АКЦИОНЕРНОЕ ОБЩЕСТВО

«Аладдин Р.Д.»

УТВЕРЖДЕН

RU.АЛДЕ.03.01.046 32 01–ЛУ

СРЕДСТВО ЗАЩИТЫ ИНФОРМАЦИИ НА СЪЕМНЫХ МАШИННЫХ НОСИТЕЛЯХ

SECURFLASH

Руководство системного программиста

RU.АЛДЕ.03.01.046 32 01

Листов 91

2025

Литера O_1

Подпись и дата	
Инв. № дубл.	
Взам. инв. №	
Подпись и дата	
Инв. № подл.	

АННОТАЦИЯ

Настоящий документ представляет собой руководство системного программиста программного средства RU.АЛДЕ.03.01.046 «Средство защиты информации на съемных машинных носителях SecurFlash» (далее – программное средство). Документ предназначен для уполномоченного персонала, осуществляющего установку, администрирование и аудит программного средства.

Документ содержит общие сведения о данном программном средстве, его структуре, установке, настройке, администрировании и аудите в среде поддерживаемых операционных систем, а также о работе с программными компонентами RU.АЛДЕ.03.01.047 «Программа администратора SecurFlash» (далее — программа администратора) и RU.АЛДЕ.03.01.049 «Сервер управления SecurFlash» (далее — сервер управления), которые входят в состав программного средства.

СОДЕРЖАНИЕ

ПРИНЯТЫЕ СОКРАЩЕНИЯ

ВПУЗ — встроенная привилегированная учетная запись администратора;

КОИ — контур обработки информации;

ОС — операционная система;

ПА — программа администратора;

ПП — программа пользователя;

СВТ — средства вычислительной техники;

СУ — сервер управления.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Администратор программного средства (администратор): Уполномоченный сотрудник, осуществляющей установку, настройку и администрирование программного средства.

Базовый пароль: пароль, заданный при создании учетной записи пользователя.

Контур обработки информации: совокупность СВТ с предустановленными ОС и компонентами программного средства, учетных записей и инициализированных носителей, администрируемых под управлением одного сервера управления.

Политики безопасности: набор предустановленных администратором настроек безопасности, используемый в рамках текущего контура обработки информации.

Пользователь программного средства (пользователь): Уполномоченный сотрудник, имеющий права на работу с инициализированным носителем после предоставления ему соответствующих прав администратором.

Программа администратора: Программа администратора SecurFlash RU.АЛДЕ.03.01.047 - программный компонент из состава программного средства, предназначенный для администрирования: политик безопасности, учетных записей, носителей, разрешений, режима аудита.

Программа пользователя: Программа пользователя SecurFlash RU.АЛДЕ.03.01.048 - программный компонент из состава программного средства, предназначенный для обеспечения санкционированного доступа пользователей к инициализированным носителям.

Программное средство: Средство защиты информации на съемных машинных носителях SecurFlash.

Сервер управления (сервер): Сервер управления SecurFlash RU.АЛДЕ.03.01.049 – программный компонент из состава программного средства, предназначенный для обеспечения развертывания контура обработки информации на одном или нескольких СВТ.

Носитель (машинный носитель): «Доверенный корпоративный флеш-накопитель Aladdin eFlash» АЛДЕ.467669.061 со встроенным разъемом USB (тип А). Приобретается отдельно.

Файл-контейнер (контейнер): Хранилище атрибутов безопасности. Для доступа к нему устанавливается пароль.

Централизованная иерархическая система (иерархическая система): Совокупность взаимосвязанных между собой серверов управления из состава программного средства, образованная от одного (центрального) сервера управления, с правом нижестоящих (по отношению к центральному) серверов управления на добавление новых серверов управления, использующаяся при построении территориально распределенной структуры объектов.

1 ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММНОМ СРЕДСТВЕ

1.1 Назначение

Программное средство «Средство защиты информации на съемных машинных носителях SecurFlash» RU.АЛДЕ.03.01.046 предназначено для управления доступом к информации, хранящейся на инициализированных носителях.

1.2 Требования к операционным системам

Программное средство осуществляет функционирование в среде следующих операционных систем (далее — ОС):

- Windows 7 SP1;
- Windows 10;
- Astra Linux 1.6 SE «Смоленск» (x64);
- Astra Linux 1.7 SE «Смоленск» (x64);
- Альт 8 СП.

1.3 Требования к аппаратному обеспечению

1.3.1 Требования к средствам вычислительной техники

Минимальные требования к аппаратной конфигурации средств вычислительной техники (далее – СВТ) соответствуют аналогичным требованиям ОС, на которые устанавливается программное средство.

Разрешение экрана монитора СВТ должно быть не менее 1024x768 точек.

Для обращения программного средства к носителям используются свободные USB-порты (типа A).

1.3.2 Требования к носителям

В качестве носителя используется «Доверенный корпоративный флеш-накопитель Aladdin eFlash» АЛДЕ.467669.061.

Поддерживаемая емкость носителя – до 1 ТБ.

1.4 Эксплуатационные ограничения при работе с носителями

1.4.1 Срок использования носителя

Рекомендуемый срок использования носителя — один год[1].

1.5 Требования безопасности при работе с носителями

Извлечение носителя должно выполняться только после отключения скрытого раздела. Отключение скрытого раздела выполняется с использованием программы пользователя.

Извлечение носителя должно выполняться только после успешного выполнение процедуры «Безопасное извлечение устройств и дисков» (для операционных систем семейства Microsoft Windows) или команды (процедуры) размонтирования (для операционных систем семейства Linux). Это связано с особенностями работы операционных систем с внешними запоминающими устройствами (дисками): для ускорения работы часть данных сохраняется в памяти СВТ и при некорректном извлечении носителя эти данные скорее всего будут потеряны (не будут принудительно записаны на носитель во время выполнения процедуры извлечения).

Не рекомендуется открытие хранимых на носителе документов непосредственно на самом носителе. Для работы с документами необходимо скопировать их на локальный диск СВТ. Это связано с тем, что при открытии документов на носителе происходит преждевременное исчерпание ресурсов встроенной флеш-памяти за счет работы автоматического сохранения.

[1] Применяемые при эксплуатации программного средства носители покупаются отдельно и могут использовать флеш-память различного типа, с различным допустимым количеством циклов перезаписи, поэтому срок использования носителя носит рекомендательный характер и может уточнятся эксплуатирующей организацией в зависимости от модели применяемых накопителей и интенсивности их эксплуатации.

2 СТРУКТУРА ПРОГРАММНОГО СРЕДСТВА

2.1 Состав программного средства

Программное средство включает в свой состав:

– программный компонент «Программа администратора SecurFlash» RU.АЛДЕ.03.01.047 (далее – программа администратора, ПА) предназначена для администрирования: политик безопасности, учетных записей, носителей, разрешений, режима аудита;

– программный компонент «Программа пользователя SecurFlash» RU.АЛДЕ.03.01.048 (далее – программа пользователя, ПП) предназначена для обеспечения санкционированного доступа пользователей к скрытым разделам инициализированных носителей;

– программный компонент «Сервер управления SecurFlash» RU.АЛДЕ.03.01.049 (далее – сервер управления, СУ) предназначен для обеспечения развертывания контура обработки информации на одном или нескольких СВТ.

2.2 Описание контура обработки информации

Под контуром обработки информации (далее — КОИ) подразумевается совокупность СВТ с предустановленными ОС и компонентами программного средства, учетных записей, инициализированных носителей, администрируемых под управлением единого сервера управления.

2.2.1 Иерархия контуров обработки информации

Программное средство обеспечивает возможность построения иерархии КОИ с территориально распределенной структурой. Построение иерархии КОИ условно изображено на рисунке 1.

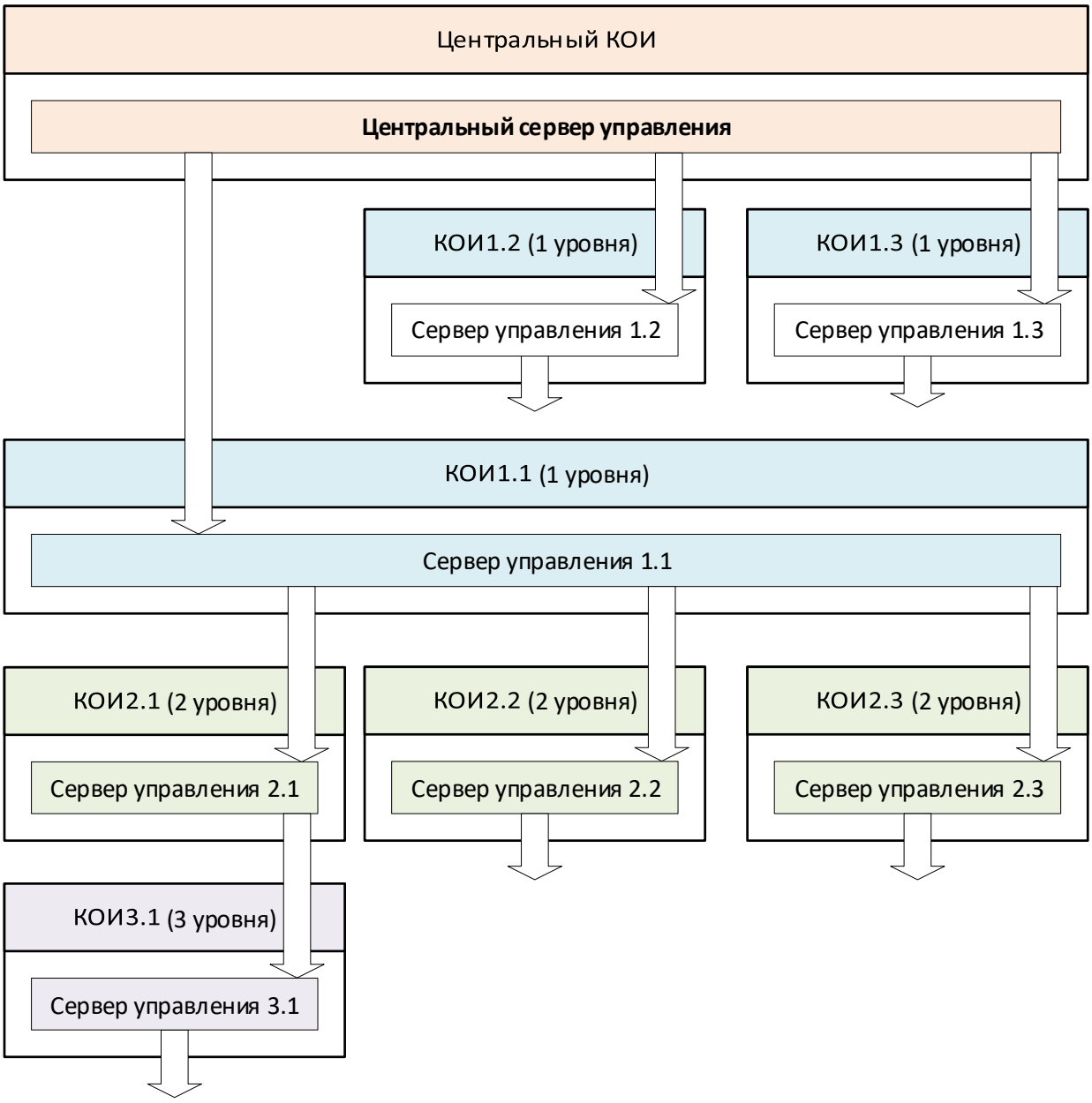


Рисунок 1 – Условное изображение иерархии КОИ

Центральный КОИ стоит во главе иерархии. В рамках иерархической структуры каждый КОИ может иметь несколько нижестоящих КОИ, все КОИ, кроме центрального, обязательно имеют только один вышестоящий КОИ.

Вышестоящие и нижестоящие КОИ построены, соответственно, на основе вышестоящих серверов управления и нижестоящих серверов управления.

Построение иерархии КОИ проводится «сверху вниз», начиная с Центрального КОИ. Количество нижестоящих КОИ определяется при развертывании программного средства SecurFlash и может, при необходимости, наращиваться или сокращаться.

2.2.1 Роли и учетные записи

При эксплуатации программного средства предусмотрены две роли.

Администратор — осуществляет общее проектирование КОИ, устанавливает компоненты программного средства и производит их первоначальное конфигурирование, осуществляет администрирование программного средства, включающее общие настройки администрирования, текущее администрирование используемых носителей и аудит. При первоначальной конфигурации КОИ создается встроенная привилегированная учетная запись (ВПУЗ) привилегированного администратора.

Пользователь — осуществляет эксплуатацию программного средства после получения инициализированного носителя и прав доступа к нему от администратора.

Перед началом эксплуатации программного средства каждый уполномоченный пользователь получает персональную учетную запись в соответствии с предварительно установленной для него ролью.

В таблице 1 приведены используемые роли и учетные записи.

Таблица 1 – Роли и учетные записи

Учетная запись/роль	Компонент программного средства	Данные для авторизации	Кто создает учетную запись и присваивает права на авторизацию
Привилегированный администратор/ администратор	Сервер управления, программа администратора	Контейнер встроенной привилегированной учетной записи/ пароль	Привилегированный администратор создает учетную запись, права на авторизацию присваивает администратор вышестоящего КОИ
Администратор/ администратор	Программа администратора	Контейнер администратора/ пароль	Привилегированный администратор или администратор
Пользователь/ пользователь	Программа пользователя	Логин/ пароль	Администратор

2.2.2 Типы СВТ

СВТ, на которых развернуто программное средство, условно разделяются на типы в рамках КОИ.

Перечень типов СВТ приведен в таблице 2.

Таблица 2 – Типы СВТ и базы данных

Тип СВТ (режим функционирования)	Функциональное назначение	База данных
СВТ центрального сервера управления КОИ (сетевое)	Управление КОИ во взаимодействии с базой данных КОИ	База данных сервера управления КОИ
СВТ сервера управления КОИ (сетевое)	Управление КОИ во взаимодействии с базой данных КОИ	База данных сервера управления КОИ
СВТ сервера управления КОИ, совмещенное с СВТ администратора (сетевое)	Реализация функций сервера управления КОИ и администрирования КОИ на одном сетевом СВТ	База данных сервера управления КОИ
СВТ администратора (сетевое)	Администрирование КОИ	База данных сервера управления КОИ
СВТ сервера управления КОИ, совмещенное с СВТ администратора (автономное)	Реализация функций сервера управления КОИ и администрирования КОИ на одном автономном СВТ	База данных сервера управления КОИ
СВТ пользователя (сетевое)	Работа пользователя с инициализированными носителями	База данных сервера управления КОИ
СВТ пользователя (автономное)	Работа пользователя с инициализированными носителями	База данных сервера управления КОИ, локальная база данных СВТ пользователя

СВТ могут быть настроены в двух режимах функционирования – сетевой или автономный.

Центральный сервер управления стоит во главе иерархии КОИ и имеет самоподписаннный сертификат.

Каждый нижестоящий сервер управления должен получить сертификат у вышестоящего сервера управления (расположенного на один уровень иерархии выше).

Сервер управления КОИ работает с базой данных, в которой содержится текущая информация по администрированию носителей, аудиту и настройкам в рамках КОИ.

Автономное СВТ администратора реализует функции администрирования и сервера управления КОИ на одном СВТ, не подключенном к сети. При таком построении возможна работа только с автономными СВТ пользователей в рамках КОИ.

Автономные СВТ пользователя работают с собственной локальной базой данных, а также с базой данных сервера управления КОИ посредством импорта и экспорта файлов.

Используемые сетевые и автономные СВТ пользователей должны быть зарегистрированы в базе данных сервера управления КОИ.

2.2.3 Структура контура обработки информации

Структура построения КОИ, во взаимодействии с вышестоящим и нижестоящим КОИ, условно показана на рисунке 2.

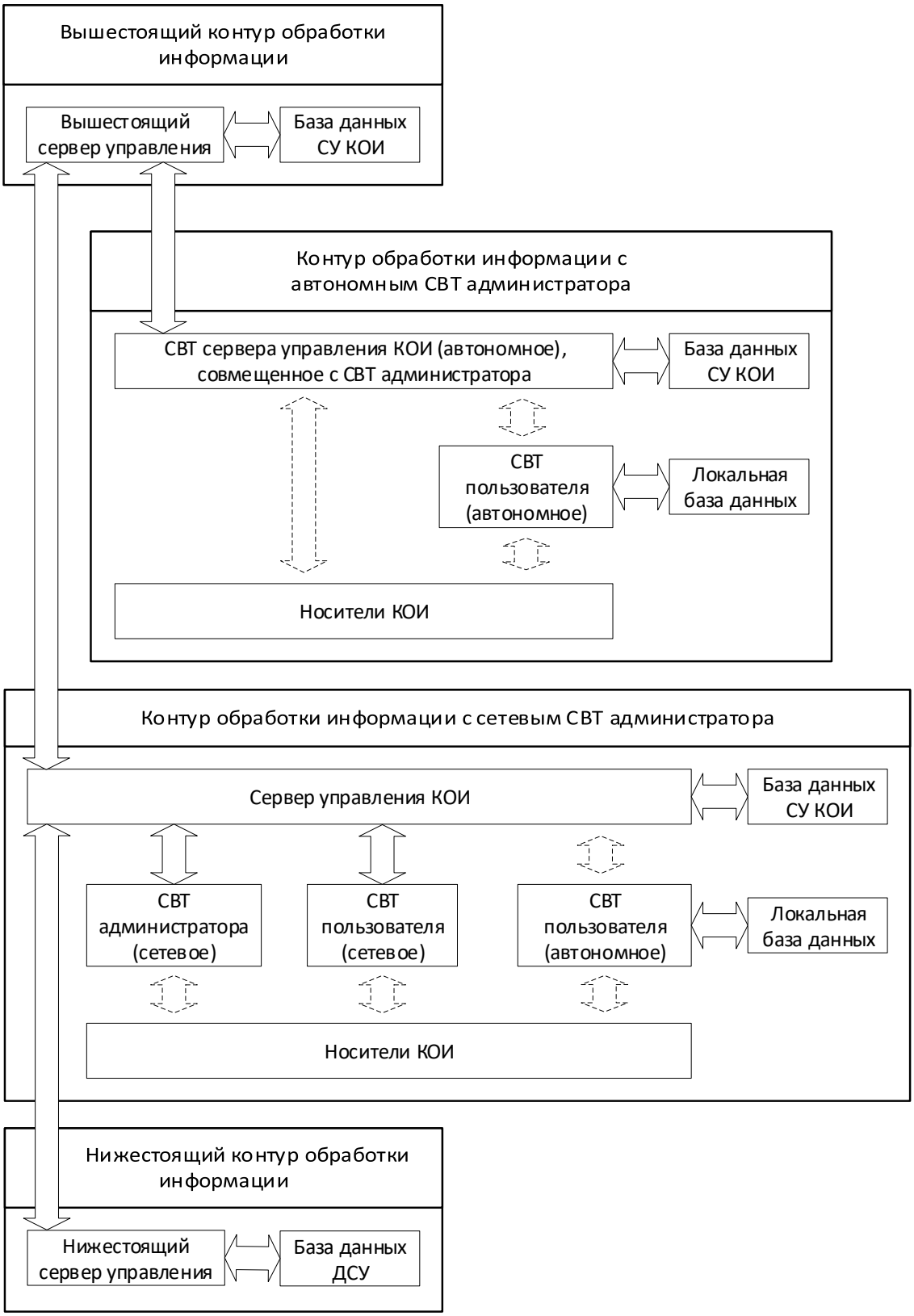


Рисунок 2 – Условное изображение структуры построения КОИ в рамках иерархии

Подробно построение и первоначальное конфигурирование КОИ описаны в разделах 3 и 4.

3 ПОСТРОЕНИЕ КОИ И УСТАНОВКА КОМПОНЕНТОВ ПРОГРАММНОГО СРЕДСТВА

Построение КОИ и установка компонентов программного средства осуществляется в следующей последовательности:

1) определение состава персонала с правами (ролями) администраторов и пользователей в соответствии с 2.2.1, стр. 12. При этом один сотрудник может иметь права доступа с несколькими ролями;

2) изучение персоналом эксплуатационной документации на программное средство в соответствии с установленными ролями:

– администраторы должны быть ознакомлены с настоящим документом, а также с документами RU.АЛДЕ.03.01.046 30 01-1 «Средство защиты информации на съемных машинных носителях SecurFlash. Формуляр. Часть 1. Общие сведения» и RU.АЛДЕ.03.01.046 30 01-2 «Средство защиты информации на съемных машинных носителях SecurFlash. Формуляр. Часть 2. Свидетельства о приемке, упаковке и маркировке»;

– пользователи должны быть ознакомлены с документом «Средство защиты информации на съемных машинных носителях SecurFlash. Руководство оператора» RU.АЛДЕ.03.01.046 34 01 (далее – руководство оператора);

3) определение перечня СВТ для работы персонала с соответствующими ролями в рамках КОИ, согласно 3.1;

4) определение компонентов программного средства для установки на каждое СВТ, согласно 3.2;

5) установка компонентов программного средства на СВТ, согласно 3.3.

3.1 Определение перечня СВТ контура обработки информации

Построение КОИ начинается с определения перечня СВТ, которые планируется использовать в составе КОИ и определения их типов в соответствии с 2.2.2 (стр. 12).

СВТ КОИ выбираются с учетом следующих требований и допущений:

– на каждое СВТ должна быть предустановлена операционная система из перечня поддерживаемых операционных систем, приведенного в 1.2, (стр. 8);

– сетевые СВТ должны быть подключены к единой сети;

– КОИ управляется одним сервером управления;

– при необходимости, одно СВТ может совмещать функционал сервера управления КОИ, администратора и пользователя;

– физический доступ персонала к СВТ КОИ должен быть регламентирован с учетом степени конфиденциальности обрабатываемой информации.

3.2 Определение компонентов программного средства для установки

3.2.1 Установочные пакеты программного средства

Программное средство содержит следующие установочные пакеты:

1) установочный пакет сервера управления;
2) установочный пакет программы администратора;
3) установочный пакет программы пользователя.

Полное наименование установочного пакета содержит наименование, тип ОС и тип платформы, например: sf_admin_al1.7_x64.deb.

Перечень установочных пакетов компонентов программного средства для поддерживаемых ОС средства приведен в таблице 3.

Сервер управления должен быть установлен в первую очередь.

Таблица 3 – Установочные пакеты компонентов программного средства

Установочный пакет компонентов программного средства	Наименование пакета	Примечание
Astra Linux 1.6 SE «Смоленск» (x64)		
Установочный пакет сервера управления	sf_acc_server_al1.6_amd64.deb	
Установочный пакет программы администратора	sf_admin_al1.6_amd64.deb	
Установочный пакет программы пользователя (необязательно)	sf_user_al1.6_amd64.deb	
Операционная система Astra Linux 1.7 SE «Смоленск» (x64)		
Установочный пакет сервера управления	sf_acc_server_al1.7_amd64.deb	
Установочный пакет программы администратора	sf_admin_al1.7_amd64.deb	
Установочный пакет программы пользователя (необязательно)	sf_user_al1.7_amd64.deb	
Альт 8 СП		

Установочный пакет компонентов программного средства	Наименование пакета	Примечание
Установочный пакет сервера управления	sf_acc_server-alt8.0.x86_64.rpm	Для Альт 8 СП версий до 8,4
	sf_acc_server-alt8.4.x86_64.rpm	Для Альт 8 СП версии 8,4 и старше
Установочный пакет программы администратора	sf_admin-alt8.0.x86_64.rpm	Для Альт 8 СП версий до 8,4
	sf_admin-alt8.4.x86_64.rpm	Для Альт 8 СП версии 8,4 и старше
Установочный пакет программы пользователя (необязательно)	sf_user-alt8.0.x86_64.rpm	Для Альт 8 СП версий до 8,4
	sf_user-alt8.4.x86_64.rpm	Для Альт 8 СП версии 8,4 и старше
Операционная система Microsoft Windows 7,10 (x86)		
Установочный пакет сервера управления	SFAccServer_win-x86_ru-Ru.msi	
Установочный пакет программы администратора	SFAdmin_win-x86_ru-Ru.msi	
Установочный пакет программы пользователя (необязательно)	SFUser_win-x86_ru-Ru.msi	
Операционная система Microsoft Windows 7, 10 (x64)		
Установочный пакет сервера управления	SFAccServer_win-x64_ru-Ru.msi	
Установочный пакет программы администратора	SFAdmin_win-x64_ru-Ru.msi	
Установочный пакет программы пользователя (необязательно)	SFUser_win-x64_ru-Ru.msi	

Перечень пакетов, которые необходимо установить на СВТ различных типов, приведен в таблице 4.

Таблица 4 – Установочные пакеты для различных типов СВТ

Тип СВТ	Установочный пакет	Примечание
СВТ центрального сервера управления КОИ (сетевое),	1. Установочный пакет сервера управления	Требуется инициализация сервера управления после установки

Тип СВТ	Установочный пакет	Примечание
СВТ сервера управления КОИ (сетевое), СВТ сервера управления КОИ, совмещенное с СВТ администратора (сетевое), СВТ сервера управления КОИ, совмещенное с СВТ администратора (автономное)	2. Установочный пакет программы администратора	
	3. Установочный пакет программы пользователя (необязательно)	
СВТ администратора (сетевое)	1. Установочный пакет сервера управления	Не требуется инициализация сервера управления после установки
	2. Установочный пакет программы администратора	
	3. Установочный пакет программы пользователя (необязательно)	
СВТ пользователя (сетевое)	1. Установочный пакет сервера управления	Не требуется инициализация сервера управления после установки
	2. Установочный пакет программы пользователя	
СВТ пользователя (автономное)	1. Установочный пакет сервера управления	Не требуется инициализация сервера управления после установки
	2. Установочный пакет программы пользователя	

3.3 Установка и запуск компонентов программного средства (для ОС семейства Linux)

Последовательность установки пакетов на СВТ должна соответствовать перечням графы «Установочные пакеты» в таблице 4, раздела 3.2.

3.3.1 Установка компонентов программного средства для ОС AstraLinux

3.3.1.1 Установка и запуск сервера управления для ОС AstraLinux

Для установки сервера управления необходимо выполнить следующие действия:

1) скопировать установочный пакет сервера управления для необходимой операционной системы семейства Linux (в соответствии с таблицей 3) в домашний каталог пользователя;

2) перейти в каталог, в который скопирован пакет, выполнив команду:

```
cd /[путь до каталога]
```

3) выполнить команду для устанавливаемого пакета:

– для ОС Astra Linux 1.6:

```
sudo apt install ./sf_acc_server_al1.6_amd64.deb
```

– для ОС Astra Linux 1.7:

```
sudo apt install ./sf_acc_server__al1.7_amd64.deb
```

Исполняемый файл программы будет установлен в каталог:

```
/usr/local/bin
```

Файл настроек sets.ini будет создан в каталоге:

```
 /opt/Aladdin/SF
```

После установки запуск сервера управления выполняется автоматически.

3.3.1.2 Установка программы администратора для ОС AstraLinux

Перед установкой программы администратора должен быть установлен пакет сервера управления.

Для установки программы администратора необходимо выполнить следующие действия:

1) скопировать установочный пакет программы администратора для необходимой операционной системы семейства Linux (в соответствии с таблицей 3) в домашний каталог пользователя;

2) перейти в каталог, в который скопирован пакет, выполнив команду:

```
cd /[путь до каталога]
```

3) выполнить команду для устанавливаемого пакета:

– для ОС Astra Linux 1.6:

```
sudo apt install ./sf_admin_al1.6_amd64.deb
```

– для ОС Astra Linux 1.7:

```
sudo apt install ./sf_admin_al1.7_amd64.deb
```

Исполняемый файл программы будет установлен в каталог:

```
/usr/local/bin
```

3.3.1.3 Установка программы пользователя для ОС AstraLinux

Перед установкой программы пользователя должен быть установлен пакет сервера управления.

Для установки программы пользователя необходимо выполнить следующие действия:

1) скопировать установочный пакет программы пользователя для необходимой операционной системы семейства Linux (в соответствии с таблицей 3) в домашний каталог пользователя;

2) перейти в каталог, в который скопирован пакет, выполнив команду:

```
cd /[путь до каталога]
```

3) выполнить команду для устанавливаемого пакета:

– для ОС Astra Linux 1.6:

```
sudo apt install ./sf_user_al1.6_amd64.deb
```

– для ОС Astra Linux 1.7:

```
sudo apt install ./sf_user_al1.7_amd64.deb
```

Исполняемый файл программы будет установлен в каталог:

```
/usr/local/bin
```

3.3.2 Установка компонентов программного средства для ОС Альт 8 СП

3.3.2.1 Установка и запуск сервера управления для ОС Альт 8 СП

Для установки сервера управления необходимо выполнить следующие действия:

1) скопировать установочный пакет сервера управления для необходимой операционной системы семейства Linux (в соответствии с таблицей 3) в домашний каталог пользователя;

2) перейти в каталог, в который скопирован пакет, выполнив команду:

```
cd /[путь до каталога]
```

3) выполнить команду для устанавливаемого пакета:

– для Альт 8 СП версий до 8,4:

```
sudo apt-get install ./sf_acc_server-alt8.0.x86_64.rpm
```

– для Альт 8 СП версии 8,4 и старше:

```
sudo apt-get install ./sf_acc_server-alt8.4.x86_64.rpm
```

Исполняемый файл программы будет установлен в каталог:

```
/usr/local/bin
```

Файл настроек sets.ini будет создан в каталоге:

```
/opt/Aladdin/SF
```

После установки запуск сервера управления выполняется автоматически.

3.3.2.2 Установка программы администратора для ОС Альт 8 СП

Перед установкой программы администратора должен быть установлен пакет сервера управления.

Для установки программы администратора необходимо выполнить следующие действия:

1) скопировать установочный пакет программы администратора для необходимой операционной системы семейства Linux (в соответствии с таблицей 3) в домашний каталог пользователя;

2) перейти в каталог, в который скопирован пакет, выполнив команду:

```
cd /[путь до каталога]
```

3) выполнить команду для устанавливаемого пакета:

– для Альт 8 СП версий до 8,4:

```
sudo apt-get install ./sf_admin-alt8.0.x86_64.rpm
```

– для Альт 8 СП версии 8,4 и старше:

```
sudo apt-get install ./sf_admin-alt8.4.x86_64.rpm
```

Исполняемый файл программы будет установлен в каталог:

```
/usr/local/bin
```

3.3.2.3 Установка программы пользователя для ОС Альт 8 СП

Перед установкой программы пользователя должен быть установлен пакет сервера управления.

Для установки программы пользователя необходимо выполнить следующие действия:

1) скопировать установочный пакет программы пользователя для необходимой операционной системы семейства Linux (в соответствии с таблицей 3) в домашний каталог пользователя;

2) перейти в каталог, в который скопирован пакет, выполнив команду:

```
cd /[путь до каталога]
```

3) выполнить команду для устанавливаемого пакета:

– для Альт 8 СП версий до 8,4:

```
sudo apt-get install ./sf_user-alt8.0.x86_64.rpm
```

– для Альт 8 СП версии 8,4 и старше:

```
sudo apt-get install ./sf_user-alt8.4.x86_64.rpm
```

Исполняемый файл программы будет установлен в каталог:

```
/usr/local/bin
```

3.3.3 Запуск компонентов программного средства (для ОС семейства Linux)

3.3.3.1 Запуск программы администратора (для ОС Astra Linux)

Для запуска программы администратора перейти в меню «Пуск», раздел «Утилиты» выбрать пункт «SecurFlash. Программа администратора».

3.3.3.2 Запуск программы пользователя (для ОС AstraLinux)

Для запуска программы пользователя перейти в меню «Пуск», раздел «Утилиты», выбрать пункт – «SecurFlash. Программа пользователя».

3.3.3.3 Запуск программы пользователя с правами настройки (для ОС AstraLinux)

Для запуска программы пользователя с правами настройки необходимо выполнить следующие действия:

– перейти в меню «Пуск», раздел «Утилиты», выбрать пункт – «SecurFlash. Программа пользователя (администратор)»;

– при необходимости, ввести пароль суперпользователя и подтверждение пароля суперпользователя.

3.3.3.4 Запуск программы администратора (для ОС Альт 8 СП)

Для запуска программы администратора перейти в меню «Пуск» – «Приложения» – «Инструменты», выбрать пункт – «SecurFlash. Программа администратора».

3.3.3.5 Запуск программы пользователя (для ОС Альт 8 СП)

Для запуска программы пользователя перейти в меню «Пуск» – «Приложения» – «Инструменты», выбрать пункт – «SecurFlash. Программа пользователя».

3.3.3.6 Запуск программы пользователя с правами настройки (для ОС Альт 8 СП)

Для запуска программы пользователя с правами настройки необходимо выполнить следующие действия:

– перейти в меню «Пуск» – «Приложения» – «Инструменты», выбрать пункт – «SecurFlash. Программа пользователя (администратор)»;

– при необходимости, ввести пароль суперпользователя и подтверждение пароля суперпользователя.

3.4 Установка и запуск компонентов программного средства (для ОС семейства Windows)

3.4.1 Установка компонентов программного средства (для ОС семейства Windows)

3.4.1.1 Установка и запуск сервера управления

Для установки сервера управления выполнить следующие действия:

1) запустить пакет установки сервера управления в соответствии с таблицей 3 (для соответствующей разрядности ОС Windows):

– для ОС Windows (x86): `SFAccServer_win-x86_ru-Ru.msi`

– для ОС Windows (x64): `SFAccServer_win-x64_ru-Ru.msi`

2) откроется окно установщика (рисунок 3), нажать кнопку «Далее»;

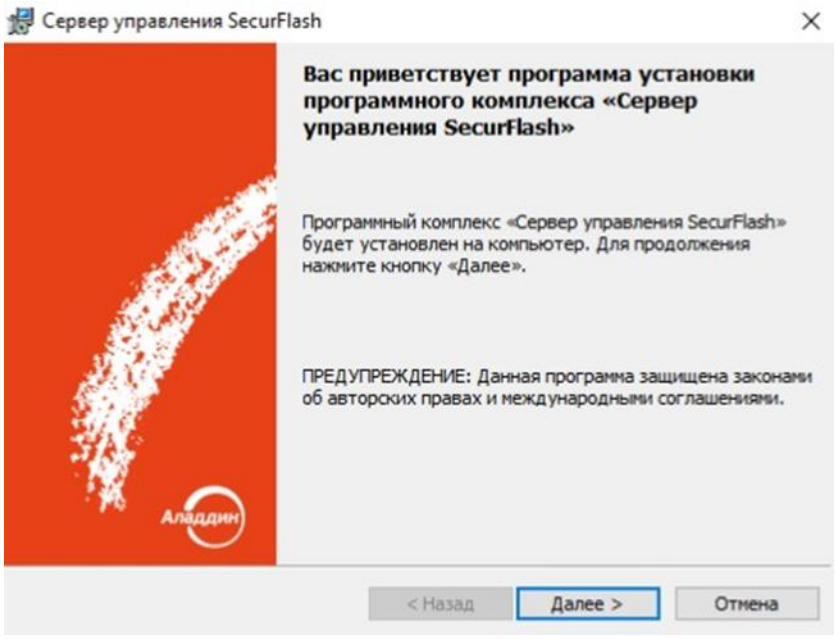


Рисунок 3

3) принять условия в открывшемся окне лицензионного соглашения (рисунок 4) и нажать кнопку «Далее»;

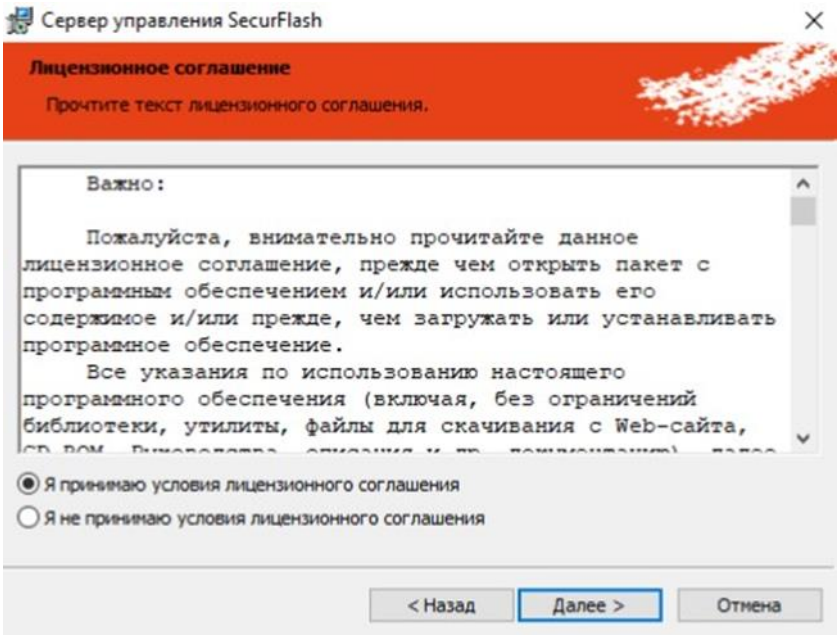


Рисунок 4

4) в открывшемся окне (рисунок 5) выбрать папку для установки или оставить значение по умолчанию, нажать кнопку «Далее»;

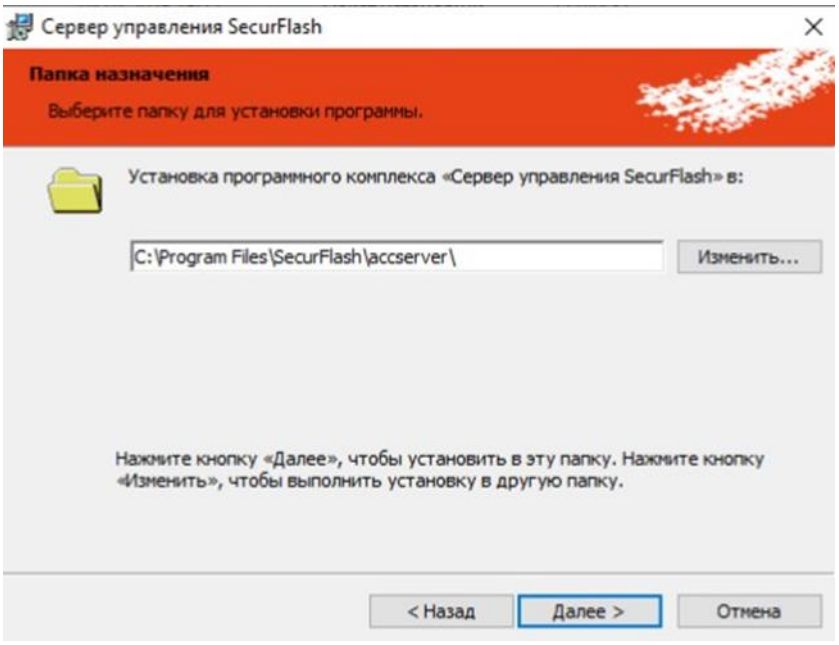


Рисунок 5

5) в открывшемся окне подтверждения установки (рисунок 6) нажать кнопку «Установить»;

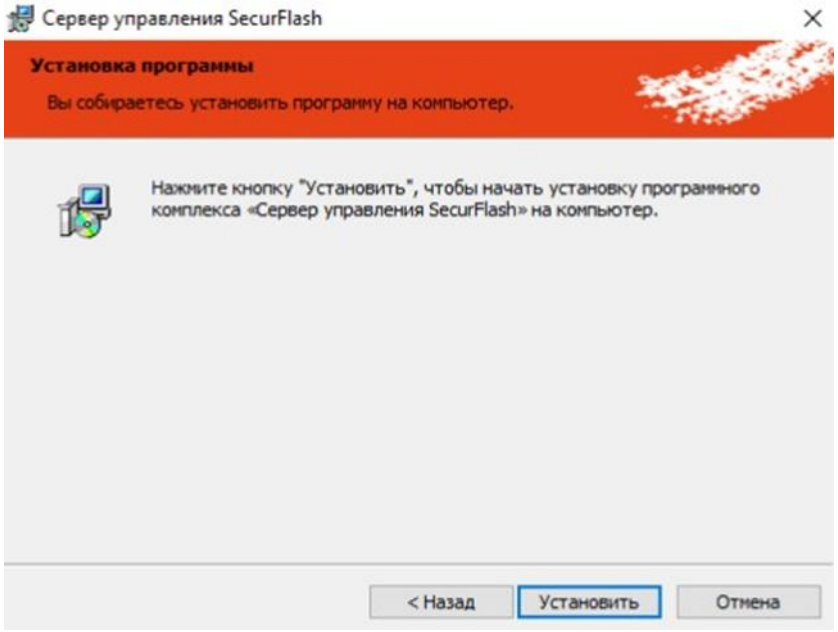


Рисунок 6

6) в открывшемся окне контроля учетных записей (рисунок 7) ввести логин и пароль администратора и нажать кнопку «Да»;

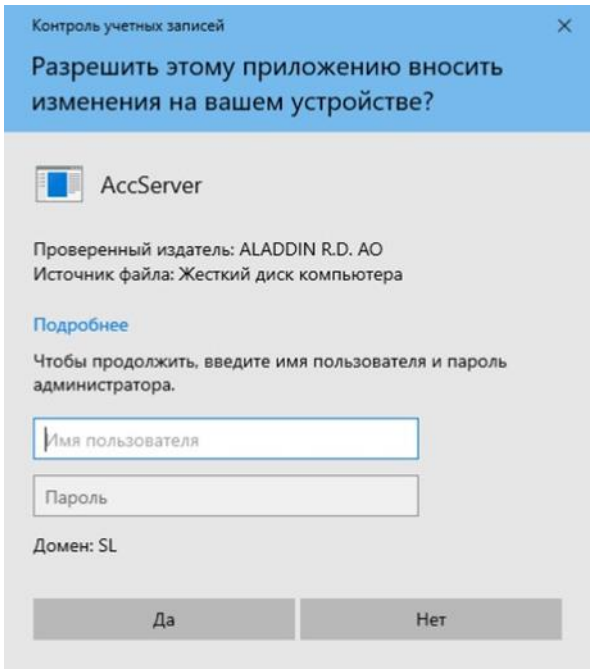


Рисунок 7

7) в открывшемся окне завершения установки (рисунок 8) нажать кнопку «Готово»;

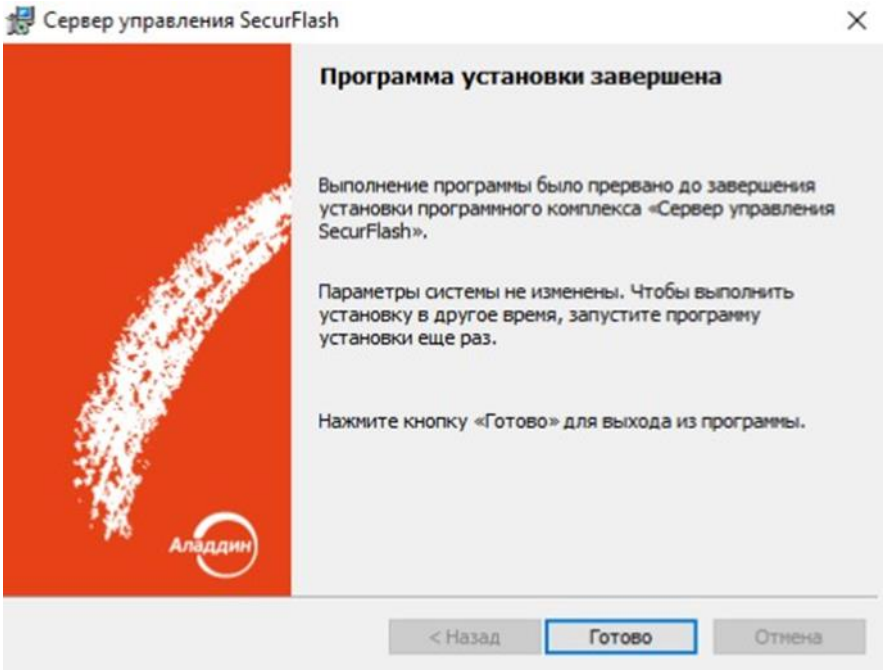


Рисунок 8

8) после завершения установки выполнить перезагрузку операционной системы.

После установки запуск сервера управления выполняется автоматически.

3.4.1.2 Установка программы администратора

Перед установкой пакета программы администратора должен быть установлен пакет сервера управления.

Для установки пакета программы администратора необходимо выполнить следующие действия:

1) запустить пакет установки программы администратора в соответствии с таблицей 3 (для соответствующей разрядности ОС Windows):

– для ОС Windows (x86): `SFAdmin_win-x86_ru-Ru.msi`

– для ОС Windows (x64): `SFAdmin_win-x64_ru-Ru.msi`

2) откроется окно установщика (рисунок 9), нажать кнопку «Далее»;

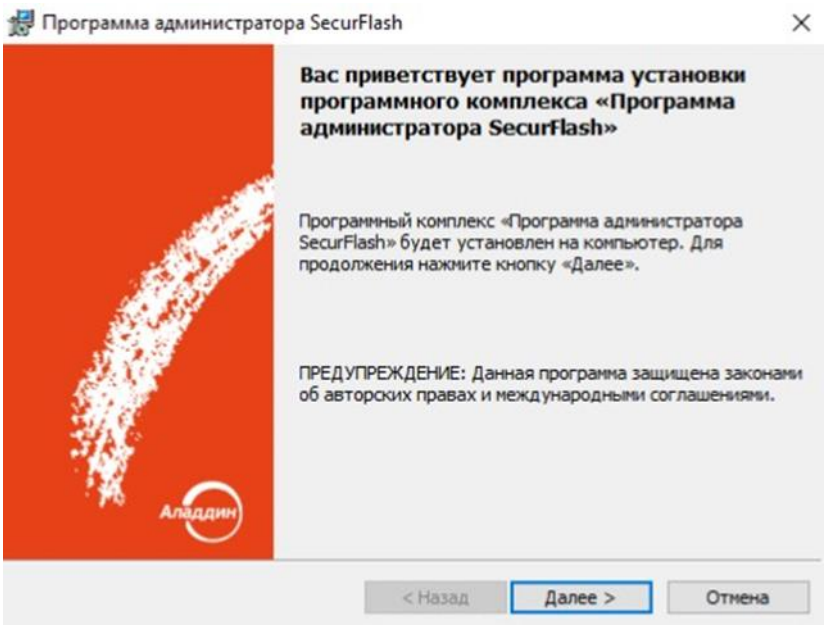


Рисунок 9

3) принять условия в открывшемся окне лицензионного соглашения (рисунок 10) и нажать кнопку «Далее»;

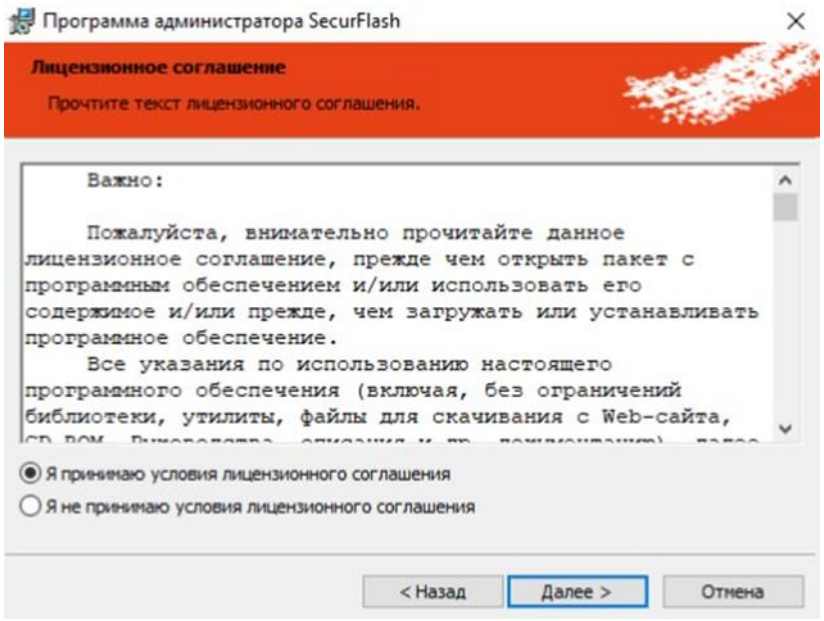


Рисунок 10

4) в открывшемся окне (рисунок 11) выбрать папку для установки или оставить значение по умолчанию;

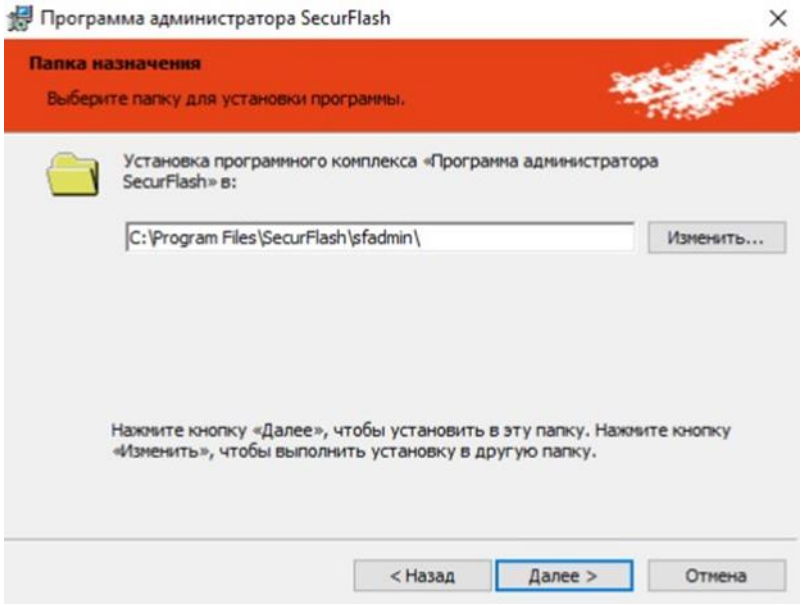


Рисунок 11

5) в открывшемся окне подтверждения установки (рисунок 12) нажать кнопку «Установить»;

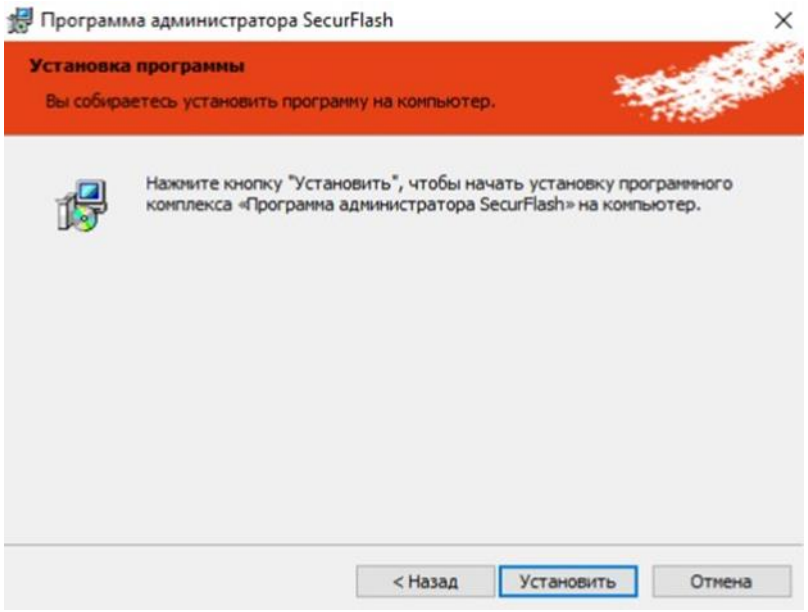


Рисунок 12

6) в открывшемся окне контроля учетных записей (рисунок 13) ввести логин и пароль администратора и нажать кнопку «Да»;

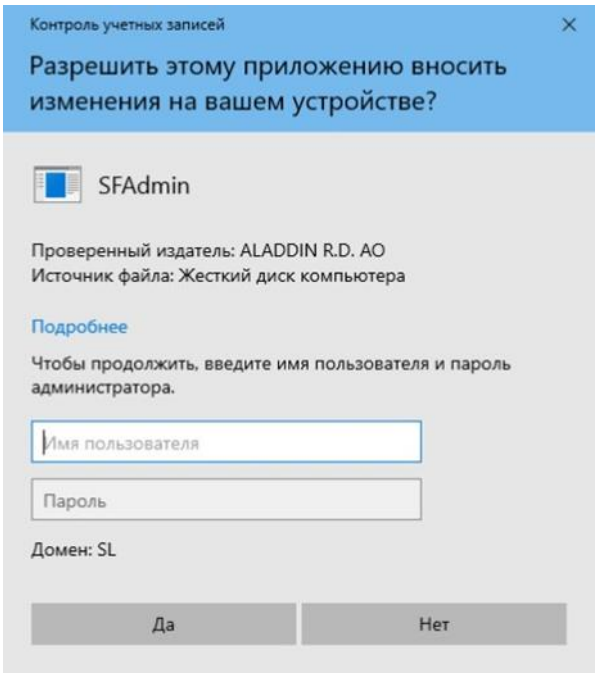


Рисунок 13

7) в открывшемся окне завершения установки (рисунок 14) нажать кнопку «Готово».

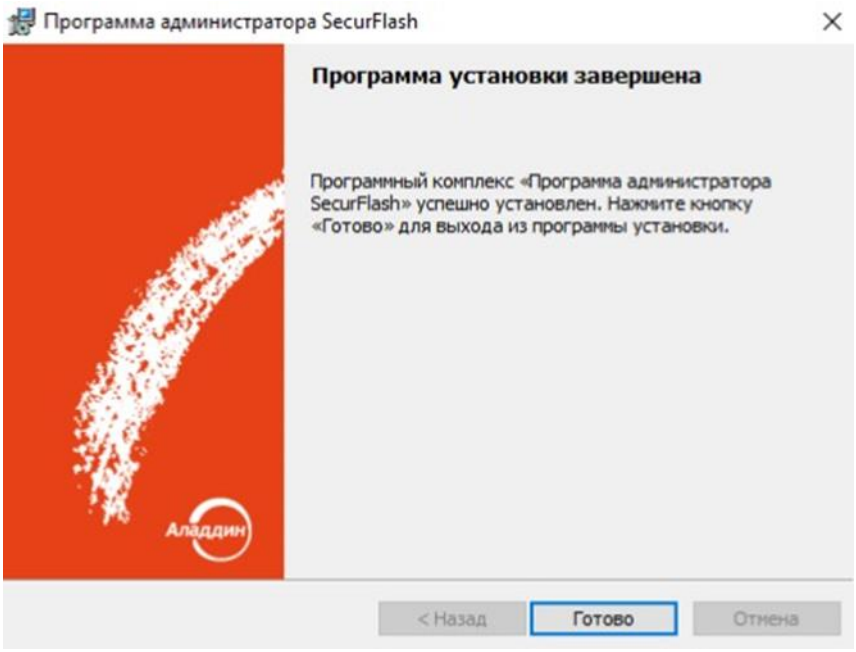


Рисунок 14

3.4.1.3 Установка программы пользователя

Перед установкой пакета программы пользователя должен быть установлен пакет сервера управления.

Для установки пакета программы пользователя необходимо выполнить следующие действия:

1) запустить пакет установки программы пользователя в соответствии с таблицей 3 (для соответствующей разрядности ОС Windows):

- для ОС Windows (x86): `SFUser_win-x86_ru-Ru.msi`
- для ОС Windows (x64): `SFUser_win-x64_ru-Ru.msi`

2) откроется окно установщика (рисунок 15), нажать кнопку «Далее»;

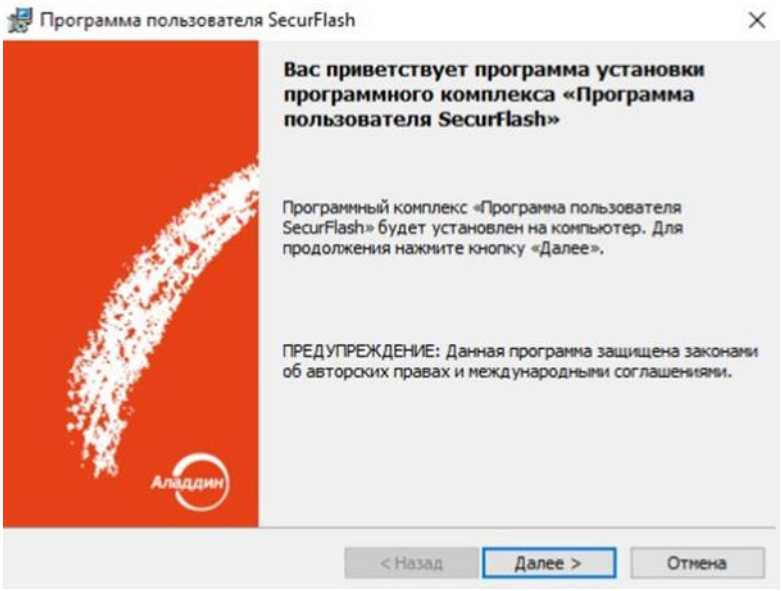


Рисунок 15

3) принять условия в открывшемся окне лицензионного соглашения (рисунок 16) и нажать кнопку «Далее»;

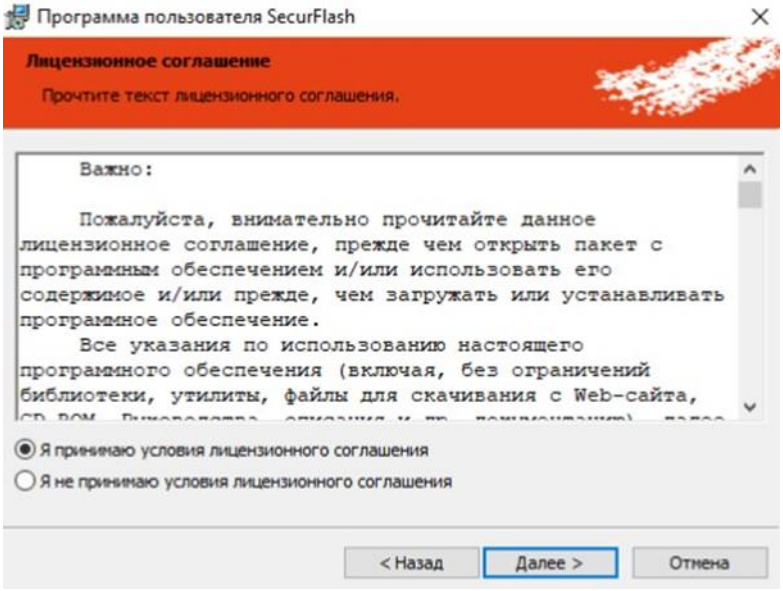


Рисунок 16

4) в открывшемся окне (рисунок 17) выбрать папку для установки или оставить значение по умолчанию;

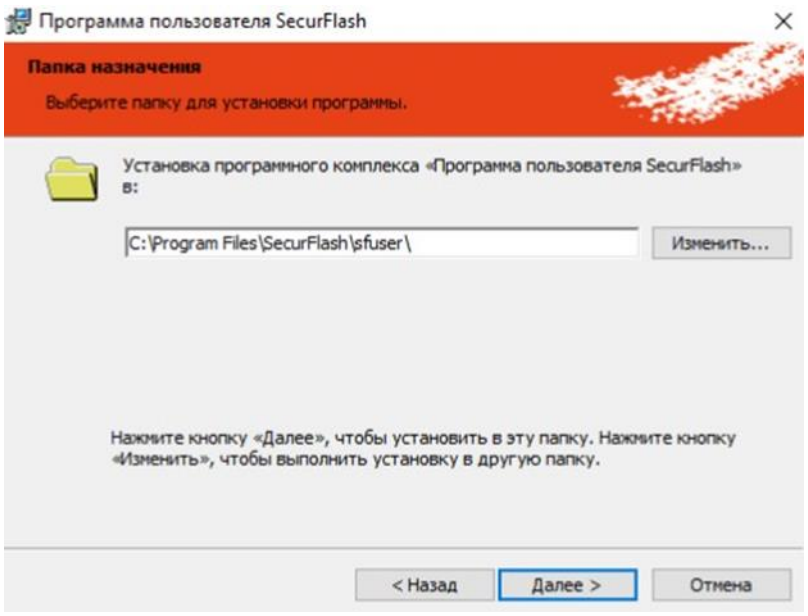


Рисунок 17

5) в открывшемся окне подтверждения установки (рисунок 18) нажать кнопку «Установить»;

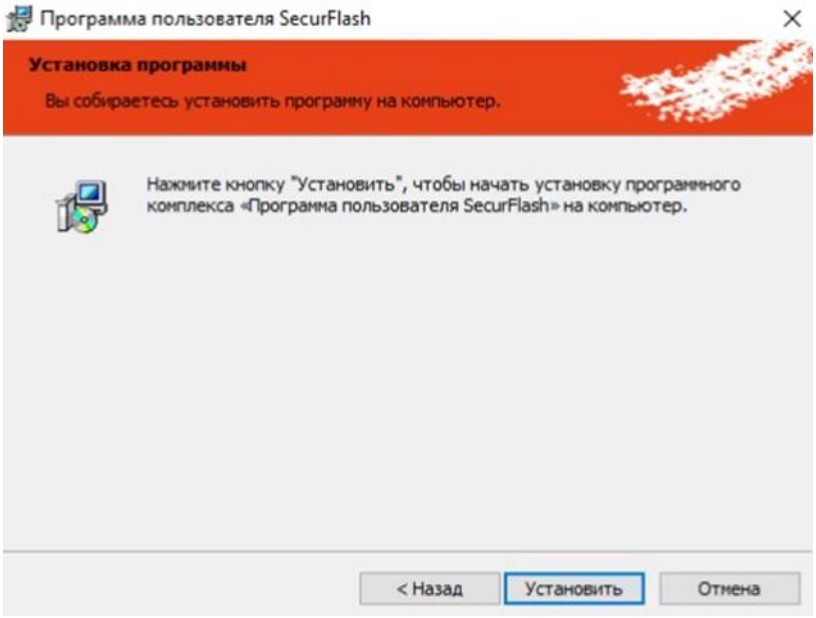


Рисунок 18

6) в открывшемся окне контроля учетных записей (рисунок 19) ввести логин и пароль администратора и нажать кнопку «Да»;

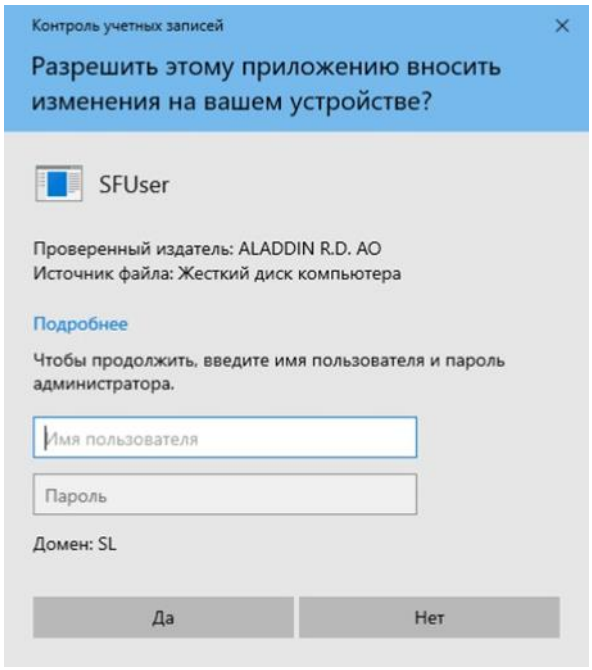


Рисунок 19

7) в открывшемся окне завершения установки (рисунок 20) нажать кнопку «Готово».

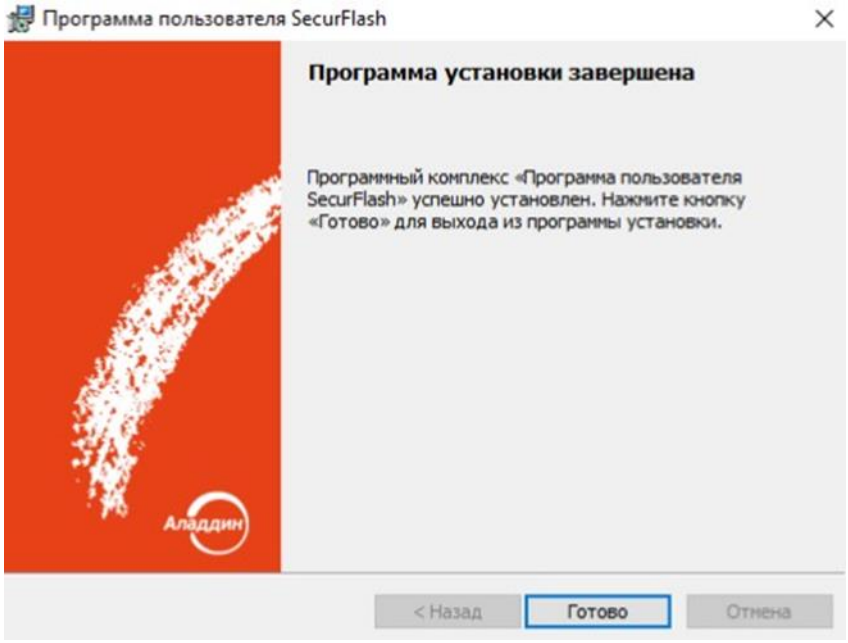


Рисунок 20

3.4.2 Запуск компонентов программного средства (для ОС семейства Windows)

3.4.2.1 Запуск программы администратора

Для запуска программы администратора перейти в меню «Пуск» – выбрать пункт «Программа администратора SecurFlash».

3.4.2.2 Запуск программы пользователя

Для запуска программы пользователя перейти в меню «Пуск», выбрать пункт – «Программа пользователя SecurFlash».

3.4.2.3 Запуск программы пользователя с правами настройки

Для запуска программы пользователя с правами настройки необходимо выполнить следующие действия:

– перейти в меню «Пуск», выбрать пункт – «Программа пользователя SecurFlash (администратор)»;

– в открывшемся окне контроля учетных записей (рисунок 21) ввести логин и пароль администратора, нажать кнопку «Да».

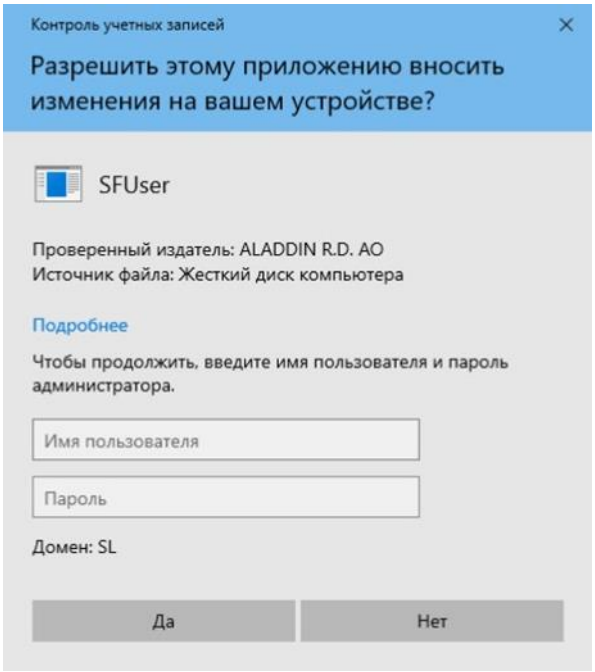


Рисунок 21

3.5 Завершение работы и удаление компонентов программного средства

3.5.1 Завершение работы компонентов программного средства (для ОС семейства Linux)

Для завершения работы программы пользователя и программы администратора необходимо нажать кнопку закрытия (крестик) в правом верхнем углу окна программы.

Для завершения работы сервера управления необходимо выполнить команду:

```
sudo systemctl stop sfaccserver
```

Примечание – Для повторного запуска сервера управления необходимо выполнить команду: sudo systemctl start sfaccserver.servise

3.5.2 Удаление компонентов программного средства (для ОС семейства Linux)

3.5.2.1 Удаление сервера управления

Для удаления сервера управления выполнить команду:

```
sudo apt-get remove sfaccserver
```

3.5.2.2 Удаление программы администратора

Для удаления программы администратора выполнить команду:

```
sudo apt-get remove sfadmin
```

3.5.2.3 Удаление программы пользователя

Для удаления программы пользователя выполнить команду:

```
sudo apt-get remove sfuser
```

3.5.3 Завершение работы программных компонентов (для ОС семейства Windows)

Для завершения работы программы пользователя и программы администратора необходимо нажать кнопку закрытия (крестик) в правом верхнем углу окна программы.

Для завершения работы сервера управления необходимо выполнить следующие действия:

– нажать CTRL+ALT+DEL, в меню выбрать пункт «Диспетчер задач» – вкладку «Службы»;

– выбрать службу `SecurFlash Access Server`, нажать правую кнопку мыши и в выпадающем контекстном меню выбрать пункт «Остановить»;

– выбрать службу `SecurFlash DB Server`, нажать правую кнопку мыши и в выпадающем контекстном меню выбрать пункт «Остановить».

Примечание – Для возобновления работы сервера управления, необходимо во вкладке «Службы» диспетчера задач выбрать пункт меню «Запустить» для служб SecurFlash Access Server и SecurFlash DB Server.

3.5.4 Удаление компонентов программного средства (для ОС семейства Windows)

3.5.4.1 Удаление сервера управления

Для удаления сервера управления перейти в меню «Пуск» – «Параметры» – «Приложения» - «Приложения и возможности» – «Сервер Управления SecurFlash», выбрать пункт «Удалить».

3.5.4.2 Удаление программы администратора

Для удаления программы администратора перейти в меню «Пуск» – «Параметры» – «Приложения» - «Приложения и возможности» – «Программа администратора SecurFlash», выбрать пункт «Удалить».

3.5.4.3 Удаление программы пользователя

Для удаления программы пользователя перейти в меню «Пуск» – «Параметры» – «Приложения» - «Приложения и возможности» – «Программа пользователя SecurFlash», выбрать пункт «Удалить».

4 ПЕРВОНАЧАЛЬНОЕ КОНФИГУРИРОВАНИЕ ПРОГРАММНОГО СРЕДСТВА

Последовательность первоначальной настройки после установки программных компонентов программного средства на СВТ:

1) первоначальная настройка сервера управления (4.1, стр. 38):

– инициализация сервера управления и создание встроенной привилегированной учетной записи (ВПУЗ);

– настройка одного из двух режимов функционирования сервера управления – сетевой или автономный;

2) первоначальная настройка СВТ администратора (4.2, стр. 40):

– настройка режима функционирования СВТ администратора – сетевой или автономный;

– авторизация в программе администратора с использованием контейнера ВПУЗ, создание учетной записи администратора;

– авторизация администратора;

– создание списка разрешенных IP адресов сетевых СВТ администраторов и сетевых СВТ пользователей;

– регистрация на вышестоящем сервере управления;

– регистрация нижестоящих серверов управления;

– создание политики безопасности;

– создание учетных записей пользователей;

3) первоначальная настройка СВТ пользователей (4.3, стр.52):

– настройка режима функционирования СВТ пользователей – сетевой или автономный;

– регистрация СВТ пользователей.

4.1 Первоначальная настройка сервера управления

4.1.1 Инициализация сервера управления КОИ и создание встроенной привилегированной учетной записи

Первоначальная настройка сервера управления производится в следующей последовательности:

1) для проведения первоначальной инициализации сервера выполнить команду:

```
sudo sfaccserver -i
```

2) на завершающем этапе инициализации будет запрошен путь сохранения контейнера встроенной привилегированной учетной записи:

```
Init container path (/root/data/):
```

3) ввести путь сохранения контейнера ВПУЗ;

4) далее будет запрошен пароль контейнера ВПУЗ:

```
Set container password:
```

5) ввести пароль ВПУЗ, соответствующий установленным политикам сложности;

6) после ввода пароля ВПУЗ, откроется запрос на повторный ввод пароля:

```
Confirm password:
```

7) и запрос на подтверждение запуска сервера управления:

```
Start service [Y/n]:
```

8) после завершения инициализации сервера управления контейнер ВПУЗ будет сохранен в установленной папке.

4.1.2 Настройка режима функционирования сервера управления

Предусмотрено два режима функционирования сервера управления – автономный и сетевой.

В автономном режиме администрирование КОИ и реализация функций сервера управления осуществляется на одном автономном СВТ, при этом, в рамках КОИ, возможна работа только с автономными СВТ пользователей.

В сетевом режиме возможно подключение к сети сервера управления сетевых СВТ администраторов и сетевых СВТ пользователей.

По умолчанию сервер управления настроен на автономный режим функционирования.

Для настройки сетевого режима функционирования сервера управления КОИ выполнить следующие действия:

1) запустить в текстовом редакторе файл `sets.ini`, расположенный в папке:

```
/opt/Aladdin/SF/sets.ini
```

2) в разделе:

```
[CertResponder]
Addr=127.0.0.1
```

и поле:

```
[DBServer]
Addr=127.0.0.1
```

заменить значение параметра «Addr» на значение IP адреса СВТ сервера управления, например:

```
Addr=192.168.91.101
```

3) сохранить изменения и перезапустить сервер управления командой:

```
sudo systemctl restart sfaccserver.service
```

4.2 Первоначальная настройка СВТ администратора

4.2.1 Настройка режима функционирования СВТ администратора

Всего предусмотрено два режима функционирования СВТ администратора: автономный и сетевой.

В автономном режиме администрирование КОИ и реализация функций сервера управления КОИ осуществляются на одном автономном СВТ администратора. При таком варианте настройки КОИ отсутствует возможность регистрации сетевых СВТ пользователей.

При сетевом режиме работы функции сервера управления КОИ и администрирования КОИ могут быть разнесены на разные СВТ или совмещаться на одном СВТ. Также возможно регистрирование в КОИ сетевых СВТ пользователей.

По умолчанию все СВТ администраторов настроены на автономный режим функционирования.

Для настройки сетевого режима функционирования СВТ администратора выполнить следующие действия:

1) запустить в текстовом редакторе файл sets.ini, расположенный в папке:

```
/opt/Aladdin/SF/sets.ini
```

2) в разделе:

```
[CertResponder]
Addr=127.0.0.1
```

и поле:

```
[DBServer]
```

```
Addr=127.0.0.1
```

заменить значение параметра «Addr» на значение внешнего IP адреса СВТ сервера управления, к которому необходимо подключиться администратору, например: `Addr=192.168.91.101`

3) сохранить изменения и перезапустить службу командой:

```
sudo systemctl restart sfaccserver.service
```

4.2.2 Создание учетной записи администратора

После авторизации администратора с использованием ВПУЗ программа администратора функционирует с ограничениями – доступно только создание учетной записи администратора.

Создание учетной записи администратора производится в следующей последовательности:

1) запустить программу администратора;

2) в открывшемся окне авторизации администратора нажать кнопку  и выбрать файл контейнера постоянной ВПУЗ (создание контейнера ВПУЗ описано в 4.1.1, стр. 38);

3) откроется окно программы администратора с ограничениями по функциональным возможностям (рисунок 22)

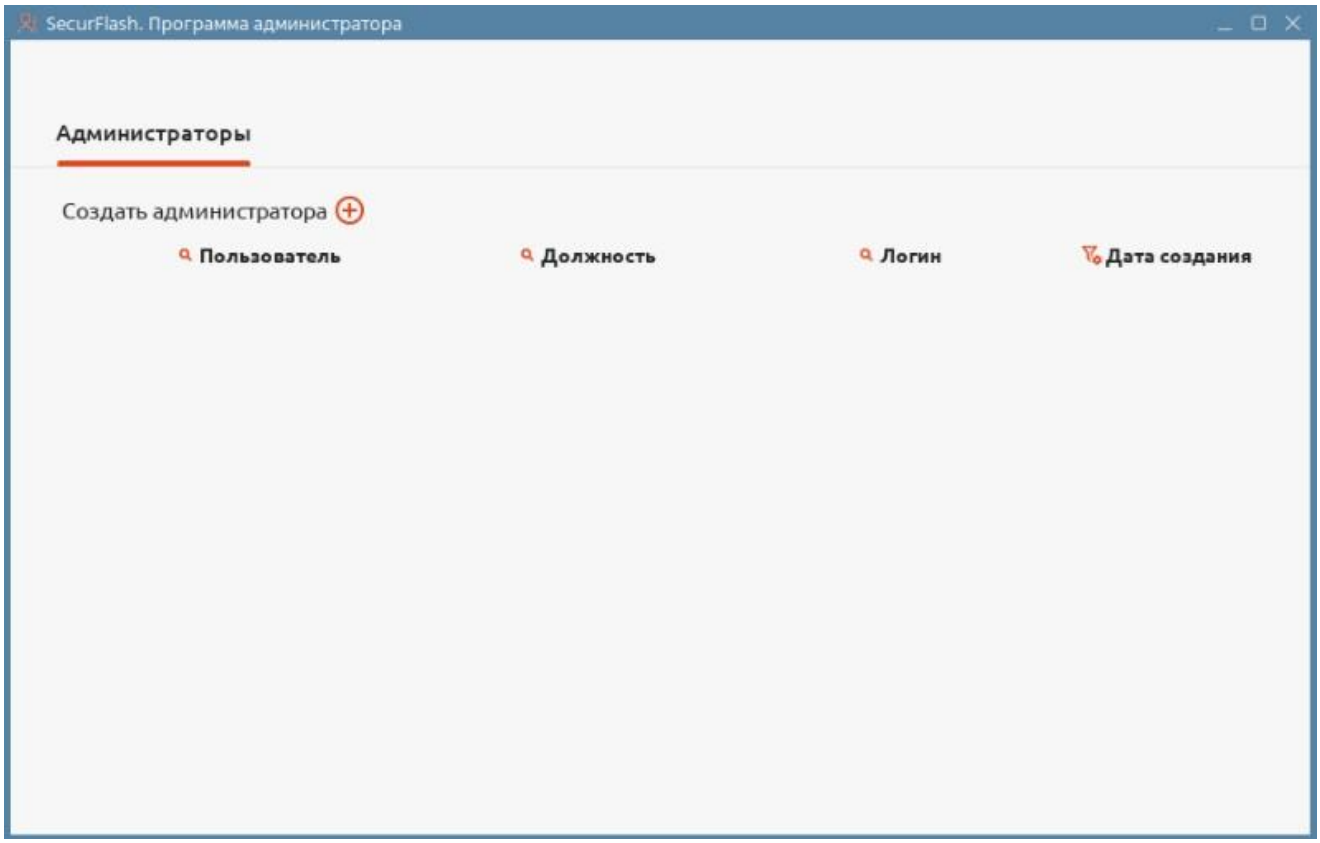


Рисунок 22 – Программа администратора после авторизации по ВПУЗ

4) во вкладке «Администраторы» нажать кнопку «Создать администратора», в открывшемся окне «Создание администратора» заполнить поля «Администратор», «Должность», нажать кнопку далее «Далее»;

5) в окне «Создание администратора»:

– ввести название контейнера администратора. По умолчанию, контейнер администратора сохраняется в домашний каталог `/home/[имя пользователя}/Aladdin/SF/admins`. При необходимости, каталог контейнера можно изменить при помощи кнопки 🗀;

– ввести пароль и подтверждение пароля администратора. Пароль должен содержать цифры, прописные и строчные буквы, спецсимволы и иметь длину не менее 12 символов. Нажать кнопку «Создать»;

6) откроется информационное окно, подтверждающее создание учетной записи администратора. Учетная запись созданного администратора появится во вкладке «Администраторы»;

7) закрыть программу администратора.

4.2.3 Авторизация администратора

Авторизация администратора в программе администратора с использованием контейнера учетной записи производится в следующей последовательности:

1) запустить программу администратора на СВТ администратора. Для этого выбрать ярлык «Программа администратора SecurFlash» в меню «Пуск», раздел «Утилиты». В открывшемся окне авторизации администратора нажать кнопку 🗀 и выбрать файл контейнера администратора;

2) в поле «Пароль» ввести пароль контейнера, нажать кнопку «Войти». Откроется окно программы администратора с полными функциональными возможностями (рисунок 23).

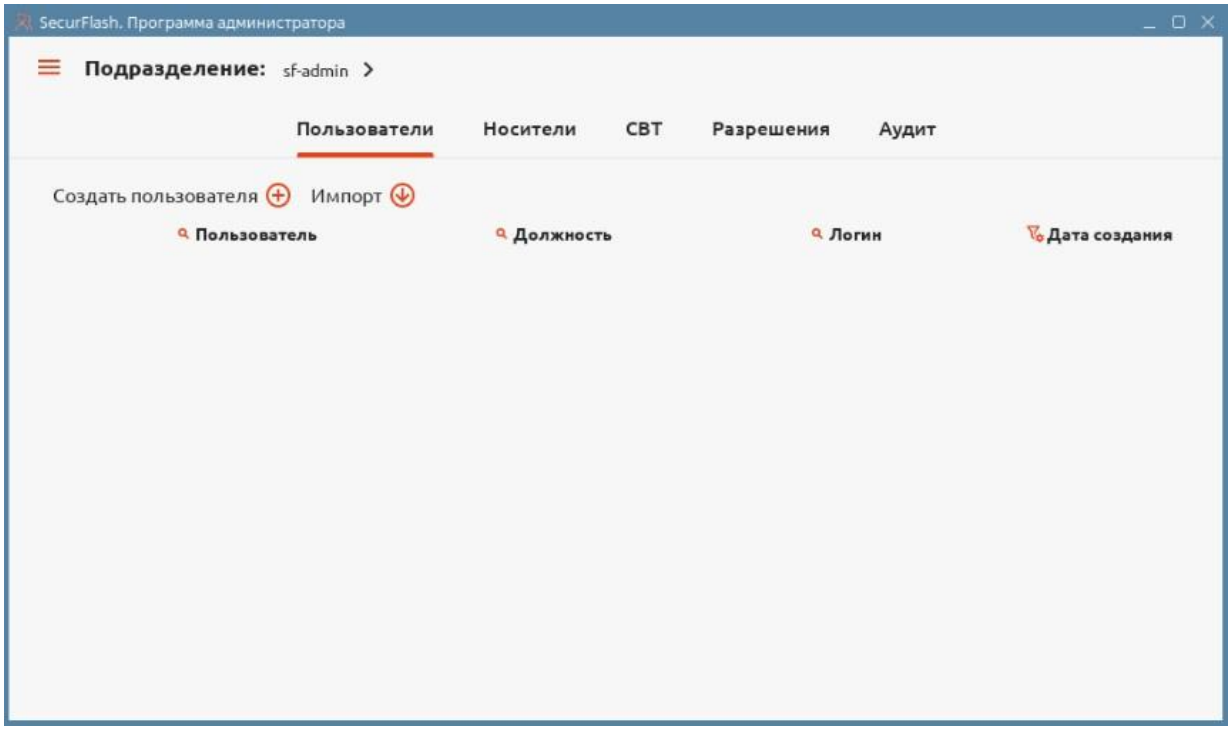


Рисунок 23 – Программа администратора с полными функциональными возможностями

4.2.4 Создание перечня разрешенных IP адресов

Перечень разрешенных IP адресов создается только при сетевом режиме функционирования сервера управления КОИ.

IP адрес сервера управления КОИ прописывать в перечне разрешенных IP адресов не требуется, так как подключение к нему доступно всегда.

Управление списком разрешенных IP адресов осуществляется во вкладке «Сетевой доступ» окна настроек программы администратора.

Для перехода в данную вкладку необходимо после авторизации в программе администратора нажать кнопку перехода в главное меню , в главном меню нажать кнопку , в открывшемся окне настроек администрирования выбрать вкладку «Сетевой доступ» (рисунок 24).

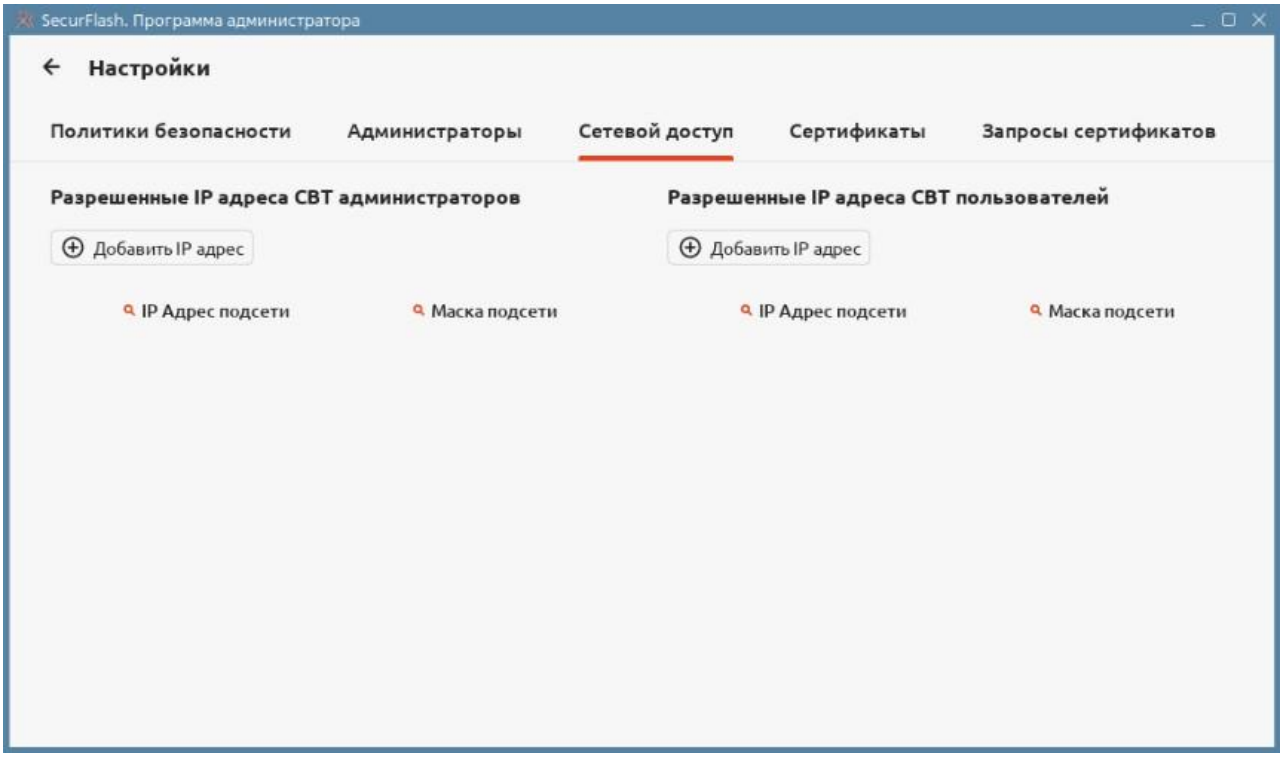


Рисунок 24 – Окно настроек администрирования, вкладка «Сетевой доступ»

Вкладка «Сетевой доступ» содержит два перечня:

1) «Разрешенные IP адреса СВТ администраторов» – IP адреса сетевых СВТ администраторов, с которых разрешено подключаться к серверу управления через программу администратора;

2) «Разрешенные IP адреса СВТ пользователей» – IP адреса сетевых СВТ пользователей, с которых разрешена автоматическая регистрация в автоматическом режиме.

Автоматическая регистрация означает, что запрос на регистрацию, полученный от СВТ пользователя, будет одобрен сервером управления в автоматическом режиме без дополнительной санкции администратора, и ответный файл регистрации автоматически поступит на СВТ пользователя.

Правила, применяемые к списку IP адресов СВТ администраторов:

1) локальное подключение к серверу управления через программу администратора разрешено всегда, даже если IP сервера управления не указан в списке;

2) если перечень пуст, то подключиться к серверу управления можно с любого IP адреса.

Правило, применяемое к списку IP адресов СВТ пользователей: если перечень пуст, то автоматическая регистрация СВТ пользователя недоступна для всех СВТ пользователя.

Для создания записи в списке разрешенных IP адресов необходимо выполнить следующие действия:

1) в поле «Разрешенные IP адреса СВТ администраторов» или «Разрешенные IP адреса СВТ пользователей» нажать кнопку «Добавить IP адрес»;

2) в открывшемся окне «Добавить IP адрес» ввести IP адрес и маску подсети СВТ, задав диапазон разрешенных IP адресов;

3) нажать кнопку «Добавить».

Появится новая запись в соответствующей таблице. Если требуется добавить новый диапазон, то необходимо повторить вышеописанные действия.

Внимание! Редактирование списка разрешенных IP адресов через файл настроек `sets.ini` не допускается, так как данные изменения не будут применены корректно.

Работа с вкладкой «Сетевой доступ» описана в 6.2.3 (стр. 72).

4.2.5 Регистрация на вышестоящем севере управления

Регистрация на вышестоящем сервере управления выполняется для всех серверов управления, кроме центрального.

Регистрацию на вышестоящем сервере управления необходимо выполнять перед регистрацией нижестоящих серверов управления.

Перед началом регистрации на вышестоящем сервере управления, необходимо на СВТ администратора запустить программу администратора и авторизоваться в ней, используя файл-контейнер и пароль администратора (4.2.3). Далее перейти в главное меню программы при помощи кнопки  . Из главного меню перейти в окно настроек администрирования, нажав кнопку  .

В окне настроек администрирования перейти во вкладку «Запросы сертификатов», далее – во вкладку второго уровня «Исходящие» (рисунок 25).

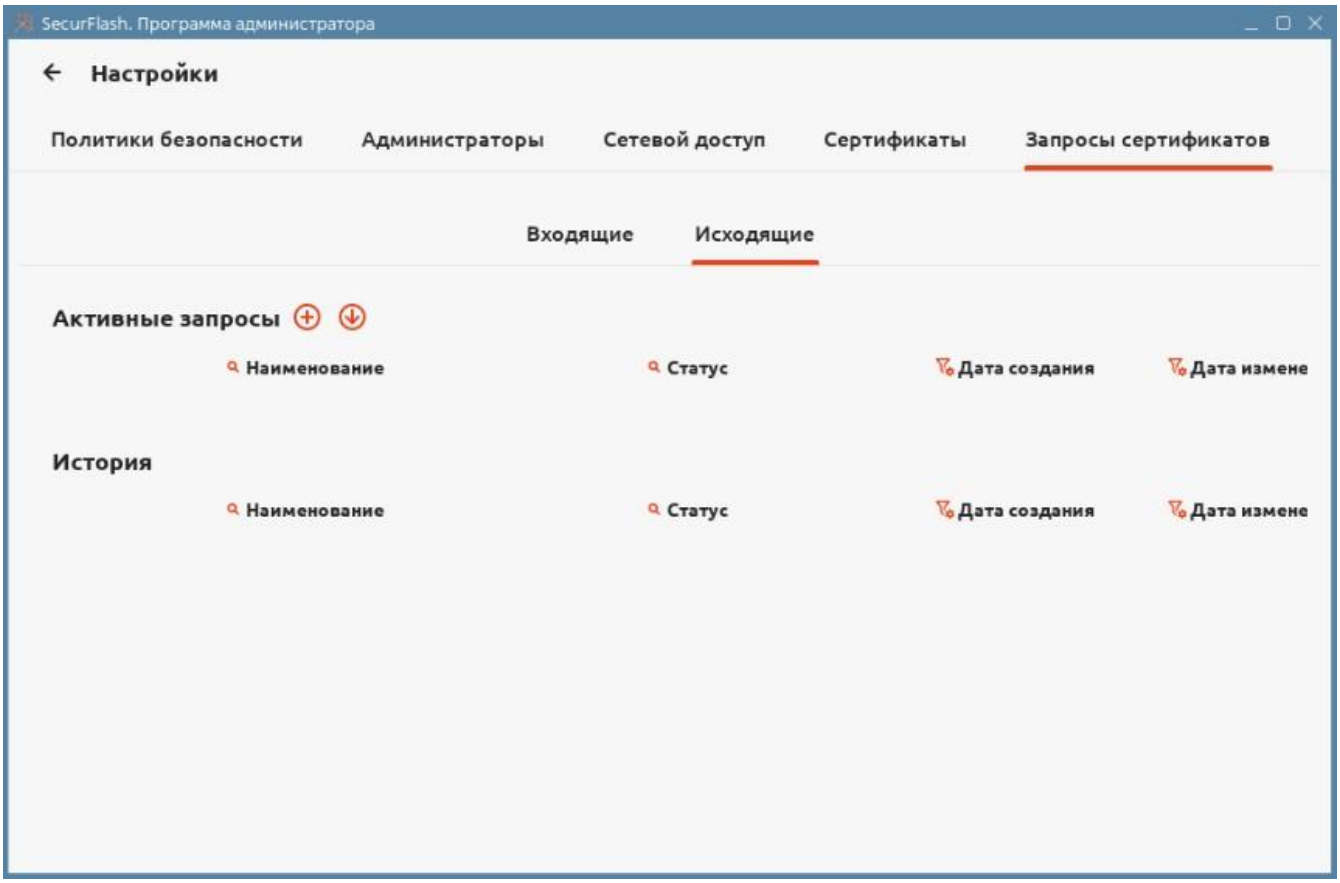


Рисунок 25 – Окно настроек администрирования, вкладка «Запросы сертификатов» – «Исходящие»

Вкладка «Исходящие» содержит активные исходящие запросы в поле «Активные запросы» и перечень архивных исходящих запросов в перечне «История».

Для регистрации на вышестоящем сервере управления необходимо выполнить следующие действия:

1) во вкладке «Исходящие» нажать кнопку ⊕, в открывшемся окне запроса нажать кнопку 🗀 и указать путь сохранения файла запроса. Нажать кнопку «Создать»;

2) передать файл запроса администратору вышестоящего сервера управления для регистрации и выпуска сертификата (4.2.6);

3) перейти во вкладку «Сертификаты», вкладку второго уровня «Свои»;

4) нажать кнопку ⊕, в открывшемся окне указать путь к сертификату, полученному от администратора вышестоящего сервера управления, импортировать сертификат;

5) в таблице вкладки «Свои» отобразится импортированный сертификат, подписанный вышестоящим сервером управления.

Примечание – После импорта сертификата от вышестоящего сервера управления контейнер ВПУЗ перестанет работать.

4.2.6 Регистрация нижестоящих серверов управления

Перед началом регистрации нижестоящего сервера управления необходимо на СВТ администратора вышестоящего сервера управления запустить программу администратора и авторизоваться в ней, используя файл-контейнер и пароль администратора (4.2.3). Далее перейти в главное меню программы при помощи кнопки . Из главного меню перейти в окно настроек администрирования, нажав кнопку .

В окне настроек администрирования перейти во вкладку «Запросы сертификатов», далее – во вкладку второго уровня «Входящие» (рисунок 26).

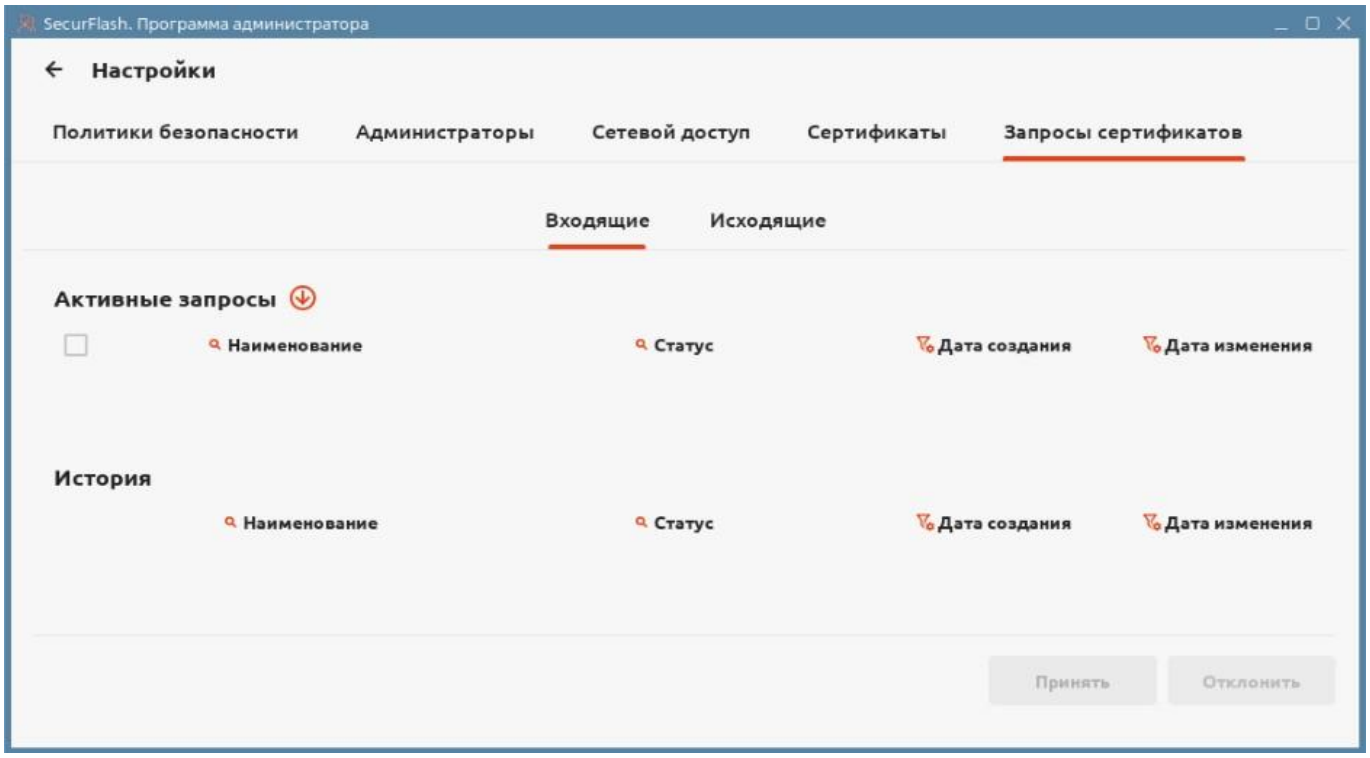


Рисунок 26 – Окно настроек администрирования, вкладка «Запросы сертификатов» – «Входящие»

Вкладка «Входящие» содержит активные входящие запросы в поле «Активные запросы» и перечень архивных входящих запросов в перечне «История».

Для регистрации нижестоящего сервера управления необходимо выполнить следующие действия:

1) получить файл запроса на сертификат от администратора нижестоящего сервера управления и перенести его в каталог `/opt/Aladdin/SF/svt`

2) во вкладке «Входящие» нажать кнопку , в открывшемся окне запроса нажать кнопку и указать путь к и файлу запроса. Импортировать файл запроса;

3) в таблице «Активные запросы» появится импортированный запрос со статусом «На рассмотрении»;

4) выделить импортированный запрос при помощи программного указателя и нажать кнопку «Принять»;

5) прейти во вкладку «Сертификаты» – вкладку второго уровня – «Нижестоящие». Убедиться, что в таблице нижестоящих сертификатов появилась запись о новом выпущенном сертификате;

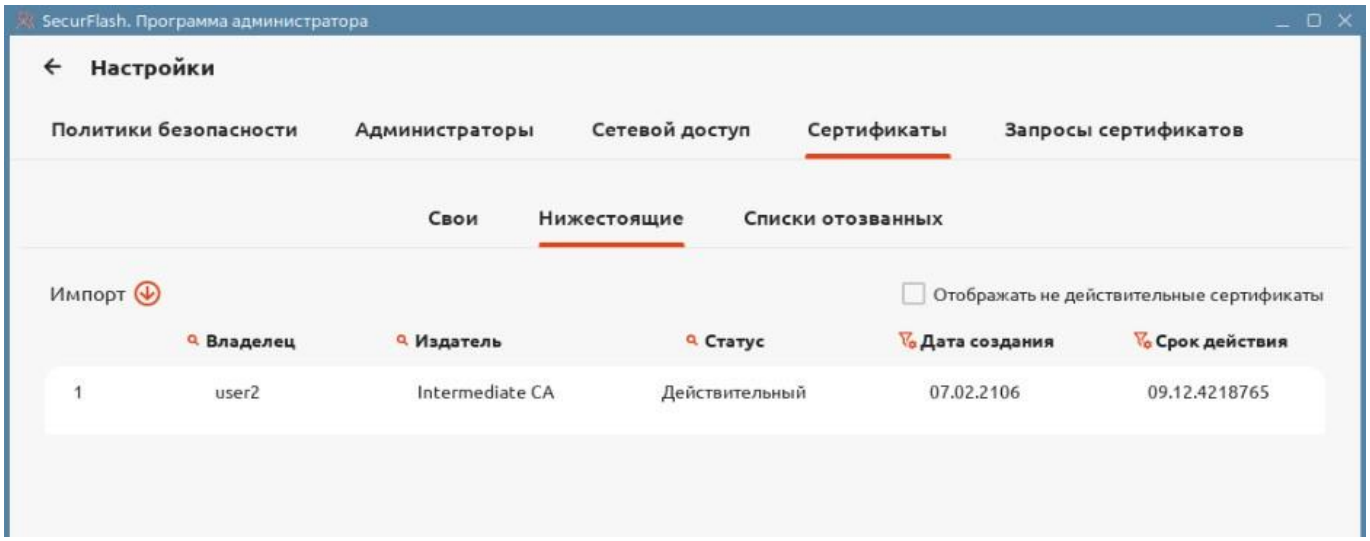


Рисунок 27 – Окно настроек администрирования, вкладка «Сертификаты» – «Нижестоящие»

6) выбрать нижестоящий сертификат, нажать правую кнопку мыши и в выпадающем контекстном меню выбрать «Экспорт»;

7) передать зарегистрированный сертификат администратору нижестоящего сервера управления.

Файл сертификата будет создан в каталоге `/opt/Aladdin/SF/svt`. Нижестоящий сервер управления будет зарегистрирован в иерархии серверов управления.

Администратор нижестоящего сервера управления должен импортировать зарегистрированный сертификат (4.2.5).

Интерфейсы вкладок «Сертификаты» и «Запросы сертификатов» подробно описаны в 6.2.4 (стр. 74).

4.2.7 Создание политики безопасности

Для упрощения администрирования носителей в рамках текущего КОИ, программа предоставляет возможность создания и редактирования политик, содержащих предустановленные администратором фиксированные настройки безопасности.

Для открытия окна настроек администрирования (рисунок 28) необходимо перейти в главное меню программы при помощи кнопки и нажать кнопку .

Работа с политиками безопасности осуществляется во вкладке «Политики безопасности» окна настроек.

Возврат в главное меню осуществляется при помощи кнопки .

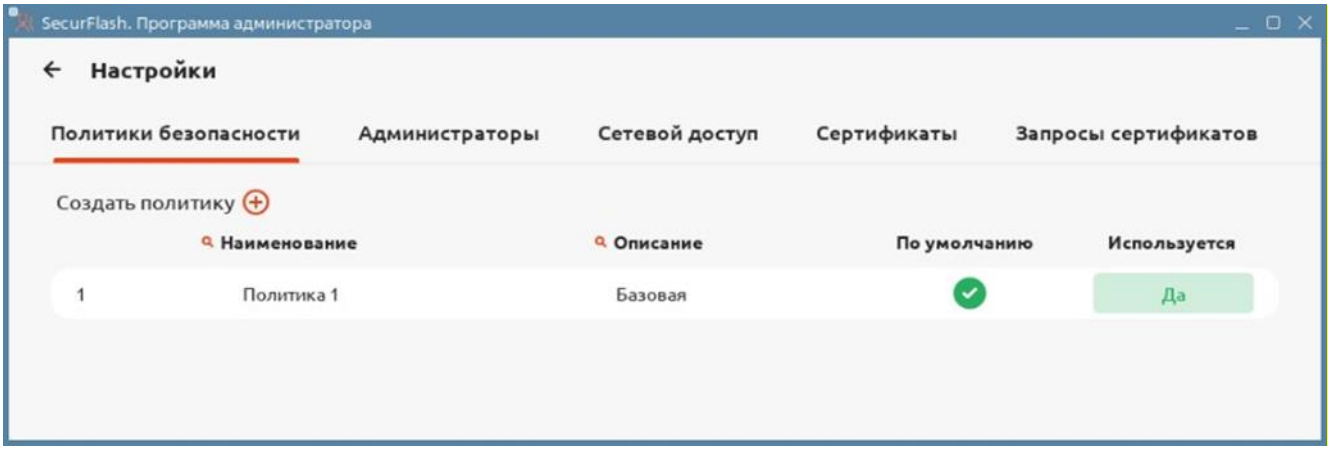


Рисунок 28 – Окно настроек администрирования, вкладка «Политики безопасности»

Перечень созданных политик безопасности отображается во кладке «Политики безопасности» в табличном виде.

Знак отображает политику, используемую по умолчанию.

В поле «Используется» отображается информация о текущем использовании политики в рамках КОИ (Да/Нет).

Для создания политики безопасности необходимо выполнить следующие действия:

1) нажать кнопку во вкладке «Политики безопасности»;

2) откроется окно «Создание политики», вкладка «Общие сведения». Ввести наименование политики, описание политики. При необходимости, установить программный указатель «Использовать по умолчанию» для использования создаваемой политики в качестве политики по умолчанию. Первая созданная политика безопасности будет использована как политика по умолчанию автоматически. Нажать кнопку «Далее»;

Примечание – Политика, имеющая признак «Использовать по умолчанию», будет использоваться при создании учетных записей пользователей (4.2.8).

3) на вкладке «Контроль доступа» установить параметр: «Разрешить администратору смену пароля пользователя» – да/нет. Нажать кнопку «Далее»;

4) на вкладке «Политика паролей» установить параметры паролей пользователей:

- минимальная длина пароля;
- требуемая сложность пароля – наличие строчных букв (a-z), цифр (0-9), прописных букв (A-Z), спецсимволов (!.,~);
- максимально возможное количество неуспешных попыток ввода пароля в течение одной сессии;
- ограничение срока действия пароля (в днях);
- нажать кнопку «Далее»;

5) на вкладке «Журналирование» выбрать один из вариантов действия при переполнении журнала носителя:

- циклическая перезапись – журнал аудита носителя после полного заполнения будет перезаписываться;
- блокировка носителя до выгрузки журнала – после полного заполнения журнала аудита носитель будет заблокирован, до момента выгрузки журнала администратором;
- при необходимости, установить оповещение о скором переполнении журнала аудита носителя (когда остается менее 10% свободно пространства);
- нажать кнопку «Создать».

После выполнения сценария созданная политика отобразится в таблице.

Политика устанавливается как политика по умолчанию, если она единственная в таблице или соответствующий параметр задан при создании.

Интерфейсы вкладки «Политики безопасности» подробно описаны в 6.2.1 (стр. 68).

4.2.8 Создание учетной записи пользователя

Работа с учетными записями пользователей осуществляется во вкладке «Пользователи» (рисунок 29) главного окна программы.

Перечень созданных учетных записей пользователей отображается в табличном виде.

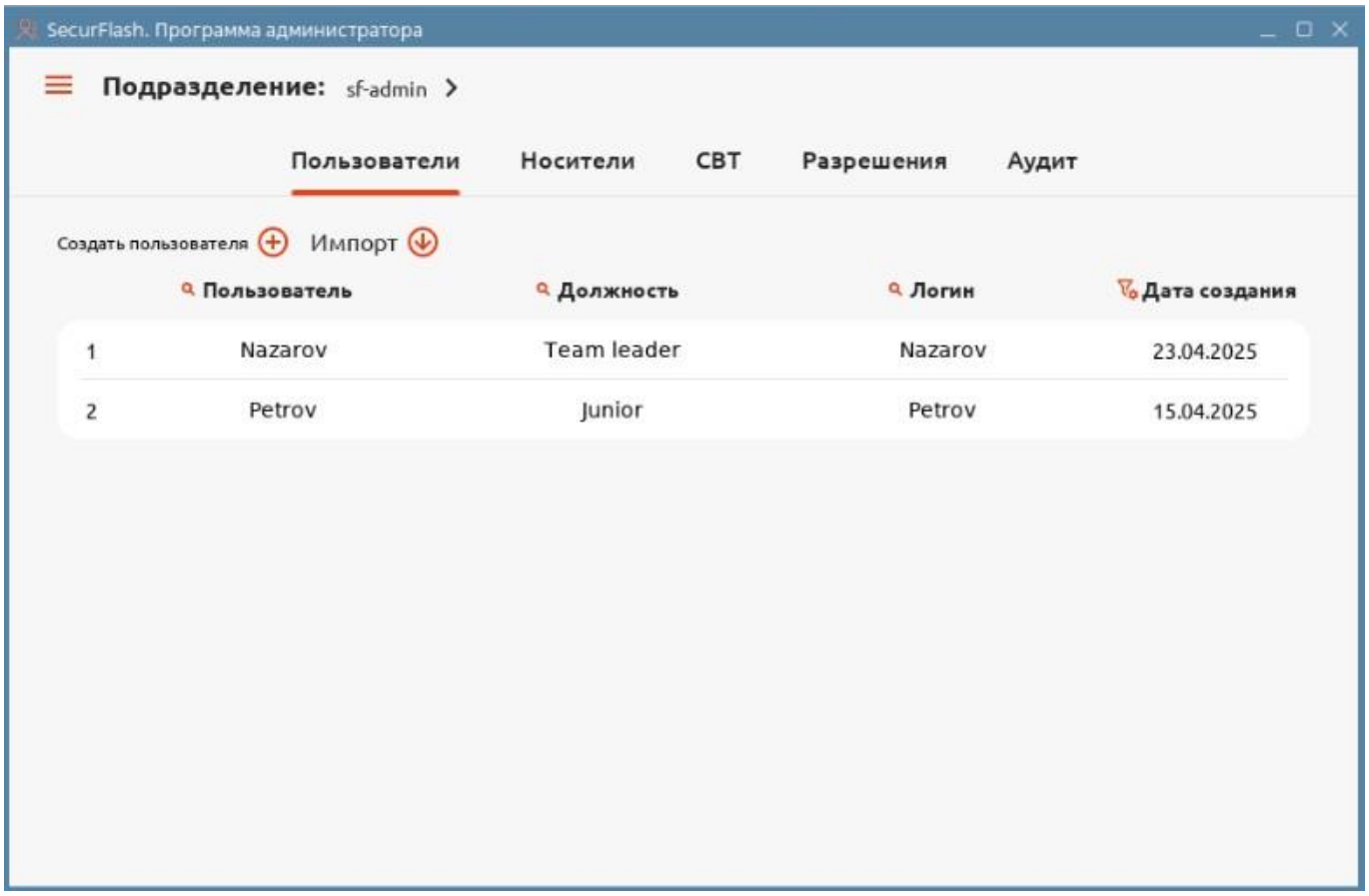


Рисунок 29 – Окно настроек администрирования, вкладка «Пользователи»

Для создания учетной записи пользователя выполнить следующие действия:

1) убедиться, что требуемая политика безопасности создана (4.2.1, стр. 40);

2) во вкладке «Пользователи» нажать кнопку ⊕;

3) в открывшемся окне «Создание пользователя» указать ФИО и должность пользователя. Нажать кнопку «Далее»;

4) в следующем окне ввести логин пользователя, пароль пользователя и подтверждение пароля. Нажать кнопку «Создать».

Созданная учетная запись пользователя отобразится в таблице пользователей. К учетной записи будет применена политика безопасности, указанная по умолчанию.

4.2.9 Создание учетных записей пользователей из csv-файла

В программе администратора предусмотрена возможность создания группы учетных записей с помощью заранее подготовленного csv-файла.

Таблица csv-файла должна содержать заполненные строки учетных записей. Столбцы таблицы должны иметь следующие наименования в указанном порядке:

- «ФИО»;
- «Должность»;
- «Логин»;
- «Пароль»;
- «Подтверждение пароля».

Для создания группы учетных записей пользователей из csv-файла выполнить следующие действия:

1) убедиться, что требуемая политика безопасности создана (4.2.7);
2) во вкладке «Пользователи» нажать кнопку «Импорт»;
3) в открывшемся окне нажать кнопку  папки и указать путь к csv-файлу с информацией об учетных записях пользователей в требуемом формате. Нажать кнопку «Создать».

Созданные учетные записи пользователей отобразится в таблице пользователей. К учетным записям будет применена политика безопасности, указанная по умолчанию.

Интерфейсы вкладки «Пользователи» подробно описаны в 6.3.1 (стр. 76).

4.3 Первоначальная настройка СВТ пользователей

4.3.1 Настройка режима функционирования СВТ пользователей

Предусмотрено два режима функционирования СВТ пользователей: сетевой и автономный.

По умолчанию СВТ пользователя функционирует в автономном режиме.

Для настройки сетевого режима необходимо выполнить следующие действия:

1) запустить в текстовом редакторе файл sets.ini, расположенный в папке:

```
/opt/Aladdin/SF/sets.ini
```

2) в поле:

```
[CertResponder]
Addr=127.0.0.1
```

и поле:

```
[DBServer]
Addr=127.0.0.1
```

заменить значение параметра «Addr» на значение внешнего IP адреса СВТ сервера управления, к которому необходимо подключить ПП, например `Addr=192.168.91.101`

3) сохранить изменения и перезапустить службу командой:

```
sudo systemctl restart sfaccserver.service
```

4.3.2 Регистрация СВТ пользователей

Упрощенно процесс регистрации СВТ пользователей состоит из:

- отправки запроса на регистрацию из программы пользователя;
- регистрации запроса в программе администратора и экспорта сертификата;
- регистрации сертификата в программе пользователя.

IP адрес сетевых СВТ пользователей может быть включен или не включен в таблицу разрешенных IP адресов.

Для сетевых СВТ пользователей с IP адресами, включенными в перечень разрешенных, регистрация запроса и экспорт сертификата осуществляются в автоматическом режиме и не требует дополнительного подтверждения в программе администратора. Подробно сценарии регистрации сетевых и автономных СВТ пользователей описаны в 4.3.2.1, 4.3.2.2.

Программа пользователя работает в режиме ограниченной функциональности до момента подтверждения регистрации СВТ пользователя. В ограниченном режиме доступны только функции регистрации.

4.3.2.1 Регистрация сетевого СВТ пользователя

Регистрация сетевого СВТ пользователя возможна только в том случае, если сервер управления КОИ также настроен на сетевой режим.

Регистрация выполняется в следующей последовательности:

1) запустить программу администратора на сетевом СВТ администратора. Авторизоваться в программе администратора с использованием контейнера администратора (4.2.3, стр. 43);

2) запустить программу пользователя режиме настройки на СВТ пользователя (3.4.2.3, стр. 35);

3) в окне «Настройки» программы пользователя нажать кнопку «Запрос на регистрацию». Подтвердить создание файла запроса в каталоге по умолчанию: `/opt/Aladdin/SF/svt`

4) если IP адрес включен в перечень разрешенных IP адресов и автоматическая регистрация доступна, то:

– нажать кнопку «Регистрация»;

– в открывшемся окне нажать кнопку  и выбрать файл сертификата (cert) из каталога: `/opt/Aladdin/SF/svt`

– завершить процесс регистрации, нажав кнопку «Зарегистрировать»;

5) если IP адрес не включен в перечень разрешенных IP адресов и автоматическая регистрация не доступна, то:

– в главном окне программы администратора выбрать вкладку «СВТ». В таблице СВТ выбрать новую запись со статусом «Не зарегистрирован». Нажать кнопку «Зарегистрировать». СВТ будет зарегистрировано на сервере управления. Файл сертификата (расширение cert) будет создан в каталоге `/opt/Aladdin/SF/svt`

– перенести созданный файл сертификата из каталога `/opt/Aladdin/SF/svt` на регистрируемое СВТ пользователя в тот же каталог;

– в программе пользователя нажать кнопку «Регистрация»;

– в открывшемся окне нажать кнопку  и выбрать файл сертификата (cert) из каталога `/opt/Aladdin/SF/svt` и завершить процесс регистрации, нажав кнопку «Зарегистрировать».

4.3.2.2 Регистрация автономного СВТ пользователя

Регистрация автономного СВТ пользователя возможна и при сетевом, и при автономном режиме функционирования сервера управления КОИ.

Регистрация сетевого СВТ пользователя выполняется следующим образом:

1) запустить программу администратора на сетевом СВТ администратора. Авторизоваться в программе администратора с использованием контейнера администратора (4.2.3, стр. 43);

2) запустить программу пользователя в режиме настроек на СВТ пользователя (3.4.2.3, стр. 35);

3) в окне «Настройки» программы пользователя нажать кнопку «Запрос на регистрацию». Подтвердить создание файла запроса в каталоге по умолчанию: `/opt/Aladdin/SF/svt`

4) перенести файл запроса на СВТ администратора в каталог: `/opt/Aladdin/SF/svt`

5) в главном окне программы администратора выбрать вкладку «СВТ». Нажать кнопку «Добавить СВТ». В открывшемся окне нажать иконку папки и выбрать файл запроса в каталоге: `/opt/Aladdin/SF/svt`

6) в таблице СВТ выбрать новую запись со статусом «Не зарегистрирован». Нажать кнопку «Зарегистрировать». СВТ пользователя зарегистрирован на сервере управления, файл сертификата (cert) будет создан в каталоге: `/opt/Aladdin/SF/svt`

7) в таблице папки СВТ выбрать запись зарегистрированного СВТ и нажать кнопку «Экспорт» (или можно нажать правую кнопку мыши и выбрать «Экспорт» в открывшемся контекстном меню);

8) в открывшемся окне нажать кнопку  и выбрать имя и путь сохранения файла регистрации СВТ;

9) переместить файл регистрации на СВТ пользователя;

10) в окне «Настройки» программы пользователя нажать кнопку «Обновление разрешений». Указать путь к файлу регистрации СВТ. Данная операция необходима для корректной работы механизма проверки сертификата СВТ на СВТ пользователя, а также для переноса списка актуальных разрешений на СВТ пользователя;

11) нажать кнопку «Регистрация»;

12) в открывшемся окне нажать кнопку  и выбрать файл сертификата (cert) из каталога `/opt/Aladdin/SF/svt` и завершить процесс регистрации, нажав кнопку «Зарегистрировать»;

13) закрыть программу пользователя;

14) выполнить команду:

```
sudo systemctl restart sfaccserver.service
```

Работа с программой пользователя подробно описана в документе «Средство защиты информации на съемных машинных носителях SecurFlash. Руководство оператора» RU.АЛДЕ.03.01.046 34 01.

Работа с вкладкой «СВТ» подробно описана в 6.3.3 (стр. 80).

5 ОСНОВНЫЕ СЦЕНАРИИ АДМИНИСТРИРОВАНИЯ КОИ

5.1 Сценарии администрирования сервера управления КОИ

5.1.1 Автоматический запуск, остановка, запуск и перезапуск сервера управления

Сервер управления запускается автоматически в режиме службы в случае нештатного отключения питания, сбоя ОС, штатной перезагрузки сервера управления.

Для проверки состояния сервера управления используется команда:

```
sudo systemctl status sfaccserver.service
```

Для принудительной остановки сервера управления используется команда:

```
sudo systemctl stop sfaccserver.service
```

Для запуска сервера управления после остановки используется команда:

```
sudo systemctl start sfaccserver.service
```

Для перезапуска сервера управления используется команда:

```
sudo systemctl restart sfaccserver.service
```

5.1.2 Создание дополнительного контейнера встроенной привилегированной учетной записи

Дополнительный контейнер ВПУЗ сервера управления используется для следующих целей:

– использование в качестве резервного контейнера ВПУЗ;

– выдача новому администратору сервера управления для настройки нового СВТ администратора (4.2.2, стр. 41).

Создание дополнительного контейнера ВПУЗ производится в следующей последовательности:

1) выполнить команду:

```
sudo sfaccserver -c
```

2) ввести пароль контейнера ВПУЗ (4.1.1, стр. 38):

```
Container password:
```

3) ввести имя путь сохранения и имя нового контейнера:

```
New container path (/root/new_account.pfx):
```

или оставить текущее состояние, нажав «Enter»;

4) ввести пароль дополнительного контейнера:

```
Set new container password:
```

5) подтвердить пароль дополнительного контейнера:

```
Confirm password:
```

6) дополнительный контейнер ВПУЗ будет сохранен в заданной папке.

5.1.3 Переход на нижестоящий сервер управления

Для реализации сценариев администрирования носителя необходимо запустить программу администратора и авторизоваться в ней, используя файл-контейнер и пароль администратора (4.2.3, стр. 43).

Нажать кнопку перехода в главном меню  .

В дереве главного меню выбрать нижестоящий сервер управления.

5.2 Сценарии администрирования носителей

Для реализации сценариев администрирования носителя необходимо запустить программу администратора и авторизоваться в ней, используя файл-контейнер и пароль администратора (4.2.3, стр. 43).

Работа с носителями осуществляется во вкладках «Носители» или «Разрешения».

Интерфейсы вкладки «Носители» подробно описаны в 6.3.2, стр. 78.

Интерфейсы вкладки «Разрешения» подробно описаны в 6.3.4, стр. 82.

5.2.1 Инициализация носителя

Управление носителями осуществляется в главном окне программы администратора, во вкладке «Носители» (рисунок 30).

При инициализации администратором устанавливаются разрешения на доступ к носителю определенных пользователей и только на определенных СВТ. Можно установить права для всех пользователей на всех СВТ.

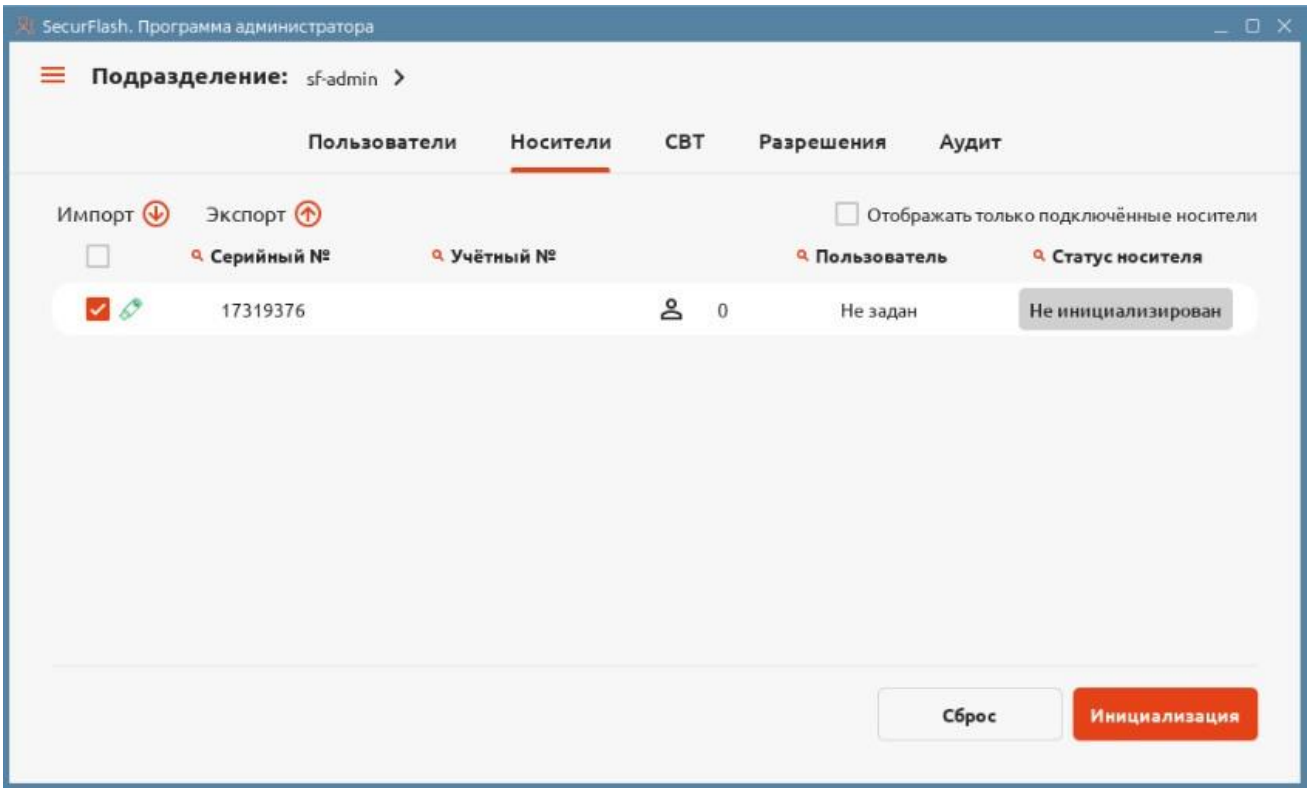


Рисунок 30 – Окно администрирования, вкладка «Носители»

Перечень носителей отображается в табличном виде.

Для инициализации носителя необходимо выполнить следующие действия:

1) убедиться, что требуемая политика безопасности создана (4.2.7, стр. 49);

2) убедиться, что требуемые учетные записи пользователей созданы (4.2.8, стр. 50; 4.2.9, стр. 52);

3) подключить неинициализированный носитель (или несколько носителей) к СВТ администратора. Подключенные носители отображаются в таблице пиктограммой зеленого цвета ;

4) выбрать подключенный носитель (носители), используя программный указатель , нажать кнопку «Инициализация»;

5) в открывшемся окне «Инициализация носителя» нажать на поле «Не настроен»;

6) в открывшемся окне «Инициализация» указать:

– учетный номер носителя;

– нажать на поле «Пользователь не выбран». В выпадающем списке выбрать пользователей инициализируемого носителя. Для начала инициализации необходимо выбрать минимум одного пользователя;

– установить переключатель «Доступ ко всем СВТ подразделения», если требуется выдать разрешение на работу со всеми зарегистрированными СВТ в рамках КОИ. Если переключатель не установлен, то после инициализации необходимо будет во вкладке «Разрешения» установить разрешения для конкретных СВТ (5.2.2);

– при необходимости, установить переключатель «Упрощенный режим хранения» – включение данного режима увеличит скорость доступа к защищенному разделу;

– установить переключатель «Распечатать информационную карточку о носителе», если необходимо отправить на печать информационную карточку носителя;

7) в окне «Инициализация носителя» нажать кнопку «Ок»;

8) если требуется инициализировать более одного носителя, то выполнить перечисления 5) – 7) для остальных носителей;

9) нажать кнопку «Инициализировать» в окне «Инициализация носителя».

После завершения процесса инициализации статус носителя (носителей) в таблице вкладки «Носители» изменится на «Инициализирован».

Инициализированный носитель передается пользователю вместе с логином и паролем учетной записи. Пользователю также сообщается информация об установках используемой политики безопасности.

5.2.2 Редактирование разрешений носителя на доступ к СВТ

Управление разрешениями осуществляется в главном окне программы, во вкладке «Разрешения» (рисунок 31).

При редактировании разрешений администратором устанавливаются права на доступ к носителю только на определенных СВТ, зарегистрированных в рамках КОИ.

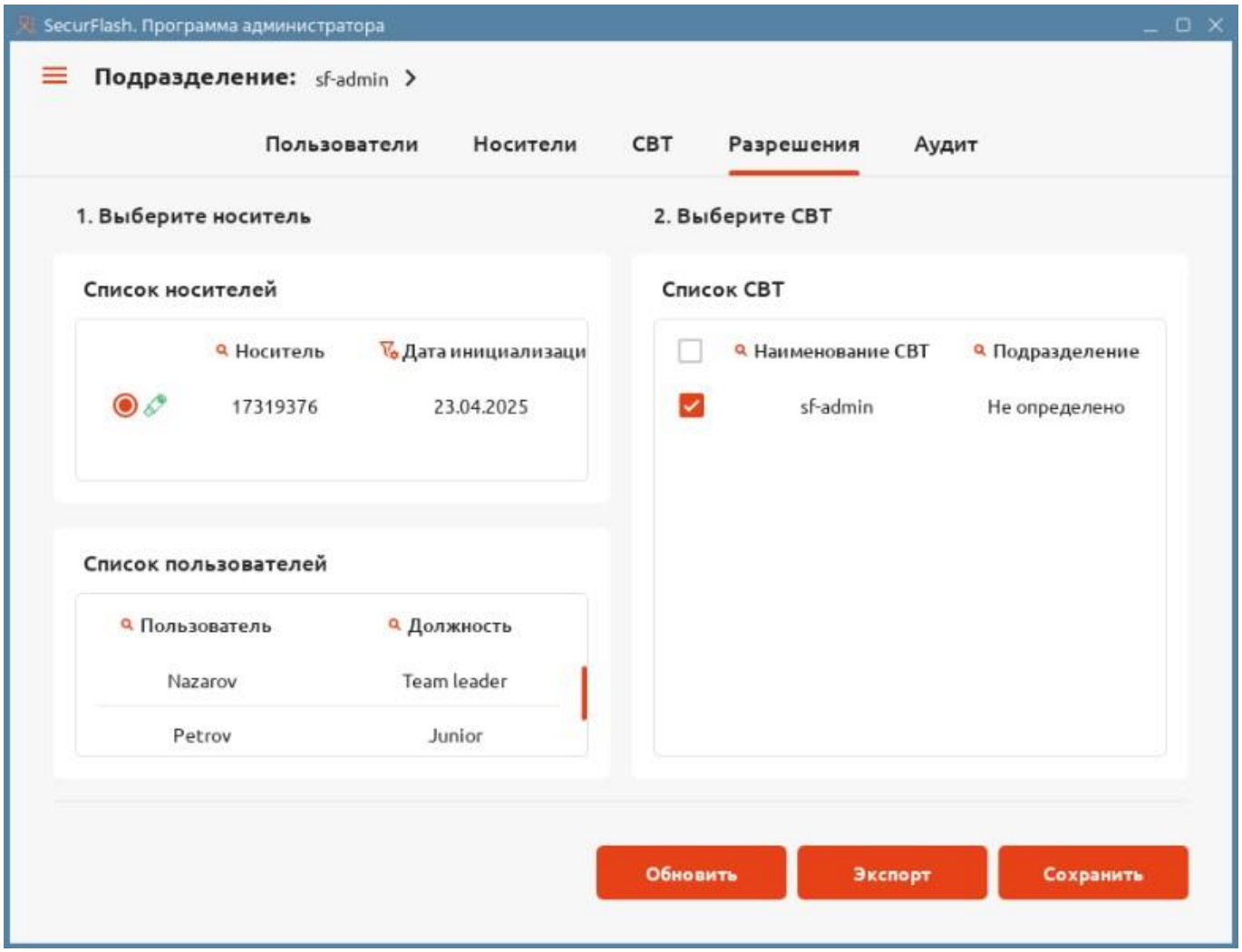


Рисунок 31 – Окно администрирования, вкладка «Разрешения»

Для изменения списка разрешений носителя необходимо сделать следующее:

1) подключить инициализированный носитель (инициализация носителя описана в 5.2.1);
2) перейти во вкладку «Разрешения»;
3) выбрать инициализированный ранее носитель в таблице «Список носителей»;
4) выбрать СВТ, на работу с которыми необходимо выдать разрешение, в таблице «Список СВТ»;
5) нажать кнопку «Сохранить».

Если носитель физически подключен к СВТ администратора, то разрешения запишутся на носитель в момент сохранения.

После изменения и обновления разрешений защищенный скрытый раздел носителя можно будет подключить только на тех зарегистрированных СВТ пользователей, на которые были выданы разрешения.

5.2.3 Разблокировка носителя

Количество неуспешных попыток ввода пароля пользователем при подключении защищенного раздела ограничено значением, установленным применяемой политикой безопасности. Если пользователь превысит установленное значение неуспешных попыток ввода пароля, то носитель будет заблокирован. Для разблокировки необходимо передать носитель администратору своего КОИ.

Для разблокировки носителя администратор должен выполнить следующие действия:

1) подключить заблокированный носитель к СВТ администратора;
2) перейти на вкладку «Носители»;
3) выбрать заблокированный носитель, нажать правую кнопку мыши и в выпадающем контекстном меню выбрать «Разблокировка носителя».

После разблокировки статус носителя изменится на «Инициализирован», и его можно будет вернуть пользователю.

5.2.4 Сброс носителя

Для проведения сброса необходимо выбрать инициализированный носитель во вкладке «Носители» и нажать кнопку «Сброс».

После сброса статус носителя в таблице изменится на «Не инициализирован», вся информация в защищенном разделе носителя и информация об установленных разрешениях станет удалена.

Использование носителя после сброса возможно только при повторной инициализации (5.2.1, стр. 57).

5.3 Администрирование СВТ пользователей

5.3.1 Отмена регистрации СВТ пользователя

Для выполнения отмены регистрации СВТ пользователя необходимо запустить программу администратора и авторизоваться в ней, используя файл-контейнер и пароль администратора (4.2.3, стр. 43).

Перечень СВТ пользователей отображается во вкладке «СВТ» (рисунок 32).

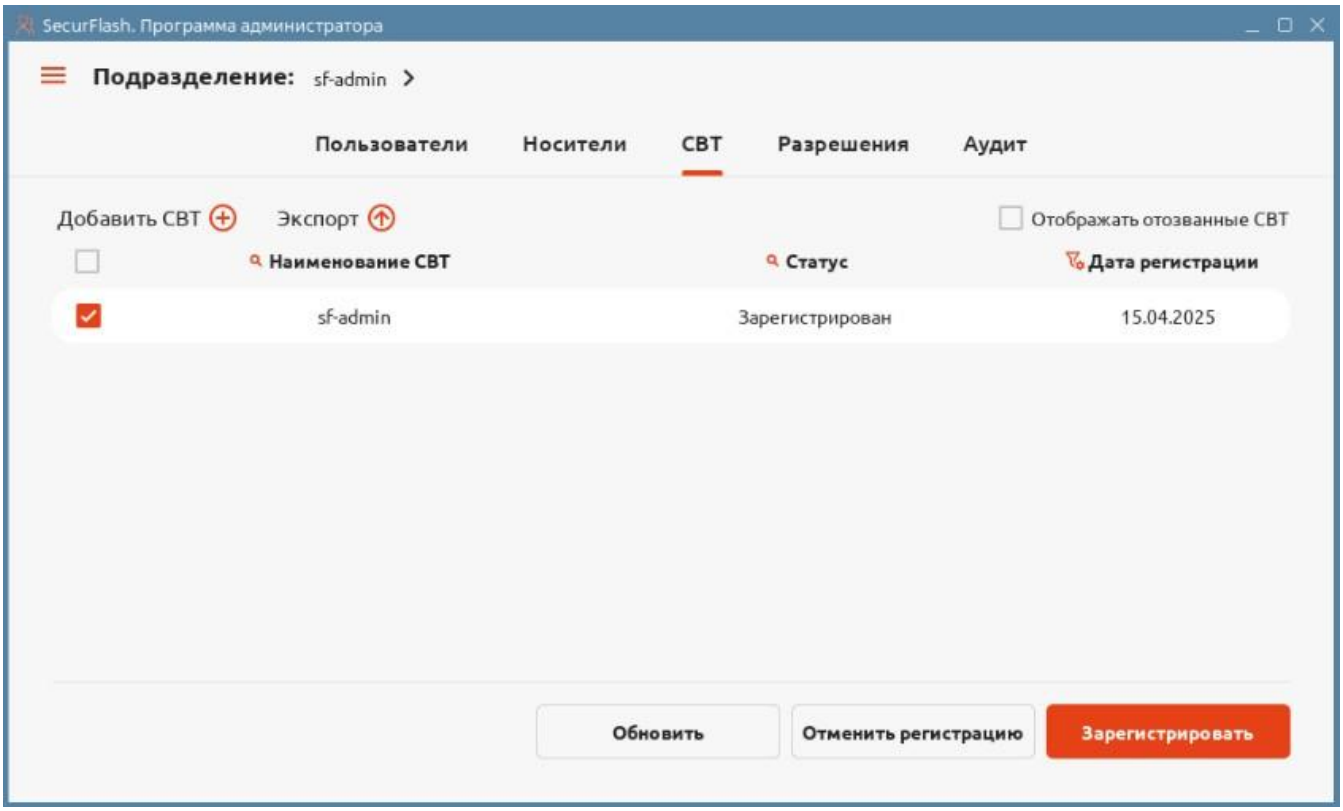


Рисунок 32 – Главное окно программы администратора, вкладка «Аудит»

Для отзыва регистрации сетевого СВТ пользователя, необходимо в таблице вкладки «СВТ» выделить нужное сетевое СВТ при помощи программного указателя и нажать кнопку «Отменить регистрацию». Отзыв регистрации произойдет в автоматическом режиме, дополнительных действий не требуется. Статус СВТ в таблице изменится на «Отозвано».

Для отзыва регистрации автономного СВТ пользователя необходимо выполнить следующие действия:

1) в таблице вкладки «СВТ» выделить нужное автономное СВТ при помощи программного указателя и нажать кнопку «Отменить регистрацию». Статус СВТ в таблице изменится на «Отозвано»;

2) выбрать отозванное СВТ и нажать правую кнопку мыши, в выпадающем контекстном меню выбрать пункт «Экспорт»;

3) в открывшемся окне выбрать путь сохранения файла регистрации СВТ при помощи кнопки ;

4) переместить файл регистрации на автономное СВТ пользователя;

5) запустить программу пользователя в режиме настроек;

6) перейти в настройки программы пользователя, нажать кнопку «Обновление разрешений». При помощи кнопки  указать путь к файлу отзыва регистрации СВТ. Импортировать файл разрешений;

7) выполнить команду:

```
sudo systemctl restart sfaccserver.service
```

5.4 Сценарии аудита

Для реализации сценариев аудита необходимо запустить программу администратора и авторизоваться в ней, используя файл-контейнер и пароль администратора (4.2.3, стр. 43).

Аудит осуществляется во вкладке «Аудит».

Интерфейсы вкладки «Аудит» подробно описаны в 6.3.5, стр. 84.

5.4.1 Просмотр событий безопасности

Просмотр событий аудита доступен администратору во вкладке «Аудит» (рисунок 33). Все события представлены в табличном виде, для упрощения поиска предусмотрена возможность использования контекстного фильтра.

Программный указатель  в графе «НСД» служит для отображения только событий несанкционированного доступа.

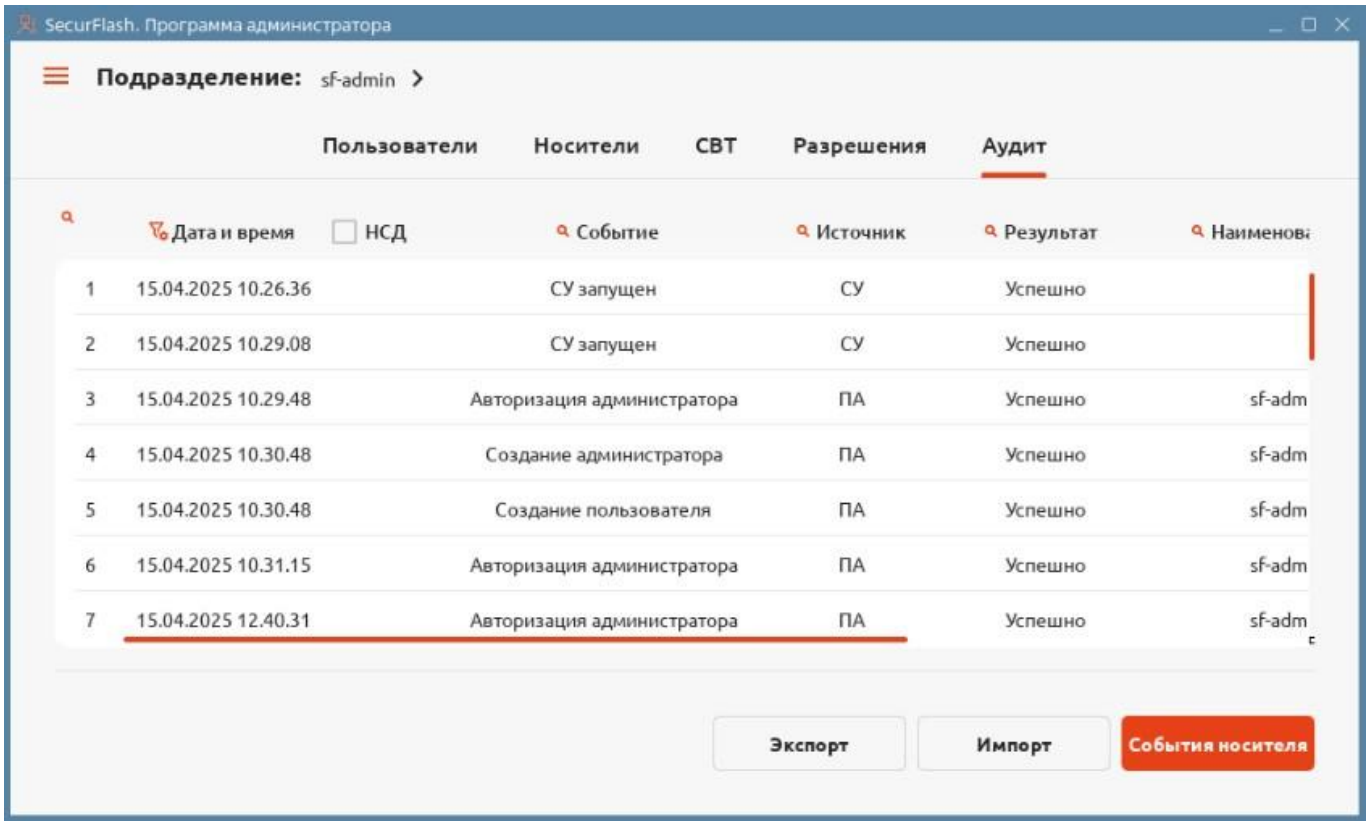


Рисунок 33 – Главное окно программы администратора, вкладка «Аудит»

5.4.2 Импорт событий безопасности с носителя

События аудита, связанные с носителем, регистрируются на локальном журнале носителя. Импорт локальных журналов осуществляется для их консолидации в основном журнале аудита с возможностью просмотра событий локальных журналов во вкладке «Аудит».

Для импорта журнала носителя необходимо выполнить следующие действия:

1) подключить носитель к USB-разъему СВТ администратора;

2) во вкладке «Аудит» нажать кнопку «События носителя»;

3) в открывшемся окне «Выбор носителя» выбрать подключенный носитель и нажать кнопку «Ок»;

4) события носителя будут импортированы в основной журнал и отобразятся в таблице вкладки «Аудит».

5.4.3 Импорт, экспорт и удаление (при экспорте) журнала аудита

Во вкладке «Аудит» предусмотрена возможность экспорта, импорта и удаления журнала аудита. Экспорт и импорт могут применяться, например, для архивирования журнала. Также импорт может применяться для импортирования журнала автономного СВТ пользователя.

Для экспорта журнала аудита необходимо выполнить следующие действия:

1) во вкладке «Аудит» нажать кнопку «Экспорт»;
2) в открывшемся окне «Экспорт журнала», при необходимости, установить путь для экспорта файла журнала при помощи кнопки  ;
3) при необходимости удалить журнал из базы данных после экспорта, установить программный указатель  в поле «Удалить данные из БД после экспорта»;
4) нажать кнопку «Экспорт».

Файл журнала будет сохранен в указанной папке. Таблица журнала во вкладке «Аудит» будет очищена, если был установлен соответствующий указатель.

Для импорта журнала аудита необходимо выполнить следующие действия»:

1) во вкладке «Аудит» нажать кнопку «Импорт»;
2) в открывшемся окне «Импорт журнала» установить путь к папке импортируемого файла журнала при помощи кнопки  ;
3) нажать кнопку «Импорт».

Журнал будет импортирован в основной журнал аудита.

6 ОПИСАНИЕ ИНТЕРФЕЙСОВ ПРОГРАММЫ АДМИНИСТРАТОРА

Интерфейсы программы администратора содержат три основных элемента:

- главное меню (6.1, стр. 66);
- окно настроек администрирования (6.2, стр.67);
- окно администрирования (6.2.4, стр. 74).

6.1 Главное меню программы администратора

Запустить программу администратора и авторизоваться в ней, используя файл-контейнер и пароль администратора (4.2.3, стр. 43). После успешной авторизации откроется окно администрирования (главное окно программы).

Для перехода в главное меню программы администратора нажать кнопку .

Главное меню (рисунок 34) содержит дерево серверов управления в рамках иерархической структуры.

Кнопка «Обновить дерево» служит для обновления отображаемой иерархической структуры.

В нижней части главного меню расположена кнопка перехода в окно настроек администрирования и кнопка открытия справочного окна о программе .

Рисунок 34 – Главное меню программы администратора

Для просмотра информации о программе администратора в главном меню нажать кнопку , при этом откроется информационное окно «О программе» (рисунок 35).

Рисунок 35 – Окно «О программе»

Окно «О программе» содержит сведения о наименовании и разработчике программы администратора, а также информацию о версии, номере сборки и контактные данные тех. поддержки.

6.2 Окно настроек администрирования

Окно настроек администрирования (рисунок 36) открывается авторизованным администратором после нажатия кнопки в главном меню.

Возврат в главное меню осуществляется при помощи кнопки .

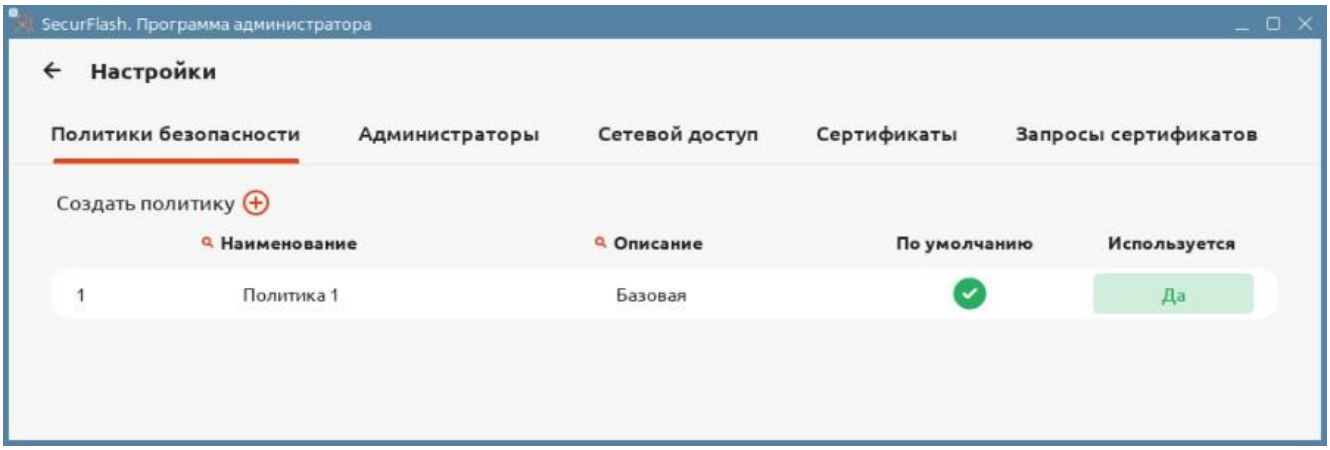


Рисунок 36 – Окно настроек администрирования, вкладка «Политики безопасности»

Окно настроек администрирования содержит следующие вкладки:

1) «Политики безопасности» — управление политиками безопасности (4.2.7, стр.49);
2) «Администраторы» — управление учетными записями администраторов (6.2.2, стр. 70);
3) «Сетевой доступ» — управление настройками сетевого доступа (6.2.3, стр. 72);
4) «Сертификаты» – управление сертификатами серверов в рамках иерархической системы (6.2.4, стр. 74);
5) «Запросы сертификатов» – управление запросами сертификатов (6.2.5, стр. 75).

6.2.1 Политики безопасности

Управление политиками безопасности осуществляется во вкладке «Политики безопасности» окна настроек администрирования. Перечень созданных политик безопасности отображается в табличном виде (рисунок 36). Для работы с политиками безопасности доступны следующие функции:

1) создание политики безопасности – кнопка «Создать политику» (4.2.7, стр. 49);
2) редактирование политики безопасности – пункт «Редактировать» в контекстном меню;
3) клонирование политики безопасности – пункт «Клонировать» в контекстном меню;
4) установка использования по умолчанию для политики безопасности – пункт «Использовать по умолчанию» в контекстном меню;
5) удаление политики безопасности – пункт «Удалить» в контекстном меню;
6) информация о политике безопасности – пункт «Информация» в контекстном меню.

Таблица перечня политик безопасности содержит следующие графы:

1) наименование – задается при создании политики безопасности, можно редактировать;

2) описание – задается при создании политики безопасности, можно редактировать;

3) по умолчанию – отображает знаком политику, используемую по умолчанию. В рамках КОИ может быть определена только одна политика по умолчанию;

4) используется – отображает информацию об использовании политики в КОИ (Да/Нет).

Поиск по таблице осуществляется с помощью кнопок контекстного фильтра в графах «Наименование» и «Описание».

Описание действий администратора по управлению политиками безопасности приведено в таблице 5.

Таблица 5 – Действия администратора по управлению политиками безопасности

Сценарий	Описание действия
1. Создание политики безопасности	Создание политики безопасности описано в 4.2.7 (стр. 49)
2. Редактирование политики безопасности	В окне настроек администрирования во вкладке «Политики безопасности» выбрать в таблице строку с требуемой политикой и нажать правую кнопку мыши. В появившемся контекстном меню необходимо выбрать строку «Редактировать». Откроется окно «Редактирование политики». Действия по изменению настроек безопасности в окне редактирования аналогичны действиям при создании политики. После завершения редактирования нажать кнопку «Сохранить»
	Откроется информационное окно подтверждения. После нажатия кнопки «ОК» изменения в настройках политики будут сохранены
3. Клонирование политики безопасности	В окне настроек администрирования во вкладке «Политики безопасности» выбрать в таблице строку с требуемой политикой и нажать правую кнопку мыши. В появившемся контекстном меню необходимо выбрать строку «Клонировать». Откроется окно «Клонирование политики». При необходимости, в окне клонирования возможно осуществление редактирования настроек по аналогии с функцией редактирования. Нажать кнопку «Сохранить»
	Откроется информационное окно подтверждения. После нажатия кнопки «ОК» клонированная политика отобразится в таблице
4. Установка использования по умолчанию для политики безопасности	В окне настроек администрирования во вкладке «Политики безопасности» выбрать в таблице строку с требуемой политикой и нажать правую кнопку мыши. В появившемся контекстном меню выбрать строку «Использовать по умолчанию». В строке с выбранной политикой, в графе «По умолчанию» отобразится знак

Сценарий	Описание действия
5. Удаление политики безопасности	В окне настроек администрирования во вкладке «Политики безопасности» выбрать в таблице строку с требуемой политикой и нажать правую кнопку мыши. В появившемся контекстном меню выбрать строку «Удалить». Откроется информационное окно подтверждения удаления. После нажатия кнопки «ОК» выбранная политика будет удалена
6. Информация о политике безопасности	В окне настроек администрирования во вкладке «Политики безопасности» выбрать в таблице строку с требуемой политикой и нажать правую кнопку мыши. В появившемся контекстном меню выбрать строку «Информация». Откроется информационное окно «Просмотр политики» в котором отображены подробные сведения о выбранной политике. Для закрытия информационного окна нажать кнопку «ОК»

6.2.2 Администраторы

Управление учетными записями администраторов осуществляется во вкладке «Администраторы» окна настроек администрирования. Для работы с учетными записями администраторов доступны следующие функции:

1) создание учетной записи администратора – кнопка «Создать администратора». (4.2.2, стр. 41);

2) редактирование учетной записи администратора – кнопка «Редактировать» в контекстном меню;

3) удаление учетной записи администратора – кнопка «Удалить» в контекстного меню;

4) получение подробной информации об учетной записи администратора – кнопка «Информация» в контекстном меню.

Перечень созданных учетных записей администраторов отображается в табличном виде (рисунок 37).

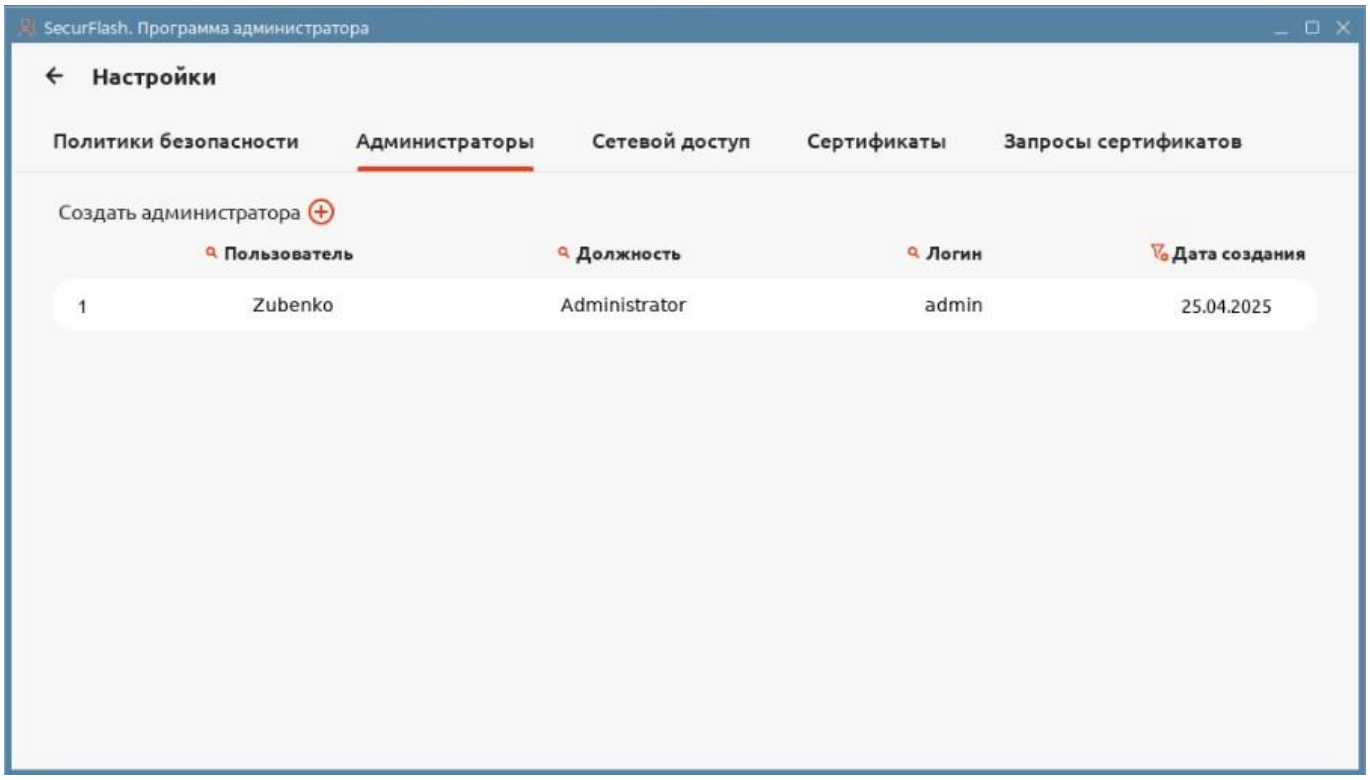


Рисунок 37 – Окно настроек администрирования, вкладка «Администраторы»

Таблица перечня учетных записей администраторов содержит следующие графы:

1) «Администратор» – задается при создании учетной записи администратора, можно редактировать;

2) «Должность» – задается при создании учетной записи администратора, можно редактировать;

3) «Контейнер» – задается при создании учетной записи администратора, можно редактировать;

4) «Дата создания» – значение устанавливается автоматически при создании учетной записи администратора.

Поиск по таблице осуществляется с помощью кнопок контекстного фильтра в графах «Администратор», «Должность» и «Логин», также доступен контекстный фильтр в формате «от и до» (кнопка) в графе «Дата создания».

Описание действий по управлению учетными записями администраторов приведено в таблице 6.

Таблица 6 – Действия администратора по управлению учетными записями администраторов

Сценарий	Описание действия
1. Создание учетной записи администратора	4.2.2, стр. 41
2. Редактирование учетной записи администратора	В окне настроек администрирования во вкладке «Администраторы» выбрать в таблице строку с требуемой учетной записью администратора и нажать правую кнопку мыши. В появившемся контекстном меню выбрать строку «Редактировать». Откроется окно «Редактирование администратора», в котором можно отредактировать: – поле «Администратор»; – поле «Должность». После завершения редактирования нажать кнопку «ОК» Откроется информационное окно подтверждения. После нажатия кнопки «ОК», изменения в настройках учетной записи администратора будут сохранены.
3. Удаление учетной записи администратора	В окне настроек администрирования во вкладке «Администраторы» выбрать в таблице строку с требуемой учетной записью администратора и нажать правую кнопку мыши. В появившемся контекстном меню выбрать строку «Удалить». Откроется информационное окно подтверждения. После нажатия кнопки «ОК» учетная запись администратора будет удалена Удаление учетной записи администратора также отзывает сертификат администратора для защиты от возможного копирования контейнера администратора
4. Информация об учетной записи администратора	В окне настроек администрирования во вкладке «Администраторы» выбрать в таблице строку с требуемой учетной записью администратора и нажать правую кнопку мыши. В появившемся контекстном меню выбрать строку «Информация». Откроется окно с информацией о выбранной учетной записи администратора

6.2.3 Сетевой доступ

Управление настройками сетевого доступа для СВТ администраторов и СВТ пользователей осуществляется во вкладке «Сетевой доступ» окна настроек администрирования. Вкладка содержит редактируемые перечни (рисунок 38):

1) «Разрешенные IP адреса СВТ администраторов» – содержит IP адреса сетевых СВТ, с которых разрешено администрирование КОИ;

2) «Разрешенные IP адреса СВТ пользователей» – содержит IP адреса сетевых СВТ, с которых можно проводить регистрацию из программы пользователя в автоматическом режиме (без дополнительной санкции администратора в программе администратора);

Для работы с разрешенными IP адресами доступны следующие функции:

1) добавление – кнопка «Добавить IP адрес» (4.2.4, стр. 43);
2) редактирование – кнопка «Редактировать» в контекстном меню;
3) удаление – кнопка «Удалить» в контекстном меню.

Если перечень разрешенных IP адресов администратора не содержит ни одного IP адреса, то сервер управления КОИ считает все IP адреса разрешенными.

IP адрес сервера управления КОИ прописывать в перечне разрешенных IP адресов не требуется, так как подключение к нему доступно всегда.

При редактировании перечней доступны функции добавления, редактирования и удаления разрешенных IP адресов.

Каждая таблица перечня IP адресов содержит следующие графы:

1) «IP адрес подсети»;
2) «Маска подсети».

Поиск по таблицам осуществляется с помощью кнопок контекстного поиска .

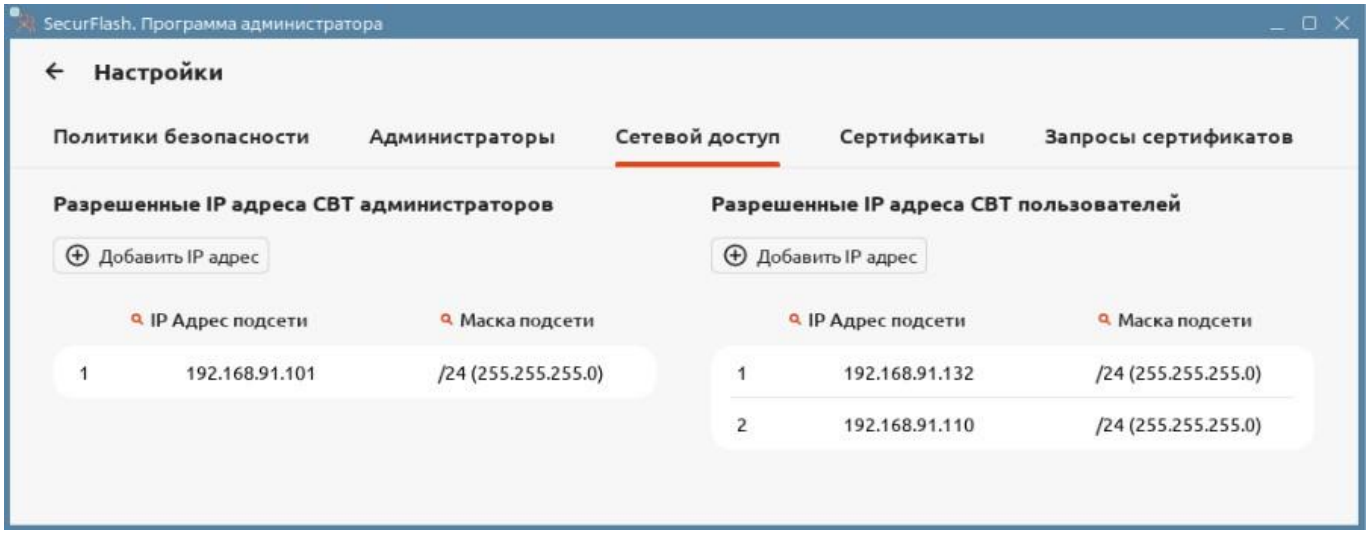


Рисунок 38 – Окно настроек администрирования, вкладка «Сетевой доступ»

Описание действий по настройкам сетевого доступа приведено в таблице 7.

Таблица 7 – Действия администратора по настройкам сетевого доступа

Сценарий	Описание действия
Добавление IP адреса СВТ	4.2.4, стр. 43

Сценарий	Описание действия
Редактирование IP адреса СВТ	Во вкладке «Сетевой доступ» выбрать в одной из таблиц строку с IP адресом и нажать правую кнопку мыши. В появившемся контекстном меню выбрать пункт «Редактировать». Откроется окно редактирования, в котором можно изменить IP адрес и маску подсети. Отредактировать данные IP адреса и нажать кнопку «Добавить»
	Откроется информационное окно. После нажатия кнопки «ОК» измененные данные редактируемого IP адреса СВТ отобразятся в таблице
Удаление IP адреса СВТ	Во вкладке «Сетевой доступ» выбрать в одной из таблиц строку с IP адресом и нажать правую кнопку мыши. В появившемся контекстном меню выбрать строку «Удалить». В открывшемся окне подтверждения нажать «Да». После подтверждения IP адрес будет удален

6.2.4 Сертификаты

Вкладка «Сертификаты» (рисунок 39) содержит сведения о сертификатах текущего сервера управления и нижестоящих серверов управления, в рамках иерархической системы.

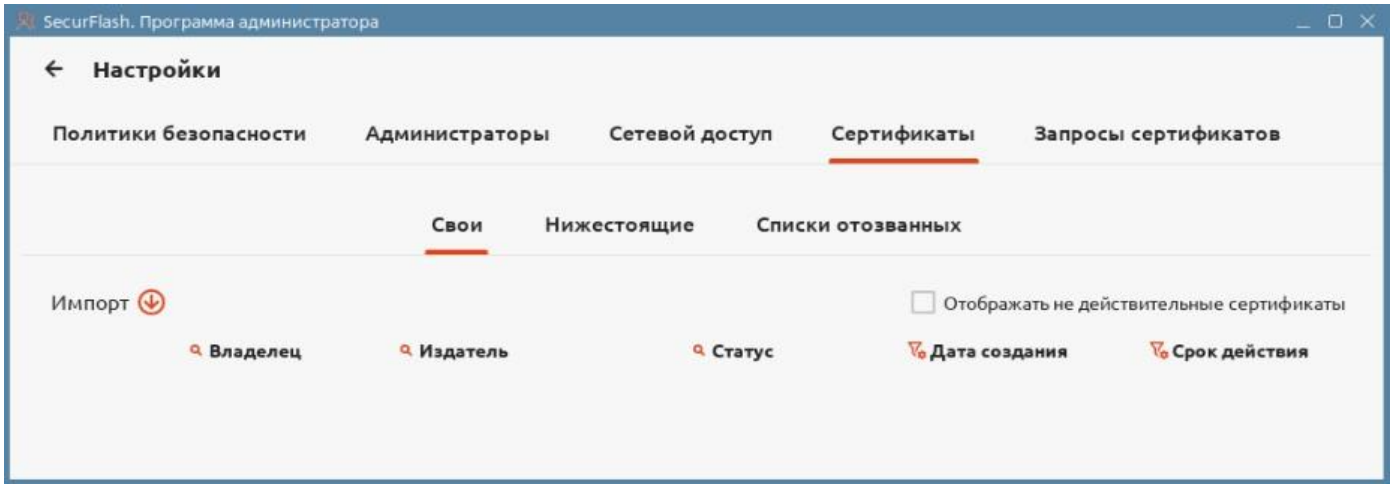


Рисунок 39 – Окно настроек администрирования, вкладка «Сертификаты»

Вкладка содержит три вкладки второго уровня:

1) «Свои» – содержит таблицу перечня сертификатов текущего сервера управления. Вкладка содержит интерфейсы:

– программный переключатель в поле «Отображать недействительные сертификаты» служит отображения всех своих сертификатов, включая недействительные;

– кнопка служит для импорта своих сертификатов;

2) «Нижестоящие» – содержит таблицу перечня сертификатов зарегистрированных нижестоящих серверов управления. Вкладка содержит интерфейсы:

– программный переключатель в поле «Отображать недействительные сертификаты» служит отображения всех нижестоящих сертификатов, включая недействительные;

– кнопка служит для импорта нижестоящих сертификатов.

Поиск по таблице осуществляется с помощью кнопок контекстного фильтра в графах «Владелец», «Издатель» и «Статус», также доступен контекстный фильтр в формате «от и до» (кнопка) в графах «Дата создания» и «Срок действия».

6.2.5 Запросы сертификатов

Вкладка «Запросы сертификатов» (рисунок 40) содержит сведения о входящих и исходящих запросах сертификатов.

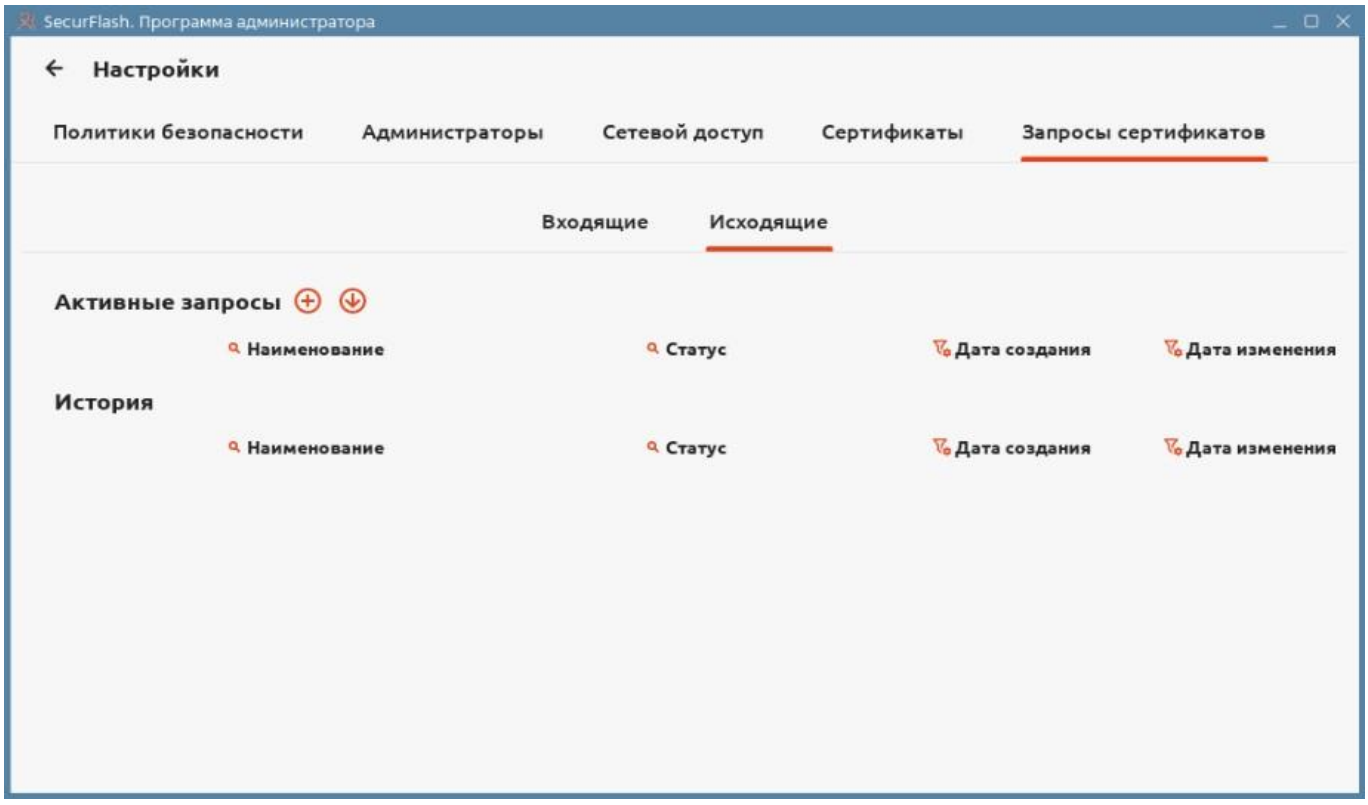


Рисунок 40 – Окно настроек администрирования, вкладка «Запросы сертификатов»

Вкладка содержит две вкладки второго уровня:

1) «Исходящие» – содержит активные исходящие запросы в поле «Активные запросы» и перечень архивных исходящих запросов в перечне «История». Вкладка содержит интерфейсы:

– кнопка служит для создания исходящего запроса;

– кнопка служит для импорта истории исходящих запросов.

2) «Входящие» – содержит активный входящий запрос в поле «Активные запросы» и перечень архивных входящих запросов в перечне «История». Вкладка содержит интерфейсы:

– кнопка служит для импорта входящих запросов;

– программный переключатель служит для выбора всех входящих запросов.

Таблицы перечней запросов содержат следующие графы:

– «Наименование»;

– «Статус»;

– «Дата создания»;

– «Дата изменения».

Поиск по таблицам перечней осуществляется с помощью кнопок контекстного фильтра в графах «Наименование» и «Статус», также доступен контекстный фильтр в формате «от и до» (кнопка) в графах «Дата создания» и «Дата изменения».

6.3 Окно администрирования (главное окно программы)

Окно администрирования (главное окно программы) открывается после авторизации администратора (4.2.3, стр. 43).

Окно администрирования (главное окно программы) включает следующие вкладки (рисунок 41):

– «Пользователи» – управление учетными записями пользователей (6.3.1, стр. 76);

– «Носители» – управление носителями (6.3.2, стр. 78);

– «СВТ» – управление СВТ (6.3.3, стр. 80);

– «Разрешения» – управление разрешениями (6.3.4, стр. 82);

– «Аудит» – аудит (6.3.5, стр. 84).

6.3.1 Пользователи

Управление учетными записями пользователей осуществляется во вкладке «Пользователи». Перечень созданных учетных записей пользователей отображается в табличном виде (рисунок 41).

Для работы с учетными записями пользователей доступны следующие функции:

1) создание учетной записи пользователя – кнопка «Создать пользователя». (4.2.8, стр. 50);

2) импорт списка учетных записей пользователей из csv-файла – кнопка «Импорт»;

3) редактирование учетной записи пользователя – пункт «Редактировать» в контекстном меню;

4) удаление учетной записи пользователя – пункт «Удалить» в контекстного меню;

5) получение подробной информации об учетной записи пользователя – пункт «Информация» в контекстном меню.

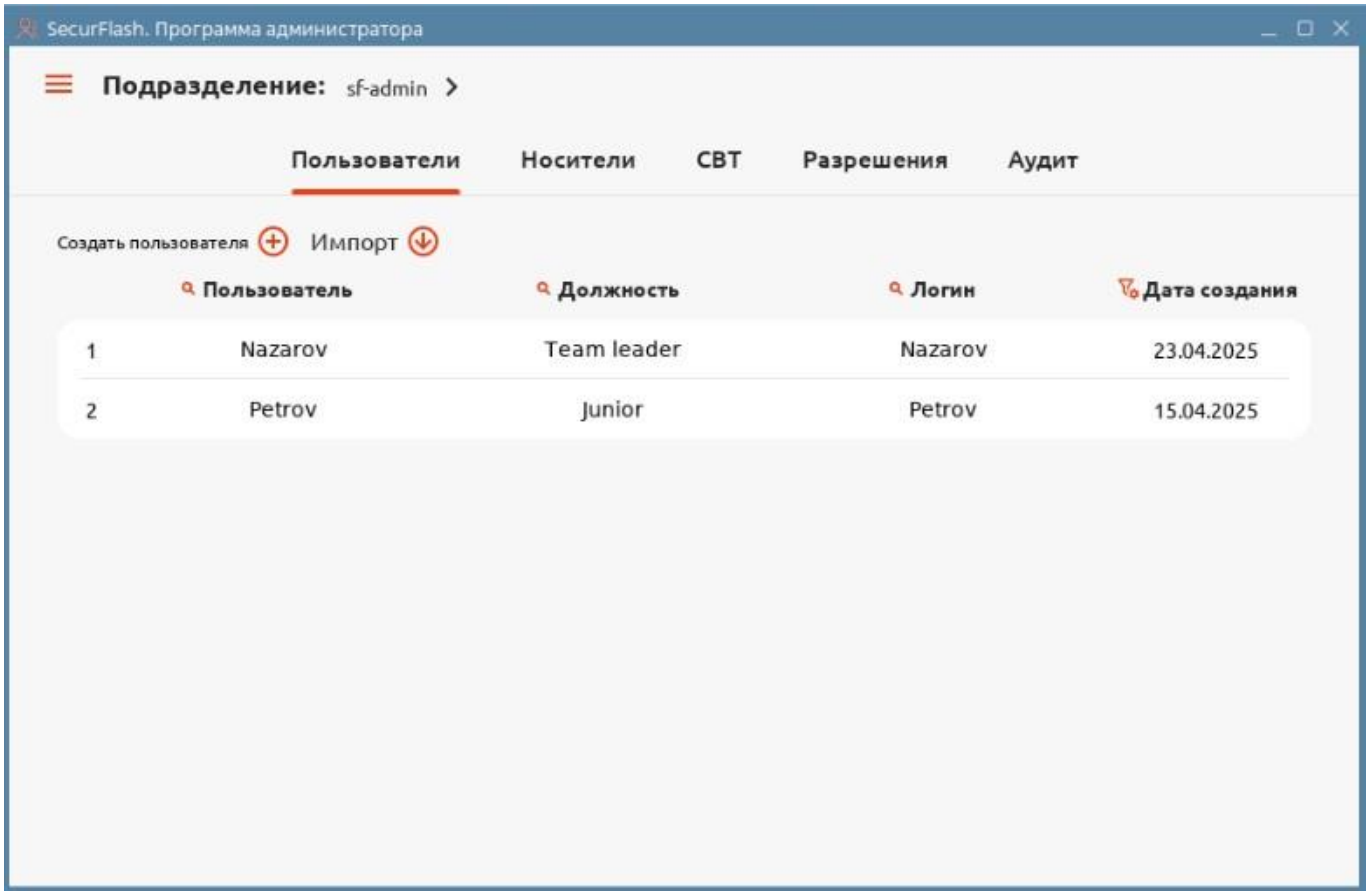


Рисунок 41 – Окно администрирования, вкладка «Пользователи»

Таблица перечня содержит следующие графы:

– «Пользователь» – задается при создании учетной записи пользователя, можно редактировать;

– «Должность» – задается при создании учетной записи пользователя, можно редактировать;

– «Логин» – задается при создании учетной записи пользователя, можно редактировать;

– «Дата создания» – задается при создании учетной записи пользователя.

Поиск по таблице осуществляется с помощью кнопок контекстного фильтра в графах «Пользователь», Должность и «Логин», также доступен контекстный фильтр в формате «от и до» (кнопка) в графе «Дата создания».

Описание действий по управлению учетными записями пользователей приведено в таблице 8.

Таблица 8 – Действия администратора по управлению учетными записями пользователей

Сценарий	Описание действия
1. Создание учетной записи пользователя	4.2.8 (стр. 50)
2. Редактирование учетной записи пользователя	Во вкладке «Пользователи» выбрать в таблице строку с требуемой учетной записью пользователя и нажать правую кнопку мыши. В появившемся контекстном меню выбрать строку «Редактировать». Откроется окно редактирования учетной записи, в котором можно отредактировать поля: 1) Политику безопасности (при условии, что создано несколько политик). 2) «ФИО»; 3) «Должность»; 4) «Логин». Ввести базовый учетной записи пользователя для подтверждения редактирования. Нажать кнопку «Ок» Откроется информационное окно подтверждения сохранения изменений. После нажатия кнопки «Ок» учетная запись пользователя будет отредактирована
3. Удаление учетной записи пользователя	Во вкладке «Пользователи» выбрать в таблице строку с требуемой учетной записью пользователя и нажать правую кнопку мыши. В появившемся контекстном меню выбрать строку «Удалить». Откроется окно с подтверждением запроса на удаление. После нажатия кнопки «Да» учетная запись пользователя будет удалена
4. Информация об учетной записи пользователя	Во вкладке «Пользователи» выбрать в таблице строку с требуемой учетной записью пользователя и нажать правую кнопку мыши. В появившемся контекстном меню выбрать строку «Информация». Откроется окно с информацией о выбранной учетной записи пользователя

6.3.2 Носители

Управление носителями осуществляется во вкладке «Носители» (рисунок 42).

Для работы с носителями доступны следующие функции:

1) инициализация носителя – кнопка «Инициализация» (5.2.1, стр. 57);
2) сброс носителя – кнопка «Сброс» (5.2.4, стр. 61);

3) разблокировка носителя – пункт «Разблокировка носителя» в контекстном меню (5.2.3, стр. 61);

4) импорт перечня носителей – кнопка «Импорт»;

5) экспорт перечня носителей – кнопка «Экспорт»;

6) удаление носителя – пункт «Удалить» в контекстного меню;

7) получение подробной информации о носителе – пункт «Информация» в контекстном меню.

Инициализированный носитель передается пользователю вместе с логином и базовым паролем учетной записи.

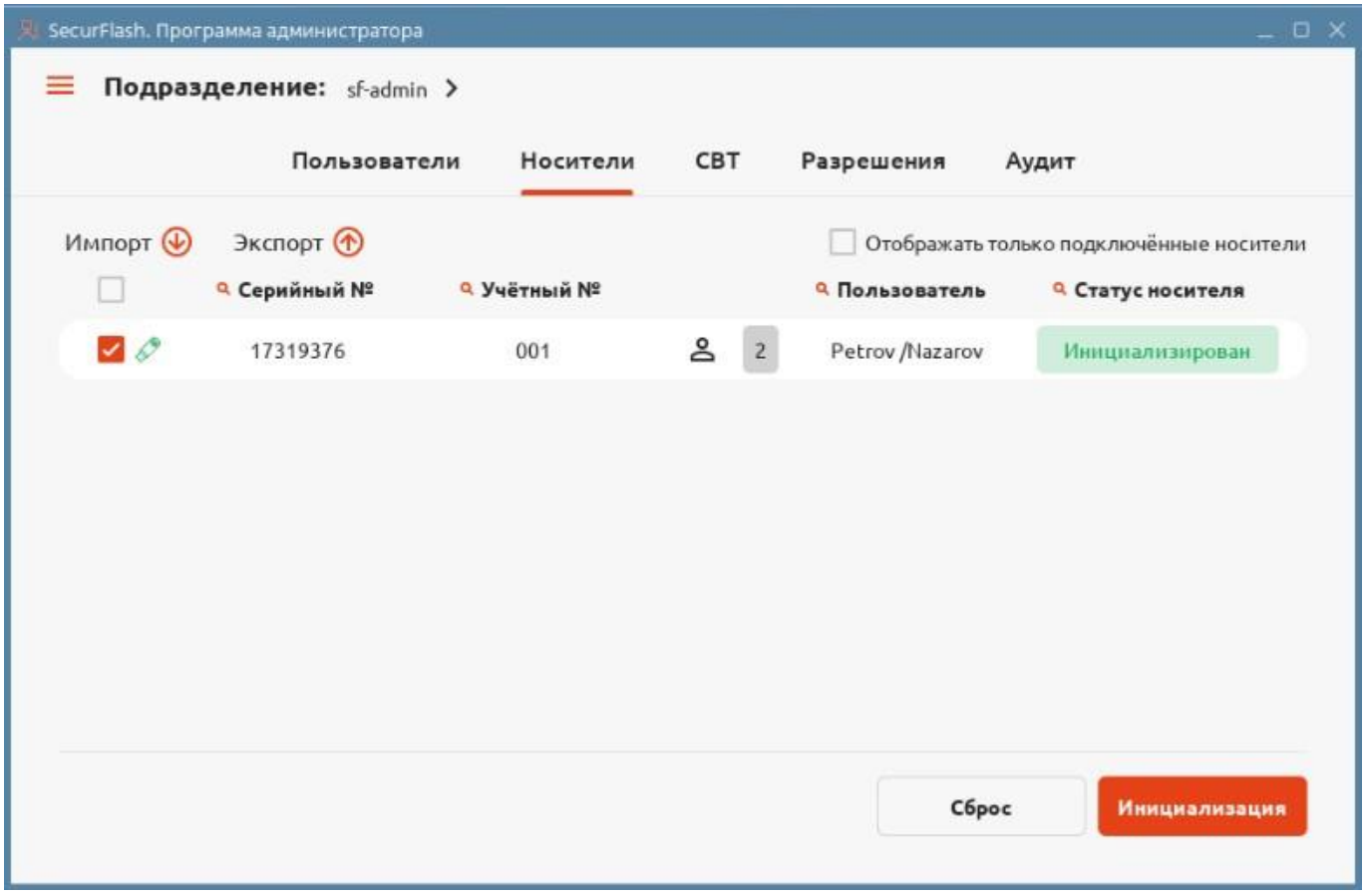


Рисунок 42 – Окно администрирования пользователей и аудита, вкладка «Носители»

Перечень носителей отображается в табличном виде.

Таблица перечня содержит следующие графы:

1) «Серийный №» – задается при производстве носителя, автоматически копируется в базу данных при инициализации;

2) «Учетный №» – задается при инициализации;

3) «Пользователь» – пользователи имеющие права доступа к носителю;

4) «Статус носителя» – «Инициализирован», «Не инициализирован», «Заблокирован».

Знак  с цифрой – отображает количество пользователей для данного носителя.

Программный указатель  служит для выделения подключенного носителя (носителей) при выполнении операций инициализации или сброса.

Подключенные носители отображаются в таблице зеленой пиктограммой  , не подключенные – серой пиктограммой  .

В верхней части окна расположен программный указатель  для отображения в таблице только подключенных носителей.

Поиск по таблице осуществляется с помощью кнопки контекстного фильтра  в графах «Серийный №», «Учетный №», «Пользователь» и «Статус носителя».

Описание действий по управлению учетными носителями приведено в таблице 9.

Таблица 9 – Действия администратора по управлению учетными носителями

Сценарий	Описание действия
Инициализация носителя	5.2.1 (стр. 57)
Сброс носителя	5.2.4 (стр. 61)
Разблокировка носителя	5.2.3 (стр. 61)
Удаление носителя	Убедиться, что носитель извлечен и запись о нем в таблице вкладки «Носители» отмечена серой пиктограммой  . Выбрать удаляемый носитель в таблице, нажать правую кнопку мыши и в контекстном меню выбрать строку «Удалить». В открывшемся окне запроса на подтверждение нажать кнопку «Да». Носитель будет удален из таблицы
Информация о носителе	В таблице вкладки «Носители» выбрать носитель. Нажать правую кнопку мыши и в контекстном меню выбрать строку «Информация». Откроется окно с информацией о выбранном носителе

6.3.3 СВТ

Управление СВТ пользователей осуществляется во вкладке «СВТ». Для управления СВТ доступны функции:

1) регистрация СВТ – кнопка «Зарегистрировать» (4.3.2, стр. 53; 4.3.2.2 стр. 54);
2) отмена регистрации СВТ – кнопка «Отменить регистрацию» (5.3.1, стр. 61);
3) удаление СВТ пункт «Удалить» в контекстном меню.

Перечень СВТ отображается в табличном виде (рисунок 43).

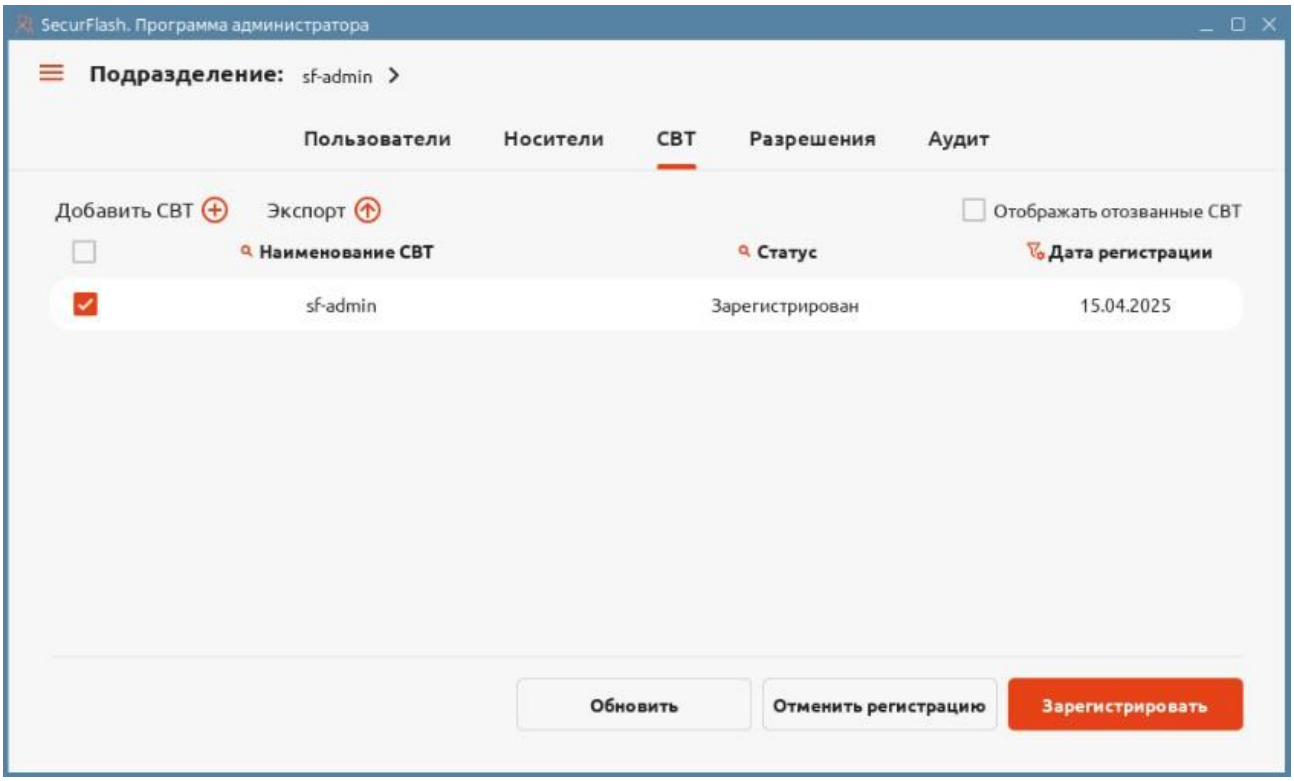


Рисунок 43 – Окно администрирования, вкладка «СВТ»

Таблица содержит следующие графы:

1) «Наименование СВТ» – значение поля считывается из файла запроса СВТ, можно редактировать;

2) «Статус» – может иметь значения «Не зарегистрирован», «Зарегистрирован» или «Отозван». СВТ отображаются как незарегистрированные, если для них получен запрос на регистрацию, но регистрация еще не одобрена. Сетевые и автономные СВТ, прошедшие процедуру регистрации в КОИ, отображаются как зарегистрированные. СВТ с отмененной регистрацией или с отклоненным запросом отображаются со статусом «Отозван»;

3) «Дата регистрации» – поле заполняется автоматически при регистрации СВТ.

Программный указатель слева ☑ служит для выделения одного или нескольких СВТ.

Программный указатель ☑ Отображать отозванные СВТ служит для отображения СВТ со всеми статусами, включая отозванные.

Поиск по таблице осуществляется с помощью кнопки контекстного фильтра в графах «Наименование СВТ» и «Статус», в графе «Дата создания» доступен контекстный фильтр в формате «от и до» (кнопка).

Описание действий по управлению СВТ приведено в таблице 10.

Таблица 10 – Действия администратора по управлению СВТ

Сценарий	Описание действия
Регистрация СВТ	4.3.2, стр. 53 4.3.2.2, стр. 54
Отмена регистрации СВТ	5.3.1, стр. 61
Удаление СВТ	В таблице вкладки «СВТ» выбрать СВТ или при помощи программного указателя выбрать несколько СВТ, нажать правую кнопку мыши и в выпадающем контекстном меню выбрать пункт «Удалить». В открывшемся окне подтверждения нажать кнопку «Да». Выбранный СВТ будет удален из таблицы, его регистрация будет отозвана
Информация об СВТ	В таблице вкладки «СВТ» выбрать СВТ, нажать правую кнопку мыши и в выпадающем контекстном меню выбрать пункт «Информация». В открывшемся окне «Просмотр СВТ» отобразится следующая информация об СВТ: – наименование СВТ; – статус; – дата регистрации

6.3.4 Разрешения

Администратор имеет возможность изменить перечень СВТ, на которых разрешена работа с носителем.

Установленные разрешения хранятся в базе данных сервера управления и на самом носителе.

Управление разрешениями осуществляется во вкладке «Разрешения», которая содержит поля «Список носителей», «Список» пользователей» и «Список СВТ» (рисунок 44).

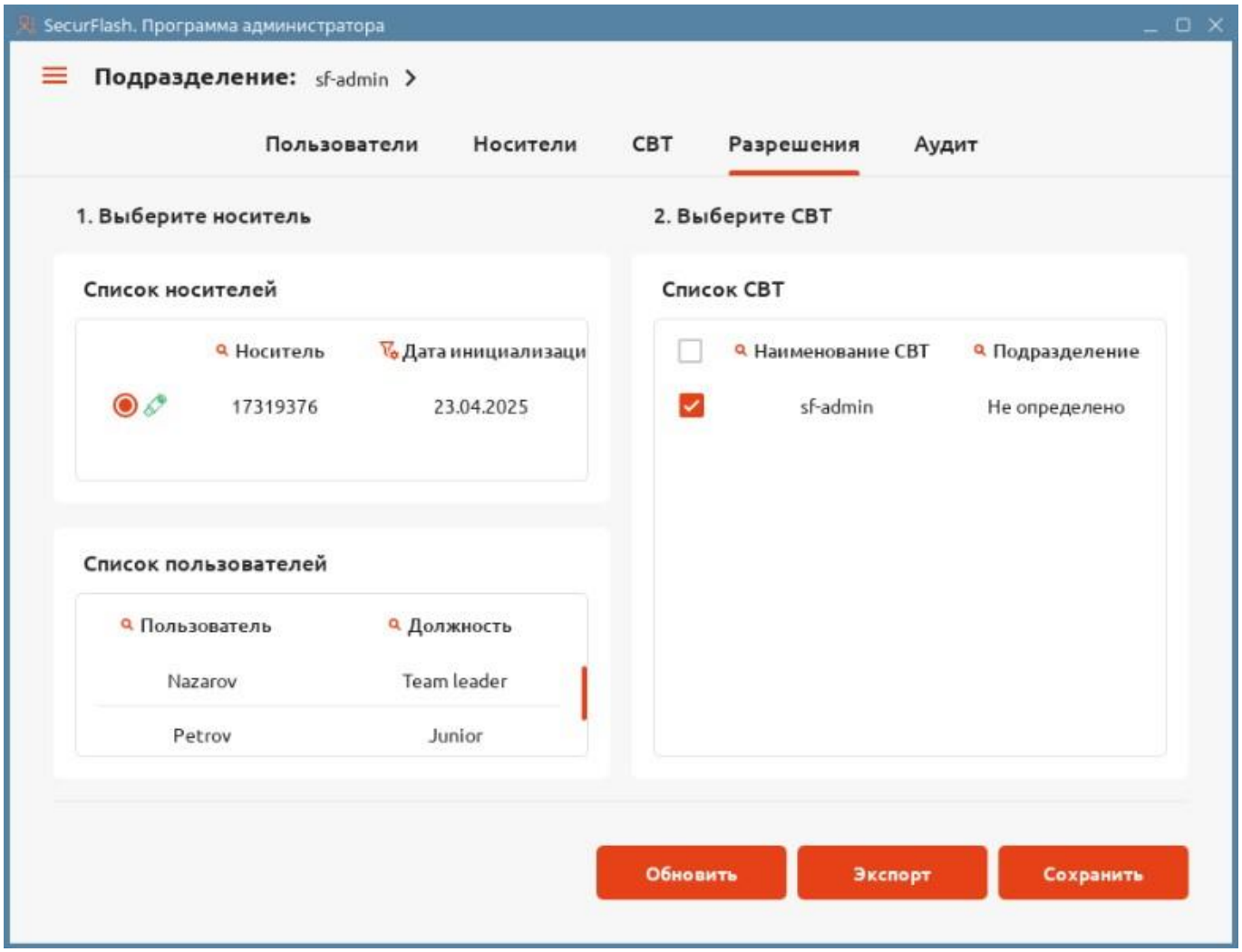


Рисунок 44 – Окно администрирования, вкладка «Разрешения»

Поле «Список носителей» содержит таблицу перечня инициализированных носителей со следующими графами:

1) «Носитель» – значение соответствует серийному номеру носителя;
2) «Дата инициализации» – заполняется автоматически при инициализации носителя.

Программный переключатель  слева служит для выделения носителя, для которого необходимо изменить разрешения.

Поле «Список пользователей» содержит таблицу перечня пользователей, имеющих права доступа к выбранному носителю, со следующими графами:

1) «Пользователь» – ФИО пользователя, прописанные в учетной записи, можно изменять при редактировании учетной записи;

2) «Должность» – должность пользователя, прописанная в учетной записи, можно изменять при редактировании учетной записи.

Поле «Список СВТ» содержит таблицу перечня СВТ, на которых разрешена работа с выбранным носителем, со следующими графами:

1) «Наименование СВТ» – соответствует значению поля «Наименование СВТ» во вкладке «СВТ», можно редактировать;

2) «Подразделение».

Программный указатель  слева служит для выбора одного или нескольких СВТ.

Кнопка «Обновить» служит для обновления списков разрешений.

Кнопка «Экспорт» служит для экспорта файла разрешений на автономные СВТ пользователей и сетевые СВТ пользователей в ручном режиме. Файл разрешений используется для удаленного обновления разрешений при подключении носителей к программе пользователя на СВТ пользователя.

Кнопка «Сохранить» служит для сохранения измененных разрешений на носитель.

Поиск по таблицам осуществляется с помощью кнопки контекстного фильтра  в графах «Носитель», «Пользователь», «Должность», «Наименование СВТ» и «Подразделение», также доступен контекстный фильтр в формате «от и до» (кнопка ) в графе «Дата инициализации».

При выборе записей полей «Список носителей» и «Список пользователей» доступны пункты контекстного меню «Удалить» и «Информация».

При выборе записей поля «Список СВТ» доступны пункты контекстного меню «Редактировать», «Удалить» и «Информация».

6.3.5 Аудит

При функционировании программного средства все события аудита регистрируются в базе данных сервера управления, локальных базах данных автономных СВТ пользователей и журналах носителей.

Просмотр событий аудита доступен администратору во вкладке «Аудит» (рисунок 45), в которой имеются следующие функции:

1) просмотр событий в табличном виде (5.4.1, стр. 63);
2) просмотр событий с использованием фильтров;
3) импорт событий безопасности с носителя – кнопка «События носителя» (5.4.2, стр. 64);

4) импорт, экспорт (с возможностью удаления) – кнопки «Импорт», «Экспорт» (5.4.3, стр. 65).

Таблица аудита содержит следующие графы:

1) порядковый номер события в таблице журнала аудита;
2) «Дата и время» – дата и время регистрации события;
3) «НСД» – событие попытки несанкционированного доступа;
4) «Событие» – краткое описание события;
5) «Источник» –компонент программного средства, на котором сгенерировано событие (ПА, ПП или СУ);
6) «Результат» – результат события;
7) «Наименование СВТ» – наименование СВТ, на котором было сгенерировано событие;
8) «ФИО» – ФИО администратора или пользователя;
9) «Носитель» – серийный номер носителя, на котором было сгенерировано событие.

Поиск по таблице осуществляется с помощью кнопки контекстного фильтра в графах «Событие», «Источник», «Результат», «Наименование СВТ», «ФИО» и «Носитель», также доступен контекстный фильтр в формате «от и до» (кнопка) в графе «Дата время».

Программный указатель в графе «НСД» служит для отображения только событий несанкционированного доступа.

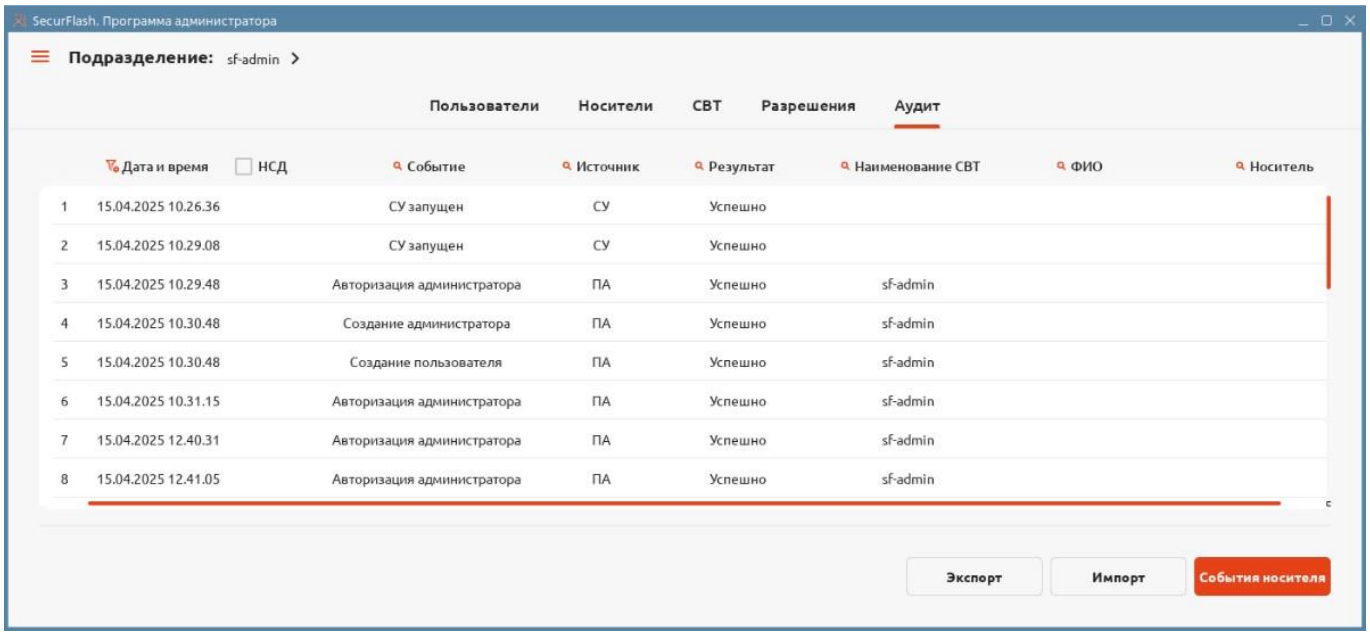


Рисунок 45 – Окно администрирования, вкладка «Разрешения»

7 ОБРАЩЕНИЕ В СЛУЖБУ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

Время работы службы технической поддержки изготовителя с 09:00 до 18:00 по московскому времени (GMT+3), кроме выходных и праздничных дней.

Запросы на техническую поддержку оформляются в виде электронного документа через Web-сайт изготовителя (производителя) или по электронной почте.

Контактные данные службы технической поддержки изготовителя (производителя):

– URL-адрес для обращений: https://www.aladdin-rd.ru/support/tickets/create;
– телефон: +7 (499) 702-39-68;
– адрес электронной почты: support.sf@aladdin.ru.

Техническая поддержка программного средства «Средство защиты информации на съемных машинных носителях SecurFlash» оказывается в течение гарантийного срока.

Для всех случаев обращения в службу технической поддержки должен быть указан идентификатор сертифицированного средства (номер программного средства предприятия), при этом обращение обязательно регистрируется в службе технической поддержки.

Техническая поддержка программного средства в течение гарантийного срока включает:

– возможность консультаций по настройке, а также особенностям эксплуатации и применения программного средства;
– возможность моделирования неисправного (неработоспособного) состояния программы на стенде изготовителя (производителя) и помощь в решении возникшей проблемы/затруднения при работе с программой;
– исправление программных дефектов, обнаруженных в программе владельцем (пользователем) программного средства или производителем (изготовителем) и не относящихся к недостаткам безопасности;
– обновление программного средства для устранения программных дефектов, не относящихся к недостаткам безопасности;
– совершенствование программного средства, не связанное с функциями безопасности. Изменения вносятся по решению изготовителя (производителя) в рамках повышение качества функционирования программы, её совершенствования и/или расширения функциональных возможностей.

ПРИЛОЖЕНИЕ 1

Сообщения об ошибках

Таблица 11 – Сообщения об ошибках для сценария 4.2.3 «Авторизация администратора»

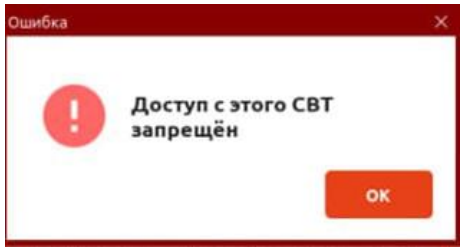
Сценарий	Сообщение об ошибке	Необходимые действия
Авторизация администратора	Укажите контейнер	Указать путь к контейнеру администратора
	Неверный пароль	Ввести корректный пароль для контейнера учетной записи администратора
		Создать новую учетную запись администратора, используя ВПУЗ, взамен учетной записи с истекшим сроком действия. Если истек срок действия ВПУЗ, то пересоздать ВПУЗ
		Добавить IP адрес СВТ администратора в перечень разрешенных

Таблица 12 – Сообщения об ошибках для сценариев 4.2.7 «Создание политики безопасности» и 6.2.1 «Политики безопасности»

Сценарий	Сообщение об ошибке	Необходимые действия
Создание политики безопасности	Наименование отсутствует	Ввести наименование политики безопасности
	Наименование уже используется. Выберите другое.	Ввести другое наименование политики безопасности
Редактирование политики безопасности	Наименование отсутствует	Ввести наименование политики безопасности

Таблица 13 – Сообщения об ошибках для сценариев 4.2.2 «Создание учетной записи администратора» и 6.2.2 «Администраторы»

Сценарий	Сообщение об ошибке	Необходимые действия
Создание учетной записи администратора	ФИО отсутствует	Заполнить поле «Администратор»
	Должность отсутствует	Заполнить поле «Должность»
	Название отсутствует	Заполнить поле «Название контейнера»
	Пароль отсутствует	Ввести пароль, соответствующий политике безопасности
	Пароли не совпадают	Ввести корректное подтверждение пароля
	Сообщения о несоответствии пароля используемой политике безопасности	Ввести пароль, соответствующий политике безопасности
Редактирование учетной записи администратора	ФИО отсутствует	Заполнить поле «Администратор»

Сценарий	Сообщение об ошибке	Необходимые действия
	Должность отсутствует	Заполнить поле «Должность»
	Название отсутствует	Заполнить поле «Название контейнера»
	Пароль отсутствует	Ввести корректный старый пароль
	Введен неверный пароль	Ввести корректный старый пароль

Таблица 14 – Сообщения об ошибках для сценариев 4.2.8 «Создание учетной записи пользователя», 6.3.1 «Пользователи»

Сценарий	Сообщение об ошибке	Необходимые действия
1. Создание учетной записи пользователя	ФИО отсутствует	Ввести ФИО пользователя
	Должность отсутствует	Ввести должность пользователя
	Логин отсутствует	Ввести логин пользователя
	Пароль отсутствует	Ввести пароль пользователя
	Пароли не совпадают	Ввести корректное подтверждение пароля
	Сообщения о несоответствии пароля используемой политике безопасности	Ввести пароль, соответствующий политике безопасности
2. Редактирование учетной записи пользователя	ФИО отсутствует	Ввести ФИО пользователя

Сценарий	Сообщение об ошибке	Необходимые действия
	Должность отсутствует	Ввести должность пользователя
	Логин отсутствует	Ввести логин пользователя
	Сообщения о несоответствии пароля используемой политике безопасности	Ввести пароль, соответствующий политике безопасности

Таблица 15 – Сообщения об ошибках для сценариев 5.2 «Сценарии администрирования носителей», 6.3.2 «Носители» и 6.3.4 «Разрешения»

Сценарий	Сообщение об ошибке	Необходимые действия
1. Удаление носителя	Извлеките носитель и повторите операцию	Извлечь носитель и повторить операцию удаления
2. Редактирование разрешений носителя на доступ к СВТ		Выбрать хотя бы одно СВТ в поле «Список СВТ» вкладки «Разрешения»

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					