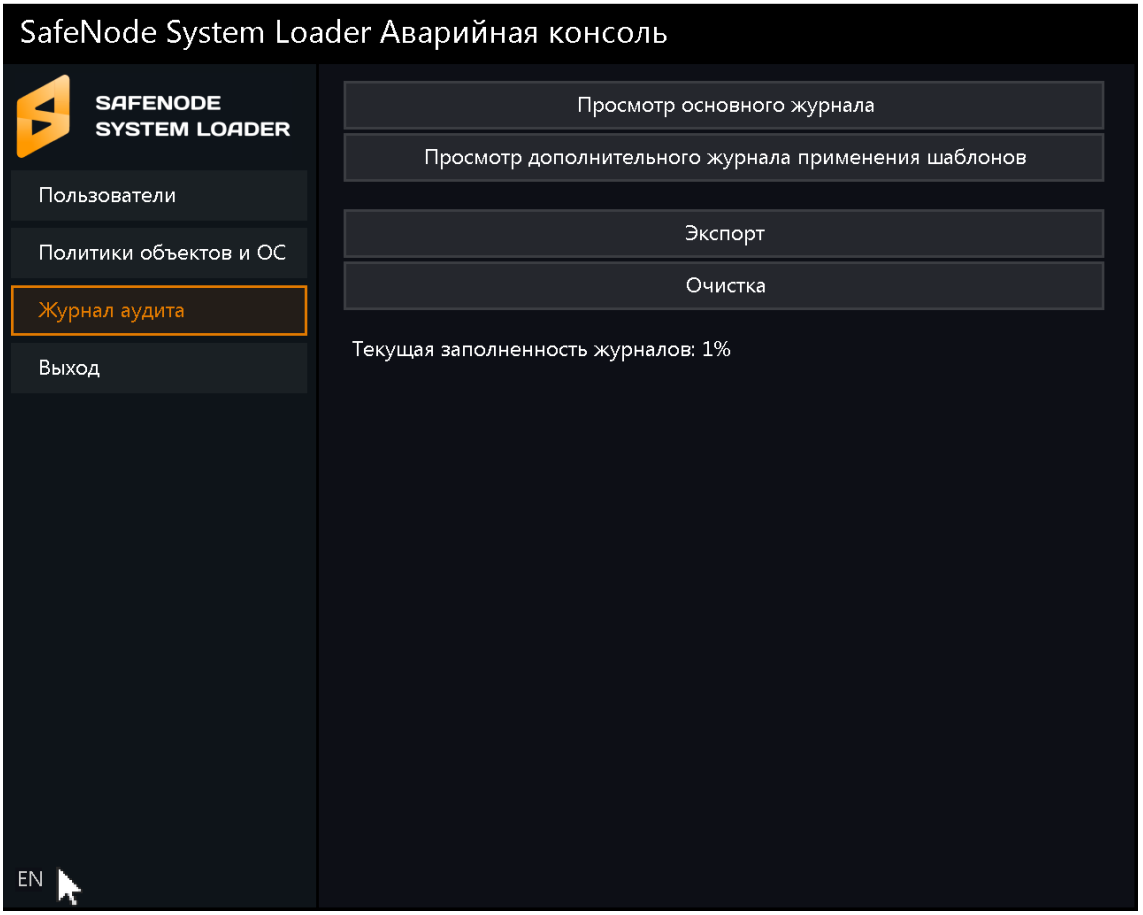


Рисунок 15.17 – Журнал аудита

АБ имеет возможность:

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

Возможность просмотра основного и дополнительного журналов аудита, экспорта журналов аудита на внешнее устройство хранения данных (без их удаления) доступна также пользователям с назначенной ролью аудитора.

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

15.3.2 В основном журнале аудита регистрируются все действия АБ (изменение общих настроек изделия, изменения настроек политик аутентификации и КЦ, действия с учетными записями пользователей) и действия пользователей.

Также в основной журнал аудита регистрируются сообщения при срабатывании механизмов КЦ объектов.

15.3.3 Для просмотра основного журнала аудита необходимо нажать кнопку | ***Просмотр основного журнала*** |. В появившемся диалоговом окне ***«Просмотр основного журнала»*** все события, регистрируемые в основном журнале аудита, разделены построчно (рисунок 15.18).

Деление осуществляется в соответствии со значением параметра ***«Количество записей в журнале для отображения»***, установленного в подразделе ***«Основные настройки»*** (возможные значения параметра приведены в таблице 10.1) в псевдографической консоли СДЗ.

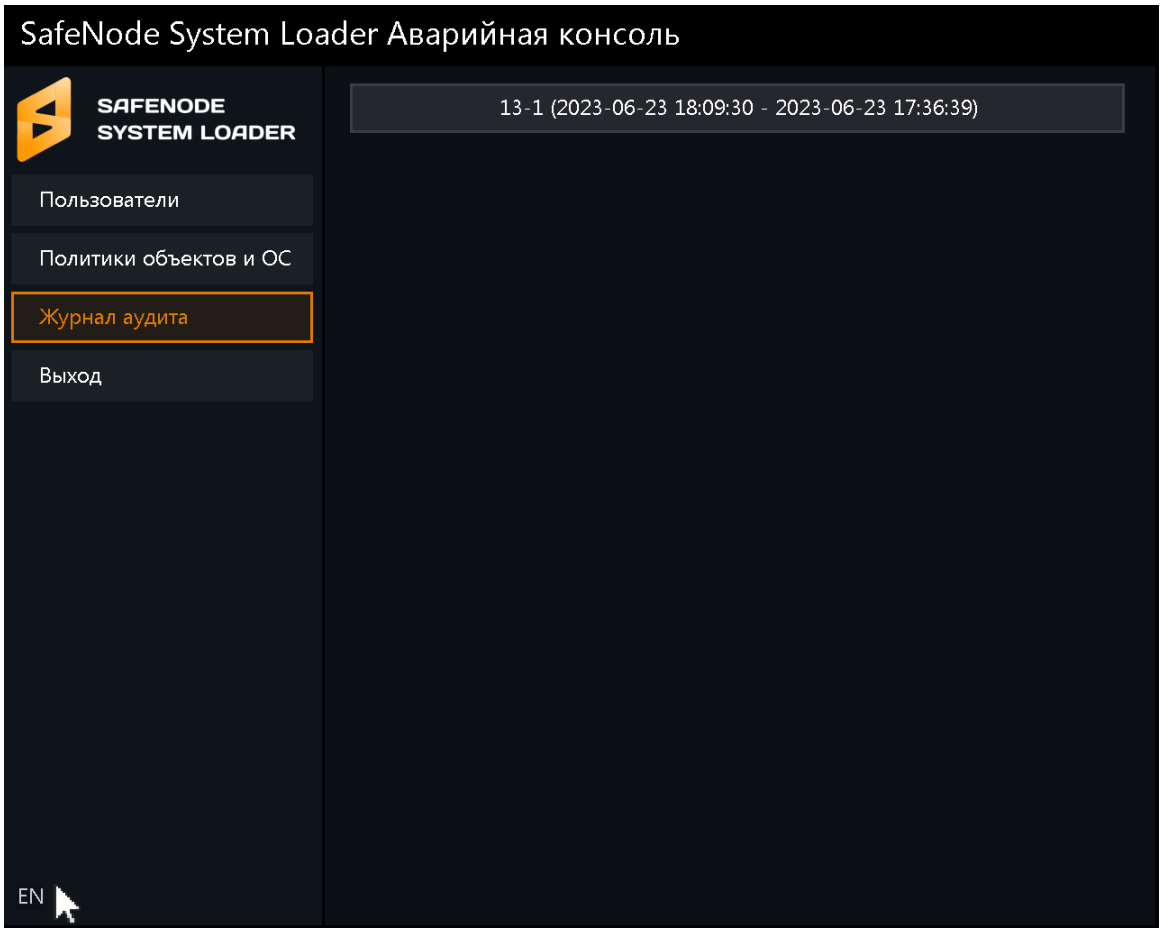


Рисунок 15.18 – Список периодов событий основного журнала аудита

15.3.4 Для просмотра необходимо выбрать строку, соответствующую выбранному периоду времени, за которое требуется просмотреть события, регистрируемые в основном журнале (рисунок 15.19).

15.3.5 Список событий, регистрируемых в основном журнале аудита, приведен в таблице 11.1 руководства.

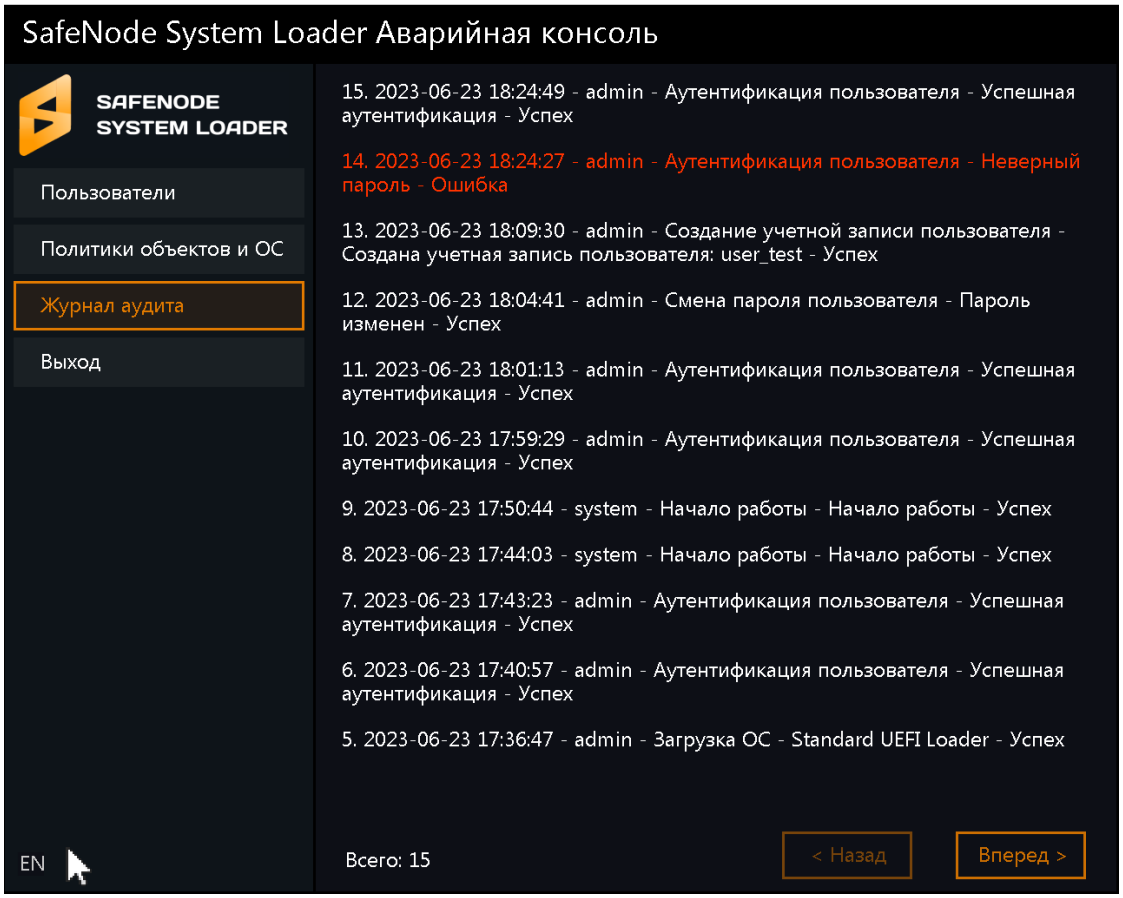


Рисунок 15.19 – Просмотр основного журнала аудита

15.3.6 Каждому событию присваивается порядковый номер и указывается:

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

15.3.7 Строки с сообщениями об ошибках выделены красным цветом (рисунок 15.19).

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

15.3.9 Для просмотра дополнительного журнала применения шаблонов необходимо нажать кнопку | ***Просмотр дополнительного журнала применения шаблонов*** | (рисунок 15.17).

15.3.10 В появившемся диалоговом окне ***«Просмотр дополнительного журнала применения шаблонов»*** все события, регистрируемые в основном журнале, разделены построчно в соответствии со значением параметра ***«Количество записей в журнале для отображения»***, установленного в подразделе ***«Основные настройки»***.

15.3.11 АБ необходимо выбрать строку, соответствующую периоду времени, за которое требуется просмотреть события, регистрируемые в дополнительном журнале применения шаблонов.

15.3.12 В появившемся диалоговом окне ***«Просмотр дополнительного журнала применения шаблонов»*** АБ предоставляется возможность просмотра всех действий, по применению шаблонов к политикам (рисунок 15.20).

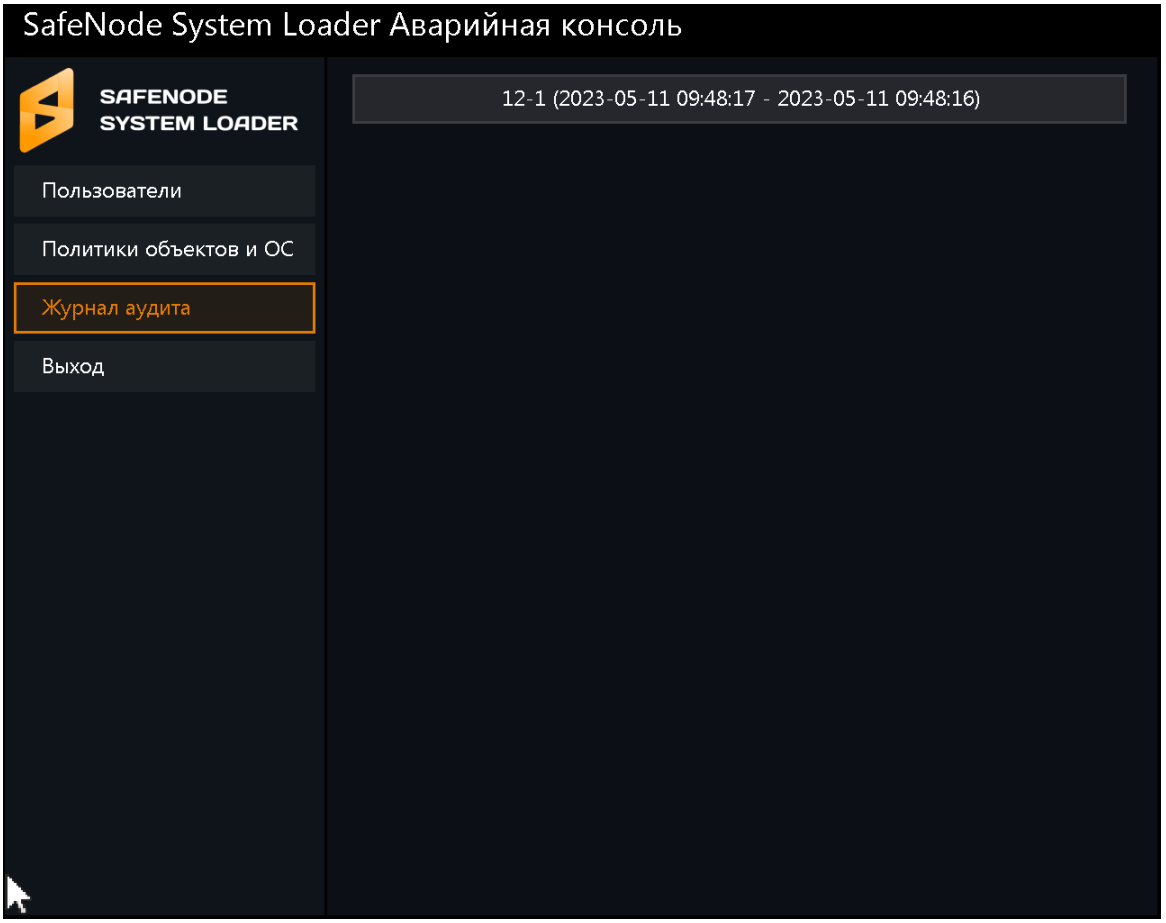


Рисунок 15.20 – Просмотр дополнительного журнала применения шаблонов

15.3.13 Каждому событию присваивается порядковый номер и указывается:

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

15.3.14 Строки с сообщениями об ошибках выделены красным цветом (рисунок 15.20).

15.3.15 АБ имеет возможность экспортировать журналы аудита на внешнее устройство хранения данных. Для этого необходимо:

- подключить устройство хранения данных к ЭВМ;
- в разделе ***«Журнал аудита»*** нажать кнопку **|*Экспорт*|** (рисунок 15.17);
- в новом диалоговом окне выбрать устройство хранения данных и нажать кнопку **|*Выбрать*|** (рисунок 15.21);
- при успешном экспорте журналов на экран ЭВМ будет выведено сообщение (рисунок 15.22).

15.3.16 Журналы аудита будут сохранены в корневой раздел выбранного устройства хранения данных в файлы ***sdzlog.csv*** и ***sdzlogT.csv*** (рисунок 15.21).

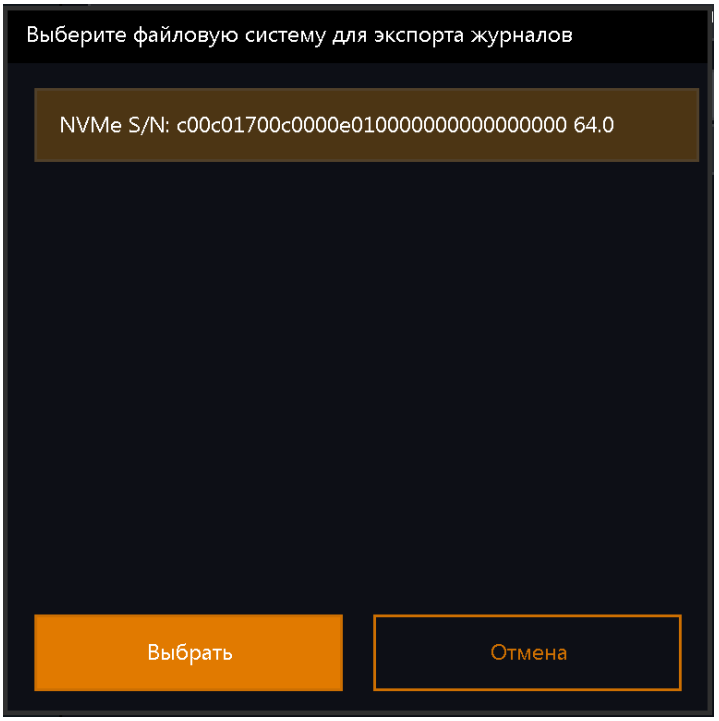


Рисунок 15.21 – Выбор устройства хранения данных для экспорта журналов аудита

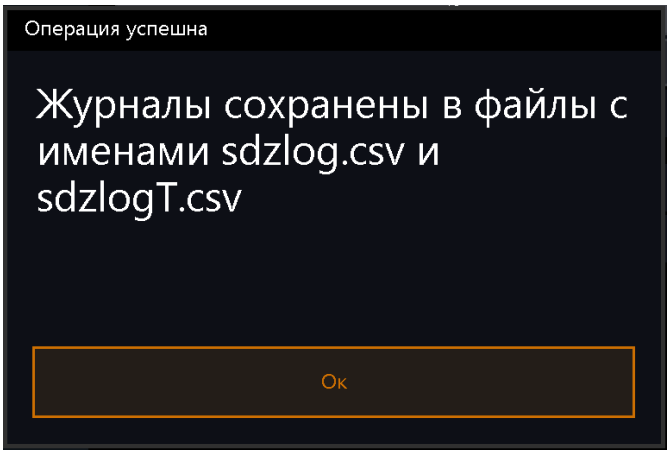
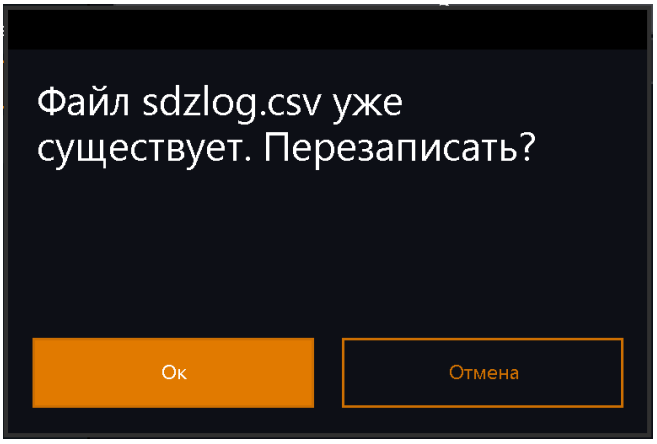
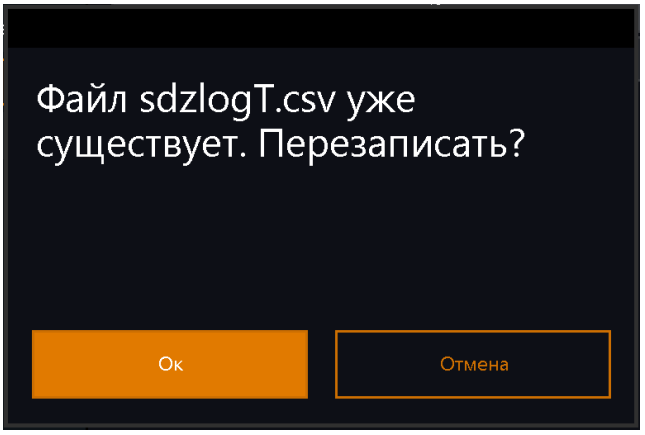


Рисунок 15.22 – Успешный экспорт журналов аудита

15.3.17 В случае существования на выбранном устройстве хранения данных файла с таким именем АБ на экран ЭВМ будет выведено предупреждение (рисунок 15.23 а, б).



а)



б)

Рисунок 15.23 – Перезапись файлов журналов аудита

Рекомендуется периодически осуществлять экспорт журналов на внешнее устройство хранения данных.

15.3.18 АБ имеет возможность удалить записи журналов аудита без их экспорта.

15.3.19 Для очистки журналов АБ необходимо нажать кнопку ***«Очистка»*** (рисунок 15.17) и в новом диалоговом окне подтвердить очистку журналов (рисунок 15.24).

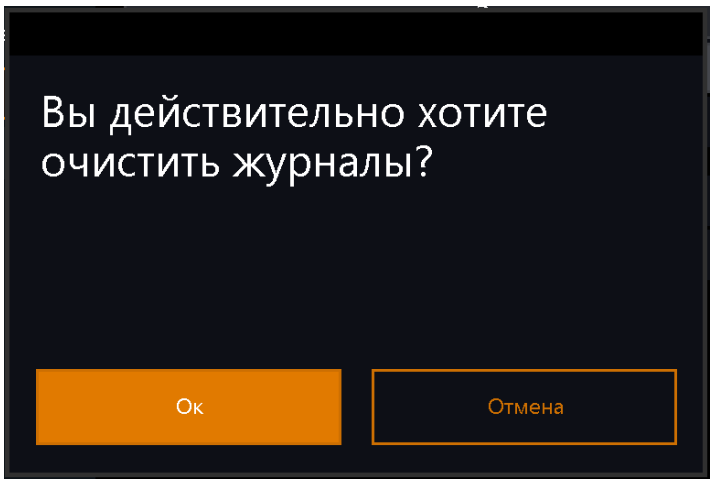


Рисунок 15.24 – Очистка журналов аудита

15.3.20 После завершения выполнения операции АБ будет выведено сообщение ***«Журналы аудита очищены»*** (рисунок 15.25) и в системном журнале добавится запись о произведенной операции.

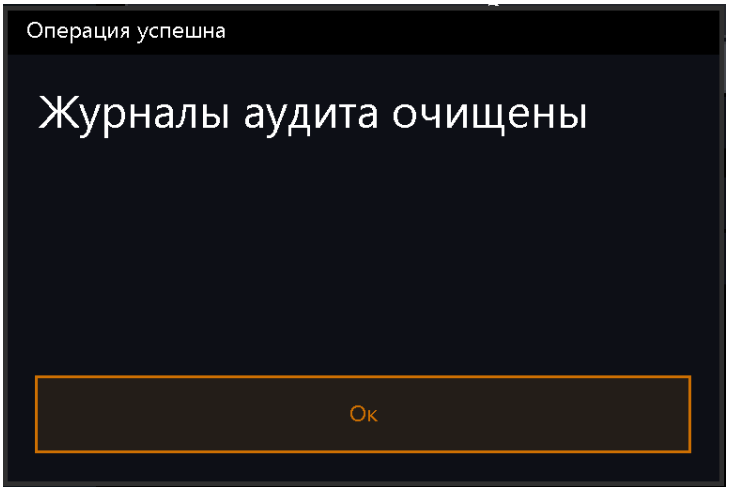


Рисунок 15.25 – Успешная очистка журналов

15.4 Выход из аварийной консоли СЗД

15.4.1 Для выхода из консоли АБ необходимо в главном окне аварийной консоли (рисунок 15.1) нажать кнопку | ***Выход*** | (рисунок 15.26) и выбрать необходимое действие.

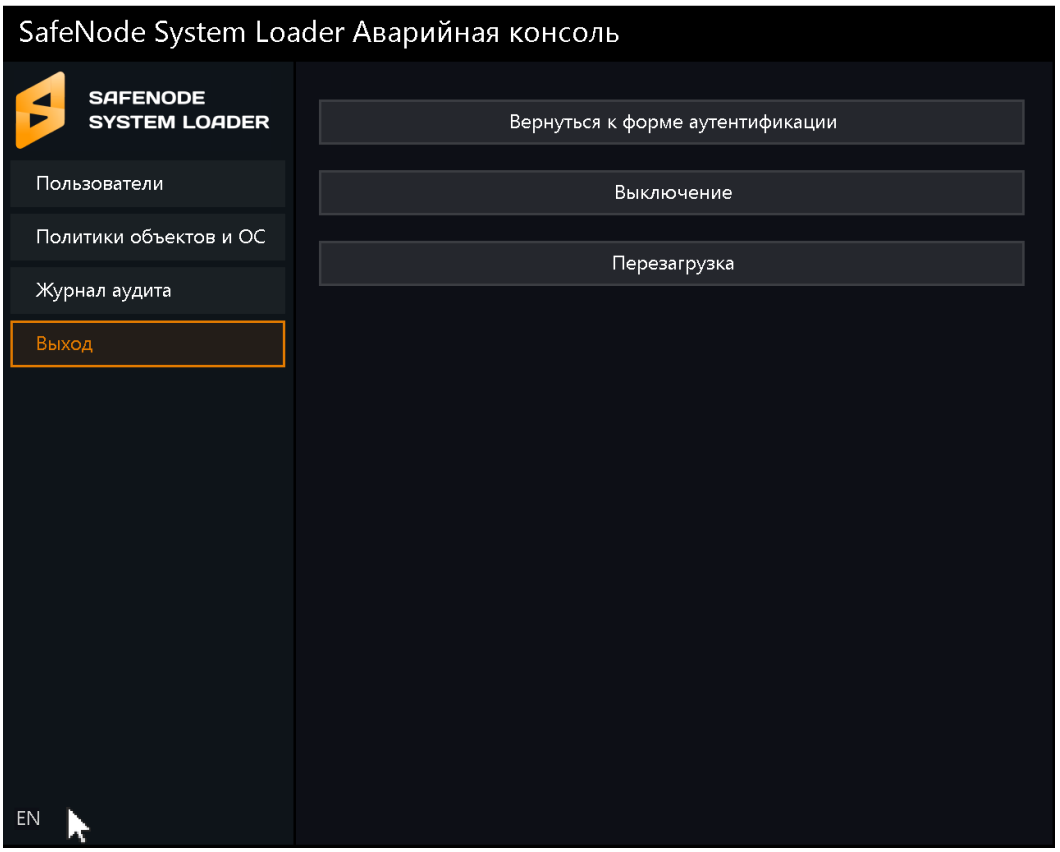


Рисунок 15.26 – Раздел «Выход» аварийной консоли СДЗ

15.4.2 Для возврата в меню аутентификации АБ необходимо выбрать кнопку | ***Вернуться к форме аутентификации*** | (рисунок 15.26).

15.4.3 Для перезагрузки ЭВМ необходимо выбрать кнопку | ***Перезагрузка*** | (рисунок 15.26).

15.4.4 Для выключения ЭВМ необходимо выбрать кнопку | ***Выключение*** | (рисунок 15.26).

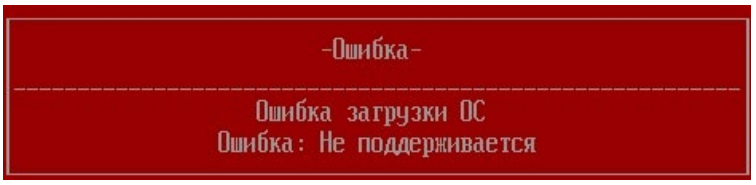
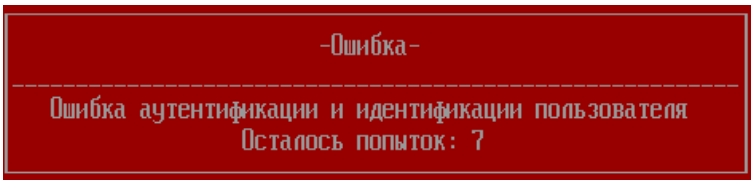
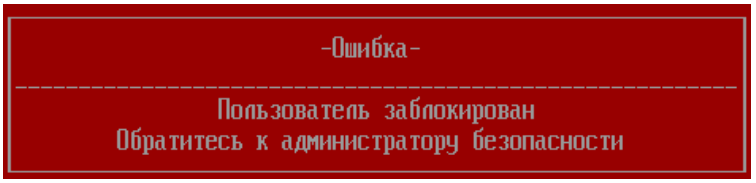
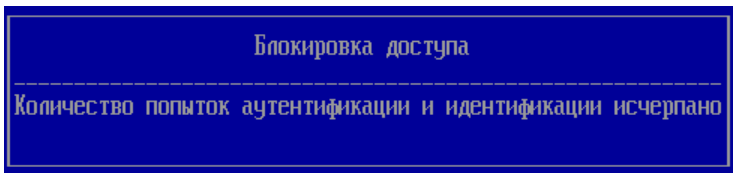
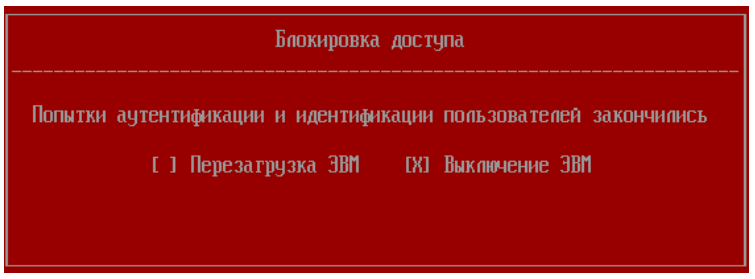
16 Сообщения об ошибках и порядок действий по их устранению

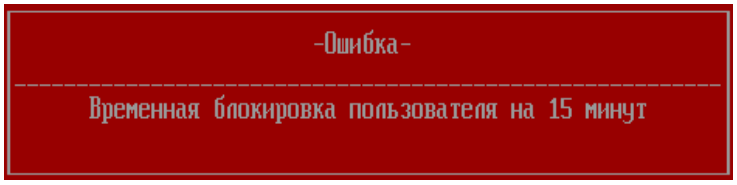
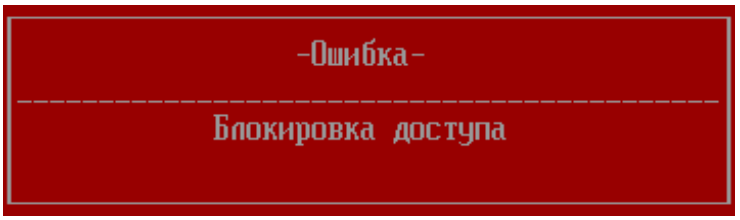
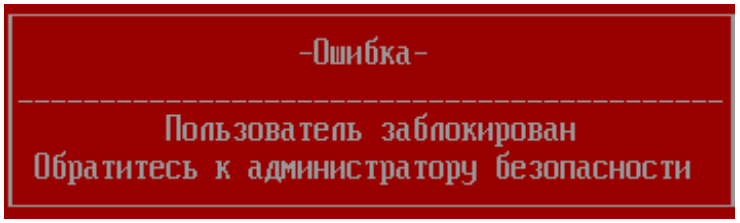
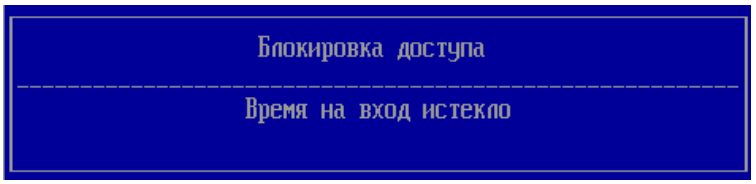
16.1 В процессе работы изделия в составе ЭВМ возможно возникновение ситуаций, при которых АБ на экран ЭВМ в диалоговых окнах выдаются различные информационные сообщения и сообщения об ошибках.

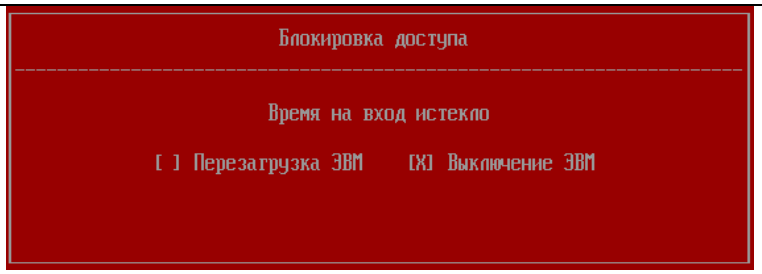
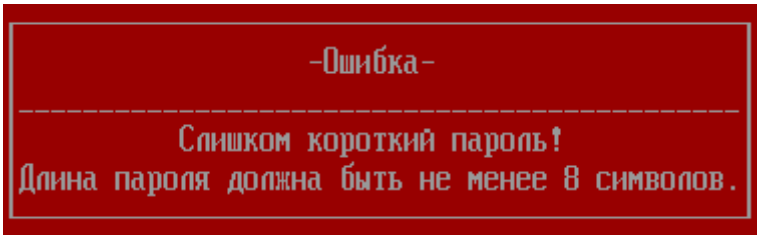
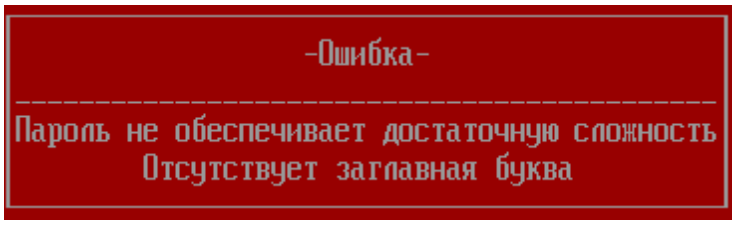
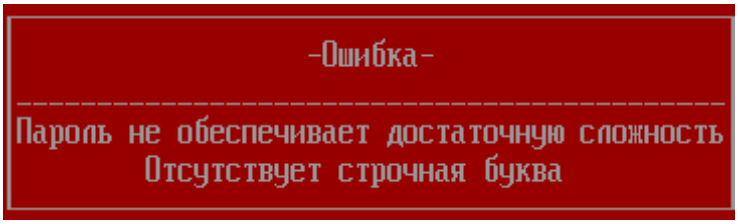
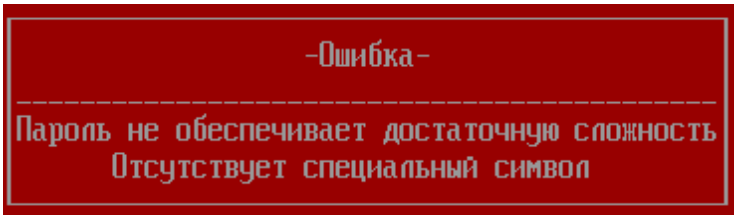
16.2 Перечень сообщений и их типы, причины возникновения и порядок действий АБ по их устранению приведен в таблице 16.1.

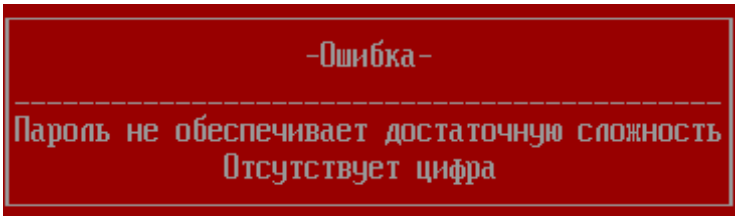
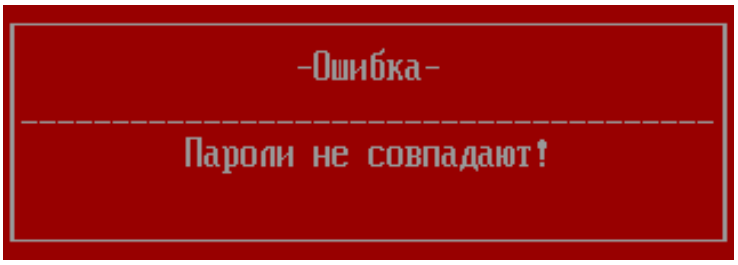
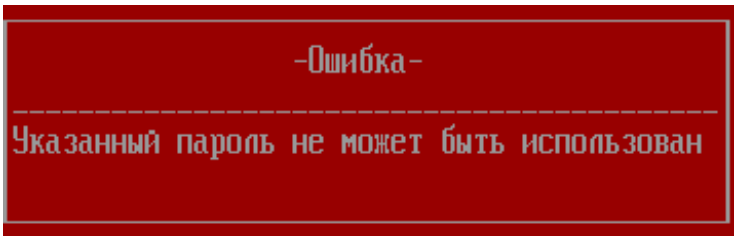
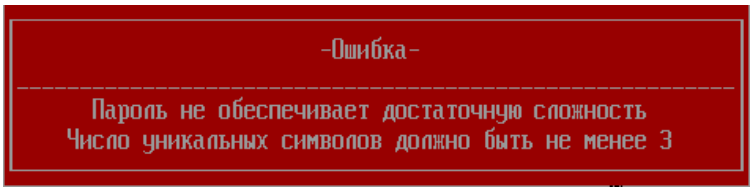
Таблица 16.1 – Перечень сообщений об ошибках при работе ПО изделия

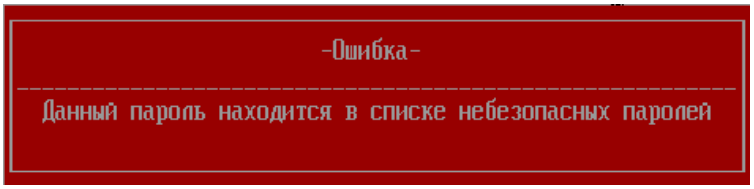
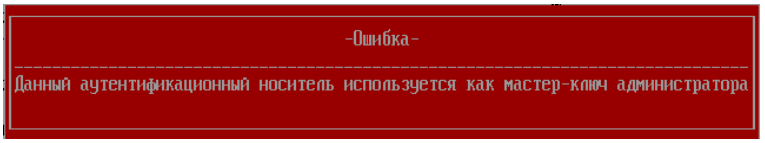
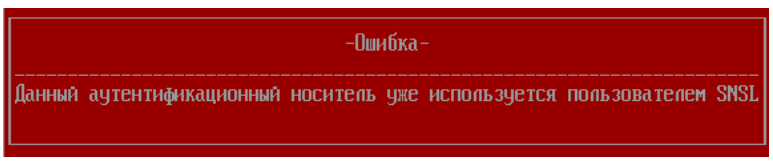
№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий АБ
1	**Ошибка System blocked!** 	**Причины:** Некорректный ключ БД или поврежденная БД изделия **Порядок действий:** Обратиться к АБ для восстановления изделия
2	**Ошибка System blocked!** 	**Причины:** Несоответствие в проверке 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. Список всех возможных кодов ошибок выдаваемых АБ в сообщении ***«System blocked»***, приведен в **Приложении В**.

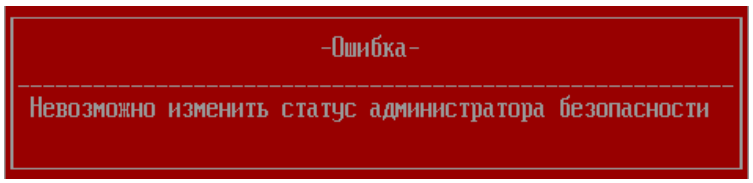
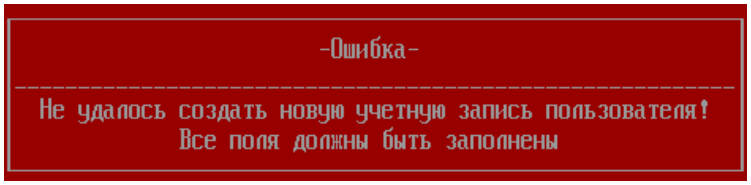
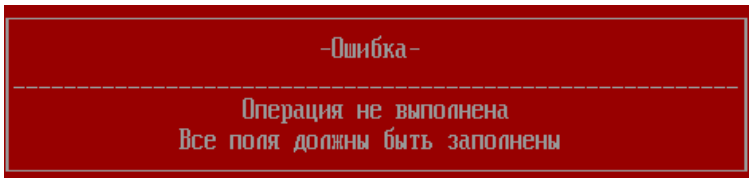
№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий АБ
		Порядок действий: Обратиться к АБ для восстановления изделия
4	**Ошибка загрузки ОС** 	**Причины:** В качестве загрузчика ОС указан неверный файл **Порядок действий:** Указать верный файл загрузчика в пункте меню ***«Контроль 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.

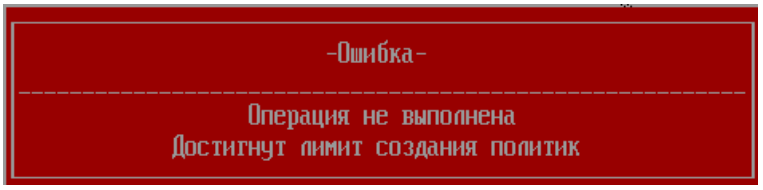
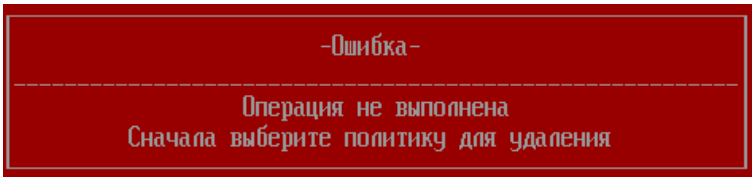
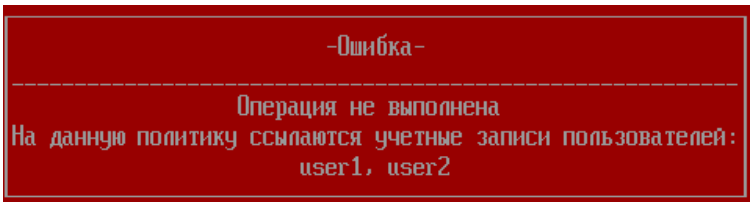
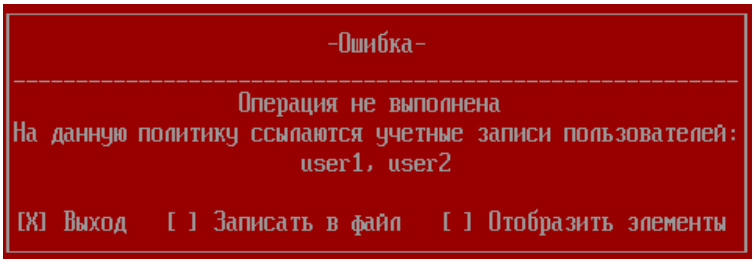
№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий АБ
7	**Временная блокировка пользователя на N минут** 	**Причины:** Достигнуто максимально разрешенное количество индивидуальных попыток аутентификации пользователя **Порядок действий:** Обратиться к АБ
8	**Блокировка доступа. Пользователь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

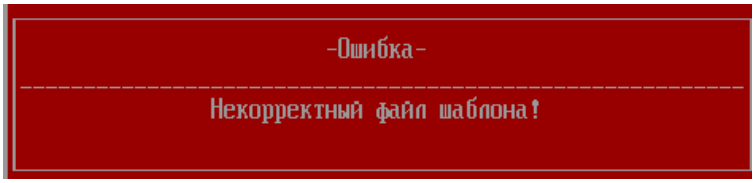
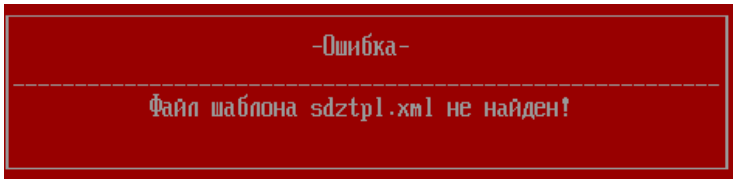
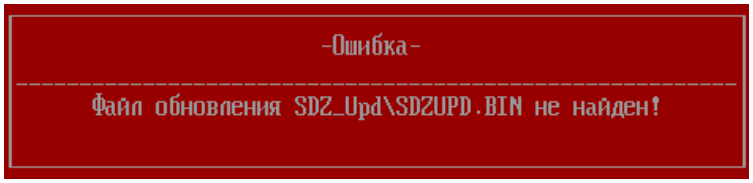
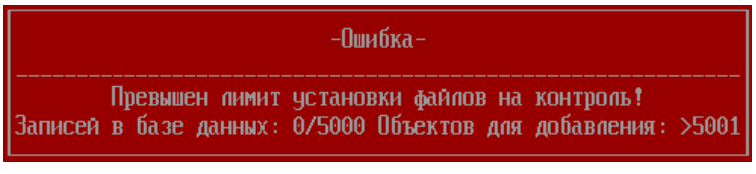
№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий АБ
		
10	**Слишком короткий пароль!** 	**Причины:** Новый пароль пользователя не удовлетворяет требованиям по минимальной длине пароля **Порядок действий:** Ввести пароль длиной не менее 8 символов
11	**Отсутствует заглавная буква** 	**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 **Порядок действий:** Ввести новый пароль, который будет содержать хотя бы один специальный символ

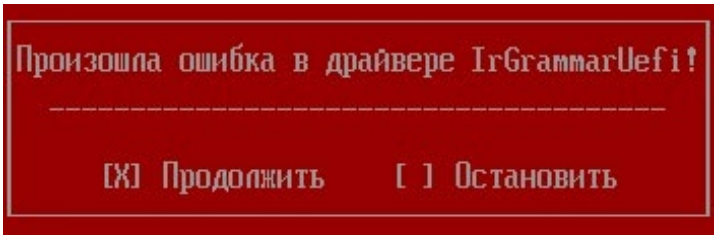
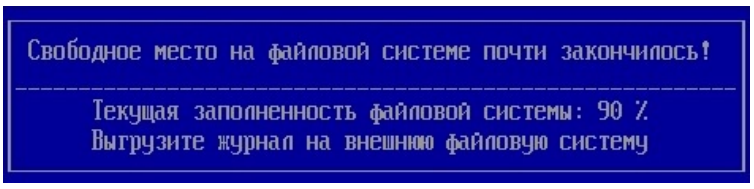
№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий АБ
14	**Отсутствует цифра** 	**Причины:** Новый пароль пользователя не удовлетворяет требованиям по сложности **Порядок действий:** Ввести новый пароль, который будет содержать хотя бы одну цифру
15	**Пароли не совпадают!** 	**Причины:** 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 БД. 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	**Пароль не обеспечивает достаточную сложность. Число уникальных символов должно быть не менее N** 	**Причины:** 1. Новый пароль содержит меньшее количество уникальных символов. **Порядок действий:** 1. Необходимо указать новый пароль пользователя, который содержит необходимое количество уникальных символов

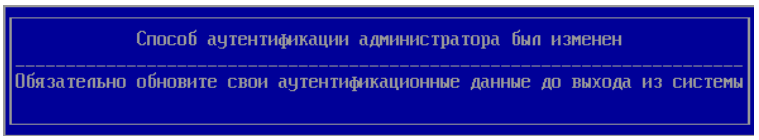
№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий АБ
		согласно политике аутентификации
18	**Данный пароль находится в списке небезопасных паролей** 	**Причины:** 1. Новый пароль совпадает с паролем из перечня небезопасных паролей. **Порядок действий:** 1. Необходимо указать новый пароль пользователя, который удовлетворяет требованиям согласно политике аутентификации
19	**Неверный PIN-код!** 	**Причины:** Введен неверный PIN-код персонального идентификатора АБ **Порядок действий:** Ввести верный PIN-код
20	**Данный аутентификационный носитель используется как мастер-ключ администратора** 	**Причины:** В качестве АНП пользователю (АБ) выбран носитель, который используется в качестве мастер-ключа администратора **Порядок действий:** Выбрать другой АНП
21	**Данный аутентификационный носитель уже используется пользователем SNSL** 	**Причины:** В качестве мастер-ключа администратора выбран носитель, который используется в качестве АНП для входа пользователем или АБ **Порядок действий:** Выбрать другой АНП

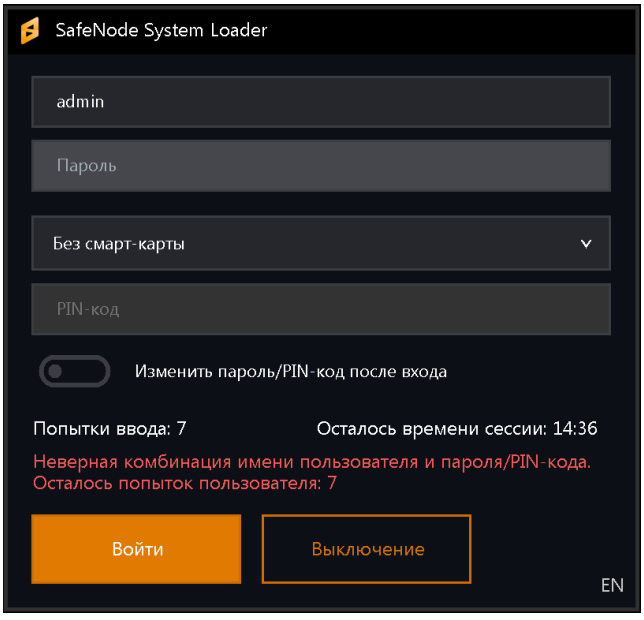
№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий АБ
22	**Невозможно изменить статус администратора безопасности** 	**Причины:** При редактировании учетной записи пользователя АБ осуществлена попытка изменить параметр ***Статус*** и заблокировать АБ **Порядок действий:** Продолжить редактировать учетную запись АБ. Параметр ***Статус*** не подлежит редактированию
23	**Не удалось создать новую учетную запись пользователя!** 	**Причины:** При создании новой учетной записи пользователя заполнены не все поля, обязательные к заполнению **Порядок действий:** Заполнить все обязательные поля
24	**Все поля должны быть заполнены** 	**Причины:** При создании/редактировании политики аутентификации или политики КЦ заполнены не все поля, обязательные к заполнению **Порядок действий:** Заполнить все обязательные поля
25	**Политика с указанным именем уже существует** 	**Причины:** Имя создаваемой политики совпадает с политикой, уже существующей в БД **Порядок действий:** Указать новое имя политики, отличное от предыдущего

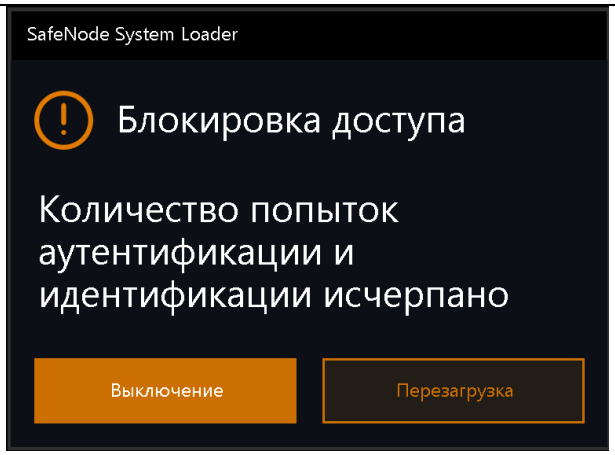
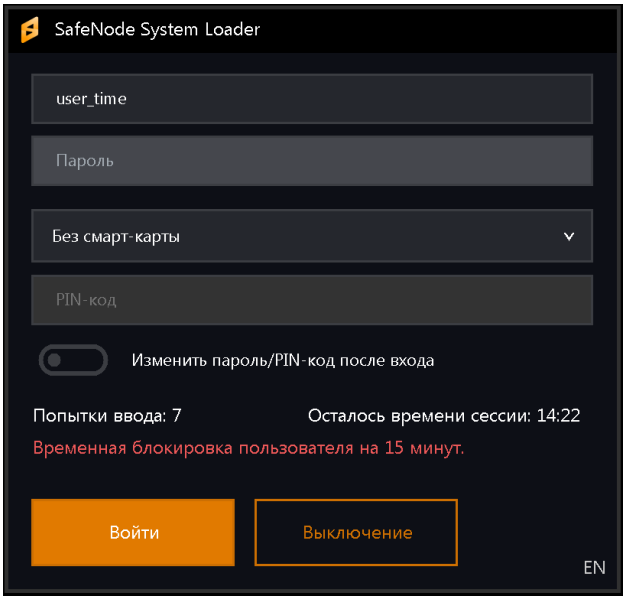
№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий АБ
26	**Достигнут лимит создания политик** 	**Причины:** Превышено максимальное количество созданных политик. Установленный предел количества политик – 20. **Порядок действий:** Удалить неиспользуемые групповые политики и повторить операцию создания политики
27	**Выберите политику для удаления**  	**Причины:** При удалении политики, имя удаляемой политики не выбрано **Порядок действий:** Выбрать имя удаляемой политики и повторить операцию удаления
28	**На политику ссылаются учетные записи пользователей**  	**Причины:** На удаляемую политику ссылаются учетные записи пользователей **Порядок действий:** 1. Поочередно перейти в учетные записи пользователей, которым назначена данная политика, и отредактировать учетные записи путем назначения им другой политики. 2. Повторить действия по удалению политики.

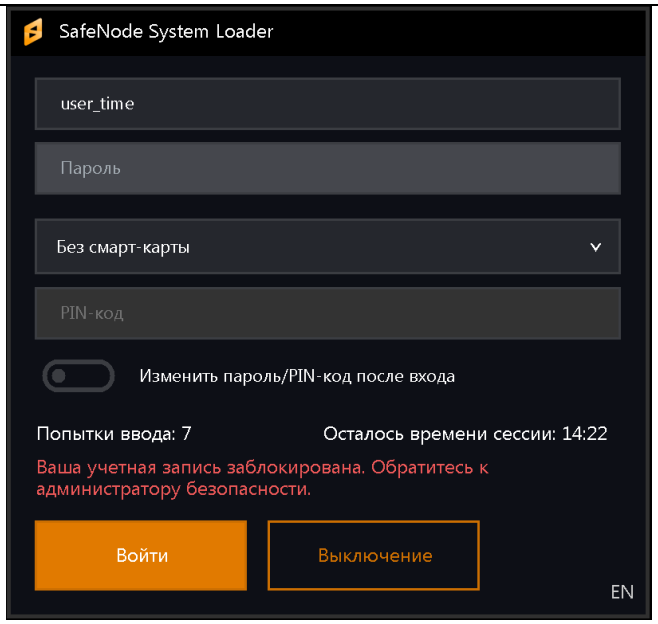
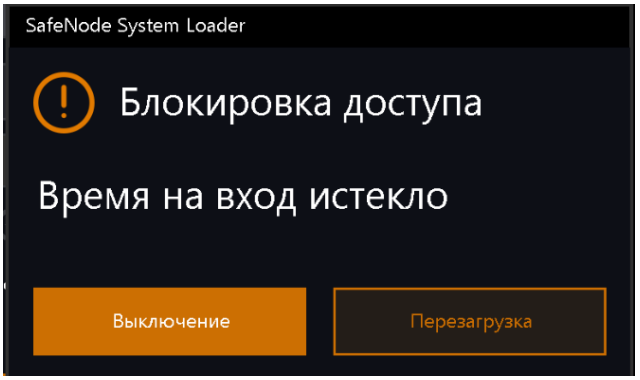
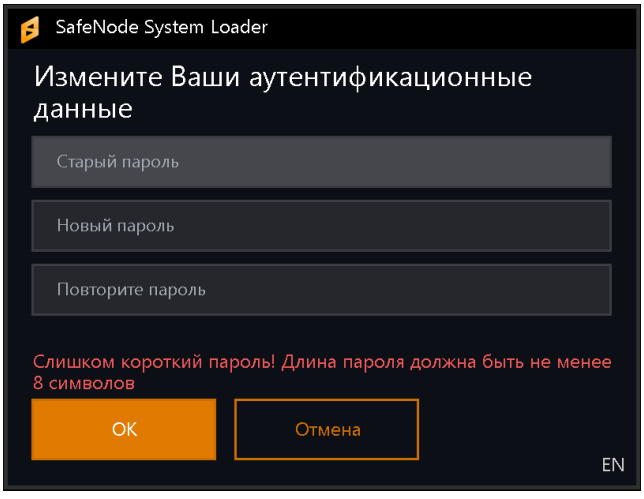
№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий АБ
29	**Некорректный файл шаблона** 	**Причины:** Файл применяемого шаблона поврежден **Порядок действий:** Использовать другой файл шаблона или создать новый
30	**Файл шаблона не найден** 	**Причины:** Файл применяемого шаблона не найден **Порядок действий:** Проверить наличие файла шаблона sdztpl.xml в корневом разделе выбранного устройства хранения данных
31	**Файл обновления не найден** 	**Причины:** Файл обновления ПО изделия не найден **Порядок действий:** Проверить наличие файла обновления SDZUPD.BIN в директории SDZ_Upd в корневом разделе выбранного устройства хранения данных
32	**Превышен лимит установки файлов на контроль!** 	**Причины:** Превышено максимальное количество контролируемых объектов, установленное в разделе ***«Основные настройки»*** **Порядок действий:** Изменить установленное значение максимального количества контролируемых объектов файловой системы в разделе ***«Основные настройки»***

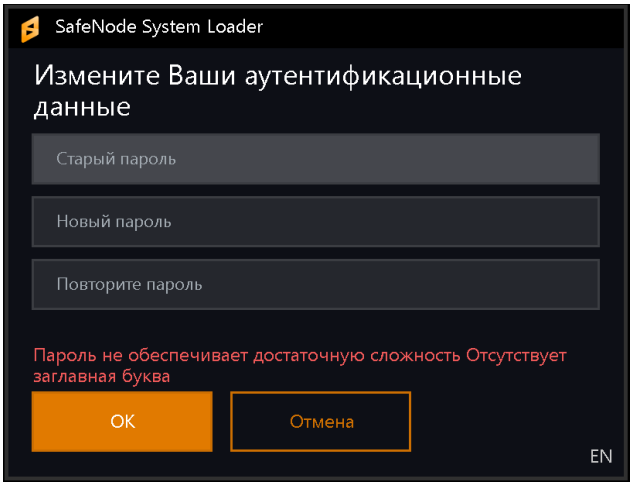
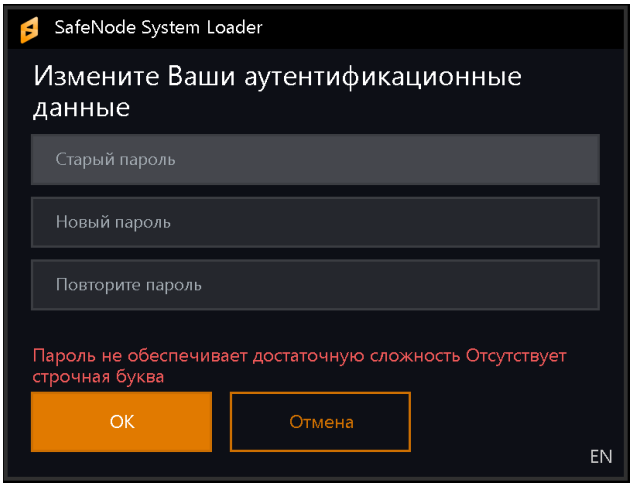
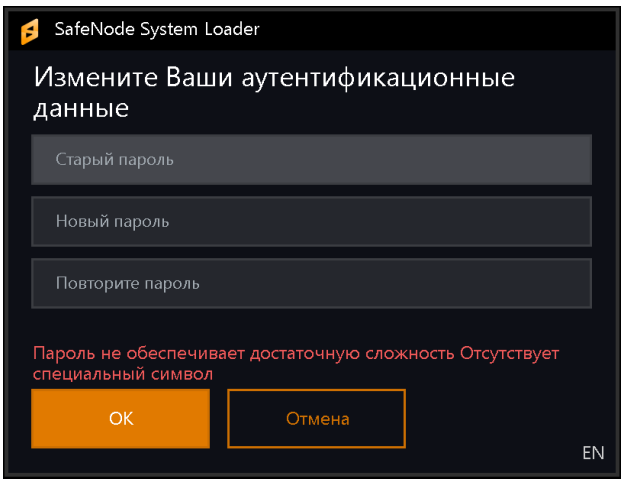
№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий АБ
33	**Ошибка установки на контроль** 	**Причины:** Установка на КЦ устройства CD/DVD-ROM, не содержащего подключенный носитель CD/DVD **Порядок действий:** Подключить носитель CD/DVD и повторить действия по установке на контроль
34	**Журналирование контроля исполнения кода отключено** 	**Причины:** Экспорт журнала контроля исполнения кода при отсутствии в параметре ***«Контроль исполнения кода»*** значения ***«Включен с журналированием»*** **Порядок действий:** Установить в параметре ***«Контроль исполнения кода»*** значение ***«Включен с журналированием»*** и повторить операцию экспорта
35	**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
36	**Свободное место на файловой системе почти закончилось!** 	**Причины:** Предупреждающее сообщение о заполнении файловой системы на 90%. Возможна аутентификация и идентификация АБ и пользователей

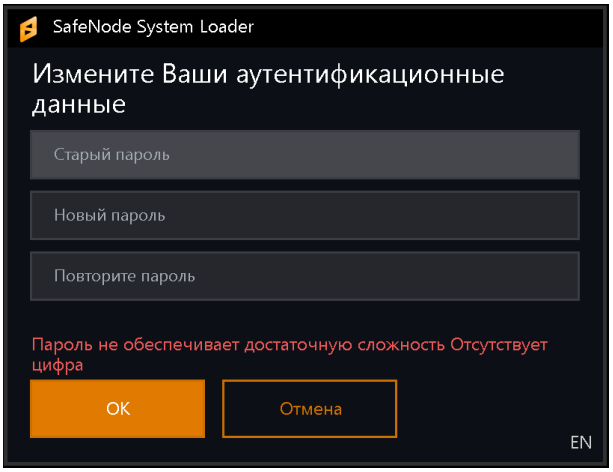
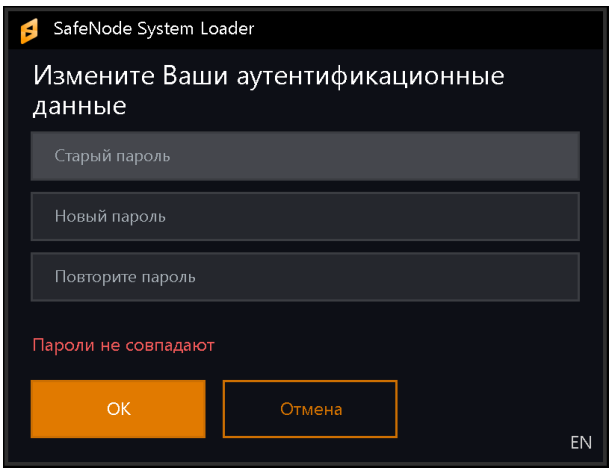
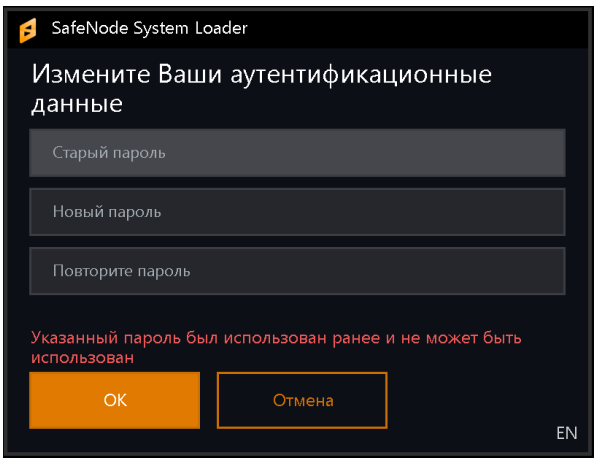
№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий АБ
		Порядок действий: Выполнить аутентификацию и идентификацию АБ в системе и сохранить журнал на внешний носитель
37	**Свободное место на файловой системе закончилось!** 	**Причины:** Сообщение о заполнении файловой системы на 95%. Возможна аутентификация и идентификация АБ. **Порядок действий:** Выполнить аутентификацию и идентификацию АБ в системе и сохранить журнал на внешний носитель
38	**Способ аутентификации администратора был изменен** 	**Причины:** Предупреждающее сообщение об изменении типа аутентификации в политике аутентификации ***admin policy*** после применения шаблона политик безопасности **Порядок действий:** Обновить аутентификационные данные в соответствии с произведенными изменениями в политике ***admin policy*** до выхода из системы
39	**Блокировка доступа** 	**Причины:** Достижение максимально допустимого времени бездействия АБ при работе с консолью **Порядок действий:** Перезагрузить ЭВМ и осуществить аутентификацию и (или) идентификацию в консоли АБ

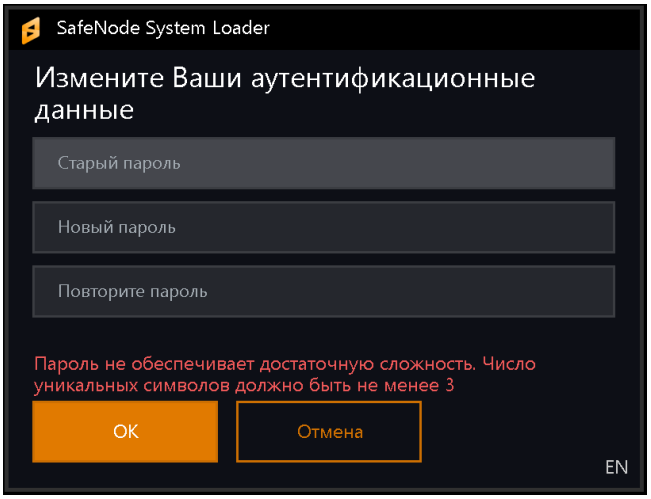
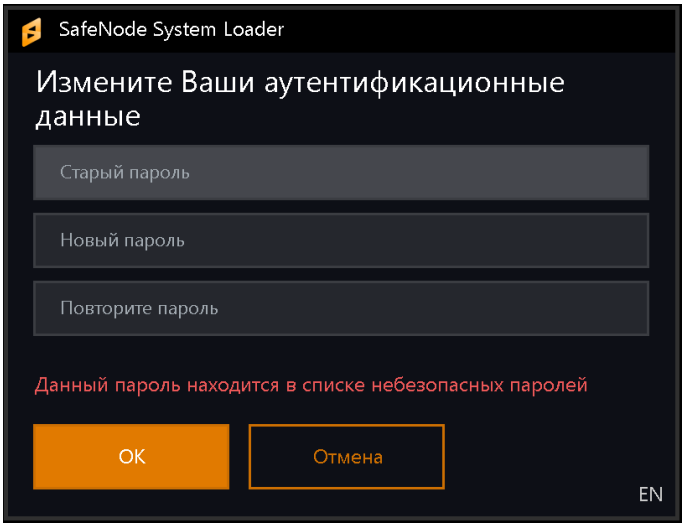
№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий АБ
40	**Ошибка. Указанный адрес недоступен** 	**Причины:** Неправильно указан адрес сервера LDAP или неверно сконфигурированы сетевые настройки ЭВМ **Порядок действий:** Проверить корректность указанных настроек в пункте меню ***«Параметры сети и LDAP»***
41	**Ошибка. Не найдено ни одной ОС для запуска. Будет загружена консоль СДЗ** 	**Причины:** На ЭВМ отсутствует установленная штатная ОС **Порядок действий:** Обратиться к АБ
42	**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
43	**Блокировка доступа. Количество попыток аутентификации и идентификации исчерпано**	**Причины:** Возникает при исчерпании всех попыток аутентификации пользователя

№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий АБ
		**Порядок действий:** 1. Выключить ЭВМ или перезагрузить ЭВМ и повторно выполнить процедуру идентификации и аутентификации. 2. При повторении ошибки обратиться к АБ.
44	**Временная блокировка пользователя на N минут** 	**Причины:** Достигнуто максимально разрешенное количество индивидуальных попыток аутентификации пользователя **Порядок действий:** Обратиться к АБ
45	**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

№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий АБ
		автоматически. 3. При установленной АБ защите от перевода времени, в системе обнаружен перевод времени назад, превышающий допустимый. **Порядок действий:** Обратиться к АБ
46	**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
47	**Слишком короткий пароль!** 	**Причины:** Новый пароль пользователя не удовлетворяет требованиям по минимальной длине пароля **Порядок действий:** Ввести пароль длиной не менее 8 символов

№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий АБ
48	**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
49	**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
50	**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

№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий АБ
51	**Отсутствует цифра** 	**Причины:** Новый пароль пользователя не удовлетворяет требованиям по сложности **Порядок действий:** Ввести новый пароль, который будет содержать хотя бы одну цифру
52	**Пароли не совпадают!** 	**Причины:** Несовпадение нового пароля и его подтверждения **Порядок действий:** Ввести верный новый пароль и его подтверждение
53	**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 АБ
		пользователя, отличный от текущего.
54	**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.
55	**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.

Приложение А

Перечень файлов ОС Windows 10 x64 версии 1909, рекомендуемых для установки на КЦ

№	Каталог	Файл
1	**…\Boot** или **…\EFI\Microsoft\Boot**	memtest.efi
2	**…\Windows**	explorer.exe
3	**…\Windows\System32**	audiodg.exe
4		autochk.exe
5		consent.exe
6		csrsrv.dll
7		dllhost.exe
8		dwm.exe
9		gdi32.dll
10		hal.dll
11		KernelBase.dll
12		LogonUI.exe
13		lsasrv.dll
14		lsass.exe
15		lsm.dll
16		ntdll.dll
17		ntoskrnl.exe
18		SearchIndexer.exe
19		services.exe
20		smss.exe
21		spoolsv.exe
22		svchost.exe
23		taskhostw.exe
24		user32.dll

25		userinit.exe
26		win32k.sys
27		wininit.exe
28		winlogon.exe
29	…\Windows\System32\drivers\	acpi.sys
30		afd.sys
31		atapi.sys
32		ataport.sys
33		bowser.sys
34		Classpnp.sys
35		cng.sys
36		csc.sys
37		dxgkrnl.sys
38		dxgmms1.sys
39		fileinfo.sys
40		fltMgr.sys
41		fvevol.sys
42		hdaudbus.sys
43		http.sys
44		i8042prt.sys
45		intelppm.sys
46		luafv.sys
47		mpsdrv.sys
48		msrpc.sys
49		ndis.sys
50		netbt.sys
51		netio.sys
52		nsiproxy.sys
53		ntfs.sys

54		nwifi.sys
55		partmgr.sys
56		pciide.sys
57		pciidex.sys
58		raspptp.sys
59		rdyboost.sys
60		serenum.sys
61		serial.sys
62		srv.sys
63		srv2.sys
64		tcpip.sys
65		tdi.sys
66		usbehci.sys
67		usbport.sys
68		volmgr.sys
69		volsnap.sys
70		vwififlt.sys
71		watchdog.sys
72		Wdf01000.sys

Приложение Б

Перечень файлов ОС Linux семейств Red Hat и Debian, рекомендуемых для установки на КЦ

№	Каталог	Файл
ОС Red Hat Enterprise Linux, Fedora, CentOS		
1	/boot	.vmlinuz-NNN.hmac
2		config-NNN
3		initramfs-NNN.img
4		initrd-NNN.img
5		Symvers-NNN.gz
6		System.map-NNN
7		tboot.gz
8		vmlinuz-NNN
9	/boot/efi/EFI/BOOT /EFI/BOOT	BOOTX64.EFI
10		fbx64.efi
11	/boot/efi/EFI/redhat /EFI/redhat	grub.efi
12	/lib/modules/NNN/	*
ОС Ubuntu		
13	/boot	abi-NNN
14		config-NNN
15		initrd.img-NNN
16		memtest86+.bin
17		memtest86+.elf
18		memtest86+_multiboot.bin
19		retpoline-NNN
20		System.map-NNN
21		vmlinuz-NNN
22	/boot/efi/EFI/BOOT /EFI/BOOT	bootx64.efi
23		grubx64.efi

24	/boot/efi/EFI/ubuntu /EFI/ubuntu	fwupx64.efi
25		grub.cfg
26		grubx64.efi
27		mmx64.efi
28		shimx64.efi
29	/boot/efi/EFI/ubuntu/fw /EFI/ubuntu/fw	
30	/boot/grub/[1]	*
31	/lib/modules/NNN/	*

Примечание 1. На КЦ устанавливаются все файлы, расположенные в указанной директории.

Приложение В

Список возможных кодов ошибок, выдаваемых АБ в сообщении ***«System blocked»***. Пример сообщения и порядок действий АБ по устранению приведен в таблице 15.1 (строка 2).

№	*Код ошибки*	*Описание ошибки*
		Общие ошибки
1	0x101	Неизвестная ошибка
2	0x102	Виртуальная память в системе закончилась
3	0x103	Файловая система находится в режиме «только чтение»
		Ошибки инициализации и установки
4	0x110	Раздел с главным модулем не найден и не найдена директория первичной загрузки
5	0x111	Ошибка проверки или создания директории установки
6	0x112	Ошибка в функции записи NVRAM переменной
7	0x113	Файл контроля исполнения кода не найден
8	0x114	Ошибка установки настроек в драйвере контроля исполнения кода
		Ошибки проверки цифровых подписей
9	0x120	Хеш-сумма модуля проверки ЭЦП неверна
10	0x121	Файл БД ЭЦП не найден
11	0x122	Неправильная структура каталога директории установки, обнаружены лишние файлы
12	0x123000	Неправильная структура каталога директории установки, обнаружены недостающие файлы. Последние два числа в коде ошибки указывают на номер удаленного файла согласно БД ЭЦП
13	0x124000	Ошибка проверки цифровой подписи файла. Последние два числа в коде ошибки указывают на номер некорректного файла согласно расположению в директории
		Ошибки БД
14	0x130	Основная БД повреждена или некорректный ключ преобразования
15	0x131	Журнал поврежден или некорректный ключ преобразования
16	0x132	БД АНП повреждена или некорректный ключ преобразования
17	0x133	Основной БД нет или она пустая
18	0x134	БД журнала нет или она пустая

19	0x135	БД АНП нет или она пустая
20	0x136	Некорректный запрос в БД
21	0x137	Некорректный запрос в БД журнала
22	0x138	Некорректный запрос в БД АНП
Ошибки ключей подписи и преобразования		
23	0x140	Открытый ключ проверки ЭЦП не найден в хранилище
24	0x141	Ключ преобразования не найден в хранилище
25	0x142	Переменная с хеш-суммой драйвера проверки ЭЦП не найдена в хранилище
26	0x143	Переменная с информацией об установочном режиме не найдена
27	0x144	Ключ журнала аудита не найден
28	0x145	Открытый ключ проверки ЭЦП не найден в директории хранения модулей BIOS при восстановлении модулей
29	0x146	Переменная с хеш-суммой драйвера проверки ЭЦП не найдена в директории хранения модулей BIOS при восстановлении модулей
30	0x147	Невозможно создать файл install_config.txt в директории инсталлятора для EFI модулей при восстановлении модулей
31	0x148	Модуль для установки изделия на ЭВМ не найден в директории инсталлятора для EFI модулей при восстановлении модулей
Ошибки однократного входа в BIOS		
32	0x170	Протокол однократного входа в BIOS не найден
33	0x171	Ошибка открытия однократного входа в BIOS
Ошибки загрузки модулей		
34	0x180	Ошибка загрузки модуля проверки ЭЦП
35	0x181	Ошибка загрузки модуля контроля исполнения кода
36	0x182	Ошибка загрузки модуля работы с АНП
Активация		
37	0x200	Не удалось создать уникальный идентификатор платформы
38	0x210	Открытый ключ не найден при восстановлении ключей
39	0x211	Переменная с хеш-суммой драйвера проверки ЭЦП не найдена при восстановлении ключей
40	0x212	Ошибка генерации секретного ключа при восстановлении ключей

Перечень сокращений

ACPI	–	Advanced Configuration and Power Interface (усовершенствованный интерфейс управления конфигурацией и питанием)
AD	–	Active Directory (службы каталогов корпорации Microsoft для операционных систем семейства Windows Server)
BIOS	–	Basic Input Output System (базовая система ввода-вывода)
EXT3, EXT4	–	Extended File System (расширенная файловая система)
FAT32	–	File Allocation Table (таблица размещения файлов)
GPT	–	GUID Partition Table (таблица разделов GUID, часть спецификации UEFI)
GRUB	–	Grand Unified Bootloader (загрузчик операционной системы от проекта GNU)
LDAP	–	Lightweight Directory Access Protocol (протокол прикладного уровня для доступа к службе каталогов X.500)
LILO	–	LInux Loader (стандартный загрузчик для Linux и BSD-систем)
LSB	–	Linux Standard Base (совместный проект семейства операционных систем, основанных на Linux)
MAC	–	Media Access Control (управление доступом к среде)
MBR	–	Master Boot Record (главная загрузочная запись)
MD4, MD5	–	Message Digest 4, Message Digest 5, (алгоритмы криптографического хэширования)
NTFS	–	New Technology File System (файловая система новой технологии)
PIN	–	Personal Identification Number (личный идентификационный номер)
PKI	–	Public Key Infrastructure (инфраструктура открытых ключей)
SHA1	–	Secure Hash Algorithm 1 (алгоритм криптографического хэширования)
SMBIOS	–	System Management BIOS (системное управление BIOS)
TLS	–	Transport Layer Security (протокол защиты транспортного уровня)

UDF	–	Universal Disk Format (универсальный дисковый формат)
UEFI	–	Unified Extensible Firmware Interface
URI	–	Uniform Resource Identifier (унифицированный идентификатор ресурса)
USB	–	Universal Serial Bus
АБ	–	Администратор безопасности
АРМ	–	Автоматизированное рабочее место
АНП	–	Аутентификационный носитель пользователя
БД	–	База данных
ГОСТ	–	Государственный стандарт
ДСЧ	–	Датчик случайных чисел
ИАФ	–	Идентификация и аутентификация
КИ	–	Конфиденциальная информация
КЦ	–	Контроль целостности
ОС	–	Операционная система
ПО	–	Программное обеспечение
С	–	Секретно
СДЗ	–	Средство доверенной загрузки
ФС	–	Файловая система
ФСТЭК	–	Федеральная служба по техническому и экспортному контролю Российской Федерации
ЭВМ	–	Электронно-вычислительная машина
ЭД	–	Эксплуатационная документация
ЭЦП	–	Электронная цифровая подпись