ГАЗИНФОРМ СЕРВИС

Средство доверенной загрузки «SafeNode System Loader»

Руководство по эксплуатации
Часть 3

Руководство администратора Linux/Windows

Санкт-Петербург, 2024

Содержание

Введение

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

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 указаниям документа «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 1. Руководство по установке. ГМТК.468269.060РЭ1».

Описание управления параметрами изделия из псевдографической консоли СДЗ в среде UEFI BIOS приведено в документе «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 2. Руководство администратора. ГМТК.468269.060РЭ2».

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».

Расположенные на полях руководства знаки указывают на примечания.

Степени важности примечаний:

Важная информация, информация предостерегающего характера.

Дополнительная информация, примеры.

1 Варианты исполнения консоли управления параметрами изделия

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

1.2 Запуск графического интерфейса в ОС Linux и ОС Windows возможен только после предварительной установки изделия и настройки всех параметров, необходимых для функционирования изделия, в том числе обязательного создания политики аутентификации АБ и его учетной записи.

1.3 Порядок действий АБ по настройке и управлению параметрами изделия описан в документе «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 2. Руководство администратора. ГМТК.468269.060РЭ2».

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

- **псевдографическая консоль СДЗ**, исполняемая в среде **UEFI BIOS** (рисунок 1.1) и запускаемая по требованию АБ. Доступна АБ только после успешного прохождения их процедуры аутентификации и идентификации после включения питания электронно-вычислительной машины (ЭВМ) и старте программного обеспечения (ПО) изделия. Дополнительно доступна загрузка **графической аварийной консоли СДЗ** (**аварийная консоль АБ**) (рисунок 1.2);
- **графическая консоль СДЗ**, запускаемая по требованию АБ из среды ОС **Windows** (рисунок 1.3) 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.
- **графическая консоль СДЗ Linux** (**консоль АБ Linux**, рисунок 1.4), 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.

1.5 База данных (БД) изделия является единой для всех консолей управления СДЗ.

1.6 Графические консоли СДЗ для ОС Linux и ОС Windows имеют схожие интерфейсы, однако при этом имеются различия при настройке параметров. В таблице 1.1 приведены отличия в настройке параметров СДЗ для всех вариантов

исполнения консолей управления СДЗ.

1.7 Данное руководство описывает графическую консоль при работе в ОС Windows. При работе с графической консолью в ОС Linux следует также использовать данное руководство и таблицу 1.1 настоящего документа.

Рисунок 1.1 – Интерфейс консоли АБ в среде UEFI BIOS

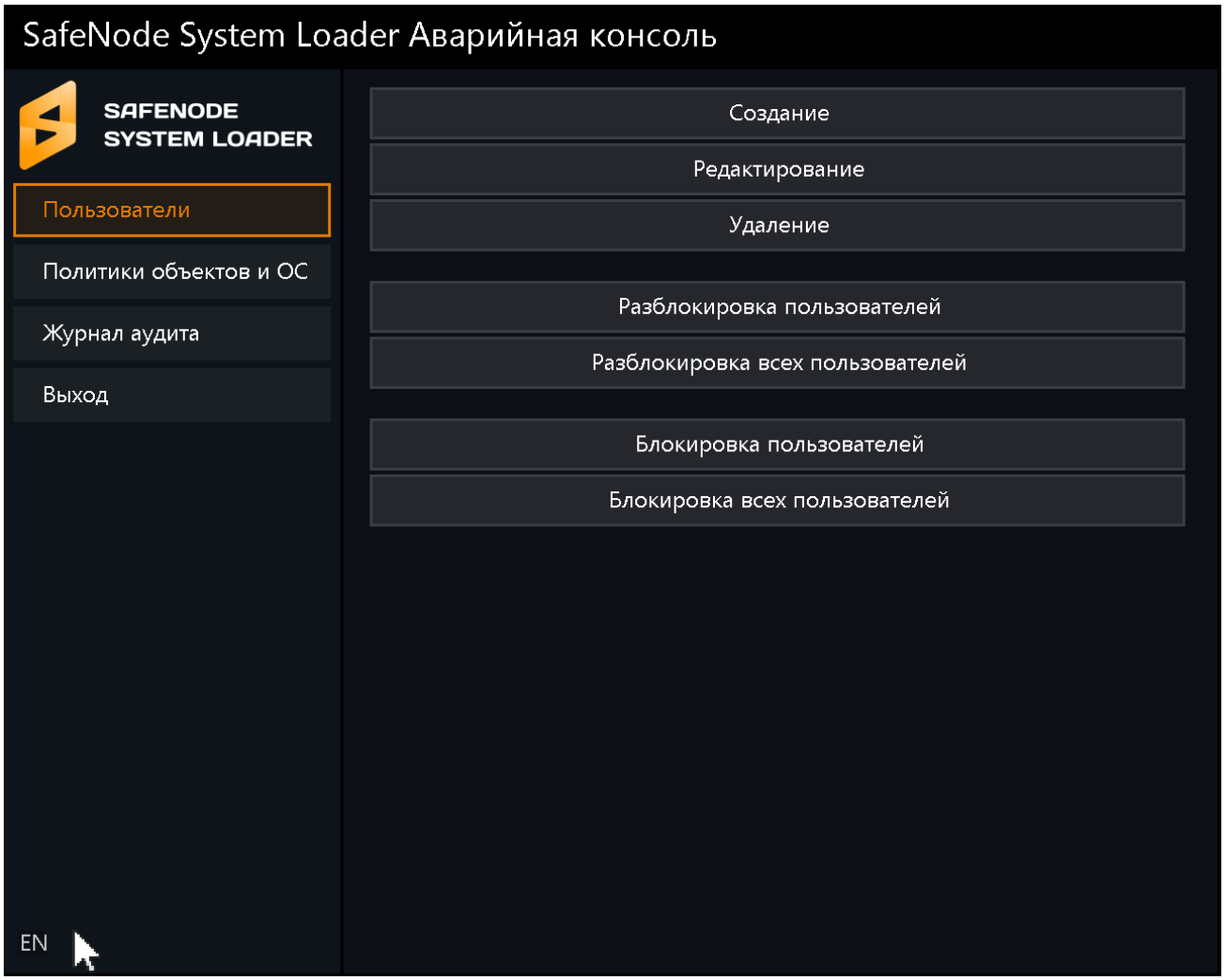


Рисунок 1.2 – Аварийная консоль АБ

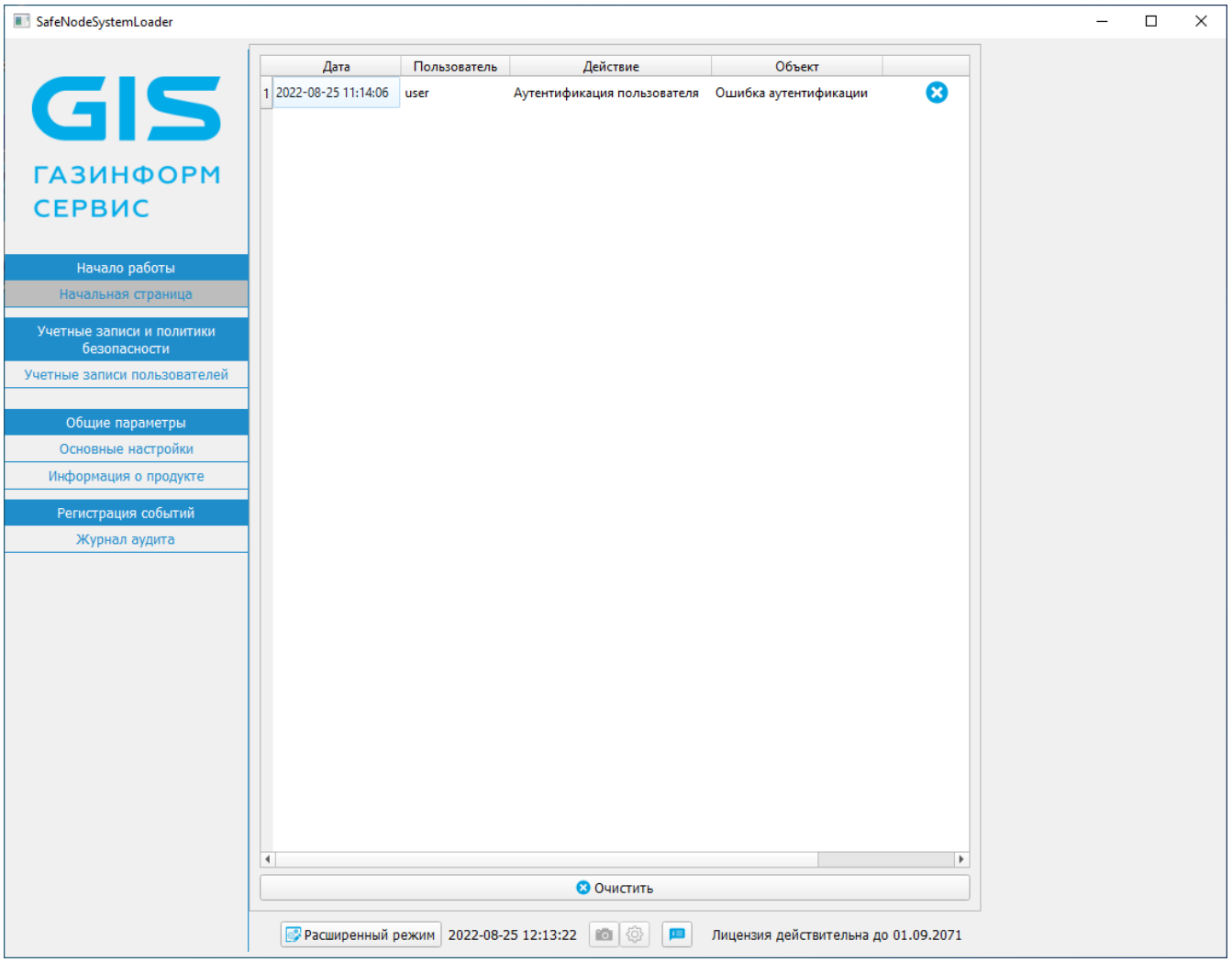


Рисунок 1.3 – Интерфейс консоли АБ в ОС Windows

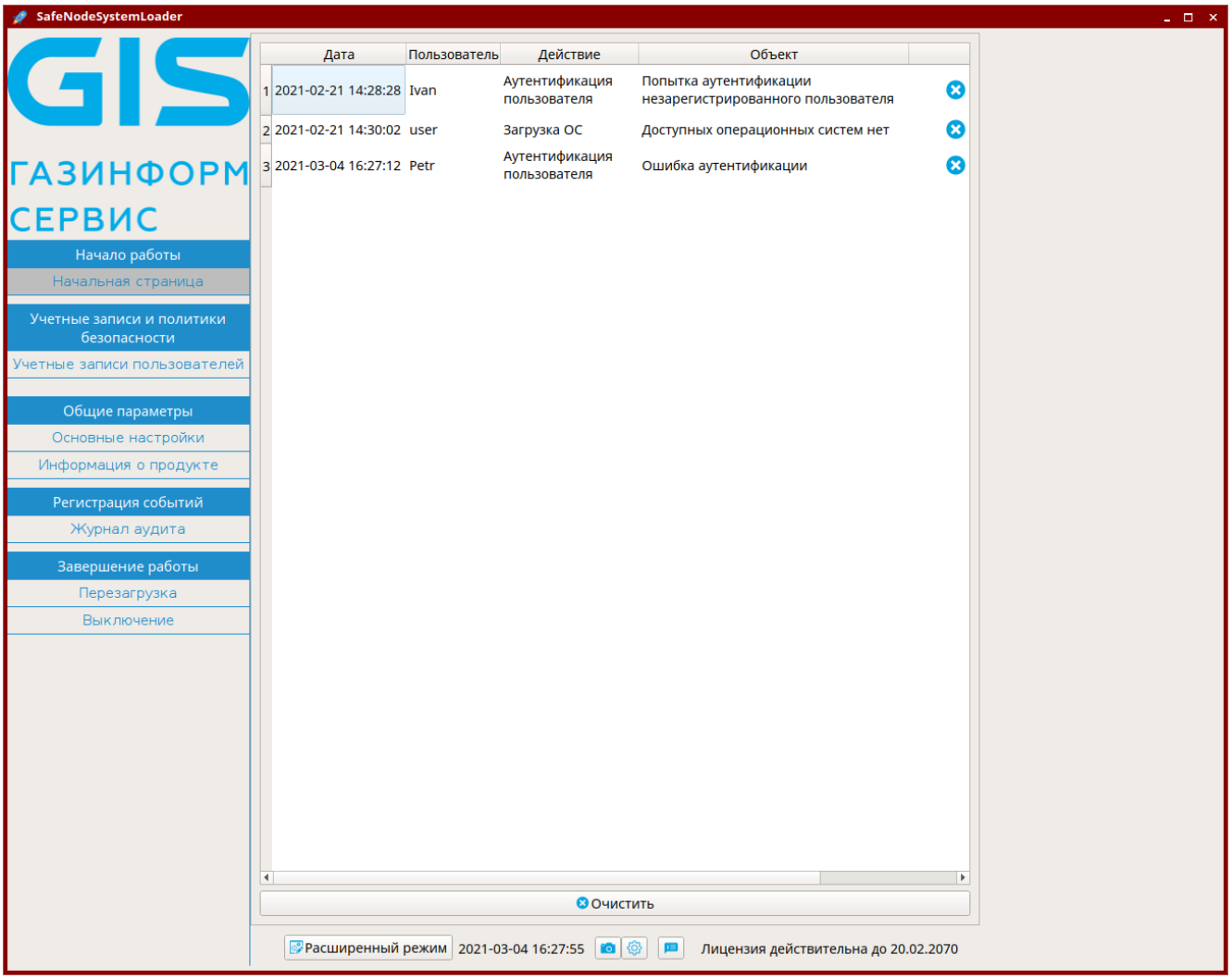


Рисунок 1.4 – Интерфейс консоли АБ в ОС Linux

Таблица 1.1 – Отличия в настройке параметров изделия из различных вариантов исполнения консоли АБ

№ п/п.	Наименование параметра	UEFI	Linux	Windows	Примечание
Раздел «Учетные записи и политики безопасности»					
Подраздел «Учетные записи пользователей»					
1	Разблокировка пользователей	+	+	+	
2	Разблокировка всех пользователей	+	–	–	В консоли Windows/Linux отсутствует
3	Блокировка пользователей	+	–	–	В консоли Windows/Linux отсутствует
4	Блокировка всех пользователей	+	–	–	В консоли Windows/Linux отсутствует

№ п/п.	Наименование параметра	UEFI	Linux	Windows	Примечание
Подраздел «Политики аутентификации пользователей»					
5	Блокировать создание популярных паролей	–	+	+	В консоли АБ UEFI отсутствует
Подраздел «Политики контроля целостности и загрузки ОС»					
6	Проверка целостности объектов	+	–	–	В консоли АБ Windows/Linux отсутствует
7	Пересчет контрольных сумм объектов	+	–	–	В консоли АБ Windows/Linux отсутствует
Подраздел «Политика контроля целостности и загрузки ОС»					
8	Применить шаблон	+	+	+	Создание шаблона политик возможно только в консоли АБ Windows/Linux
Раздел «Общие параметры»					
Подраздел «Основные настройки»					
Пункт «Параметры сети и LDAP»					
9	Редактирование файла hosts	–	+	+	В консоли АБ UEFI отсутствует
10	Редактирование файла krb5.conf	–	+	+	В консоли АБ UEFI отсутствует
11	Редактирование файла ldap.conf	–	+	+	В консоли АБ UEFI отсутствует
12	Редактирование файла root.cer	–	+	+	В консоли АБ UEFI отсутствует
13	Проверить доступность сервера LDAP или Kerberos	+	–	–	В консоли АБ Windows/Linux отсутствует
Пункт «Настройки времени»					
14	Дата	+	–	–	В консоли АБ Windows/Linux отсутствует
15	Время	+	–	–	В консоли АБ Windows/Linux отсутствует
16	Часовой пояс	+	–	–	В консоли АБ Windows/Linux отсутствует
17	Адрес NTP сервера	+	–	–	В консоли АБ Windows/Linux

№ п/п.	Наименование параметра	UEFI	Linux	Windows	Примечание
					отсутствует
18	Синхронизировать время автоматически	+	–	–	В консоли АБ Windows/Linux отсутствует
Пункт «Прочие параметры»					
19	Режим отображения основного меню	+	–	–	В консоли АБ Windows/Linux управляется отдельной кнопкой внизу окна
20	Реактивация лицензии	–	+	+	В консоли АБ UEFI отсутствует
Пункт «Настройки идентификатора»					
21	Кнопка обновления списка АНП	–	+	+	В консоли АБ отсутствует
22	Поле выбора АНП	–	+	+	
23	Смена PIN-кода	–	+	+	
24	Пароль восстановления	–	+	+	Смена пароля восстановления доступна в консоли АБ UEFI при редактировании учетной записи АБ
25	Кнопка 	–	+	+	
26	Кнопка «Установить»	–	+	+	
27	Подключить устройства	–	+	–	В консоли АБ UEFI/Windows отсутствует
28	Журнал объекта	–	+	+	В консоли АБ UEFI отсутствует
29	Создание шаблона	–	+	+	В консоли АБ UEFI отсутствует
30	Оптимизация базы данных	+	–	–	В консоли АБ Windows/Linux отсутствует
31	Обновить системное ПО	+	–	–	В консоли АБ Windows/Linux отсутствует
32	Мягкий режим	+	+	+	
33	Разрешить однократный вход в BIOS	+	–	–	В консоли АБ Windows/Linux отсутствует
34	Удалить СДЗ	+	–	–	В консоли АБ Windows/Linux отсутствует
Подраздел «Диагностика»					
35	Проверка целостности модулей	+	–	–	В консоли АБ Windows/Linux отсутствует

№ п/п.	Наименование параметра	UEFI	Linux	Windows	Примечание
36	Проверка целостности оперативной памяти	+	–	–	В консоли АБ Windows/Linux отсутствует
37	Проверка памяти при загрузке системы	+	–	–	В консоли АБ Windows/Linux отсутствует
38	Тип блокировки	+	–	–	В консоли АБ Windows/Linux отсутствует
Подраздел «Информация о продукте»					
39	Цифровые подписи ПО	–	+	+	В консоли АБ UEFI отсутствует

1.8 Переключение языка ввода (английский/русский) в консоли АБ осуществляется следующим образом:

- в консоли АБ Linux с помощью сочетания клавиш **< *Alt* >** + **< *Shift* >**, при переключении на русский язык ввода на клавиатуре включается индикация клавиши ***Scroll Lock***;

- в консоли АБ Windows с помощью сочетания клавиш языковой панели, установленных в настройках ОС Windows, или с помощью языковой панели для переключения раскладки клавиатуры.

2 Запуск графического интерфейса консоли АБ в ОС Linux

2.1 Для запуска графического интерфейса консоли АБ в ОС Linux необходимо предварительно произвести установку в соответствии с документом «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 1. Руководство по установке. ГМТК.468269.060РЭ1».

2.2 Графическая консоль после установки располагается по пути **/usr/share/sdz/bin/**.

2.3 Для запуска консоли АБ необходимо открыть терминал и запустить файл на исполнение. На рисунке 2.1 приведен пример запуска консоли с использованием терминала в ОС Astra Linux 1.6.

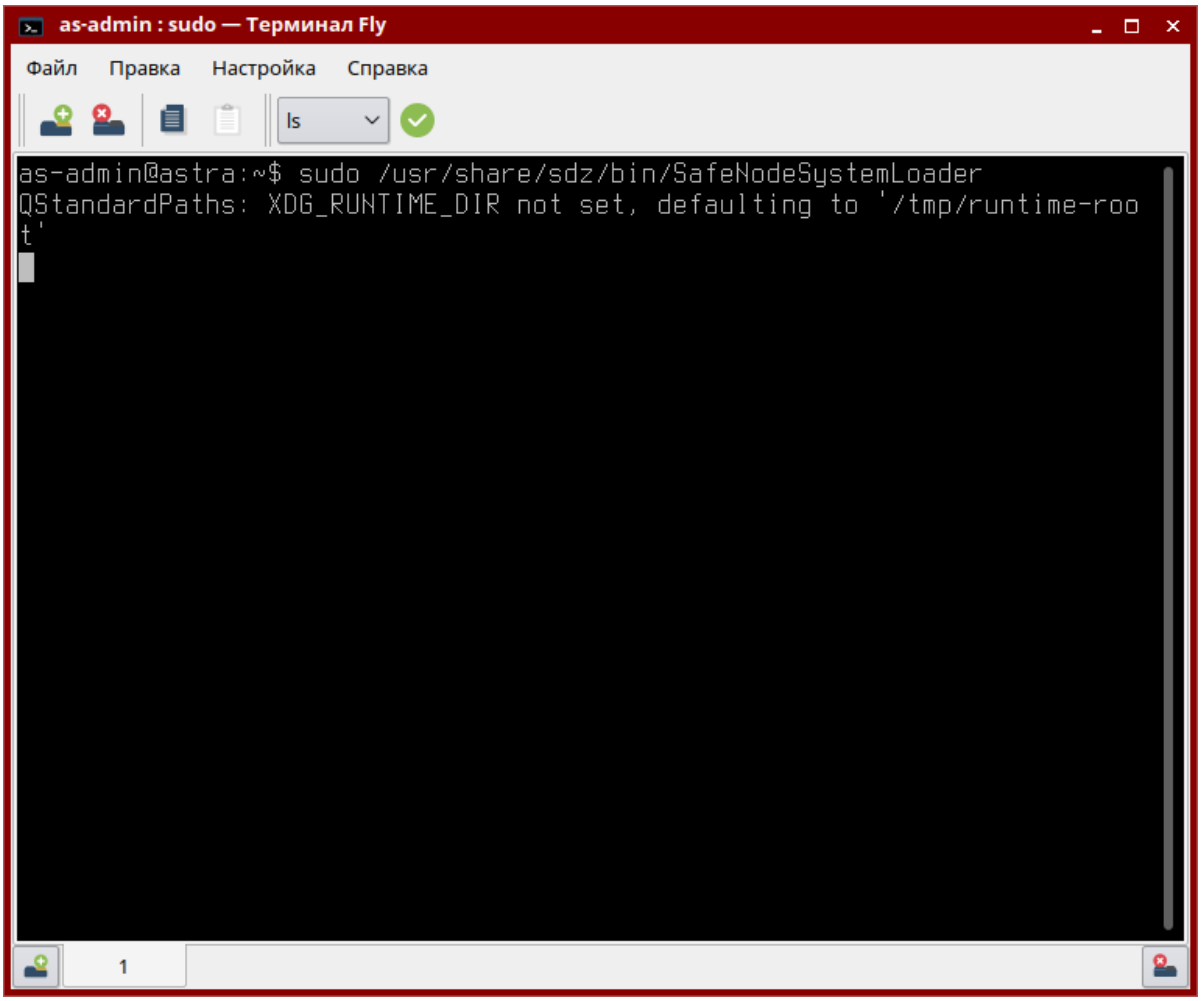


Рисунок 2.1 – Запуск консоли АБ в ОС Linux

2.4 При успешной загрузке ПО изделия на экране ЭВМ появится окно графического интерфейса изделия с приглашением к идентификации и аутентификации АБ (рисунок 2.2).

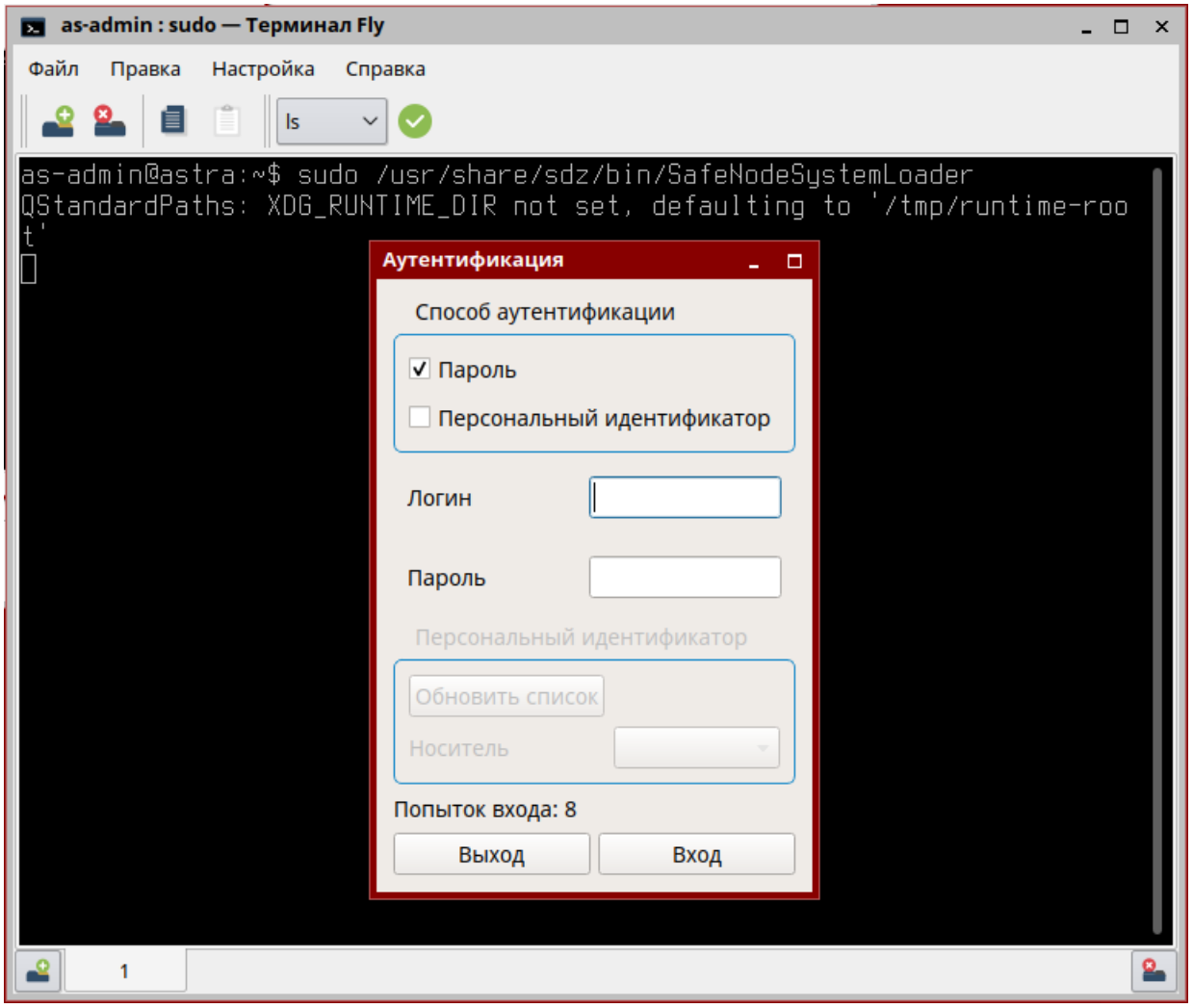


Рисунок 2.2 – Диалоговое окно для ввода аутентификационных данных

2.5 После корректного указания аутентификационных данных АБ на экране ЭВМ появится окно консоли АБ в ОС Linux (рисунок 1.4).

3 Запуск графического интерфейса консоли АБ в ОС Windows

Для запуска графического интерфейса консоли АБ в ОС Windows необходимо осуществить аутентификацию в ОС Windows под учетной записью, имеющей административные права (состоящей в локальной группе «Администраторы»).

3.1 Запуск графического интерфейса консоли АБ в ОС Windows осуществляется после загрузки ОС Windows с помощью запуска на выполнение файла ***SafeNodeSystemLoader.exe***.

3.2 При успешной загрузке ПО изделия на экране ЭВМ появится окно для ввода аутентификационных данных АБ (рисунок 3.1).

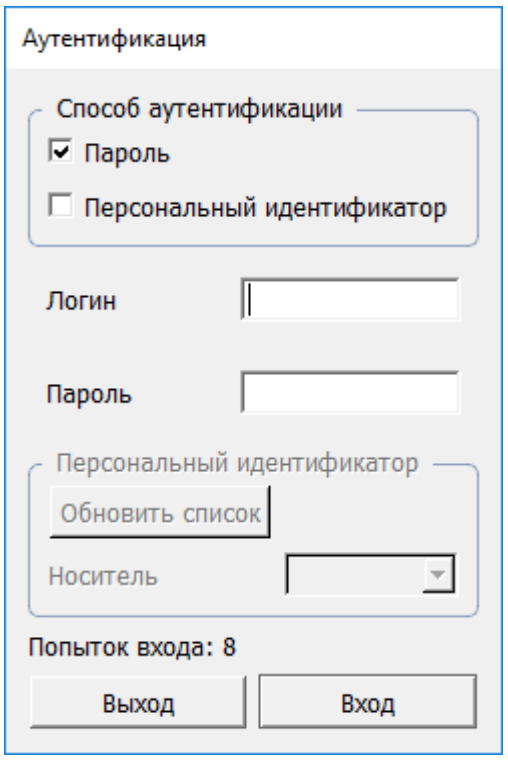


Рисунок 3.1 – Аутентификация для приложения ***SafeNodeSystemLoader***

3.3 В окне аутентификации АБ необходимо ввести идентификационные и аутентификационные данные, указанные при первичной настройке изделия в консоли АБ в соответствии с политикой аутентификации, назначенной АБ.

3.4 В случае, если после установки изделия на ЭВМ была загружена ОС без

первичной настройки изделия (см. раздел 3 документа «Средство доверенной загрузки «SafeNode System Loader». Часть 2. Руководство администратора. ГМТК.468269.060РЭ2»), после запуска графического интерфейса консоли Windows необходимо указать аутентификационные данные АБ, установленные по умолчанию:

- имя учетной записи пользователя – ***admin***;
- пароль – ***12345678***.

В целях обеспечения безопасности после первой успешной аутентификации АБ осуществляется принудительная смена пароля, используемого по умолчанию.

3.5 После успешной процедуры аутентификации и идентификации АБ появится диалоговое окно для принудительной смены его пароля (рисунок 3.2).

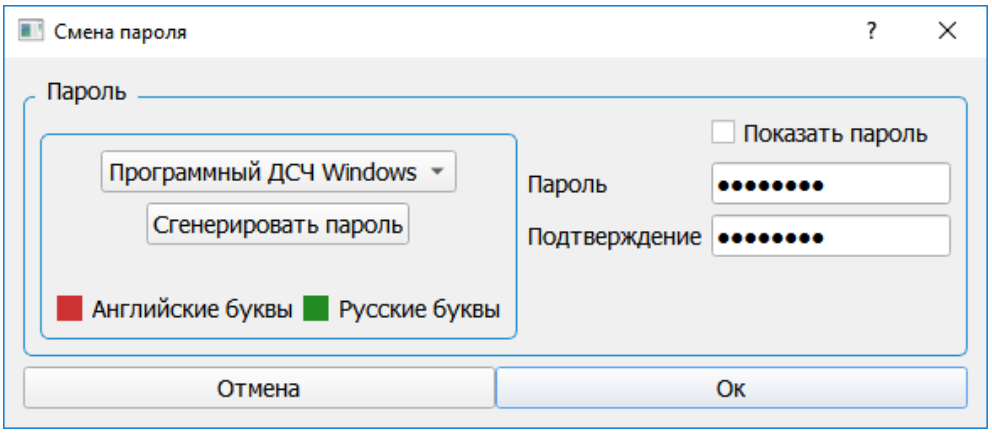


Рисунок 3.2 – Принудительная смена пароля АБ, установленного по умолчанию

3.6 Для смены пароля АБ необходимо в окне (см. рисунок 3.2) указать новый пароль и его подтверждение. Новый пароль должен удовлетворять минимальным требованиям к сложности: содержать хотя бы одну строчную букву и иметь минимальную длину в 8 символов. В случае несоблюдения установленных требований появится соответствующее информационное сообщение.

3.7 При выполнении всех заданных требований к качеству пароля произойдет его смена и появится информационное сообщение (рисунок 3.3).

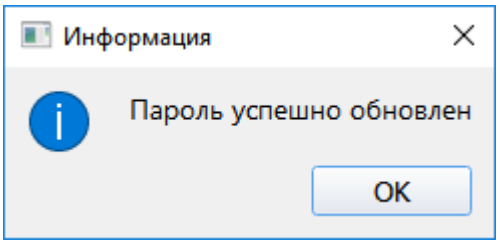


Рисунок 3.3 – Успешное изменение пароля

3.8 После успешного прохождения процедуры идентификации и аутентификации АБ доступен графический интерфейс консоли АБ Windows (рисунок 1.2).

3.9 Доступ к консоли АБ Windows блокируется через заданное в настройках время неактивности АБ (таблица 10.1), при этом на экране появляется окно аутентификации АБ (рисунок 3.1). Для возобновления работы в консоли АБ Windows необходимо заново ввести идентификационные и аутентификационные данные АБ.

3.10 При исчерпании количества попыток аутентификации и идентификации АБ на экране ЭВМ появится окно, представленное на рисунке 3.4.

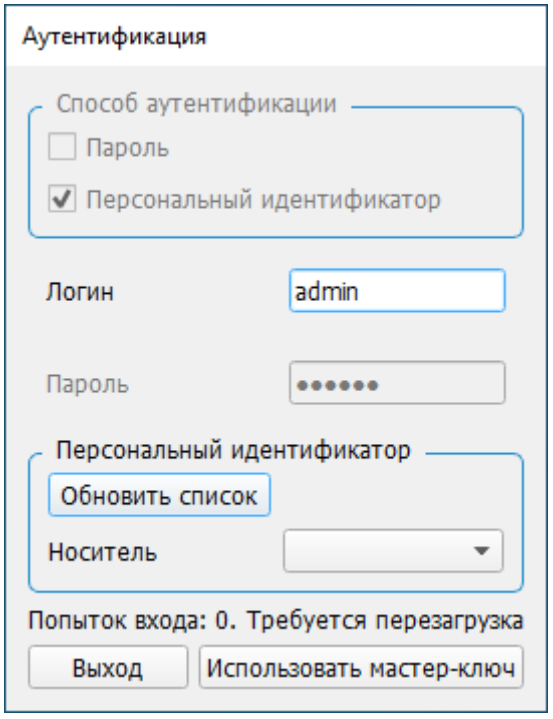


Рисунок 3.4 – Исчерпание попыток аутентификации и идентификации

3.11 Для дальнейшей работы необходимо перезагрузить ЭВМ и повторно осуществить запуск графического интерфейса консоли АБ в ОС Windows. В окне для ввода аутентификационных данных (рисунок 3.1) указать корректные данные для прохождения процедуры аутентификации идентификации АБ.

3.12 В случае утраты пароля АБ, PIN-кода администратора АНП или потери АНП,

используется мастер-ключ для сброса аутентификационных данных АБ до значений по умолчанию. Назначение мастер-ключа администратору безопасности рассмотрено в подразделе 9.3 документа.

3.13 Для восстановления доступа с помощью мастер-ключа необходимо:

- подключить мастер-ключ АБ к ЭВМ;
- в диалоговом окне аутентификации в разделе ***Персональный идентификатор*** воспользоваться кнопкой ***«Обновить список»*** (рисунок 3.5), затем нажать кнопку ***«Использовать мастер ключ»***;

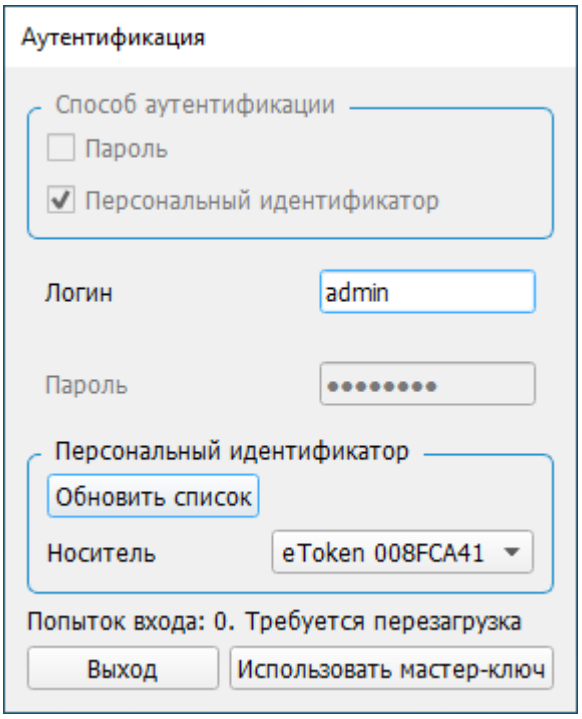


Рисунок 3.5 – Отображение мастер-ключа в списке

- в появившемся информационном окне с предупреждением о сбросе аутентификационных данных АБ к значению по умолчанию нажать ***«Да»*** (рисунок 3.6);

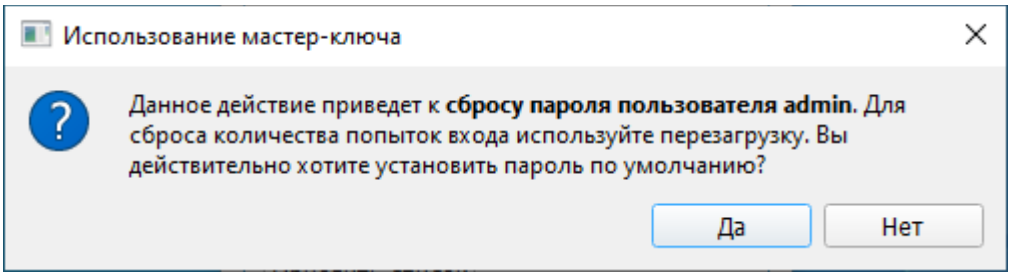


Рисунок 3.6 – Предупреждение о сбросе аутентификационных данных АБ

- ввести PIN-код мастер-ключа (рисунок 3.7);

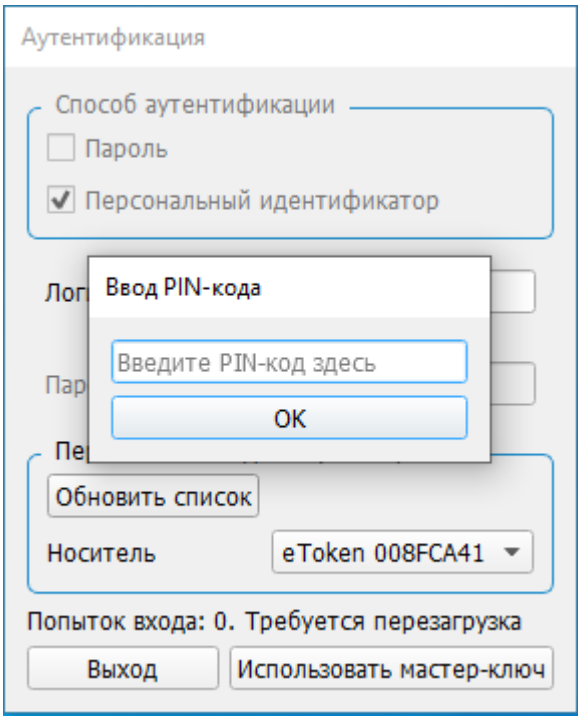


Рисунок 3.7 – Ввод PIN-кода АНП

3.14 При успешном сбросе аутентификационных данных АБ будет выведено сообщение (рисунок 3.8).

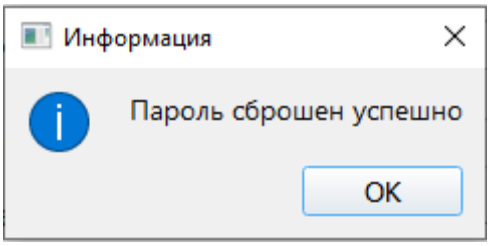


Рисунок 3.8 – Успешный сброс аутентификационных данных АБ

3.15 Для выхода из мягкого режима функционирования СДЗ 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»

3.16 Для смены пароля восстановления необходимо:

- перейти в раздел ***Основные настройки → Настройки идентификатора*** (рисунок 3.9);

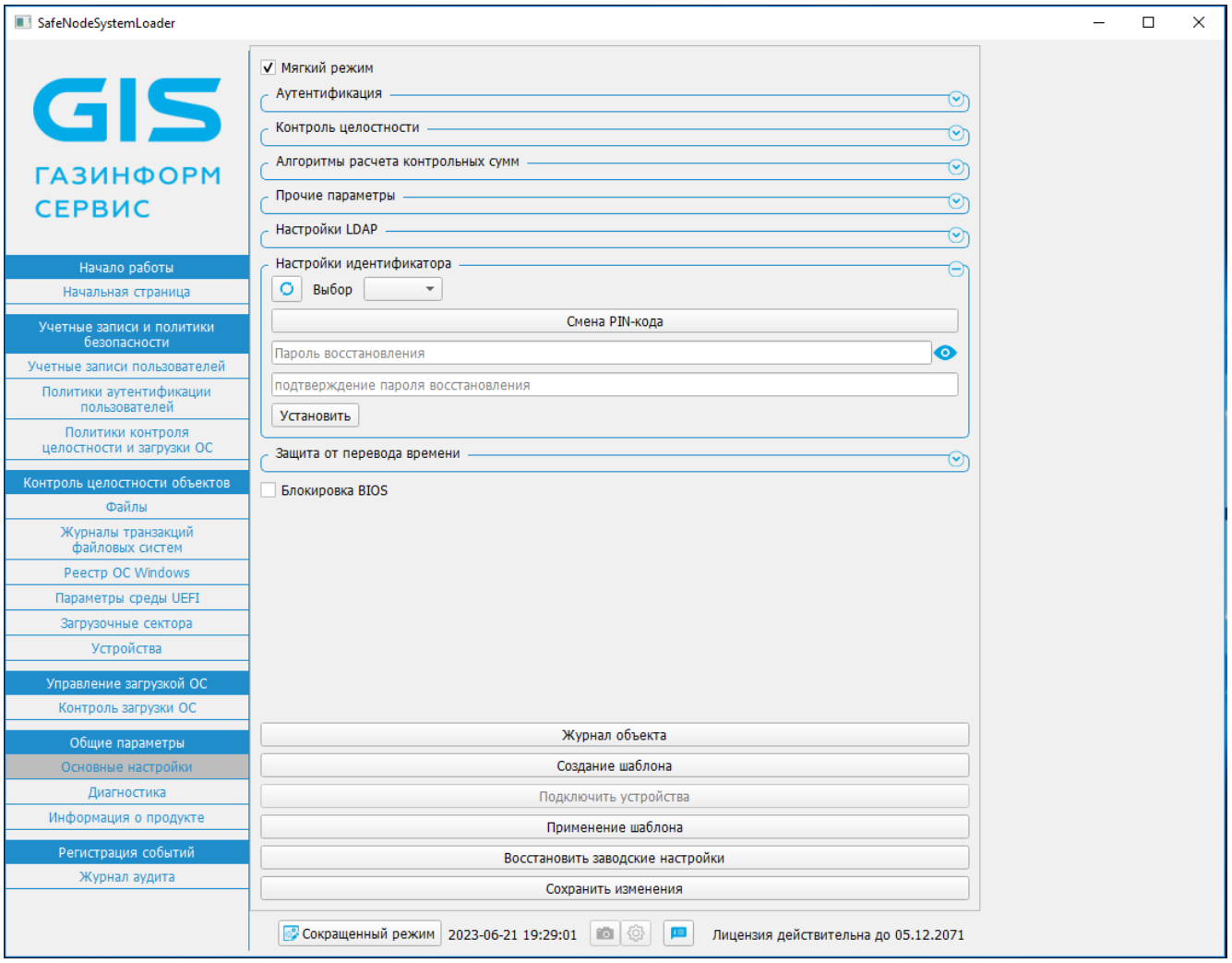


Рисунок 3.9 – Раздел ***Основные настройки***

- указать новое значение в поле ***«Пароль восстановления»***;
- подтвердить указанное значение в поле ***«Подтверждение пароля восстановления»*** и затем нажать кнопку ***«Установить»***;
- появится информационное сообщение с предложением подключить мастер-ключ администратора (рисунок 3.10).

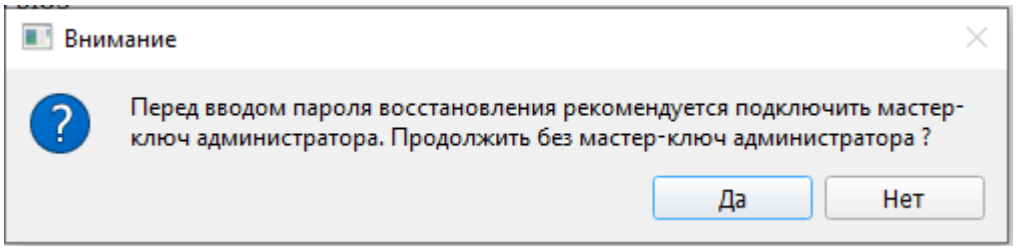


Рисунок 3.10 – Информационное сообщение

Использование мастер-ключа администратора рекомендуется для резервного сохранения пароля восстановления.

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

3.17 Для резервного копирования значения пароля восстановления на мастер-ключ администратора следует выбрать ***«Нет»*** и затем:

- подключить мастер-ключ АБ к ЭВМ;
- в диалоговом окне (рисунок 3.9) в разделе ***Настройки идентификатора*** воспользоваться кнопкой ***«Обновить список»*** и выбрать из выпадающего списка мастер-ключ АБ для хранения пароля восстановления;
- в появившемся диалоговом окне указать PIN-код мастер-ключа АБ;
- затем указать новое значение в поле ***«Пароль восстановления»***, подтвердить введенное значение и затем нажать кнопку ***«Установить»***.

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.

3.18 При успешной установке пароля восстановления будет выведено сообщение (рисунок 3.11).

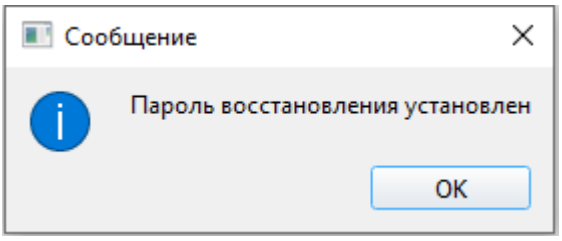


Рисунок 3.11 – Успешная установка пароля восстановления

3.19 Для смены значения пароля восстановления без резервного копирования на мастер-ключ АБ необходимо после указания нового значения пароля в появившемся диалоговом окне (рисунок 3.10) выбрать ***«Да»***, затем будет выведено сообщение об успешной установке пароля (рисунок 3.11).

3.20 В случае, если пароль восстановления не был сменен, то при первом выходе из мягкого режима будет выведено сообщение (рисунок 3.12).

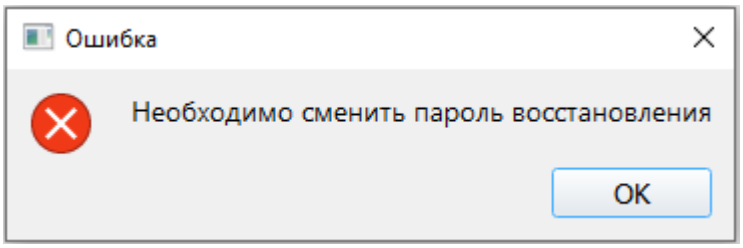


Рисунок 3.12 – Сообщение о необходимости сменить пароль восстановления

4 Описание основного окна консоли АБ Windows

4.1 Начальная страница. Сигнализация о нарушениях

4.1.1 После аутентификации АБ доступна начальная страница консоли АБ Windows, содержащая список ошибочных действий пользователя, зафиксированных при работе пользователя с изделием (рисунок 4.1).

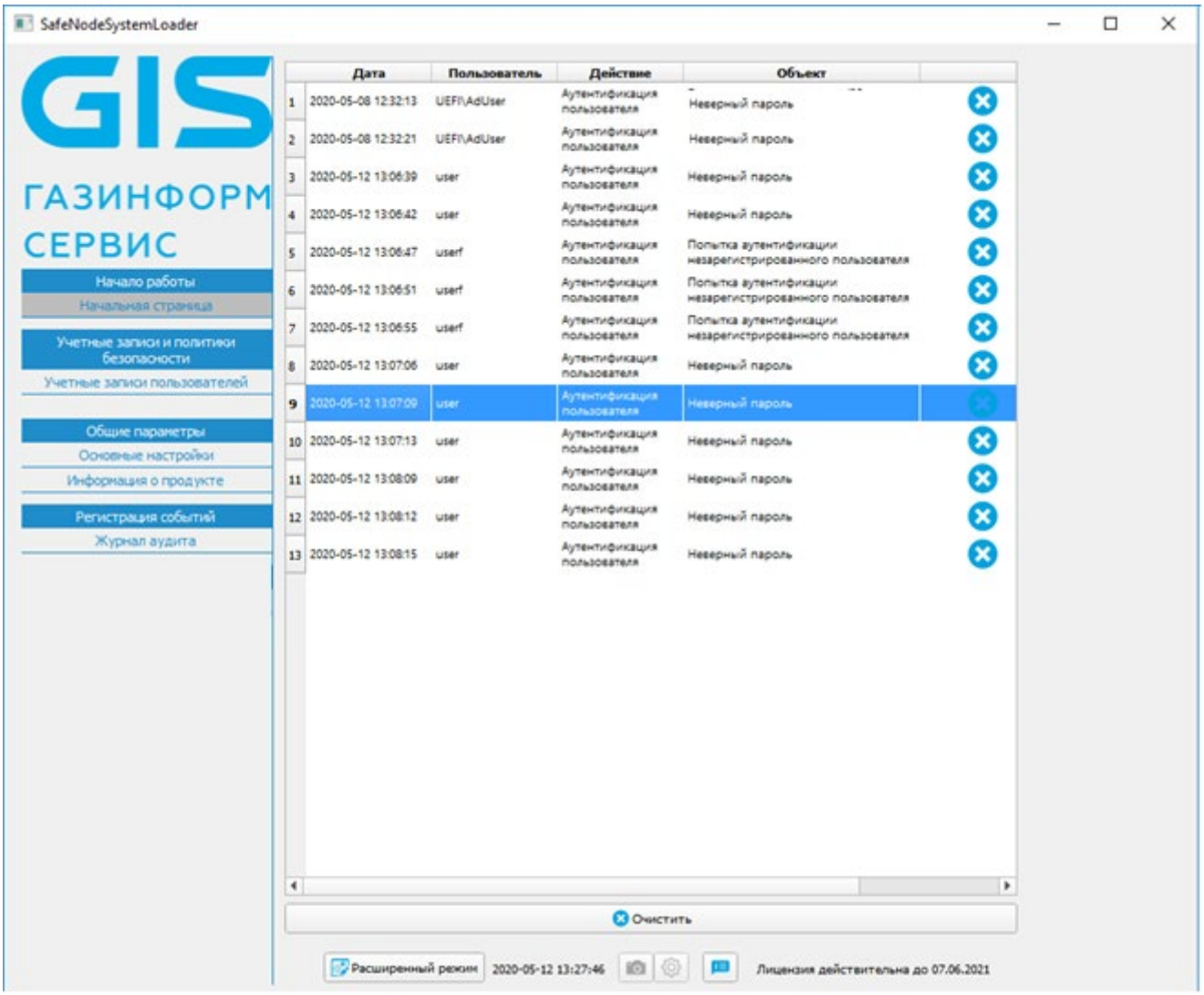


Рисунок 4.1 – Начальная страница консоли АБ Windows

4.1.2 Список ошибочных событий, зафиксированных в журнале аудита, хранится в БД изделия в качестве событий, на которые АБ не отреагировал, и будет выводиться при каждом аутентификации и (или) идентификации в консоль АБ Windows до момента очистки списка по кнопке ***«Очистить»*** (рисунок 4.1).

4.1.3 Список всех событий, зафиксированных в журнале аудита, приведен в таблице 11.1.

4.2 Описание основного окна консоли АБ Windows

4.2.1 Основное окно консоли АБ Windows доступно только АБ после успешного прохождения им процедуры аутентификации и идентификации (рисунок 4.2).

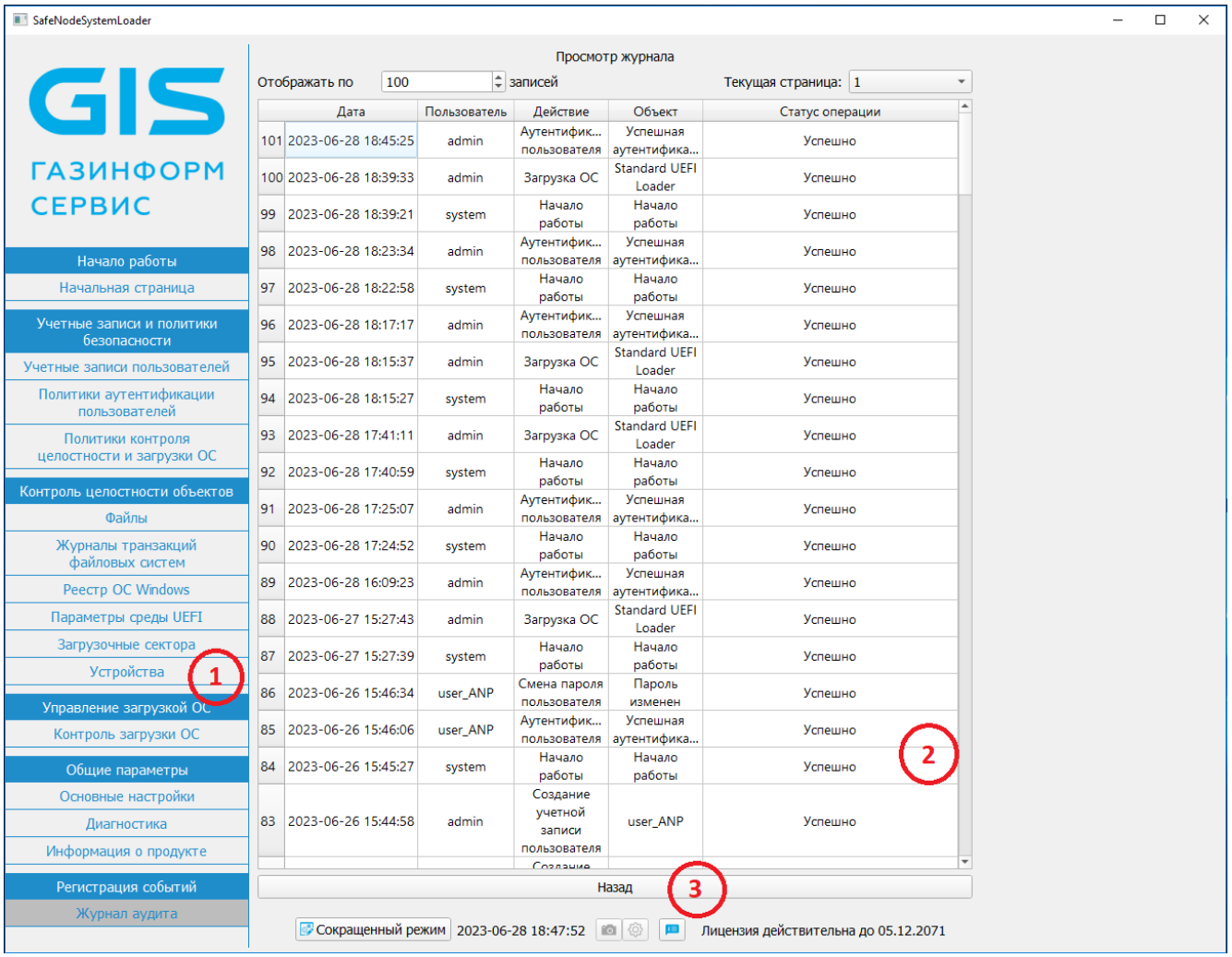


Рисунок 4.2 – Основное окно графического интерфейса консоли ОС Windows

4.2.2 На рисунке 4.2 цифрами в кругах обозначены:

- поле 1 – основное меню консоли АБ Windows;
- поле 2 – отображение содержания пунктов меню для просмотра и редактирования параметров;
- поле 3 – располагаются кнопки для смены текущего режима отображения, снимка экрана и сохранения в выбранную директорию, поле с текущей датой и временем (рисунок 4.2).

Рисунок 4.3 – Нижнее поле консоли АБ Linux

4.2.3 Кнопка  предназначена для сохранения снимка экрана в предварительно созданную директорию (только для консоли АБ Linux).

4.2.4 Кнопка  предназначена для настройки времени задержки создания снимка в интервале 0 … 60 секунд, выбор директории для сохранения снимка осуществляется по кнопке  (только для консоли АБ Linux).

4.2.5 Кнопка  предназначена для вывода всплывающих подсказок в поле 3 рисунка 4.2.

В консоли АБ Windows функциональные возможности по сохранению снимков экрана отсутствует.

Для сохранения снимка экрана из консоли АБ Linux необходимо одновременно подключить два USB-устройства, при этом сохранение будет осуществляться на один из носителей.

4.2.6 Основное окно консоли АБ Windows имеет два режима отображения элементов: сокращенный и расширенный. По умолчанию осуществляется отображение сокращенного режима меню, переключение между режимами осуществляется при помощи кнопки, расположенной внизу консоли: ***«Расширенный режим»*** / ***«Сокращенный режим»*** (рисунок 4.2).

4.2.7 Основные функциональные возможности консоли АБ Windows:

- управление учетными записями пользователей: создание, редактирование, удаление, блокировка, разблокировка (раздел 9);
- управление политиками идентификации и аутентификации пользователей и АБ: создание, редактирование или удаление (раздел 8);
- управление политиками КЦ объектов и загрузки ОС: создание, редактирование и удаление (раздел 6);
- создание шаблонов политик безопасности (подраздел 10.3)
- 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 7.3);
- управление общими настройками аутентификации и идентификации пользователей и КЦ объектов (подраздел 10.1);
- восстановление заводских настроек изделия (подраздел 10.4);
- получение данных о произведенных настройках безопасности на автоматизированных рабочих местах (АРМ) с установленным изделием (подраздел 10.2);
- проведение диагностики изделия (подраздел 10.5);
- просмотр информации о продукте (подраздел 10.6);
- работа с журналом аудита: просмотр сообщений о действиях АБ и пользователей, экспорт журнала на внешнее устройство хранения данных, очистка журнала (раздел 11).

4.2.8 В таблице 4.1 приведено описание пунктов меню консоли при расширенном режиме функционирования (рисунок 4.2).

Таблица 4.1 – Перечень пунктов меню, подпунктов и их назначение в консоли АБ

Пункт меню	Подпункт меню	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
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	

Пункт меню	Подпункт меню	Назначение
	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, получение данных о произведенных настройках безопасности на АРМ с установленным изделием, восстановление заводских настроек изделия
	Диагностика	Настройка параметров диагностики изделия
	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 Управление учетными записями пользователей, политиками аутентификации и идентификации пользователей и КЦ

5.1 Процесс управления параметрами учетных записей пользователей состоит из следующих 4 основных этапов:

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

- файлов и/или каталогов;
- журналов завершенности транзакций файловых систем;
- 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, статус.

Одной учетной записи пользователя допускается назначение нескольких политик КЦ и загрузки ОС. В случае обнаружения нарушения целостности в нескольких назначенных политиках применяются правила наиболее строгого типа блокировки.

5.2 Перед созданием учетной записи пользователя АБ необходимо:

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

5.3 При настройке КЦ объектов для каждой политики доступны следующие варианты контроля целостности:

- **контроль файлов** –КЦ файлов и (или) каталогов загружаемой ОС, файлов и/или каталогов пользователя
- **контроль журналов транзакций файловых систем** – КЦ 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, таблиц среды и карты памяти UEFI;
- **контроль загрузочных секторов** – КЦ загрузочных секторов устройств хранения данных;
- **контроль устройств** – контроль аппаратных устройств (аппаратной конфигурации) ЭВМ;
- **контроль загрузки ОС** – назначение одной или нескольких ОС для доверенной загрузки пользователю.

5.4 Тип реакции при нарушении КЦ единый на все объекты контроля и устанавливается при создании политики КЦ объектов и загрузки ОС (подраздел 6.1).

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 по умолчанию необходимо сменить до выхода из мягкого режима иначе пользователь будет заблокирован.

6 Управление политиками КЦ объектов и загрузки ОС

6.1 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.

6.1.1 Для создания новой политики КЦ и загрузки ОС необходимо выбрать в расширенном окне главного окна консоли АБ Windows подпункт меню ***«Политики контроля целостности объектов и загрузки ОС»*** (рисунок 4.2).

6.1.2 В появившемся диалоговом окне во вкладке «***Создание»*** (рисунок 6.1) необходимо заполнить поле ***«Имя»***, указать параметр ***«Тип блокировки»*** и выбрать какие объекты будут устанавливаться на контроль в создаваемой политике (рисунок 6.2).

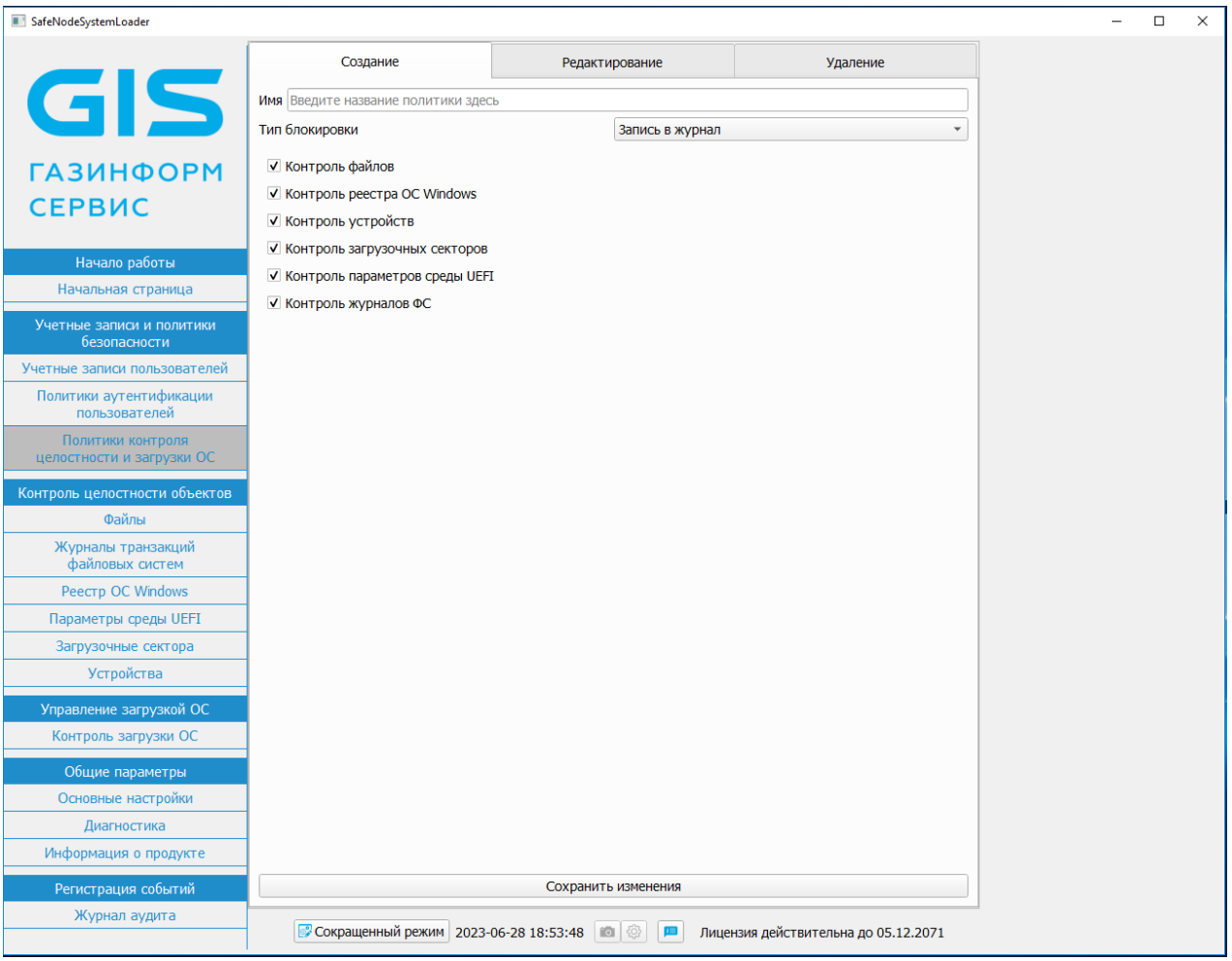


Рисунок 6.1 – Управление параметрами политики КЦ объектов и загрузки ОС

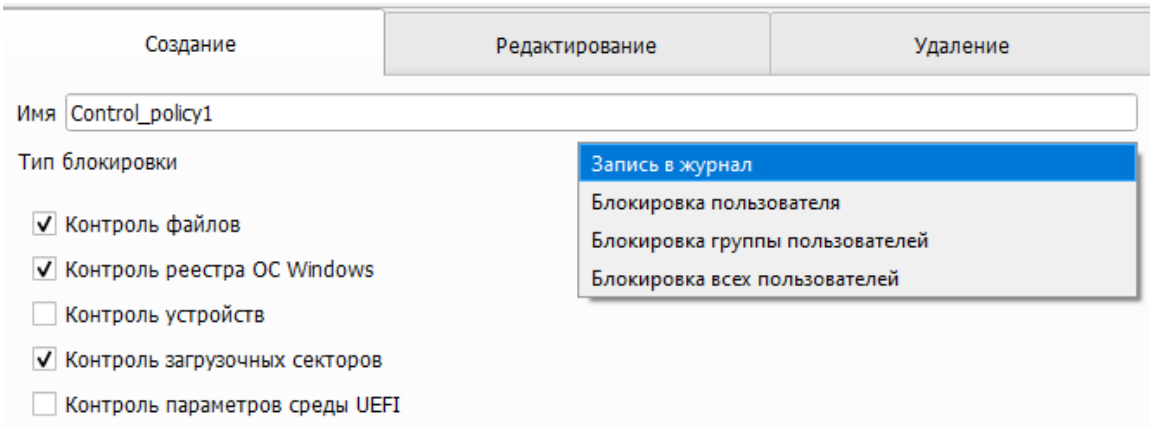


Рисунок 6.2 – Указание необходимых параметров для создания политики

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

КЦ объектов по умолчанию осуществляется после успешной идентификации и 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 данного пользователя доступ к системе всех пользователей, за исключением АБ, будет блокирован.

6.1.3 Для сохранения сформированной политики необходимо нажать кнопку ***«Сохранить изменения»***, при этом на экране ЭВМ появится новое диалоговое окно, в котором необходимо подтвердить создание политики (рисунок 6.3).

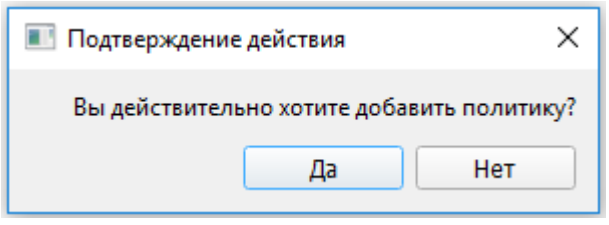


Рисунок 6.3 – Создание политики КЦ и загрузки ОС

6.1.4 Успешное создание политики КЦ объектов и загрузки ОС подтверждается сообщением в новом диалоговом окне (рисунок 6.4).

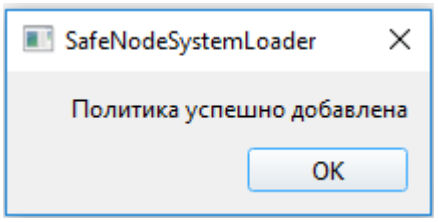


Рисунок 6.4 – Успешное создание политики КЦ и загрузки ОС

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 создание политики будет невозможно и во вкладке «*Создание*» появится сообщение «*Достигнут лимит создания политик*» (рисунок 6.5).

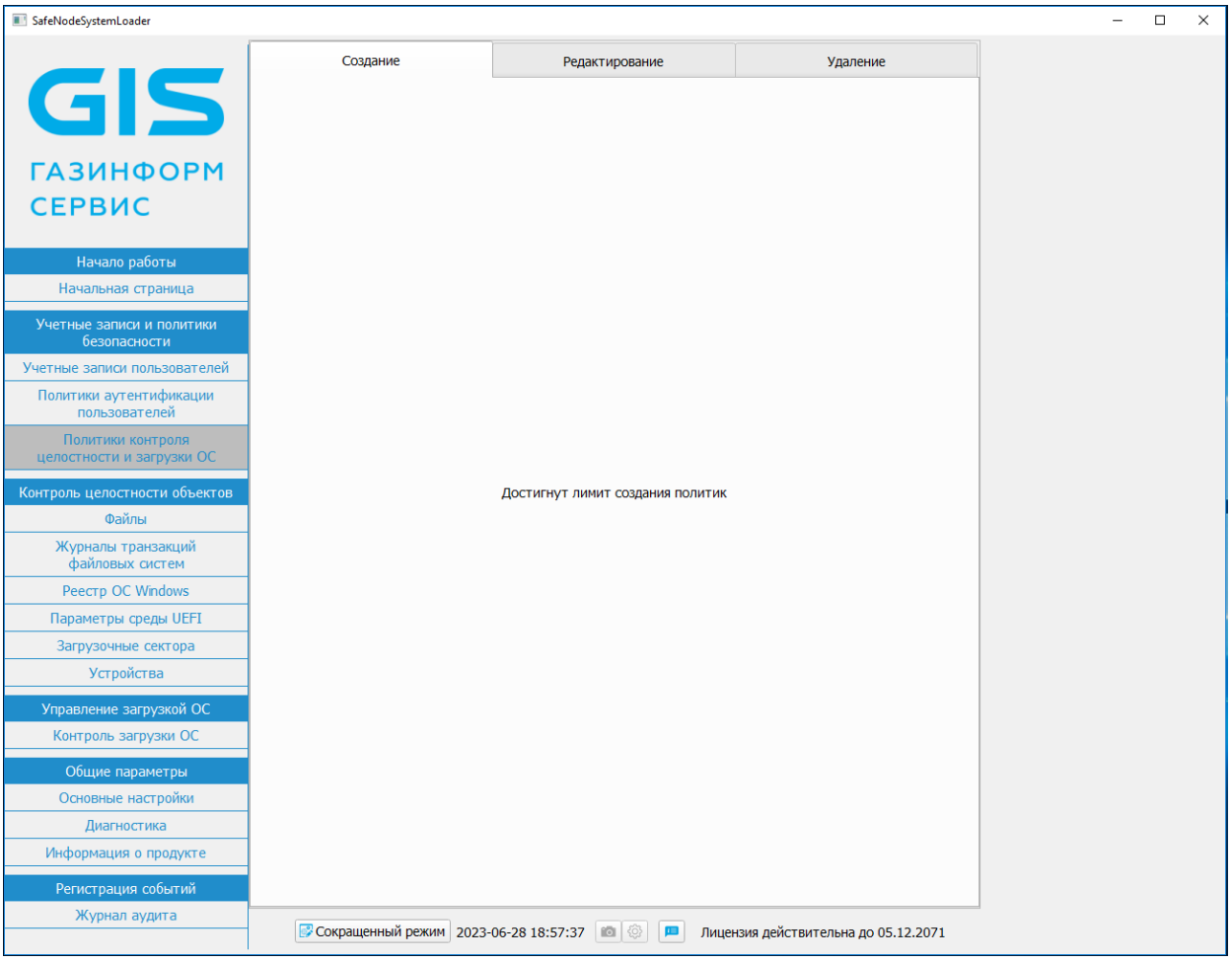


Рисунок 6.5 – Ограничение при создании политики КЦ и загрузки ОС

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

6.2.1 Объекты контроля для каждой политики устанавливаются индивидуально, при этом одни и те же объекты КЦ могут включаться в разные политики КЦ и загрузки ОС.

6.2.2 Для управления объектами КЦ необходимо предварительно выбрать настраиваемую политику, для этого:

1) В пункте меню ***«Контроль целостности объектов»*** (рисунок 4.2) перейти в требуемый элемент КЦ.

2) В появившемся диалоговом окне (рисунок 6.6) выбрать из списка политику контроля, для которой будет осуществляться настройка КЦ и нажать кнопку ***«ОК»***.

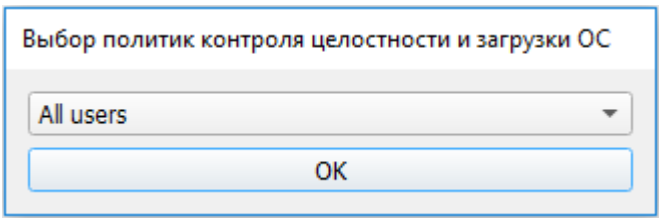


Рисунок 6.6 – Выбор политики для редактирования списка объектов КЦ

6.3 Редактирование политики КЦ и загрузки ОС

6.3.1 Для редактирования существующей политики КЦ и загрузки ОС необходимо выбрать в главном окне консоли АБ Windows подпункт меню «***Политики контроля целостности объектов и загрузки ОС»*** (рисунок 4.2).

6.3.2 В появившемся диалоговом окне необходимо перейти во вкладку ***«Редактирование»*** (рисунок 6.7) и выбрать имя редактируемой политики. При этом в нижней части окна отобразятся доступные для редактирования параметры политики КЦ и загрузки ОС (рисунок 6.8).

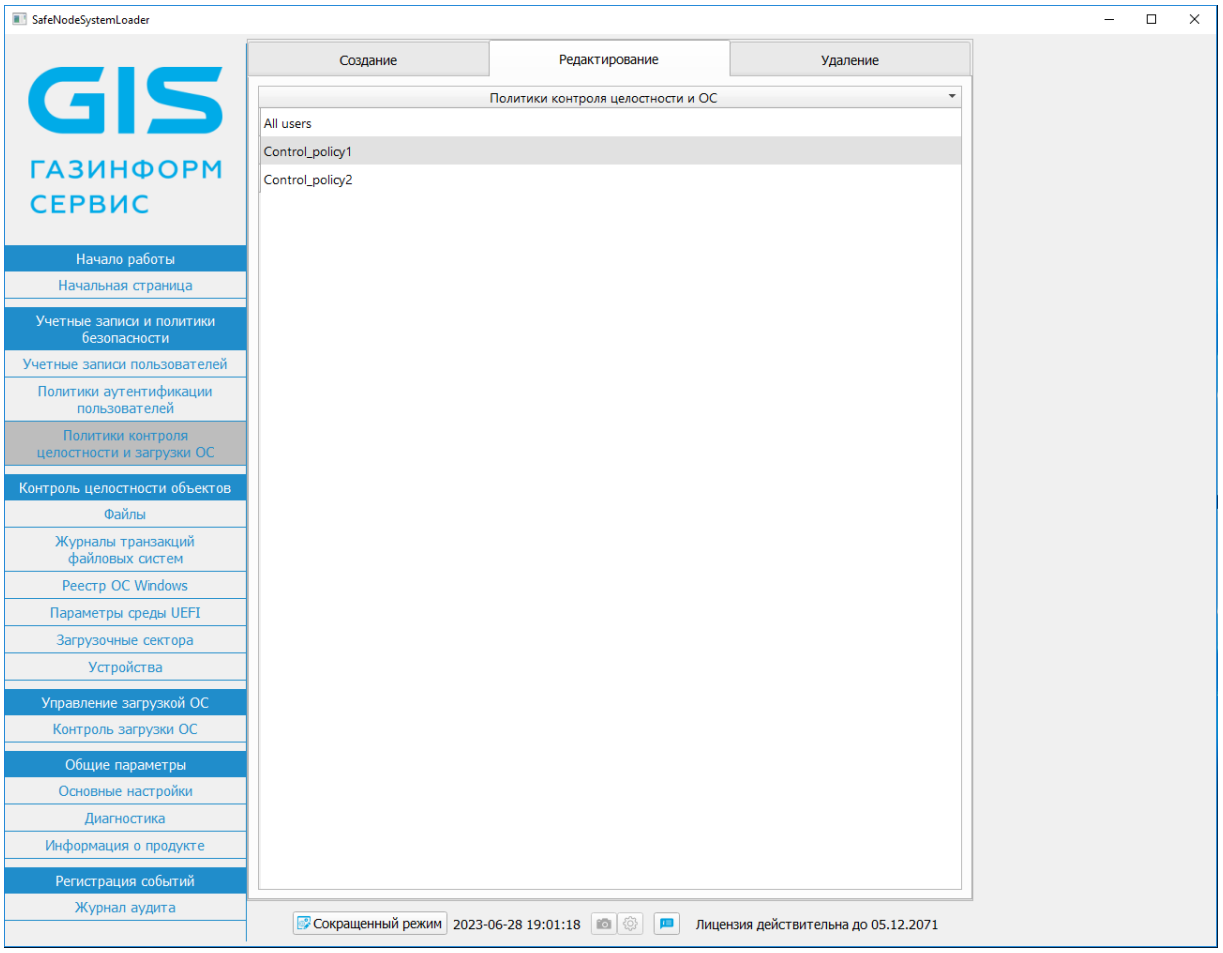


Рисунок 6.7 – Редактирование политики КЦ и загрузки ОС

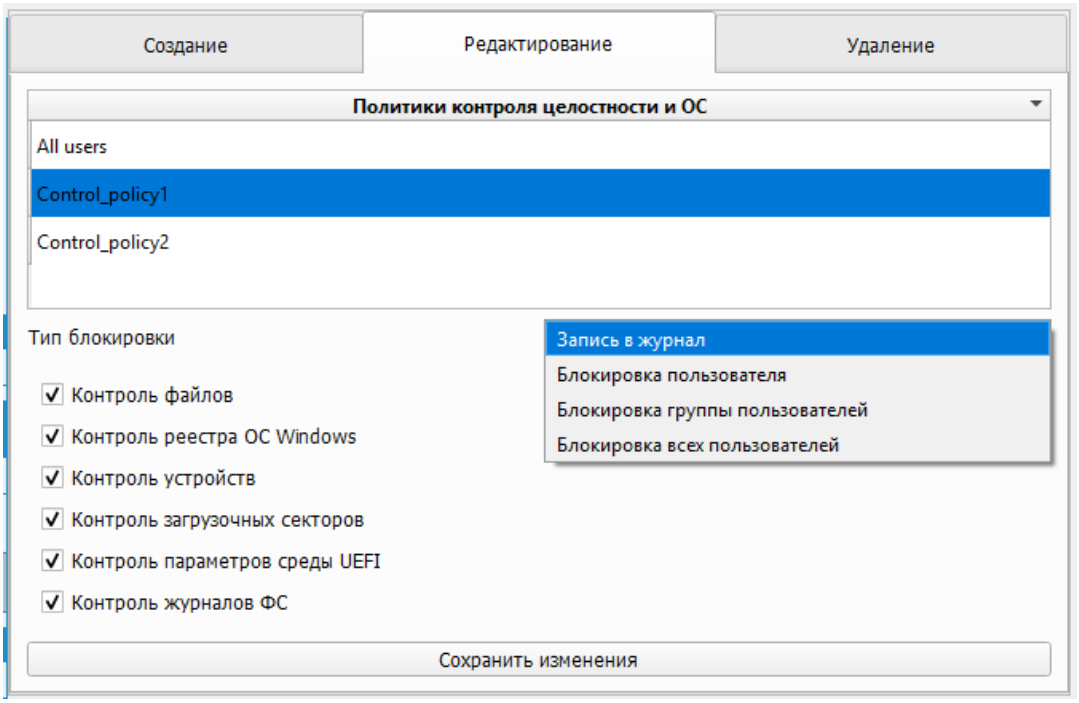


Рисунок 6.8 – Доступные для редактирования параметры политики КЦ и загрузки ОС

6.3.3 Для сохранения изменений редактируемой политики КЦ и загрузки ОС АБ необходимо нажать кнопку ***«Сохранить изменения»***. При этом на экране ЭВМ появится новое диалоговое окно, в котором необходимо подтвердить изменения, внесенные в политику (рисунок 6.9).

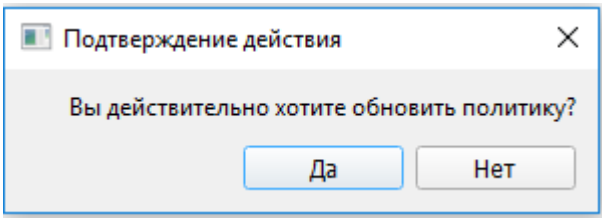


Рисунок 6.9 – Подтверждение изменений в политике КЦ и загрузки ОС

6.3.4 Успешное изменение политики КЦ объектов и загрузки ОС подтверждается сообщением в новом диалоговом окне (рисунок 6.10).

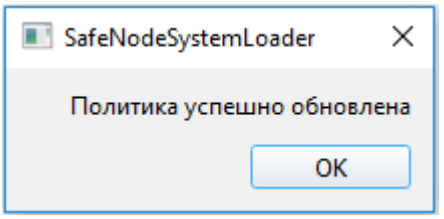


Рисунок 6.10 – Успешное изменение политики КЦ и загрузки ОС

6.4 Удаление политики КЦ и загрузки ОС

6.4.1 Для удаления существующей политики КЦ и загрузки ОС необходимо выбрать в главном окне консоли АБ Windows подпункт меню «***Политики контроля целостности объектов и загрузки ОС»*** (рисунок 4.2).

6.4.2 В появившемся диалоговом окне АБ необходимо перейти во вкладку ***«Удаление»*** (рисунок 6.11) и выбрать имя удаляемой политики КЦ и загрузки ОС. При этом на экране ЭВМ появится диалоговое окно, в котором необходимо подтвердить удаление выбранной групповой политики (рисунок 6.12).

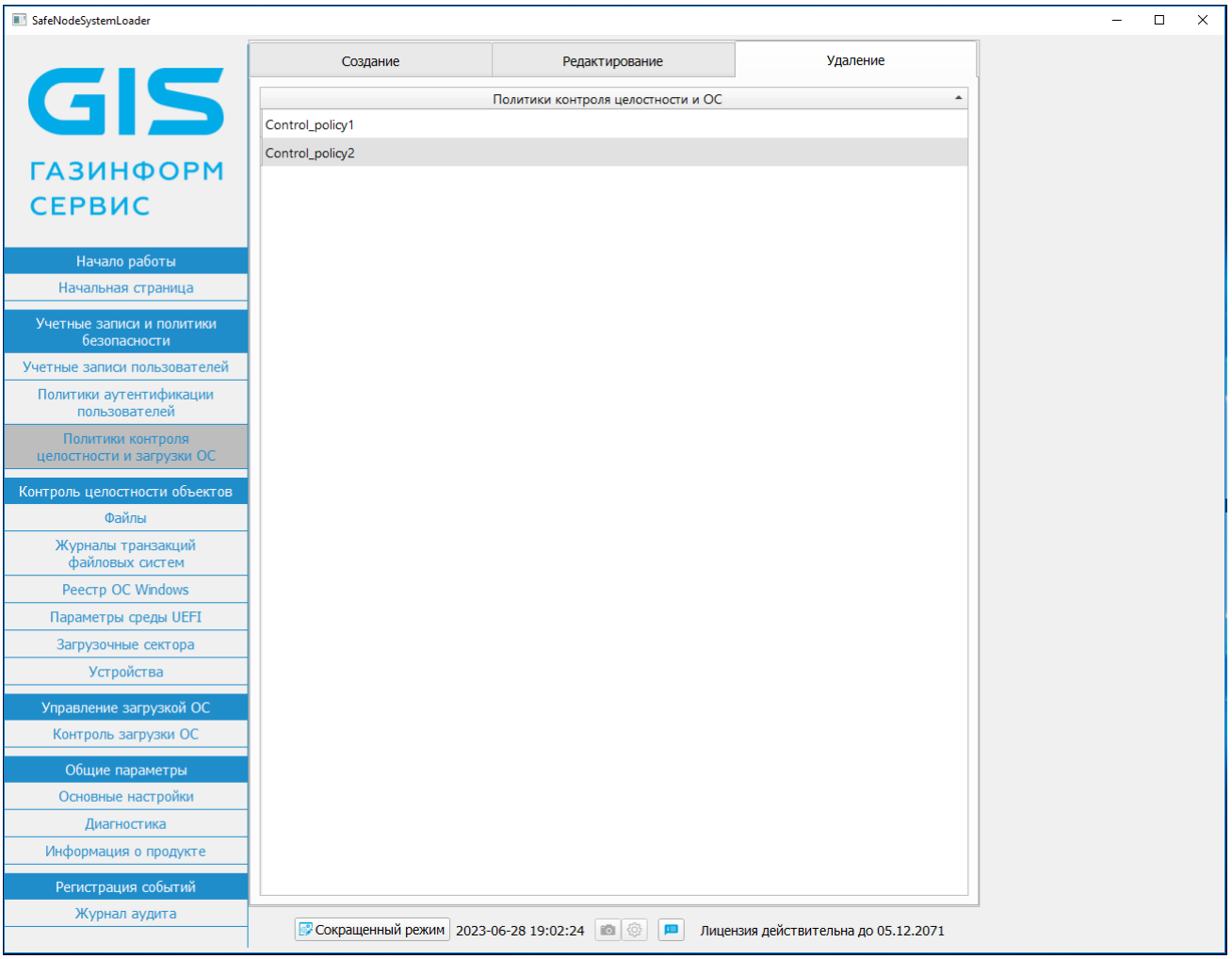


Рисунок 6.11 – Удаление политики КЦ и загрузки ОС

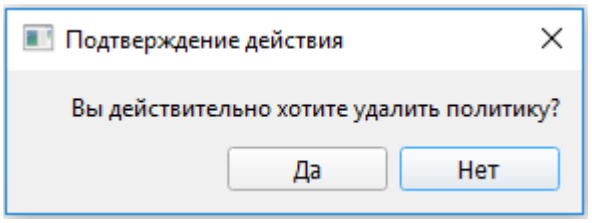


Рисунок 6.12 – Подтверждение удаления политики КЦ и загрузки ОС

Удаление групповых политик производится поочередно.

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

6.4.3 Успешное удаление политики КЦ объектов и загрузки ОС подтверждается сообщением в новом диалоговом окне (рисунок 6.13).

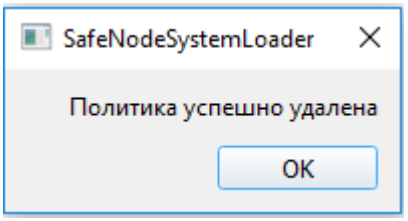


Рисунок 6.13 – Успешное удаление политики КЦ и загрузки ОС

Если политика КЦ объектов и загрузки ОС 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 некоторые учетные записи пользователей»*** (рисунок 6.14).

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.

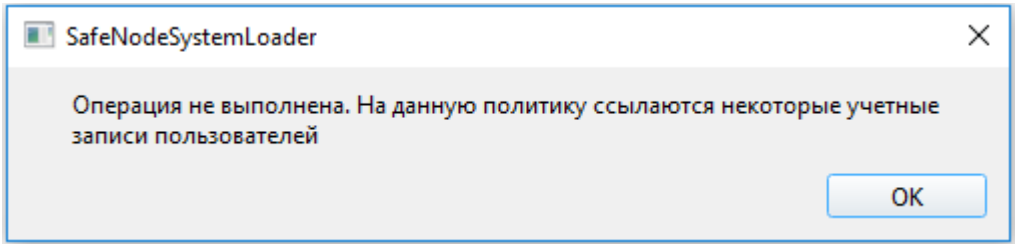


Рисунок 6.14 – Ошибка удаления политики КЦ и загрузки ОС

7 Контроль целостности объектов

7.1 Общие правила установки объектов на КЦ

7.1.1 Пункт меню консоли АБ Windows ***«Контроль целостности объектов»*** предназначен для установки объектов на КЦ путем редактирования соответствующей политики КЦ и загрузки ОС. Действия по установке объектов на КЦ совершаются АБ в следующей последовательности:

1) Перейти в соответствующий подпункт меню ***«Контроль целостности объектов»*** для выбора и установки на КЦ файлов, журналов транзакций файловых систем, реестра ОС Windows, параметров среды UEFI, загрузочных секторов и устройств.

2) Выбрать политику КЦ объектов и загрузки ОС, для которой будут произведены изменения.

3) Появление диалогового окна, отображающего:

- список подключенных к ЭВМ устройств хранения данных (для подпунктов ***«Файлы»***, ***«Журналы транзакций файловых систем»***, ***«Реестр ОС Windows»*** и ***«Загрузочные сектора»***);
- перечень переменных, драйверов, системных таблиц и карты памяти UEFI (для подпункта ***«Параметры среды UEFI»***);
- перечень аппаратных устройств ЭВМ (для подпункта ***«Устройства»***).

4) Установить необходимые объекты на КЦ во вкладке ***«Файловый менеджер»*** (***«Обзор»***, ***«Менеджер реестра»***, ***«Менеджер»***, ***«Обзор устройств»*** – в зависимости типа контролируемых объектов) путем установки отметок рядом с необходимыми объектами.

При установке объектов на КЦ необходимо учитывать следующие особенности:

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

Рекомендуется устанавливать на КЦ не более 1000 файлов!

Указание максимально значения количества контролируемых объектов осуществляется в подпункте меню *«Основные настройки»* (см. подраздел 10.1).

При превышении установленного максимального количества, будет выведено сообщение *«Невозможно поставить на контроль данное количество файлов!» («Превышен лимит установки объектов реестра на контроль!»)* и установка объектов на КЦ не будет выполнена.

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

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

7.1.2 Для редактирования перечня объектов, установленных на КЦ необходимо:

1) Перейти в соответствующий подпункт меню ***«Контроль целостности объектов»*** для выбора и установки на КЦ файлов, журналов транзакций файловых систем, реестра ОС Windows, параметров среды UEFI, загрузочных секторов и устройств.

2) Выбрать политику КЦ объектов и загрузки ОС, для которой необходимо отредактировать перечень объектов КЦ.

3) Перейти во вкладку ***«Контролируемые файлы»*** (***«Контроль»***, ***«Контролируемые объекты»*** **–** в зависимости типа контролируемых объектов), удалить отметки напротив требуемых объектов и воспользоваться кнопкой ***«Удалить выбранные».*** По кнопке ***«Удалить все»*** все файлы и каталоги, установленные на контроль, снимаются с него.

7.1.3 Пересчет контрольных сумм для объектов, установленных на КЦ, производится в следующей последовательности:

1) Перейти в соответствующий подпункт меню ***«Контроль целостности объектов»*** для выбора и установки на КЦ файлов, журналов транзакций файловых систем, реестра ОС Windows, параметров среды UEFI, загрузочных секторов и устройств.

В текущей версии ПО изделия установка на КЦ файлов и объектов реестра ОС Windows, расположенных на твердотельных накопителях (SSD M.2), не поддерживается из консоли АБ Windows.

Для установки на КЦ подобных объектов следует использовать консоль АБ или консоль АБ Linux.

В случае, если раздел примонтирован не в корень файловой системы, то он ставится на КЦ через отдельный раздел в списке ФС. Установка такого раздела через корневую ФС приведет к ошибкам при контроле целостности.

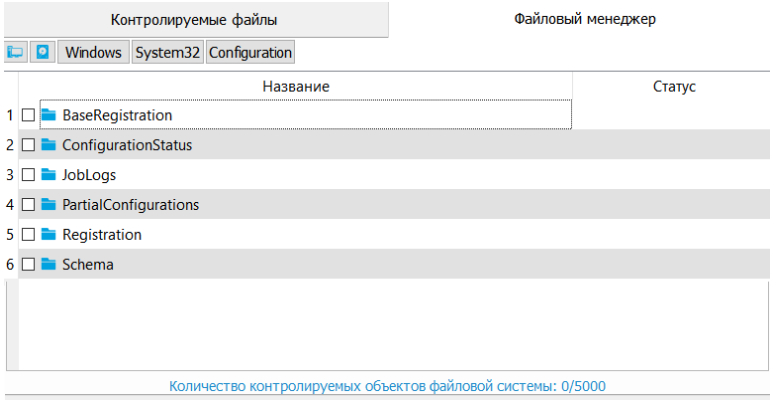
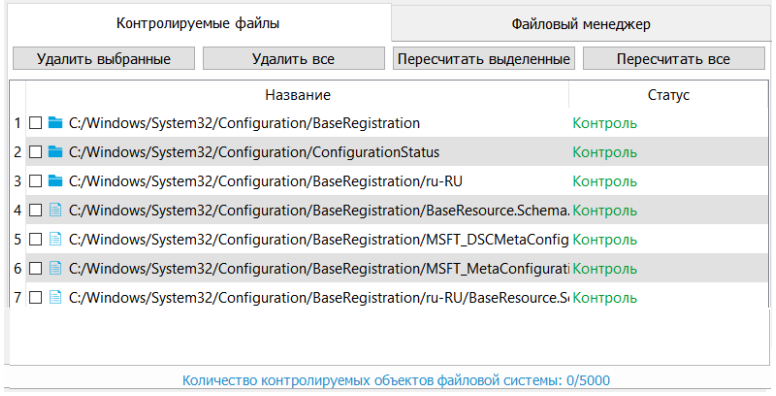
2) Выбрать политику КЦ объектов и загрузки ОС, для которой необходимо выполнить перерасчет контрольных сумм объектов КЦ.

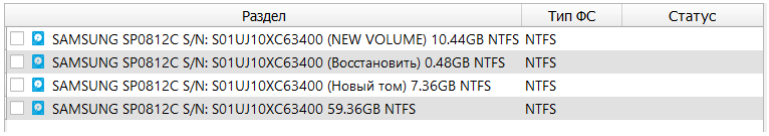
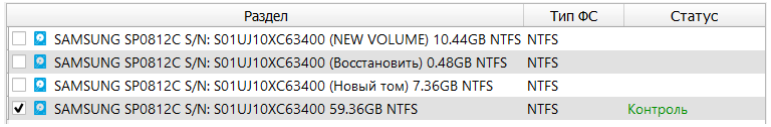
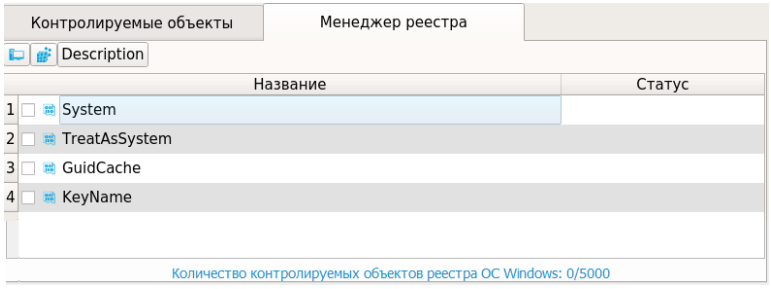
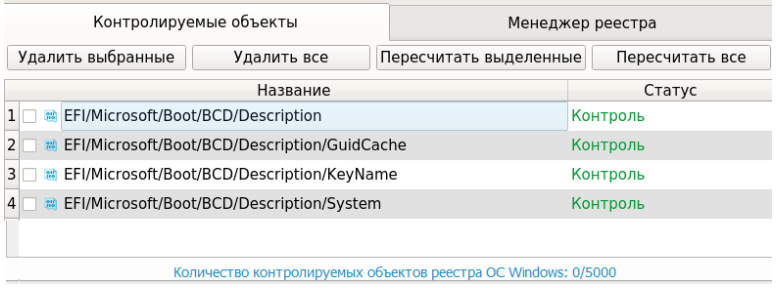
3) Перейти во вкладку ***«Контролируемые файлы»*** (***Контроль***, ***Контролируемые объекты*** – в зависимости типа контролируемых объектов), установить отметки напротив требуемых объектов и воспользоваться кнопкой ***«Пересчитать выделенные».*** Сохранение контрольных сумм всех выбранных объектов произойдет автоматически. При нажатии кнопки ***«Пересчитать все»*** будет выполнен пересчет всех объектов с нарушением целостности.

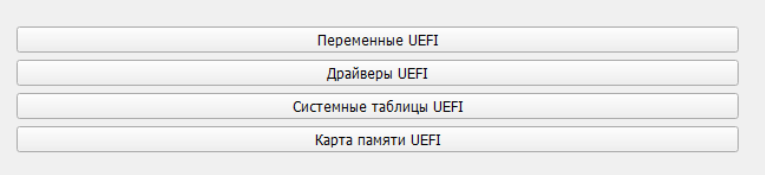
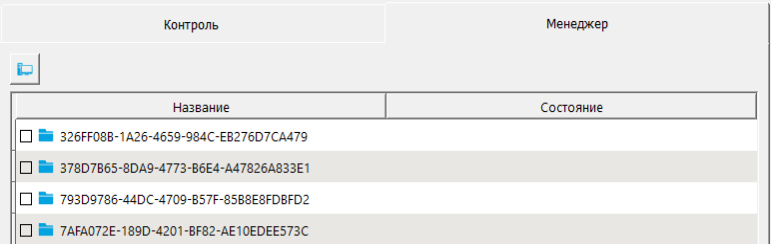
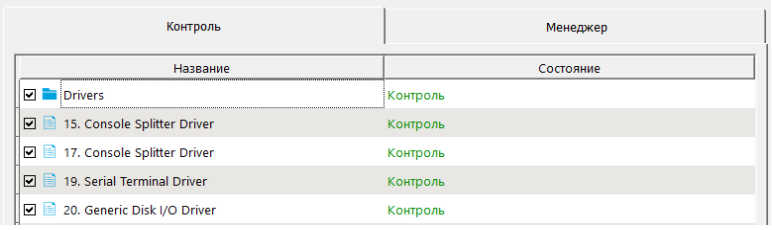
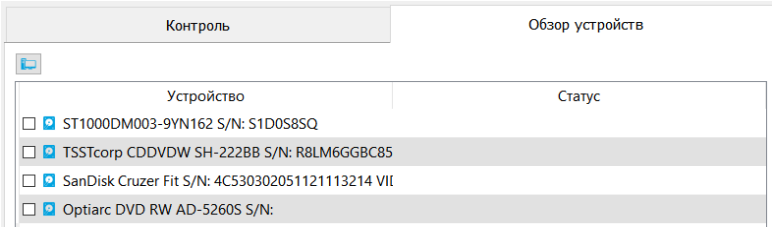
Процедура просмотра нарушений КЦ и исправления ошибок приведена в подразделе 7.3.

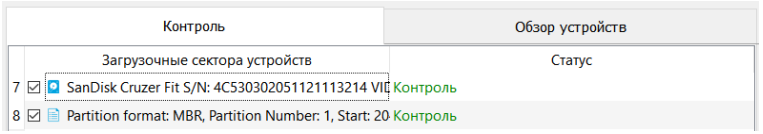
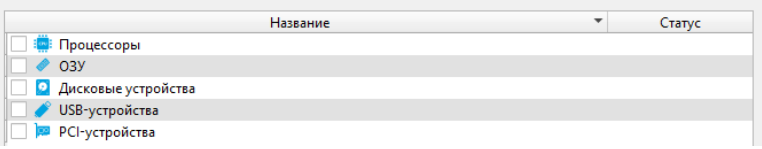
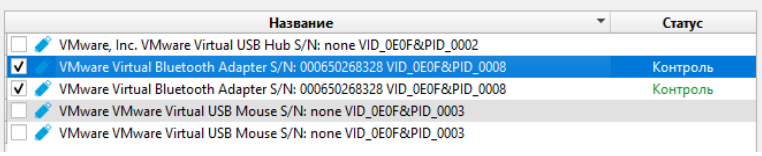
7.1.4 Процедура и особенности выбора и установки объектов на КЦ приведены в таблице 7.1.

Таблица 7.1 – Постановка объектов на КЦ

№ п.п.	Пункт меню *«Контроль целостности объектов»*	Внешний вид диалогового окна в консоли АБ	Описание диалогового окна	Примечание
1	***Файлы***	Вкладка ***«Файловый менеджер»***:  Вкладка «***Контролируемые файлы»***:  	Каталоги верхнего уровня отображаются в верхней части вкладки ***«Файловый менеджер»*** в виде кнопок с наименованием каталога. Для возврата в каталог верхнего уровня необходимо нажать на кнопку с наименованием каталога. Возврат к структуре каталогов и файлов выбранного устройства хранения данных осуществляется по кнопке  . Возврат к выбору необходимого устройства хранения данных осуществляется по кнопке  . Просмотр списка файлов и каталогов, установленных на КЦ, доступен во вкладке ***«Контролируемые файлы»***. Установка на/снятие с КЦ файлов и каталогов осуществляется по общим правилам, указанным в настоящем документе. В нижней части вкладки отображается соотношение количества поставленных на контроль объектов файловой системы к общему количеству объектов файловой системы  	Перечень системных файлов ОС семейства Windows и Linux, рекомендуемых к установке на КЦ, приведен в Приложениях А и Б настоящего документа

№ п.п.	Пункт меню *«Контроль целостности объектов»*	Внешний вид диалогового окна в консоли АБ	Описание диалогового окна	Примечание
2	***Журналы транзакций файловых систем***	Диалоговое окно ***«Журналы транзакций файловых систем»***:  Установка на контроль объекта:  	Установка на КЦ журналов завершенности транзакций файловых систем осуществляется в пункте меню ***«Журналы транзакций файловых систем»***, который содержит список подключенных к ЭВМ устройств хранения данных. Установка на/снятие с КЦ журналов завершенности транзакций файловых систем осуществляется по общим правилам, указанным в настоящем документе	
3	***Реестр ОС Windows***	Вкладка ***Менеджер реестра***  Вкладка ***«Контролируемые объекты»***:  	Для выбора и установки на КЦ объектов реестра ОС Windows необходимо перейти во вкладку ***«Менеджер реестра»***, содержащую список объектов реестра ОС Windows. Установленные на КЦ объекты отображаются во вкладке ***«Контролируемые объекты»***. Установка на/снятие с КЦ реестра ОС Windows осуществляется по общим правилам, указанным в настоящем документе. В нижней части вкладки отображается соотношение количества поставленных на контроль объектов реестра ОС Windows к общему количеству объектов реестра ОС Windows Количество контролируемых объектов реестра ОС Windows: 0/5000	В Приложении В приведено соответствие между названиями основных ветвей реестра ОС Windows и названиями ветвей реестра, отображаемыми в редакторе реестра **regedit**

№ п.п.	Пункт меню *«Контроль целостности объектов»*	Внешний вид диалогового окна в консоли АБ	Описание диалогового окна	Примечание
4	***Параметры среды UEFI***	Общий вид диалогового окна:  Вкладка ***«Менеджер»***:  Вкладка ***«Контроль»***: 	В диалоговом окне необходимо выбрать параметр среды UEFI, устанавливаемый на контроль (переменные, драйвера, системные таблицы или карта памяти UEFI). Внешний вид окон для установки данных объектов на КЦ аналогичен и содержит вкладки ***«Менеджер»*** и ***«Контроль»***. Вкладка ***«Менеджер»*** предназначена для выбора и установки на КЦ выбранного параметра среды UEFI. Установленные на КЦ объекты отображаются во вкладке ***«Контроль»***. Установка на/снятие с КЦ параметров среды UEFI осуществляется по общим правилам, указанным в настоящем документе	
5	***Загрузочные сектора***	Вкладка ***«Обзор устройств»***: 	Для выбора и установки на КЦ загрузочных секторов необходимо перейти во вкладку ***«Обзор устройств»***, содержащую список подключенных к ЭВМ устройств хранения данных. Установленные на КЦ объекты отображаются во вкладке ***«Контроль»***.	**Невозможна установка на КЦ устройства CD/DVD-ROM, не содержащего подключенный носитель CD/DVD**

№ п.п.	Пункт меню *«Контроль целостности объектов»*	Внешний вид диалогового окна в консоли АБ	Описание диалогового окна	Примечание
		Вкладка ***«Контроль»***: 	Установка на/снятие с КЦ загрузочных секторов осуществляется по общим правилам, указанным в настоящем документе	
6	***Устройства***	Общий вид окна:  	Диалоговое окно содержит список аппаратных устройств ЭВМ. Установка на/снятие с КЦ устройств осуществляется по общим правилам, указанным в настоящем документе	**Установленное на КЦ USB-устройство будет недоступно пользователю только во время процедуры доверенной загрузки ОС** При эксплуатации изделия на некоторых ЭВМ (например, Acer Veriton N4660G) необходимо изменить значение параметра «Режим SATA» в BIOS Setup согласно рекомендациям документа «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 1. Руководство по установке. ГМТК.468269.060РЭ1

7.2 Контроль загрузки ОС

7.2.1 При выборе в меню **«Управление загрузкой ОС»** подпункта ***«Контроль загрузки ОС»*** (рисунок 4.2) и последующем выборе редактируемой политики КЦ и загрузки ОС на экране ЭВМ появится диалоговое окно (рисунок 7.1), содержащее список установленных ОС на данной ЭВМ.

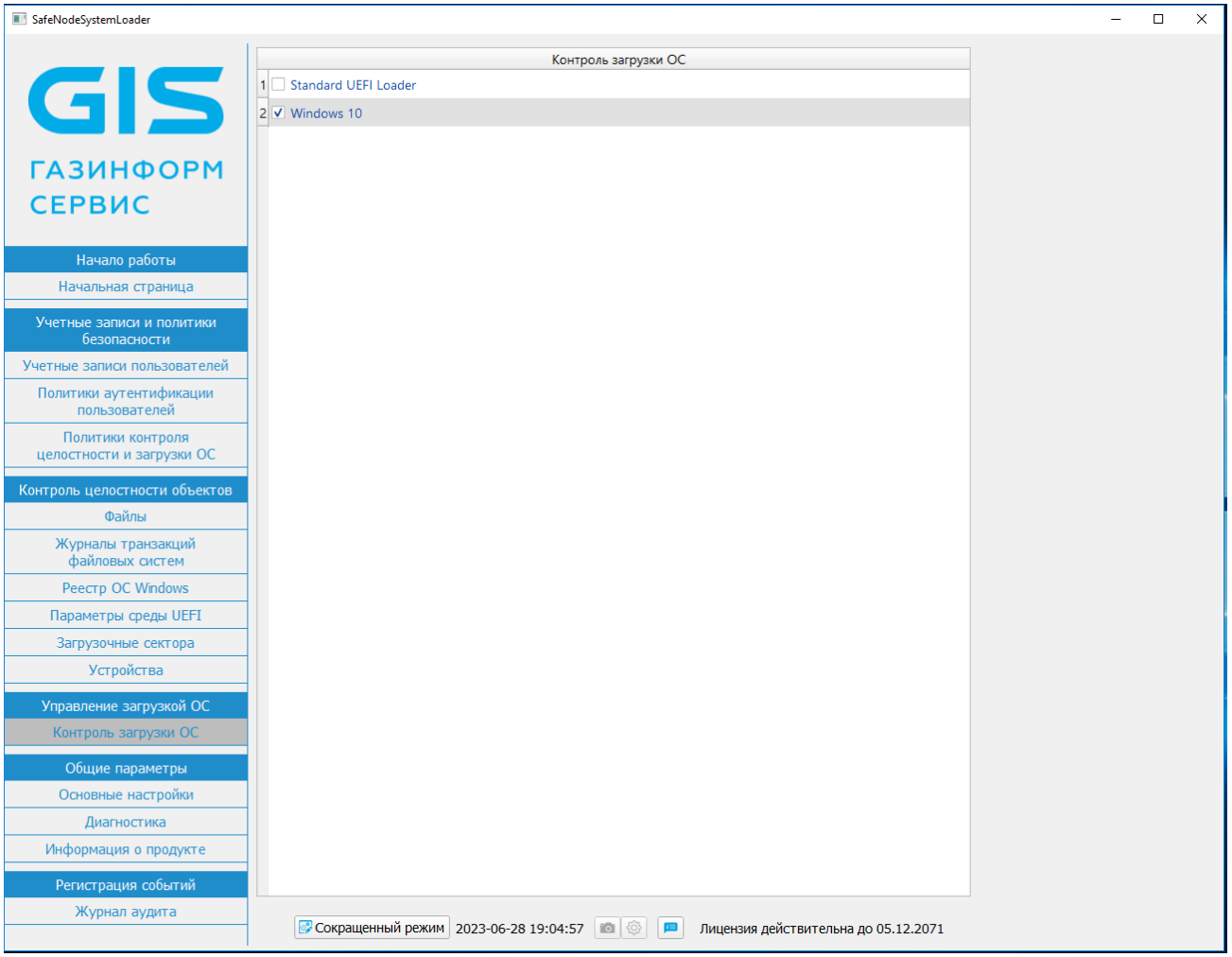


Рисунок 7.1 – Список ОС для доверенной загрузки пользователям

7.2.2 Установленные на ЭВМ ОС в режиме **UEFI** отображаются на экране голубым цветом, в режиме **Legacy Boot** – фиолетовым цветом (рисунок 7.2).

7.2.3 Для определения ОС в качестве доверенной для загрузки пользователем, необходимо установить отметку в поле напротив требуемой ОС (рисунок 7.2).

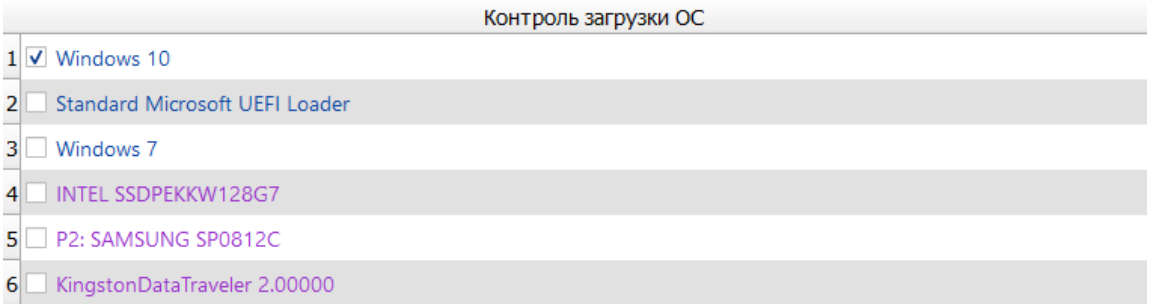


Рисунок 7.2 – Выбор ОС для доверенной загрузки пользователям

7.2.4 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.

Необходимо обратить внимание, что установка нескольких ОС на единый MBR раздел устройства хранения данных повлечет за собой невозможность разграничить доступ пользователя к загрузке этих ОС.

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

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

7.2.5 Появление в списке отсутствующей ОС, выделенной красным цветом с поясняющей надписью: ***«ОС не найдена»*** (рисунок 7.3), означает, что определенная для доверенной загрузки пользователю ОС удалена с ЭВМ.

7.2.6 При снятии данной отметки появится информационное сообщение ***«Данная ОС будет удалена из списка. Хотите продолжить?»*** (рисунок 7.4). После подтверждения действия ОС будет удалена из списка и больше не будет отображаться.

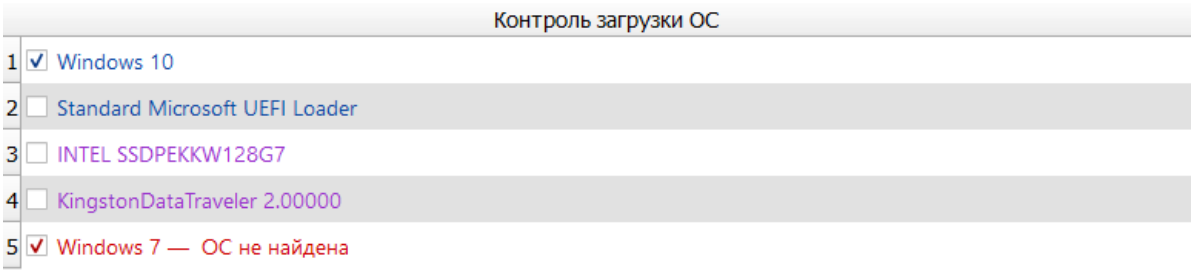


Рисунок 7.3 – Отображение отсутствующей ОС на ЭВМ

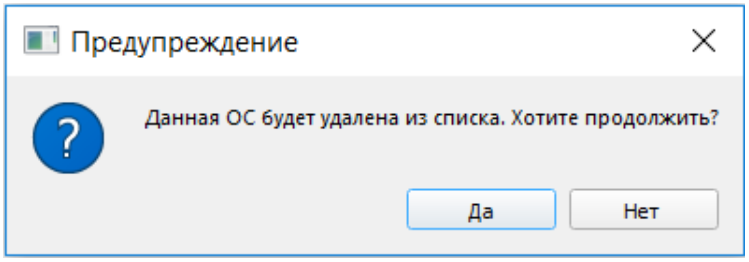


Рисунок 7.4 – Удаление отсутствующей ОС из списка

7.3 Устранение ошибок КЦ

7.3.1 При работе пользователей в системе возможно нарушение КЦ объектов.

7.3.2 В зависимости от выбранного типа реакции на нарушение КЦ аутентификация и (или) идентификация пользователя в систему может быть ограничен (рисунок 7.5). Для разблокировки пользователя(-ей) необходимо выполнить аутентификацию и идентификацию АБ.

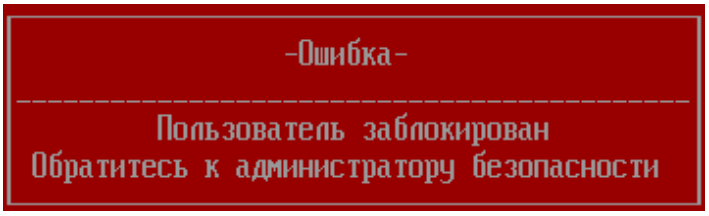


Рисунок 7.5 – Сообщение о блокировке пользователя

7.3.3 После выполнения успешной аутентификации и идентификации АБ на начальной странице (рисунок 4.2) необходимо ознакомиться с нарушениями, зафиксированными при работе пользователя.

7.3.4 Для устранения нарушений КЦ АБ необходимо перейти в соответствующий пункт меню ***«Контроль целостности объектов»*** (рисунок 4.2) и выбрать политику КЦ и загрузки ОС с выявленным нарушением целостности.

7.3.5 Во вкладке ***«Контролируемые файлы»*** будут отображаться все устройства

хранения данных (каталоги), в которых выявлены нарушения целостности (рисунок 7.6).

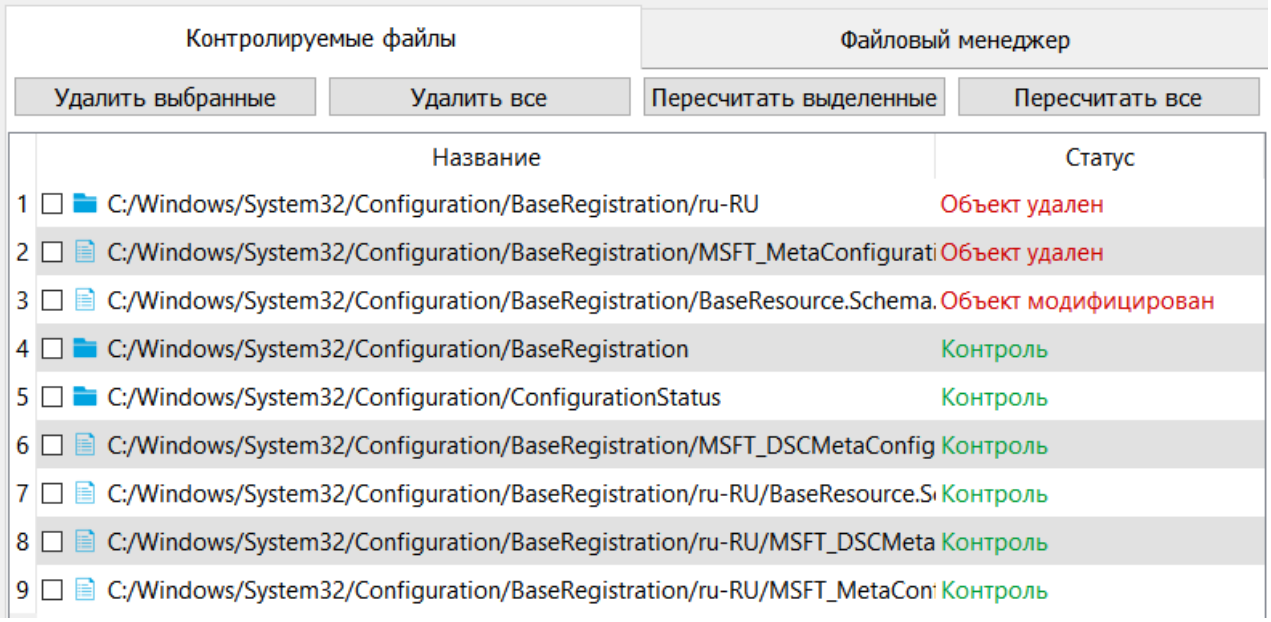


Рисунок 7.6 – Устройство хранения данных с нарушением целостности файлов

7.3.6 Статус объектов КЦ в которых выявлены нарушения, различается в зависимости от действий, произведенных над содержимым контролируемого объекта (рисунок 7.6):

- ***«Объект удален»;***
- ***«Объект модифицирован».***

7.3.7 Для удаления выборочных объектов с КЦ необходимо установить отметку в поле напротив требуемого объекта и нажать кнопку ***«Удалить выбранные»***. По кнопке ***«Удалить все»*** все объекты, установленные на контроль, удаляются с него.

7.3.8 Для пересчета контрольной суммы выборочных объектов с нарушением целостности необходимо установить отметку в поле напротив требуемого объекта и нажать кнопку ***«Пересчитать выделенные»***, при этом пересчет и сохранение контрольных сумм всех выбранных объектов произойдет автоматически. По кнопке ***«Пересчитать все»*** произойдет пересчет всех объектов с нарушением целостности.

7.3.9 После устранения нарушения КЦ объектов необходимо выполнить разблокировку учетных записей пользователей (подраздел 9.2).

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 Windows (рисунок 4.2) выбрать подпункт меню ***«Политики аутентификации пользователей»***.

8.1.2 В появившемся диалоговом окне во вкладке ***«Создание»*** необходимо ввести имя создаваемой политики аутентификации пользователей в поле ***«Имя»*** (рисунок 8.1).

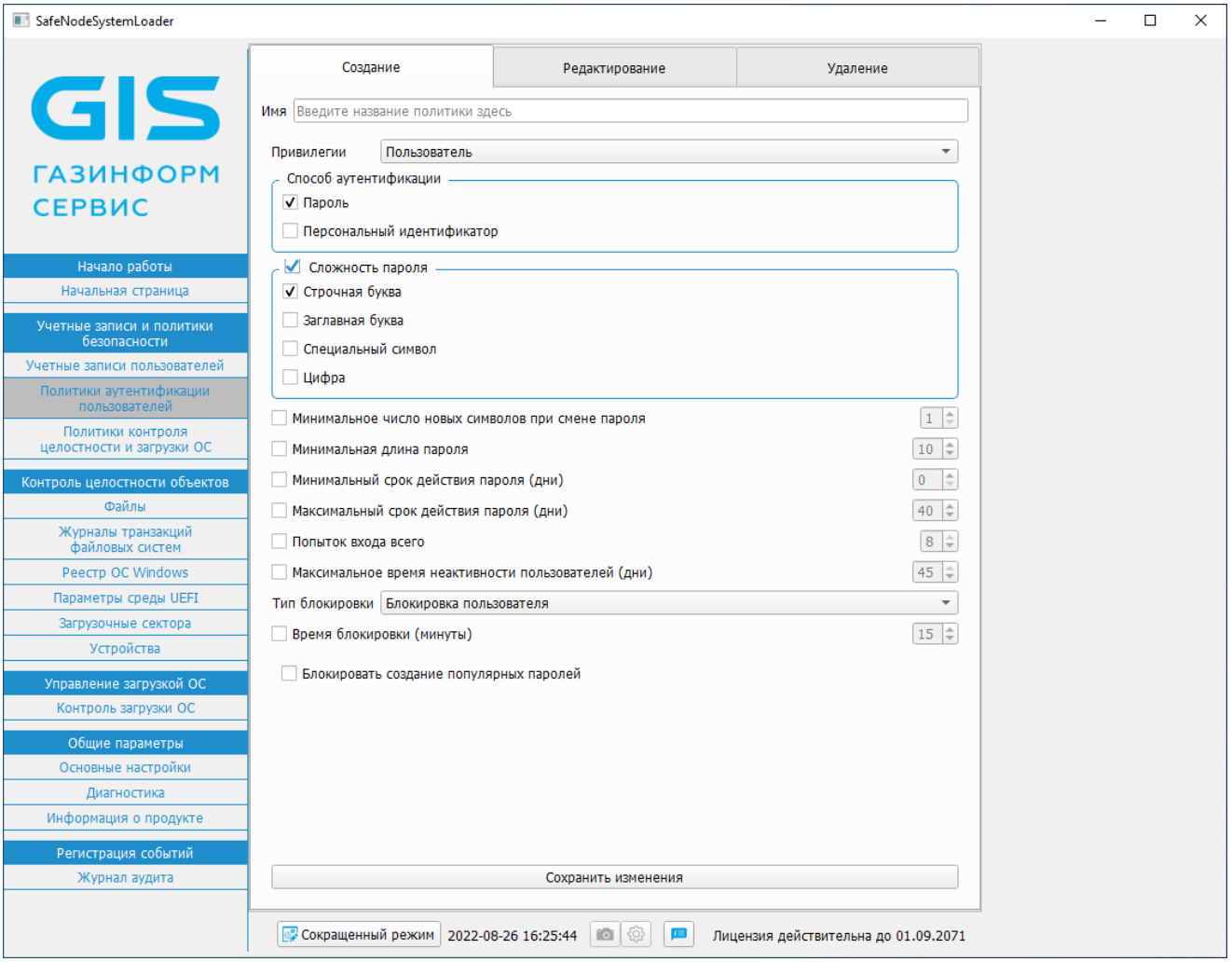


Рисунок 8.1 – Создание политики аутентификации пользователей

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 таким именем уже существует. Введите другое»*** (рисунок 8.2).

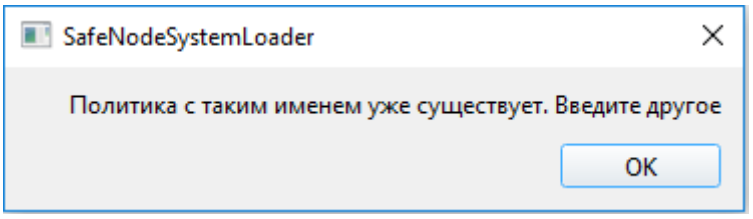


Рисунок 8.2 – Ошибка при создании политики аутентификации пользователей

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

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	Способ аутентификации	[Пароль] Персональный идентификатор		Для определения двухфакторной аутентификации необходимо установить два значения – Пароль и персональный идентификатор
4	Сложность пароля	[Строчная буква] Заглавная буква Цифра Специальный символ		Поле предназначено для установки сложности пароля.
5	Минимальное число новых символов при смене пароля	1	1…8	Минимальное число новых символов при смене пароля
6	Минимальная длина пароля	10	8…32	
7	Минимальный срок действия	0	0…45	Меньше или равно максимальному сроку действия.

№	Наименование поля	Возможные значения поля [по умолчанию]	Минимальное … максимальное значения	Примечание
	пароля (дни)			При установке значения параметра «0» смена пароля возможна с текущей даты
8	Максимальный срок действия пароля (дни)	40	1…45	
9	Попыток входа всего	8	1…8	Применяется только при аутентификации до загрузки ОС. При аутентификации в консоли АБ Linux/Windows количество попыток входа неизменно и равно «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	Блокировать создание популярных паролей			При активации данного поля добавляется список популярных паролей, запрещенных к использованию. При необходимости, можно выделить требуемые пароли и исключить их из 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 Для редактирования списка популярных паролей, запрещенных к использованию, после активации соответствующего поля (рисунок 8.3), необходимо воспользоваться соответствующими кнопками:

- для удаления пароля(ей), выделить требуемые и нажать кнопку ***«Удалить выделенные»***;
- для добавления пароля в словарь, ввести требуемую последовательность в строке поиска и нажать кнопку «+».

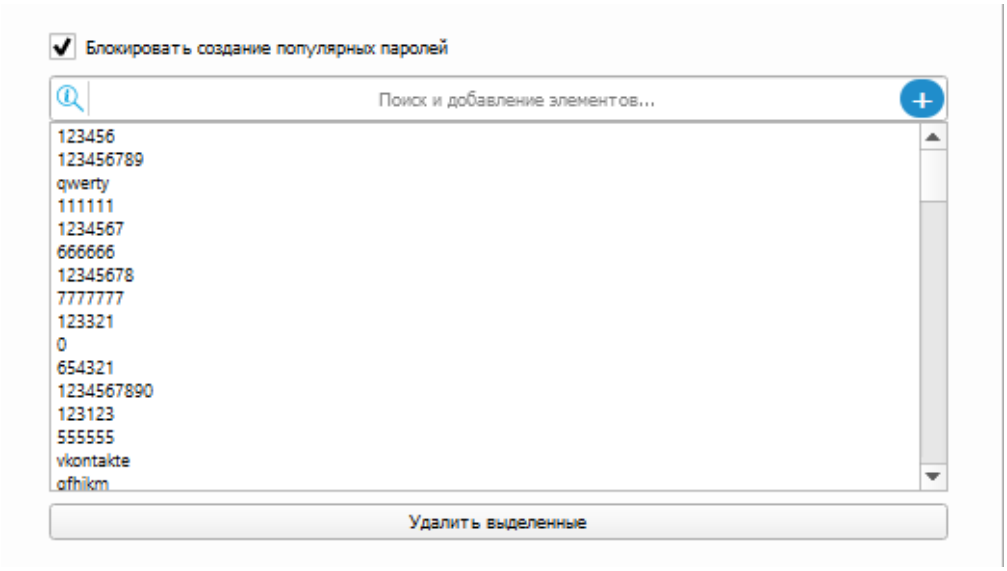


Рисунок 8.3 – Редактирование перечня популярных паролей

8.1.5 После установки полей (рисунок 8.1) для сохранения изменений в создаваемой политике аутентификации необходимо нажать на кнопку ***«Сохранить изменения»***, при этом на экране ЭВМ появится новое диалоговое окно, в котором необходимо подтвердить создание политики (рисунок 8.4).

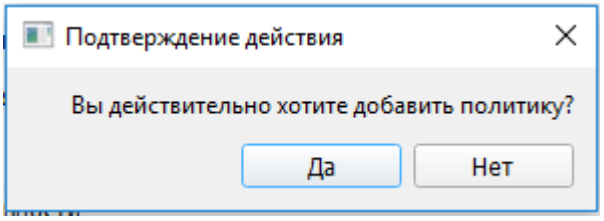


Рисунок 8.4 – Подтверждение создания политики аутентификации пользователей

8.1.6 Успешное создание политики аутентификации пользователей подтверждается сообщением в новом диалоговом окне (рисунок 8.5).

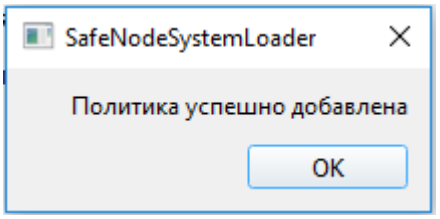


Рисунок 8.5 – Успешное создание политики аутентификации пользователей

В ПО изделия установлено ограничение на создание политик аутентификации.

Допускается создавать не более 20 политик.

При превышении установленного максимального количества политик аутентификации, создание политики будет невозможно, при этом во вкладке *«Создание»* появится сообщение *«Достигнут лимит создания политик»* (рисунок 6.5).

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.

8.2 Редактирование политики аутентификации пользователей

8.2.1 Для редактирования существующей политики аутентификации пользователей необходимо выбрать в главном окне (рисунок 4.2) подпункт меню ***«Политики аутентификации пользователей»***.

8.2.2 В появившемся диалоговом окне АБ необходимо перейти во вкладку

«Редактирование» (рисунок 8.6) и выбрать имя редактируемой политики аутентификации пользователей. При этом в нижней части окна отобразятся доступные для редактирования параметры политики аутентификации пользователей (рисунок 8.7).

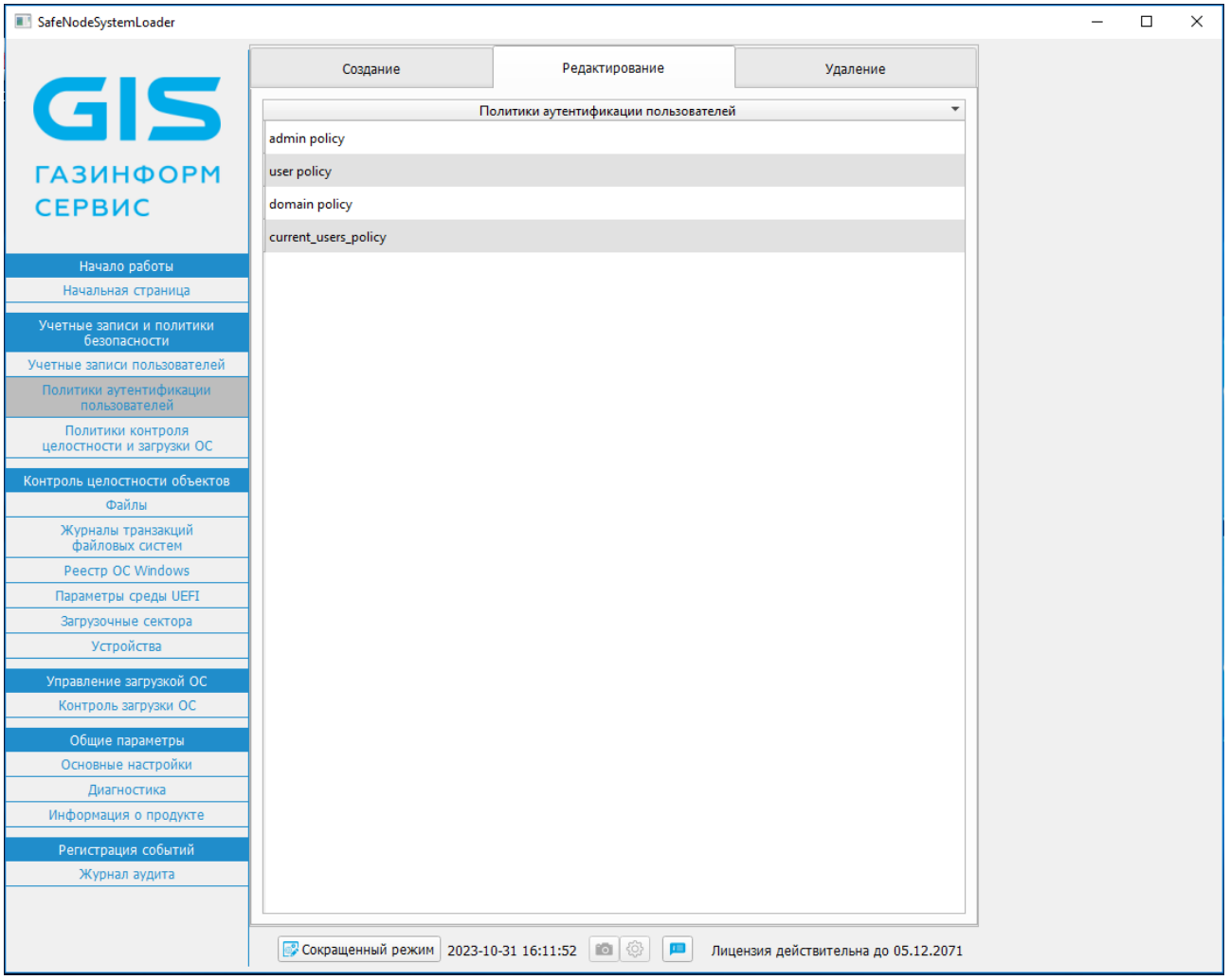


Рисунок 8.6 – Список политик аутентификации пользователей, доступных для редактирования

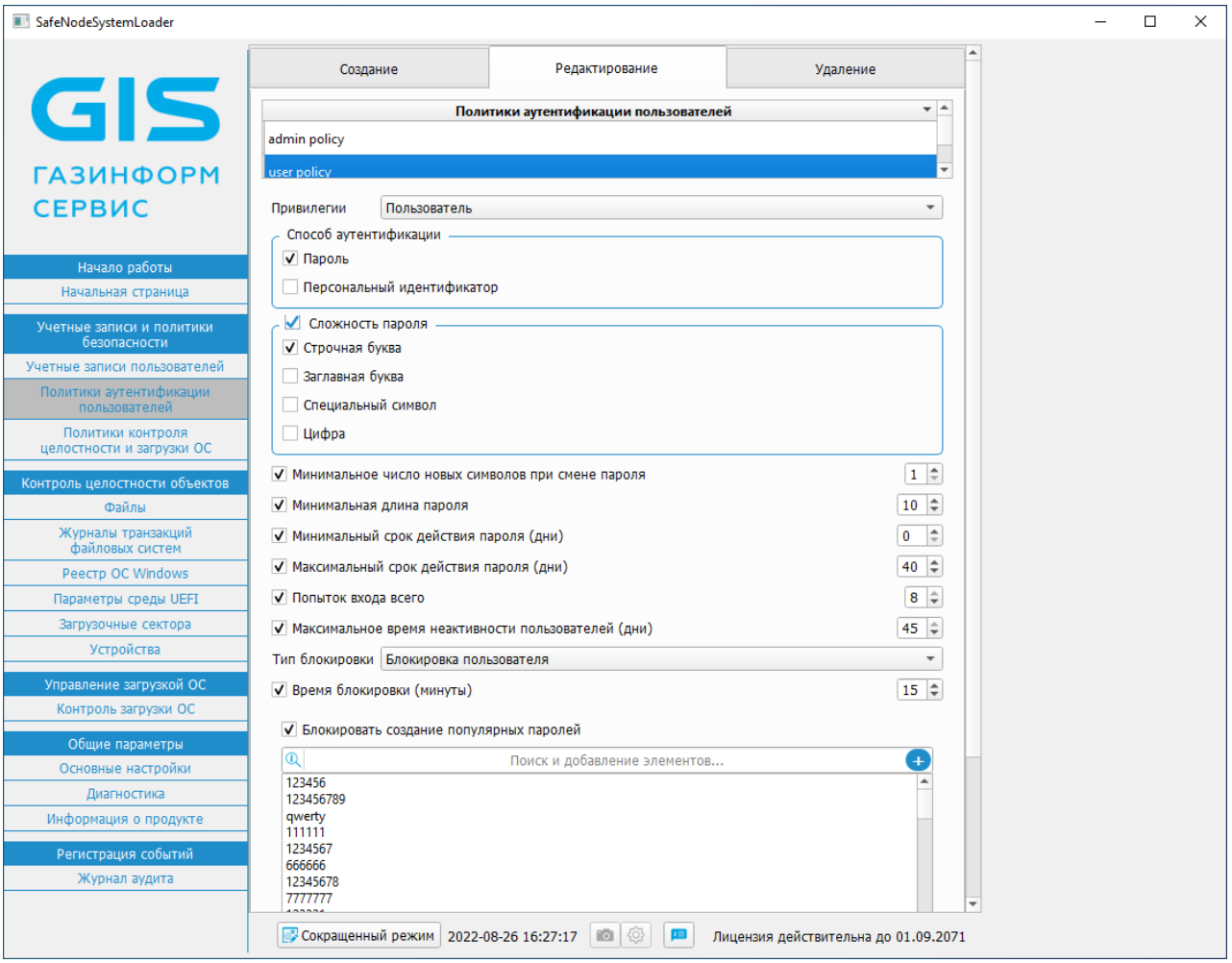


Рисунок 8.7 – Редактирование политики аутентификации пользователей

8.2.3 Доступные для редактирования параметры политики аутентификации пользователя (рисунок 8.7) и их значения приведены в таблице 8.1.

8.2.4 Для сохранения изменений редактируемой политики аутентификации необходимо нажать кнопку ***«Сохранить изменения»*** (рисунок 8.7). При этом на экране ЭВМ появится новое диалоговое окно, в котором необходимо подтвердить изменения, внесенные в политику (рисунок 8.8).

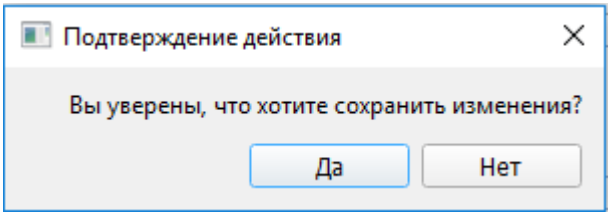


Рисунок 8.8 – Подтверждение сохранения изменений

8.2.5 Успешное изменение политики аутентификации подтверждается сообщением в новом диалоговом окне (рисунок 8.9).

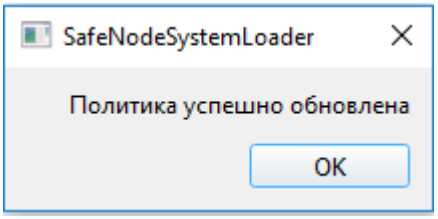


Рисунок 8.9 – Успешное обновление политики

8.3 Удаление политики аутентификации пользователей

8.3.1 Для удаления существующей политики аутентификации пользователей необходимо выбрать в главном окне (рисунок 4.2) подпункт меню ***«Политики аутентификации пользователей»***.

8.3.2 В появившемся диалоговом окне АБ необходимо перейти во вкладку ***«Удаление»*** (рисунок 8.10) и выбрать имя удаляемой политики аутентификации пользователей. При этом на экране ЭВМ появится диалоговое окно, в котором необходимо подтвердить удаление выбранной политики (рисунок 8.11).

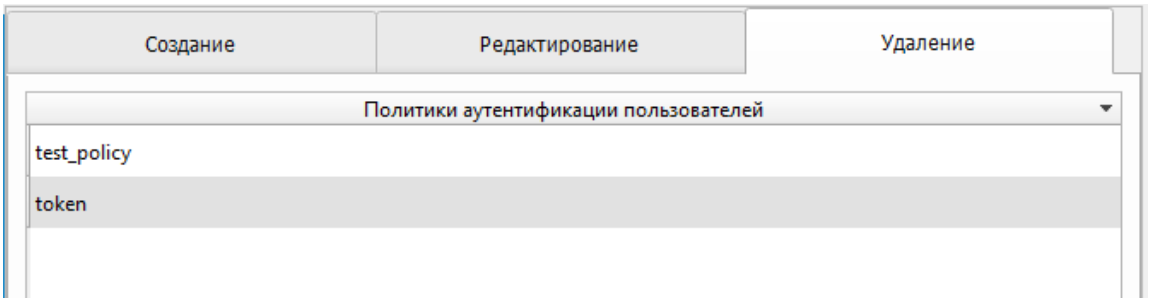


Рисунок 8.10 – Диалоговое окно для удаления политики аутентификации

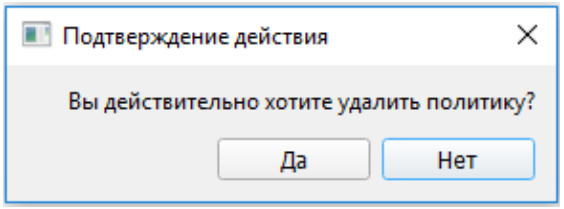


Рисунок 8.11 – Подтверждение удаления политики аутентификации пользователей

Удаление политик аутентификации производится поочередно.

Политики ***admin policy***, ***user policy*** и ***domain policy*** являются предустановленными и недоступны для удаления.

8.3.3 Успешное удаление политики аутентификации пользователей подтверждается сообщением в новом диалоговом окне (рисунок 8.12).

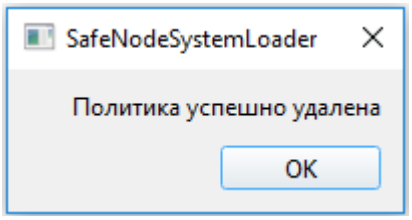


Рисунок 8.12 – Успешное удаление политики аутентификации пользователей

Если политика аутентификации была назначена хотя бы одной учетной записи пользователя, то удаление выполнено не будет и на экран ЭВМ будет выведено сообщение: ***«Операция не выполнена. На данную политику ссылаются некоторые учетные записи пользователей»*** (рисунок 8.13).

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.

Далее действия по удалению политики необходимо повторить.

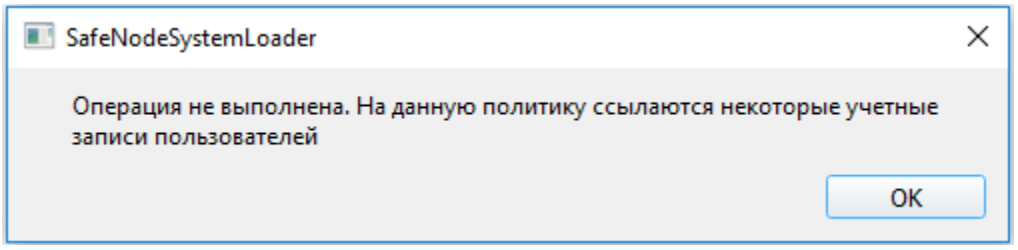


Рисунок 8.13 – Ошибка при удалении политики аутентификации пользователей

9 Управление учетными записями пользователей

9.1 Создание учетной записи пользователя

9.1.1 Для создания новой учетной записи пользователя необходимо выбрать в главном окне консоли АБ Windows (рисунок 4.2) подпункт меню «***Учетные записи пользователей»***.

9.1.2 В появившемся диалоговом окне во вкладке ***«Создание»*** (рисунок 9.1) АБ необходимо указать все требуемые параметры для создания учетной записи пользователя.

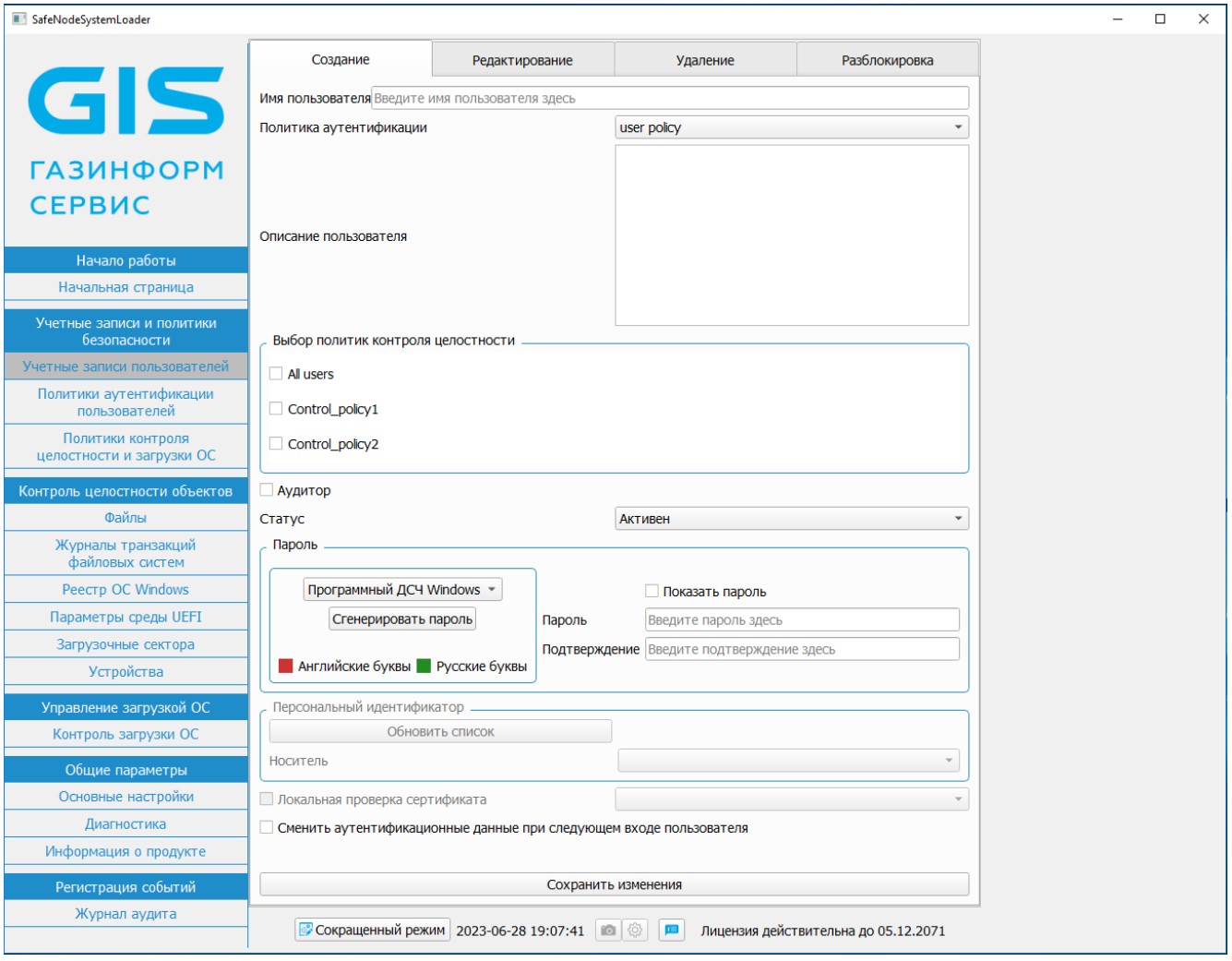


Рисунок 9.1 – Создание учетной записи пользователя

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

9.1.4 Сложность пароля или PIN-кода аутентификационных носителей пользователей (АНП) определяется путем использования в нем сочетания заглавных букв, строчных букв, цифр и специальных символов из определенного разработчиком алфавита пароля, приведенного в таблице 9.2.

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; 2) остальные символы не могут специальными символами
2	Политика аутентификации	Введенное значение [user policy]	Указание названия политики аутентификации, по правилам которой будет обрабатываться данная учетная запись пользователя
3	Описание пользователя	Произвольная текстовая строка	Поле предназначено для формирования описания учетной записи пользователя. Максимальная длина поля –48 символов.
4	Выбор политик контроля целостности	Введенное значение	Выбор политики КЦ и загрузки ОС, по правилам которой будет обрабатываться данная учетная запись пользователя
5	Аудитор	[Отключен] Включен	При назначении прав аудитора пользователю предоставляется дополнительная возможность просмотра и экспорта журнала аудита без его очистки
6	Статус	[Активен] Заблокирован	С помощью данного параметра осуществляется блокировка и разблокировка учетных записей пользователей, за исключением учетной записи АБ
Раздел «Пароль»			
7	Генерация пароля	Сгенерированное значение пароля	Поле предназначено для генерации пароля с использованием программного датчика случайных чисел. Активизируется при нажатии кнопки ***«Сгенерировать пароль»***
8	Пароль	Значение пароля	Поле предназначено для установки пароля.

№	Наименование поля	Возможные значения поля [по умолчанию]	Примечание
			Допускается использование символов из таблицы 9.2.
9	Подтверждение	Значение пароля	Поле предназначено для подтверждения введенного пароля
10	Показать пароль		Поле предназначено для отображения символов вводимого пароля
Раздел «Персональный идентификатор»			
11	Обновить список		Кнопка предназначена для обновления списка АНП
12	Персональный идентификатор	Присвоенный персональный идентификатор	Поле предназначено для выбора и установки АНП
13	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: При изменении сертификата для входа на АНП необходимо повторно назначить носитель пользователю!
14	Сменить аутентификационные данные при следующем входе пользователя	[Включено] Отключено	Принудительное изменение аутентификационных данных пользователя при его первой успешной аутентификации

Таблица 9.2 – Алфавит пароля и PIN-кодов АНП

№	Наименование	Допустимые символы	Количество символов, шт.
1	Заглавные буквы	A…Z	26
		А…Я	33
2	Строчные буквы	a…z	26

№	Наименование	Допустимые символы	Количество символов, шт.
		a…я	33
3	Цифры	0…9	10
4	Специальные символы	! @ # $ % ^ & * ( ) _	11
Итого:			**139**

9.1.5 В поле ***«Политика аутентификации»*** (рисунок 9.1) необходимо выбрать имя ранее созданной политики аутентификации пользователей (рисунок 9.2).

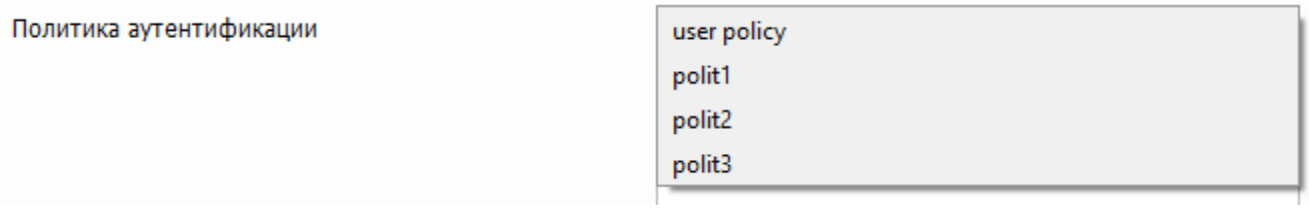


Рисунок 9.2 – Выбор политики аутентификации пользователей

9.1.6 В области ***«Выбор политик контроля целостности»*** (рисунок 9.3) необходимо выбрать имя одной или нескольких ранее созданных политик КЦ объектов и загрузки ОС.

Рисунок 9.3 – Выбор политики КЦ и загрузки ОС

9.1.7 В области ***«Персональный идентификатор»*** осуществляется назначение пользователю АНП для использования его в качестве средства аутентификации.

Один АНП можно назначить нескольким пользователям в качестве персонального носителя для прохождения процедуры аутентификации.

9.1.8 Список PIN-кодов пользователя и администратора АНП, назначенных по умолчанию, и информация по установке необходимых PKI-клиентов приведена в пунктах 5.3.4 и 5.3.5 документа «Средство доверенной загрузки «SafeNode System Loader».

Руководство по эксплуатации. Часть 2. Руководство администратора. ГМТК.468269.060РЭ2».

9.1.9 Перечень идентификаторов, управление которыми доступно из консоли АБ, изменяется в зависимости от варианта исполнения консоли, поэтому при работе с персональными идентификаторами следует использовать сведения таблицы 9.3.

Таблица 9.3 – Управление АНП из различных вариантов исполнения консоли

№ п/п.	Наименование АНП	UEFI	Linux	Windows	Примечание
Устройства JaCarta					
1	JaCarta PKI	+	+	+	
2	JaCarta ГОСТ (USB-носитель и смарт-карта)	+	+	+	
3	JaCarta PKI/ГОСТ	+	+	+	
4	JaCarta-2 ГОСТ (USB-носитель и смарт-карта)	+	–	+	Недоступно управление в консоли АБ Linux
5	JaCarta SF/ГОСТ	+	–	+	Недоступно управление в консоли АБ Linux
Устройства Рутокен					
6	Рутокен ЭЦП	+	+	+	
7	Рутокен ЭЦП 2.0 (USB-носитель и смарт-карта)	+	+	+	
8	Рутокен ЭЦП 3.0 (USB-носитель и смарт-карта)	+	+	+	
9	Рутокен Lite	+	+	+	
10	Рутокен 2151	+	–	+	Недоступно управление в консоли АБ Linux
11	Рутокен ЭЦП PKI (смарт-карта)	+	+	+	
Устройства eToken					
12	eToken Pro Java	+	+	+	
13	SafeNet eToken 5100	+	+	+	
14	SafeNet eToken 5105	+	+	+	
15	SafeNet eToken 5200	+	+	+	
16	SafeNet eToken 5205	+	+	+	

9.1.10 В случае, если при указании пароля пользователя будет использовано выражение из перечня популярных паролей[1], будет выведено соответствующее предупреждение (рисунок 9.4). Необходимо указать другой пароль для использования.

[1] При условии, что в используемой политике аутентификации активировано поле ***«Блокировать создание популярных паролей».***

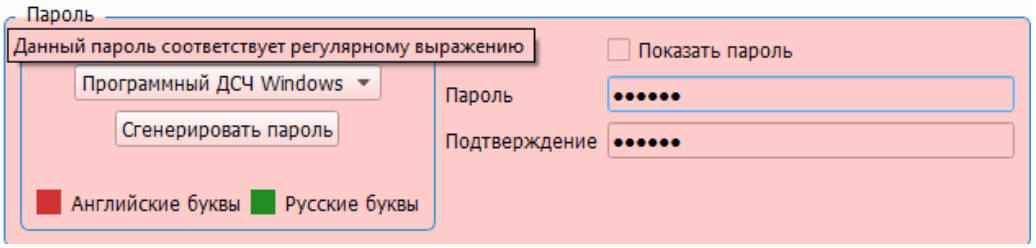


Рисунок 9.4 – Совпадение указанного пароля с перечнем популярных

9.1.11 После установки полей для сохранения изменений в создаваемой учетной записи пользователя АБ необходимо нажать на кнопку ***«Сохранить изменения»*** (рисунок 9.1), при этом на экране ЭВМ появится новое диалоговое окно, в котором необходимо подтвердить создание учетной записи пользователя (рисунок 9.5).

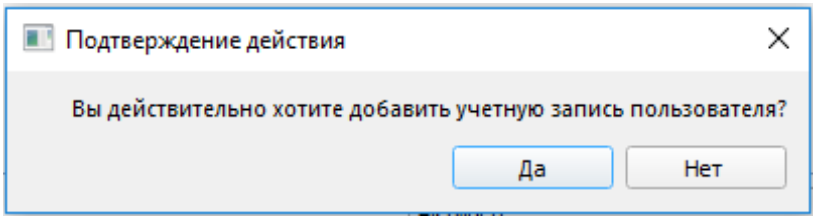


Рисунок 9.5 – Подтверждение добавления учетной записи пользователя

9.1.12 Успешное создание учетной записи пользователя подтверждается сообщением (рисунок 9.6).

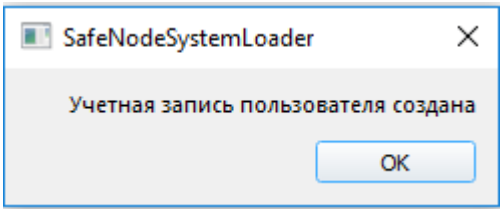


Рисунок 9.6 – Успешное создание учетной записи пользователя

9.1.13 В случае, если какое-либо из обязательных полей не было заполнено, появится сообщение с предупреждением, при этом не заполненный параметр будет подсвечен красным цветом (рисунок 9.7).

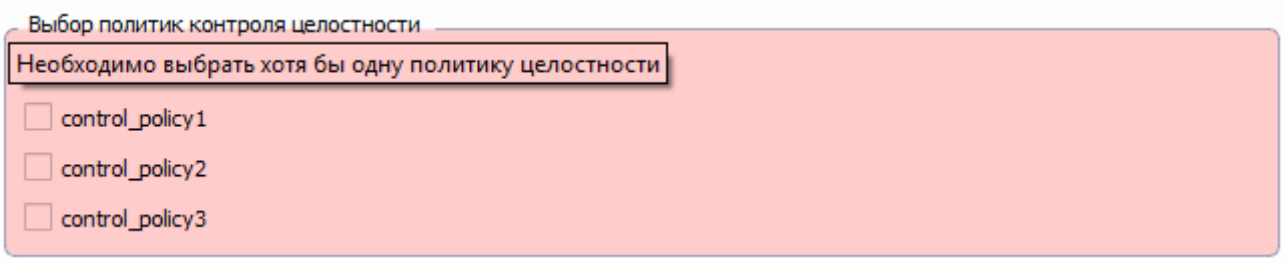


Рисунок 9.7 – Ошибка при сохранении учетной записи пользователя

9.2 Редактирование учетной записи пользователя

9.2.1 Для редактирования существующей учетной записи пользователя необходимо выбрать в главном окне (рисунок 4.2) подпункт меню ***«Учетные записи пользователей»***.

9.2.2 В появившемся диалоговом окне АБ необходимо перейти во вкладку ***«Редактирование»*** (рисунок 9.8) и выбрать имя редактируемой учетной записи пользователя. При этом в нижней части окна отобразятся доступные для редактирования параметры учетной записи пользователя (рисунок 9.9).

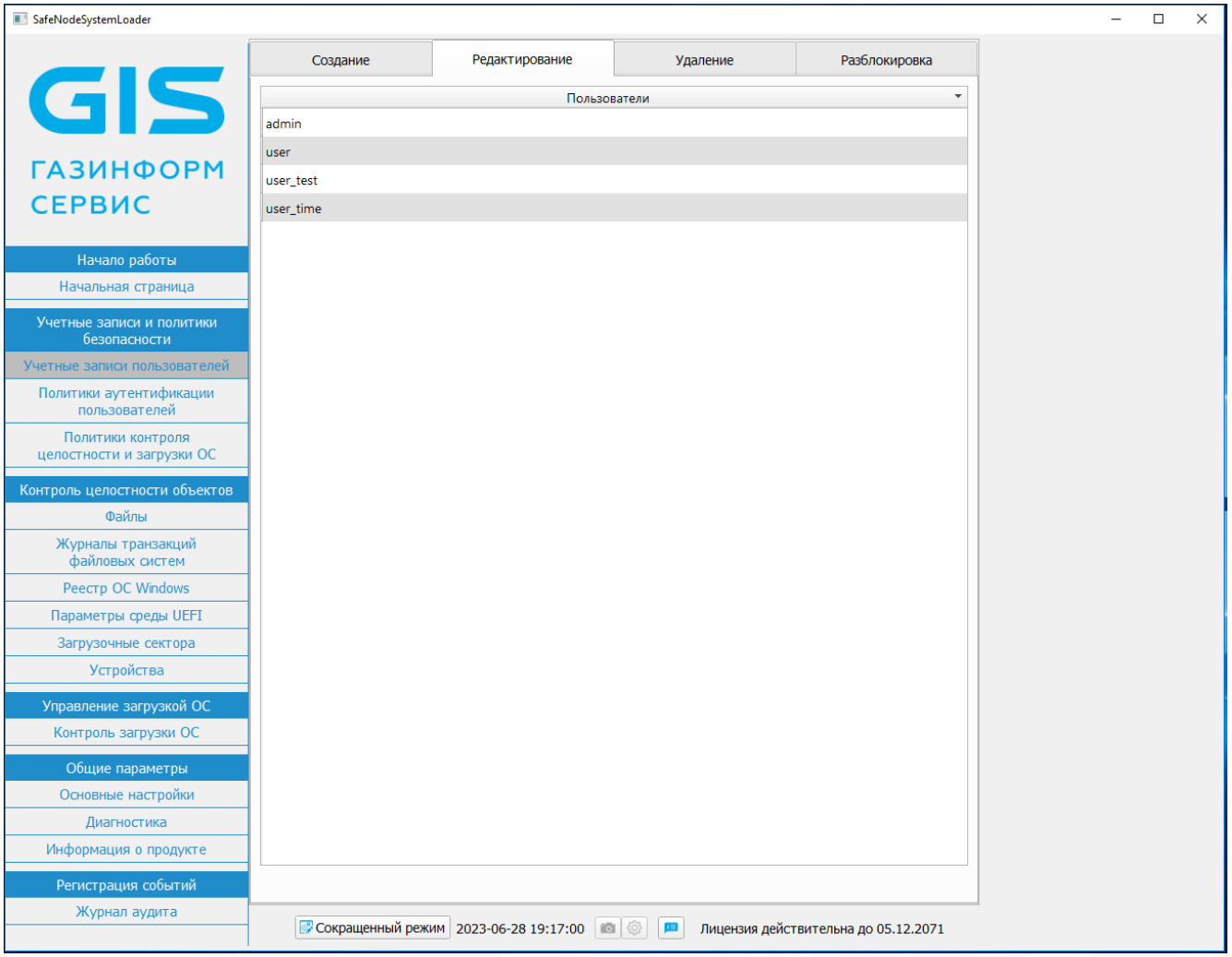


Рисунок 9.8 – Список доступных для редактирования учетных записей пользователей

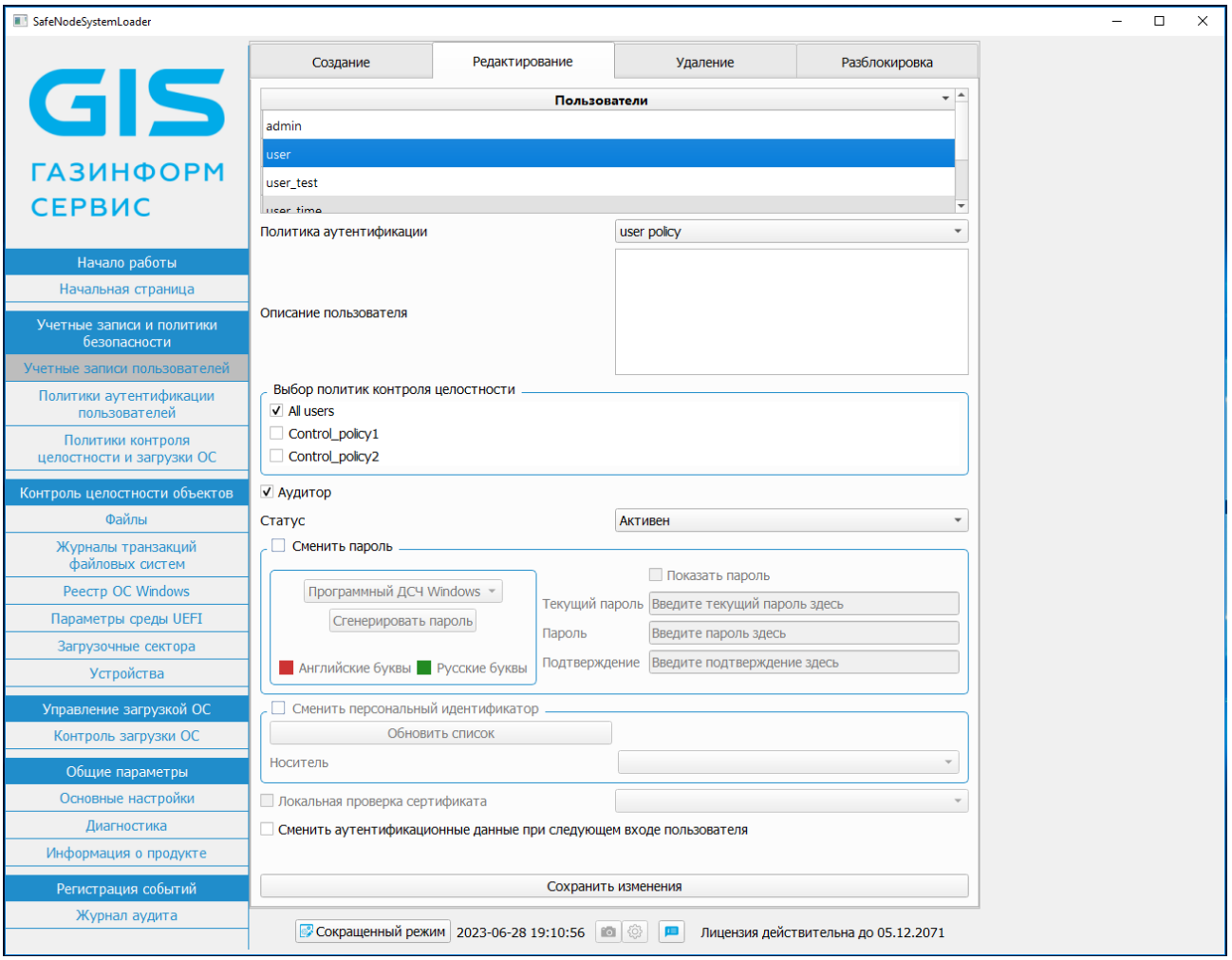


Рисунок 9.9 – Редактирование учетной записи пользователя

9.2.3 Доступные для редактирования параметры учетной записи пользователя (рисунок 9.9) и их значения приведены в таблице 9.1.

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

9.2.4 Для сохранения изменений редактируемой учетной записи пользователя необходимо нажать на кнопку ***«Сохранить изменения»*** (рисунок 9.9). При этом на экране ЭВМ появится новое диалоговое окно, в котором необходимо подтвердить изменения, внесенные в учетную запись пользователя (рисунок 9.10).

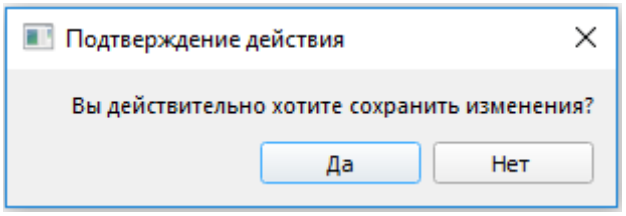


Рисунок 9.10 – Подтверждение изменений учетной записи пользователя

9.2.5 Успешное изменение учетной записи пользователя подтверждается сообщением в новом диалоговом окне (рисунок 9.11).

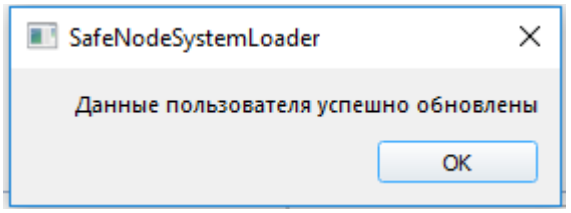


Рисунок 9.11 – Успешное изменение учетной записи пользователя

9.3 Назначение мастер-ключа АБ

9.3.1 Мастер ключ администратору безопасности в графической консоли Windows назначается путем редактирования учетной записи АБ. Доступные для редактирования параметры учетной записи пользователя и их значения приведены в таблице 9.1. В отличие от учетной записи пользователя, АБ дополнительно доступно назначение мастер ключа, который в дальнейшем может использоваться для сброса аутентификационных данных.

9.3.2 Для назначения мастер-ключа, необходимо подключить поддерживаемый изделием АНП к ЭВМ. Затем необходимо выбрать в главном окне (рисунок 4.2) подпункт меню ***«Учетные записи пользователей»***.

9.3.3 В появившемся диалоговом окне необходимо перейти во вкладку ***«Редактирование»*** (рисунок 9.8) и выбрать имя редактируемой учетной записи ***admin***. При этом в нижней части окна отобразятся доступные для редактирования параметры учетной записи АБ (рисунок 9.12).

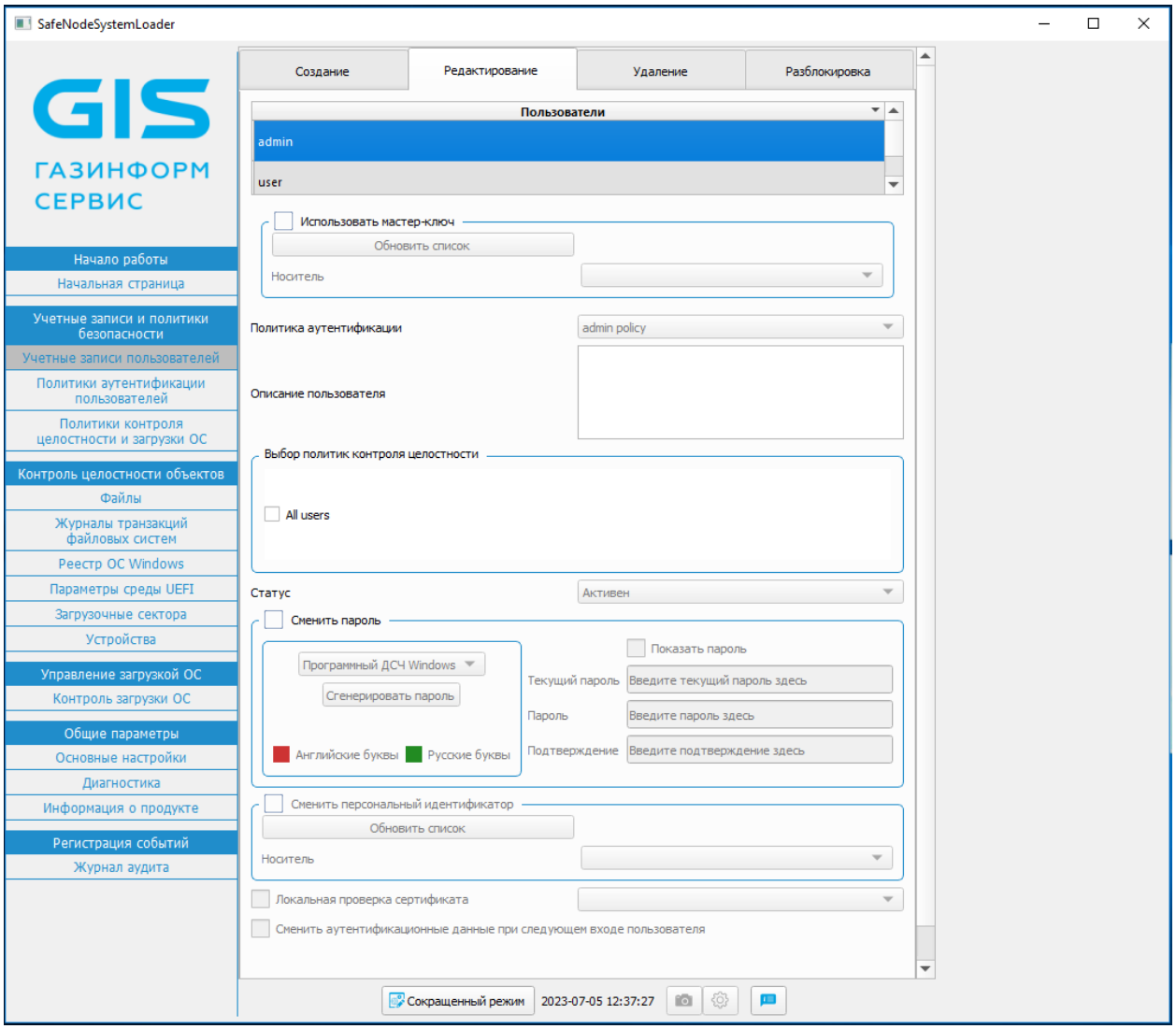


Рисунок 9.12 – Редактирование учетной записи АБ

9.3.4 Активировать поле ***«Использовать мастер-ключ»*** и нажать кнопку ***«Обновить список»***, напротив поля ***«Носитель»*** в выпадающем списке выбрать требуемый АНП для назначения (рисунок 9.13).

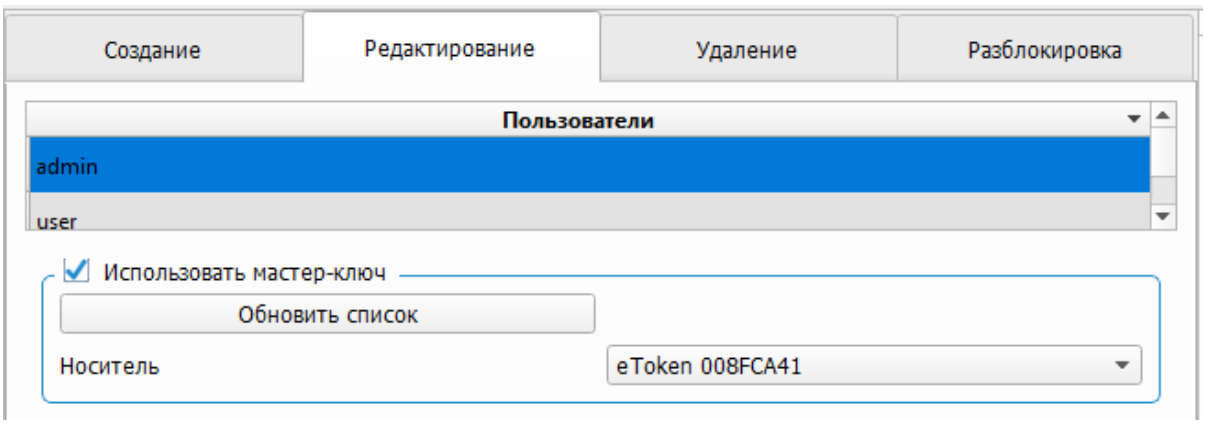


Рисунок 9.13 – Выбор АНП для назначения мастер-ключом

9.3.5 После внесенных изменений В окне редактирования учетной записи нажать кнопку ***«Сохранить изменения»***, в окне подтверждения выбрать ***«Да»*** (рисунок 9.14).

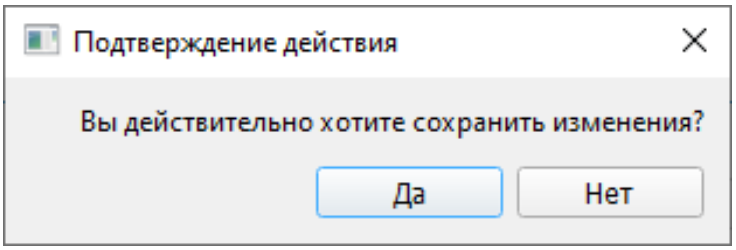


Рисунок 9.14 – Подтверждение внесенных изменений

9.3.6 После подтверждения внесенных изменений появится окно, в котором необходимо указать PIN-код АНП (рисунок 9.15).

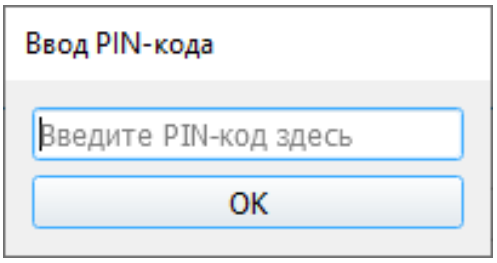


Рисунок 9.15 – Окно ввода PIN-кода

9.3.7 В случае корректно указанного PIN-кода АНП появится сообщение об успешном редактировании учетной записи (рисунок 9.16).

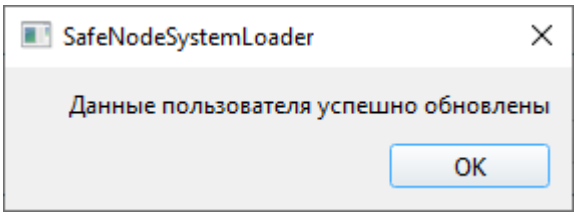


Рисунок 9.16 – Успешное обновление данных пользователя

9.3.8 Назначенный АНП в качестве мастер-ключа можно использовать для сброса аутентификационных данных АБ.

Мастер-ключ используется только для сброса данных.

АНП, выбранный в качестве мастер-ключа, не может быть назначен в качестве АНП для входа пользователя или АБ.

После назначения мастер-ключ можно использовать для сброса аутентификационных данных АБ в любой из консолей изделия: псевдографической и графических консолях СДЗ Windows и Linux.

9.4 Удаление учетной записи пользователя

9.4.1 Для удаления существующей учетной записи пользователя АБ необходимо выбрать в главном окне (рисунок 4.2) подпункт меню ***«Учетные записи пользователей»***.

9.4.2 В появившемся диалоговом окне АБ необходимо перейти во вкладку ***«Удаление»*** (рисунок 9.17) и выбрать имя удаляемой учетной записи пользователя. При этом на экране ЭВМ появится диалоговое окно, в котором необходимо подтвердить удаление выбранной учетной записи (рисунок 9.18).

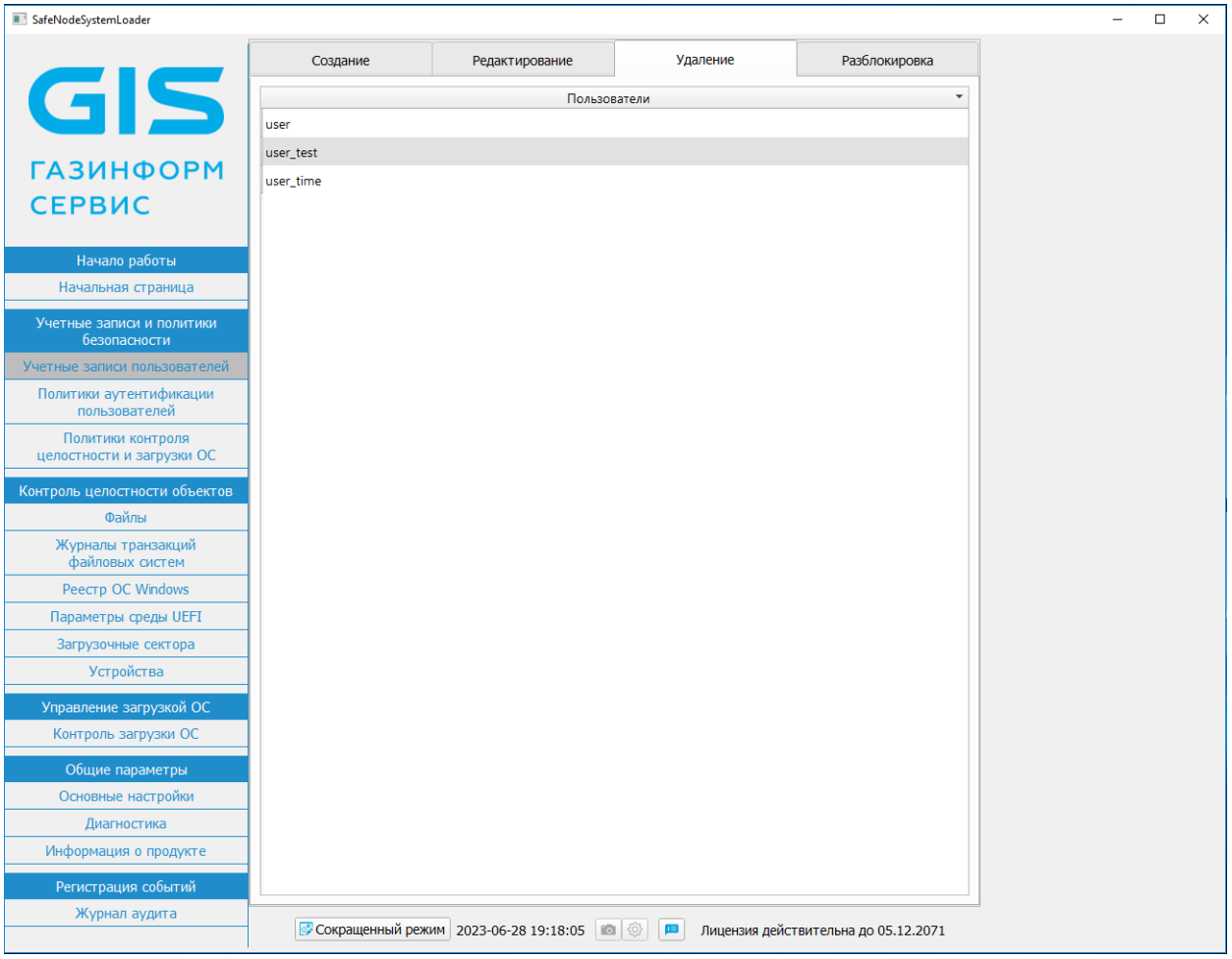


Рисунок 9.17 – Удаление учетной записи пользователя

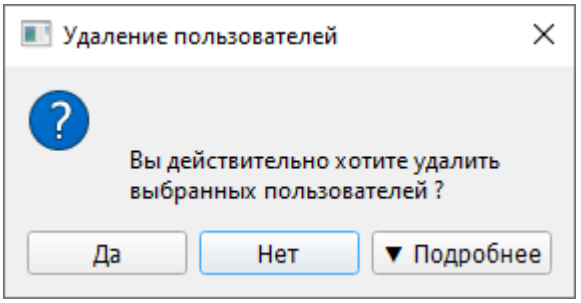


Рисунок 9.18 – Подтверждение удаления учетной записи пользователя

9.4.3 Успешное удаление учетной записи пользователя подтверждается сообщением в новом диалоговом окне (рисунок 9.19).

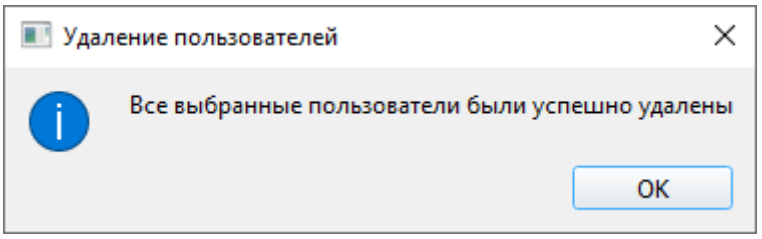


Рисунок 9.19 – Успешное удаление учетной записи пользователя

После удаления учетной записи пользователя из БД изделия исключено ее 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.

10 Общие параметры

Меню ***«Общие параметры»*** в главном окне консоли АБ Windows (рисунок 4.2) предназначено для настройки общих параметров изделия, диагностики изделия и сброса параметров к заводским настройкам.

10.1 Основные настройки: аутентификация, контроль целостности, алгоритмы расчета контрольных сумм, прочие параметры

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

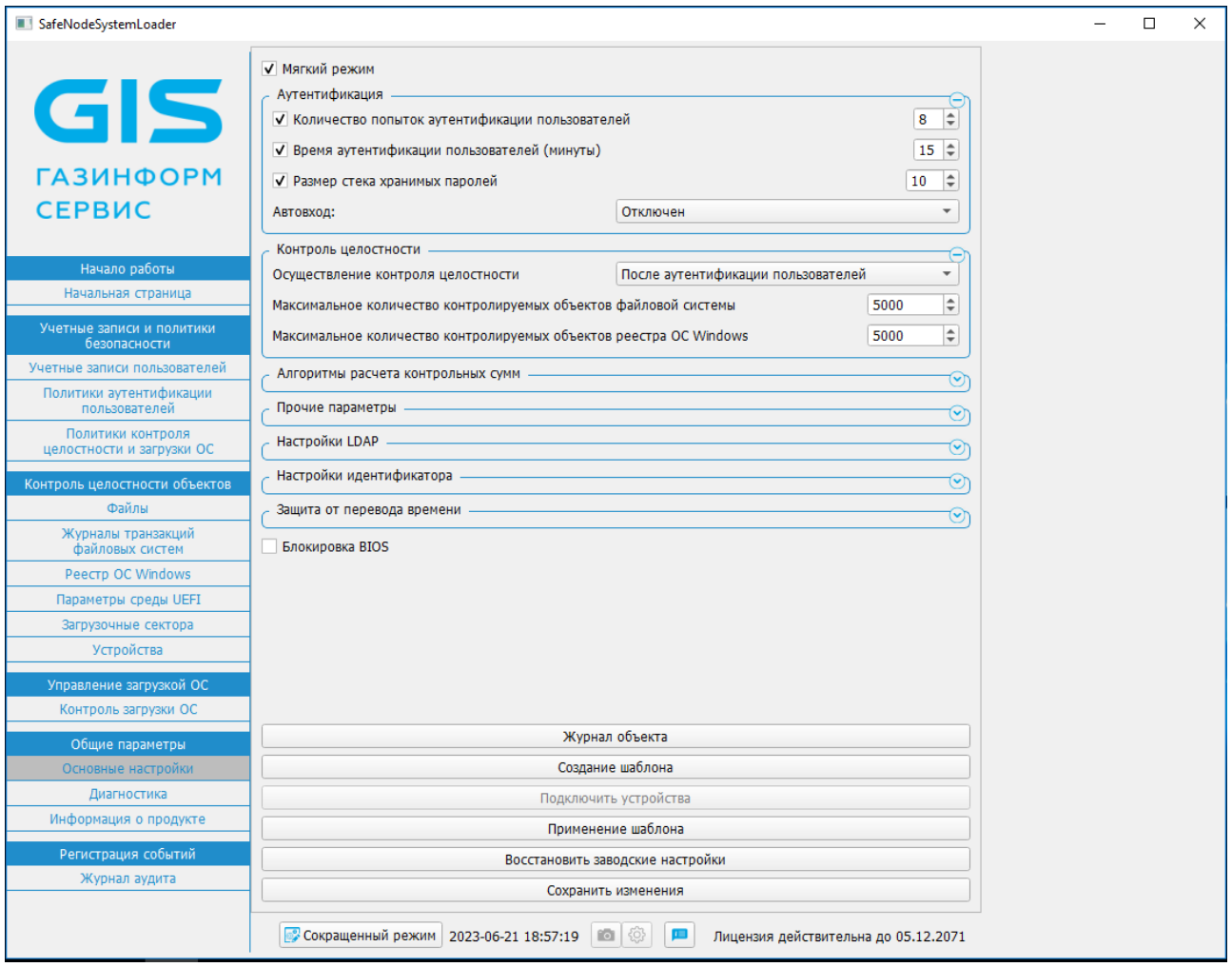


Рисунок 10.1 – Содержимое окна ***«Основные настройки»***

10.1.2 В верхней части окна расположено поле ***«Мягкий режим»***. 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.

Отключение и включение мягкого режима осуществляется по требованию АБ, после первого отключения мягкого режима осуществляется принудительная смена пароля восстановления.

10.1.3 Все разделы, расположенные в окне ***«Основные настройки»***, представлены в виде свернутых списков, для просмотра полного содержимого раздела необходимо открыть соответствующий список.

10.1.4 В таблице 10.1 приведены поля и их возможные значения доступные для настройки в подпункте ***«Основные настройки»*** (рисунок 10.1).

Таблица 10.1 – Возможные значения полей подпункта ***«Основные настройки»***

№	Наименование поля	Возможные значения поля [по умолчанию]	Минимальное … максимальное значения	Примечание
Раздел «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	
4	Автовход	[Отключен] [Учетная запись пользователя]		Возможность указать учетной записи пользователя автоматическую аутентификацию с АНП. Доступно только для одной учетной записи
Раздел «Контроль целостности»				
5	Осуществление контроля целостности	[После аутентификации пользователей] До аутентификации пользователей		
6	Максимальное количество	[5000]	1…9 999 999	

№	Наименование поля	Возможные значения поля [по умолчанию]	Минимальное … максимальное значения	Примечание
	контролируемых объектов файловой системы			
7	Максимальное количество контролируемых объектов реестра ОС Windows	[5000]	1…9 999 999	
Раздел «Алгоритмы расчета контрольных сумм»				
8	Алгоритм расчета контрольных сумм аутентификации пользователей	MD4 [MD5] SHA1 SHA256 SHA384 SHA512		
9	Алгоритм расчета контрольных сумм контроля целостности	MD4 [MD5] SHA1 SHA256 SHA384 SHA512		
Раздел «Прочие параметры»				
10	Количество циклов очистки памяти	[1]	1…5	Количество циклов перезаписи при очистке памяти СДЗ
11	Язык меню	[ru-RU] en-US		Язык отображения меню
12	Максимальное время бездействия администратора (минуты)	[0]	0…30	
13	Интерфейс командной строки	[Включен] Отключен		Установка параметра для работы с командной строкой
14	Реактивация лицензии			Активации нового ключа лицензии
Раздел «Настройки LDAP»				

№	Наименование поля	Возможные значения поля [по умолчанию]	Минимальное … максимальное значения	Примечание
15	Использование сетевой подсистемы	Включена [Отключена]		
16	MAC-адрес	Текущее значение параметра		MAC-адрес сетевой карты ЭВМ
17	Использование статического IP-адреса	Включено [Отключено]		
18	IP-адрес	[0.0.0.0]	0.0.0.0 … 255.255.255.255	
19	Маска подсети	[0.0.0.0]	0.0.0.0 … 255.255.255.255	
20	Основной шлюз	[0.0.0.0]	0.0.0.0 … 255.255.255.255	
21	Аутентификация LDAP	Включена [Отключена]		Установка параметра для аутентификации LDAP
22	Префикс и суффикс пользователей			Уникальное имя учетной записи пользователя
23	Использование Kerberos	Включено [Отключено]		Использование преобразования Kerberos
24	Использование белого списка пользователей	Включено [Отключено]		
25	Редактирование файла hosts			
26	Редактирование файла krb5.conf			
27	Редактирование файла ldap.conf			
28	Редактирование списка пользователей			Добавление или удаление доменных пользователей в систему и формирование белого списка доменных пользователей

№	Наименование поля	Возможные значения поля [по умолчанию]	Минимальное … максимальное значения	Примечание
Раздел «Настройки идентификатора» [2]				
29	Кнопка 			Кнопка предназначена для обновления списка АНП
30	Выбор			Поле выбора АНП из списка
31	Смена PIN-кода			Смена PIN-кода АНП
32	Пароль восстановления			Поле для смены пароля восстановления. Максимальное количество символов 32
33	Кнопка 			Кнопка предназначена для отображения действительного значения вводимого пароля восстановления
34	Кнопка «Установить»			Устанавливает введенное значение пароля восстановление
Раздел «Защита от перевода времени»				
35	Включить защиту	Включение Отключение		Включение/выключение защиты от перевода пользователем времени назад
36	Допустимый сдвиг (часы)	1	1 … 24	Максимально допустимый сдвиг по времени в часах в пределах которого нарушение не регистрируется
37	[Блокировка пользователя] Запись в журнал Временная блокировка пользователя			Тип блокировки при обнаружении нарушения

[2] Данный раздел меню предназначен для смены PIN-кода АНП без использования сторонних утилит производителей идентификаторов.

№	Наименование поля	Возможные значения поля [по умолчанию]	Минимальное … максимальное значения	Примечание
	Блокировка группы пользователя Блокировка всех пользователей			
Прочие параметры				
38	Блокировка BIOS	Установка запрета перезаписи UEFI BIOS ЭВМ в обход изделия		
39	Журнал объекта	Предназначено для генерации отчета о произведенных настройках безопасности на объекте информатизации		
40	Создание шаблона	Предназначено для создания шаблона с установленными и настроенными параметрами политик безопасности		
41	Подключить устройства	Подключение внешнего носителя информации для сохранения снимков экрана[3]		
42	Применение шаблона	Предназначено для применения шаблона с установленными и настроенными параметрами политик безопасности		
43	Восстановить заводские настройки	Восстановление параметров изделия до заводских настроек		
44	Сохранить изменения	Сохранение внесенных в настройки изменений		

10.1.5 После внесения изменений в разделы ***«Алгоритмы расчета контрольных сумм»***, ***«Контроль целостности»***, ***«Аутентификация»*** и ***«Прочие параметры»*** для сохранения выбранных значений необходимо нажать кнопку ***«Сохранить изменения»*** (рисунок 10.1). При этом в новом диалоговом окне будет выведено сообщение об успешном изменении настроек (рисунок 10.2).

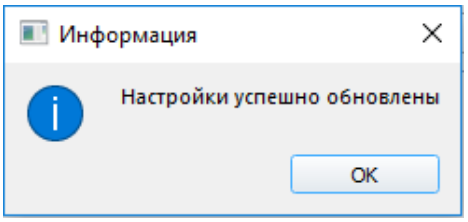


Рисунок 10.2 – Успешное изменение настроек

[3] Доступно только в консоли АБ Linux.

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

10.2 Настройки LDAP

Пункт ***«Настройки LDAP»*** предназначен для установки сетевых настроек ЭВМ, на которой установлено изделие, и адреса 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 LDAP указать необходимость активации преобразования TLS.**

10.2.1 Для осуществления настройки параметров сети на ЭВМ необходимо в разделе ***«Основные настройки»*** раскрыть пункт ***«Настройки LDAP»*** (рисунок 10.3).

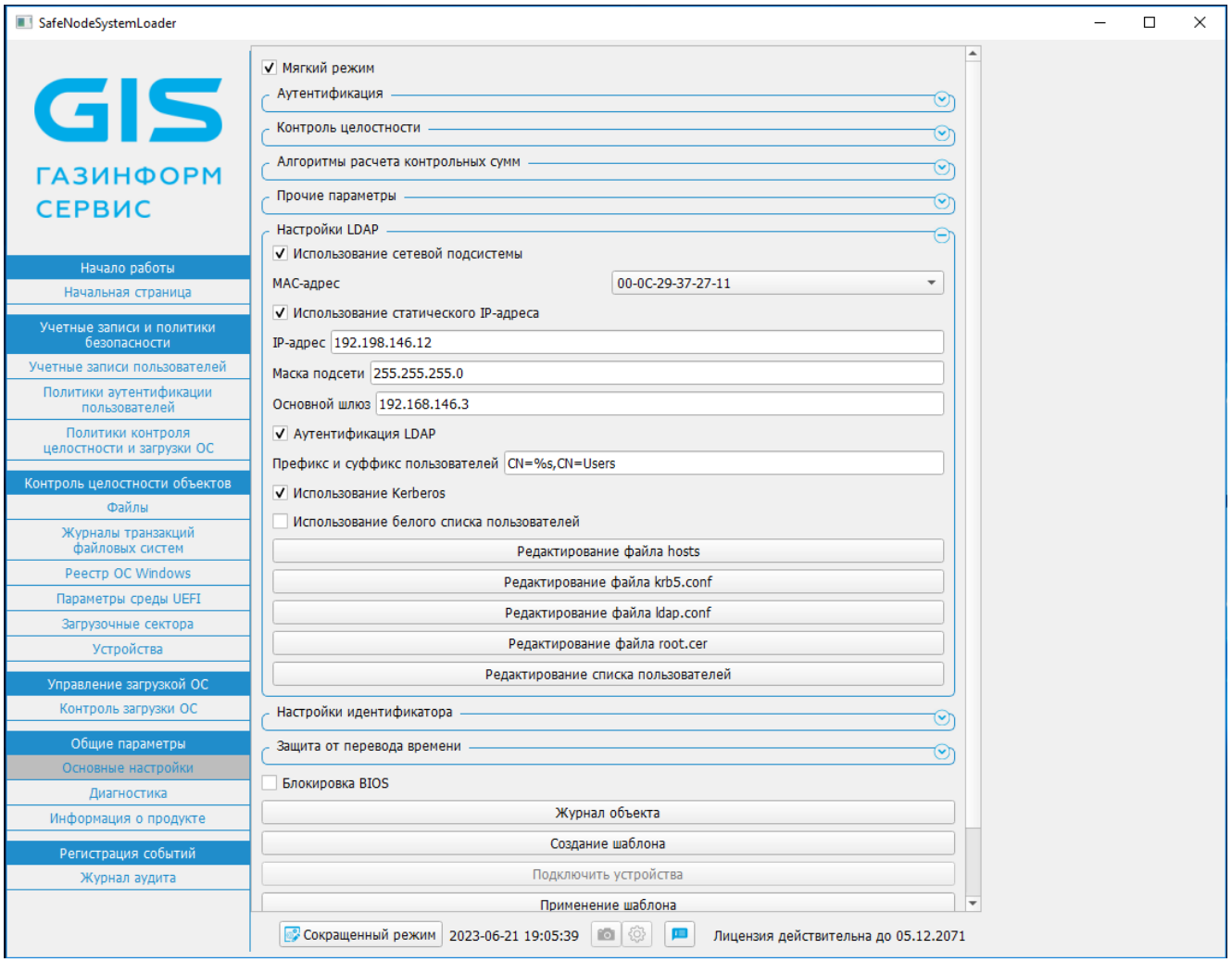


Рисунок 10.3 – Настройка параметров сети и LDAP

10.2.2 Для настройки сетевых параметров ЭВМ, на которой установлено изделие, необходимо включить взаимодействие по сети, установив отметку в поле ***«Использование сетевой подсистемы»***.

10.2.3 В поле ***«MAC»*** автоматически будет установлен MAC-адрес сетевой карты ЭВМ, данный параметр не подлежит изменению.

10.2.4 Параметр ***«Использование статического IP-адреса»*** позволяет указать способ получения сетевых настроек – статически или динамически. При установке отметки в поле ***«Использование статического IP-адреса»***, поля ***«IP-адрес»***, ***«Маска подсети»*** и ***«Основной шлюз»*** необходимо заполнить вручную. При снятии отметки (используется динамический IP -адрес) – данные поля заполняются автоматически.

10.2.5 После конфигурирования сетевых настроек ЭВМ необходимо указать настройки LDAP сервера. Для включения параметра аутентификации LDAP необходимо установить отметку в поле ***«Аутентификация LDAP***».

10.2.6 Поле ***«Префикс и суффикс пользователей»*** (рисунок 10.3) предназначено для установки уникального имени (DN) учетной записи пользователя, состоящего из префикса и суффикса и определяющего имя и домен для аутентификации пользователей (формат ввода учетной записи пользователя приведен на рисунке 10.3).

10.2.7 Для аутентификации пользователей с сервером LDAP по протоколу Kerberos следует перейти в поле ***«Использование Kerberos»*** и установить отметку.

10.2.8 Для формирования белого списка доменных пользователей следует перейти в поле ***«Использование белого списка пользователей»*** и установить отметку.

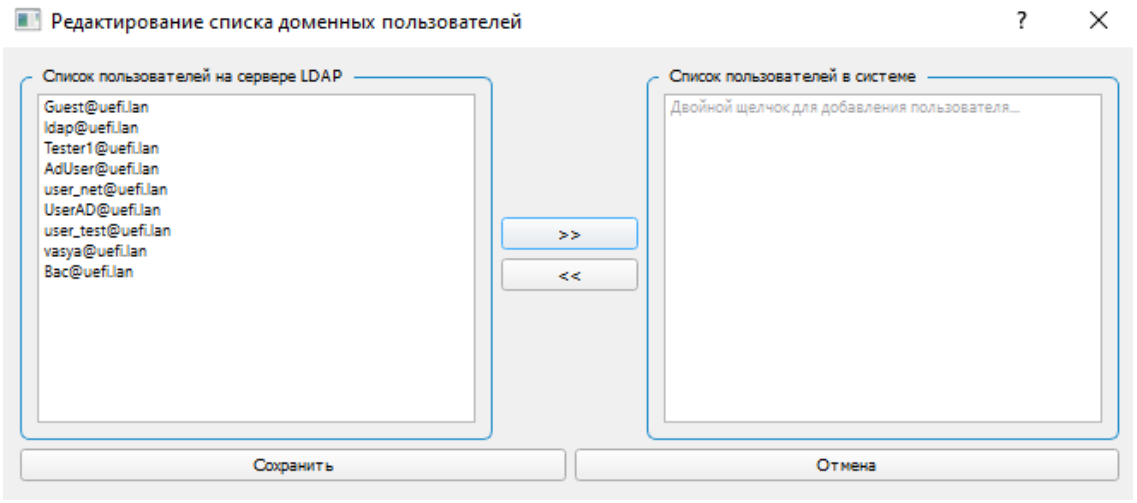
10.2.9 При включении аутентификации LDAP[4] устанавливается полное доверие LDAP серверу: при успешной аутентификации пользователя в изделии с учетной записью, зарегистрированной на LDAP сервере, автоматически создается учетная запись в БД изделия. Пользователю назначается политика аутентификации ***«domain policy»*** и политика контроля целостности и ОС ***«All users»***.

В случае отсутствия сетевого соединения при указанных параметрах аутентификации LDAP работа изделия осуществляется в автономном режиме. При этом если аутентификация учетной записи пользователя, зарегистрированной на сервере LDAP, была выполнена ранее, вход будет осуществлен по последнему паролю, введенному при наличии сетевого подключения и сохраненному в БД изделия.

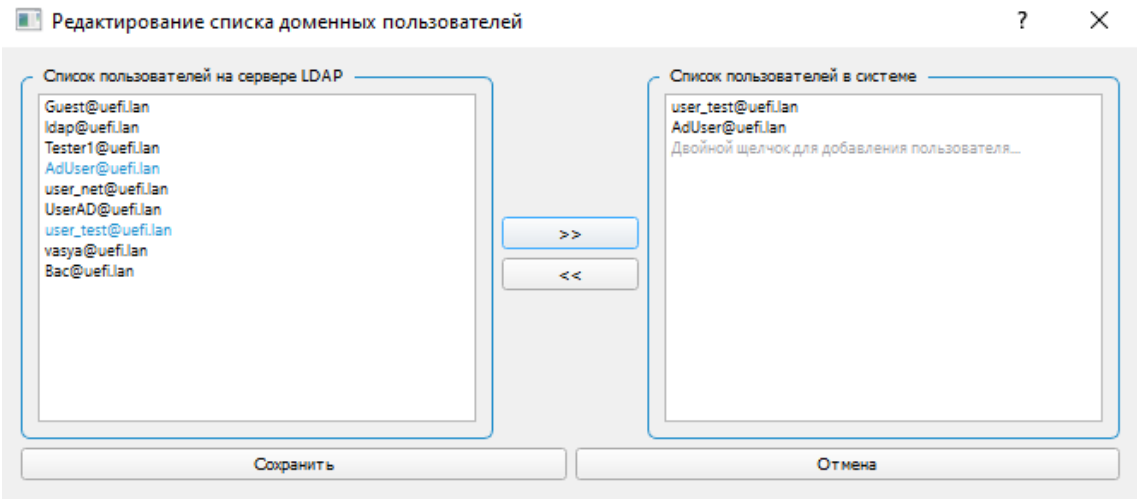
10.2.10 Для формирования белого списка доменных пользователей необходимо выбрать поле ***«Редактирование списка пользователей»*** (рисунок 10.3). В появившемся диалоговом окне (рисунок 10.4) необходимо выбрать доменных пользователей для добавления в систему или удаления из нее. [5]

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

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



а)



б)

Рисунок 10.4 – Редактирование белого списка пользователей

10.2.11 В консоли реализована возможность редактирования конфигурационных файлов ***hosts***, ***krb5.conf*** и ***ldap.conf***. Необходимо выбрать конфигурационный файл для редактирования и нажать соответствующую кнопку, например, ***«Редактирование файла hosts»*** (рисунок 10.5).

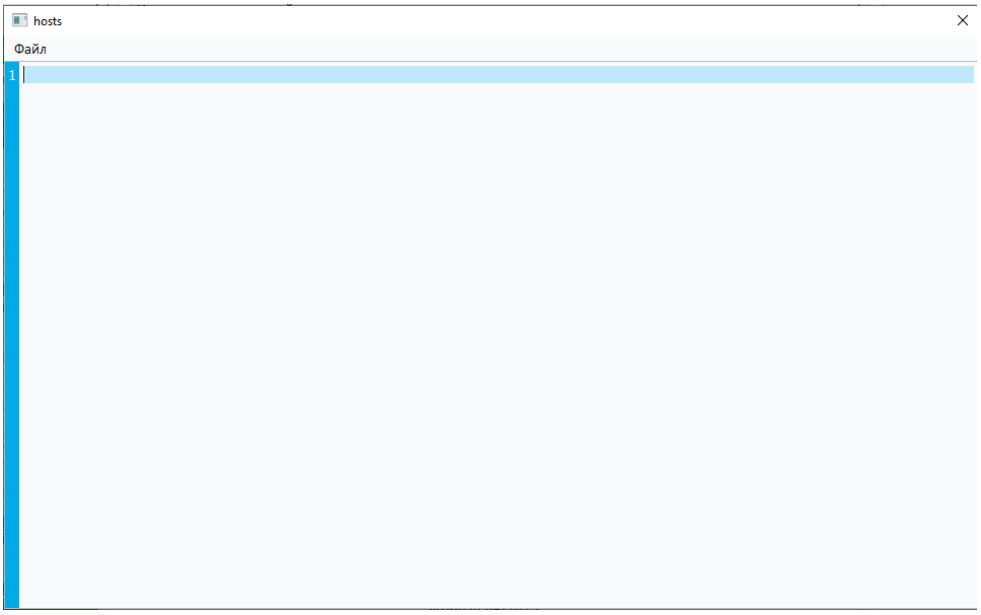


Рисунок 10.5 – Открытие окна «Редактирование файла host»

10.2.12 Откроется окно для внесения соответствующих настроек. С помощью меню файл (рисунок 10.5) доступно сохранение, загрузка примера или закрытие окна (рисунок 10.6).

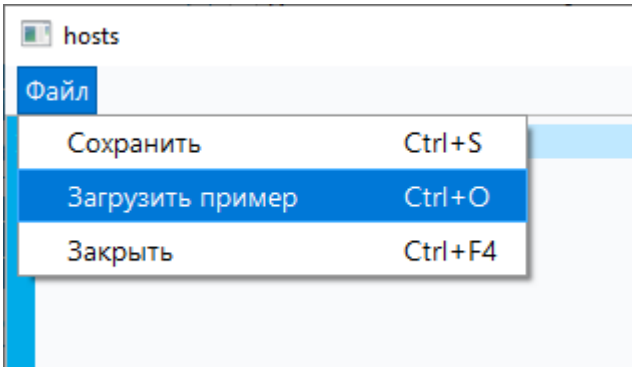


Рисунок 10.6 – Меню диалогового окна «Редактирование файла host»

10.2.13 С помощью пункта меню «Загрузить пример» загрузится шаблон для внесения изменений в соответствии с требуемыми сетевыми настройками (рисунок 10.7).

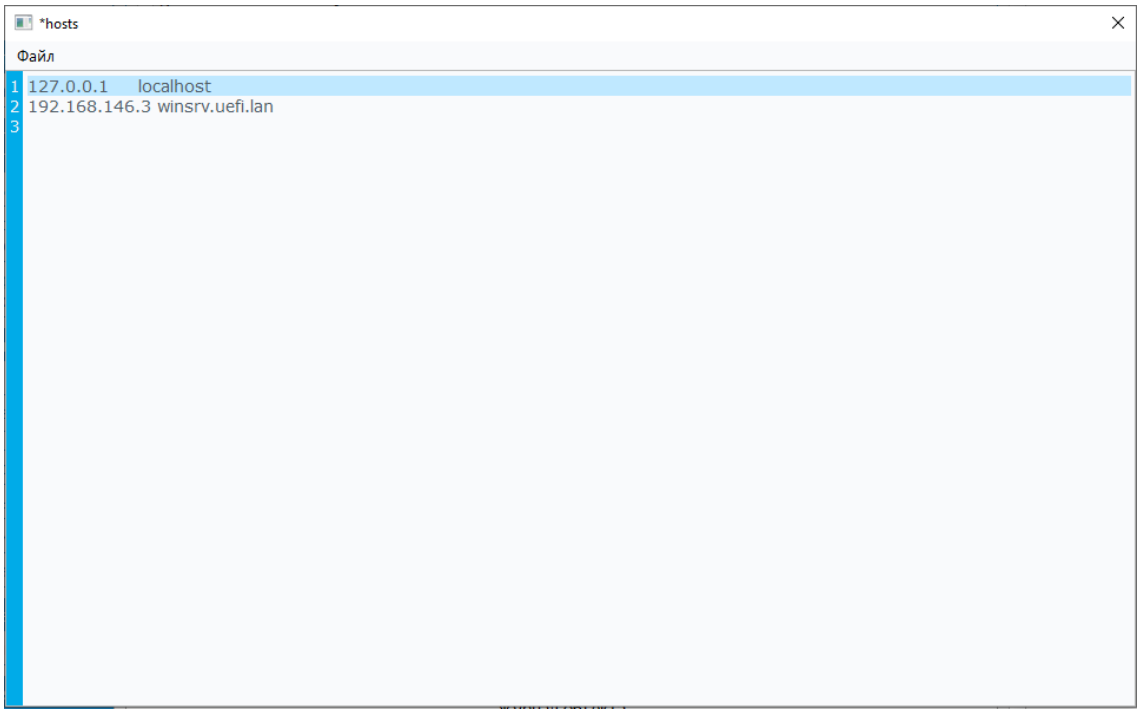


Рисунок 10.7 – Загрузка примера для редактирования

10.2.14 После внесения соответствующих изменений необходимо выбрать ***Файл*** → ***Сохранить***, а затем закрыть окно. Необходимые изменения будут сохранены.

10.2.15 Для сохранения выбранных значений необходимо нажать кнопку ***«Сохранить изменения»*** (рисунок 10.3). При этом в новом диалоговом окне будет выведено сообщение об успешном изменении настроек (рисунок 10.2).

10.2.16 В Приложение Д текущего документа приведена настройка поддержки списка отозванных сертификатов при аутентификации в домене.

10.3 Журнал объекта

10.3.1 В изделии присутствует возможность получения данных о настройках политик безопасности, установленных на ЭВМ. Для этого необходимо выбрать кнопку ***«Журнал объекта»*** и дождаться появления диалогового окна (рисунок 10.8).

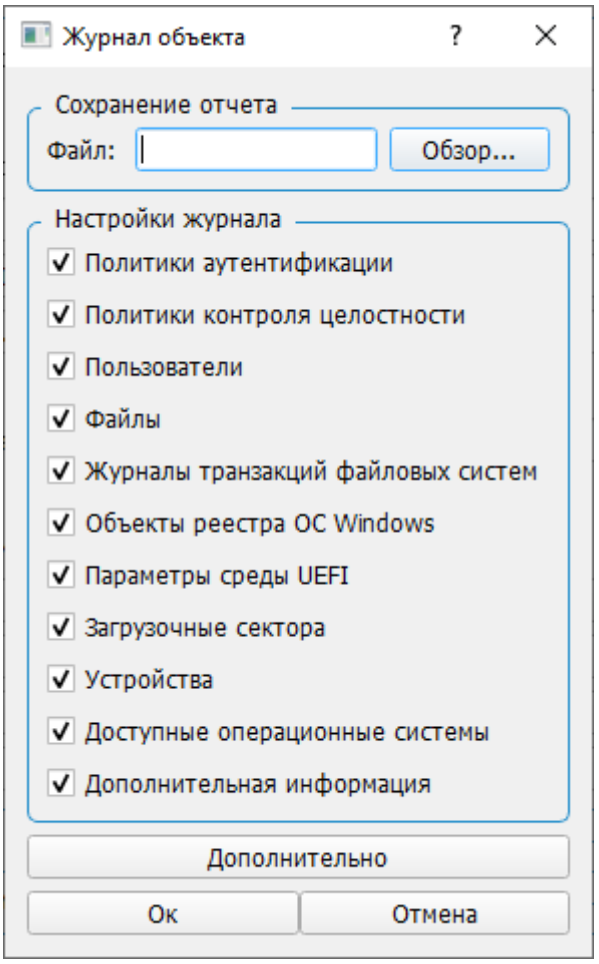


Рисунок 10.8 – Журнал объекта

10.3.2 В зависимости от установленных опций отчет будет содержать сведения о контролируемых объектах и настройках политик безопасности (рисунок 10.8). Для добавления информации об АРМ пользователя необходимо воспользоваться кнопкой ***«Дополнительно»*** (рисунок 10.9) и заполнить требуемые поля.

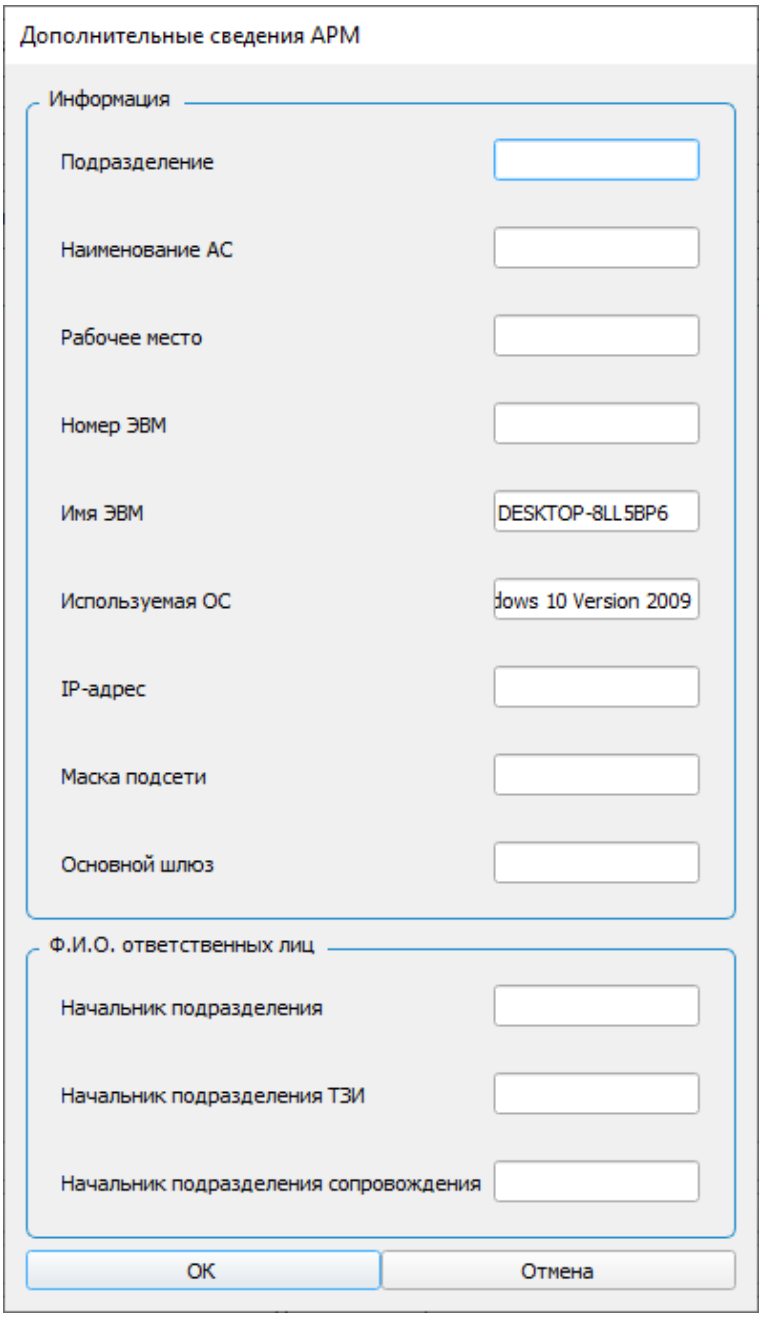


Рисунок 10.9 – Добавление данных для отчета об АРМ пользователя

10.3.3 После заполнения требуемых полей, необходимо нажать кнопку ***«OK»*** (рисунок 10.9). Сохранение отчета произойдет после указания имени отчета в поле ***«Сохранение отчета»*** в формате ***.html*** (рисунок 10.8).

10.4 Создание шаблона

10.4.1 Для обеспечения перемещения настроек с одной ЭВМ на другую в изделии присутствует поддержка создания и применения шаблонов политик безопасности.

10.4.2 Для создания шаблона необходимо нажать кнопку ***«Создание шаблона»***, (рисунок 10.1), при этом появится диалоговое окно, представленное на рисунке 10.10.

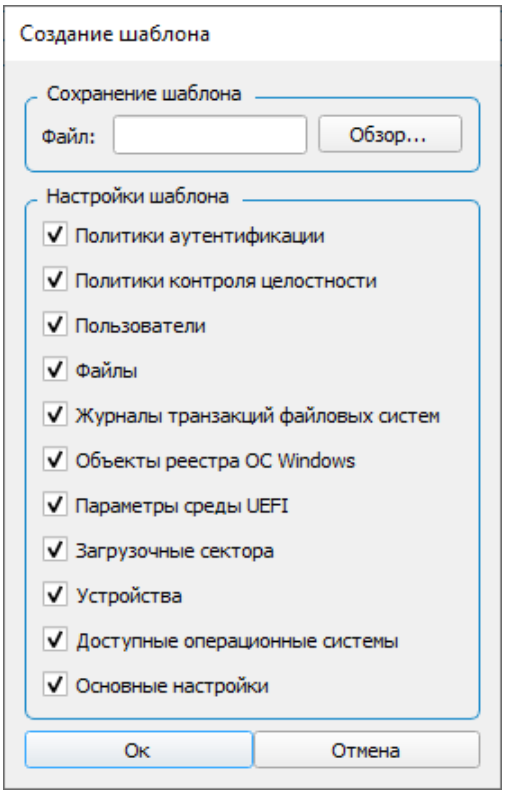


Рисунок 10.10 – Создание шаблона политик безопасности

10.4.3 После установки всех необходимых для сохранения параметров политик, требуется указать имя и место сохранения файла шаблона в области ***«Сохранение шаблона»***.

10.4.4 При нажатии на кнопку «***Ок***» будет выведено информационное сообщение об успешности операции создания шаблона в указанной директории (рисунок 10.11).

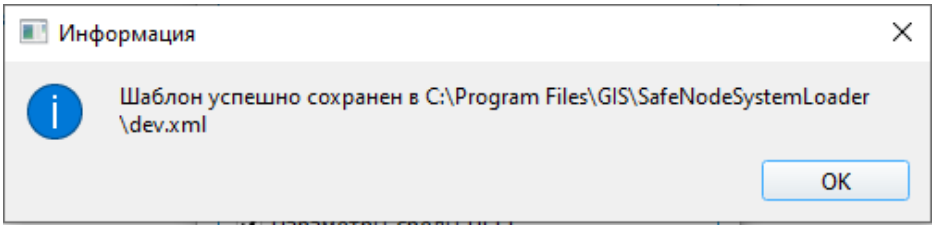


Рисунок 10.11 – Успешное сохранение шаблона политик безопасности

При сохранении шаблона в соответствии с указанными настройками будут сохранены все существующие политики безопасности на ЭВМ.

10.5 Применение шаблона

10.5.1 Для применения шаблона политик безопасности необходимо нажать кнопку ***«Применение шаблона»*** (рисунок 10.1), при этом появится диалоговое окно, представленное на рисунке 10.12.

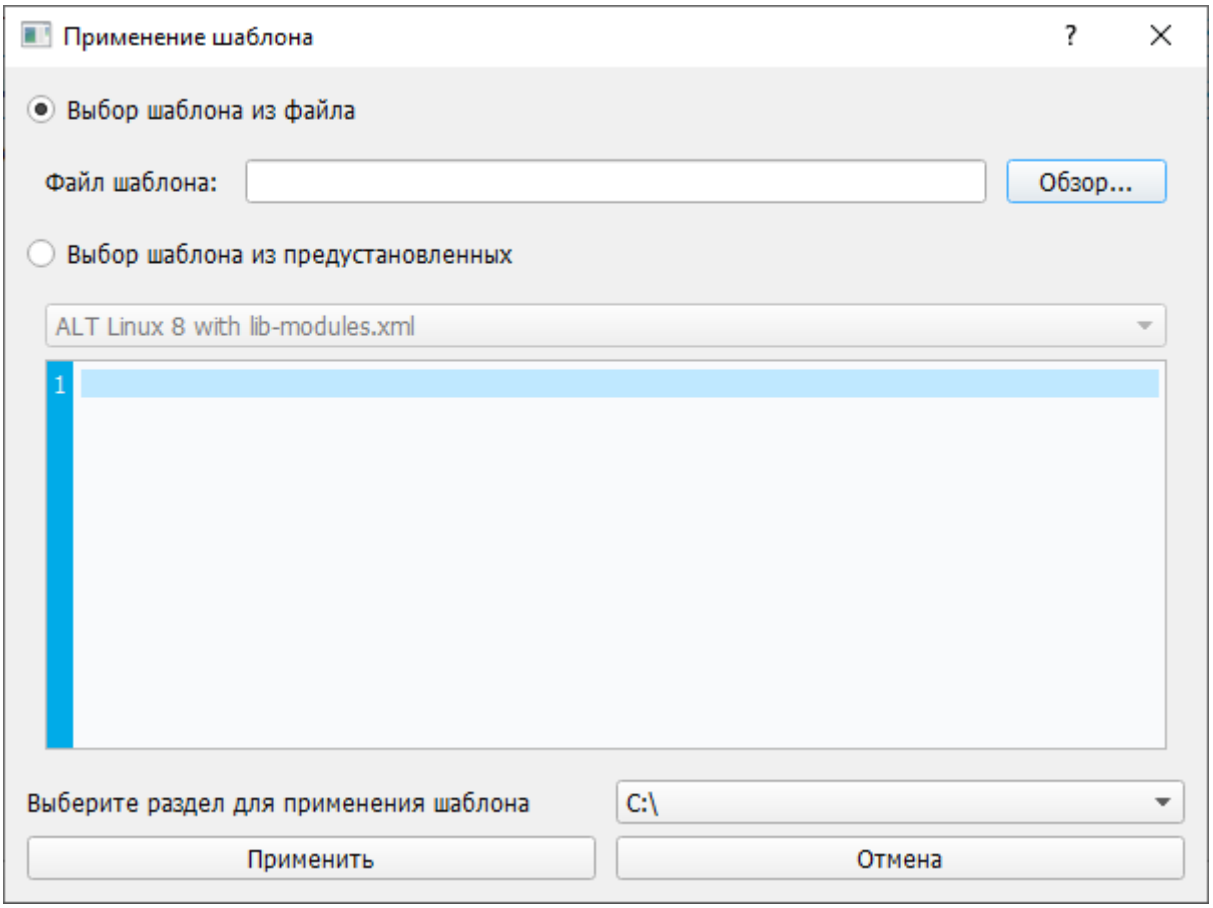


Рисунок 10.12 – Диалоговое окно применения шаблона политик безопасности

10.5.2 В качестве шаблона можно использовать созданный ранее файл в ручную (см. подраздел 10.4), либо набор предустановленных шаблонов на выбор.

10.5.3 Для применения созданного ранее шаблона, необходимо в поле ***«Выбор шаблона из файла»*** указать шаблон, который планируется к применению, помощью кнопки ***«Обзор»***. В поле ***«Выберите раздел для применения шаблона»*** требуется указать раздел системы с файлами и ключами реестра, для которых применяются настройки безопасности, затем нажать ***«Применить»*** (рисунок 10.13).

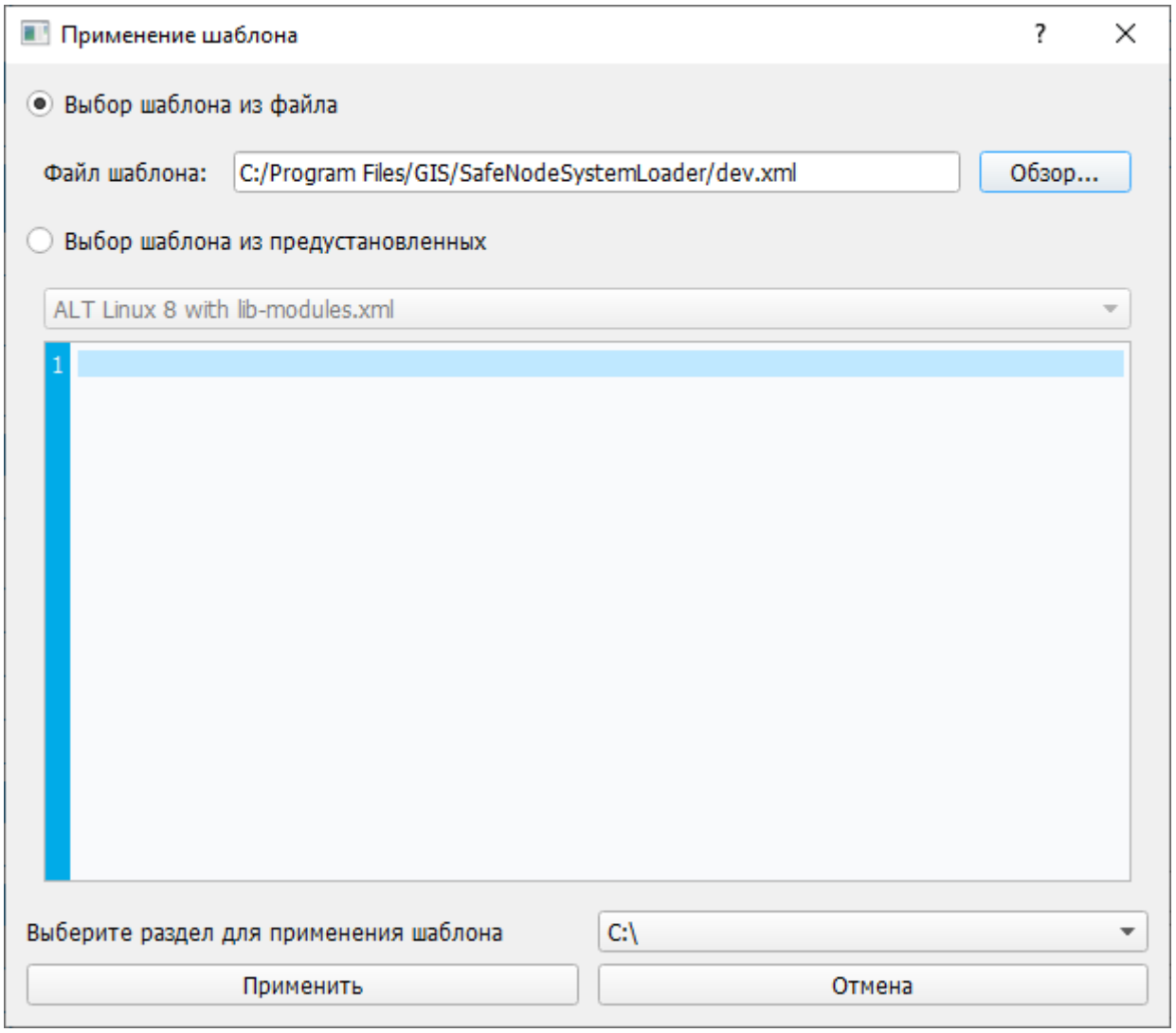


Рисунок 10.13 – Указание необходимых параметров для применения шаблона

10.5.4 В случае успешного применения шаблона в диалоговом окне будет выведено сообщение об успешном применении шаблона (рисунок 10.14).

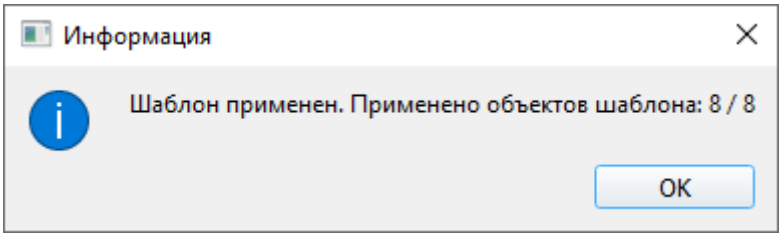


Рисунок 10.14 – Успешное применение шаблона

10.5.5 Если настройки безопасности не применимы к данному разделу, будет выведено сообщение о невозможности применить шаблон (рисунок 10.15).

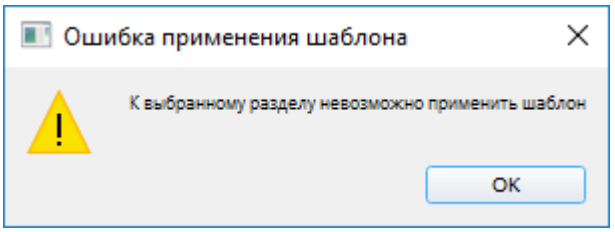


Рисунок 10.15 – Ошибка применения шаблона

10.5.6 Примененные настройки безопасности, заданные в файле шаблона, будут отображены в журнале применения шаблонов.

10.5.7 Для применения предустановленного шаблона необходимо перейти в поле ***«Выбор шаблона из предустановленных»*** и выбрать требуемый, в зависимости от операционной системы, из выпадающего списка (рисунок 10.16).

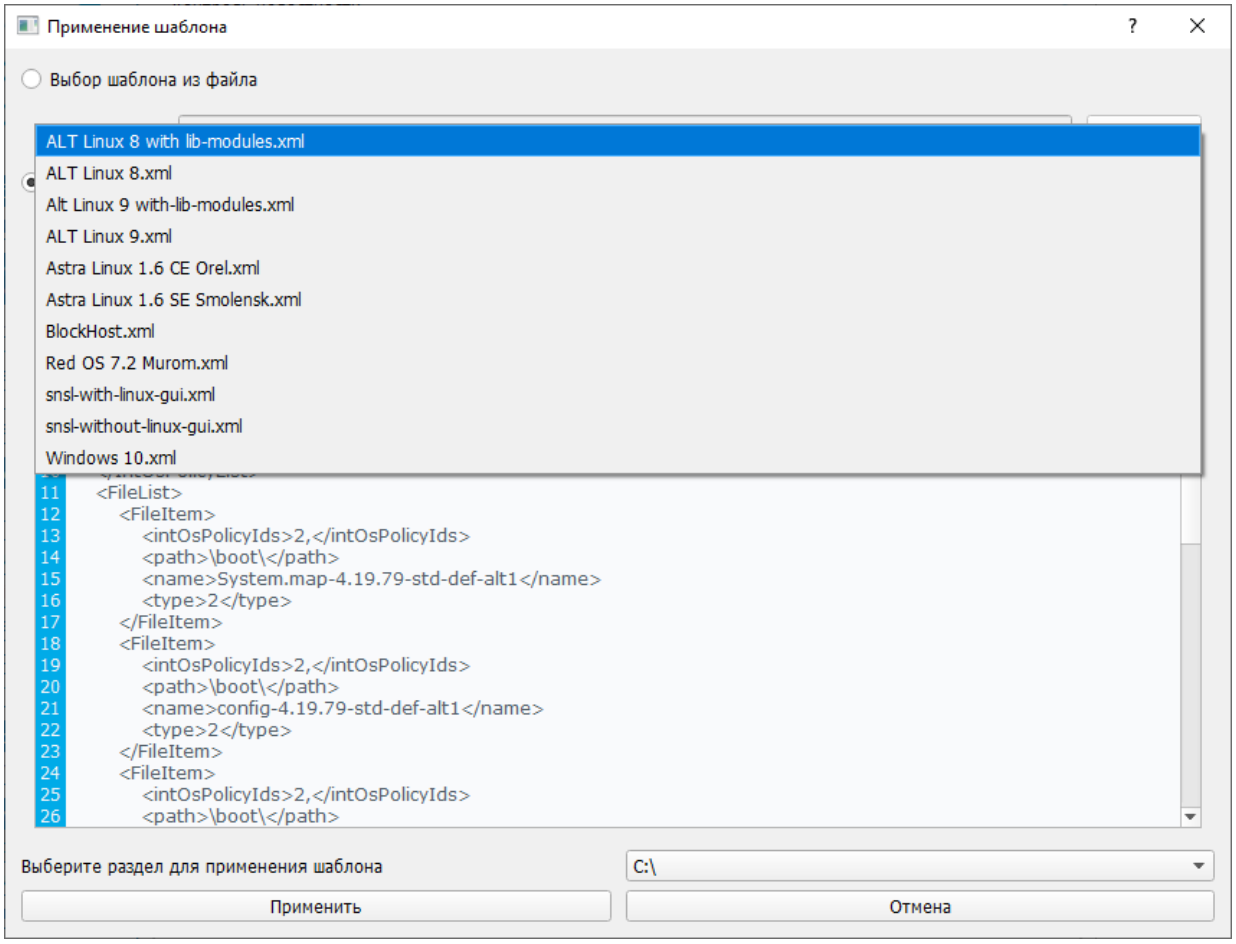


Рисунок 10.16 – Выбор шаблона из предустановленных

10.5.8 Затем в поле ***«Выберите раздел для применения шаблона»*** требуется указать раздел системы с файлами и ключами реестра, для которых применяются настройки безопасности, затем нажать ***«Применить»***.

10.5.9 В случае успешного применения шаблона в диалоговом окне будет выведено сообщение об успешном применении шаблона (рисунок 10.14).

10.5.10 Если на ЭВМ установлен клиент СЗИ от НСД «Блокхост-Сеть 4», то для постановки на контроль целостности файлов клиента воспользоваться предустановленным шаблоном BlockHost.xml. Применение данного шаблона обеспечит неизменность загружаемого СЗИ от НСД[6].

10.6 Восстановление заводских настроек

10.6.1 Для восстановления параметров изделия к стандартным заводским настройкам в окне ***«Основные настройки»*** необходимо нажать на кнопку ***«Восстановить заводские настройки»*** (рисунок 10.1), при этом на экран ЭВМ будет выведено диалоговое окно для подтверждения восстановления настроек (рисунок 10.17).

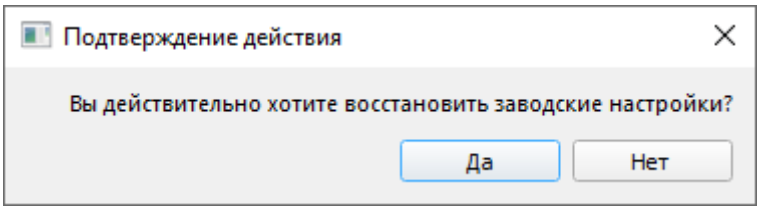


Рисунок 10.17 – Подтверждение восстановления заводских настроек изделия

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

В связи с особенностями функционирования ПО изделия для отключения защиты от входа в BIOS Setup при восстановлении настроек изделия к заводским параметрам из консоли АБ Windows/Linux необходима перезагрузка ЭВМ.

10.7 Диагностика. Контроль исполнения кода

10.7.1 Для диагностики работы изделия АБ необходимо выбрать в главном окне (рисунок 4.2) подпункт меню «***Диагностика»*** (рисунок 10.18).

[6] Применение данного шаблона доступно только для клиентов СЗИ от НСД, установленных на ОС семейства Windows.

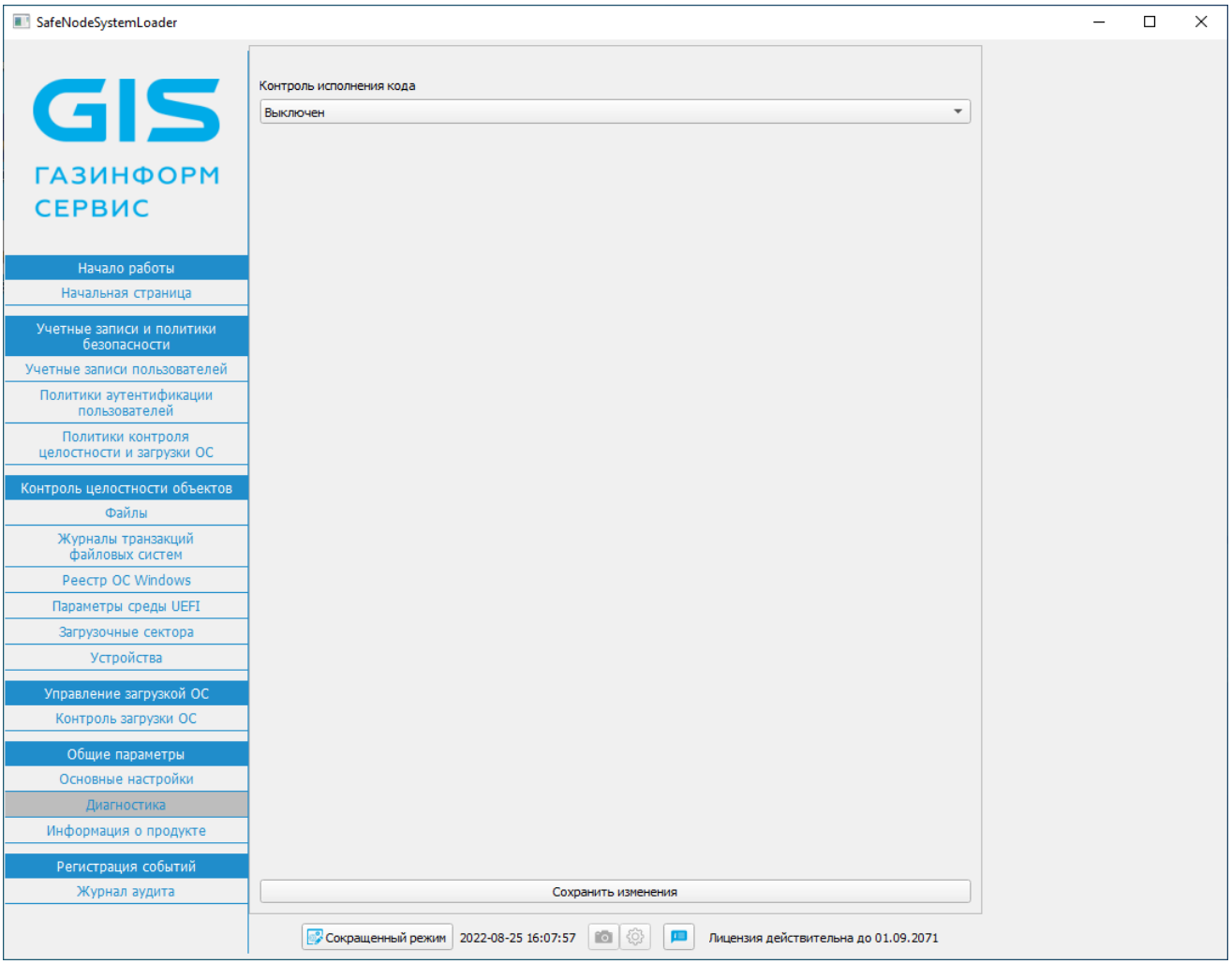


Рисунок 10.18 – Диагностика изделия

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

10.7.3 По умолчанию параметр ***«Контроль исполнения кода»*** выключен. Для включения данного параметра АБ необходимо в поле «Контроль исполнения кода» выбрать требуемый вариант.

10.7.4 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.

10.7.5 Для сохранения установленных настроек выбрать ***«Сохранить изменения»*** внизу диалогового окна (рисунок 10.18). Изменения вступят в силу после перезагрузки ЭВМ.

10.7.6 При выявлении ошибок в работе или загрузке изделия АБ необходимо предоставить файл журнала в службу технической поддержки предприятия-изготовителя для проведения дополнительной диагностики и устранения неполадок[7].

10.8 Информация о продукте

10.8.1 Подпункт меню ***«Информация о продукте»*** меню ***«Общие параметры»*** содержит сведения о предприятии-изготовителе изделия и сведения о версии ПО (рисунок 10.19).

10.8.2 По кнопке ***«Контрольные суммы ПО»*** открывается окно, содержащее сведения о контрольных суммах каждого модуля ПО (рисунок 10.20).

10.8.3 По кнопке ***«Цифровые подписи ПО»*** открывается окно, содержащее сведения о цифровых подписях каждого модуля ПО (рисунок 10.21).

10.8.4 Для экспорта информации о контрольных суммах, цифровых подписях и версиях модулей ПО необходимо нажать кнопку ***«Экспорт версии ПО в файл»*** (рисунок 10.19), при этом на экран ЭВМ будет выведено новое диалоговое окно для указания директории сохранения файла.

10.8.5 В случае существования на выбранном устройстве хранения данных файла с таким именем, АБ на экран ЭВМ будет выведено предупреждение (рисунок 10.22).

[7] Сохранение отчета осуществляется в консоли АБ.

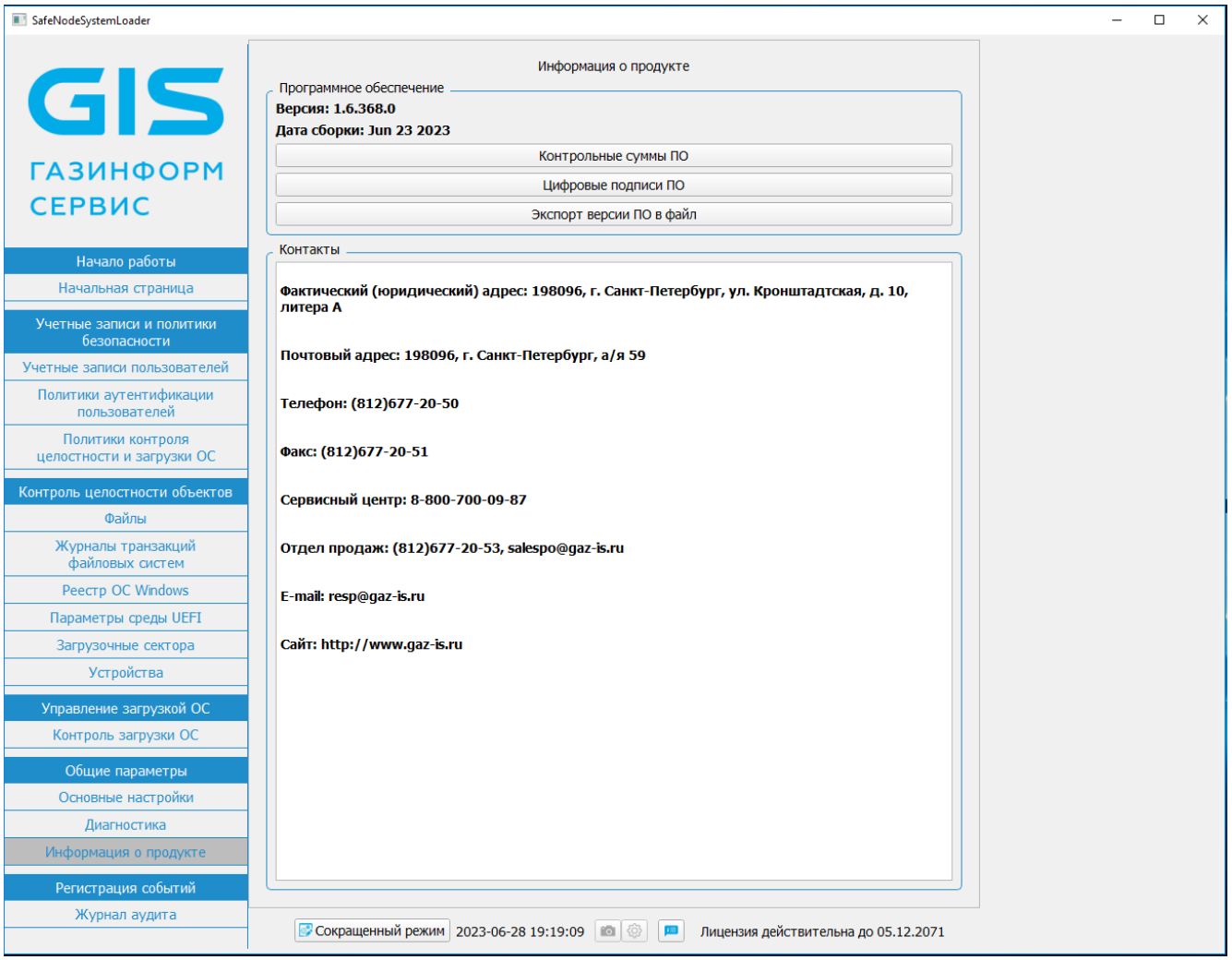


Рисунок 10.19 – Общая информация об изделии

	Название модуля	Контрольная сумма [MD5]
1	Общая ...	0d 27 ac a3 5d 24 a7 b1 ec d7 91 17 fe 97 1b dd
2	Activatr.efi	98 ee 89 b5 73 f9 1d a9 8c a0 e3 0a 0a b3 9a cf
3	Auth.efi	76 c7 be 89 19 52 9f d6 99 77 ce 66 34 e6 4e e0
4	ChInt.efi	9a fd 4d a9 bc e4 2d 94 38 37 0d 46 f2 76 da 38
5	DispEng.efi	17 a3 04 ff 01 86 88 79 dc 0b 1c c4 17 e2 54 98
6	ExpatDxe.efi	6b 84 a9 df 18 fe 39 94 a5 1a 3a f8 49 14 03 05
7	Ext2Dr.efi	46 13 f6 ec c3 c3 9f d1 7d 76 22 93 f7 45 0d 86
8	Ext4Dr.efi	30 41 62 df 15 c4 80 0c c3 1d bc cd f4 e3 81 87
9	GrCon.efi	1b e2 59 45 49 fe d9 a1 83 ba aa 5a 1d a9 4e 73
10	Hash.efi	30 08 a3 6c eb b4 65 98 ca 9d 78 cc 2e 90 5a cd
11	HiiDb.efi	53 c5 3c 41 ce a9 fa eb 1b df 6d 6f 63 89 17 a4
12	IconvDxe.efi	2f d2 79 52 1d e1 e4 07 3a 7a fa e4 8c c5 19 3e
13	Ip4Cfg.efi	20 42 76 d3 46 88 e9 7d 6c e6 26 1b cb c4 a1 9a
14	IrGrammr.efi	b6 47 3d 41 7d c9 e4 1e ff 28 4d 94 69 bb f1 5a
15	IrGrammr.g	0d 4b 61 ab a3 21 91 27 80 2e e7 ae 01 c0 01 ae
16	KbdHk.efi	e9 17 d0 10 d8 ea 80 98 5b 8b c0 62 9d 93 02 fc
17	Krb.efi	3f 6c cf 31 fa c9 80 a5 00 75 bb 0d 8d 88 74 5d
18	LangIns.efi	9a 40 2b 37 15 64 57 93 9c 43 92 ac 41 ae 9b 8d
19	Loader.efi	25 e3 c6 53 e0 cc 29 a4 d5 84 de 1d da b8 26 35
20	MainMgr.efi	f5 0c 22 d6 fb ab 3e 3d bf a6 ad dd 4f ad 39 01
21	MemCln.efi	44 a2 e6 8c fd 7b 3d 84 71 40 09 ab 26 20 bb 7e
22	MnpDxe.efi	df 90 a3 e3 7c 40 79 91 0f 4e 53 36 4b b9 d8 6d
23	MsgDxe.efi	f3 a7 1d 57 d2 83 cc f5 9d 4e ff 48 fc 93 76 44
24	NtfsDr.efi	24 2d bb b8 c8 d6 e8 90 a2 66 d6 89 a2 93 61 36
25	OpenLdap.efi	b6 8c f4 f0 39 a5 21 48 6a 32 bf 23 d9 c0 5e c9
26	OpenSC.efi	3e e8 69 e0 ed 28 7c 71 eb 78 63 9a b5 ab 35 f4
27	Orm.efi	12 b1 33 35 5e 3e 43 2e e1 ad e9 02 16 3e 98 00
28	RegExpDx.efi	d0 63 ff 47 3b 0e 65 3c 76 d0 1b d0 eb c6 f2 39
29	RemAccDx.efi	75 2c af 13 9b a5 e7 56 59 e5 e8 cd 18 de bf 0e
30	SCardRdr.efi	b7 66 a4 36 68 5e 82 88 56 4e 46 49 b2 32 44 4c
31	ScreenDr.efi	69 28 71 7d 96 a9 b2 0b ce 8a 19 23 ae 4f 8c 6a
32	SetupBr.efi	0a 10 d4 4e b1 06 fd 73 53 77 1c 61 03 ea fd 04
33	SmbiosDx.efi	d5 66 2e a1 9d 46 a4 be 7a 66 1c 63 00 fb a9 da
34	SnpDxe.efi	87 c9 70 e3 cb f5 08 70 25 8e bc 89 9b 43 63 5c
35	Sntp.efi	c2 d7 ec ff fa 6c 72 5c 9d e0 d4 c0 7d 53 68 83
36	SqlitDxe.efi	14 cd d6 c6 1a 0b 48 ee 23 a0 bf 13 a7 08 17 ac
37	TlsDxe.efi	45 3e e2 ba 84 8c a7 ef ef f5 85 72 ec bf cc b8
38	UniColl.efi	02 38 a9 cf 63 ea a1 c7 21 ce 68 50 d5 85 f8 56

Рисунок 10.20 – Контрольные суммы ПО

	Название модуля	Цифровая подпись [AES-256]
1	Activatr.efi	3b 6c 28 ac 8a 5b 49 b2 15 7e ed fd 73 4c f9 15 1d ec be dd 85 16 b2 a4 fd 0a c4 3d 5d 80 d9 51 d2 ed c2 cf eb 7e 9f 44 20 71 6b ec af 53 3f a4 49 e2 87 ab 0c 03 62 dd a0 03 99 18 9a 38 e6 3f d1 f2 c5 dc 4f 5d b3 f2 24 9b f0 96 9a e8 f5 54 27 93 ad cb a7 85 9f be f2 c2 d6 26 cf f0 49 84 80 dd 23 56 17 ce 13 08 c0 d6 f2 0a 76 d0 23 9b b1 dc 6b 55 f7 05 e0 a8 89 bf 38 43 9e 15 20 97 58 82 a4 d0 72 d1 f4 e6 ea 2d 2b 50 c8 9d 3c 93 65 32 d7 39 30 ab e0 74 65 3b 11 8b 14 c0 8e 00 57 d1 ad a1 f4 23 5a 4d a3 96 7f c9 35 c8 5e 88 69 01 9c c0 3f 7d 3d 49 66 b8 83 c7 c0 c2 96 70 1f cc 04 a2 ca a9 ed b3 36 8c 4a d0 64 fe 1c 38 79 10 75 96 d6 42 7d 0e 6e 95 27 2f 84 c5 10 1f b6 97 50 8a 2b 70 70 23 37 2b 58 b5 9f e5 10 79 f3 01 63 32 1e a2 c6 9f
2	Auth.efi	5f 4d 9f 75 42 2a 8c 0e 8c 12 85 9c 80 e1 de 17 76 50 f7 6c 02 2e 5b 6c af 9d 1e bd 91 98 a0 fd 57 a8 47 dd 36 06 28 ae fd 55 74 cc 66 35 62 11 0b 32 67 82 df 7d c1 00 3d d5 d9 41 d1 64 eb 15 f9 c4 f5 a1 e1 f2 8a 5e a6 fc f2 6d 9d 3a 8e 03 ac 23 cf e3 82 c3 39 b9 52 6d 01 3b d9 26 8e af a9 73 f5 06 c2 eb c5 8b 98 5a 60 e4 3a 05 0c be 43 33 d0 8f 09 42 06 ac 8a ec 73 9d d5 7c 6f 9f 30 ae f4 2a 9e 77 5c 23 cf ad 60 d0 ab 4c 8d ef 81 88 23 b8 0f 13 fd 27 8c fd 63 a2 c6 52 fe 43 da 58 96 7c 06 a2 fb cf 50 58 cf 87 c1 3e b1 df 88 f9 8b 5c 55 ca 06 e4 3c ea 54 d0 d7 55 3c 5b 6a e0 f0 cb 36 d3 83 eb 2f 63 e9 8f 31 3a f7 27 04 41 f2 56 10 6e fa c3 b4 2a e9 90 0e 92 65 f2 4b 81 d0 62 d8 db aa a0 c3 ca 0c 6c 95 ae 50 d3 9c e4 81 1f 5a fe 9d eb
3	ChInt.efi	29 28 7e 70 68 45 6c cf f3 89 15 b9 b4 72 eb 65 eb 43 9f 61 e8 61 34 ea 66 56 86 e3 87 75 94 c9 1b aa e4 90 0d 45 21 0f 60 9c 85 70 26 6e dd 1f ce a1 7d bf be 6f 10 cc 71 23 7e 23 22 75 fa 26 60 95 c7 79 63 dd 91 91 ce 0b 48 ef 19 34 05 7c 32 32 24 e6 c4 14 b6 5b 74 10 cd 56 c3 3a 1f e2 d3 dc f0 4e 0d 35 13 d1 24 17 88 3a 11 cf fc b0 b8 5a 7e b5 3c 18 91 c5 75 53 01 04 df 21 f1 fe 20 b6 27 dc db a3 2f d6 0f 4a af ad 09 d3 ef e9 70 ba b1 b8 fc ab a1 a9 2a 12 76 16 40 2b e5 62 7f 01 05 27 2b ad 78 fa ce 4e df a6 f9 01 c8 45 bc 14 f6 d2 37 28 c4 28 72 a0 2b 62 ae c9 73 7e 90 c4 c8 30 27 eb 05 bb 1d 1d 0e 48 e6 a1 15 4c 84 21 05 2c ce 46 e9 42 eb 1c c8 00 e3 55 d8 51 2f 65 11 b4 58 e9 47 49 24 48 fd b0 17 44 f1 26 c4 43 2e 28 78 8f c6
4	DispEng.efi	af 8a a3 c6 8b 19 ce 23 a9 02 f9 4e 4d 3d 6f fc 6a 90 83 04 3c 6c 66 61 1d d6 25 27 34 42 09 65 10 ec 91 5d ad 84 bb 37 d2 f8 e2 a4 58 f7 be f4 c6 c7 98 17 b7 86 b6 a5 aa 34 98 a8 91 57 2f 73 31 0d 3c 4f ab ed 6e 88 69 d1 6a eb 72 82 18 91 0b 80 4f cf 5d 28 1d 26 84 19 83 86 6d 00 42 e1 90 af c7 ee b4 63 a4 2a 1e 0a 0e bc 99 d6 ac 83 20 5a 53 79 79 68 95 ed ac c6 61 98 23 79 e0 2c 1a 2f 2c 05 5e 02 64 22 30 2e ab db db 6e 13 d6 ad c2 f4 da 86 d7 05 e9 bd b9 51 b4 c1 d7 e6 09 da df 9e 99 9a a3 0d 7d 95 d8 48 0d e9 d9 c1 41 45 af f3 62 d4 57 bb ed 43 8e 94 55 e4 f0 71 b1 4b 72 51 e2 b1 83 cc fb d2 fc 23 97 45 46 3e 36 0a 2d 4e 0a 3e 75 8e f7 36 2c eb 44 8e 33 7d 1c 32 05 3b 68 22 1a 4c 49 a7 04 bb ac 28 b3 ae cc 03 88 a3 31 05 21
5	ExpatDxe.efi	1c cf 98 86 a7 14 61 3c a6 33 56 d8 37 62 84 16 4a d2 9c 69 ce 65 62 3d 72 c1 1c 2b 0a cf 17 db e4 48 6a 85 76 a4 82 ae cc 73 8d 05 67 e2 85 d1 15 27 df 52 60 4e d6 99 ed dc 1e d9 5c d4 72 28 c2 68 cd 03 0d 8d 68 2d dd ae 8d 9a 9d d3 52 5b 54 40 c3 cc 4e a2 42 67 19 62 15 cd cd 55 40 58 2b 60 47 91 8f f6 43 09 22 e8 27 7f aa 81 4c f1 fe eb 6a d8 38 7e c6 18 35 28 ae 95 a8 fa 8f 56 87 fe 49 97 c9 a0 f3 97 97 38 6b ac 36 76 b5 41 5c 52 ff 2a 44 f6 bb 37 26 bc 33 66 7b 38 80 1f c9 b6 f3 ba 25 e8 05 8f 13 f9 ca f2 57 2f 22 7d 0f f0 e9 56 46 04 ad 65 e5 4f 9e f3 0a f9 3f 16 02 96 42 c9 35 9f 9e de 51 89 de 95 4e 08 43 88 20 c2 32 fa 0a 56 c1 78 9a 04 3d b2 8b 9e f2 8b b0 bc 3f c1 2f 6d 36 45 2a 70 45 1b 1b c8 cc ca 90 1b 58 1d 55 93
6	Ext2Dr.efi	39 10 be 60 80 ad 02 94 3d 36 1f 55 44 60 62 ff e8 f4 76 20 61 44 3d 8b 04 a3 5d ec 2a 48 0b a4 cc 52 39 e5 c7 e3 53 a1 26 07 0c 74 83 8d d1 2e 0f 98 70 34 85 db 3a a8 a9 1e 87 f0 c9 b2 52 52 50 27 7a 3b 51 80 2f 8c bd 60 8c f6 08 b6 8b 47 fe 03 c2 54 29 31 a7 3c f7 77 46 ef c9 03 f6 76 9c 49 9b c9 c3 c9 f4 57 93 3b e8 a2 e0 6e de 15 d3 bc a1 44 b6 2b 79 05 d4 0a 68 48 e0 9c e0 a5 e9 cc e6 39 78 c0 d2 39 ac 79 ae ea c1 de be a5 4d 5d 80 13 2b 6d d2 bb ff 7a 8a c8 f5 75 cf 7a 6e 2d f5 50 49 f1 df c4 0c 5c c1 01 e3 a2 1e fb e6 b3 61 16 36 04 c6 90 d9 ef 4b d7 cf 1c 02 b6 f7 e2 d6 db 86 93 86 74 30 b1 e1 5f 54 37 3e 6e e5 40 41 42 2f 7d 07 62 cf bf ee f3 6b 90 a1 3a 4c fd e7 2d 9b 55 8f 97 e8 ba 2d 93 b5 e4 7e 4f 1d 00 58 1b d8 1d da 39
7	Ext4Dr.efi	03 1f 32 98 bc ab 3a b0 cf b2 9d c7 d6 61 a3 be 85 d5 d0 15 9a 95 56 12 73 fc 1f 46 a6 7e 7a 44 88 02 e9 1b fa 83 20 ce f6 da e3 c5 87 23 b8 45 2b 4f 58 1d 8b ce ff 82 a4 37 27 e0 dc f2 85 89 e0 a1 84 ea ab 6b ea d8 5d 8d e6 d8 f2 ea 33 c6 38 c0 34 c8 24 7a a4 81 79 a1 9c 1b 8d 20 93 91 ed 34 85 a2 3b 46 2d 78 9e cf 92 cc 23 18 3d fe b0 53 ab fc 4d aa ff a8 6e ea f4 bc 5e e5 b4 8a 44 58 8c f3 f5 c1 9e 71 f7 25 6f 06 e4 2a c8 f5 8f 2c da 78 2e 67 1e 10 19 f4

Рисунок 10.21 – Цифровые подписи ПО

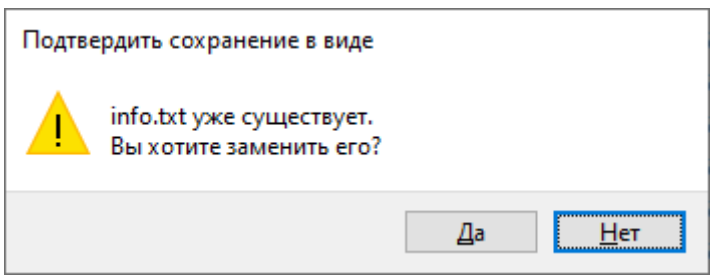


Рисунок 10.22 – Подтверждение замены файла с информацией о продукте

11 Регистрация событий. Журнал аудита

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

Для работы с журналом аудита АБ необходимо выбрать в главном окне консоли АБ Windows (рисунок 4.2) подпункт «***Журнал аудита»*** (рисунок 11.1).

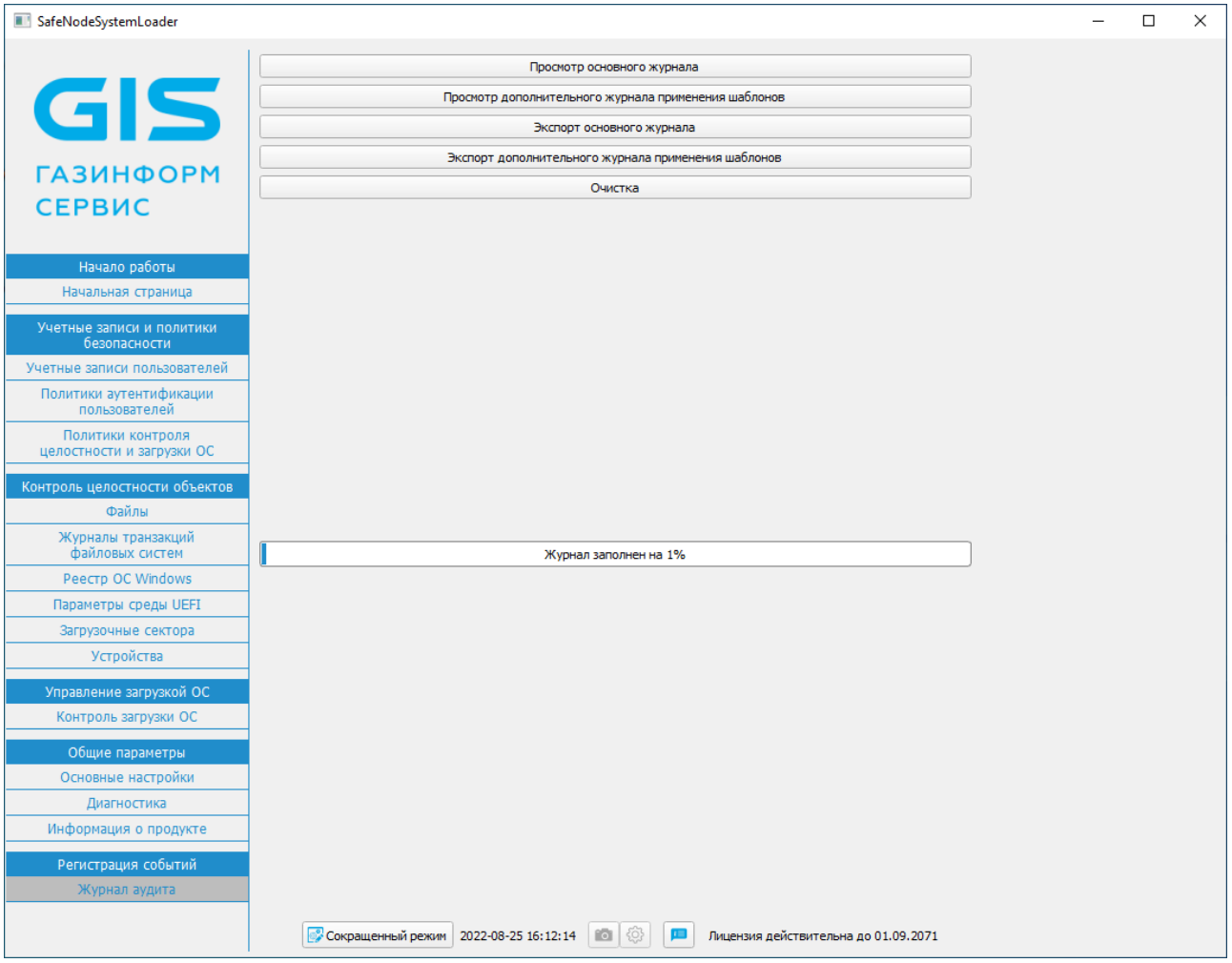


Рисунок 11.1 – Журнал аудита

АБ имеет возможность:

- просмотра журнала зарегистрированных событий;
- просмотра 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 ролью «Аудитор».

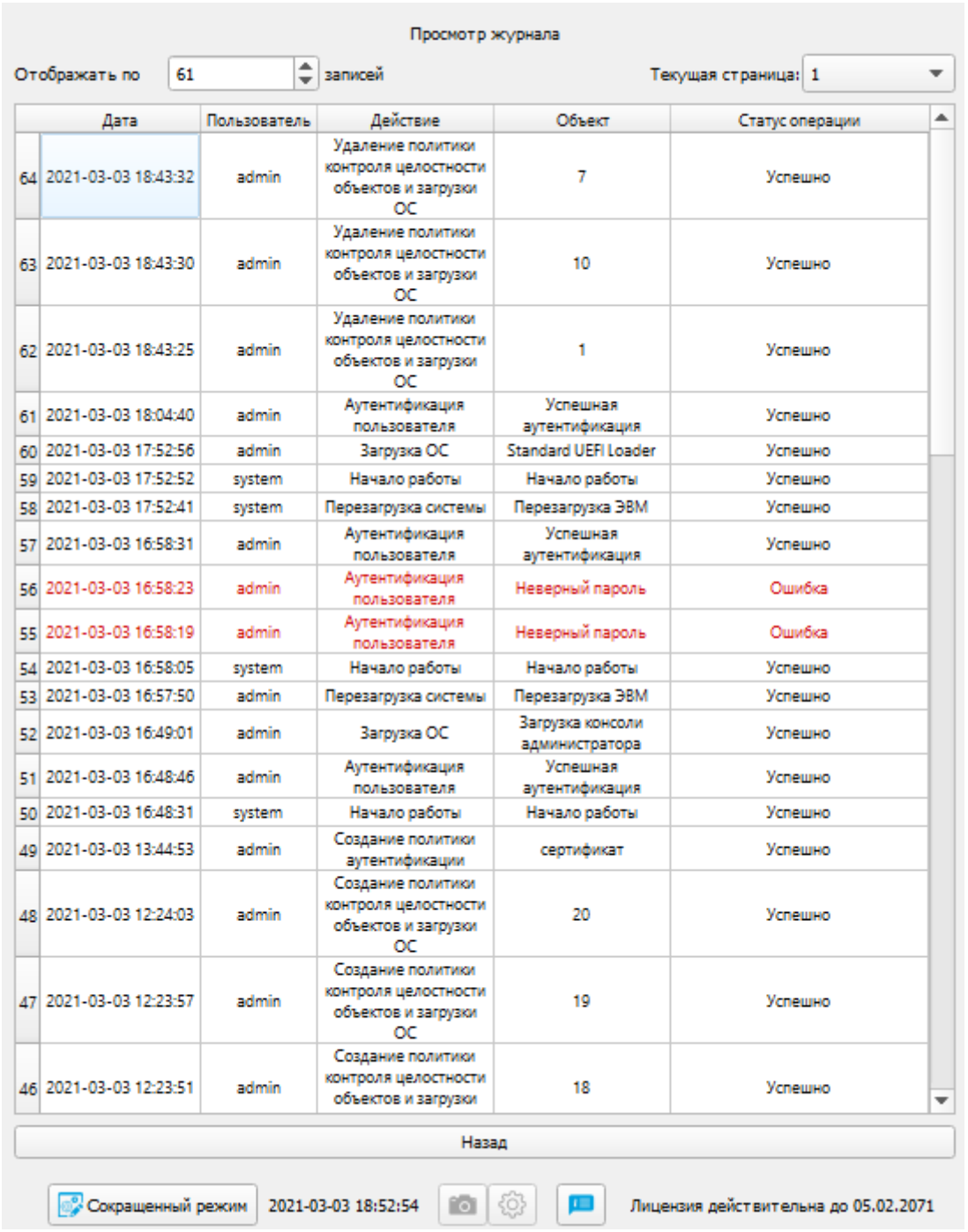
В строке ***«Журнал заполнен на …»*** отображается информация о процентном заполнении специально выделенной области для хранения данных аудита.

11.1 Просмотр журнала аудита

11.1.1 В журнале аудита регистрируются все действия АБ (изменение общих настроек изделия, изменения настроек политик аутентификации и КЦ, действия с учетными записями пользователей) и действия пользователей. Дополнительно в журнал аудита включаются сообщения при срабатывании механизмов КЦ объектов.

11.1.2 Для просмотра основного журнала аудита необходимо нажать кнопку ***«Просмотр основного журнала»*** (рисунок 11.1). Список регистрируемых в журнале событий аудита (рисунок 11.2) приведен в таблице 11.1.

11.1.3 В окне просмотра журнала (рисунок 11.1) предусмотрена настройка количества отображения записей для удобства навигации. В правом верхнем углу отображается номер текущей страницы журнала.



	Дата	Пользователь	Действие	Объект	Статус операции
64	2021-03-03 18:43:32	admin	Удаление политики контроля целостности объектов и загрузки ОС	7	Успешно
63	2021-03-03 18:43:30	admin	Удаление политики контроля целостности объектов и загрузки ОС	10	Успешно
62	2021-03-03 18:43:25	admin	Удаление политики контроля целостности объектов и загрузки ОС	1	Успешно
61	2021-03-03 18:04:40	admin	Аутентификация пользователя	Успешная аутентификация	Успешно
60	2021-03-03 17:52:56	admin	Загрузка ОС	Standard UEFI Loader	Успешно
59	2021-03-03 17:52:52	system	Начало работы	Начало работы	Успешно
58	2021-03-03 17:52:41	system	Перезагрузка системы	Перезагрузка ЭВМ	Успешно
57	2021-03-03 16:58:31	admin	Аутентификация пользователя	Успешная аутентификация	Успешно
56	2021-03-03 16:58:23	admin	Аутентификация пользователя	Неверный пароль	Ошибка
55	2021-03-03 16:58:19	admin	Аутентификация пользователя	Неверный пароль	Ошибка
54	2021-03-03 16:58:05	system	Начало работы	Начало работы	Успешно
53	2021-03-03 16:57:50	admin	Перезагрузка системы	Перезагрузка ЭВМ	Успешно
52	2021-03-03 16:49:01	admin	Загрузка ОС	Загрузка консоли администратора	Успешно
51	2021-03-03 16:48:46	admin	Аутентификация пользователя	Успешная аутентификация	Успешно
50	2021-03-03 16:48:31	system	Начало работы	Начало работы	Успешно
49	2021-03-03 13:44:53	admin	Создание политики аутентификации	сертификат	Успешно
48	2021-03-03 12:24:03	admin	Создание политики контроля целостности объектов и загрузки ОС	20	Успешно
47	2021-03-03 12:23:57	admin	Создание политики контроля целостности объектов и загрузки ОС	19	Успешно
46	2021-03-03 12:23:51	admin	Создание политики контроля целостности объектов и загрузки	18	Успешно

Рисунок 11.2 – Просмотр журнала аудита

11.1.4 Каждому событию присваивается порядковый номер и указывается:

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

11.1.5 Строки с сообщениями об ошибках выделены красным цветом (рисунок 11.2).

Таблица 11.1 – Список регистрируемых событий в журнале аудита

№	Событие	Успех/Ошибка	Комментарий
Общесистемные события			
1	Диагностика	Успех	Проверка цифровых подписей модулей: Проверка успешна
			Проверка оперативной памяти: Проверка успешна
		Ошибка	Проверка оперативной памяти: Проверка отменена
2	Изменение настроек системы	Успех	Настройки сети и LDAP изменены
			Время изменено
			Контроль исполнения кода
3	Работа с журналом	Успех	Просмотр журнала аудитором
4	Аутентификация пользователя	Успех	Автовход: Успешная аутентификация
5	Работа с шаблонами	Успех	Шаблон успешно сохранен в <путь до файла>
6	Сохранение паспорта объекта	Успех	Паспорт объекта
7	Взятие под управление под управление сервером БлокхостСеть	Успех	Успешное взятие под управление БлокхостСеть
8	Пересчет контрольных сумм объектов	Успех	Пересчет контрольных сумм объектов
9	Выход из-под управления БлокхостСеть	Успех	Успешный выход из режима управления
10	Выгрузка версий и хеш-сумм ПО в файл	Успех	Информация сохранена в файл с именем <путь до файла>
11	Пересчет хешсумм контролируемых объектов ФС	Успех	<имя учетной записи>
12	Загрузка ОС	Успех	<название операционной системы>
		Ошибка	Доступных операционных систем нет
13	Восстановление настроек по умолчанию	Успех	Заводские настройки восстановлены
14	Изменение настроек системы	Успех	Настройки изменены
			Автовход разрешен для пользователя: <имя пользователя>
15	Выключение системы	Успех	Выключение ЭВМ

№	Событие	Успех/Ошибка	Комментарий
16	Обновление системного ПО	Успех	Системное ПО обновлено
17	Начало работы	Успех	Начало работы
18	Перезагрузка системы	Успех	Перезагрузка ЭВМ
События идентификации и аутентификации пользователей			
19	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 хеш-сумма на персональном идентификаторе
			Сертификат на персональном идентификаторе некорректен, не найден или просрочен
		Успех	Успешная аутентификация
События при действиях АБ			
Работа с журналом аудита			
20	Работа с журналом	Успех	Журнал сохранен в файл с именем <путь до файла>
			Журналы аудита очищены
Работа с шаблонами			
21	Работа с шаблонами	Успех	Шаблон применен. Применено объектов шаблона: <количество>
Работа с учетными записями пользователей			
22	Создание учетной записи пользователя	Успех	Создана учетная запись пользователя: <имя пользователя>
23	Обновление учетной записи пользователя	Успех	Обновлена учетная запись <имя пользователя>
24	Удаление учетной записи пользователя	Успех	Удалена учетная запись пользователя: <имя пользователя>
Работа с политиками аутентификации пользователей			
25	Создание политики аутентификации	Успех	Создана политика аутентификации: <имя политики>

№	Событие	Успех/Ошибка	Комментарий
26	Обновление политики аутентификации	Успех	Обновлена политика аутентификации: <имя политики>
27	Удаление политики аутентификации	Успех	Удалена политика аутентификации: <имя политики>
Работа с политиками контроля целостности объектов и загрузки ОС			
28	Создание политики контроля целостности объектов и загрузки ОС	Успех	Создана политика контроля целостности объектов и загрузки ОС: <имя политики>
29	Обновление политики контроля целостности объектов и загрузки ОС	Успех	Обновлена политика контроля целостности объектов и загрузки ОС: <имя политики>
30	Удаление политики контроля целостности объектов и загрузки ОС	Успех	Удалена политика контроля целостности объектов и загрузки ОС: <имя политики>
События при действиях пользователя			
31	Смена PIN-кода устройства	Успех	Изменен PIN-код персонального идентификатора <имя идентификатора>
32	Смена пароля пользователя	Успех	Пароль изменен
События подсистемы контроля целостности			
Контроль целостности файлов			
33	Редактирование списка контролируемых объектов ФС	Успех	Политика <имя политики> Добавление <имя объекта>
			Политика <имя политики> Удаление <имя объекта>
34	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			
35	Редактирование списка контролируемых объектов реестра	Успех	Политика <имя политики> Добавление <имя объекта>
			Политика <имя политики> Удаление <имя объекта>
36	Проверка объектов реестра	Ошибка	Проверка целостности объектов реестра
			Политика <имя политики> <имя объекта> Содержимое объекта изменено
			Политика <имя политики> <имя объекта> Объект не найден

№	Событие	Успех/Ошибка	Комментарий
		Успех	Проверка целостности объектов реестра
Контроль устройств			
37	Редактирование списка контролируемых устройств	Успех	Политика <имя политики> Добавление <имя объекта>
			Политика <имя политики> Удаление <имя объекта>
38	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			
39	Редактирование списка ОС пользователей	Успех	Политика <имя политики> Добавление <наименование ОС>
			Политика <имя политики> Удаление <наименование ОС>
Контроль загрузочных секторов			
40	Редактирование списка контролируемых загрузочных областей	Успех	Политика <имя политики> Добавление <имя объекта>
			Политика <имя политики> Удаление <имя объекта>
41	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			
42	Редактирование списка целостности среды UEFI	Успех	Политика <имя политики> Добавление <имя объекта>
			Политика <имя политики> Удаление <имя объекта>
43	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			
44	Редактирование списка журналов файловых систем	Успех	Политика <имя политики> Добавление <имя объекта>
			Политика <имя политики> Удаление <имя объекта>

№	Событие	Успех/Ошибка	Комментарий
45	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			
46	Редактирование статуса пользователей	Успех	Блокировка пользователя на n минут
			Блокировка пользователя
			<имя пользователя> был заблокирован администратором
			<имя пользователя> был разблокирован администратором
			Блокировка пользователя по истечению времени неактивности

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 нажать кнопку ***«Просмотр дополнительного журнала применения шаблонов»*** (рисунок 11.1). Список событий, регистрируемых в журнале применения шаблонов (рисунок 11.3), приведен в таблице 11.2.

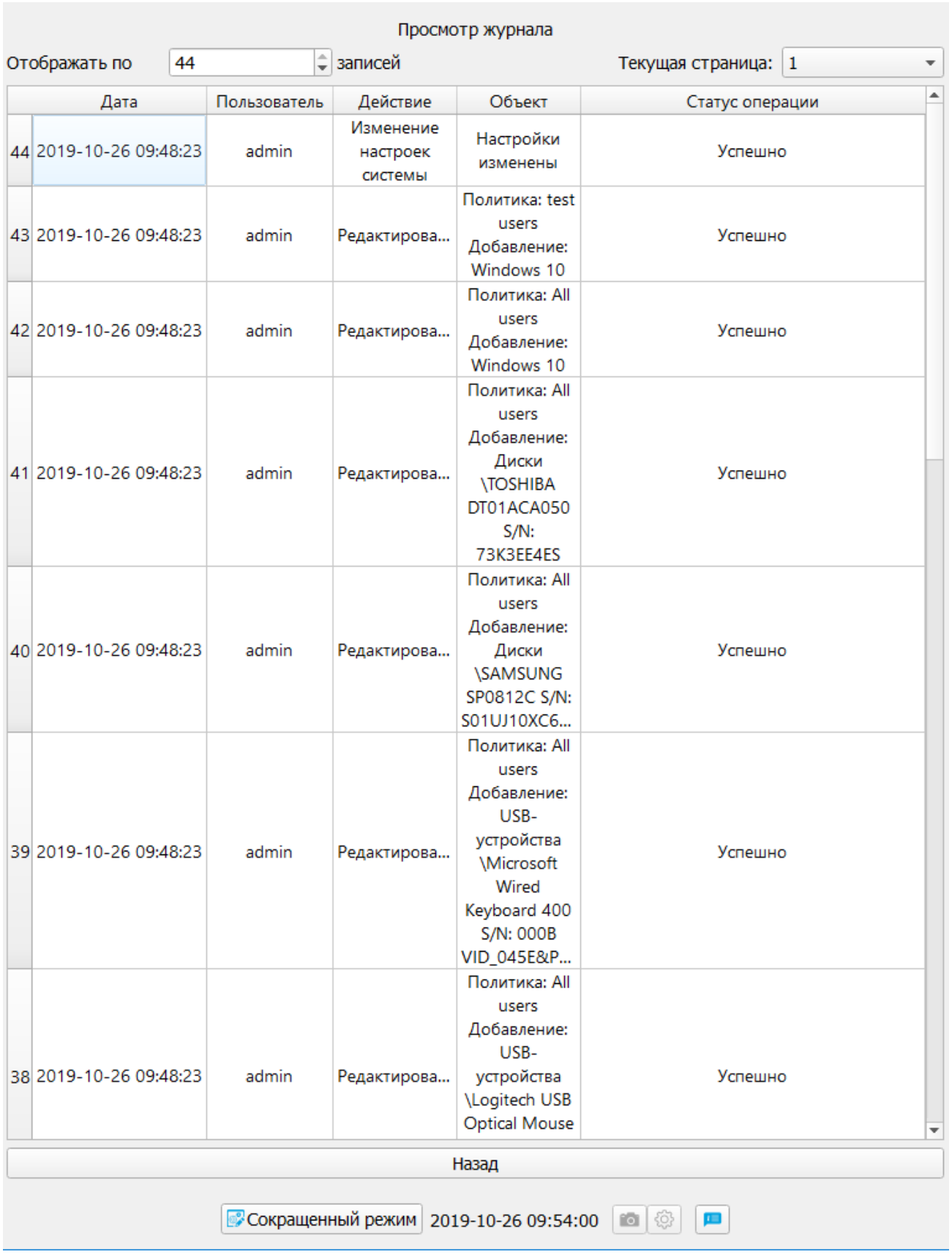


Рисунок 11.3 – Просмотр журнала применения шаблонов

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			
3	Редактирование списка контролируемых объектов реестра	Успех	Политика <имя политики> Добавление <имя объекта>
		Ошибка	
Контроль устройств			
4	Редактирование списка контролируемых устройств	Успех	Политика <имя политики> Добавление <имя объекта>
		Ошибка	
Управление загрузкой ОС			
5	Редактирование списка ОС пользователя	Успех	Политика <имя политики> Добавление <наименование ОС>
		Ошибка	
Управление дисками			
6	Редактирование списка контролируемых загрузочных областей	Успех	Политика <имя политики> Добавление <имя объекта>
		Ошибка	
Контроль целостности среды UEFI			
7	Редактирование списка целостности среды UEFI	Успех	Политика <имя политики> Добавление <имя объекта>
		Ошибка	
Работа с учетными записями пользователей			
8	Создание учетной записи пользователя	Успех	Добавление <имя пользователя>
9	Обновление учетной записи пользователя	Успех	Редактирование <имя пользователя>
Работа с политиками аутентификации пользователей			
10	Создание политики аутентификации	Успех	Добавление <имя политики>
11	Обновление политики аутентификации	Успех	Редактирование <имя политики>
Работа с политиками контроля целостности объектов и загрузки ОС			
12	Создание политики контроля целостности объектов и загрузки ОС	Успех	Добавление <имя политики>
13	Обновление политики контроля целостности объектов и загрузки ОС	Успех	Редактирование <имя политики>

11.3 Экспорт журнала аудита

11.3.1 АБ имеет возможность экспортировать файл основного журнала аудита и дополнительного журнала применения шаблонов на внешнее устройство хранения данных. Для этого необходимо:

- подключить устройство хранения данных к ЭВМ;
- нажать кнопку ***«Экспорт основного журнала»*** или ***«Экспорт дополнительного журнала применения шаблонов»*** в зависимости от необходимости (рисунок 11.1);
- в появившемся окне указать директорию сохранения журнала, а также имя файла (рисунок 11.4);
- при успешном экспорте журнала на экран ЭВМ будет выведено сообщение (рисунок 11.5).

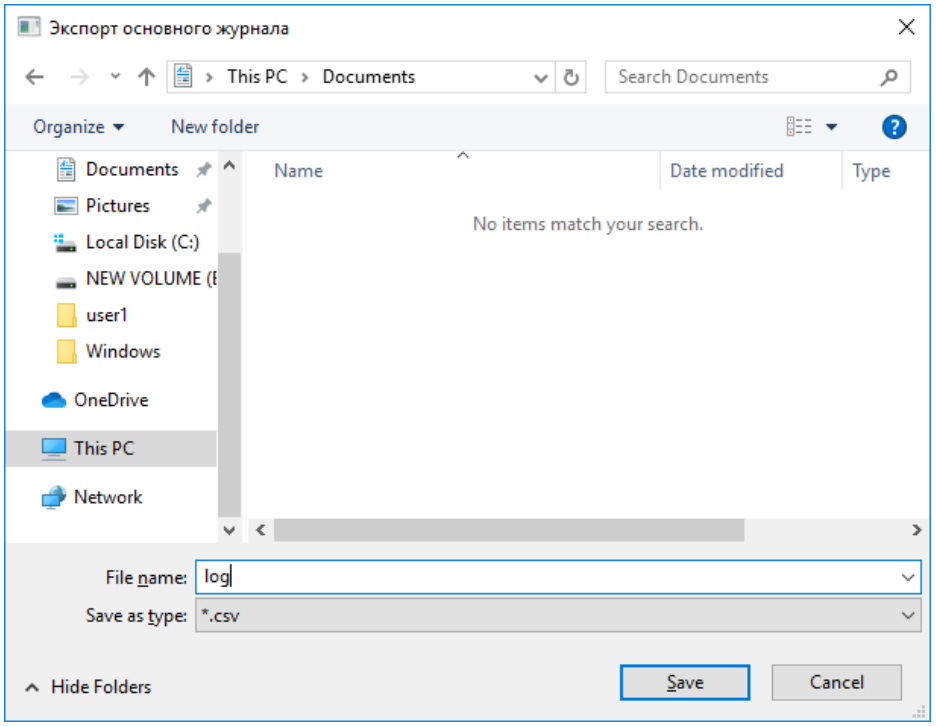


Рисунок 11.4 – Выбор устройства хранения данных для экспорта журнала аудита в файл

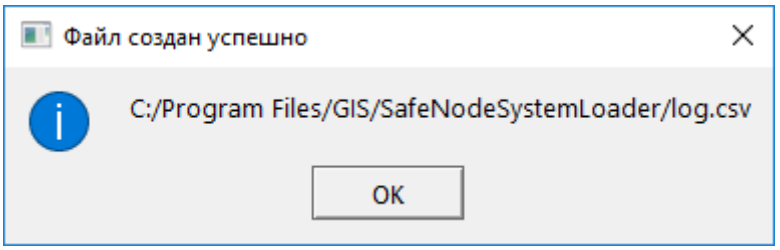


Рисунок 11.5 – Успешный экспорт журнала аудита

11.3.2 В случае существования на выбранном устройстве хранения данных файла с таким именем АБ на экран ЭВМ будет выведено предупреждение (рисунок 11.6).

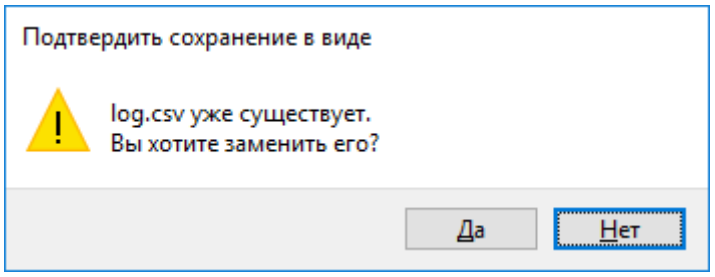


Рисунок 11.6 – Перезапись файла журнала аудита

Рекомендуется периодически осуществлять экспорт журнала на внешнее устройство хранения данных.

11.4 Очистка журнала аудита

11.4.1 АБ имеет возможность удалить записи журнала аудита без его экспорта.

11.4.2 Для очистки журналов АБ необходимо нажать на кнопку ***«Очистка»*** (рисунок 11.1), при этом в новом диалоговом окне подтвердить очистку журналов (рисунок 11.7).

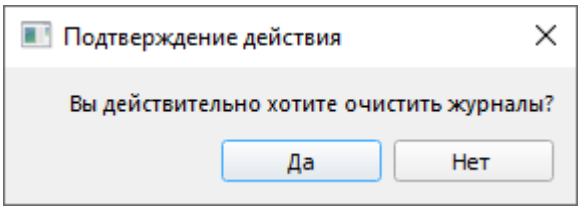


Рисунок 11.7 – Очистка журнала аудита

11.4.3 После завершения выполнения операции АБ будет выведено сообщение ***«Журналы аудита очищены»*** (рисунок 11.8) и в журнале аудита добавится запись о произведенной операции.

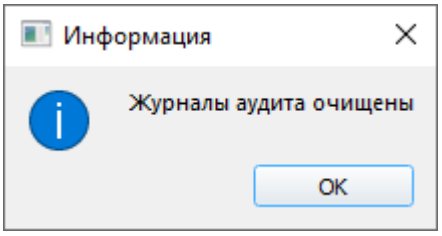


Рисунок 11.8 – Успешная очистка журналов аудита

11.5 Предупреждение о заполнении журналов

11.5.1 При заполнении журнала свыше 90% появится предупреждающая надпись (рисунок 11.9), в этом случае АБ рекомендуется выполнить экспорт журналов на внешний носитель.

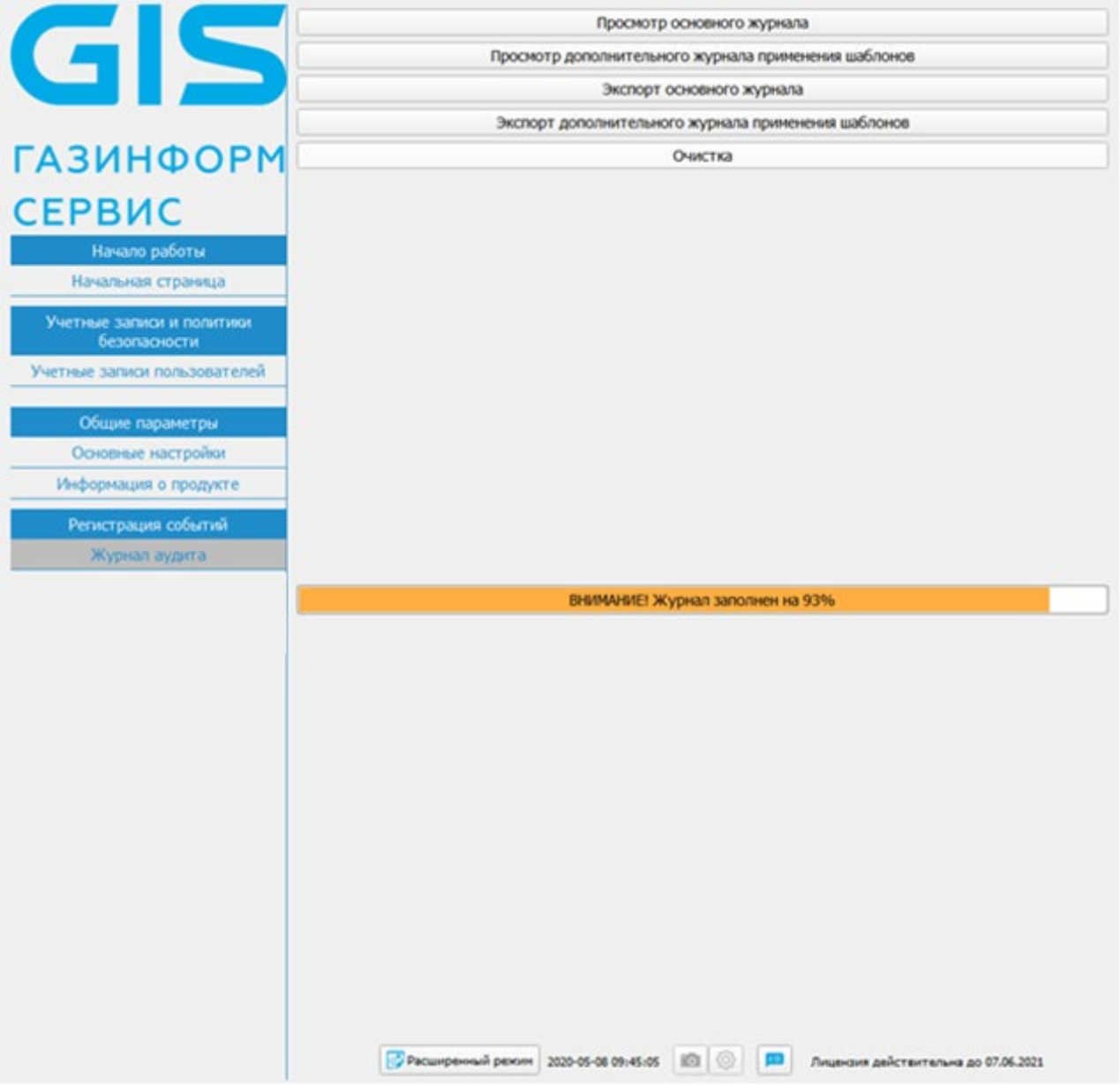


Рисунок 11.9 – Появление предупреждающей записи о заполненности журнала

11.5.2 В случае, если журнал заполнен свыше 95%, после осуществления успешной аутентификации и (или) идентификации АБ в консоли появится требование о необходимости экспорта журналов на внешний носитель.

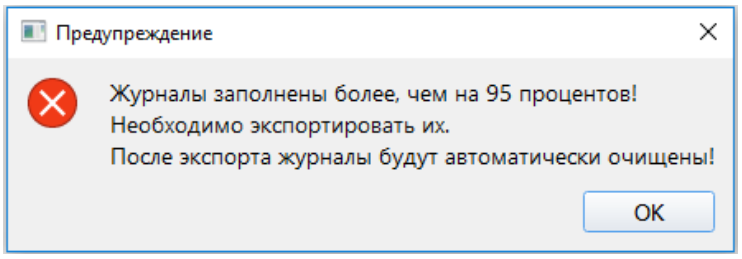


Рисунок 11.9 – Сообщение о заполненности журналов

11.5.3 Дальнейшая работа с консолью АБ Windows без выполнения процедуры экспорта журналов невозможна.

12 Интерфейс командной строки изделия

12.1 До начала работ с интерфейсом командной строки необходимо перейти в подраздел ***«Основные настройки»*** (рисунок 10.1) и установить параметр в поле ***«Интерфейс командной строки»***.

12.2 Поддерживается работа с интерфейсом командной строки в ОС семейства Windows и Linux:

- для ОС Windows осуществляется из утилиты командной строки **cmd.exe** с указанием ключа **--no-gui**;
- для ОС Linux осуществляется из терминала с указанием ключа **--no-gui**.

12.3 Опции и параметры при работе с интерфейсом командной строки аналогичны для всех видов операционных систем, отличия при работе параметров приведены в виде соответствующих примечаний в таблице 12.1.

Для работы с интерфейсом командной строки необходимо осуществить вход в ОС с административными правами. Для ОС Linux работа осуществляется с правами суперпользователя (sudo) или с помощью учетной записи root (учетная запись с полными правами доступа)

Для работы приложения в режиме командной строки необходимо выполнить аутентификацию АБ.

Аутентификация АБ осуществляется с использованием контрольной суммы пароля и\или PIN-кода АНП, при этом поддерживаются следующие алгоритмы расчета контрольных сумм: MD4, MD5, SHA1, SHA256, SHA384, SHA512.

Для ввода аутентификационных данных используются следующие ключи:

- -u опция для ввода имени пользователя (admin);
- -p опция для ввода контрольной суммы пароля АБ;
- -a опция для ввода контрольной суммы АНП АБ.

12.4 Опции и параметры для работы в командной строке приведены в таблице 12.1.

Таблица 12.1 – Опции и команды

Опция	Назначение и пример использования
-r <опция без параметров>	Команда удаления изделия с ЭВМ. Пример использования:

Опция	Назначение и пример использования
	SafeNodeSystemLoader –r
--rm-user <имя пользователя>	Команда удаления пользователя. Для удаления нескольких пользователей команда указывается несколько раз, но выполняется одной транзакцией. При возникновении ошибки удаления одного пользователя из перечня команда не будет выполнена. Пример использования: SafeNodeSystemLoader --rm-user user1 --rm-user user2 --rm-user user3
--add-user <имя файла> Параметры: --userFmt <формат входных данных> Формат входных данных является необязательным параметром, по умолчанию используется .xml	Команда добавления пользователя. Для добавления пользователя необходимо указать файл в заданном формате. Пример использования: 1) SafeNodeSystemLoader --add-user "user.xml" 2) SafeNodeSystemLoader --add-user "user.json" --userFmt json
--edit-user <имя файла> Параметры: --userFmt <формат входных данных> Формат входных данных является необязательным параметром, по умолчанию используется .xml	Команда редактирования пользователя. Для обновления данных пользователя необходимо указать файл в заданном формате. Пример использования: 1) SafeNodeSystemLoader --edit-user "user.xml" 2) SafeNodeSystemLoader --edit-user "user.json" --userFmt json
--rm-authPol <имя политики>	Команда удаления политик аутентификации. Для удаления нескольких политик команда указывается несколько раз, но выполняется одной транзакцией. При возникновении ошибки удаления одной политики аутентификации из перечня команда не будет выполнена. Пример использования: SafeNodeSystemLoader --rm-authPol policy1 --rm-authPol policy2 --rm-authPol policy3

Опция	Назначение и пример использования
--add-authPol <имя файла> Параметры: --authPolFmt <формат входных данных> Формат входных данных является необязательным параметром, по умолчанию используется .xml	Команда добавления политики аутентификации. Для добавления политики аутентификации необходимо указать файл в заданном формате. Пример использования: 1) SafeNodeSystemLoader --add-authPol "authPolicy.xml" 2)SafeNodeSystemLoader --add-authPol "authPolicy.json" --authPolFmt json
--rm-intOsPol <имя политики>	Команда удаления заданных политик контроля целостности. Для удаления нескольких политик контроля целостности команда указывается несколько раз, но выполняется одной транзакцией. При возникновении ошибки удаления одной политики контроля целостности из перечня команда не будет выполнена. Пример использования: SafeNodeSystemLoader --rm-intOsPol policy1 --rm-authPol policy2 --rm-authPol policy3
--add-intOsPol <параметры> Параметры: --intOsPolicyName <имя политики> --blockType <тип блокировки> Параметры являются обязательными к указанию	Команда добавления политики контроля целостности. Добавление политики контроля целостности осуществляется с заданием всех необходимых параметров. Пример использования: SafeNodeSystemLoader --add-intOsPol --intOsPolicyName policy1 --blockType 1
--export-log <параметры> Параметры: --log-fileName <имя файла для экспорта> --log-format <формат экспортируемого файла> Формат экспортируемого файла является необязательным параметром для указания, по	Команда экспорта журнала аудита

Опция	Назначение и пример использования
умолчанию используется формат .csv	
--exit-sm <опция без параметров>	Выход из мягкого режима. Пример использования: SafeNodeSystemLoader --exit-sm
--apply-template <имя файла> Параметры: --vol <имя раздела диска, к которому применяется политика>	Применение шаблона. Пример использования: SafeNodeSystemLoader --apply-template "template.xml" --vol "C:" При работе в ОС Linux в качестве аргумента для параметра **vol** необходимо передать раздел **root "/"** или точку монтирования, если шаблон применяется на примонтированный раздел (например, **"/mnt/fat_partition"**)
--get-info <имя каталога для сохранения информации> Параметры: --rewrite-files перезапись файлов При указании данного параметра, сохраненные ранее файлы info.txt и checksums.txt, будут перезаписаны.	Получение информации о продукте. Пример использования: SafeNodeSystemLoader.exe --get-info "./info" --rewrite-files
--registrate Параметры: --license-key ключ лицензии --email электронная почта, на которую приходят сообщения сервиса лицензирования --reactivate флаг реактивации, если он выставлен, то будет выполнена реактивация	Регистрация ключа лицензии. Пример использования: SafeNodeSystemLoader.exe --registrate --license-key "AAAAA-BBBBB-CCCCC-DDD" --email "user@test.ru"
--activate Параметры: --license-key ключ лицензии	Активация лицензии. Пример использования:

Опция	Назначение и пример использования
--email электронная почта, на которую приходят сообщения сервиса лицензирования --activationKey ключ активации --reactivate флаг реактивации, если он выставлен, то будет выполнена реактивация	SafeNodeSystemLoader --activate --license-key "AAAAA-BBBBB-CCCCC-DDD" --email "user@test.ru" --activation-key "EEEE-FFF-GGG-HHHH"
--update	Запись флага обновления в базу данных. Пример использования: SafeNodeSystemLoader --update
--network-system t/f включение/выключение сетевой подсистемы. --auth-ldap t/f включение/выключение аутентификации LDAP --ldap-location "CN=%s,CN=Users" задание префикса и суффикса пользователей --using-kerberos t/f включение/выключение Kerberos --using-whitelist t/f включение/выключение белого списка	Управление сетевыми настройками. Примеры использования: 1) Включение сетевой подсистемы: SafeNodeSystemLoader --network-system t 2) Выключение сетевой подсистемы: SafeNodeSystemLoader --network-system f 3) Выключение сетевой подсистемы и включение Kerberos SafeNodeSystemLoader --network-system f --using-kerberos t
--new-password <new passw> --pwd-type <2> Параметры: --new-password задается новый пароль в виде строки base64 шифрованный на хеш-сумме текущего пароля --pwd-type тип хеш-суммы нового пароля	Смена пароля администратора
--write-bios	Загрузка модулей в BIOS

12.5 В таблице 12.1 указаны примеры использования команд без флага ***–no gui*** и аутентификации АБ. Пример полной записи команды удаления СДЗ выглядит следующим образом:

SafeNodeSystemLoader.exe --no-gui -r -u admin -p 29ac25660e3078e87e3097d3822e50d7[8]

12.6 Поддерживаются два текстовых формата передачи данных для конфигурирования параметров изделия: *.xml и *.json.

12.7 Коды возврата командной строки приведены в Приложении Г настоящего документа.

[8] В данной версии ПО поддерживается удаление графической консоли АБ без указания контрольной суммы пароля АБ.

13 Завершение работы

13.1 Завершение работы с консолью доступно в главном окне консоли АБ Windows (рисунок 4.2) по кнопке « × ».

13.2 Для консоли АБ Linux доступна перезагрузка и выключение ЭВМ по кнопкам ***«Перезагрузка»*** и ***«Выключение»*** соответственно (рисунок 1.4).

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.

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».

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 В консоли АБ Windows СДЗ «SafeNode System Loader» будет отображена информация о том, что СДЗ взято под управление (рисунок 14.1).

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

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

14.3.10 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.

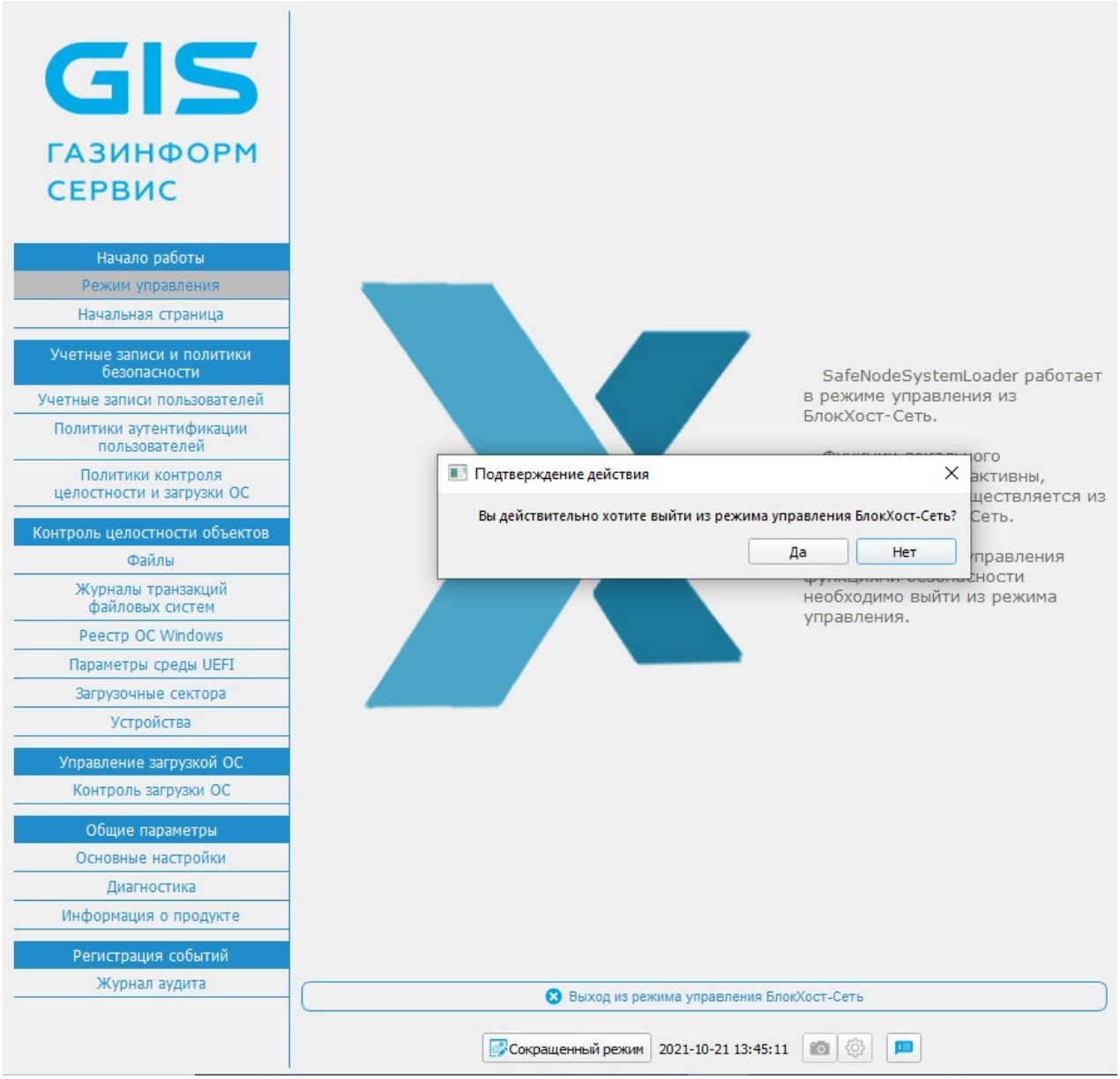


Рисунок 14.2 – Вывод консоли из-под управления СЗИ от НСД «Блокхост-Сеть 4»

14.3.11 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.

14.3.12 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 доменных пользователей и пользователей СДЗ 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.

14.3.13 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.

14.3.14 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.

14.3.15 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».

14.3.16 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».

14.3.17 Подробная информация об управлении параметрами аутентификации пользователей СДЗ «SafeNode System Loader» с помощью СЗИ от НСД «Блокхост-Сеть 4» приведена в разделе «Управление аутентификацией» документа «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора. Часть 1. Управление политиками».

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.

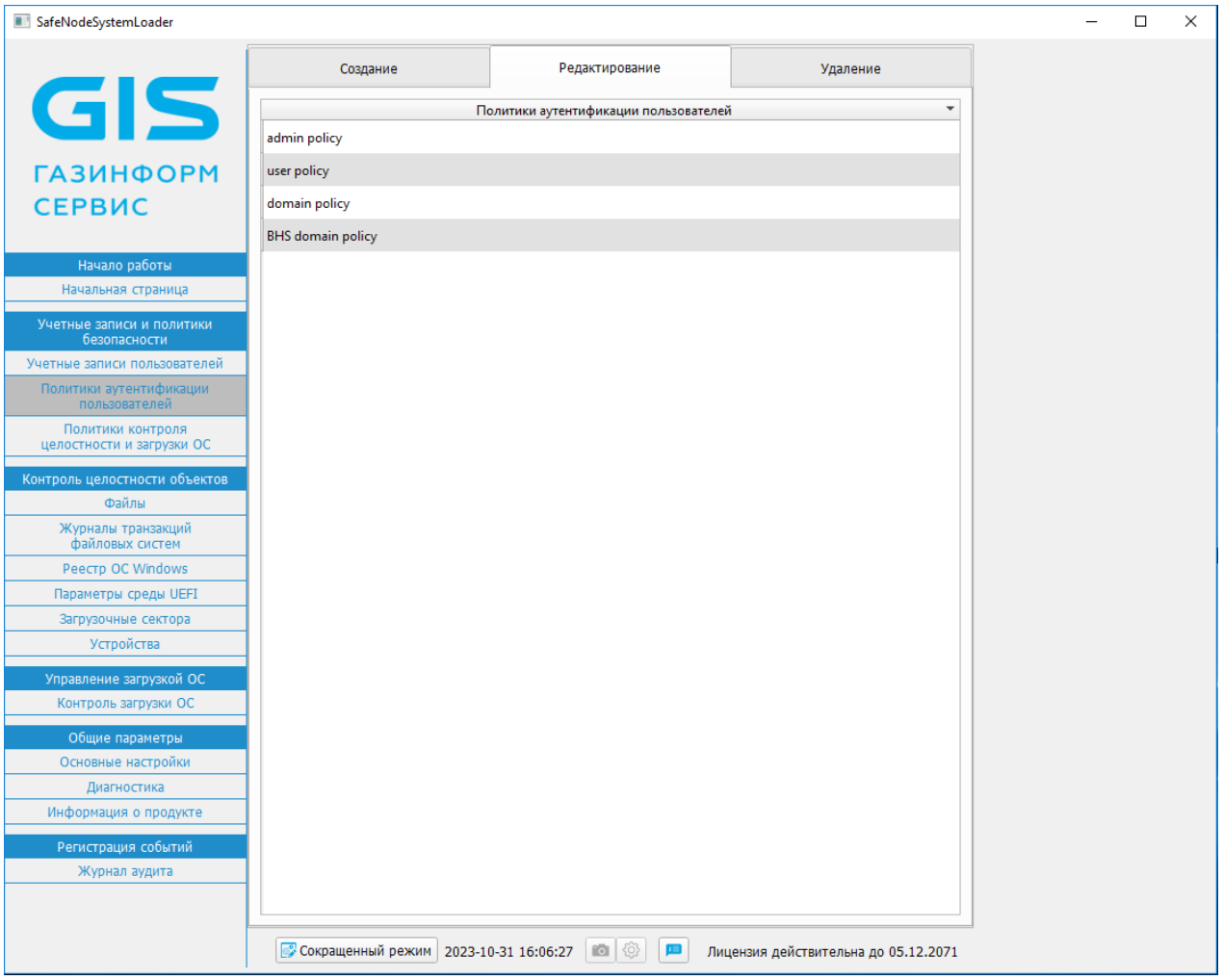


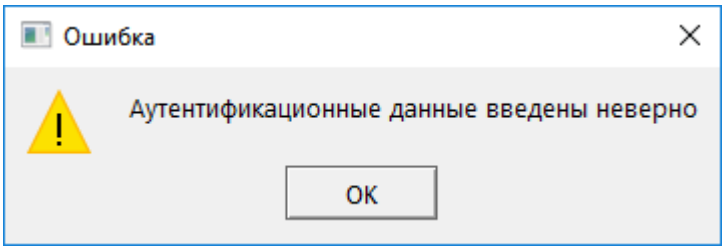
Рисунок 14.3 – Добавление политики аутентификации BHS domain policy

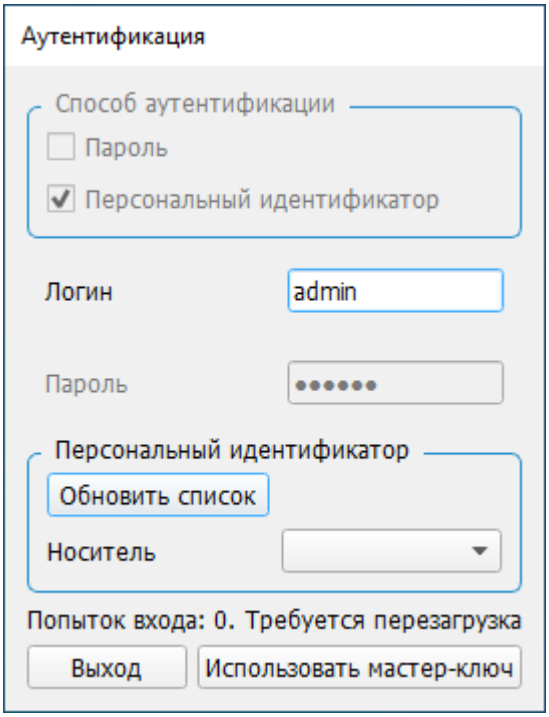
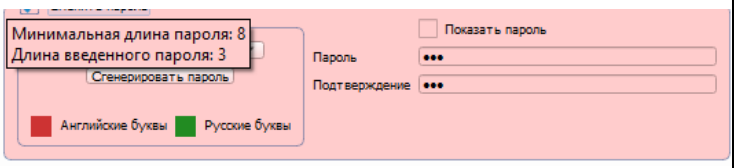
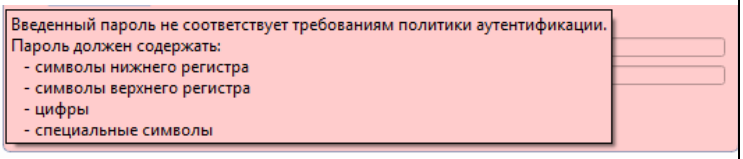
15 Сообщения об ошибках и порядок действий по их устранению

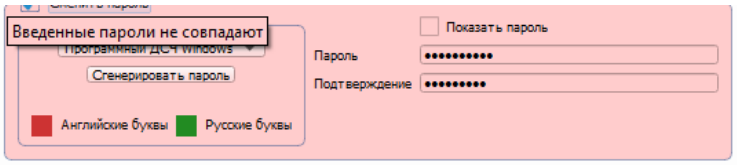
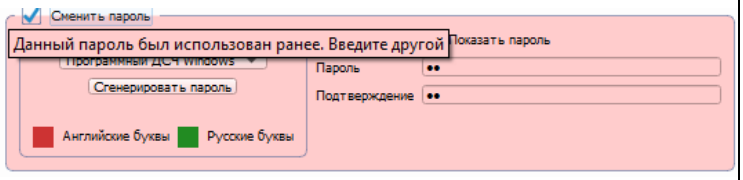
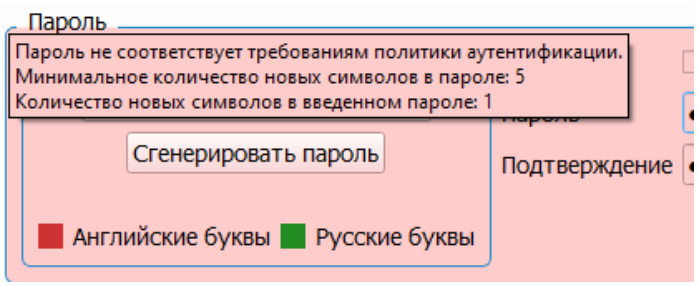
15.1 В процессе работы изделия в составе ЭВМ возможно возникновение ситуаций, при которых на экран ЭВМ в диалоговых окнах выдаются различные информационные сообщения и сообщения об ошибках.

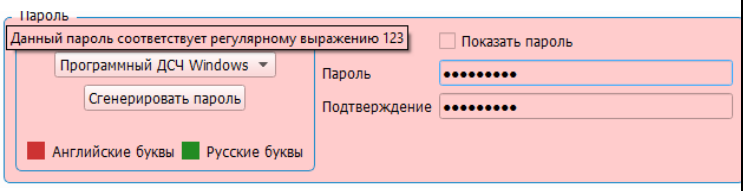
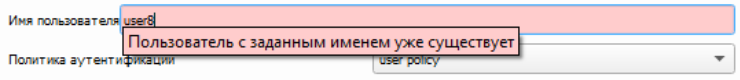
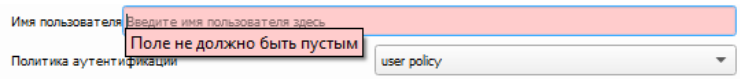
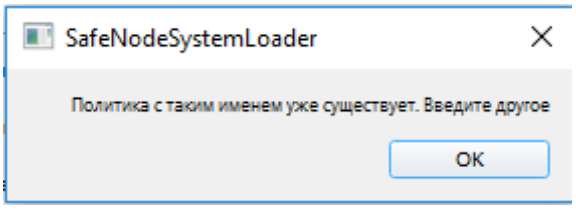
15.2 Перечень сообщений и их типы, причины возникновения и порядок действий АБ по их устранению приведен в таблице 15.1.

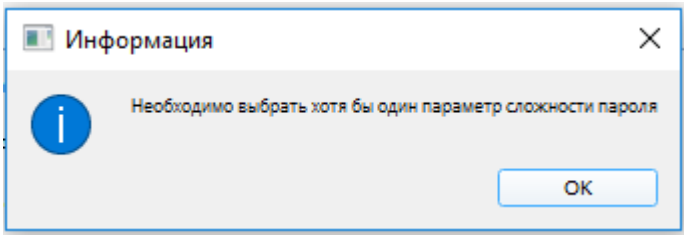
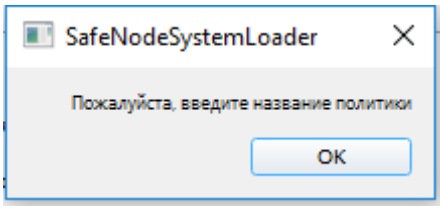
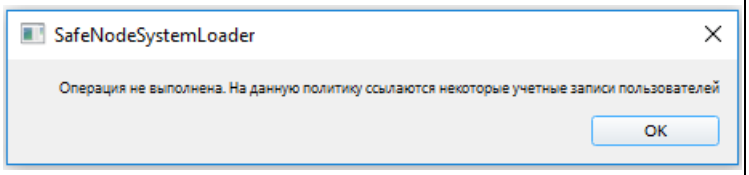
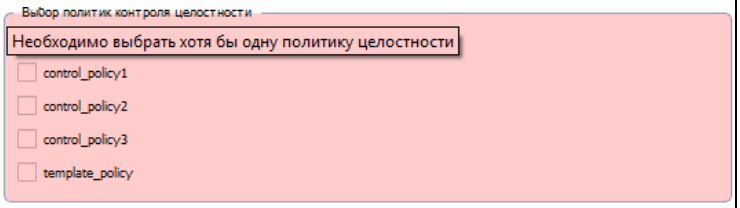
Таблица 15.1 – Перечень сообщений об ошибках при работе ПО изделия

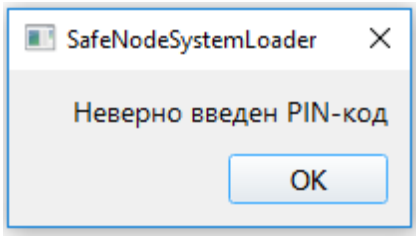
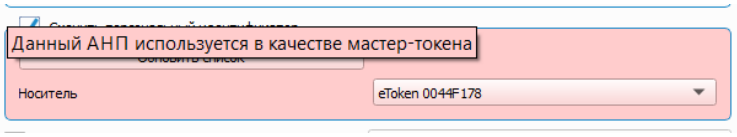
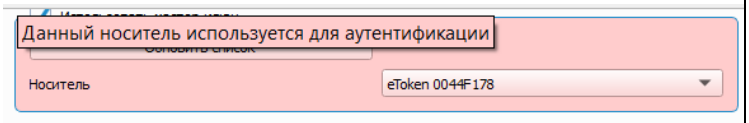
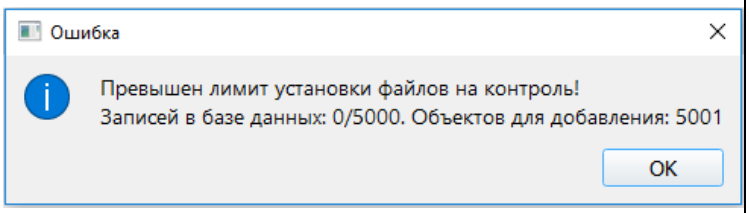
№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий АБ
1	**Аутентификационные данные введены неверно** 	**Причины:** Указание неверного идентификатора, пароля или имени учетной записи пользователя **Порядок действий:** Проверить корректность указанных аутентификационных и идентификационных данных пользователя
2	**Попыток входа: 0. Требуется перезагрузка**	**Причины:** Возникает при исчерпании всех попыток аутентификации пользователя **Порядок действий:** Выключить или перезагрузить ЭВМ и повторно выполнить процедуру идентификации и аутентификации. В случае утраты аутентификационных данных АБ воспользоваться мастер-ключом

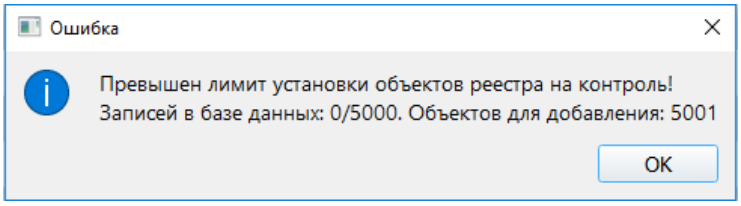
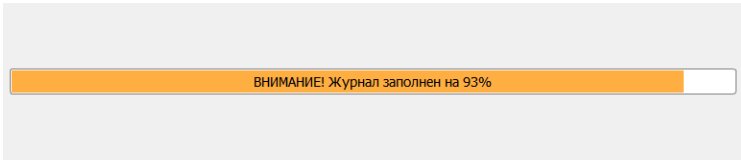
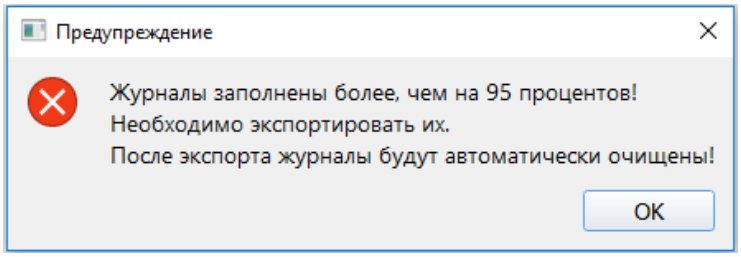
№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий АБ
		
3	**Длина пароля не соответствует требованиям по длине пароля** 	**Причины:** Новый пароль пользователя не удовлетворяет требованиям по минимальной длине пароля **Порядок действий:** Ввести пароль длиной не менее 8 символов
4	**Введенный пароль не соответствует требованиям политики аутентификации** 	**Причины:** Новый пароль пользователя не удовлетворяет требованиям паролю согласно политике аутентификации **Порядок действий:** Ввести пароль, который удовлетворяет сложности согласно политике аутентификации: длина, строчная и (или) заглавная буква и (или) спецсимвол и (или) цифра

№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий АБ
5	**Введенные пароли не совпадают** 	**Причины:** Несовпадение нового пароля и его подтверждения при создании учетной записи пользователя **Порядок действий:** Ввести верный новый пароль и его подтверждение
6	**Данный пароль был использован ранее. Введите другой** 	**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.
7	**Пароль не соответствует требованиям политики аутентификации. Минимальное количество символов в пароле: N1.** **Количество новых символов в введенном пароле: N2** 	**Причины:** Новый пароль пользователя не удовлетворяет требованиям r паролю согласно политике аутентификации **Порядок действий:** Ввести пароль, который удовлетворяет сложности согласно политике аутентификации: минимальное число уникальных символов в пароле

№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий АБ
8	**Данный пароль соответствует регулярному выражению** 	**Причины:** Новый пароль совпадает с паролем из перечня небезопасных паролей **Порядок действий:** Необходимо указать новый пароль пользователя, который удовлетворяет требованиям согласно политике аутентификации
9	**Пользователь с заданным именем уже существует** 	**Причины:** 1) При создании учетной записи пользователя указано имя уже существующего пользователя. 2) Пользователь с таким именем учетной записи был удален, но запись еще хранится в БД изделия. **Порядок действий:** Указать другое имя учетной записи пользователя
10	**Поле не должно быть пустым** 	**Причины:** При создании новой учетной записи пользователя заполнены не все поля, обязательные к заполнению **Порядок действий:** Заполнить все обязательные поля
11	**Политика с таким именем уже существует. Введите другое** 	**Причины:** При создании политики аутентификации (политики КЦ и загрузки ОС) указано имя уже существующей политики **Порядок действий:** Указать другое имя для создаваемой политики

№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий АБ
12	**Необходимо выбрать хотя бы один параметр сложности пароля** 	**Причины:** При создании новой политики аутентификации не заполнен параметр сложности пароля **Порядок действий:** Выбрать хотя бы один параметр сложности пароля
13	**Необходимо ввести название политики** 	**Причины:** При создании новой политики не заполнено название политики **Порядок действий:** Заполнить название политики
14	**На политику ссылаются некоторые 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.
15	**Необходимо выбрать хотя бы одну политику целостности** 	**Причины:** При создании учетной записи пользователя не добавлена политика КЦ и загрузки ОС **Порядок действий:** Добавить политику и сохранить изменения

№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий АБ
16	**Неверно введен PIN-код** 	**Причины:** Неверно указан PIN-код носителя при создании учетной записи пользователя **Порядок действий:** Ввести верный PIN-код носителя
17	**Данный АНП используется в качестве мастер-токена** 	**Причины:** В качестве АНП пользователю (АБ) выбран носитель, который используется в качестве мастер-ключа администратора **Порядок действий:** Выбрать другой АНП
18	**Данный носитель используется для аутентификации** 	**Причины:** В качестве мастер-ключа администратора выбран носитель, который используется в качестве АНП для входа пользователем или АБ **Порядок действий:** Выбрать другой АНП
19	**Превышен лимит установки файлов на контроль** 	**Причины:** Превышение максимально установленного значения при постановке файлов на КЦ. **Порядок действий:** 1. Установить меньшее количество файлов на КЦ, согласно ограничениям. 2. Отредактировать значение максимально устанавливаемого количества объектов на КЦ.

№	Сообщение на экране ЭВМ	Причины появления сообщения и порядок действий АБ
20	**Превышен лимит установки объектов реестра на контроль!** 	**Причины:** 1. Превышение максимально установленного значения при постановке объектов реестра на КЦ. **Порядок действий:** 1. Установить меньшее количество объектов реестра на КЦ, согласно ограничениям. 2. Отредактировать значение максимально устанавливаемого количества объектов на КЦ.
21	**Внимание! Журнал заполнен на 93%** 	**Причины:** Предупреждающее сообщение о заполнении журналов более чем на 90%. Возможна аутентификация и идентификация АБ и пользователей. **Порядок действий:** Выполнить аутентификацию и идентификацию АБ в системе и сохранить журнал на внешний носитель.
22	**Журналы заполнены более, чем на 95 процентов!** 	**Причины:** Сообщение о заполнении журналов на 95%. Возможна аутентификация и идентификация АБ **Порядок действий:** Выполнить аутентификацию и идентификацию АБ в системе и сохранить журнал на внешний носитель

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/	*
31	/lib/modules/NNN/	*

Приложение В

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

В таблице В.1 приведено соответствие между названиями основных ветвей реестра ОС Windows и названиями ветвей реестра, отображаемыми в редакторе реестра regedit.

Таблица В.1 – Соответствие названий разделов реестра в консоли АБ Windows и редакторе реестра regedit

№ п/п.	Название объектов реестра в консоли АБ (имя файла)	Название объектов реестра в редакторе regedit
<Имя устройства хранения данных>:\Windows		
1	COMPONENTS	
2	DEFAULT	HKEY_USERS\.DEFAULT
3	SAM	HKEY_LOCAL_MACHINE\SAM
4	SECURITY	HKEY_LOCAL_MACHINE\SECURITY
5	SOFTWARE	HKEY_LOCAL_MACHINE\SOFTWARE
6	SYSTEM	HKEY_LOCAL_MACHINE\SYSTEM
<Имя устройства хранения данных>:\Boot		
7	BCD	HKEY_LOCAL_MACHINE\BCD00000000

В таблице В.2 приведено соответствие между названиями основных ветвей реестра ОС Linux и названиями ветвей реестра, отображаемыми в редакторе реестра regedit.

Таблица В.2 – Соответствие названий разделов реестра в консоли АБ Linux и редакторе реестра regedit

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

Приложение Г

Коды возврата командной строки

Таблица Г.1 – Коды возврата и описание

№	Код возврата	Описание кода
1	000	Нет ошибки
2	001	Неправильно указана учетная запись пользователя
3	002	Ошибка чтения из БД
4	003	Ошибка обновления БД
5	004	Ошибка добавления в БД
6	005	Ошибка удаления из БД
7	006	Выход за границы диапазона при работе с таблицей
8	007	Новый пароль совпадает с паролем, хранимым в БД
9	008	Пароль не удовлетворяет требованиям политики аутентификации
10	009	Указан неверный PIN-код АНП
11	010	АНП не подключен
12	011	Невозможно установить заданный PIN-код
13	012	Неизвестная ошибка при работе с АНП
14	013	Пользователь с таким именем уже существует
15	014	АНП уже назначен другому пользователю
16	015	АНП не назначен пользователю
17	016	Невозможно удалить политику, так как она назначена пользователю
18	017	Необходимо указать хотя бы одну политику целостности
19	018	Учетную запись АБ удалить нельзя
20	019	Отмена действия
21	020	Необходимо сменить аутентификационные данные

№	Код возврата	Описание кода
22	021	Ошибка аутентификации
23	022	Учетная запись пользователя не найдена
24	023	Транзакция неуспешна
25	024	Интерфейс командной строки недоступен
26	025	Политика не найдена
27	026	Операция не поддерживается
28	027	Данная операция не реализована
29	028	Неверный параметр
30	029	Неверное значение привилегии
31	030	Неверное значение сложности пароля
32	031	Неверный тип аутентификации
33	032	Неверный тип блокировки
34	033	Имя не соответствует необходимым условиям
35	034	Ошибка экспорта журнала аудита
36	035	Ошибка разбора файла
37	036	Файл не найден
38	037	Не удается открыть файл
39	038	Ошибка инициализации приложения
40	039	Необходима активация
41	040	Ошибка проверки ключа лицензии
42	041	Ошибка регистрации лицензии
43	042	Ошибка генерации запроса на активацию
44	043	Ошибка активации
45	044	Ошибка сохранения лицензии в БД
46	045	Лицензия уже активирована

№	Код возврата	Описание кода
47	046	Некорректное им таблицы при попытке обновления базы данных
48	047	Не удалось выполнить запрос
49	048	Не удалось создать резервную копию
50	049	Не удалось заменить старую БД новой
51	050	Не удалось получить доступ к БД
52	051	Необходимо перезагрузка
53	052	Необходимо подтверждение электронной почты
54	053	Не удалось записать данные на носитель
55	054	Пользователь заблокирован
56	055	Неизвестная ошибка

Приложение Д

Поддержка списка отозванных сертификатов

В изделии реализована поддержка списка отозванных сертификатов. Для его настройки необходимо проделать следующие шаги:

- аутентифицироваться доменным администратором в операционной системе;

При настройке списка отозванных сертификатов с помощью графического интерфейса в ОС Linux, достаточно аутентифицироваться администратором ОС при входе.

- аутентифицироваться администратором изделия в графической консоли;
- перейти в меню ***«Общие параметры»*** → ***«Основные настройки»*** → ***«Настройки LDAP»*** (рисунок 10.3);

Проконтролировать, что все предварительные настройки для подключения LDAP аутентификации произведены корректно (см. подраздел 10.2).

- активировать поля ***«Аутентификация LDAP»*** и ***«Использование Kerberos»***;
- проконтролировать, что в конфигурационном файле ***krb5.conf*** указаны корректные параметры в соответствии с текущими настройками домена и указан путь сохранения списка отозванных сертификатов (***pkinit_revoke***), пример настроек приведен ниже:

pkinit_require_crl_checking = false
pkinit_eku_checking = none
pkinit_kdc_hostname = s09dc.pki.local
pkinit_anchors = FILE:/EFI/GIS/Db/root.cer[9]
pkinit_revoke = FILE:/EFI/GIS/Db/crl.crl
pkinit_identities = PKCS11:/

- перейти в поле ***«Редактирование списка пользователей»*** и выполнить аутентификацию в домене. Список отозванных сертификатов будет сформирован автоматически.

[9] Корневой сертификат root.cer должен содержать точку распределения CRL.

В случае, если все описанные выше шаги проделаны корректно, по указанному пути появится файл, который будет содержать список отозванных сертификатов (рисунок Д.1).

Настройка параметров LDAP через файлы конфигураций ***hosts***, ***krb5.conf*** и ***ldap.conf*** может быть осуществлена через стандартный механизм политики «Настройка подключения к домену» СЗИ от НСД «Блокхост-Сеть 4».

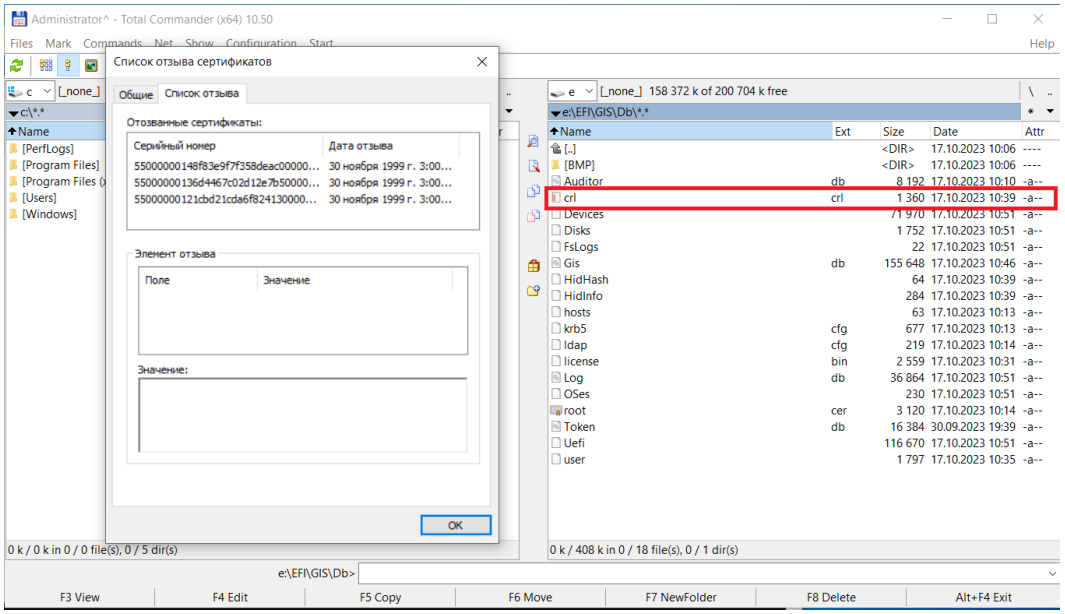


Рисунок Д.1 – Пример расположения и содержания списка отозванных сертификатов

При попытке аутентификации пользователя, у которого отозван сертификат, появится соответствующее сообщение об ошибке (рисунок Д.2).

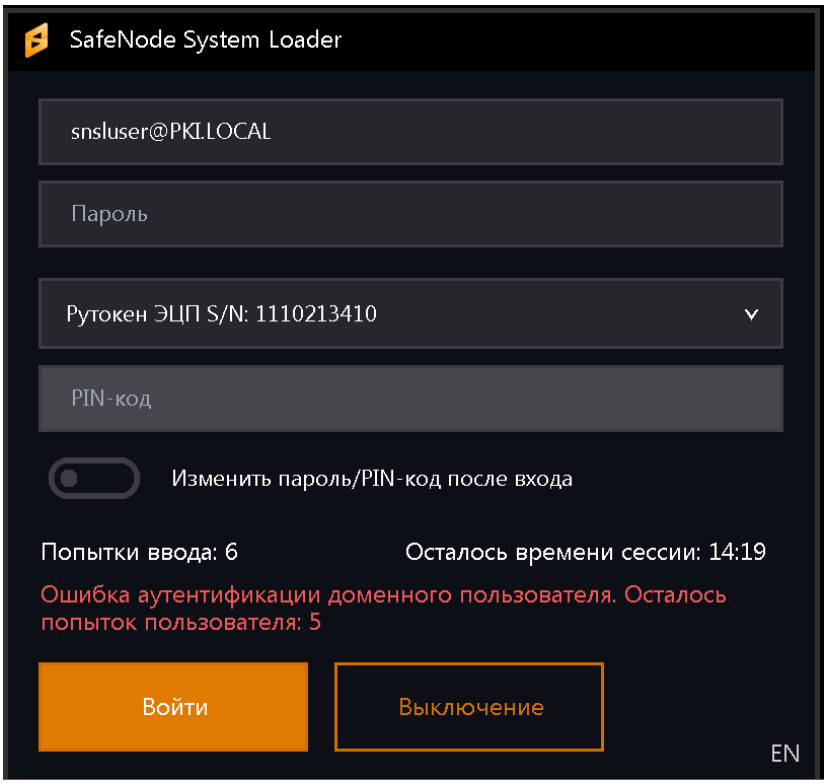


Рисунок Д.2 – Сообщение об ошибке

В случае отзыва сертификата у пользователя, администратору необходимо повторить проделанные шаги и обновить список отозванных сертификатов. В противном случае, вход пользователя с отозванным сертификатом будет возможен.

Перечень сокращений

BIOS	–	Basic Input Output System (базовая система ввода-вывода)
EXT3, EXT4	–	Extended File System (расширенная файловая система)
GPT	–	GUID Partition Table (таблица разделов GUID, часть спецификации UEFI)
LDAP	–	Lightweight Directory Access Protocol (протокол прикладного уровня для доступа к службе каталогов X.500)
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 хеширования)
SSD	–	Solid-State Drive (твердотельный накопитель)
TLS	–	Transport Layer Security (протокол защиты транспортного уровня)
UEFI	–	Unified Extensible Firmware Interface
USB	–	Universal Serial Bus
АБ	–	администратор безопасности
АРМ	–	автоматизированное рабочее место
АНП	–	аутентификационный носитель пользователя
БД		база данных
ГОСТ		государственный стандарт

ИАФ		идентификация и аутентификация
КЦ	–	контроль целостности
ОС	–	операционная система
ПО	–	программное обеспечение
СДЗ	–	средство доверенной загрузки
ФС		файловая система
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю России
ЭВМ	–	электронно-вычислительная машина
ЭД	–	эксплуатационная документация
ЭЦП	–	электронная цифровая подпись