SOLAR

SafeConnect

Версия 1.16.0

Руководство администратора SafeConnect

Москва, 2026

Содержание

1. Общие сведения 4
1.1. Возможности SafeConnect 4
1.2. Логика работы SafeConnect 5
2. Системные требования 8
3. Работа с программой 9
3.1. Запуск программного комплекса SafeConnect и первоначальная настройка 9
3.2. Вход в программу 11
3.3. Выбор языка интерфейса 14
3.4. Главное меню 15
3.5. Раздел «Главная» 16
3.6. Раздел «Сессии» 17
3.6.1. Общие сведения 17
3.6.2. Статистика и поиск 19
3.7. Раздел «Ресурсы» 27
3.7.1. Добавление ресурса 28
3.7.2. Редактирование ресурса 38
3.7.3. Удаление ресурса 38
3.8. Раздел «Учетные записи» 39
3.8.1. Добавление учетной записи 39
3.8.2. Редактирование учетной записи 42
3.8.3. Удаление учетной записи 42
3.9. Раздел «Политики» 42
3.9.1. Создание политики 43
3.9.2. Редактирование политики 47
3.9.3. Удаление политики 47
3.10. Раздел «Пользователи» 47
3.10.1. Добавление пользователя 48
3.10.2. Редактирование данных пользователя 52
3.10.3. Удаление пользователя 52
3.11. Раздел «Группы» 53
3.11.1. Создание группы 54
3.11.2. Добавление пользователей в группу 55
3.11.3. Редактирование группы 55
3.11.4. Удаление группы 55
3.12. Раздел «Роли» 56
3.12.1. Добавление роли 57
3.12.2. Редактирование роли 58
3.12.3. Удаление роли 58
3.13. Раздел «Настройки» 58
3.13.1. Лицензия 59
3.13.2. Безопасность 60
3.13.3. Интеграция с внешними системами 65
3.13.4. Настройки SMTP 68
3.13.5. Пользовательское соглашение 69
3.13.6. Репликация 71
3.13.7. Серверы LDAP 73
3.13.8. Серверы RADIUS 76
3.13.9. Сетевые настройки 77
3.13.10. Брендирование 81

3.13.11. Резервное копирование и восстановление 89
3.13.12. Система 92
3.14. Раздел «Задания» 102
3.14.1. Добавление задания 103
3.14.2. Просмотр задания 108
3.14.3. Поиск задания 117
3.14.4. Редактирование задания 118
3.14.5. Завершение задания 118
3.14.6. Управление доменными пользователями в заданиях 118
3.15. Интеграция с SafeInspect 120
3.15.1. Сетевые взаимодействия SafeInspect и SafeConnect 120
3.15.2. Настройка интеграции с SafeInspect 121
3.16. Интеграция с КриптоПро NGate 126
3.17. Пример настройки локальным пользователям доступа к удаленным ресурсам 130
4. Защита от атак подбора учетных данных 135
5. Выход из программы 136
6. Устранение неполадок 137

1. Общие сведения

Программный комплекс SafeConnect (далее – SafeConnect, Портал) предоставляет пользователю простой и безопасный способ доступа к удаленному ресурсу, если в этом возникает необходимость. Этот способ заключается в использовании веб–браузера с выходом на Портал, далее появляется возможность подключения к различным приложениям прямо из окна браузера, без использования дополнительного программного обеспечения.

SafeConnect позволяет исключить необходимость прямой публикации в сети интернет таких сервисов удаленного администрирования, как **RDP**, **SSH**, **Telnet** и др. для обеспечения доступа прямо к ресурсам **внутри сети компании**. При использовании ПК SafeConnect появляется возможность обеспечения централизованного, безопасного доступа к ресурсам компании, с возможностью применения функций **SSO** к разным ресурсам. При этом пользователь может подключаться к ресурсам с использованием аутентификационных данных, отличных от тех, которые он вводил на портале для авторизации, и при этом они ему не доступны. Доступ для пользователя обеспечивается только к тем ресурсам, к которым ему явным образом был разрешен доступ, другие ресурсы компании при этом недоступны. Они просто не публикуются у него на странице.

Портал может использоваться самостоятельно, а также может быть использован совместно с системой контроля привилегированных пользователей SafeInspect для обеспечения возможности записи действий удаленных пользователей и других функций по управлению доступом к критичным ресурсам.

1.1. Возможности SafeConnect

SafeConnect выполняет следующие задачи:

- **Создание Портала доступа** и публикации на нем ресурсов компании для удаленных пользователей. Каждому пользователю будут доступны только те ресурсы, которые ему явно были назначены;
- **Обеспечение строгой аутентификации пользователей**, а также разграничение доступа к публикуемым ресурсам;
- **Обеспечение возможности категорирования ресурсов** и пользователей по разным уровням доступа (критические ресурсы, ресурсы с персональными данными (Федеральный закон от 27.07.2006 г. № 152–ФЗ "О персональных данных" (далее – ФЗ–152)), **General Data Protection Regulation** (далее – **GDPR**)). А также **обеспечение строгого мандатного доступа к разным категориям ресурсов** в соответствии с допуском пользователей к таким категориям ресурсов;
- **Обеспечение функций SSO** (пользователь однократно авторизуется на Портале, затем подключается к ресурсам без введения пароля);
- **Обеспечение подмены пользователей при доступе к ресурсам** (при подключении через Портал, доступ к реальным ресурсам может осуществляться под другими учетными данными с автоматической их подменой);
- **Обеспечение одноразового доступа к ресурсам**, **доступа по расписанию**, с возможностью установки количества доступов и других параметров соединений;

- **Обеспечение возможности постановки задач пользователям**, что конкретно в каждом из их доступов они должны сделать (**внутренняя тикетная система**);
- **Возможность создания Портала самообслуживания**. Возможность создания групп пользователей с разными правами, где отдельные пользователи могут иметь права на создание тикетов и доступов к ресурсам, управляя, таким образом, доступом для своей группы пользователей и ресурсов;
- **Интеграция с ПК SafeInspect** для обеспечения эффективного контроля действий пользователей.

1.2. Логика работы SafeConnect

SafeConnect выполнен в виде шлюза, где обеспечивается возможность публикации приложений, обеспечивается строгая аутентификация и авторизация пользователей, с возможностью контроля подключений пользователей к ресурсам.

Для эффективного управления доступом и изменениями в SafeConnect существует **специализированная тикетная система**. Таким образом, каждый доступ обязательно получает свой тикет, и появляется возможность обеспечения диалога с администраторами ресурсов и получения необходимых заданий для пользователей с тем, чтобы они могли уточнить, что именно они могут делать в рамках предоставляемого доступа или какое задание необходимо выполнить в рамках этого доступа.

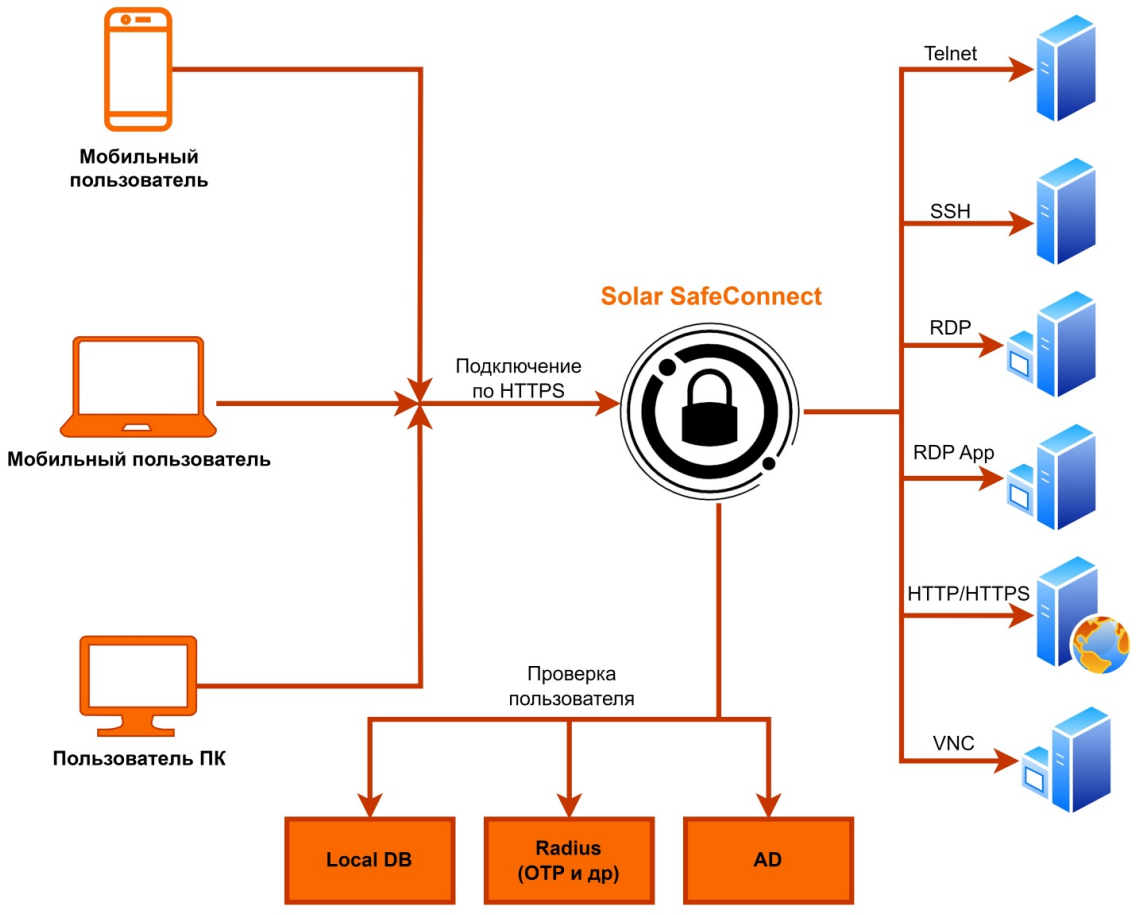


Рис. 1.1. Общая схема

Все общение между администраторами Портала и пользователями может осуществляться через **тикетную систему** SafeConnect, исключая необходимость звонить администраторам и просить сделать какой-либо доступ и другие действия. Что сильно облегчает работу компании с удаленными пользователями в целом.

Описание правил доступа состоит из нескольких компонентов: собственно **ресурсы** и **аккаунты** для доступа к этим ресурсам, а также **задание** и **политика** доступа.



Рис. 1.2. Описание правил доступа

Схематично это отражено на рисунке (Рис.1.2).

Каждый пользователь может создать **запрос на доступ к ресурсу** как для себя, так и для своей группы пользователей, или для другого пользователя. Администраторы, предоставляя доступ к ресурсу, также создают задание (тикет) для пользователя (группы пользователей), в котором кратко описывают для чего этот доступ. Далее к этому заданию добавляются необходимые **ресурсы**, **аккаунты**, с помощью которых пользователи будут осуществлять доступ, **политики**, которые регламентируют когда и каким образом этот доступ должен осуществляться.

Далее при необходимости задание утверждается (согласовывается) другими администраторами (пользователями с такими правами), доступ автоматически создается и появляется на странице Портала пользователя.

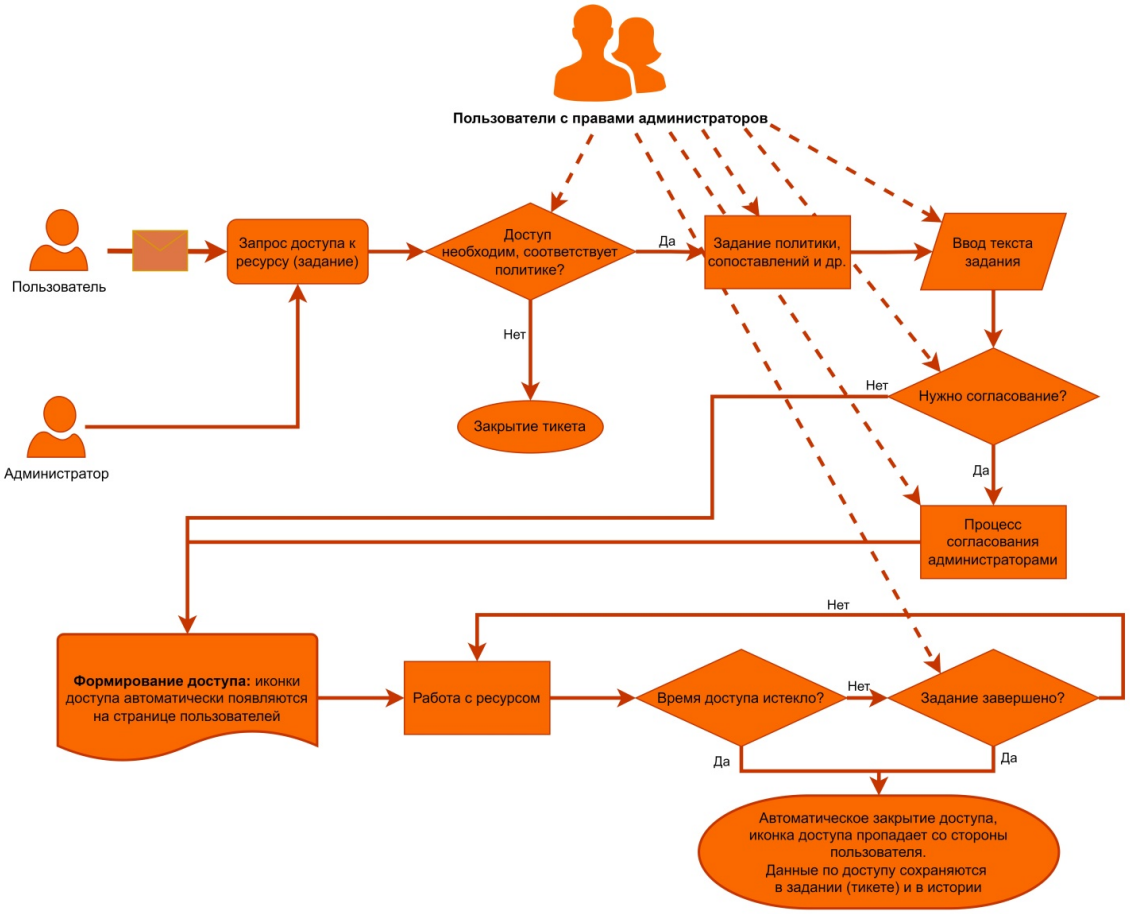


Рис. 1.3. Порядок работы по обеспечению доступа

Схематично порядок работы SafeConnect показан на рисунке Рис.1.3. При указанном подходе, каждый доступ в обязательном порядке описывается тем, кто этот доступ запрашивает или предоставляет. В любой момент времени (особенно при групповом доступе), администраторы знают каким образом и в какое время каждый пользователь получал доступ к ресурсам. При этом пользователь может в рамках работ согласовать любые параметры соединения, запросить дополнительные доступы себе или группе пользователей. В случае группового доступа у администраторов всегда есть точная информация: кто, когда и какую работу выполнял по указанному заданию.

2. Системные требования

Программный комплекс SafeConnect может быть установлен как на **аппаратное устройство** (компьютер), так и на **виртуальное устройство** (виртуальную машину). В этом разделе приведены системные требования для установки на виртуальное устройство.

Для установки SafeConnect в качестве виртуальной среды рекомендуется использовать:

- **Proxmox Virtual Environment** (версии 8.2.3, 8.2.7);
- **VMware ESXi** (версия 7.0);
- **VMware Workstation** (версия 17).

Табл. 2.1. Минимальные системные требования к виртуальной машине VMware

Спецификация	**Значение**
Память	2 GB или более
Размер диска	20 GB или более
Тип гостевой операционной системы, установленной на виртуальную машину	Тип: Linux Версия: Astra Linux Special Edition 1.7 (64-bit) с последними обновлениями безопасности
Сетевое оборудование	Минимально 1 сетевой адаптер

3. Работа с программой

3.1. Запуск программного комплекса SafeConnect и первоначальная настройка

Для запуска программного комплекса SafeConnect в веб–браузере наберите **IP–адрес**, который был введен во время инсталляции. После этого появится диалоговое окно **Создание суперадминистратора** с приглашением ввести **логин** и **пароль** суперадминистратора (Рис.3.1) .

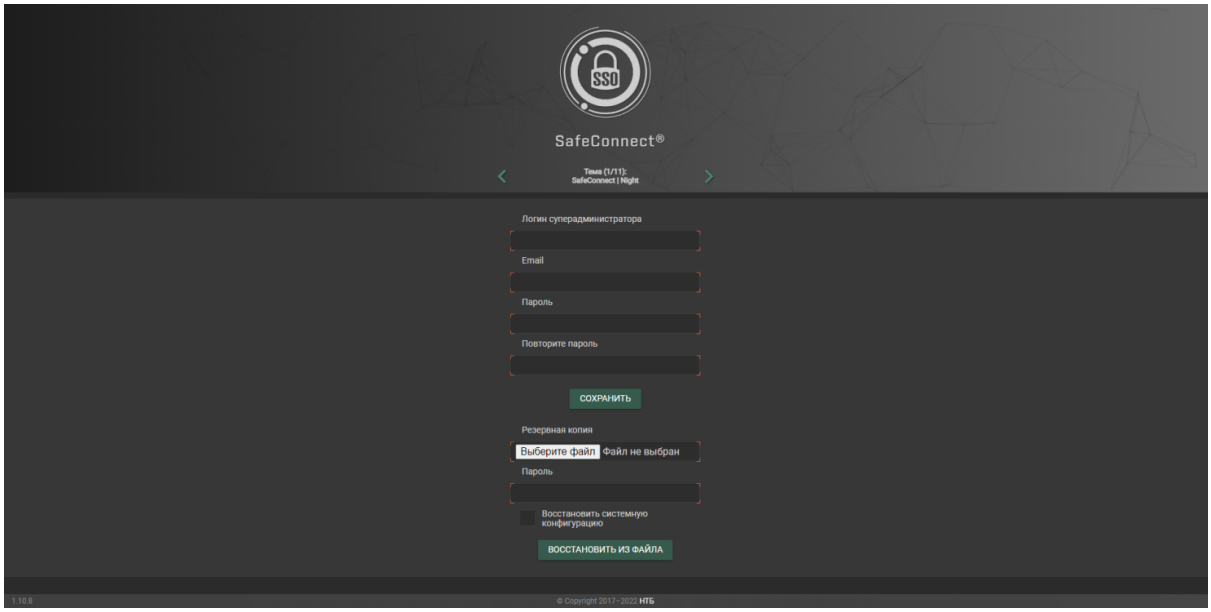


Рис. 3.1. Создание суперадминистратора

Откроется **главное окно** программного комплекса SafeConnect.

Для первоначального входа в систему нужно ввести:

- **логин суперадминистратора**,
- **e-mail**,
- **пароль**,
- **повторить пароль.**

Дополнительно есть возможность выбора **темы** (с помощью переключателя в верхнем меню) (Рис.3.2) .

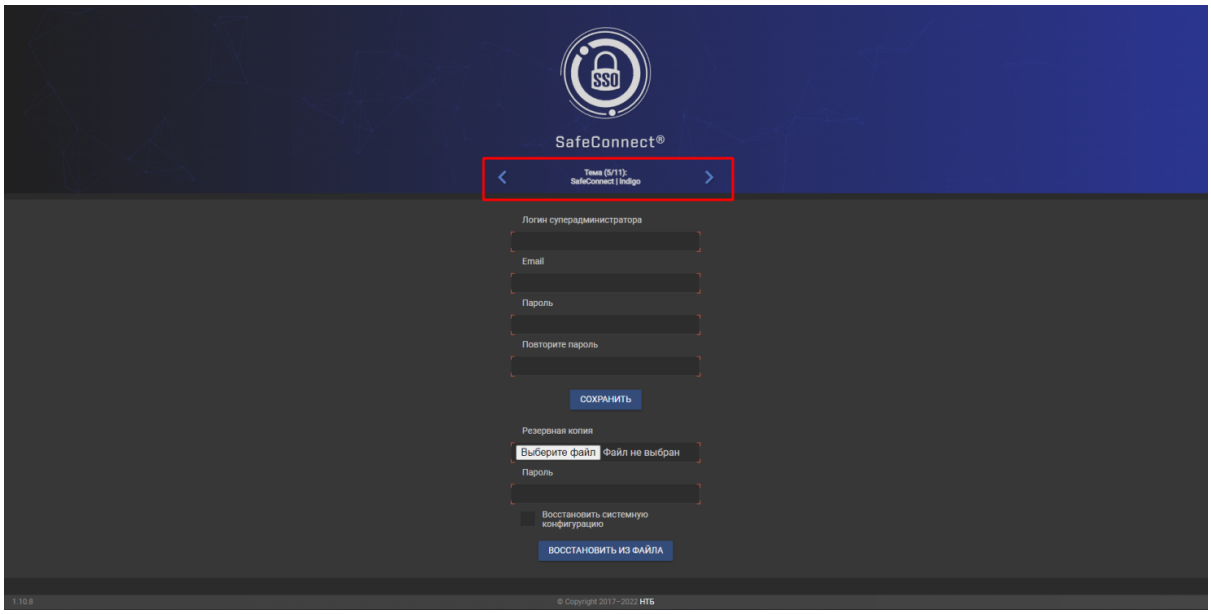


Рис. 3.2. Выбор темы

Для ввода данных нажать кнопку **Сохранить**.

Для **восстановления системы из резервной копии** сразу после установки:

- выбрать **файл резервной копии** по кнопке **Выберите файл**;
- ввести **пароль**, назначенный при создании резервной копии;
- при необходимости включить установить флажок **Восстановить системную конфигурацию**;

Примечание

Настройки сети не восстанавливаются, если резервная копия была сделана на другой машине.

- нажать кнопку **Восстановить из файла**.

После сохранения **первоначальных настроек** (после восстановления системы из резервной копии) откроется **главное окно** программного комплекса SafeConnect (Рис.3.3)
.

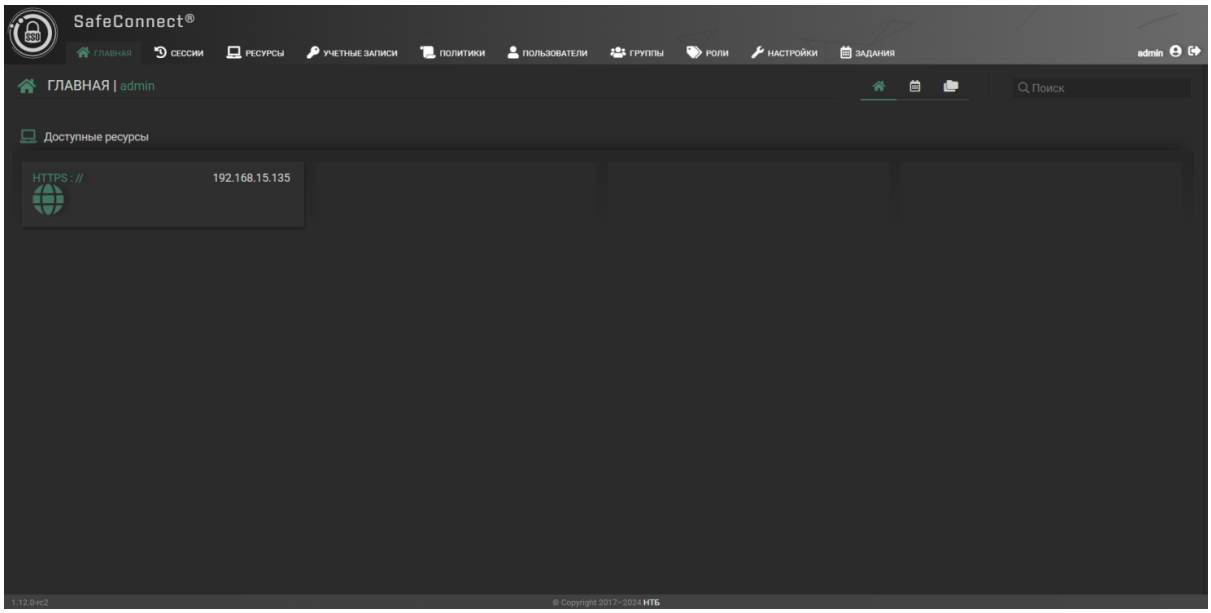


Рис. 3.3. Главное окно SafeConnect

После появления главного окна инсталляция считается завершенной.

3.2. Вход в программу

Для входа в **пользовательский интерфейс** администратора SafeConnect следует в адресной строке веб–браузера ввести **IP–адрес** системы, назначенный при установке, и нажать клавишу **Enter**. Далее на открывшейся странице входа в систему следует ввести **имя пользователя**, **пароль** и нажать кнопку **Войти**.

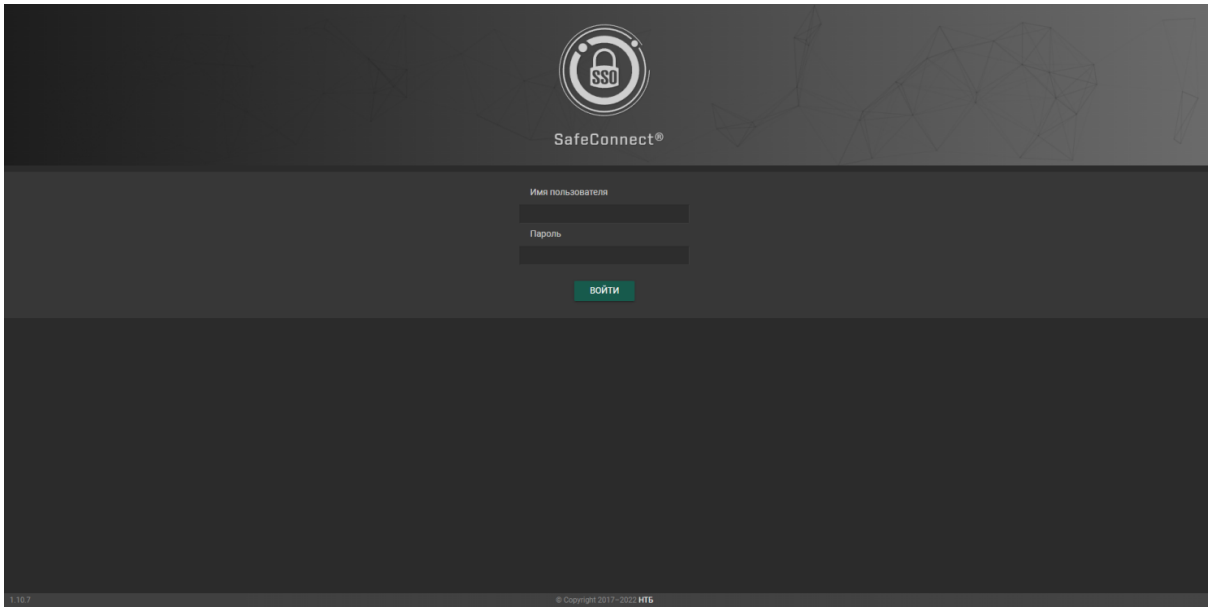


Рис. 3.4. Вход в пользовательский интерфейс

Для первого входа в SafeConnect следует использовать **идентификационные данные** суперадминистратора, которые были определены в ходе первоначальной установки. Далее откроется **главная страница** SafeConnect (Рис.3.5) .

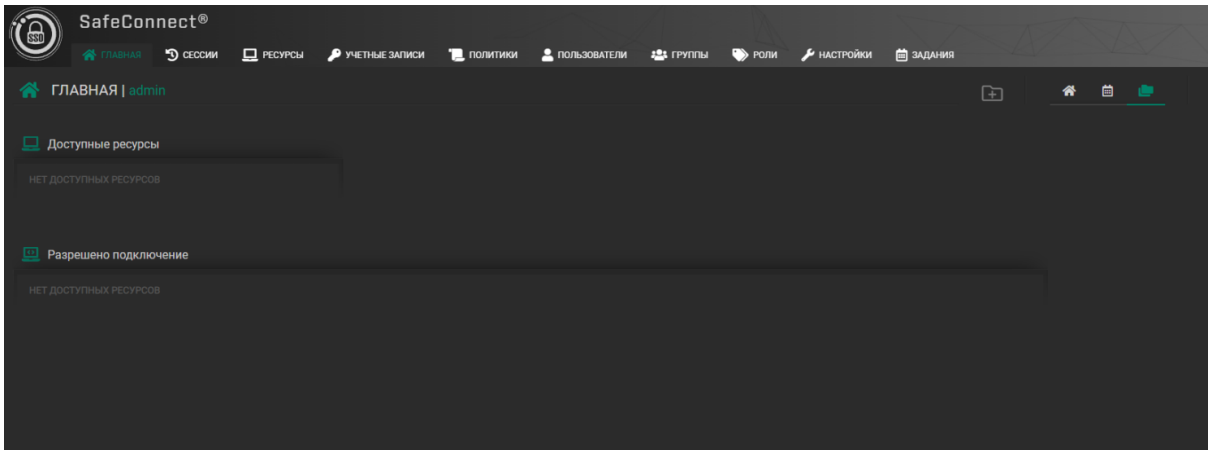


Рис. 3.5. Главная страница

На **главной странице** размещены:

- **Информационная панель** – включает в себя **название** программы, **логин** текущего пользователя, **персональную информацию** текущего пользователя (Рис.3.6), кнопку **Завершение сеанса работы текущего пользователя** (Рис.3.6);

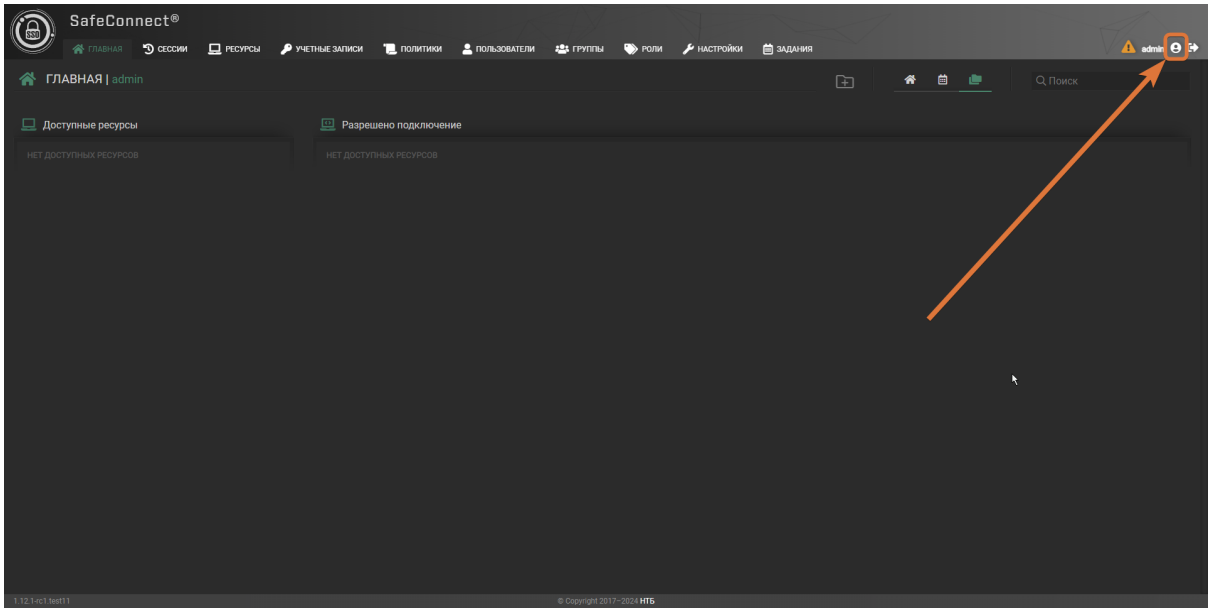


Рис. 3.6. Персональная информация текущего пользователя

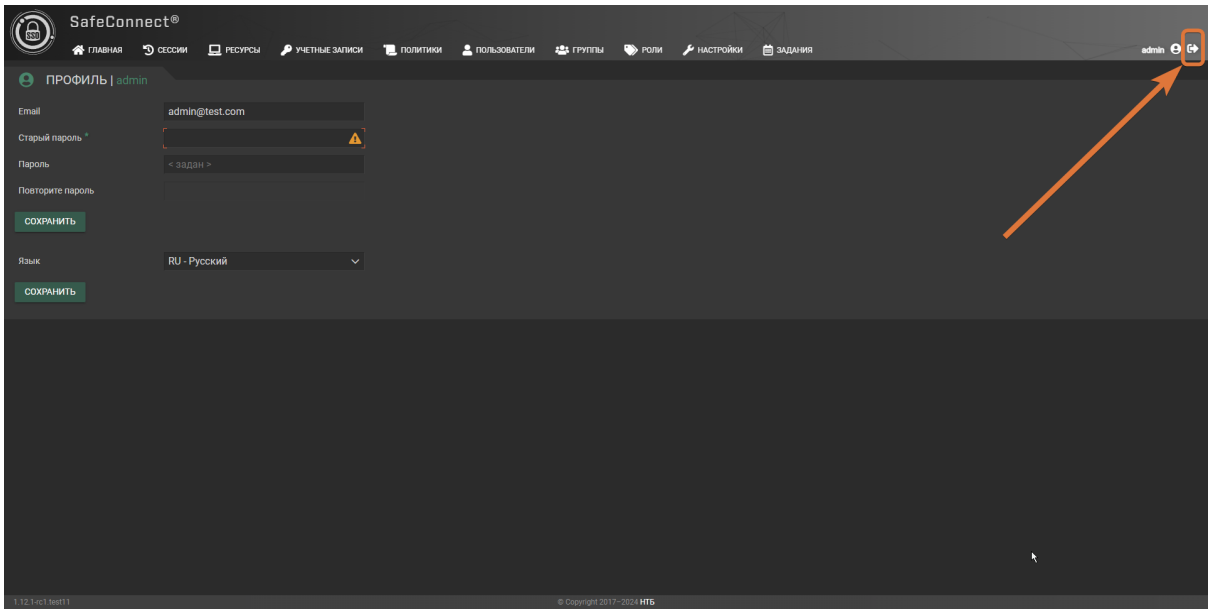


Рис. 3.7. Завершение сеанса текущего пользователя

- **Главное меню** – предоставляет пользователю возможность быстрого доступа к функциональным возможностям портала (Рис.3.8);

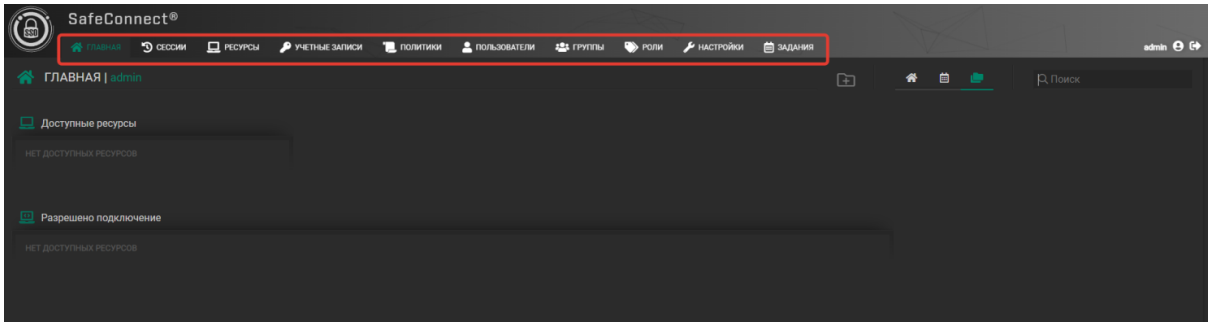


Рис. 3.8. Главное меню

- **Рабочая область** – отображает окно выбранного раздела программы (Рис.3.9);

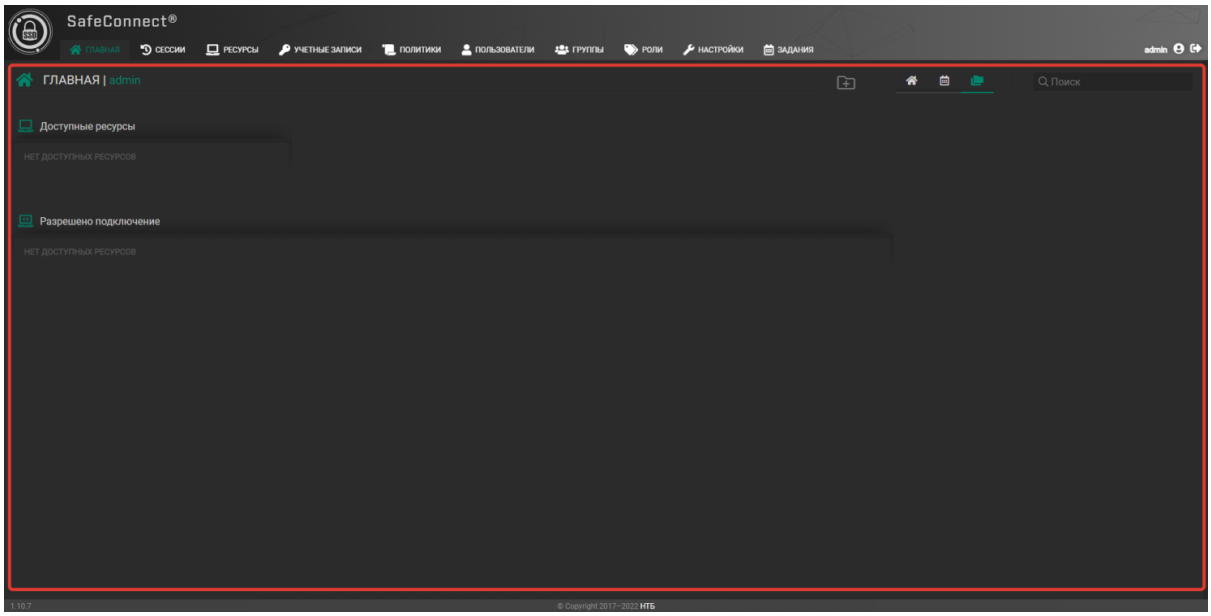


Рис. 3.9. Рабочая область

- В нижней части окна отображается **текущая установленная версия программы**.

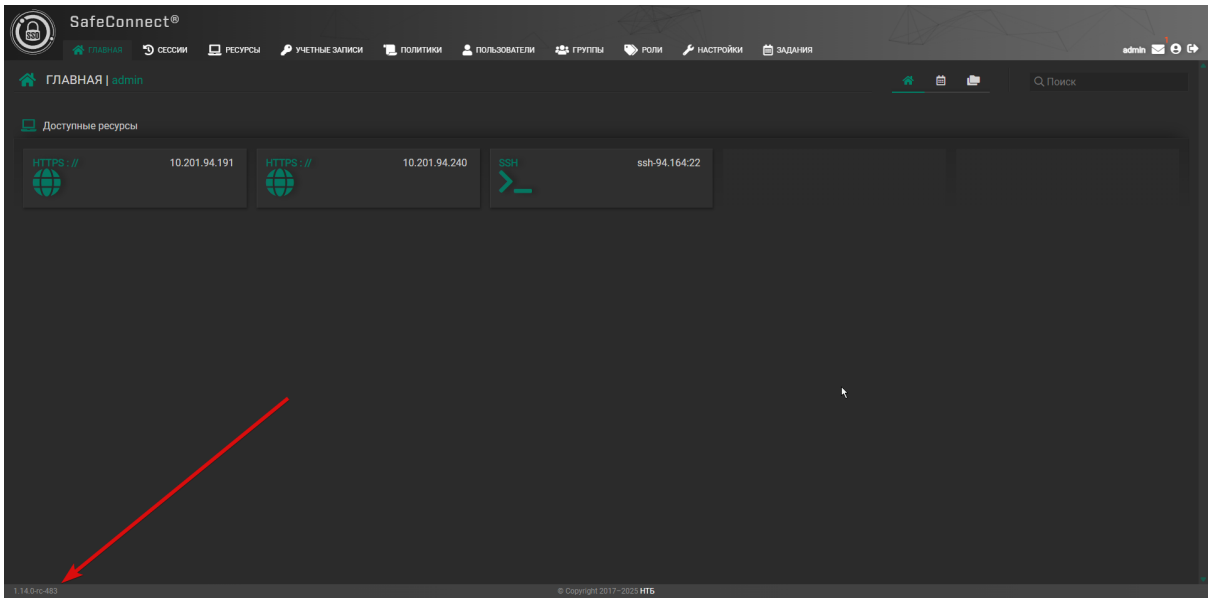


Рис. 3.10. Текущая версия программы

3.3. Выбор языка интерфейса

В **Профиле администратора** доступен выбор **языка интерфейса .** По умолчанию интерфейс SafeConnect **русский**.

Для смены языка интерфейса на английский необходимо:

1. В правом верхнем углу нажать значок **Профиль** (Рис.3.11, 1);
2. В блоке **Язык** из выпадающего списка выбрать значение **EN** – **English** (Рис.3.11, 2);

3. Сохранить конфигурацию кнопкой **Сохранить** (Рис.3.11, 3).

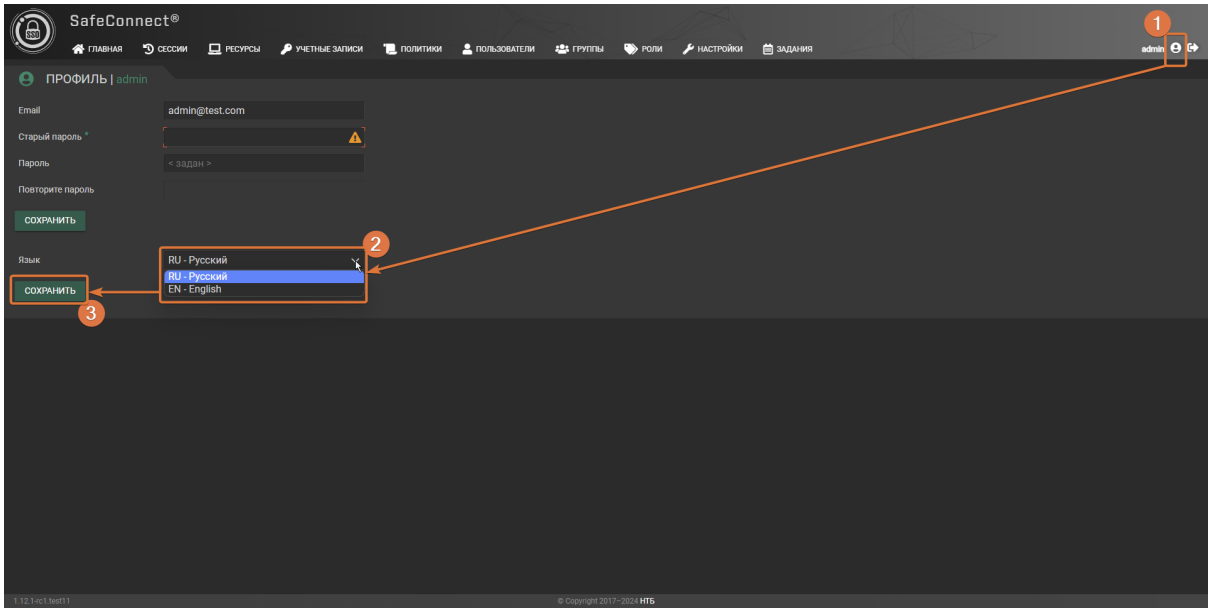


Рис. 3.11. Раздел «Настройки». Выбор языка интерфейса

3.4. Главное меню

Главное меню обеспечивает доступ ко всем разделам работы SafeConnect и позволяет производить все необходимые настройки (Рис.3.8).

Главное меню состоит из следующих разделов:

- **Главная** – отображает ресурсы, назначенные текущему пользователю;
- **Сессии** – отображает информацию о доступе пользователей к ресурсам;
- **Ресурсы** – раздел для настройки и управления доступными ресурсами;
- **Учетные записи** – раздел управления учетными записями пользователей;
- **Политики** – раздел управления политиками доступа;
- **Пользователи** – раздел управления списком пользователей Портала;
- **Группы** – раздел управления группами пользователей;
- **Роли** – раздел управления списком ролей пользователей;
- **Настройки** – раздел содержит страницы с настройками:
  - Лицензия;
  - Безопасность;
  - Интеграция с внешними системами;
  - Настройки SMTP;

- Пользовательское соглашение;
- Репликация;
- Серверы LDAP;
- Серверы RADIUS;
- Сетевые настройки;
- Брендирование;
- Резервное копирование и восстановление;
- Система;

- **Задания** – раздел позволяет создавать задания для пользователей Портала.

3.5. Раздел «Главная»

Вкладка **Главная** является домашней страницей SafeConnect и открывается после авторизации пользователя (Рис.3.5).

В **рабочей области** отображаются все доступные данному пользователю **ресурсы** и **разрешенные доступы**. Чтобы просмотреть **информацию по конкретному ресурсу**, следует кликнуть на него мышкой.

По каждому ресурсу отображается следующая информация (Рис.3.12):

- **Статус** – отображается статус ресурса (доступен для подключения или нет);
- **Тип авторизации** – способ авторизации пользователя;
- **Учетная запись** – учетная запись пользователя, кому дан доступ;
- **Подключения** – общее количество подключений (∞ – без ограничений);
- **Длительность сессии** – максимальная длительность сессии (∞ – нет ограничений по длительности);
- **Время доступа** – время, когда разрешен доступ пользователю к данному ресурсу (значок бесконечности ∞ – разрешен доступ без ограничений по времени);
- **Следующая сессия через** – промежуток времени до следующей сессии;
- **Подтверждение** – индикатор необходимости дополнительного подтверждения доступа;
- **Задание** – задание, на основании которого выдан доступ.

Для нового запроса доступа к данному ресурсу следует установить переключатель в начале строки в положение «активен» и нажать кнопку **Запросить доступ.**

Над списком ресурсов расположено поле для контекстного поиска нужного ресурса. Начать вводить в поле поиска **название ресурса** и в списке останутся только те ресурсы, в названии которых есть введенное значение.

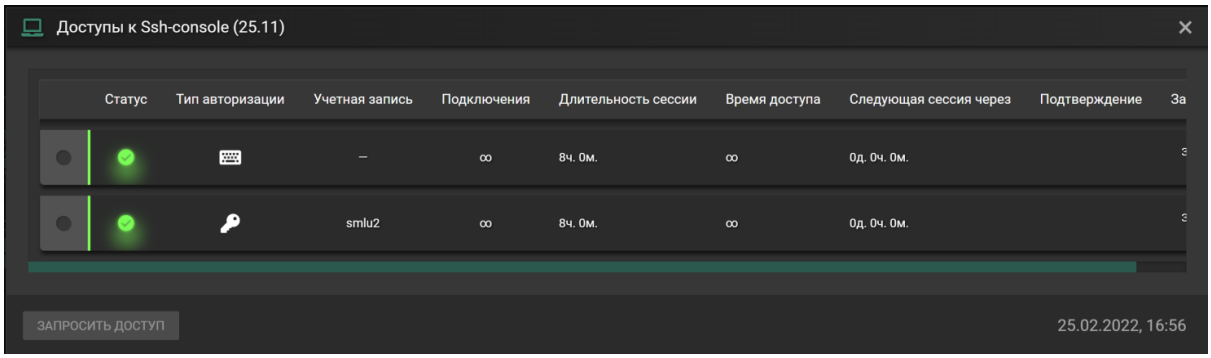


Рис. 3.12. Информация по ресурсу

3.6. Раздел «Сессии»

3.6.1. Общие сведения

В рабочей области раздела **Сессии** расположена таблица, в которой отображается информация по доступу пользователей SafeConnect к ресурсам. По каждому доступу отображается следующая информация (Рис.3.13):

- **Пользователь** – имя пользователя, осуществившего доступ к ресурсу;
- **Ресурс** – название ресурса, на который был доступ;
- **Протокол** – протокол, по которому был назначен доступ;
- **Авторизация** – тип авторизации и учетная запись;
- **Задание** – задание, на основании которого был выполнен доступ;
- **Дата создания**;
- **Начало** – дата и время начала доступа к ресурсу;
- **Окончание** – дата и время окончания пользовательской сессии;
- **Соединение** – статус подключения и длительность сессии.

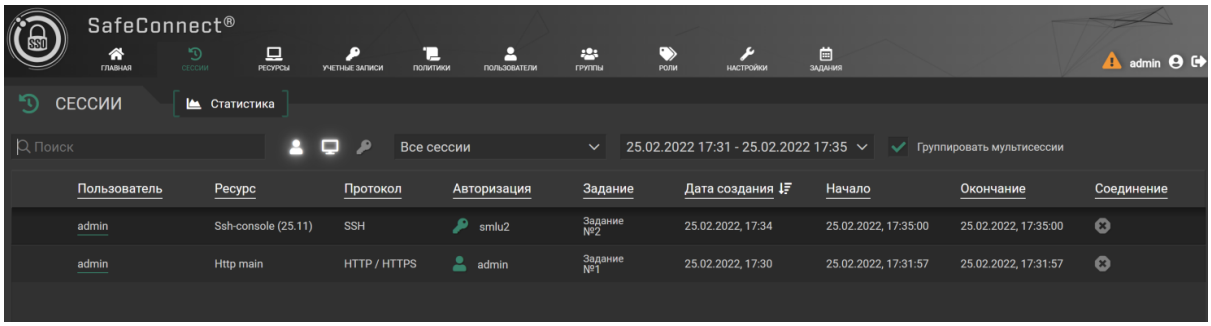


Рис. 3.13. Раздел «Сессии»

Информация в таблице может быть отсортирована по любому столбцу.

Имеется возможность редактировать персональные настройки конкретного пользователя. Для перехода на страницу **Редактирование пользователя** следует выбрать **имя пользователя**.

Также имеется возможность **редактирования задания**, на основании которого выполняется доступ. Для перехода на страницу **задания** (Рис.3.14) следует перейти по ссылке с названием задания в **строке соответствующего пользователя**.

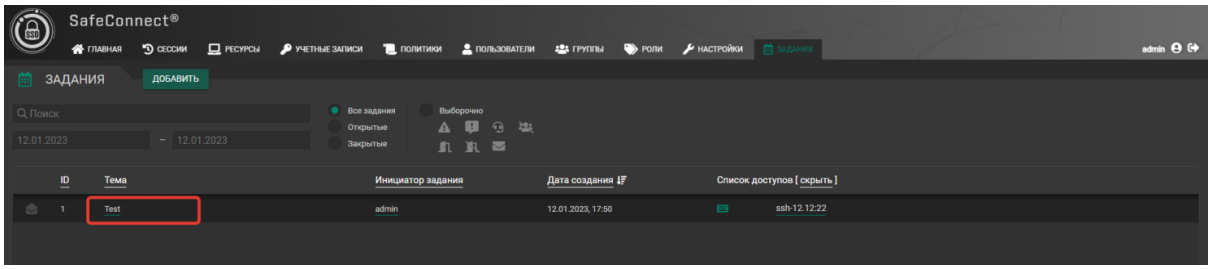


Рис. 3.14. Переход на страницу задания

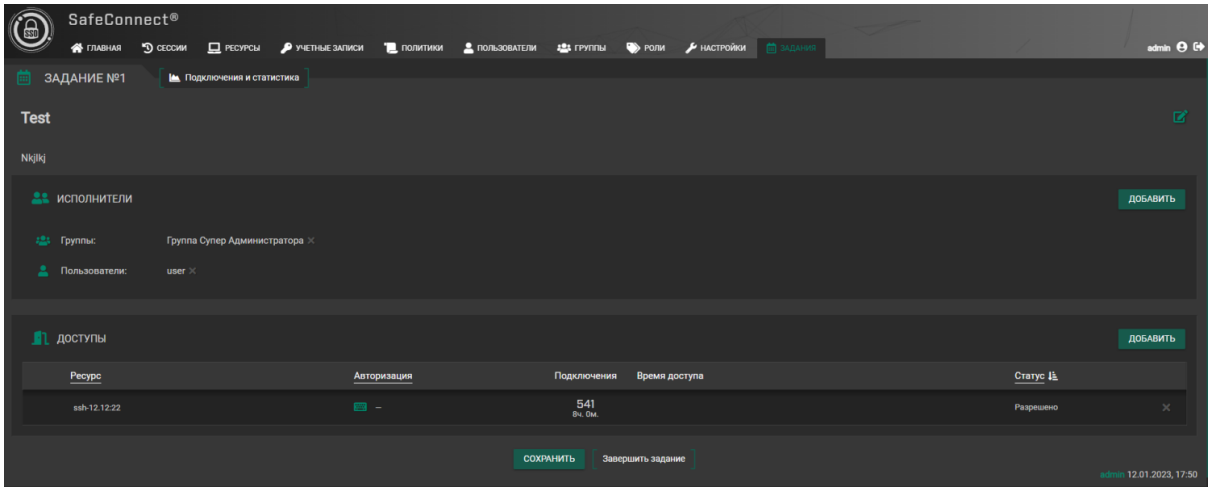


Рис. 3.15. Страница редактирования задания

На странице **редактирования задания** (Рис.3.15) можно добавить **исполнителей** или **доступы** кнопкой **Добавить,** или удалить **исполнителей** или **доступы**, нажав на значок «крестик» ✕, завершить задание кнопкой **Завершить задание**, отправить уведомление исполнителям задания (Рис.3.16).

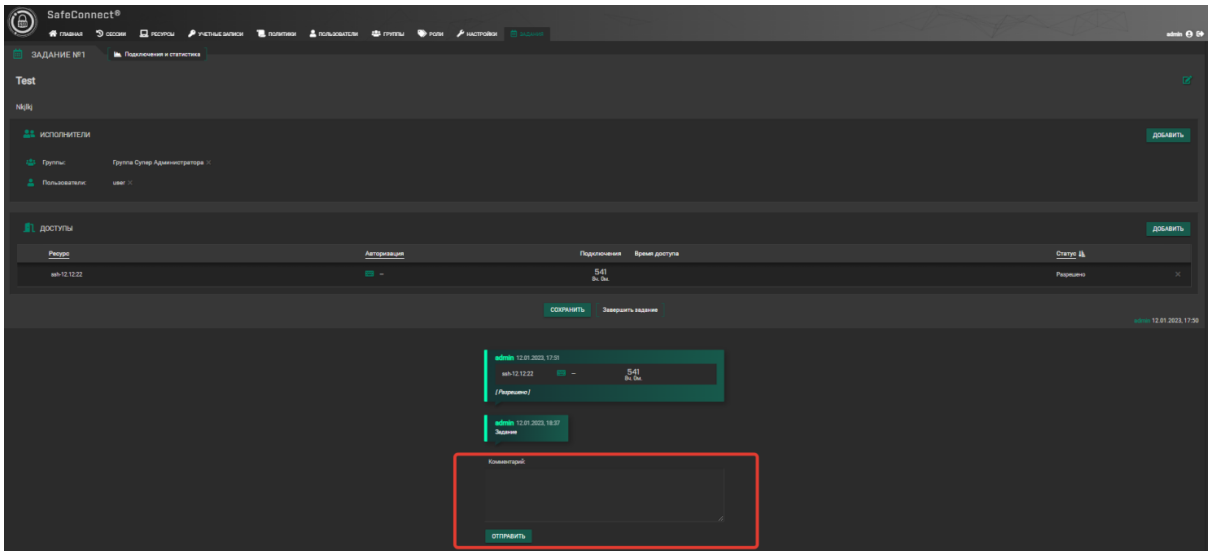


Рис. 3.16. Отправка уведомления исполнителям задания

3.6.2. Статистика и поиск

Для **просмотра статистики** необходимо перейти в раздел **Сессии** и нажать кнопку **Статистика** (Рис.3.17);

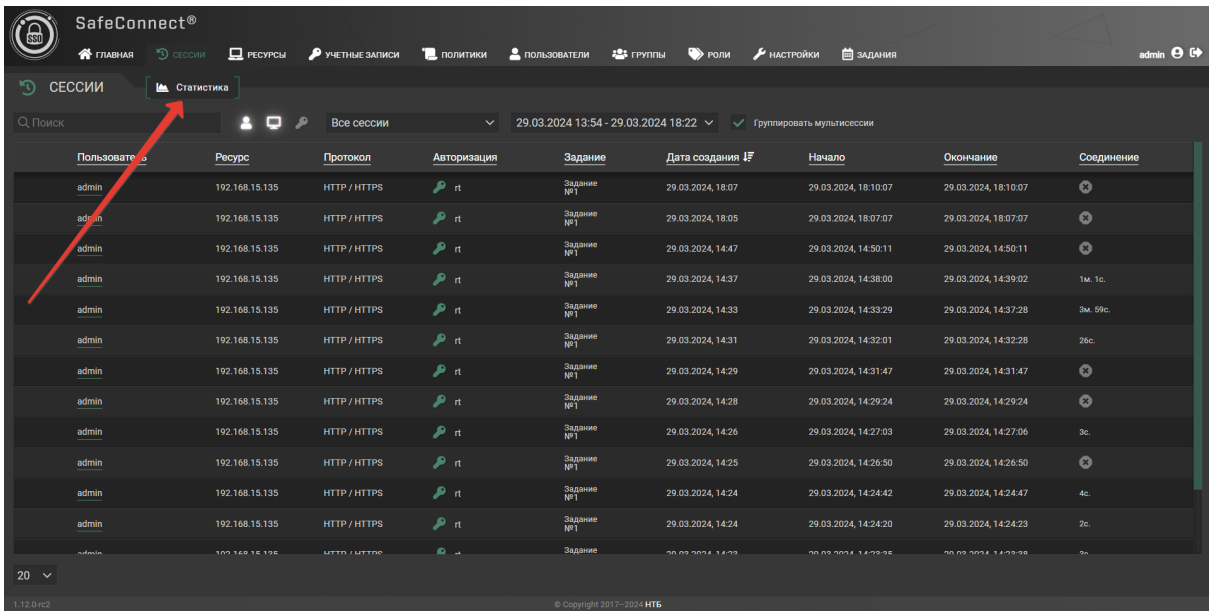


Рис. 3.17. Расположение кнопки «Статистика»

Далее для просмотра станут доступны **статистика** и **информация по подключениям** пользователя (Рис.3.18).

Настроить параметры отображаемой статистики можно следующим образом:

- **Выбор отображаемых сессий** (Рис.3.18):
  - Все сессии;
  - Установленные соединения;

- Сейчас онлайн;

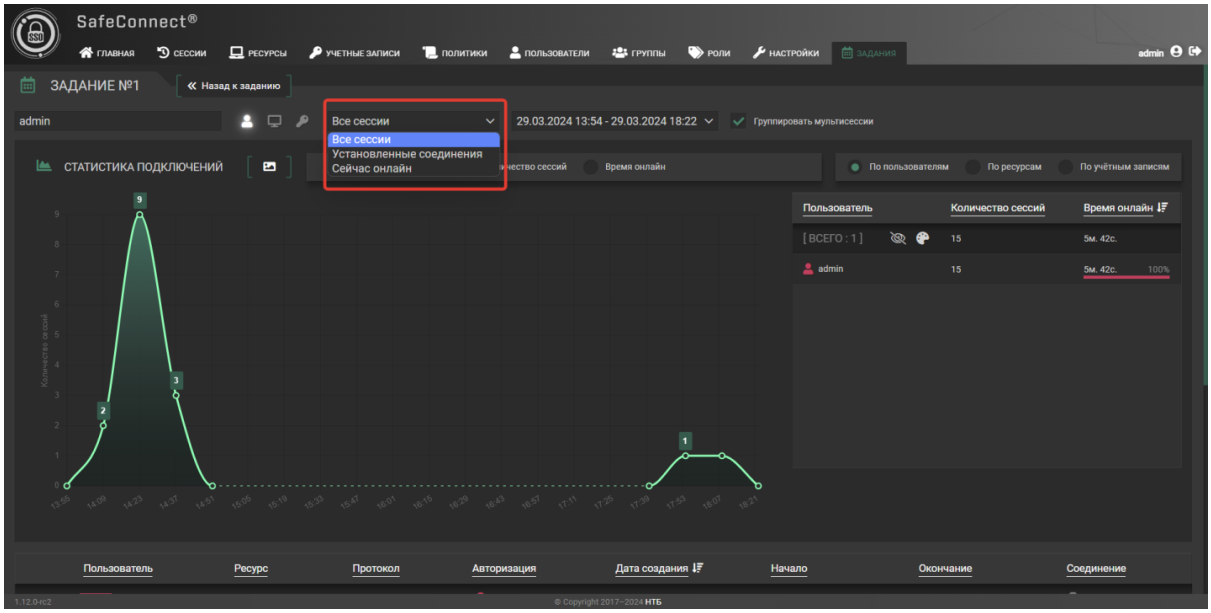


Рис. 3.18. Отображение сессий

- **Установка временного периода** (Рис.3.19):
  - **Выбор периода из списка** (Рис.3.19). Для установки значения необходимо выбрать одним щелчком мыши вариант из списка:
    - Сегодня;
    - Вчера;
    - На этой неделе;
    - В этом месяце;
    - В этом году;

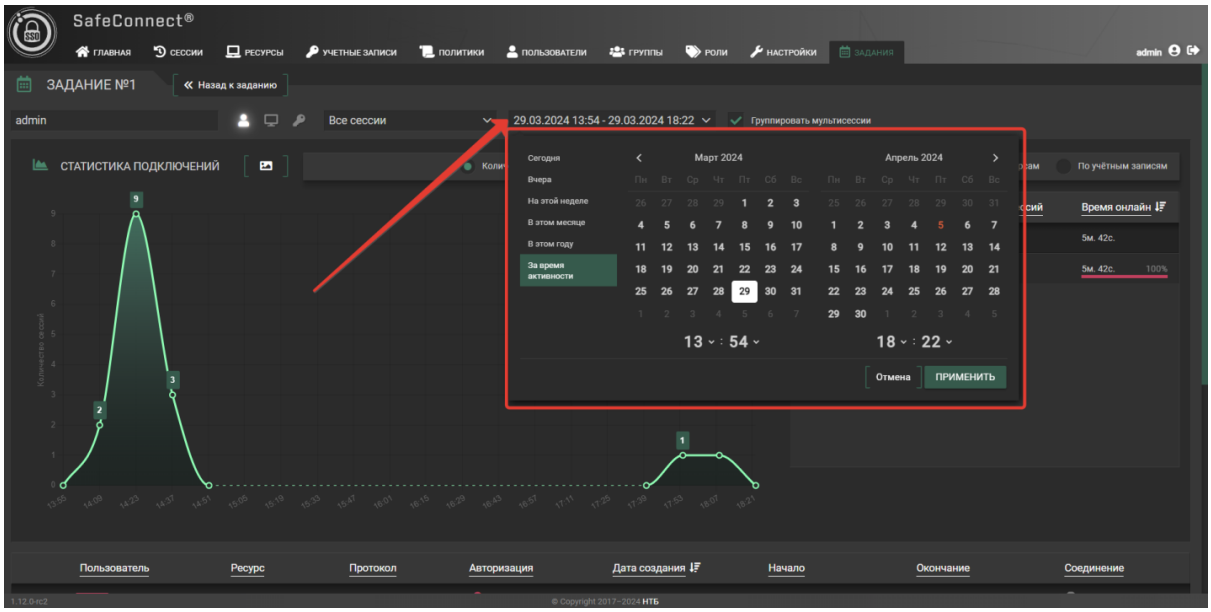


Рис. 3.19. Установка временного периода

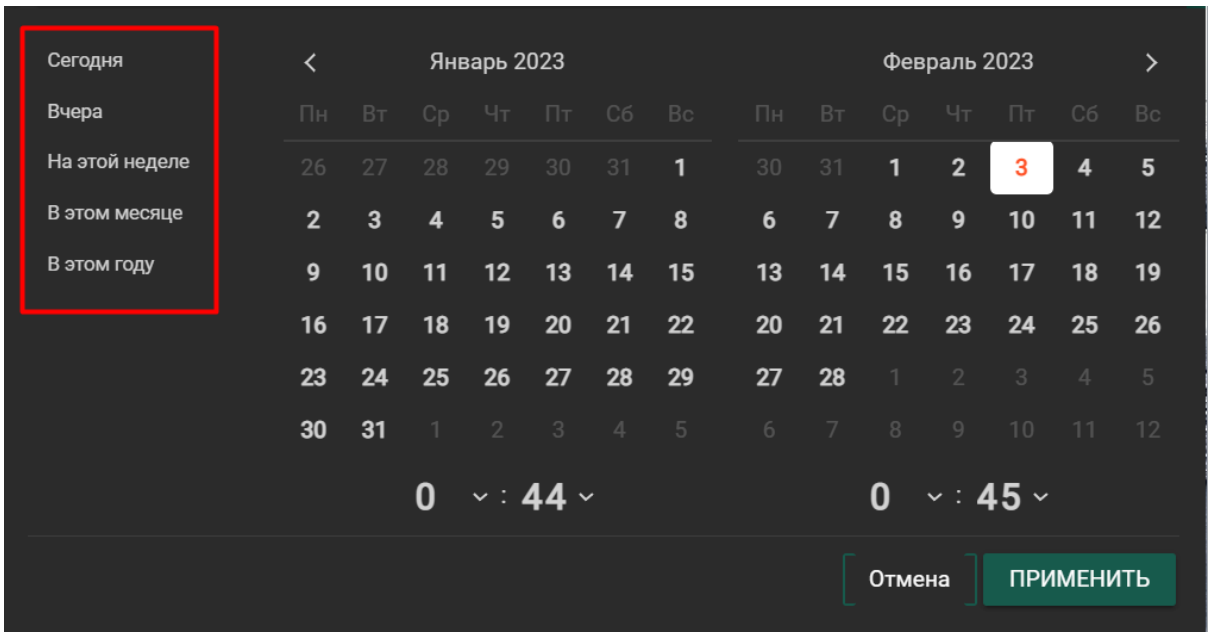


Рис. 3.20. Выбор периода из списка

- **Выбор периода вручную**. Для выбора периода вручную нажать одним щелчком на **дату начала периода**, затем одним щелчком мыши на **дату окончания периода** (Рис.3.22). Для перехода между месяцами использовать стрелки **<** и **>** (Рис.3.22);

После выбора диапазона необходимо нажать кнопку **Применить,** для выхода без изменений нажать кнопку **Отмена**;

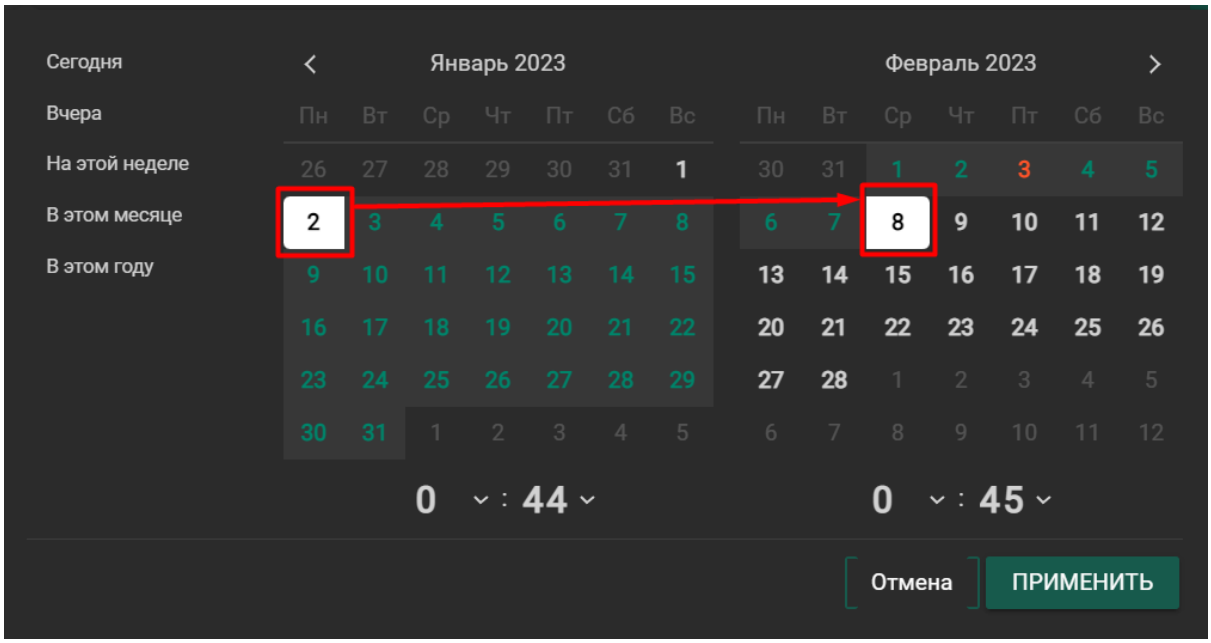


Рис. 3.21. Выбор периода вручную

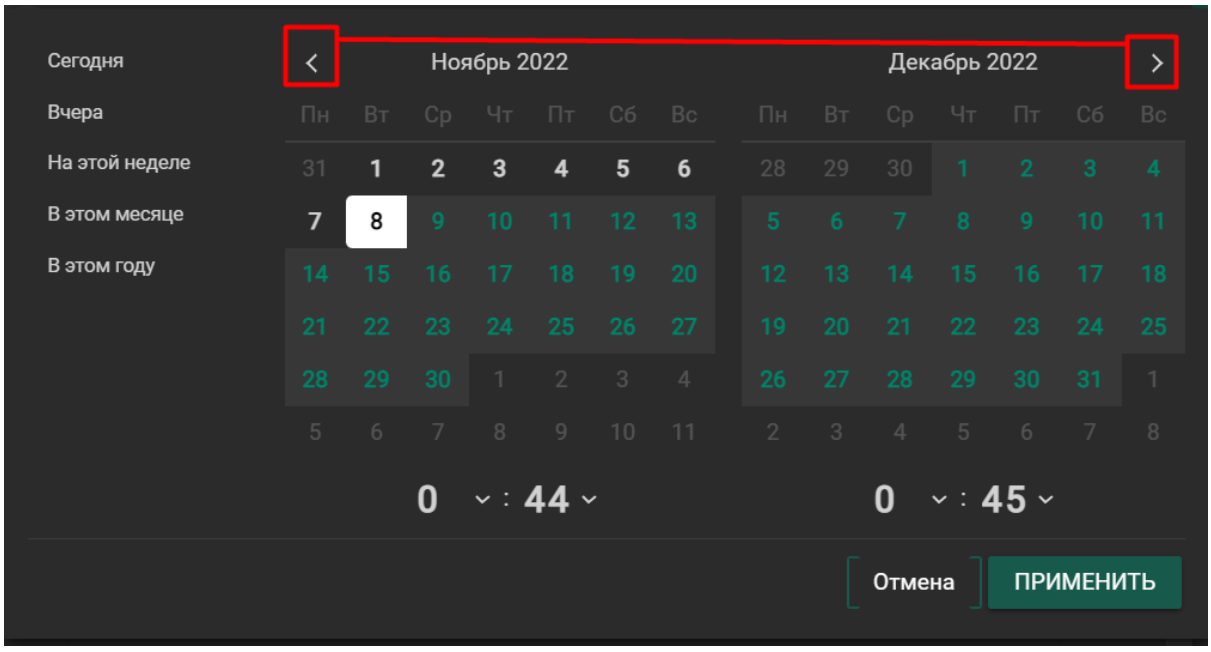


Рис. 3.22. Переход по месяцам

- **Установка времени.** Чтобы **добавить временной диапазон**, , необходимо воспользоваться **временными шкалами** и установить **время начала диапазона** и **время окончания диапазона** : последовательно нажать на цифру со значением часа, чтобы развернуть шкалу, затем на цифру со значением минут, чтобы развернуть шкалу минут (Рис.3.23). Аналогичные действия выполняются для установки **времени начала** и **времени окончания** диапазона.

После выбора диапазона нажать кнопку **Применить**, для выхода без изменений нажать кнопку **Отмена**;

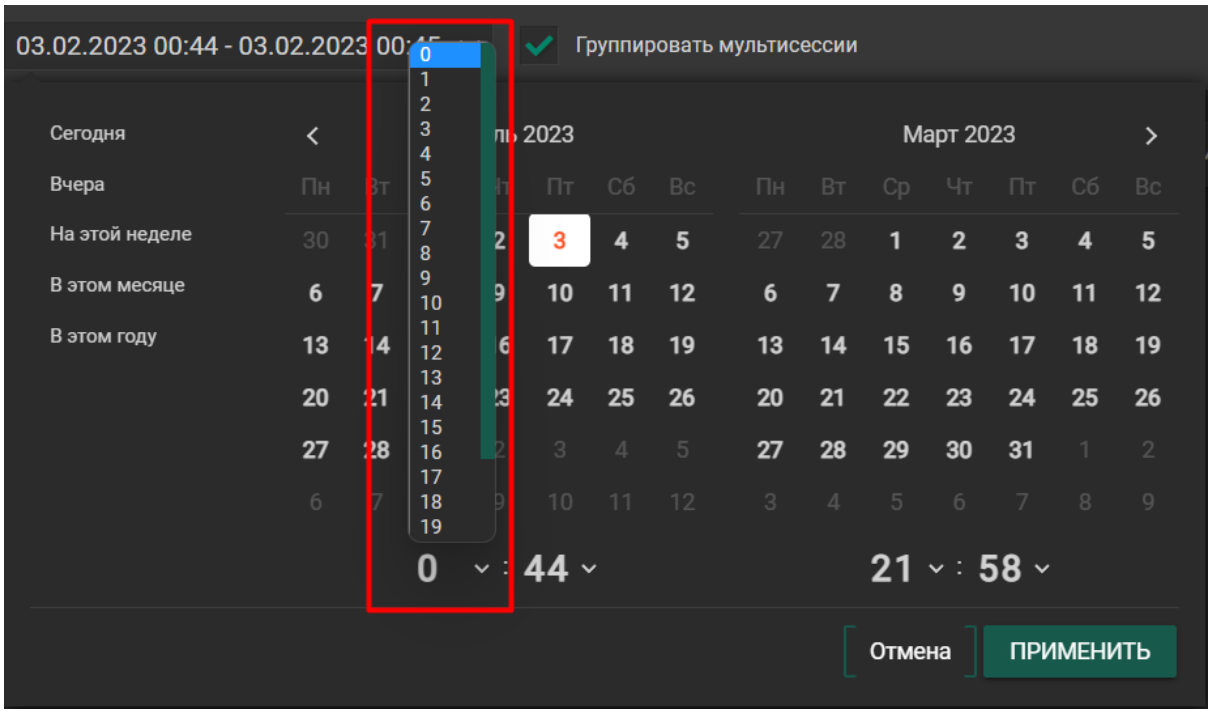


Рис. 3.23. Установка времени

Установить **дату** и **время** также можно отредактировав **верхнее поле** с отображением диапазона (Рис.3.24) .

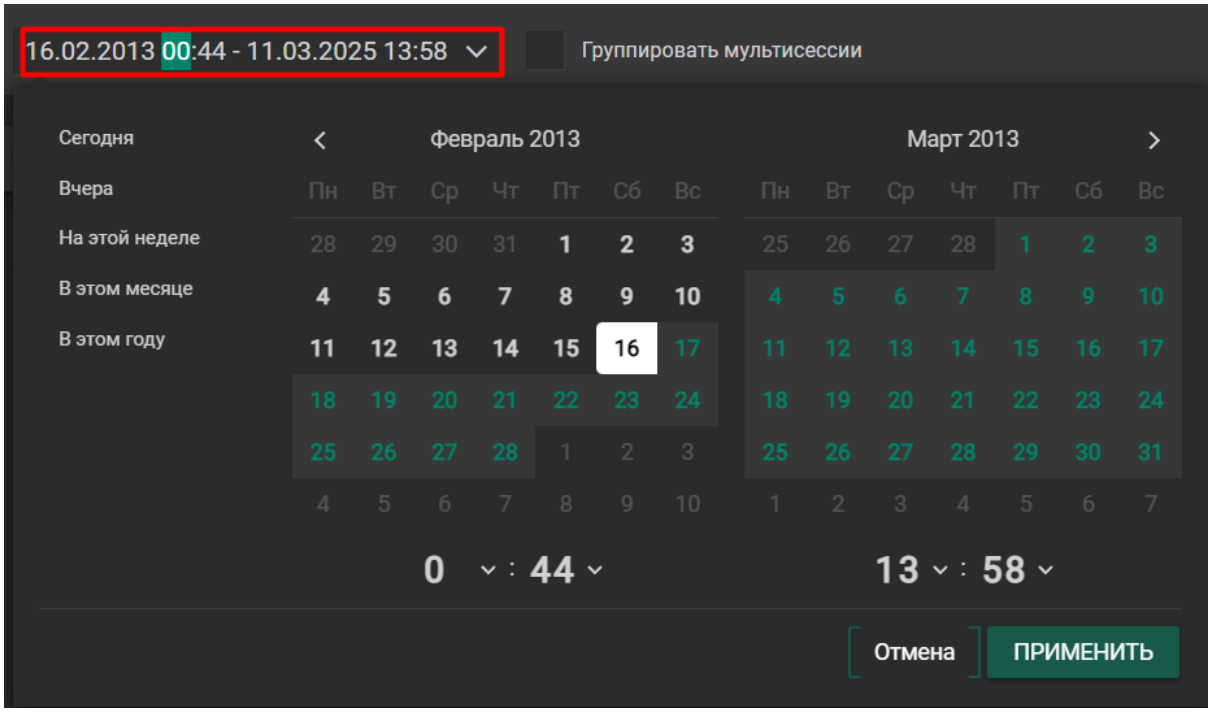


Рис. 3.24. Настройка даты и времени

- **Группировка мультисессий.** Для группировки сессий необходимо установить флажок **Группировать мультисессии** (Рис.3.25). Для разгруппировки необходимо снять данный флажок;

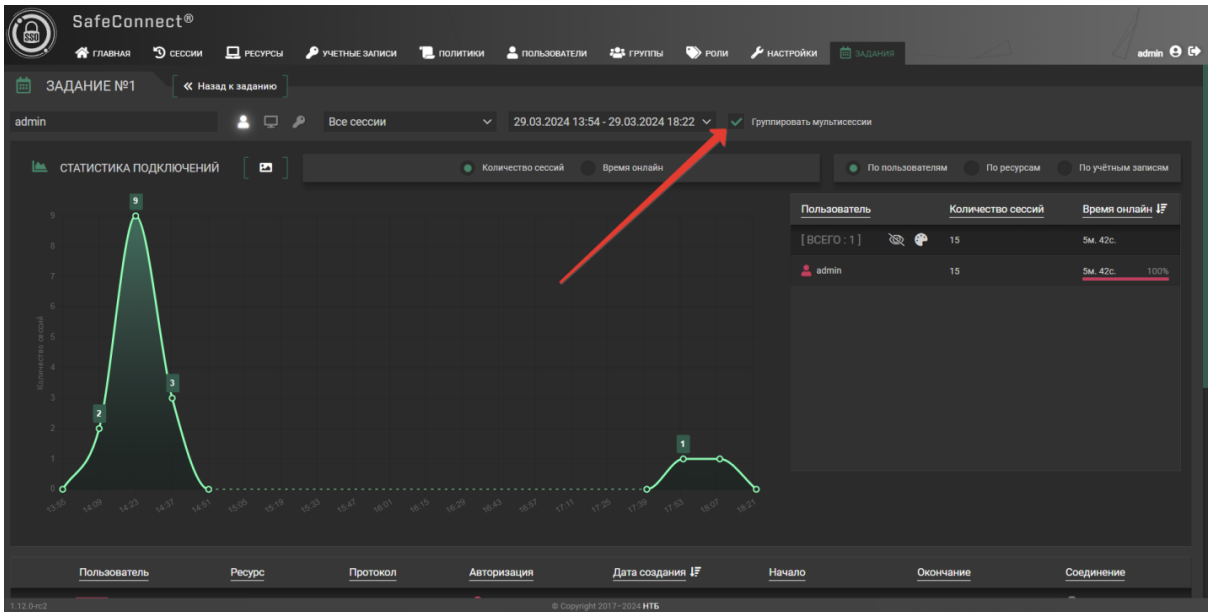


Рис. 3.25. Группировка мультисессий

- Выбор отображаемой информации:
  - **Количество сессий / Время онлайн.** Для выбора одного из значений необходимо установить переключатель в выбранное положение (Рис.3.26);
  - **По пользователям / По ресурсам / По учётным записям.** Для выбора одного из значений необходимо установить переключатель в выбранное положение (Рис.3.26);

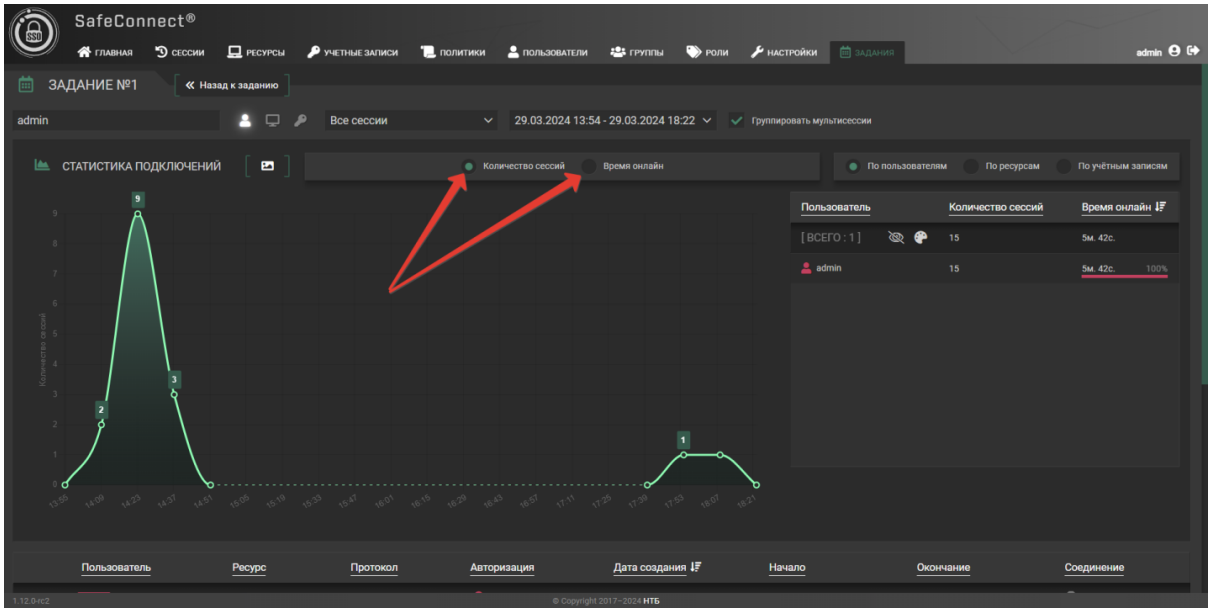


Рис. 3.26. Выбор отображаемой информации

В разделе **Статистика** доступна функция поиска. Для отображения искомой информации необходимо ввести значение в **поле поиска**. Также имеется возможность уточнить поиск:

- **Искать в имени пользователя** (включить или выключить поиск по имени пользователя);
- **Искать в названии ресурса** (включить или выключить поиск по названию ресурса);
- **Искать в названии учетной записи** (включить или выключить поиск по названию учетной записи).

Для **сохранения графика сессий** необходимо воспользоваться кнопкой загрузки изображения . В результате на локальное хранилище пользователя будет скачан файл–изображение графика в формате ***.PNG**.

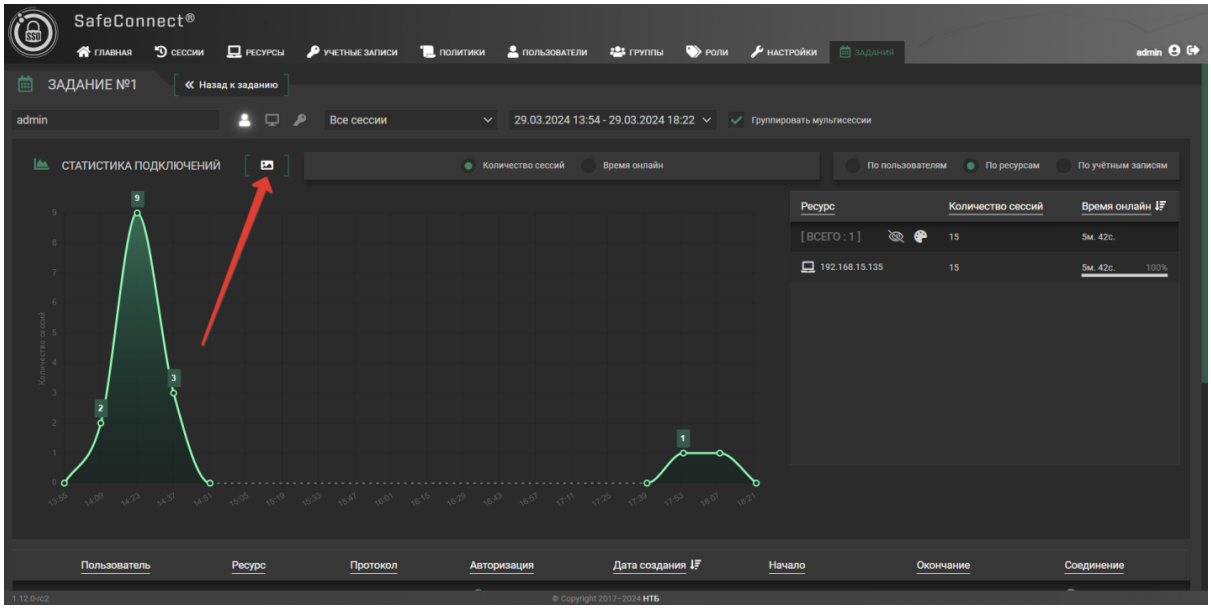


Рис. 3.27. Сохранение графика

Рядом с графиком расположены области с информацией об учетных записях и пользователях (Рис.3.28). В данной области есть возможность сортировки по столбцам. Для включения сортировки нажать на название столбца (рядом с выбранным столбцом отобразится значок сортировки по убыванию или по возрастанию).

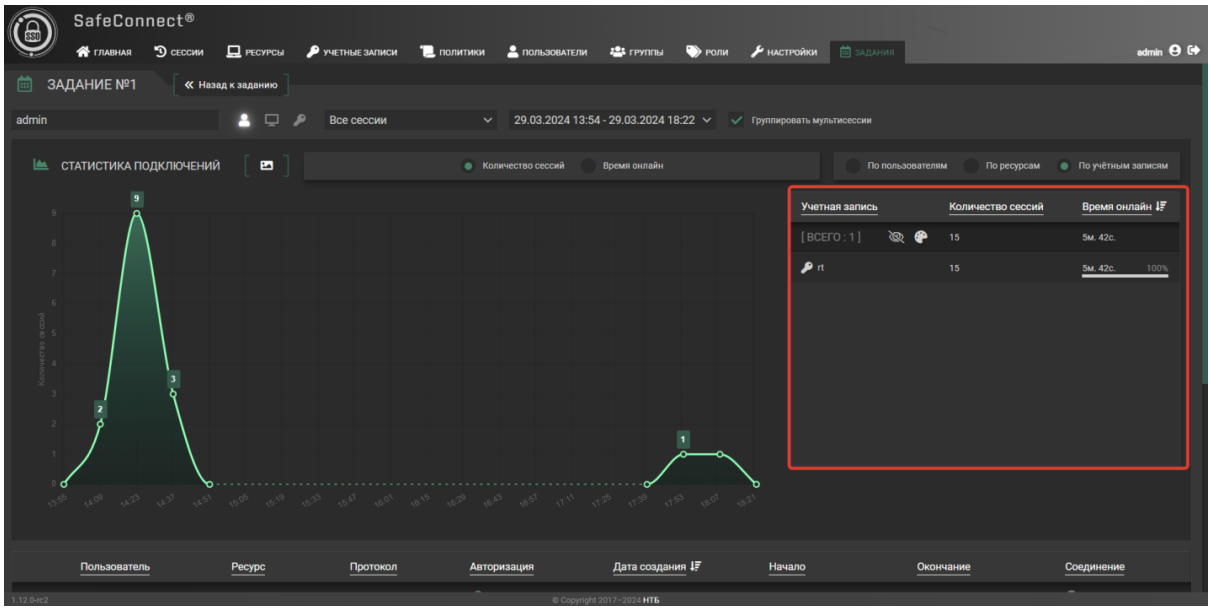


Рис. 3.28. Информация об учетных записях и пользователях

Также реализованы следующие возможности:

- при помощи кнопок скрыть  или отобразить  строчки с общим количеством записей (пользователей, ресурсов или учетных записей). Это позволяет отобразить или скрыть общее число суммы всех записей (Рис.3.29, Рис.3.30);

Примечание

У отдельных пользователей, ресурсов и учетных записей отсутствует возможность включения и выключения отображения.

- окрасить записи с текущей страницы .

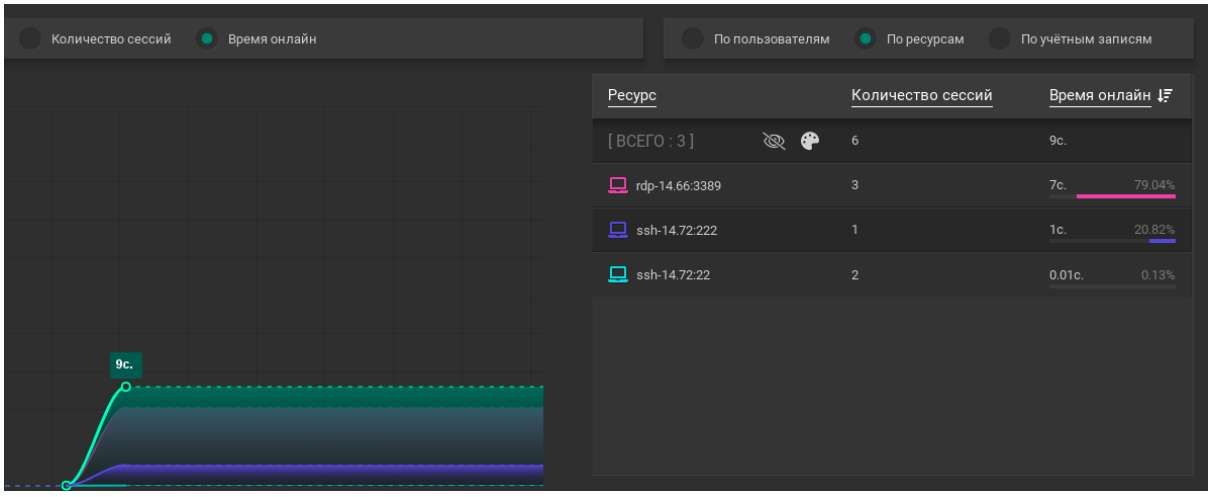


Рис. 3.29. Отображение включено

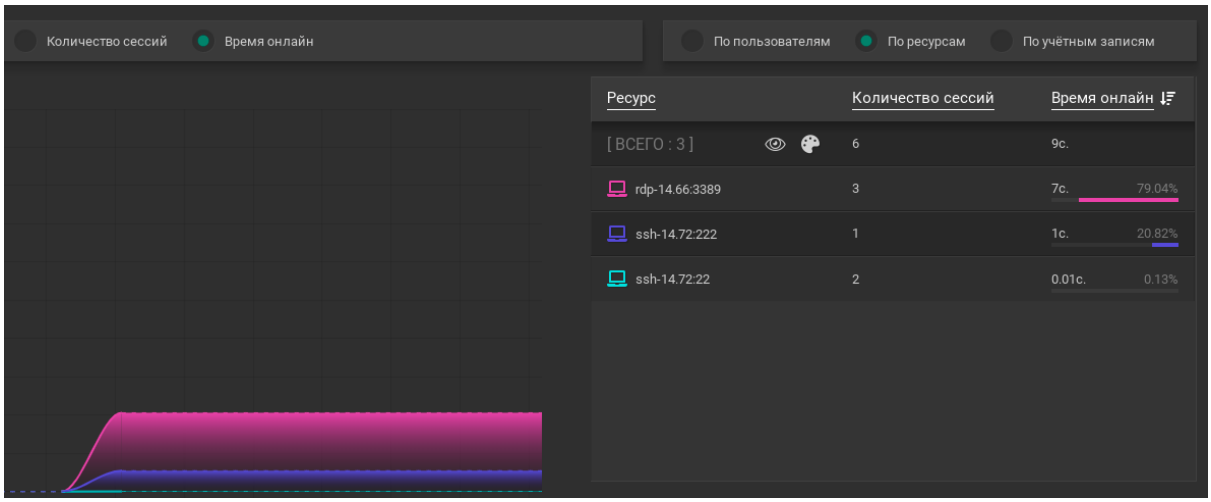


Рис. 3.30. Отображение выключено

Для выхода из просмотра статистики нажать **Скрыть статистику**.

3.7. Раздел «Ресурсы»

Раздел **Ресурсы** предназначен для формирования и управления списком ресурсов. Список формируется администратором.

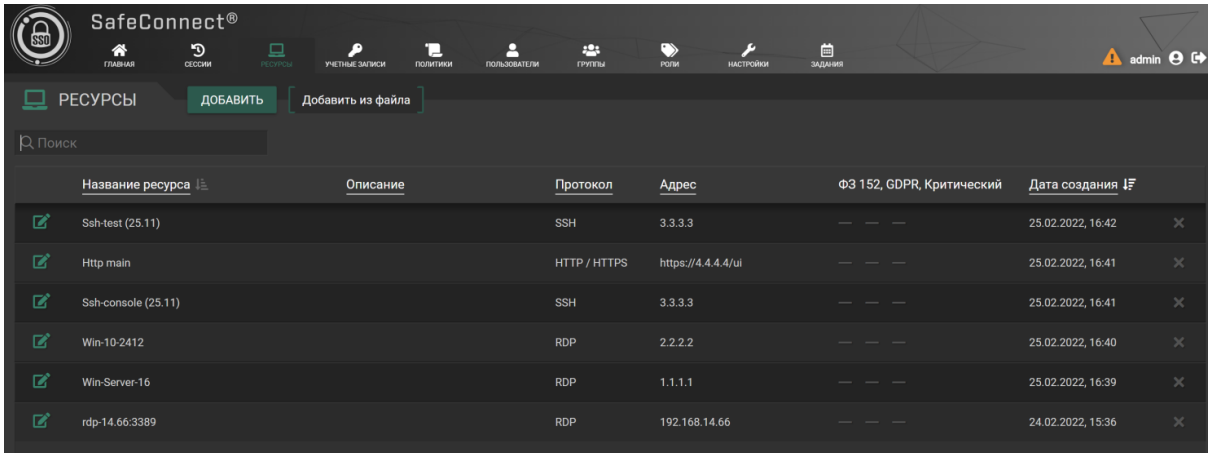


Рис. 3.31. Раздел «Ресурсы»

По каждому ресурсу отображается следующая информация:

- **Название ресурса**;
- **Описание**;
- **Протокол**;
- **Адрес** – адрес ресурса;
- **ФЗ 152, GDPR, Критический** – ресурс с данными, попадающими под действие **ФЗ–152**, **GDPR**, является критическим ресурсом инфраструктуры;
- **Дата создания** – дата создания ресурса.

Для удобства пользователя имеется возможность **фильтрации ресурсов**. Для этого в поле **Поиск** (Рис.3.32) следует ввести **название** или **IP–адрес**, или их часть, и в списке останутся только те ресурсы, которые удовлетворяют заданному значению.

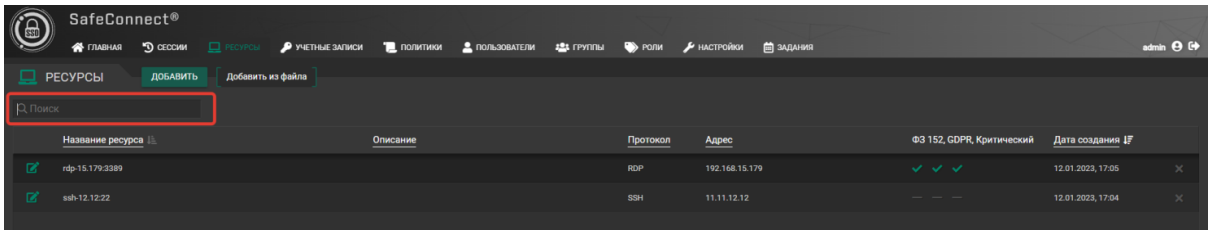


Рис. 3.32. Поле «Поиск»

3.7.1. Добавление ресурса

Для добавления в список ресурса следует перейти на вкладку **Ресурсы**, нажать кнопку **Добавить** и в открывшемся окне **Новый ресурс** (Рис.3.33) выбрать нужный протокол и заполнить форму. В зависимости от протокола меняется список параметров для заполнения:

- **Протокол** – из раскрывающегося списка выбрать нужный протокол:
  - RDP;
  - RDP App;
  - RDS;
  - SSH;
  - HTTP / HTTPS;
  - Telnet[1].

RDP (Рис.3.33):

- **Адрес** – указать **IP–адрес** или **FQDN**;
- **Порт** – изменить при необходимости (значение по умолчанию **3389**);
- **Название** – название ресурса формируется автоматически (при необходимости установить курсор в поле с названием ресурса и измените его);
- **Описание** – ввести описание ресурса (необязательное поле);
- **Ресурс с данными, попадающими под ФЗ 152** – установить флажок ☑, если ресурс содержит данные, попадающие под действие ФЗ–152;
- **Ресурс с данными, попадающими под GDPR** – установить флажок ☑, если ресурс содержит данные, попадающие под регламент защиты персональных данных **GDPR**;

[1]Настройка и открытие соединения по Telnet возможны только к целевому узлу с OS семейства Linux.

- **Критический ресурс инфраструктуры** – установить флажок ☑, если ресурс является критическим ресурсом инфраструктуры.

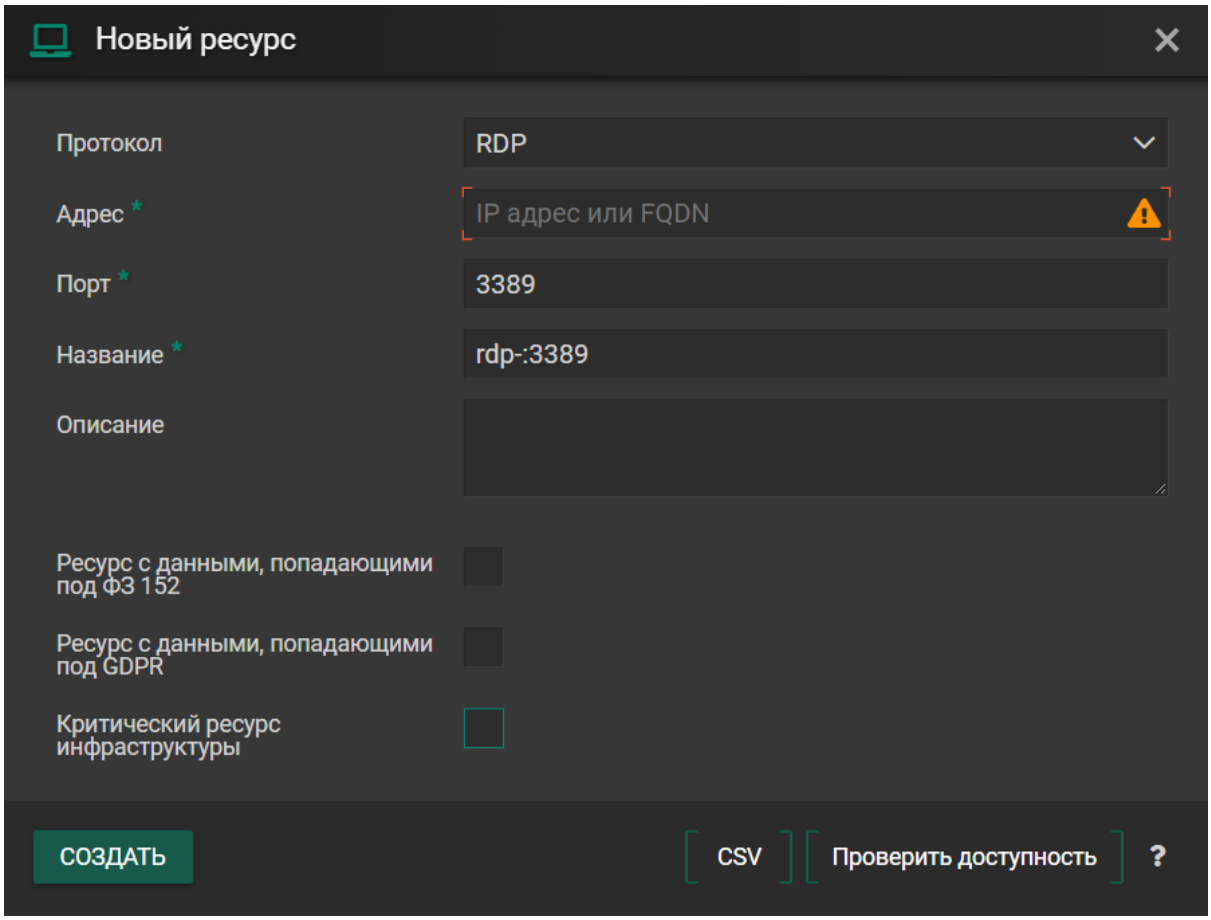


Рис. 3.33. Добавление нового ресурса (Протокол RDP)

RDP App (Рис.3.34):

- **Адрес** – указать **IP–адрес** или **FQDN**;
- **Порт** – изменить при необходимости (значение по умолчанию **3389**);
- **Полный путь к приложению** – указать путь к приложению (например, **C:\Windows\system32\calc.exe**);
- **Название** – при необходимости установить курсор в поле с названием ресурса и изменить его (название ресурса формируется автоматически);
- **Описание** – ввести описание ресурса (*необязательное поле*);
- **Ресурс с данными, попадающими под ФЗ 152** – установить флажок ☑, если ресурс содержит данные, попадающие под действие **ФЗ–152**;
- **Ресурс с данными, попадающими под GDPR** – установить флажок ☑, если ресурс содержит данные, попадающие под регламент защиты персональных данных **GDPR**;

- **Критический ресурс инфраструктуры** – установить флажок ☑, если ресурс является критическим ресурсом инфраструктуры.

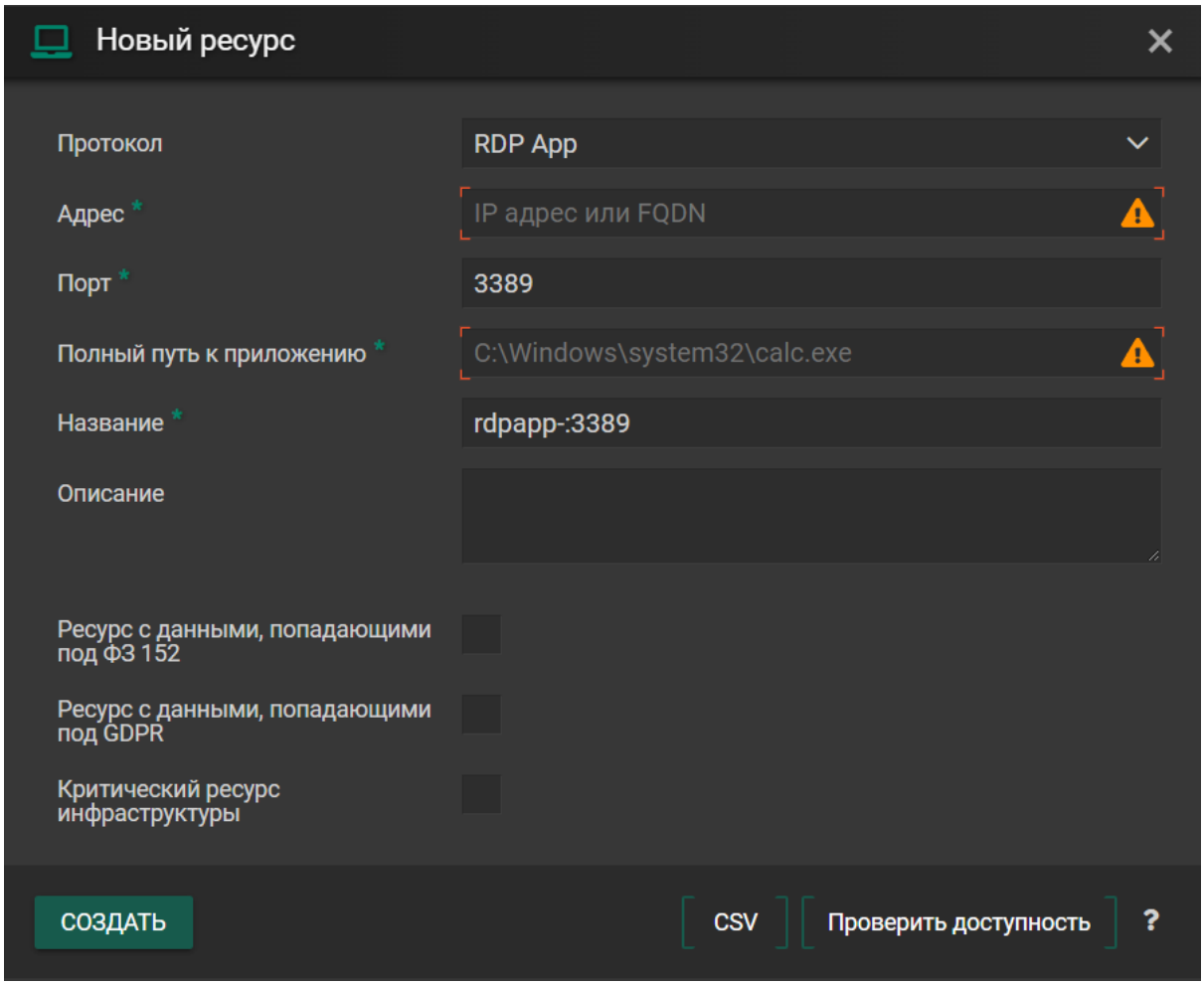


Рис. 3.34. Добавление нового ресурса (Протокол RDP App)

RDS (Рис.3.35) :

- **Адрес** – указать **IP–адрес** или **FQDN**;
- **Название** – при необходимости установить курсор в поле с названием ресурса и изменить его (название ресурса формируется автоматически);
- **Описание** – ввести описание ресурса (необязательное поле);
- **Ресурс с данными, попадающими под ФЗ 152** – установить флажок ☑, если ресурс содержит данные, попадающие под действие **ФЗ–152**;
- **Ресурс с данными, попадающими под GDPR** – установить флажок ☑, если ресурс содержит данные, попадающие под регламент защиты персональных данных **GDPR**;
- **Критический ресурс инфраструктуры** – установить флажок ☑, если ресурс является критическим ресурсом инфраструктуры.

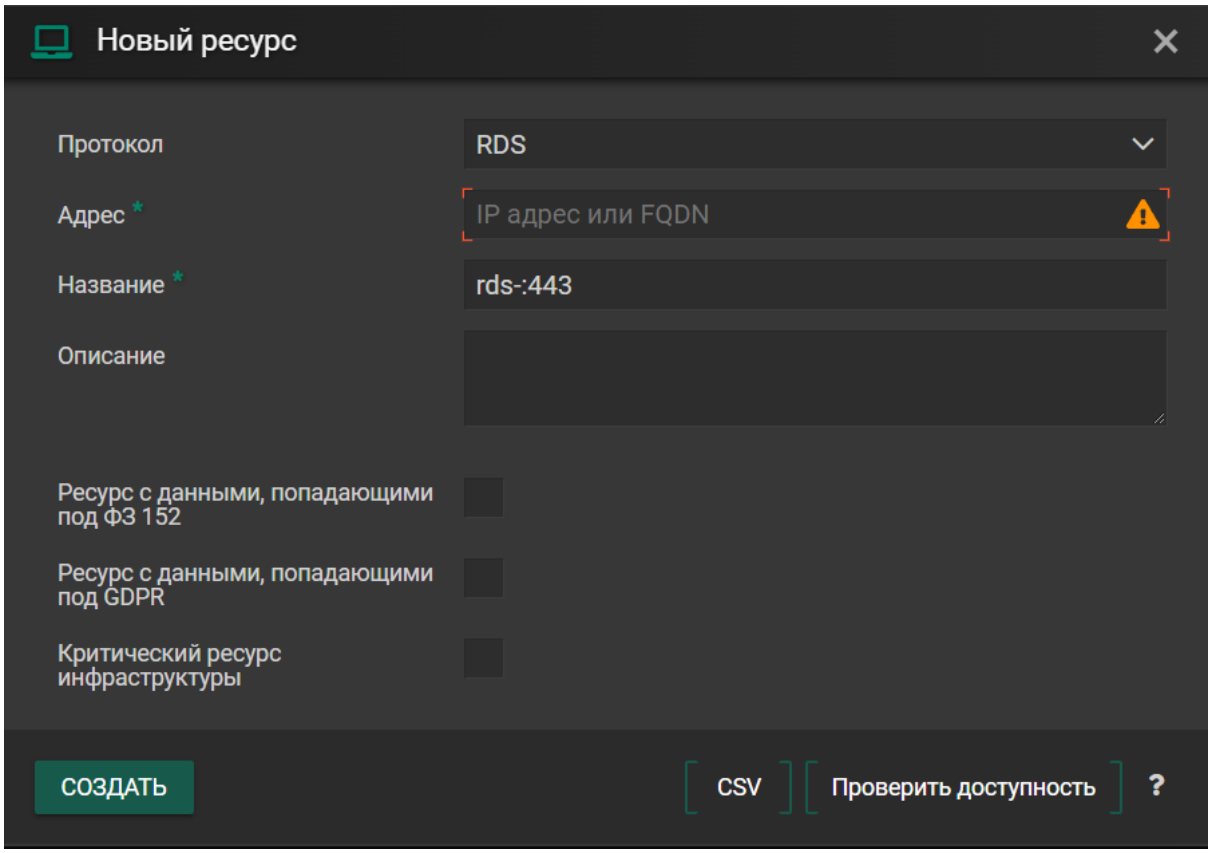


Рис. 3.35. Добавление нового ресурса (Протокол RDS)

SSH (Рис.3.36):

- **Адрес** – указать **IP–адрес** или **FQDN**;
- **Порт** – изменить при необходимости (значение по умолчанию **22**);
- **Название** – название ресурса формируется автоматически (при необходимости установить курсор в поле с названием ресурса и измените его);
- **Описание** – ввести описание ресурса (необязательное поле);
- **Ресурс с данными, попадающими под ФЗ 152** – установить флажок ☑, если ресурс содержит данные, попадающие под действие ФЗ–152;
- **Ресурс с данными, попадающими под GDPR** – установить флажок ☑, если ресурс содержит данные, попадающие под регламент защиты персональных данных **GDPR**;
- **Критический ресурс инфраструктуры** – установить флажок ☑, если ресурс является критическим ресурсом инфраструктуры.

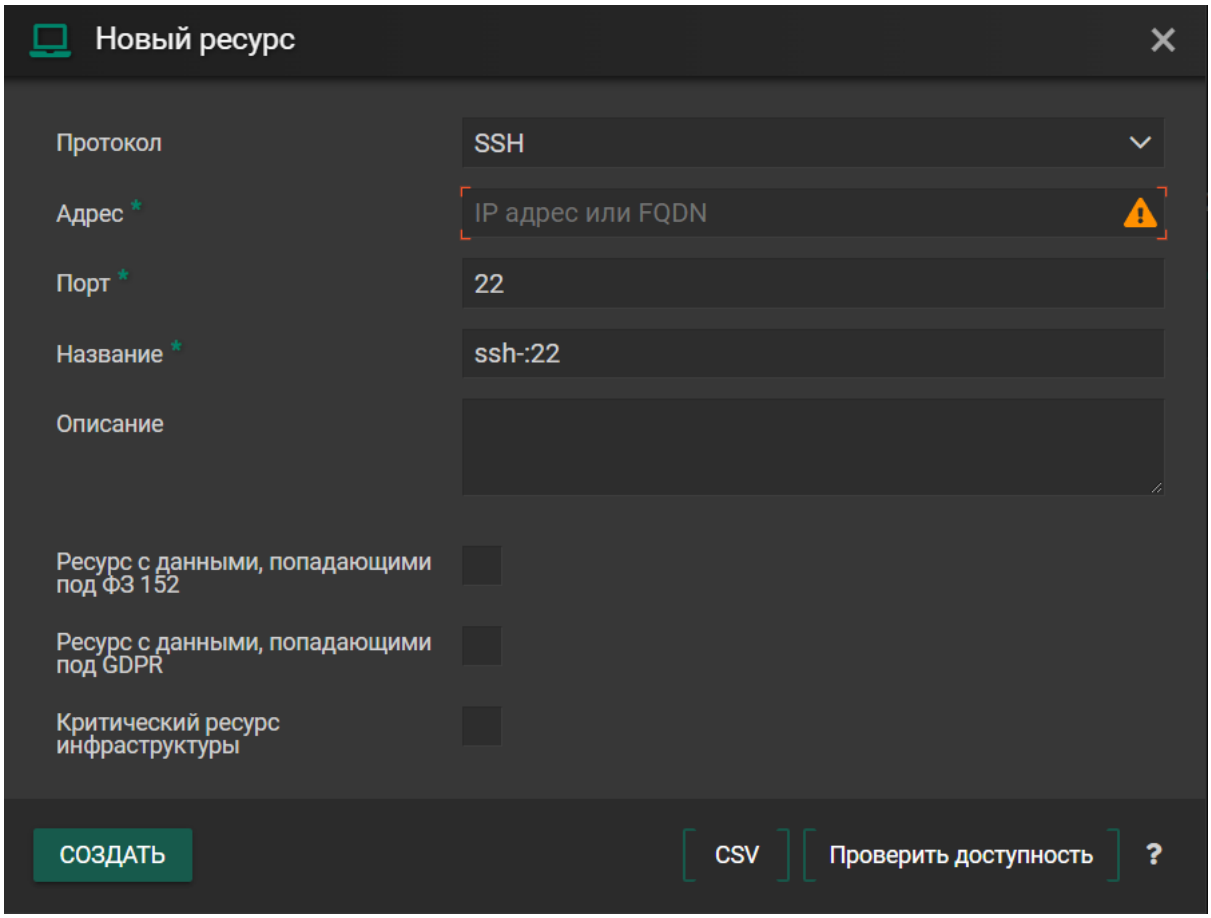


Рис. 3.36. Добавление нового ресурса (Протокол SSH)

HTTP / HTTPS (Рис.3.37) :

- **Адрес** – указать **IP–адрес** или **FQDN**;
- **Название** – название ресурса формируется автоматически (при необходимости установить курсор в поле с названием ресурса и измените его);
- **Описание** – ввести описание ресурса (*необязательное поле*);
- **Черный список** – ввести шаблоны **url** (построчно), не более 1000 символов;
- **Стратегия поиска элемента** – выбрать из выпадающего списка:
  - По атрибутам **ID** и **name**;
  - **XPath**;
  - **CSS** селектор.
- **Поле логина** – указать путь **html–элемента** на странице авторизации;
- **Поле пароля** – указать путь **html–элемента** на странице авторизации;
- **Двойное открытие вкладок при подключении (подробное описание в разделе 3.7.1.2);**

- **Повторное открытие страницы, для получения формы** – установить флажок при необходимости;
- **Basic-аутентификация** – установить флажок при необходимости;

Примечание

Стратегия поиска элемента**, поля **логин** и **пароль** будут проигнорированы системой, если установлен флажок **Basic-аутентификация.

- **Ресурс с данными, попадающими под ФЗ 152** – установить флажок, если ресурс содержит данные, попадающие под действие **ФЗ–152**;
- **Ресурс с данными, попадающими под GDPR** – установить флажок, если ресурс содержит данные, попадающие под регламент защиты персональных данных **GDPR**;
- **Критический ресурс инфраструктуры** – установить флажок, если ресурс является критическим ресурсом инфраструктуры.

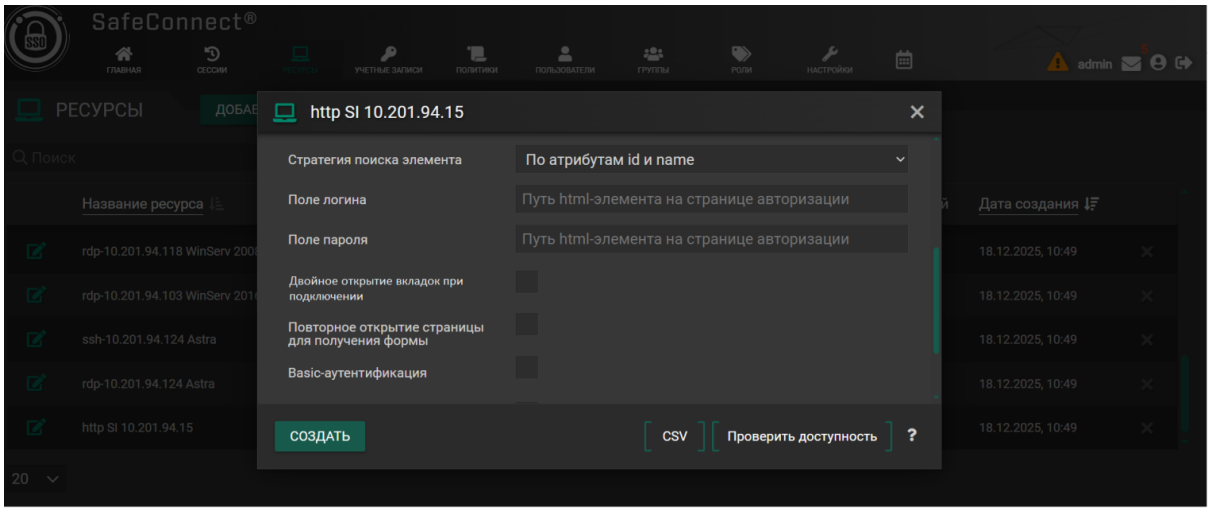


Рис. 3.37. Добавление нового ресурса (Протокол HTTP / HTTPS)

Telnet (Рис.3.38):

- **Адрес** – указать **IP–адрес** или **FQDN**;
- **Порт** – установлено значение по умолчанию **23** (изменить при необходимости);
- **Название** – название ресурса формируется автоматически (при необходимости установить курсор в поле с названием ресурса и измените его);
- **Описание** – ввести описание ресурса (*необязательное поле*);

- **Ресурс с данными, попадающими под ФЗ 152** – установить флажок, если ресурс содержит данные, попадающие под действие **ФЗ–152**;
- **Ресурс с данными, попадающими под GDPR** – установить флажок, если ресурс содержит данные, попадающие под регламент защиты персональных данных **GDPR**;
- **Критический ресурс инфраструктуры** – установить флажок, если ресурс является критическим ресурсом инфраструктуры.

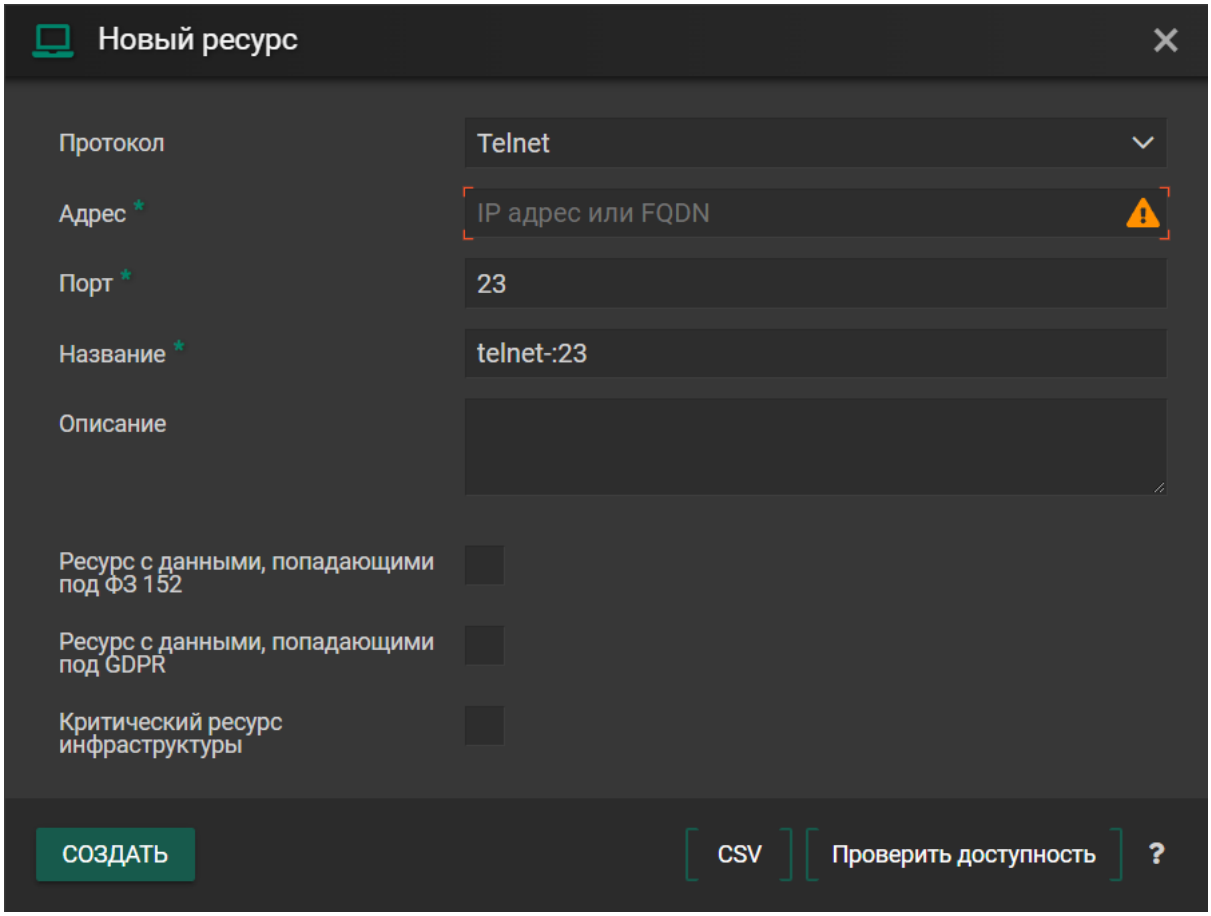


Рис. 3.38. Добавление нового ресурса (Протокол Telnet)

Предварительно можно проверить доступность создаваемого ресурса, нажав кнопку **Проверить доступность**. Если ресурс доступен, то рядом с кнопкой появится значок «галочка» .

Для формирования примера заполнения файла в формате *.csv заполнить используемые поля и нажать кнопку **CSV**. Далее будет сформирован пример (Рис.3.39).

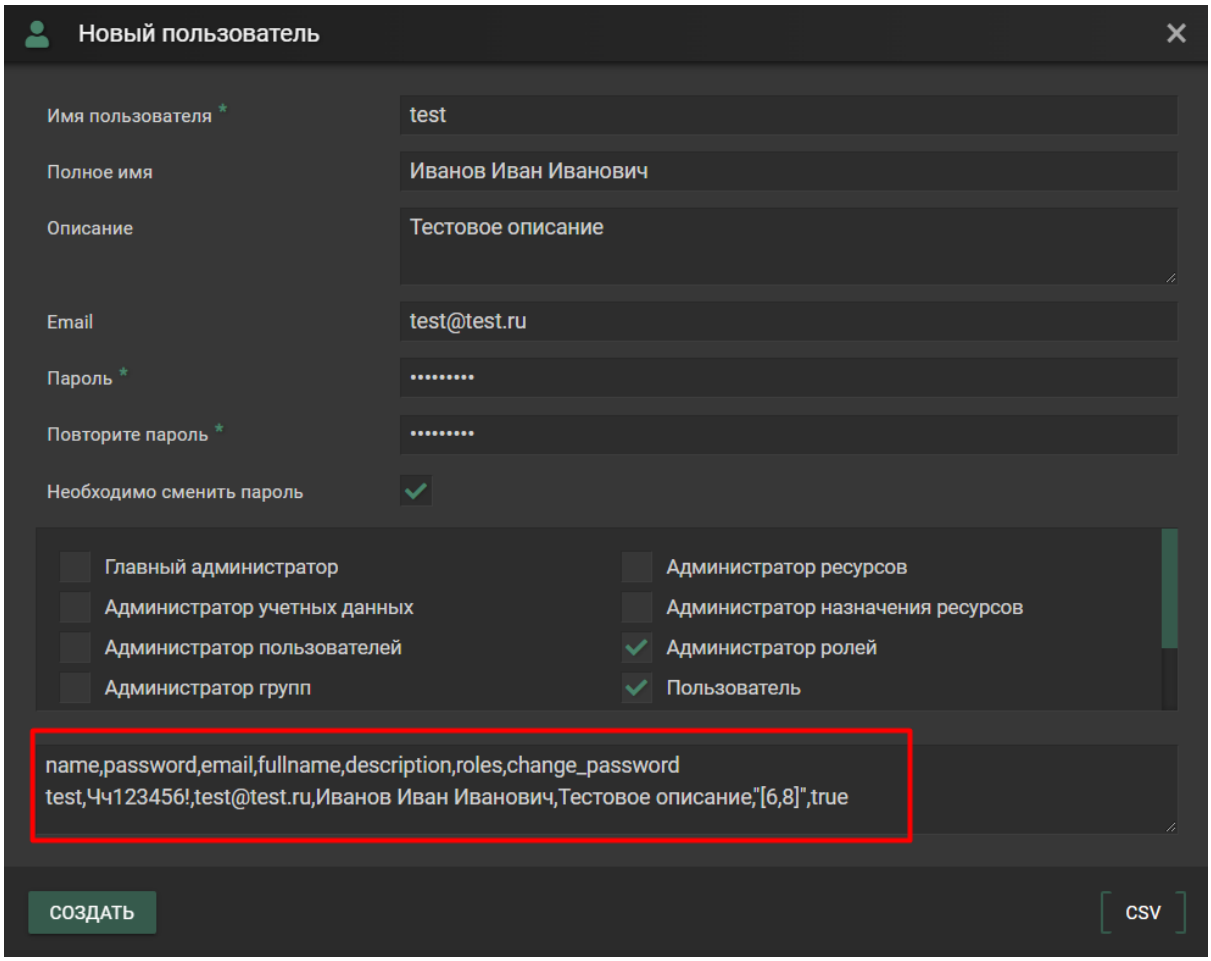


Рис. 3.39. Пример формирования csv–файла

Для завершения процесса создания следует нажать кнопку **Создать**. Информация о созданном ресурсе отобразится в списке ресурсов.

3.7.1.1. Добавление ресурсов из файла

В SafeConnect имеется возможность **загрузить ресурсы на портал из файла в формате *. csv**. Для этого следует нажать кнопку **Добавить из файла,** выбрать нужный файл и нажать кнопку **Открыть**. Ресурсы из файла отобразятся в **списке ресурсов**.

Пример заполнения файла для загрузки описан в Табл.3.1.

Табл. 3.1. Пример написания файла «Ресурсы» для загрузки

name	address	protocol	port	description	gdpr	fz152	critical	options
imported res #1 RDP	192.168.56.101	rdp	3389	rdp res desc	false	false	false	

Обозначения полей для загрузки:

- **Name** – название ресурса;
- **Address** – **IP–адрес** ресурса;
- **Protocol** – протокол (**RDP** / **RDP App** / **RDS** / **SSH** / **HTTP/HTTRS** / **Telnet**);

- **Port** – порт;
- **Description** – описание;
- **Gdpr** – ресурс с данными, подпадающими под **GDPR** (**true** – установить флажок, **false** – снять флажок);
- **fz152** – ресурс с данными, подпадающими под ФЗ–152 (**true** – установить флажок, **false** – снять флажок);
- **critical** – критический ресурс инфраструктуры (**true** – установить флажок, **false** – снять флажок);
- **options** – опциональное поле, может содержать дополнительные параметры (например, **черный список**, поля **логин** и **пароль** и т.д.).

3.7.1.2. Возможность работы с несколькими вкладками в HTTP/HTTPs-сессии

В SafeConnect реализована поддержка работы с **несколькими вкладками** в рамках **одного защищенного подключения** к веб-ресурсам. Функционал позволяет пользователю одновременно работать в нескольких вкладках без необходимости инициировать новые подключения к ресурсу (**Главная > Доступные ресурсы**).

Механизм работы:

- При запуске подключения к ресурсу система автоматически открывает интерфейс с поддержкой вкладок.
- Допускается одновременное открытие и существование **двух вкладок** в рамках одной пользовательской сессии.
- Переключение между вкладками осуществляется только с помощью стандартных сочетаний клавиш:

Табл. 3.2.

ОС	Комбинации клавиш	Действие
Windows / Linux	Ctrl + Tab	Переход к следующей вкладке
	Ctrl + PgDn	
	Ctrl + Shift + Tab	Переход к предыдущей вкладке
	Ctrl + PgUp	
	Ctrl + 1-2	Переход к вкладке по номеру
macOS	Cmd + Option + Стрелка вправо/влево	Переключение между вкладками
	Cmd + 1-2	Переход к вкладке по номеру

Настройка доступа:

- Возможность использования нескольких вкладок настраивается администратором в параметрах **конкретного HTTP/HTTPS ресурса**. По умолчанию поведение определяется политикой безопасности ресурса.
- Конфигурация выполняется в карточке ресурса SafeConnect: параметры ресурса **HTTP/HTTPS**, установить флажок **Двойное открытие вкладок при подключении.** По умолчанию данный флажок снят (пользователю доступна только одна вкладка).

- При включении опции система устанавливает жесткое ограничение – максимально возможное количество вкладок в одной сессии равно двум.

Данная настройка позволяет администратору самостоятельно решать, предоставлять ли пользователям расширенные возможности навигации или обеспечить строгий контроль над активностью сессий.

Интеграция с безопасностью и аудитом:

- **Интеграция SafeInspect и SafeConnect:** все действия во всех вкладках фиксируются в системе **SafeInspect**. Сессии отображаются в отчетах, статистике и журналах аудита наравне с обычными подключениями.
- **Передача данных:** полноценная поддержка работы с буфером обмена, а также загрузка и скачивание файлов доступны во всех открытых вкладках сессии.
- **Подтверждение доступа:** если подключение требует подтверждения (например, по заданию на доступ), оно запрашивается только **один раз** при инициализации сессии. Открытие двух вкладок в рамках этого соединения повторного подтверждения не требует.

3.7.1.3. Загрузка и скачивание файлов на HTTPS-ресурсе

В SafeConnect реализована возможность прямого обмена данными между хостовой машиной пользователя и целевым веб-ресурсом при подключении через SafeConnect. Ранее работа с ресурсом была ограничена только просмотром репозитория, теперь поддерживаются операции с файлами.

Внимание!

Все файлы, загруженные на ресурс или скачанные с него через встроенный файловый менеджер, являются временными. Они автоматически удаляются после завершения работы и отключения пользователя. При следующем подключении к ресурсу файловый менеджер будет пуст (история файлов не сохраняется).

Пользователи, подключающиеся к защищенным HTTPS–ресурсам, теперь могут выполнять стандартные действия:

- Загрузка файлов с локального компьютера на удаленный веб-ресурс.
- Скачивание файлов с ресурса на хостовую машину пользователя.

Для использования данного функционала, он должен быть явно разрешен администратором в **настройках ролей** SafeConnect (раздел **Роли**). Функционал обеспечен на уровне **Xrdp**-обработчика, обеспечивая прозрачную передачу данных внутри сессии.

Таким образом, расширен функционал SafeConnect, избавляющий пользователя от необходимости искать обходные пути для обмена файлами при работе с веб-интерфейсами критически важных ресурсов.

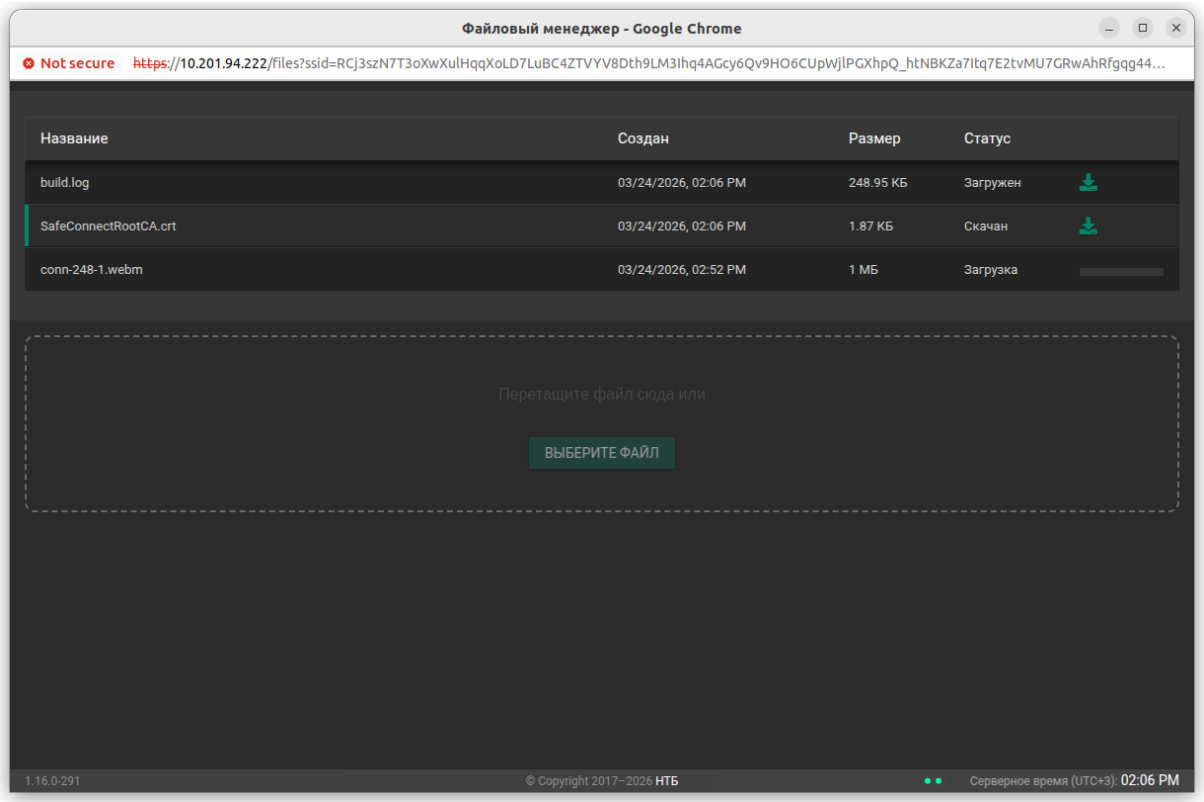


Рис. 3.40. Загрузка и скачивание файлов на HTTPs ресурсе

3.7.2. Редактирование ресурса

Чтобы внести изменения в настройки ресурса, следует перейти на вкладку **Ресурсы**, нажать на **значок редактирования** в строке редактируемого ресурса и в открывшемся окне с данными ресурса внести необходимые изменения (описание полей см. в разделе 3.7.1), проверить доступность ресурса, и нажать кнопку **Сохранить**.

3.7.3. Удаление ресурса

Для удаления ресурса следует перейти на вкладку **Ресурсы**, нажать на значок «крестик» в строке удаляемого ресурса, подтвердить удаление, нажав кнопку **ОК** в предупреждающем сообщении (Рис.3.41).

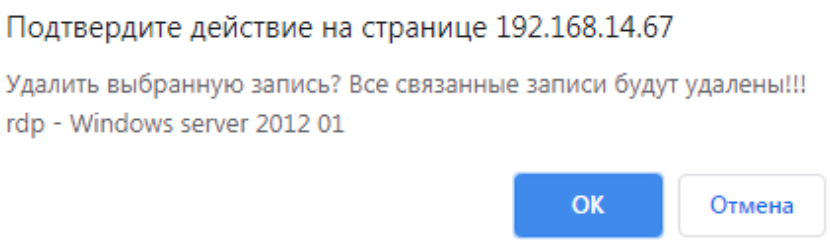


Рис. 3.41. Предупреждение при удалении ресурса

3.8. Раздел «Учетные записи»

Раздел **Учетные записи** (Рис.3.42) предназначен для управления списком учетных записей доступа к ресурсам. В рабочей области раздела отображается список всех учетных записей, зарегистрированных в SafeConnect. По каждой учетной записи отображается:

- **Имя** – присваивается автоматически, при создании учетной записи (также может указываться вручную);
- **Описание**;
- **Дата создания** – дата и время создания учетной записи.

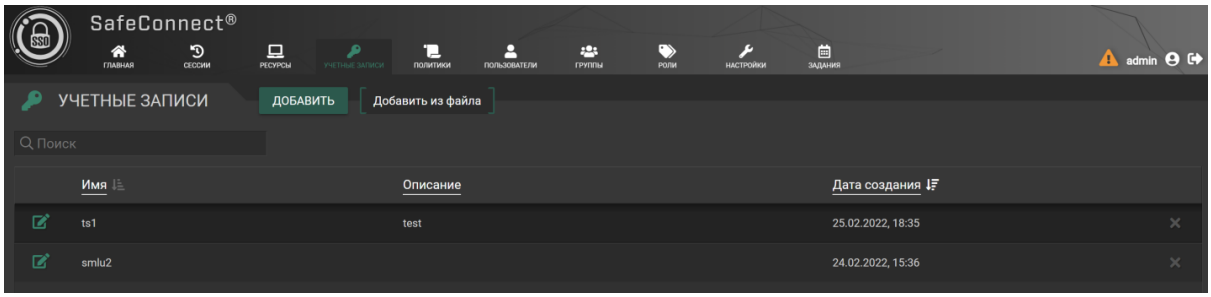


Рис. 3.42. Раздел «Учетные записи»

Для удобства пользователя имеется возможность фильтрации учетных записей по имени. Для этого в поле **Поиск** (Рис.3.43) следует ввести **имя** или его часть, и в списке останутся только те учетные записи, которые удовлетворяют заданному значению.

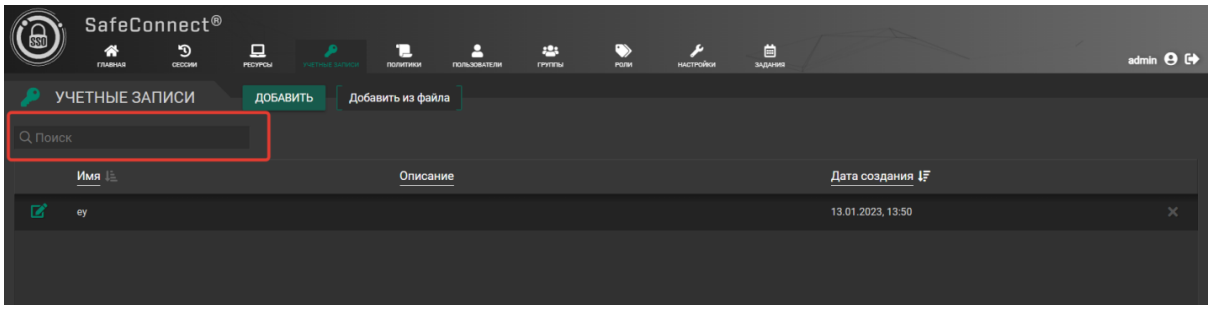


Рис. 3.43. Поиск в разделе «Учетные записи»

3.8.1. Добавление учетной записи

Для добавления в список новой учетной записи следует перейти на вкладку **Учетные записи**, нажать кнопку **Добавить** и заполнить поля формы (Рис.3.44):

- **Логин**;
- **Пароль** – задать пароль;
- **Повторите пароль**;
- **Название** – формируется автоматически (при необходимости установить курсор в поле с названием учетной записи и изменить его);
- **Описание** – необязательный параметр.

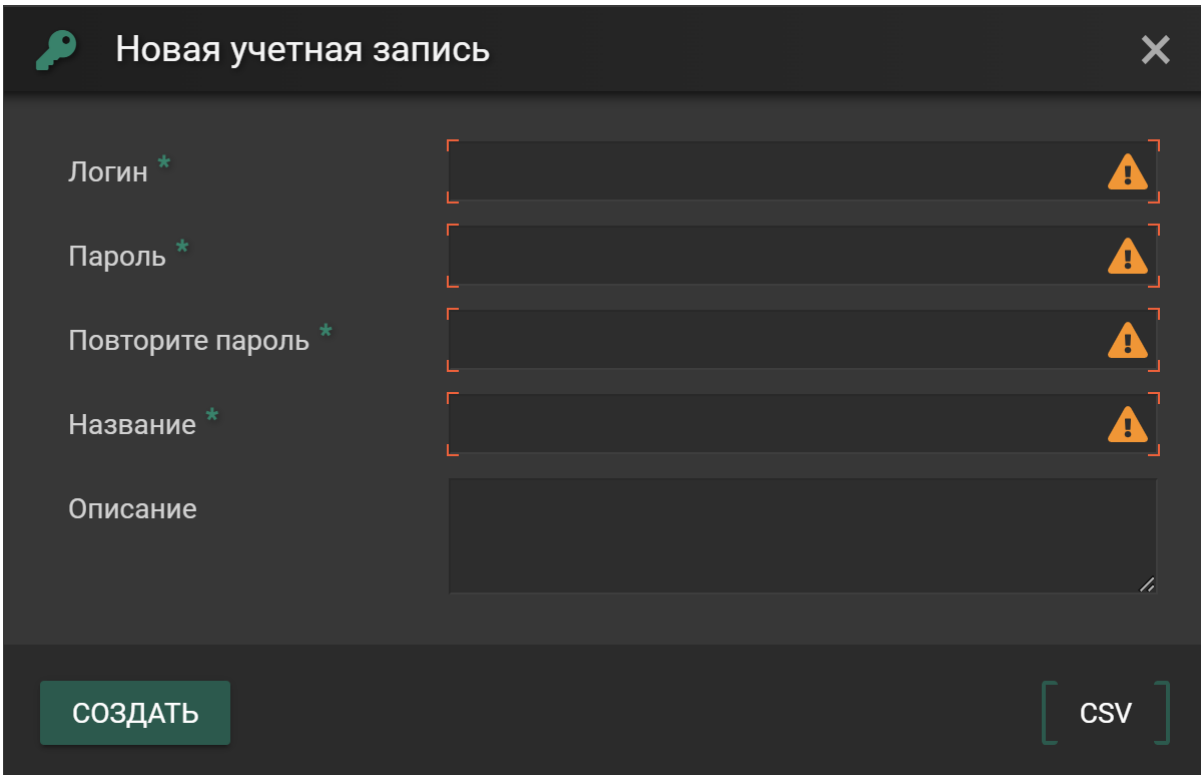


Рис. 3.44. Создание новой учетной записи

Для формирования примера заполнения файла в формате *.csv заполнить используемые **поля** и нажать кнопку **CSV**. Далее будет сформирован пример (Рис.3.45).

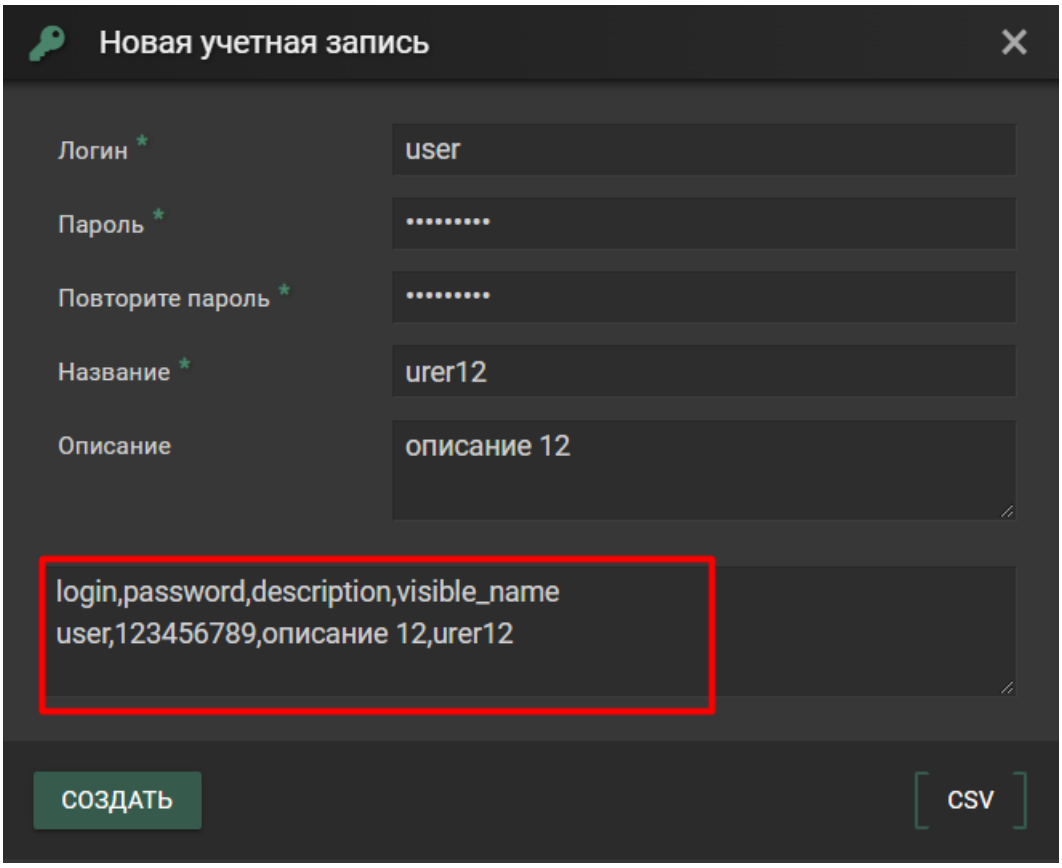


Рис. 3.45. Пример формирования csv–файла

Для завершения нажать кнопку **Создать**, учетная запись появится в списке.

Примечание

*Также имеется возможность загрузить учетные записи на портал из файла в формате *.csv. Для этого следует нажать кнопку **Добавить из файла,** выбрать нужный файл и нажать кнопку **Открыть**. Учетные записи из файла отобразятся в списке учетных записей. Пример создания файла для загрузки представлен в таблице (Табл.3.33).*

Табл. 3.3. Пример написания файла «Учетные записи» для загрузки

login	password	description	visible_name
root	qwerty	description 123	r00t
creds_2	123	description 2	

Примечание

*Если значение **visible_name** оставить пустым, оно будет сгенерировано из параметра **login**.*

Описание полей файла для загрузки:

- **Login** – логин учетной записи;

- **Password** – пароль;
- **Description** – описание;
- **visible _ name** – название (имя) учетной записи.

3.8.2. Редактирование учетной записи

Чтобы внести изменения в учетную запись, следует:

1. Перейти на вкладку **Учетные записи**;
2. Нажать кнопку редактирования в строке редактируемой учетной записи;
3. В открывшейся форме с данными учетной записи внести необходимые изменения;
4. Нажать кнопку **Сохранить**.

3.8.3. Удаление учетной записи

Для удаления учетной записи следует перейти на вкладку **Учетные записи**, нажать кнопку удаления в строке удаляемой учетной записи, подтвердить удаление, нажав кнопку **ОК** в предупреждающем сообщении (Рис.3.46).

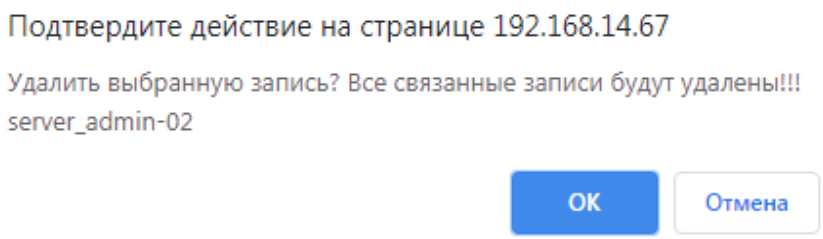


Рис. 3.46. Подтверждение удаления учетной записи

3.9. Раздел «Политики»

Раздел **Политики** (Рис.3.47) предназначен для управления политиками доступа к ресурсам. В рабочей области расположена таблица, содержащая все настроенные на портале политики доступа. По каждой политике в таблице отображается следующая информация:

- **Название политики**;
- **Длительность сессии** – максимальная длительность одной сессии;
- **Время доступа** – время, в которое ресурс будет доступен для использования;
- **Расписание** – время, в которое будет доступен ресурс;
- **SafeInspect** – если настроена интеграция с SafeInspect, отображается его **IP–адрес**;
- **Требовать подтверждения** – требуется подтверждение от администратора при открытии каждой новой сессии.

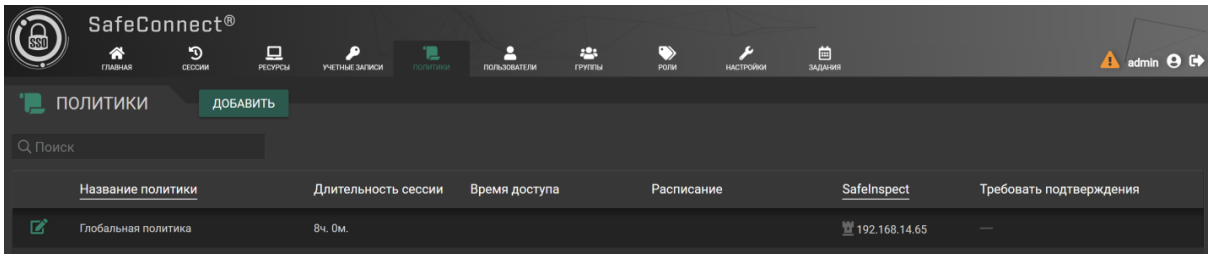


Рис. 3.47. Раздел «Политики»

Для удобства пользователя имеется возможность фильтрации списка политик по названию. Для этого в поле **Поиск** (Рис.3.48) следует ввести название политики или его часть (с учетом регистра), и в списке останутся только те учетные записи, которые удовлетворяют заданному значению.

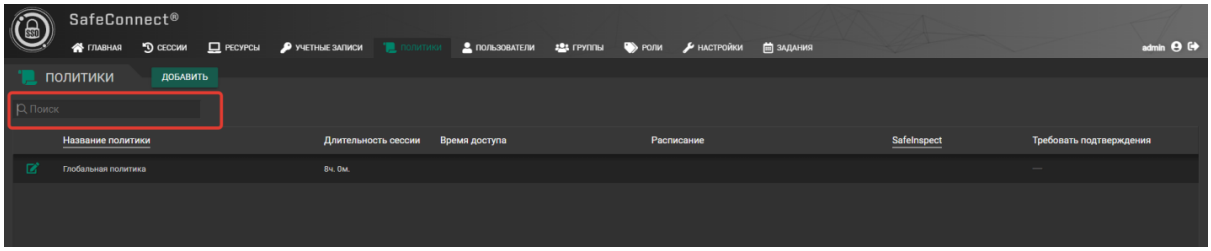


Рис. 3.48. Поиск в разделе «Политики»

3.9.1. Создание политики

Для создания новой политики следует перейти в раздел **Политики**, нажать кнопку **Добавить** и заполнить поля формы (Рис.3.49):

- **Название политики** – ввести название политики;
- **RADIUS сервер для 2 FA доступа к сессиям** – **RADIUS–сервер**, используемый для подтверждения доступа к сессиям;
- **Принудительное разрешение экрана –** выбрать значение из выпадающего списка:
  - 1024x768;
  - 1280x720;
  - 1280x1024;
  - 1600x900;
  - 1920x1080.
- **SafeInspect Бастион** – если настроено подключение через коллектор SafeInspect в режиме Бастион, установить из выпадающего списка его **IP–адрес**;

Внимание!

*При указании в политике адреса **SafeInspect Бастион**, подключения **HTTP(S)** фактически будут устанавливаться **напрямую** с SafeConnect до целевой системы. На SafeInspect в данном случае будут переданы **только данные сессий** для возможности воспроизводить сессию как видео.*

- **Максимальная длительность сессии** – указать максимальную длительность одной сессии. Чтобы задать длительность сессии без ограничения, следует указать значение **0**;
- **Короткое имя доменного пользователя при сквозной авторизации** – установить флажок , чтобы использовать короткое имя доменного пользователя при сквозной авторизации (без @domain);
- **Требовать подтверждения** – установить флажок , если требуется подтверждение от администратора при открытии каждой новой сессии;
- **Время доступа** – можно указать один или несколько диапазонов дат в формате гг-гг–мм–дд чч:мм:сс (Рис.3.49), в которые ресурс будет доступен для использования. Для добавления диапазона следует нажать кнопку **Добавить**. Для удаления диапазона следует нажать на значок «крестик» ;
- **Расписание** – задать одно или несколько расписаний (Рис.3.49), в которые ресурс будет доступен для использования. Для добавления расписания следует нажать кнопку **Добавить**. Для удаления расписания следует нажать на значок «крестик» .

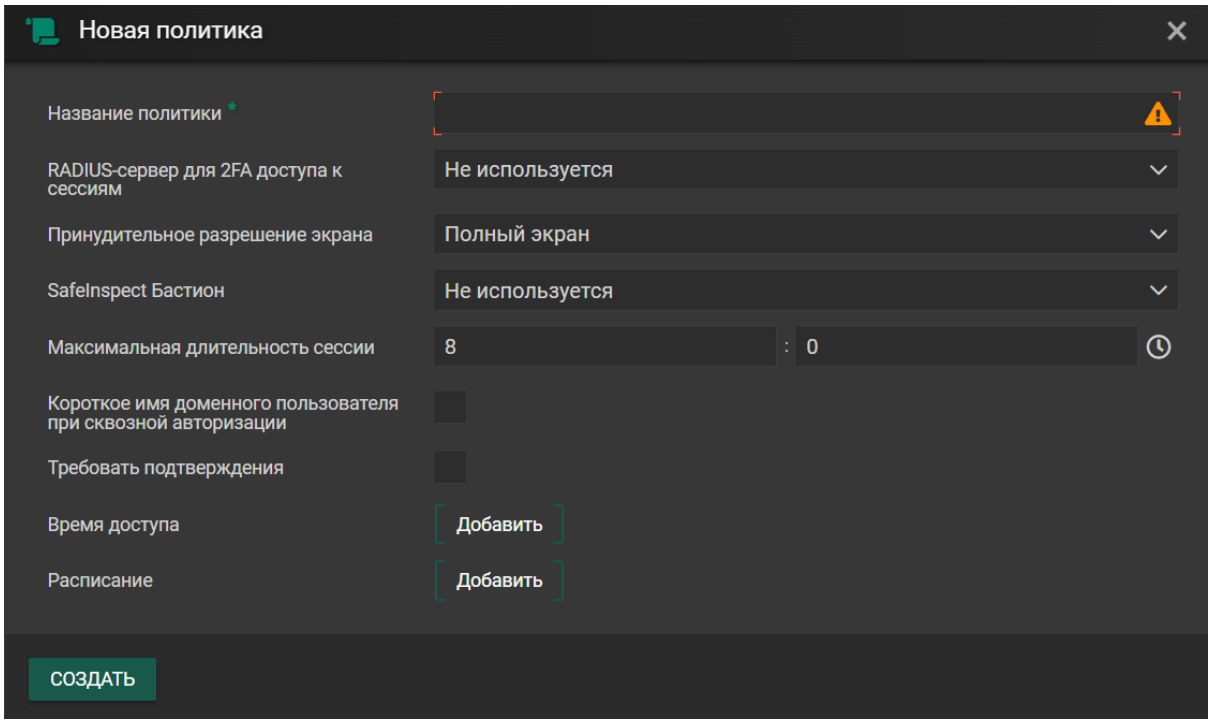


Рис. 3.49. Добавление новой политики

Пример настройки расписания:

- 10 1–20* 1,2,5 2019,2020 – это означает, что доступ к ресурсу разрешен с 10 утра, с 1 по 20 число каждого месяца, каждый понедельник, вторник и пятницу в 2019 и 2020 году.

Для удобства настройки расписания нажать в поле расписания и заполнить следующие поля (Рис.3.50):

- **Часы** – указать время начала работы (Табл.3.5);

Табл. 3.4. Форматы поля «Часы» при настройке расписания

Значение	Описание
0–23	Допустимые значения, где 0 – полночь
*	Все значения (любой час)
,	Список значений (например, *2,14,16* - означает, что время начала работы начинается в 2 часа ночи, в 14 часов дня и в 16 часов вечера)
–	Диапазон значений (допускаются также значения вида **10–11,20–21)** (например, *11–14* - означает, что время начала работы начинается в 11, 12, 13 и 14 часов дня)
/	Шаг значений в диапазоне (например, **/4* – означает каждые 4 часа; *0–20/2* – означает каждые 2 часа в диапазоне от 0 до 20 часов)

- **Числа** – указать число месяца (Табл.3.55);

Табл. 3.5. Форматы поля «Числа» при настройке расписания

Значение	**Описание**
1–31	Допустимые значения
*	Все значения (любой день месяца)
,	Список значений (например, *2,15* – означает второго и пятнадцатого числа)
–	Диапазон значений (допускаются значения вида **10–11,20–21**) (например, *1–5* – означает 1, 2, 3, 4 и 5 числа месяца)
/	Шаг значений в диапазоне (например, **/4* – означает каждые 4 дня; *1–20/2* – означает каждые 2 дня в диапазоне с 1 по 20 число)

- **Мес. (Месяцы)** – указать месяц (Табл.3.7);

Табл. 3.6. Форматы поля «Месяц» при настройке расписания

Значение	**Описание**
1–12	Допустимые значения
*	Все значения (любой месяц)
,	Список значений (например, *2,6* – означает февраль и июнь)
–	Диапазон значений, допускаются значения вида **2–5,7–12** (например, *1–3* – означает январь, февраль и март)
/	Шаг значений в диапазоне (например, **/4* – означает каждые 4 месяца; *1–8/2* – означает каждые 2 месяца в диапазоне с января по август)

- **ДН (Дни недели)** – указать дни недели (Табл.3.7);

Табл. 3.7. Форматы поля «Дни недели» при настройке расписания

Значение	**Описание**
1–7	Допустимые значения, где:

	1 – понедельник; 2 – вторник; 3 – среда; 4 – четверг; 5 – пятница; 6 – суббота; 7 – воскресенье
*	Все значения (любой день недели)
,	Список значений (например, *1,2* – означает понедельник и вторник)
–	Диапазон значений, допускаются значения вида **1–3,5–7** (например, *5–7* – означает с пятницы по воскресенье)
/	Шаг значений в диапазоне (например, **/4* – означает каждые 4 дня; *1–5/2* – означает каждые 2 дня между понедельником и пятницей)

- **Годы** – указать год (годы) (Табл.3.8);

Табл. 3.8. Форматы поля «Годы» при настройке расписания

Значение	Описание
1970–2099	Допустимые значения
*	Все значения (любой год)
,	Список значений (например, *2018,2019* – означает 2018 и 2019 годы)
–	Диапазон значений (например, *2018–2020* – означает 2018, 2019 и 2020)
/	Шаг значений в диапазоне (например, **/4* – означает каждые 4 года; *2018–2022/2* – означает каждые два года с 2018 по 2022 год)

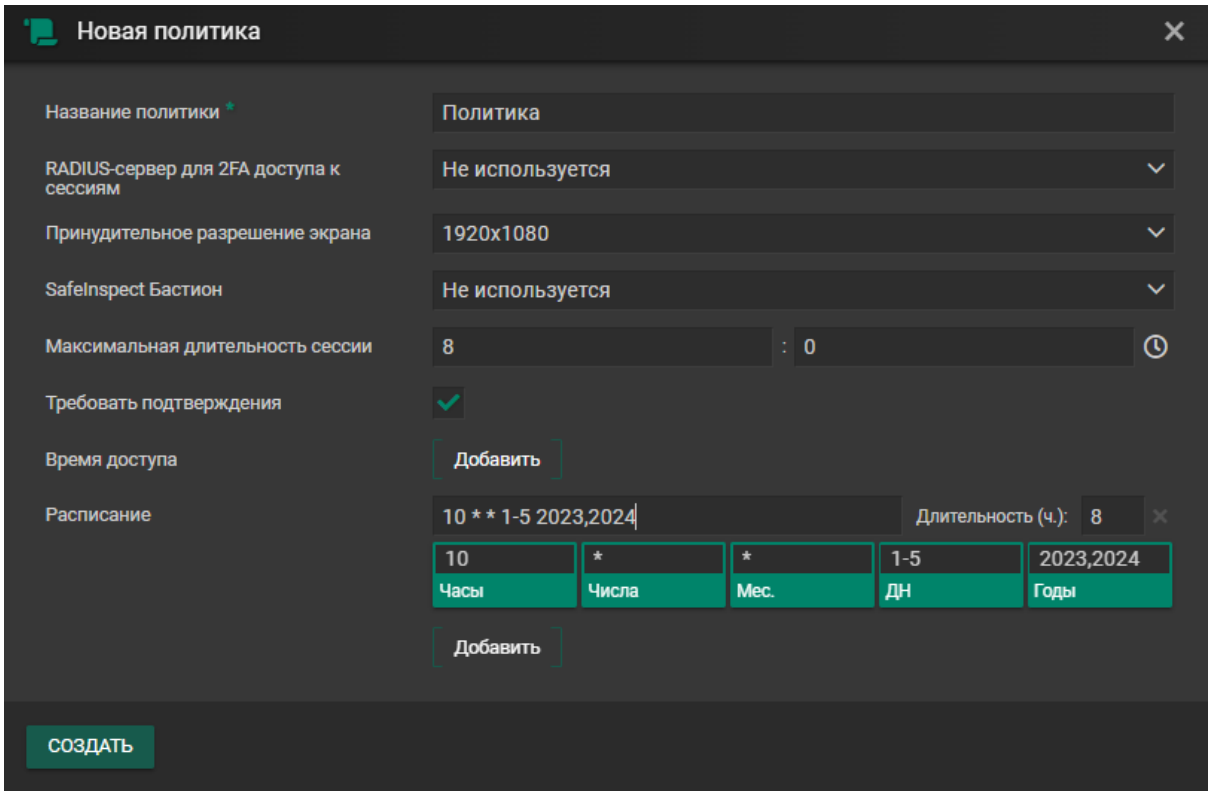


Рис. 3.50. Назначение расписания

Нажать кнопку **Создать**, после этого созданная политика отобразится в таблице.

3.9.2. Редактирование политики

Чтобы внести изменения в политику, следует перейти на вкладку **Политики** нажать кнопку в строке редактируемой политики и в открывшейся форме с параметрами политики внести необходимые изменения и нажать кнопку **Сохранить**.

3.9.3. Удаление политики

Для удаления политики следует перейти на вкладку **Политики** нажать кнопку в строке удаляемой политики подтвердить удаление, нажав кнопку **ОК** в предупреждающем сообщении (Рис.3.51).

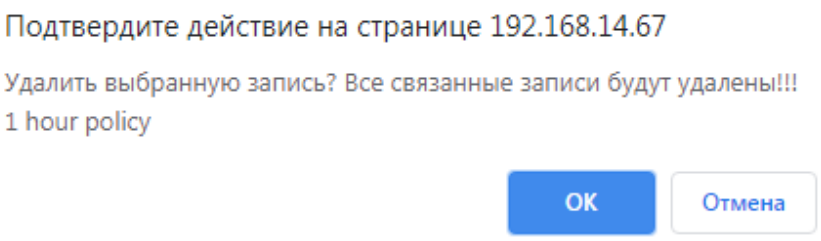


Рис. 3.51. Подтверждение удаления политики

3.10. Раздел «Пользователи»

Раздел **Пользователи** предназначен для управления списком пользователей Портала.

В **рабочей области** расположена таблица, в которой содержится информация по всем пользователям, заведенным в SafeConnect (Рис.3.52).

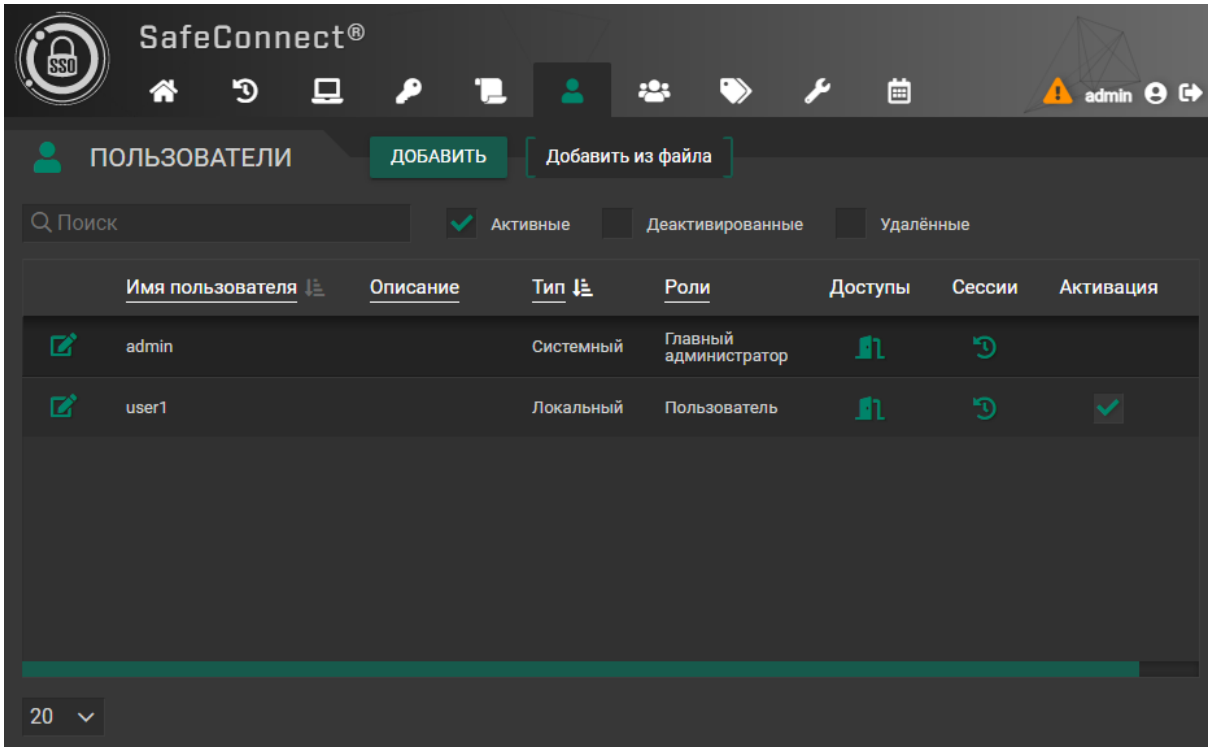


Рис. 3.52. Раздел «Пользователи»

По каждому пользователю отображается следующая информация:

- **Имя пользователя** – логин пользователя;
- **Описание** – отображается описание пользователя;
- **Тип** – тип пользователя: системный или локальный;
- **Роли** – отображаются назначенные пользователю полномочия;
- **Доступы** – при нажатии на иконку открывается список ресурсов, доступных пользователю;
- **Сессии** – сессии пользователя. При нажатии на иконку открываются сессии пользователя;
- **Активация** – позволяет активировать или заблокировать пользователя;
- **Удаление пользователя** по нажатию на значок «крестик» и последующем подтверждении удаления в предупреждающем сообщении.

3.10.1. Добавление пользователя

Для добавления пользователя на Портал следует перейти на вкладку **Пользователи**, нажать кнопку **Добавить** и заполнить поля формы (Рис.3.53):

- **Имя пользователя** – логин пользователя для входа на Портал;
- **Полное имя пользователя** – дополнительное поле для указания ФИО пользователя;
- **Описание** – при необходимости ввести дополнительную информацию о пользователе (например, организация, должность);
- **Email** – дополнительное поле для ввода адреса электронной почты пользователя;
- **Пароль** – задать пароль для учетной записи пользователя в соответствии с парольной политикой;
- **Повторите пароль** – повторно ввести пароль;
- **Необходимо сменить пароль** – установить флажок , если требуется смена пароля при следующем доступе;
- **Список ролей** – установить флажки ролей, назначенные пользователю:
  - **Главный администратор** – имеет полный набор прав;
  - **Администратор учетных данных** – управление учетными данными;
  - **Администратор пользователей** – создание и редактирование пользователей;
  - **Администратор групп** – создание и редактирование групп;
  - **Привилегированный пользователь** – доступ к сессиям с подтверждением;
  - **Администратор политик** – создание и редактирование политик;
  - **Администратор ресурсов** – управление ресурсами;
  - **Администратор назначения ресурсов** – назначение пользователям доступа к ресурсам;
  - **Администратор ролей** – создание и редактирование ролей;
  - **Пользователь**;
  - **Администратор доступа** – подтверждение запроса на доступ.

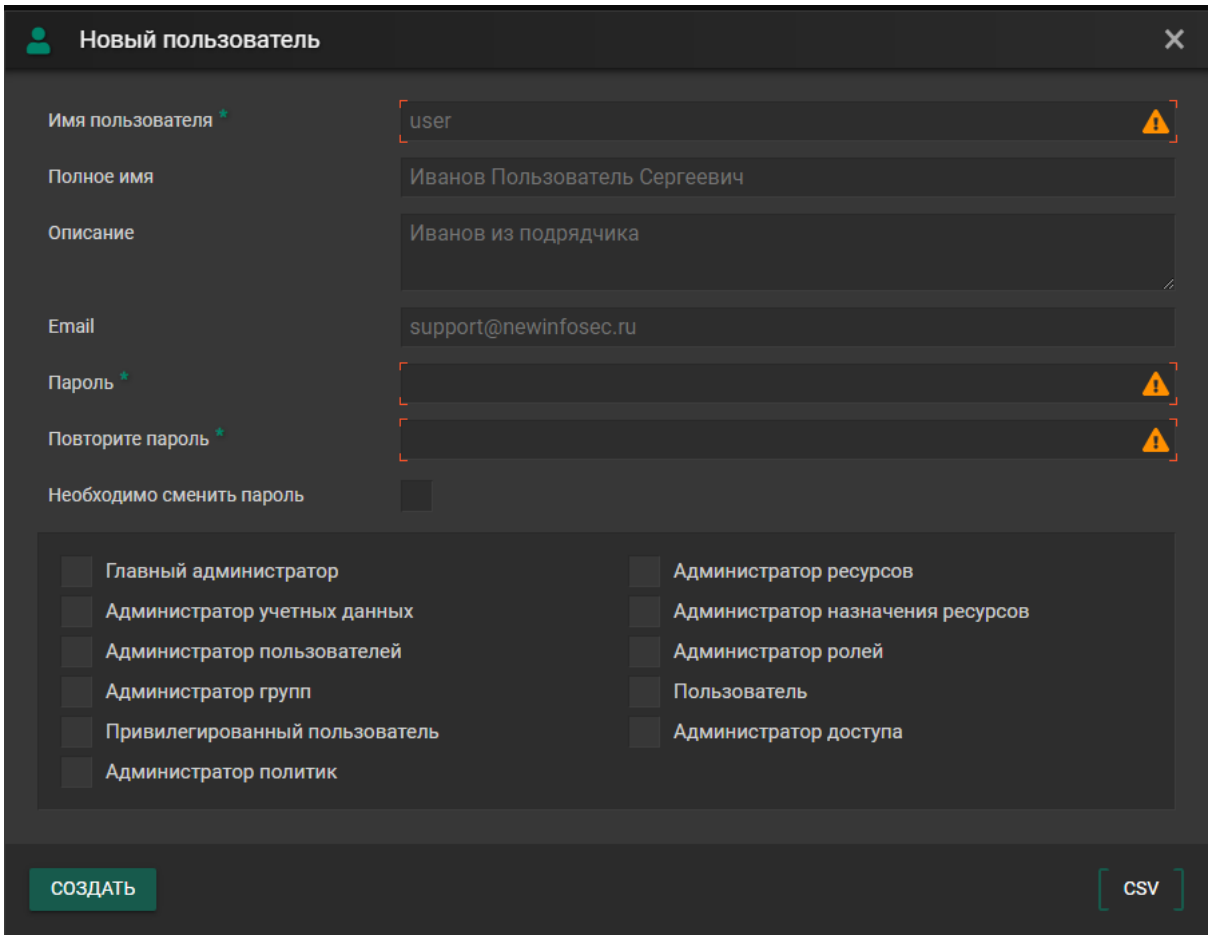


Рис. 3.53. Добавление пользователя

Для формирования примера заполнения файла в формате *.csv заполнить используемые поля и нажать кнопку **CSV**. Далее будет сформирован пример (Рис.3.54).

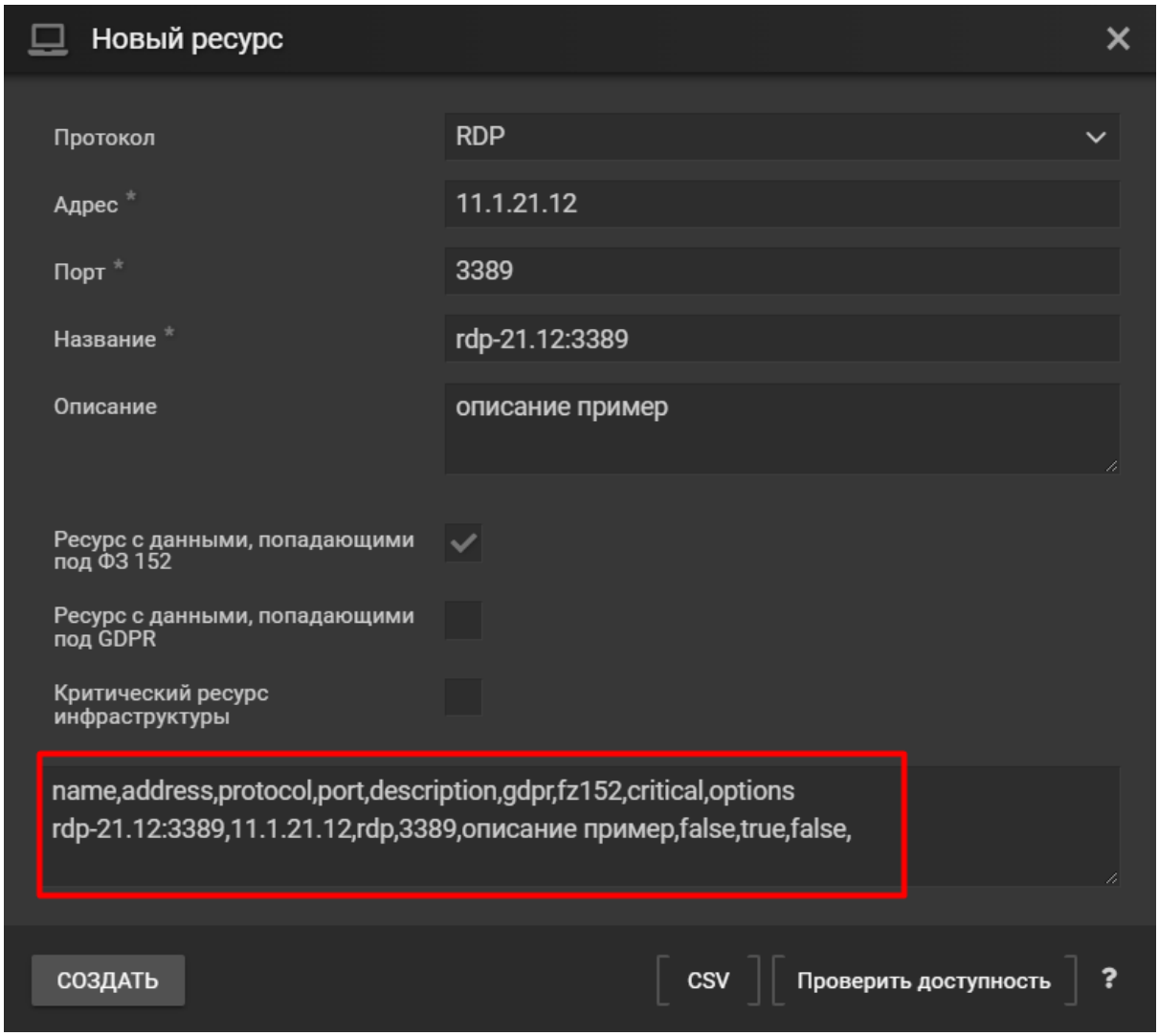


Рис. 3.54. Пример формирования csv–файла

Нажать кнопку **Создать**, информация о пользователе отобразится в таблице.

Примечание

Если на Портале настроена интеграция с SafeInspect, то следует убедиться, что SafeInspect доступен, иначе при создании пользователя будет выдана ошибка ***Не удалось добавить пользователя в SI****.*

Также имеется возможность загрузить пользователей на Портал из файла в формате ***.csv**. Для этого на вкладке **Пользователи** следует нажать кнопку **Добавить из файла,** выбрать нужный файл и нажать кнопку **Открыть**. Пользователи из файла отобразятся в таблице раздела **Пользователи**. Пример создания файла с пользователями описан в таблицах (пример – Табл.3.10, описание полей – Табл.3.1010).

Табл. 3.9. Пример написания файла «Пользователи» для загрузки

name	password	email	fullname	description	roles	change_ password
imported_user_7	Ss123456!!	Iii001@mail.com	Ivanov Ivan Ivanovich	Description1	[5]	1
imported_user_8	Ss123456!!	Ppp001@mail.com	Petrov Petr Petrovich	Description2	[10,11]	1
imported_user_9	Ss123456!!	Ppp002@mail.com	Pavlov Pavel Pavlovich	Description3	[1,2]	0

Табл. 3.10. Описание полей файла «Пользователи»

Название поля	Описание
name	Имя пользователя
password	Пароль пользователя (в соответствии с заданной парольной политикой)
email	Электронный адрес пользователя
fullname	Полное имя пользователя
description	Описание
roles	Роли пользователя в формате [1,2,3…], допустимые значения и их описание: 1 – Главный администратор – имеет полный набор прав; 2 – Администратор ресурсов – управление ресурсами; 3 – Администратор учетных данных – управление учетными данными; 4 – Администратор назначения ресурсов – назначение пользователям доступа к ресурсам; 5 – Администратор пользователей – создание и редактирование пользователей; 6 – Администратор ролей – создание и редактирование ролей; 7 – Администратор групп – создание и редактирование групп; 8 – Пользователь; 9 – Привилегированный пользователь – доступ к сессиям с подтверждением; 10 – Администратор доступа – подтверждение запроса на доступ; 11 – Администратор политик – создание и редактирование политик.
change_password	Установить флажок **Необходимо сменить пароль**, допустимые значения: 1 – да, включить; 0 – нет, оставить выключенным.

3.10.2. Редактирование данных пользователя

Чтобы внести изменения в данные пользователя, следует перейти в раздел **Пользователи**, нажать кнопку редактирования  в строке редактируемого пользователя, затем в открывшейся форме с данными пользователя внести необходимые изменения. По завершению редактирования необходимо нажать кнопку **Сохранить**.

3.10.3. Удаление пользователя

Для удаления пользователя следует перейти в раздел **Пользователи**, нажать на значок «крестик»в строке удаляемого пользователя, подтвердить удаление, нажав кнопку **ОК** в предупреждающем сообщении (Рис.3.55).

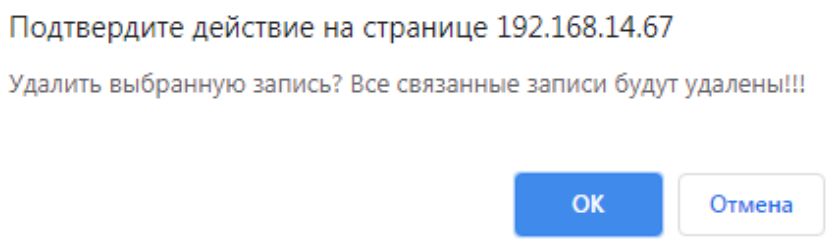


Рис. 3.55. Подтверждение удаления пользователя

Примечание

*Роль **Суперадминистратор** – это пользователь, созданный при установке Портала. **Супер-администратор** является главным администратором с максимальными полномочиями. Эту роль нельзя удалить, заблокировать или изменить полномочия.*

3.11. Раздел «Группы»

Раздел **Группы** предназначен для ведения списка групп пользователей Портала. Если имеется несколько пользователей с равными правами доступа к определенному ресурсу, можно их объединить в группу и настроить доступ к ресурсу для группы, чтобы не заводить отдельно каждого пользователя, настраивая его доступы.

В **рабочей области** раздела отображается таблица со списком групп пользователей. Для каждой группы указывается название и описание группы (Рис.3.56).

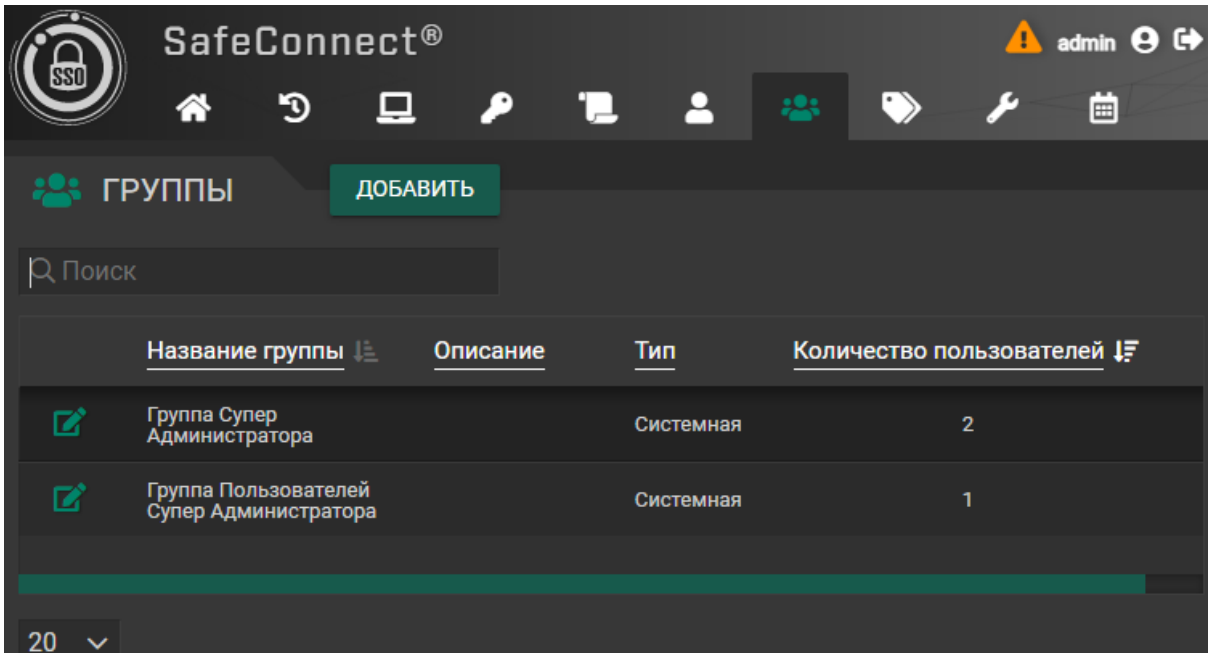


Рис. 3.56. Раздел «Группы»

Для удобства пользователя имеется возможность фильтрации списка групп по названию. Для этого в поле **Поиск** (Рис.3.57) следует ввести название группы или его часть (с учетом регистра), и в списке останутся только группы, которые удовлетворяют заданному значению.

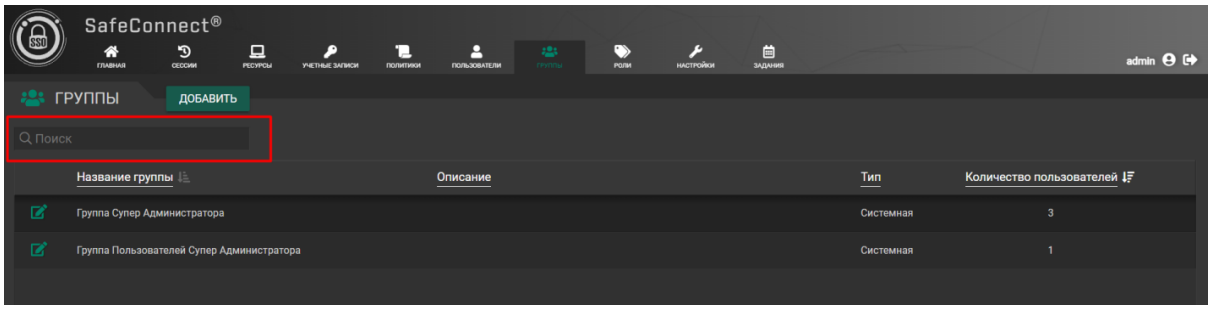


Рис. 3.57. Поиск по разделу «Группы»

Для групп пользователей в таблице отображается:

- **Название группы;**
- **Описание;**
- **Тип;**
- **Количество пользователей**.

Имеется возможность добавления и редактирования групп.

3.11.1. Создание группы

Для добавления группы пользователей следует перейти в раздел **Группы** и заполнить поля формы (Рис.3.58):

- **Название** – название группы;
- **Описание** – дополнительное поле для ввода описание группы;
- **Пользователи** – добавление пользователей из списка в состав группы.

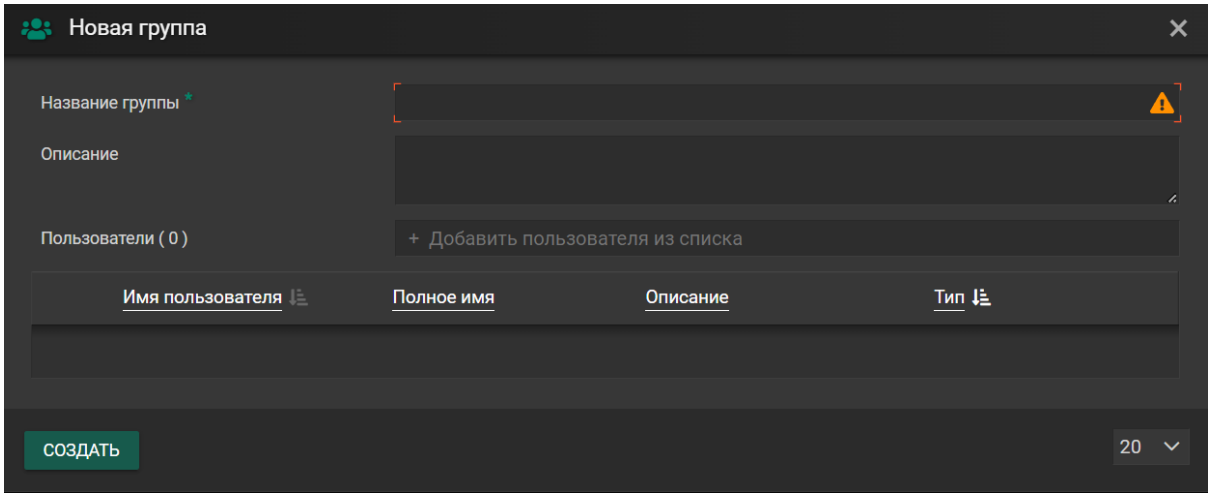


Рис. 3.58. Создание группы

После заполнения формы нажать кнопку **Создать**, группа появится в списке групп.

Примечание

Группы из добавленного LDAP–сервера создаются автоматически при добавлении LDAP–сервера.

3.11.2. Добавление пользователей в группу

Для добавления пользователей в группу нужно нажать на значок редактирования в соответствующей строке и в форме **Добавление группы** (Рис.3.58) поместить курсор в поле **Пользователи** и выбрать пользователя в выпадающем списке. После добавления пользователей в группу нажать кнопку **Сохранить**.

Примечание

LDAP–пользователей в другие LDAP–группы добавить нельзя.

3.11.3. Редактирование группы

Для редактирования группы следует перейти в раздел **Группы**, нажать кнопку редактирования в строке редактируемой группы и в открывшейся форме внести необходимые изменения и нажать кнопку **Сохранить**.

При редактировании группы можно изменить информацию о группе, добавить или удалить пользователей из группы, отредактировать личные данные пользователей.

Чтобы внести изменения в личные данные пользователя, следует нажать кнопку редактирования в строке выбранного пользователя в составе группы. Чтобы удалить пользователя из группы, следует нажать на значок «крестик» в соответствующей строке.

3.11.4. Удаление группы

Удалить можно только локальную группу, системную группу удалить нельзя.

Для удаления группы следует перейти в раздел **Группы**, нажать на значок «крестик» в строке удаляемой группы, подтвердить удаление, нажав кнопку **ОК** в предупреждающем сообщении (Рис.3.59) .

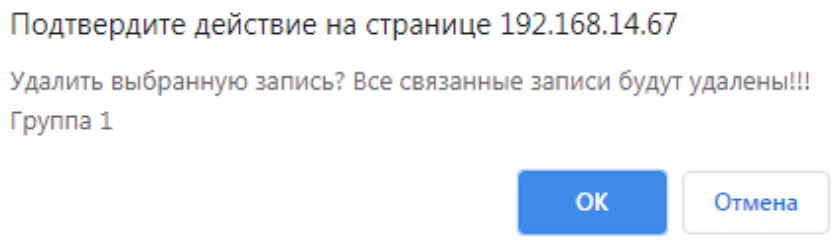


Рис. 3.59. Подтверждение удаления группы

Примечание

Группы, в состав которых входит суперадминистратор, нельзя удалить. Также нельзя удалить ***LDAP–группы****.*

3.12. Раздел «Роли»

Роли – это наборы полномочий, определяющих права пользователя на доступ к ресурсам. Когда пользователю назначена роль, он получает все полномочия, определенные в данной роли. Пользователю может быть назначено несколько ролей.

Раздел **Роли** предназначен для управления списком ролей. В рабочей области раздела расположена таблица, содержащая список всех ролей, настроенных на Портале. По каждой роли отображается название роли, описание, дата и время создания (Рис.3.60).

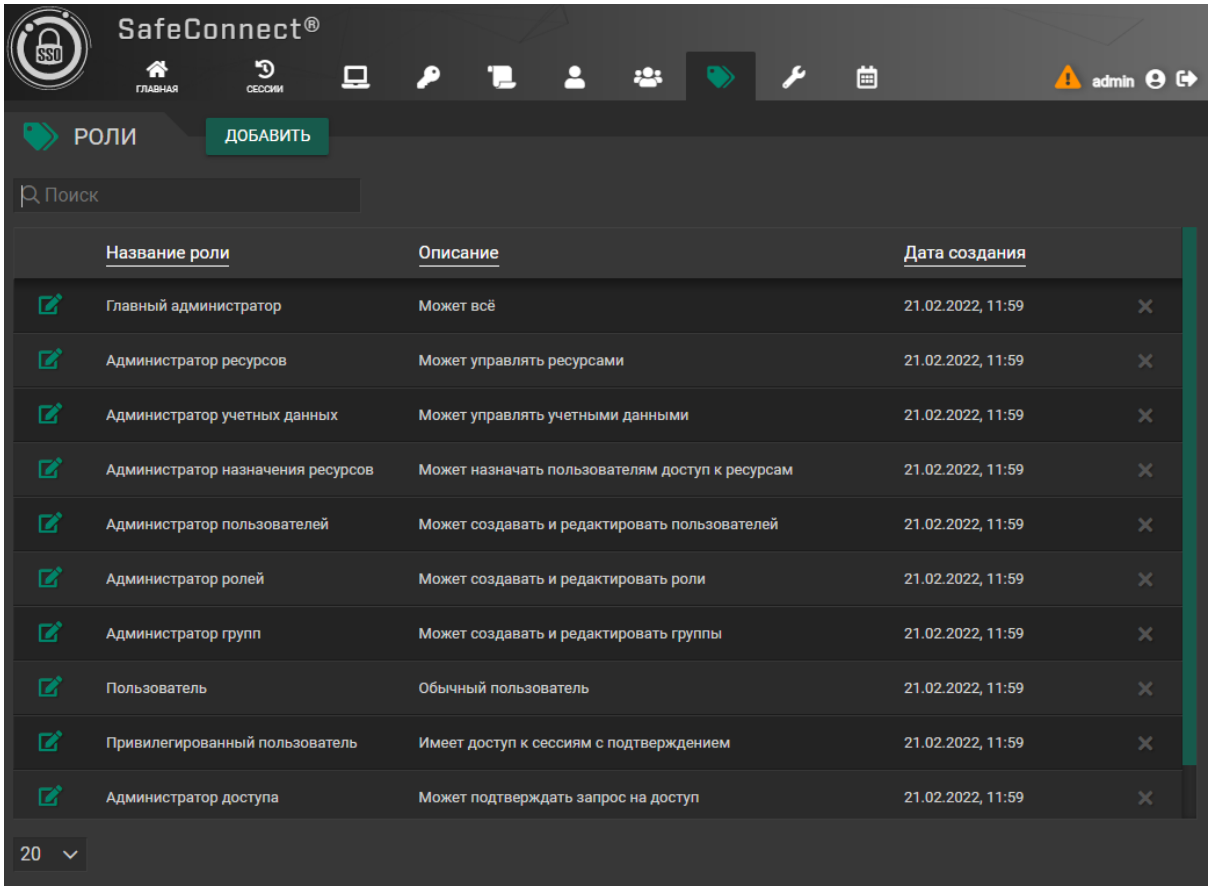


Рис. 3.60. Раздел «Роли»

На странице доступны добавление, редактирование и удаление ролей. Для удобства пользователя имеется возможность фильтрации списка ролей по названию. Для этого в поле **Поиск** (Рис.3.61) следует ввести название роли или его часть (с учетом регистра), и в списке останутся только роли, которые удовлетворяют заданному значению.

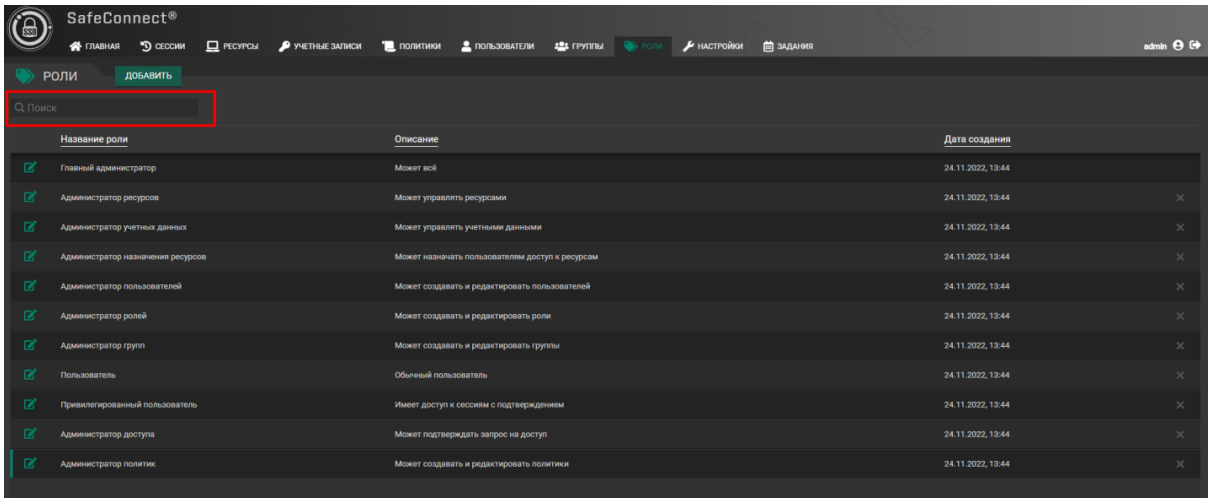


Рис. 3.61. Поиск в разделе «Роли»

3.12.1. Добавление роли

Для добавления роли следует перейти в раздел **Роли**, нажать кнопку **Добавить** и заполнить поля формы **Добавление роли** (Рис.3.62):

- **Название** – название роли;
- **Описание** – дополнительное поле для ввода описания роли;
- **Выбор полномочий** – установить флажки полномочий, разрешенных для данной роли.

Нажать кнопку **Создать**. Роль появится в списке ролей, и будет доступна для назначения пользователям.

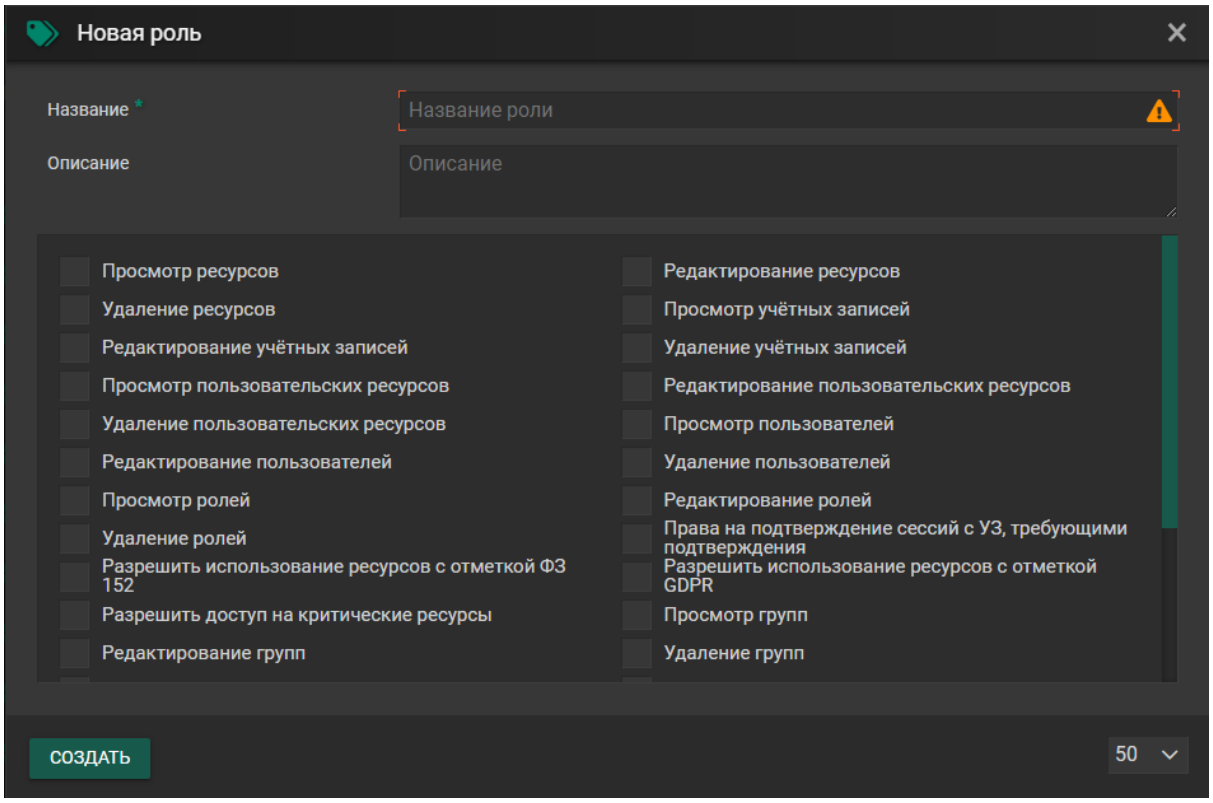


Рис. 3.62. Добавление роли

3.12.2. Редактирование роли

Для редактирования роли следует:

1. Перейти в раздел **Роли**;
2. Нажать на значок редактирования в строке редактируемой роли;
3. В открывшейся форме **Редактирование роли** внести необходимые изменения;
4. Нажать кнопку **Сохранить**.

3.12.3. Удаление роли

Для удаления роли следует перейти в раздел **Роли**, нажать на значок «крестик» в строке удаляемой роли, подтвердить удаление, нажав кнопку **ОК** в предупреждающем сообщении.

3.13. Раздел «Настройки»

Данный раздел позволяет производить настройки системы. В разделе **Настройки** (Рис.3.63) доступны следующие подразделы:

- Лицензия;
- Безопасность;
- Интеграция с внешними системами;

- Настройка SMTP;
- Пользовательское соглашение;
- Репликация;
- Серверы LDAP;
- Серверы RADIUS;
- Сетевые настройки;
- Брендирование;
- Резервное копирование и восстановление;
- Система.

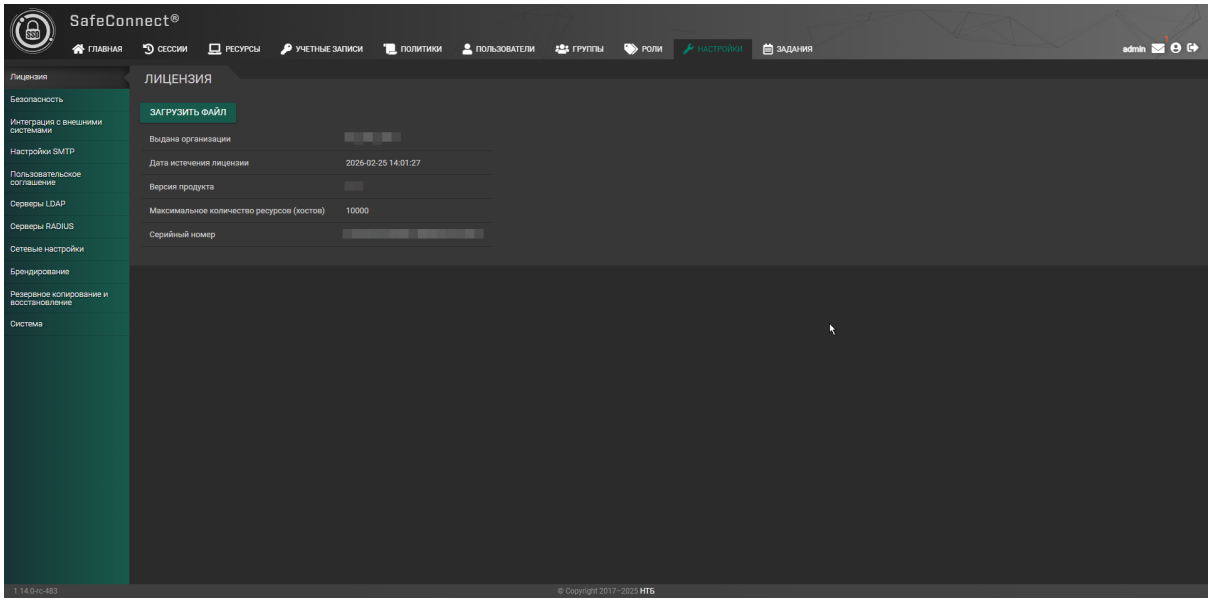


Рис. 3.63. Раздел «Настройки»

В левой части рабочей области расположен список разделов, справа – **рабочая область** выбранного раздела.

3.13.1. Лицензия

Раздел позволяет загрузить файл лицензии (Рис.3.64). По загруженной лицензии отображается следующая информация:

- **Выдана организации** – наименование организации, которой выдана данная лицензия;
- **Дата истечения лицензии**;
- **Версия продукта** – версия программы, для которой выдана лицензия;
- **Максимальное количество ресурсов (хостов)** – какое максимальное количество ресурсов позволяет добавить данная лицензия;

- **Серийный номер** – серийный номер установленной лицензии.

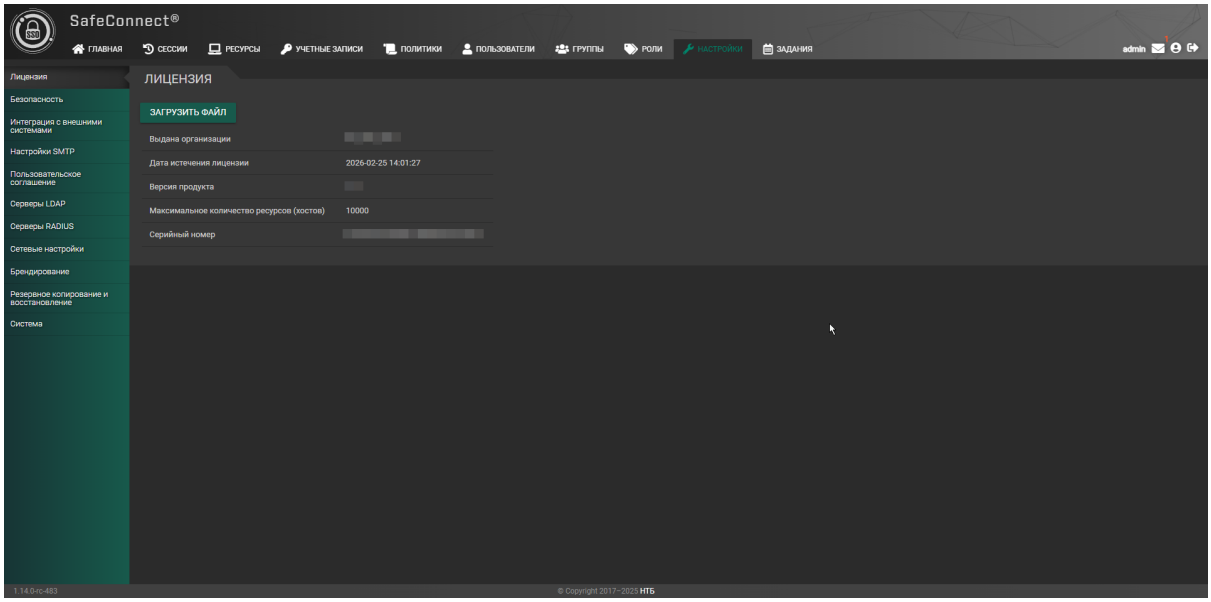


Рис. 3.64. Подраздел «Лицензия»

3.13.2. Безопасность

В разделе **Безопасность** доступны следующие функции:

- загрузка корневого сертификата;
- просмотр и копирование публичного ключа;
- добавление доверенных источников;
- настройка глобальной политики паролей.

3.13.2.1. Корневой сертификат

Для загрузки корневого сертификата необходимо перейти в раздел **Настройки > Безопасность**. В блоке **Корневой сертификат** (Рис.3.65) нажать кнопку **Скачать**.

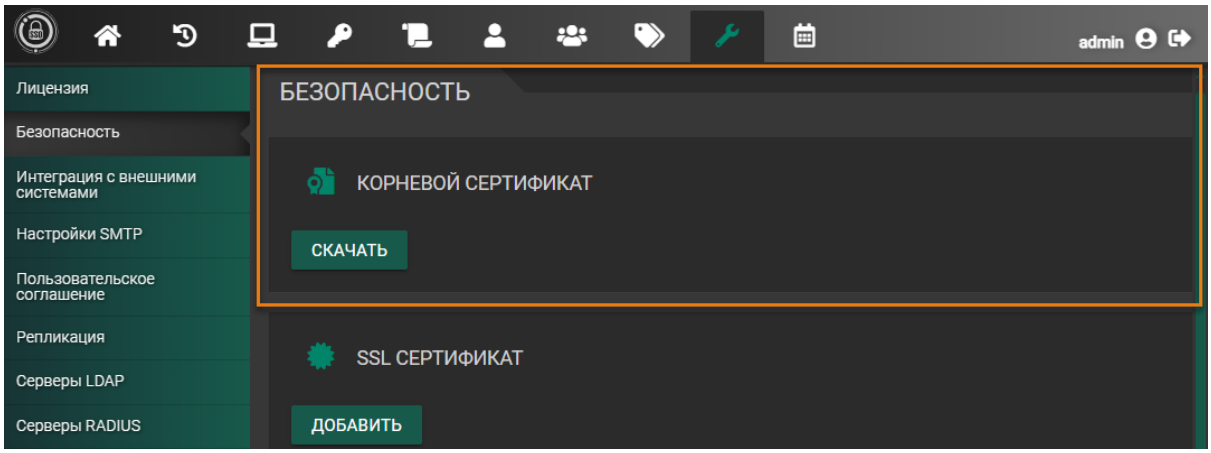


Рис. 3.65. Корневой сертификат

3.13.2.2. SSL-сертификат

В блоке **SSL-сертификат** (Рис.3.66) реализована возможность загрузки сертификата для защиты web-соединения с SafeConnect доверенным сертификатом, и интеграции с внутренним удостоверяющим центром организации.

Вы можете добавить сертификат следующим способом:

1. Изменить доменное имя, если необходимо (подробнее в разделе 3.13.9).

Примечание

При изменении доменного имени в систему автоматически добавляется и становится активным самоподписной SSL-сертификат.

2. Нажать кнопку **Добавить**. Откроется окно добавления ключей сертификата.
3. В поле **Сертификат (открытый ключ)** добавить текст открытого ключа.
4. В поле **Приватный ключ** добавить текст закрытого ключа.
5. Нажать кнопку **Добавить**.

После добавления и успешной проверки ключей сертификат будет добавлен в список сертификатов в блоке **SSL сертификат**. Самоподписной сертификат SafeConnect, используемый по умолчанию, становится архивным и начинает действовать загруженный сертификат.

После загрузки сертификата в интерфейсе доступна информация:

- **Сертификат**.
- **Издатель** – центр сертификации.
- **Дата выпуска**.
- **Дата окончания**.
- **Статус** – активен/неактивен.

Действия с сертификатом:

- Экспорт сертификата кнопкой .
- Копирование открытого ключа кнопкой .

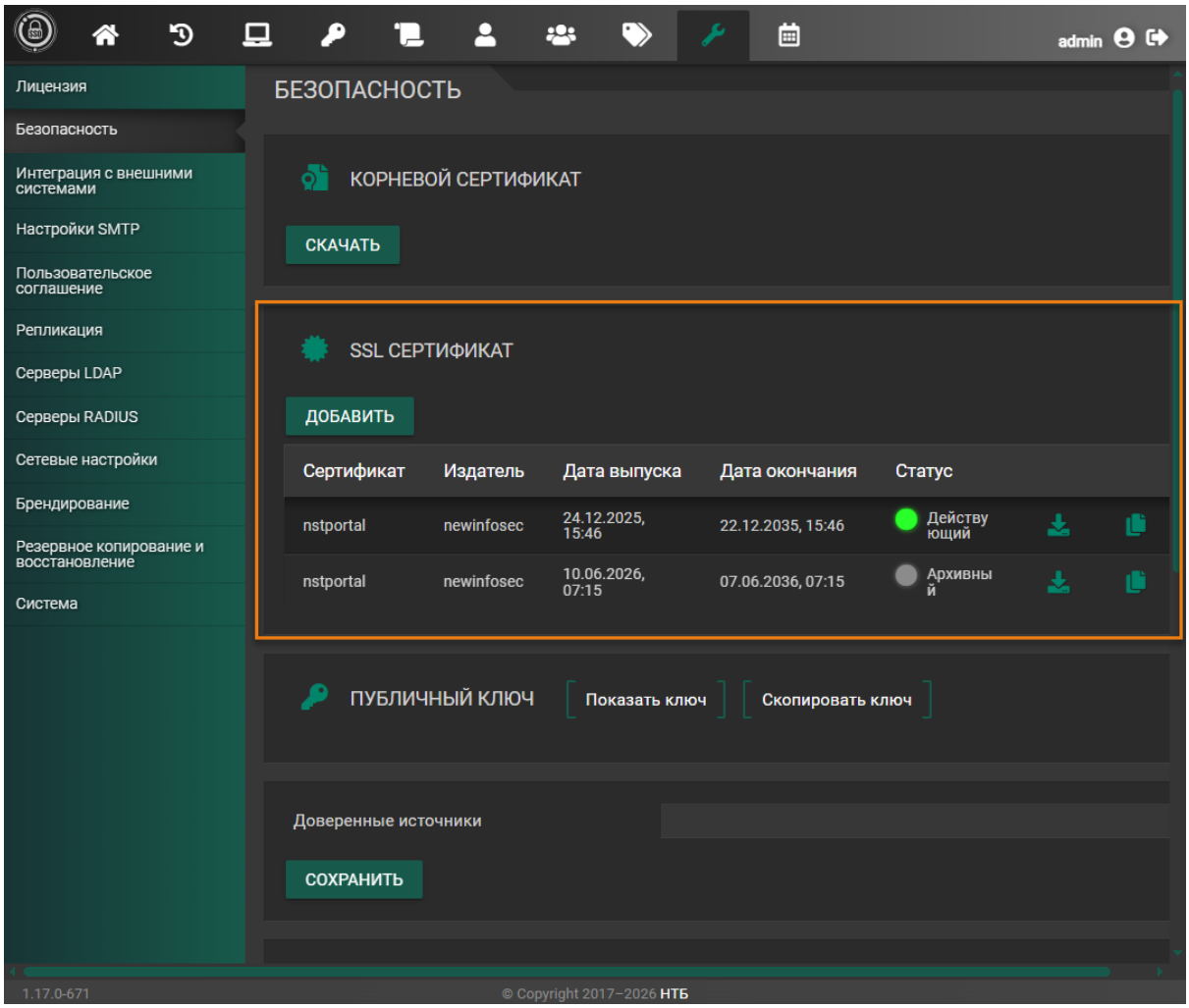


Рис. 3.66. SSL-сертификаты

3.13.2.3. Публичный ключ

В блоке **Публичный ключ** (Рис.3.67) реализована возможность просмотреть ssh–ключ по кнопке **Показать ключ**, или скопировать **публичный ssh–ключ** по кнопке **Скопировать ключ**.

Вы можете добавить данный ключ в **authorized_ keys** целевого сервера (например, для выполнения резервного копирования по расписанию).

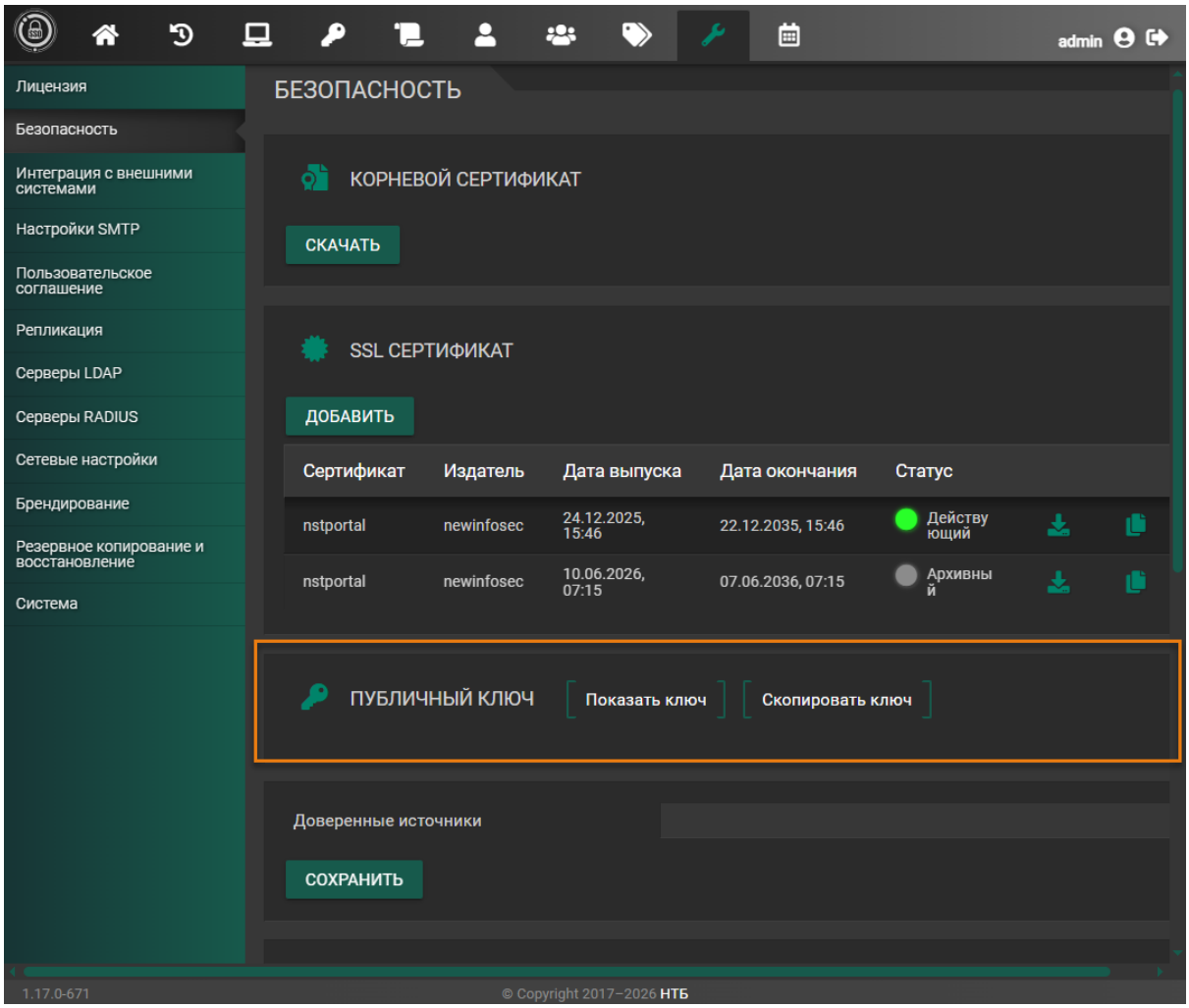


Рис. 3.67. Публичный ключ

3.13.2.4. Доверенные источники

В случае использования прокси–сервера и (или) проброса портов необходимо указать доверенные источники:

1. Перейти в раздел **Настройки > Безопасность**;
2. В поле **Доверенные источники** указать через запятую домены (порты, которые будут считаться доверенными) (Рис.3.68);
3. Нажать **Сохранить**.

Пример:

```
nstportal, 192.168.12.1, proxy.ngate.local:8443
```

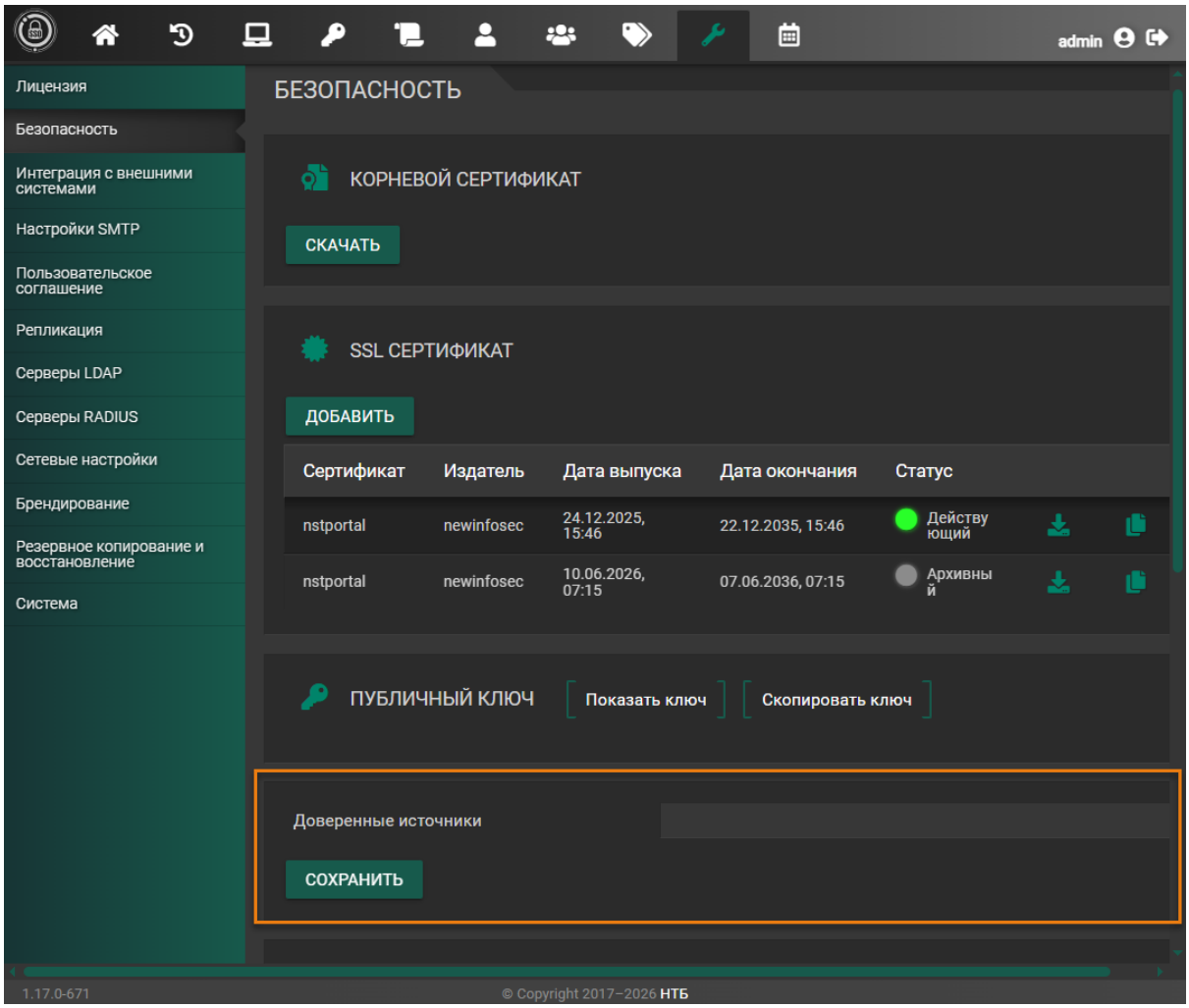


Рис. 3.68. Доверенные источники

3.13.2.5. Глобальная политика паролей

Для настройки глобальной политики паролей следует перейти в раздел **Настройки > Безопасность** и заполнить поля формы (Рис.3.69):

- **Время жизни сессии (в минутах)** – позволяет задать максимальное время бездействия, по истечении которого сессия будет прервана. Чтобы продолжить дальнейшую работу с системой, пользователю необходимо будет снова авторизоваться;
- **Минимальная длина** – указать минимальное количество символов в пароле;
- **Максимальная длина** – указать максимально допустимое количество символов в пароле;
- **Количество цифр** – указать минимальное количество цифр в пароле;
- **Количество заглавных** – указать минимальное количество заглавных букв в пароле;
- **Количество спецсимволов** – указать минимальное количество спецсимволов в пароле;
- **Шаблон** – список допустимых символов в пароле.

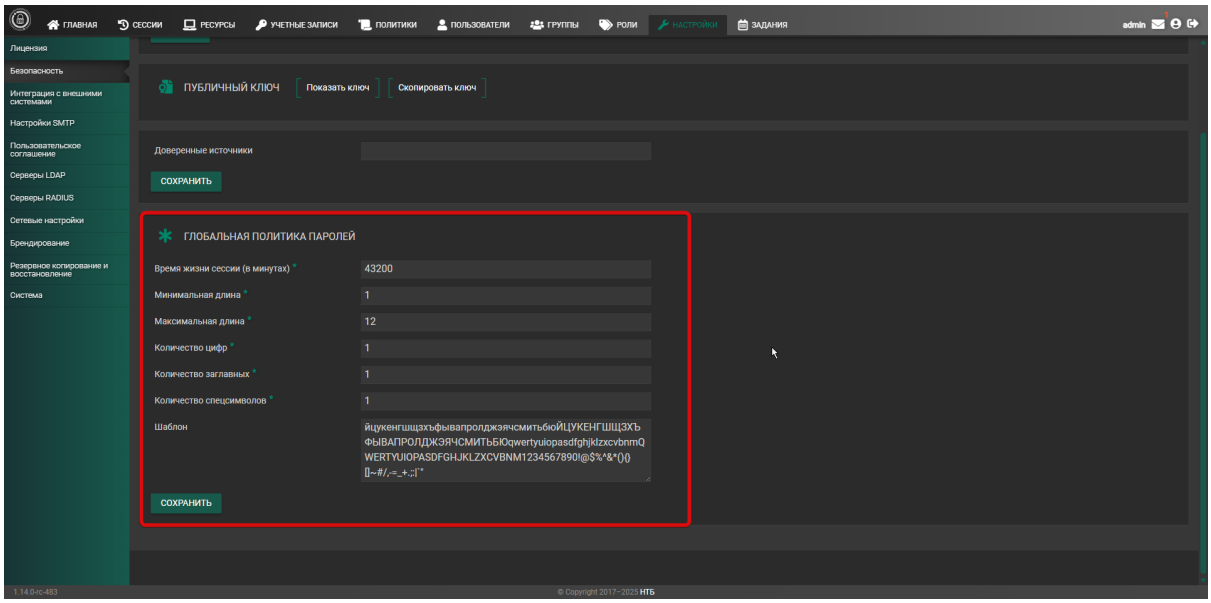


Рис. 3.69. Глобальная политика паролей

Нажать кнопку **Сохранить** для сохранения настроек глобальной политики паролей.

3.13.3. Интеграция с внешними системами

3.13.3.1. Интеграция с SafeInspect

В SafeConnect имеется возможность интеграции с **системой контроля действий привилегированных пользователей Solar** (подробнее в разделе Рис.3.70).

Для настройки интеграции в панели управления SafeInspect:

- выбрать пункт **Администраторы**;
- нажать кнопку **Сгенерировать конфигурацию API**;
- полученный файл загрузить на вкладке **SafeInspect** (раздел **Настройки > Интеграция с внешними системами**, вкладка **SafeInspect**) кнопкой **Загрузить файл** (Рис.3.71).

При включенной синхронизации  список сопоставлений в SafeInspect будет приводиться в строгое соответствие с действующими доступами в SafeConnect. Любые несоответствия будут автоматически удаляться (корректироваться).

Отключите данную опцию , если версия SafeInspect ниже 2.4.3, и вам необходимо модифицировать (добавить сопоставления) вручную. Однако делать это НЕ РЕКОМЕНДУЕТСЯ.

Удалить интеграцию с SafeInspect можно, нажав на значок «крестик».

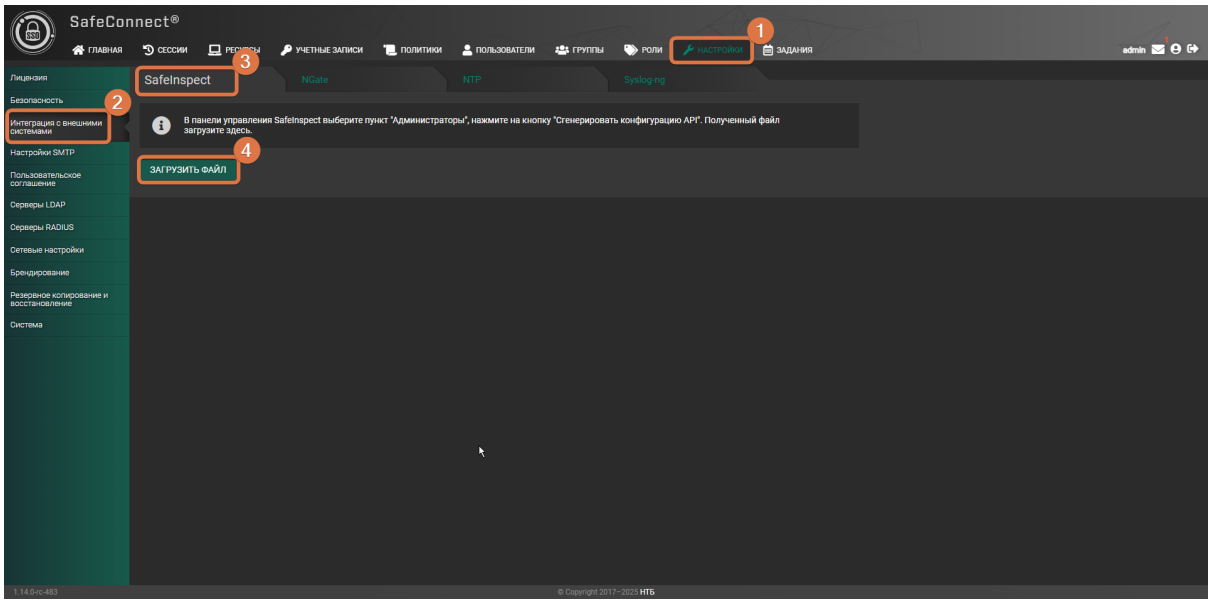


Рис. 3.70. Интеграция с SafeInspect

3.13.3.2. Интеграция с КриптоПро NGate

КриптоПро NGate – высокопроизводительный **VPN–шлюз** на базе протокола TLS, который позволяет безопасно и быстро организовать защищённый доступ удалённых пользователей к корпоративным ресурсам через незащищённые сети, например, сеть Интернет (подробнее в разделе Рис.3.71).

Для корректной работы SafeConnect:

1. Добавить домен NGate, по которому пользователи будут выполнять подключение, в список доверенных источников (раздел **Безопасность**, заполнить блок **Доверенные источники**).

2. Перейти в раздел **Настройки > Интеграция с внешними системами**, вкладка **NGate** (Рис.3.71).

3. Заполнить поля:

   - **Серийный ключ**;
   - **Подтверждение ключа**;
   - **Срок валидности заголовка X– Client– Password**;
   - **Срок валидности остальных заголовков**.

4. Для сохранения изменений нажать кнопку **Сохранить**.

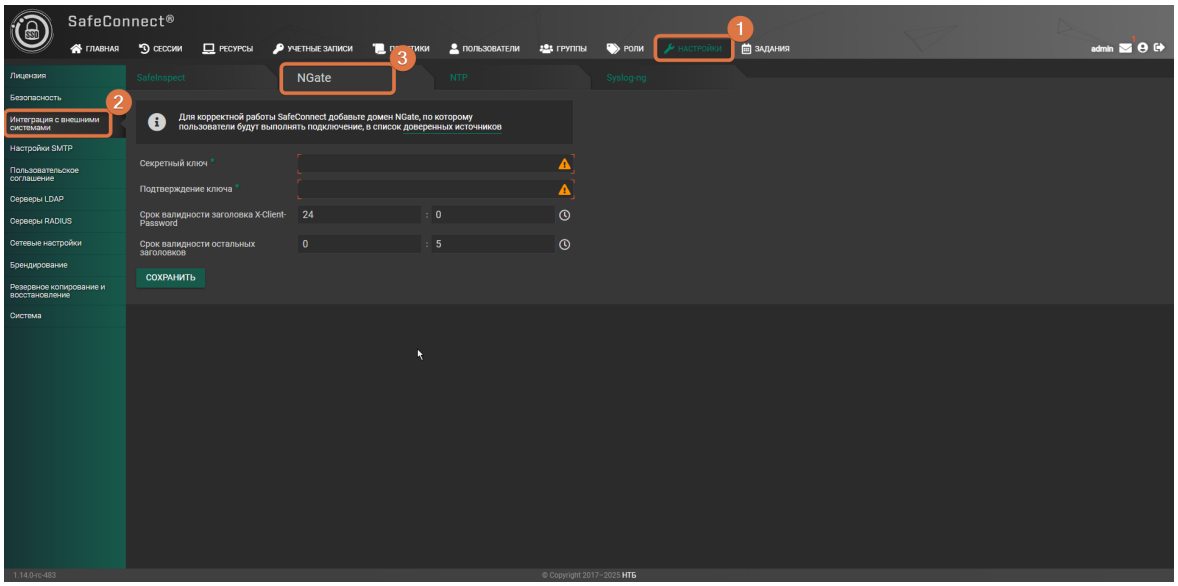


Рис. 3.71. Интеграция с КриптоПро NGate

3.13.3.3. Интеграция с NTP

NTP – сервер синхронизации времени по протоколу **NTP**. Для настройки интеграции с **NTP** перейти в раздел **Настройки > Интеграция с внешними системами**, вкладка **NTP** (Рис.3.72). Далее ввести адрес (или адреса, разделенные пробелами). Для сохранения изменений нажать **Сохранить**.

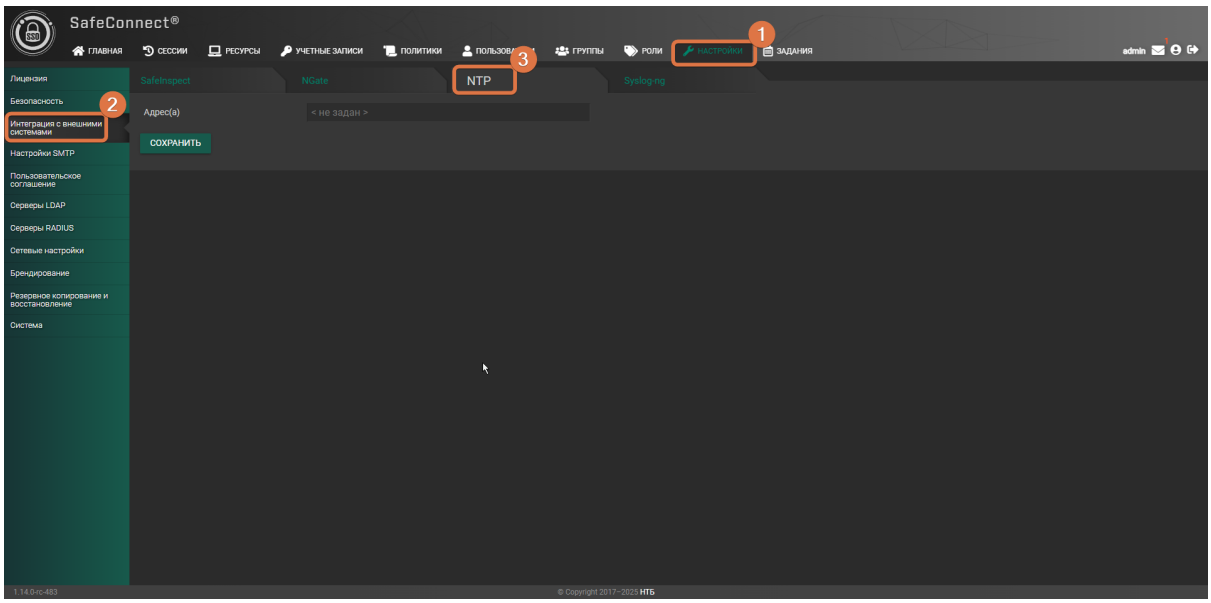


Рис. 3.72. Интеграция с NTP

3.13.3.4. Интеграция с Syslog–ng

Syslog– ng – комплект инструментов для централизованного сбора и хранения лог–файлов. Он предоставляет функции форматирования, управления потоком сообщений и классификации входящих сообщений. Syslog–ng доступен в различных дистрибутивах Linux и Unix.

В результате настройки интеграции с Syslog–ng осуществляется передача логов во внешний syslog–сервер. Данный функционал позволяет настроить адрес сервера, тип протокола передачи и формат лога.

Для настройки интеграции перейти в раздел **Настройки > Интеграция с внешними системами** , открыть вкладку **Syslog–ng** (Рис.3.73). Затем заполнить поля:

- **Адрес;**
- **Порт;**
- **Протокол** (выбрать из списка TCP или UDP);
- **Формат** (выбрать из списка CEF или LEEF).

Для сохранения изменений нажать кнопку **Сохранить**.

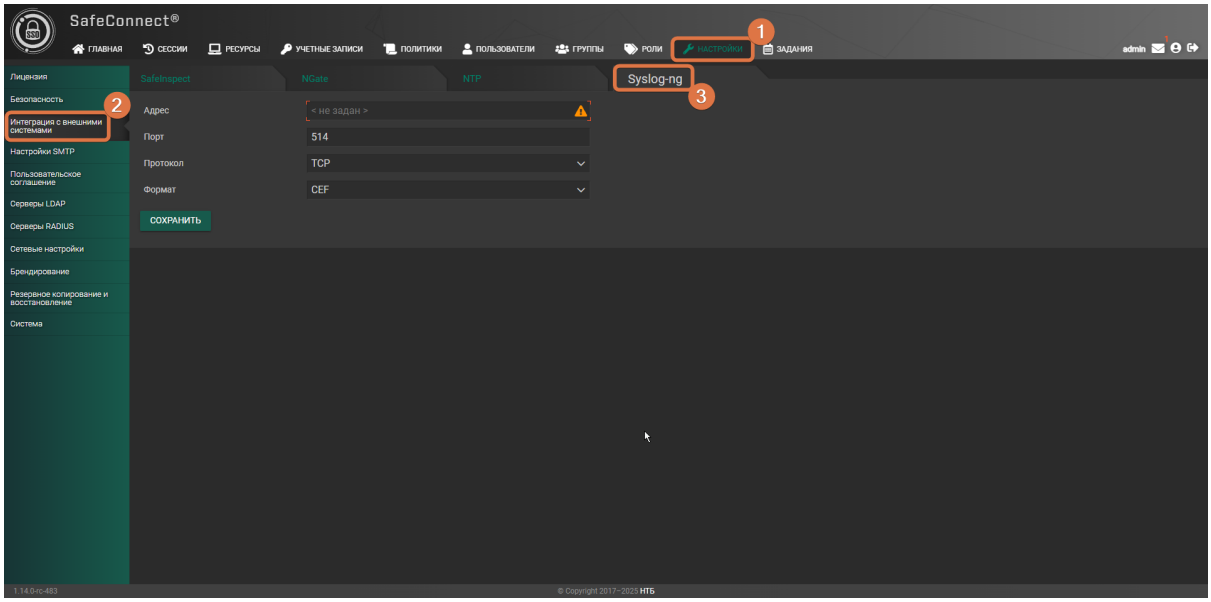


Рис. 3.73. Интеграция с Syslog–ng

3.13.4. Настройки SMTP

Для настройки SMTP следует перейти в раздел **Настройки > Настройки SMTP** и заполнить поля формы (Рис.3.74):

- **Сервер** – указать IP–адрес почтового сервера;
- **Порт** – указать порт;
- **SSL/TLS** – установить флажок при необходимости;
- **Учетная запись** – указать e–mail адрес;
- **Пароль** – указать пароль.

Проверить правильность настроек, нажав кнопку **Проверить настройки**. При этом будет отправлено тестовое письмо на вашу почту.

Нажать кнопку **Сохранить** для сохранения настроек **SMTP**.

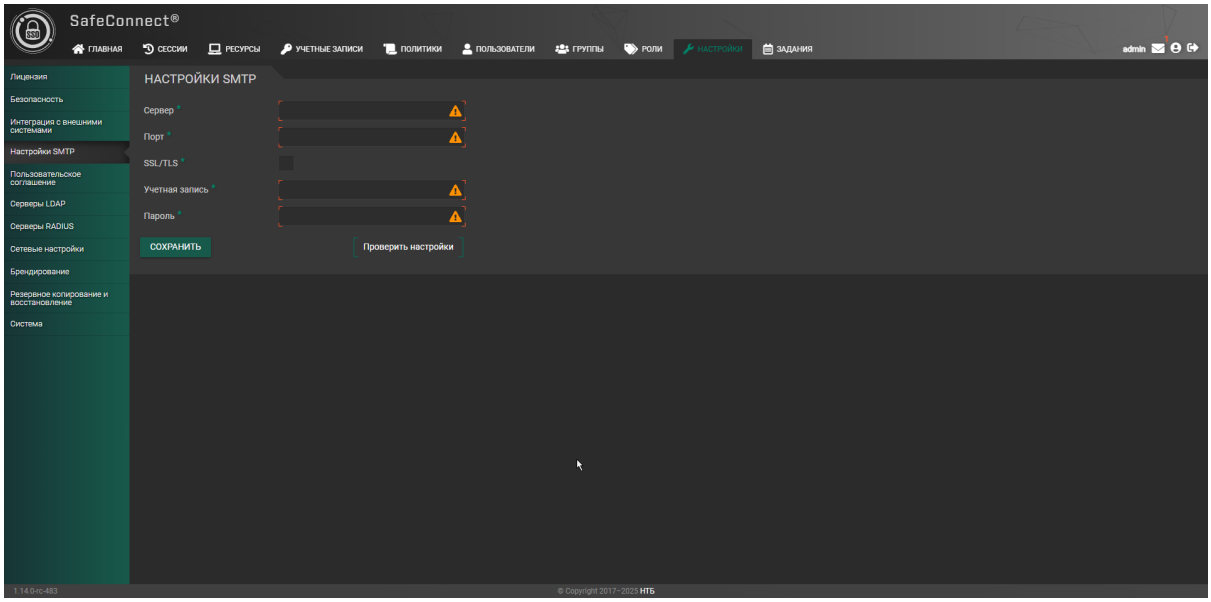


Рис. 3.74. Настройки SMTP

3.13.5. Пользовательское соглашение

Раздел позволяет при необходимости добавить текст пользовательского соглашения, который будет отображаться всем пользователям при первом входе в SafeConnect:

1. Перейти в раздел **Настройки > Пользовательское соглашение**;
2. Заполнить текстовое поле (Рис.3.75) с информацией для пользователя (текст пользовательского соглашения);
3. Нажать **Сохранить** (Рис.3.77).

После сохранения настроек продолжить работу с SafeConnect можно будет только после нажатия на кнопку **Согласен** (Рис.3.77) .

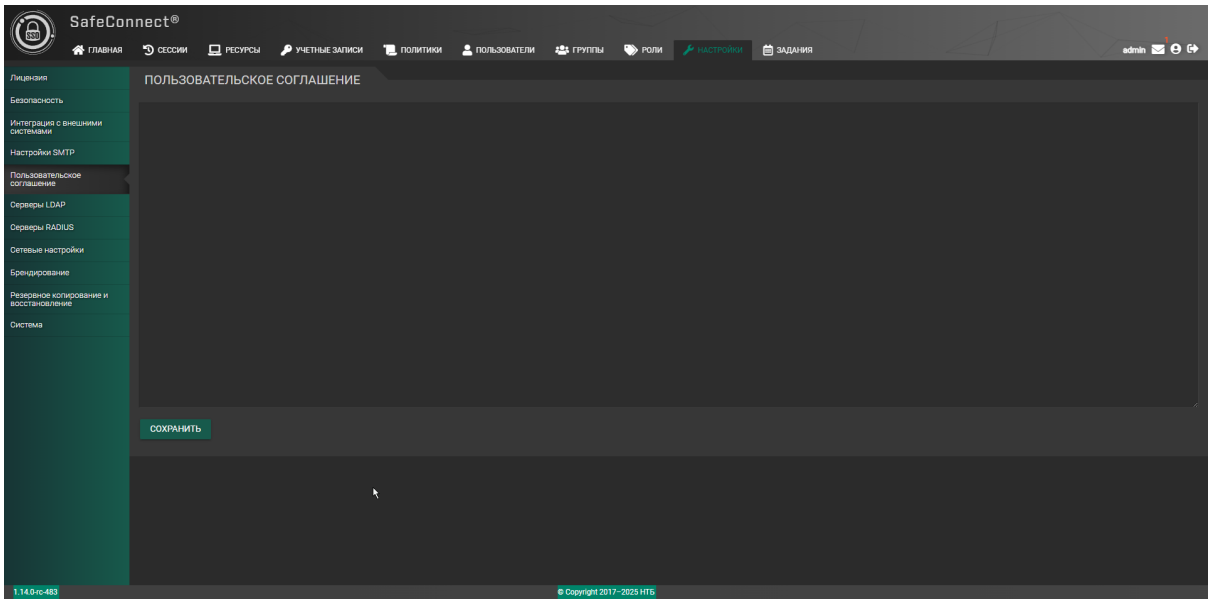


Рис. 3.75. Пользовательское соглашение

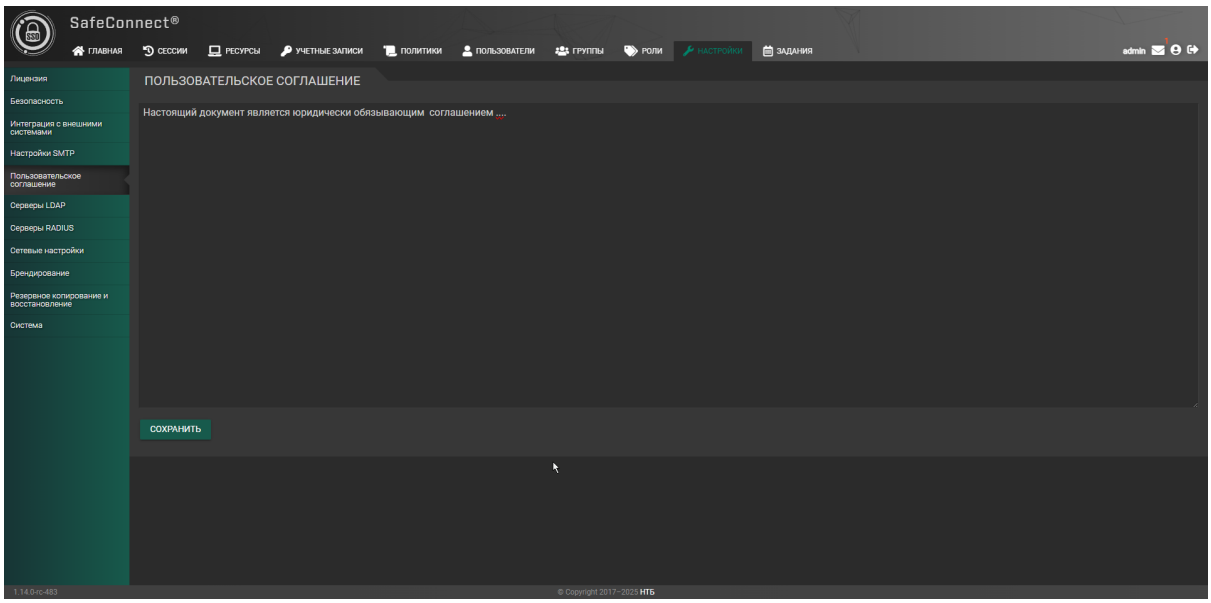


Рис. 3.76. Заполнение теста пользовательского соглашения

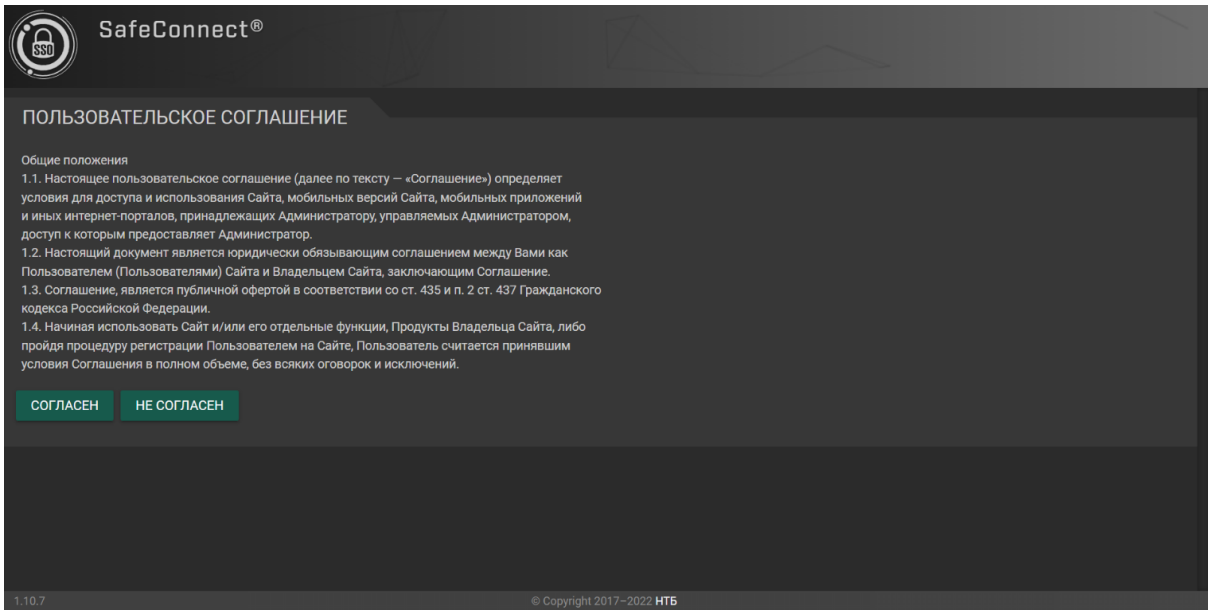


Рис. 3.77. Отображение пользовательского соглашения при входе

3.13.6. Репликация

SafeConnect может работать в кластерной конфигурации. Чтобы обеспечить синхронизацию данных между несколькими Порталами, работающими в «кластерной» конфигурации, необходимо настроить репликацию данных между этими Порталами.

Примечание

Взаимодействие разных экземпляров системы друг с другом реализовано по портам 2379, 2380, 5416, 5432, 6432, 8018.

3.13.6.1. Настройка репликации

Репликация настроена, если пользователь вводит данные на одном из них, а данные автоматически появляются на остальных порталах, которые участвуют в репликации данных.

Внимание!

Если несколько пользователей будут вводить данные в разные Порталы (произвольно), то в случае конфликта ввода данных (администраторы вводят информацию в одни и те же поля), сохранятся данные, введенные последними. Вне зависимости от того на каком Портале это было сделано.

Для настройки репликации следует воспользоваться инструкцией **Solar_SafeConnect_1.17.0_Инструкция_по_настройке_репликации**.

3.13.6.2. Мониторинг статуса репликации

В SafeConnect реализован инструмент мониторинга работоспособности модуля репликации и кластера БД. Функционал позволяет отслеживать состояние узлов и синхронизации данных (**Настройки > Репликация**).

На странице доступны следующие сведения о состоянии системы:

- **Общий статус репликации** – индикатор состояния процесса синхронизации данных (например, Активна / Ошибка / Синхронизация (Табл.3.11)).
- **Список узлов** – детализированная таблица всех участников кластера со следующими параметрами:
  - **Имя узла**.
  - **Адрес хоста** – IP-адрес или DNS-имя сервера.
  - **Статус** – текущее состояние доступности узла (например, Выполняется / Передача данных (Табл.3.11)).
  - **Роль** – отображается иконка ведущего узла в кластере.

Функционал обеспечивает полную прозрачность топологии кластера и упрощает диагностику проблем с синхронизацией.

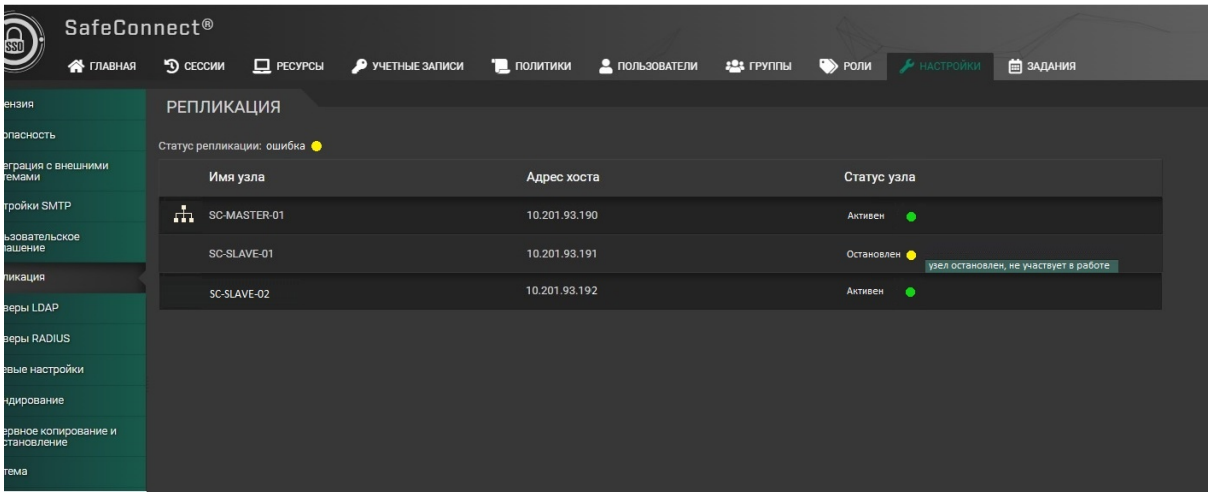


Рис. 3.78. Мониторинг модуля репликации

Табл. 3.11. Статусы репликации

№	Наименование	Статус	Условие
1	Статус репликации	Активна	Все узлы кластера доступны и стабильно работают
		Ошибка	Обнаружены остановленные узлы, репликация данных прервана
		Сбой	В узлах кластера обнаружен сбой
2	Статус узлов	Активен	Узел доступен / происходит процесс приемки репликационных данных
		Восстановление из архива	Идет процесс восстановления из архива журналов транзакций (архивное восстановление)

№	Наименование	Статус	Условие
		Остановлен	Узел остановлен, не участвует в работе кластера
		Сбой	Узел недоступен или вышел из строя

3.13.7. Серверы LDAP

3.13.7.1. Настройка серверов LDAP

SafeConnect поддерживает аутентификацию пользователей с использованием LDAP. При необходимости можно добавить несколько серверов LDAP.

Для настройки серверов LDAP следует перейти в раздел **Настройки > Серверы LDAP**, нажать кнопку **Добавить** и заполнить поля формы (Рис.3.79):

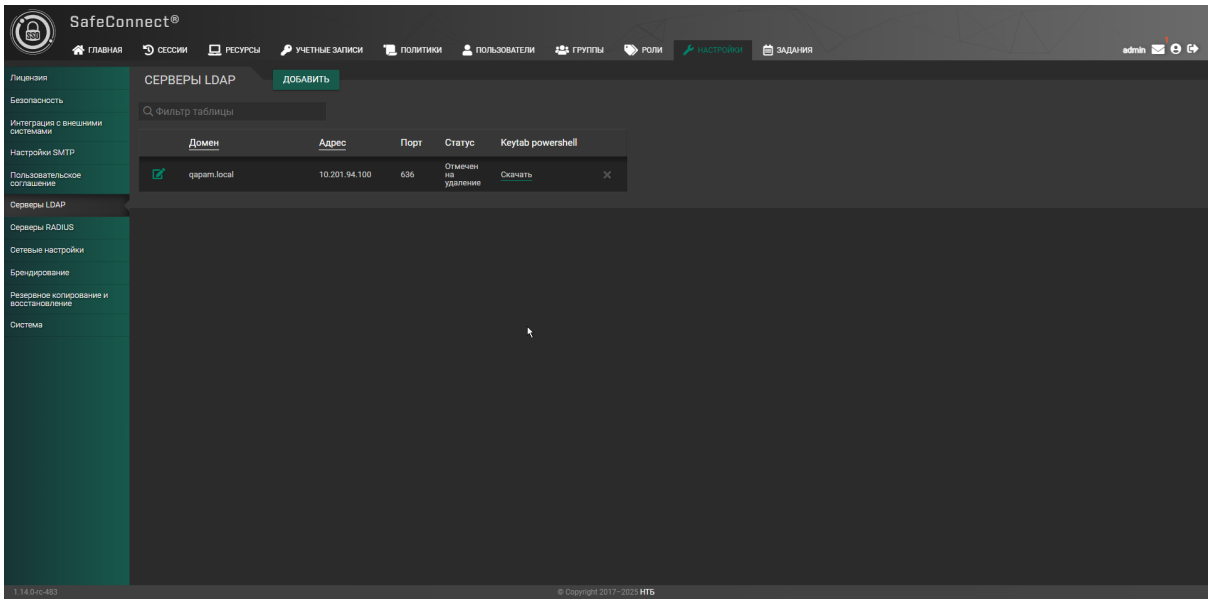


Рис. 3.79. Добавление сервера LDAP

- **Домен** – указать полное доменное имя;
- **IP–Адрес или FQDN** – указать IP–Адрес сервера LDAP;
- **Порт** – указать порт (по умолчанию указан 389);
- **Использовать TLS** – установить флажок при использовании TLS;
- **Сертификат** – вставить сертификат, используемый сервером LDAP, или любой из сертификатов центра сертификации;
- **Имя базового объекта (BaseDN)** – строка, описывающая верхний узел иерархии каталога, используется в качестве базы при поиске информации о группе пользователей. Его необходимо указать, если сервер LDAP не передаёт RootDSE (корень дерева каталога) (необязательное поле);
- **Шаблон имени входа** – по умолчанию: {username}@{domain}.

  Допустимые атрибуты:

- {username} – имя пользователя;
- {user_dn} – имя пользователя в формате DN;
- {domain} – имя домена;
- {base_dn} – имя базового объекта (Base DN);

- **Шаблон поиска пользователей** – по умолчанию: (sAMAccountName={username}).

  Допустимые атрибуты:

  - {username} – имя пользователя;

- **Шаблон поиска групп** – по умолчанию: (&(objectclass=group)(!(groupType:1.2.840.113556.1.4.803:=1))). Фильтр для LDAP групп, которые будут синхронизированы. Максимальная длина зависит от версии LDAP:

```
 &(objectclass=group)
(|(memberOf=CN=PortalGroups,CN=Users,DC=test,DC=local)
(memberOf=CN=PortalNewGroups.CN=Users,DC=test,DC=local)))
```

- **Поддержка вложенных групп AD** – установить флажок ☑, чтобы разрешить использование AD расширений в запросах LDAP. Требуется для поддержки иерархических групп LDAP;
- **Сбросить значения до рекомендуемых** – при нажатии одной из кнопок будут подставлены рекомендуемые значения в поля Шаблон имени входа, Шаблон поиска пользователей, Шаблон поиска групп:
- **Active Directory**:

Шаблон имени входа: {username}@{domain}

Шаблон поиска пользователей: (sAMAccountName={username})

Шаблон поиска групп: (&(objectclass=group)(!(groupType:1.2.840.113556.1.4.803:=1)))

- FreeIPA:

Шаблон имени входа: {user_dn}

Шаблон поиска пользователей: (&(uid={username})(objectclass=ipaobject))

Шаблон поиска групп: (objectclass=ipausergroup)

- **Имя пользователя LDAP BIND** – учетные данные для LDAP BIND. Необходимо указать, если сервер не поддерживает анонимные запросы BIND;
- **LDAP BIND пароль** – задайте пароль;
- **Подтверждение пароля** – повторно ввести пароль;
- **Удалить пароль** – установить флажок ☑ при необходимости;

- **Сквозная авторизация (kerberos)** – установить флажок при необходимости и загрузить keytab–файл для включения сквозной авторизации в SafeConnect. Для активации этой функции необходимо предварительно сгенерировать keytab-файл и создать DNS–записи для соответствующего SPN.

Нажать кнопку **Сохранить.** Если все поля заполнены корректно, и добавленный LDAP-сервер существует, запись о нем появится в списке на странице **Серверы LDAP** (**Рис.3.80**).

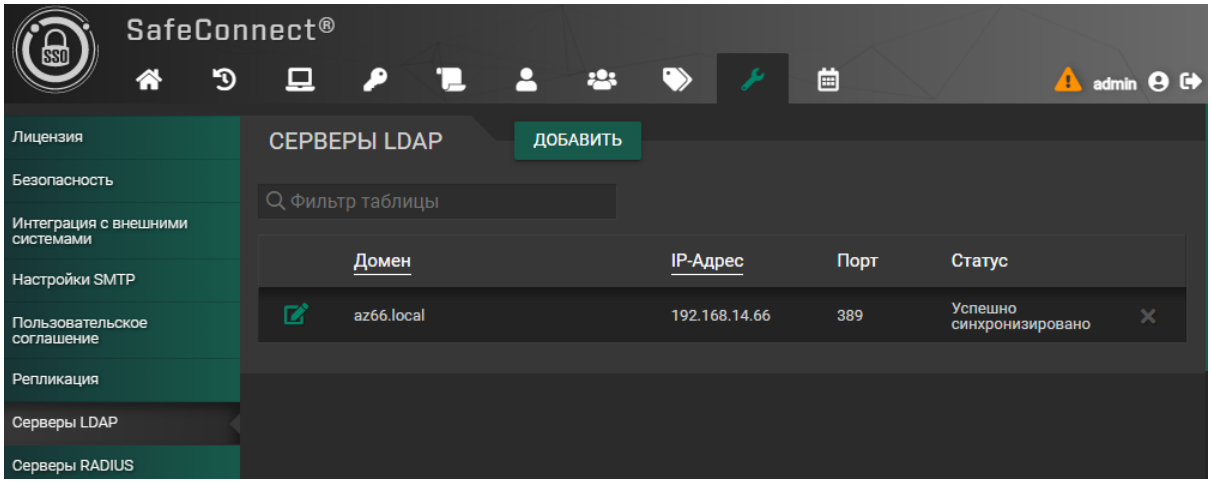


Рис. 3.80. Серверы LDAP

Для добавления следующего LDAP сервера следует нажать кнопку **Добавить** и заполнить форму.

3.13.7.2. Настройка сквозной авторизации (Kerberos)

Для корректной работы **сквозной авторизации (kerberos)** следует произвести следующие настройки:

- При установке SafeConnect или позже в настройках указать корректный DNS;
- До выполнения kerberos.ps следует создать Reverse Lookup Zone в DNS для соответствующего IP SafeConnect;
- Заменить в файле **/opt/sc-manager/static/kerberos.ps** (или https://nstportal/static/kerberos.ps) поле $domain = "..." на имя домена, и поле $ip = "..." на IP–адрес SafeConnect;
- Выполнить в **PowerShell** скрипт из файла kerberos.ps, при этом на рабочем столе будет создан файл krb5.keytab;
- В SafeConnect зайти в **Настройки > Серверы LDAP** нажать кнопку **Добавить**;
- Заполнить настройки сервера, установить флажок **Сквозная авторизация**, во всплывающем окне выбрать и загрузить файл krb5.keytab, нажать кнопку **Сохранить**;
- Зайти в Control Panel\Network and Internet\Internet Options (или в браузере Настройки > Дополнительно > Система > Настройки прокси–сервера);

- Перейти на вкладку **Security > Local Intranet > Sites** и добавить "https://nstportal" в список сайтов;
- Ввести в строке адреса браузера "nstportal/", будет выполнен переход на главную страницу SafeConnect с автоматическим логином текущего пользователя Windows.

3.13.8. Серверы RADIUS

Для настройки серверов RADIUS следует перейти в раздел **Настройки > Серверы RADIUS**, нажать **Добавить** и заполнить поля формы (Рис.3.81):

- **IP–Адрес** – указать IP–адрес сервера RADIUS;
- **Таймаут (сек)** – максимально допустимое время ожидания ответа отсервера RADIUS (в секундах);
- **Назначение** – выбрать один из вариантов работы сервера:
  - 2FA доступ к SSO SafeConnect;
  - 2FA доступ к сессиям;
  - Импорт пользователей;
  - Импорт пользователей | Авторизация;

Внимание!

*Для успешной авторизации с использованием **RADIUS-сервера** при выборе в списке **Назначение** варианта работы сервера **Импорт пользователей | Авторизация** требуется учётная запись администратора, предназначенная для выполнения этой операции. Учетная запись должна быть предварительно создана непосредственно на самом **RADIUS-сервере**. В противном случае процесс авторизации завершится ошибкой.*

- **Пароль** – задайте пароль;
- **Подтверждение пароля** – повторно ввести пароль;
- **Многодоменная архитектура** – установить флажок при необходимости.

Нажать кнопку **Сохранить**, добавленный **RADIUS сервер** отобразится в списке на странице **Серверы RADIUS**.

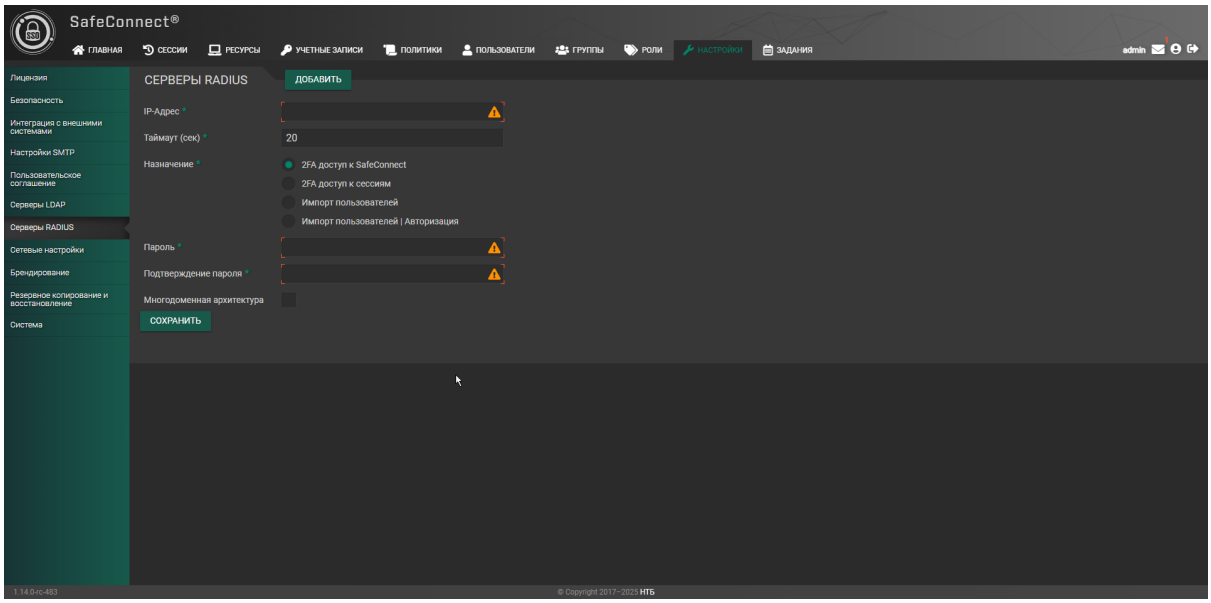


Рис. 3.81. Серверы RADIUS

Для добавления еще одного **RADIUS сервера** следует нажать кнопку **Добавить** и заполнить форму.

3.13.9. Сетевые настройки

Для изменения настроек сетевых интерфейсов следует перейти в раздел **Настройки > Сетевые настройки**.

Примечание

Перед изменением IP–адресов или шлюзов необходимо убедиться, что у вас есть консольный доступ к системе.

Внимание!

Все сетевые настройки системы необходимо производить исключительно через веб-интерфейс, в том числе и изменение доменного имени. Изменение системных файлов вручную может привести к нарушению работоспособности всей системы.

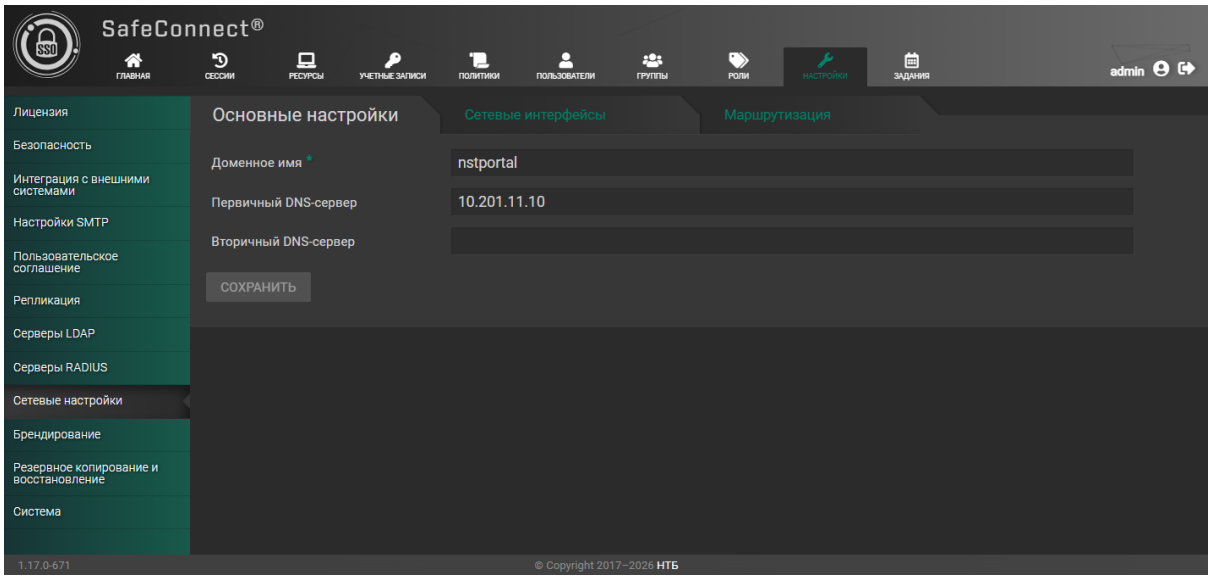


Рис. 3.82. Сетевые настройки

Во вкладке **Основные настройки** (Рис.3.83) доступны следующие параметры:

- **Доменное имя** – доменное имя хоста;
- **Первичный DNS–сервер** – доменное имя DNS–сервера или IP–адрес. Серверы доменных имен должны быть либо доступны на каких–либо непосредственно подключенных интерфейсах или через шлюз по умолчанию;
- **Вторичный DNS–сервер** – доменное DNS–имя или IP–адрес резервного сервера.

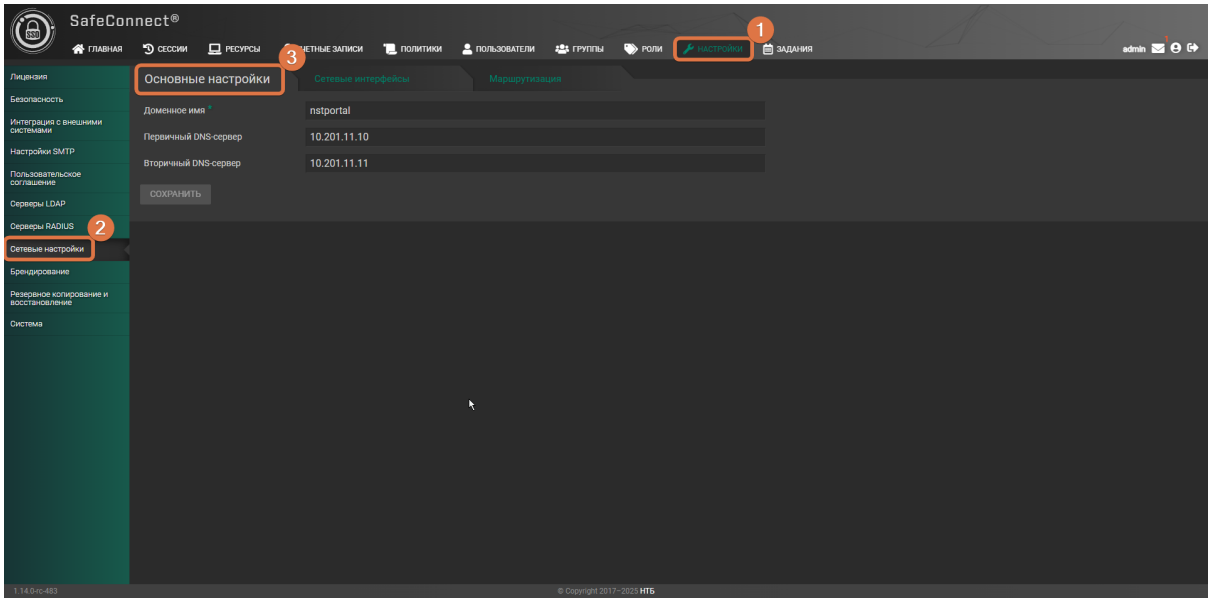


Рис. 3.83. Сетевые настройки – Основные настройки

Во вкладке **Сетевые интерфейсы** (Рис.3.84) для редактирования сетевого интерфейса следует нажать на  и в открывшейся форме редактирования внести изменения. Редактировать можно IP–адрес и маску подсети/префикс. Также реализована возможность выбора типа сетевого интерфейса: публичный (для доступа к веб–интерфейсу), приватный

(для https–ресурсов) или управления (для подключения по SSH и репликации). Для сохранения изменений необходимо нажать кнопку **Сохранить**, для закрытия формы без изменений нажать на значок «крестик».

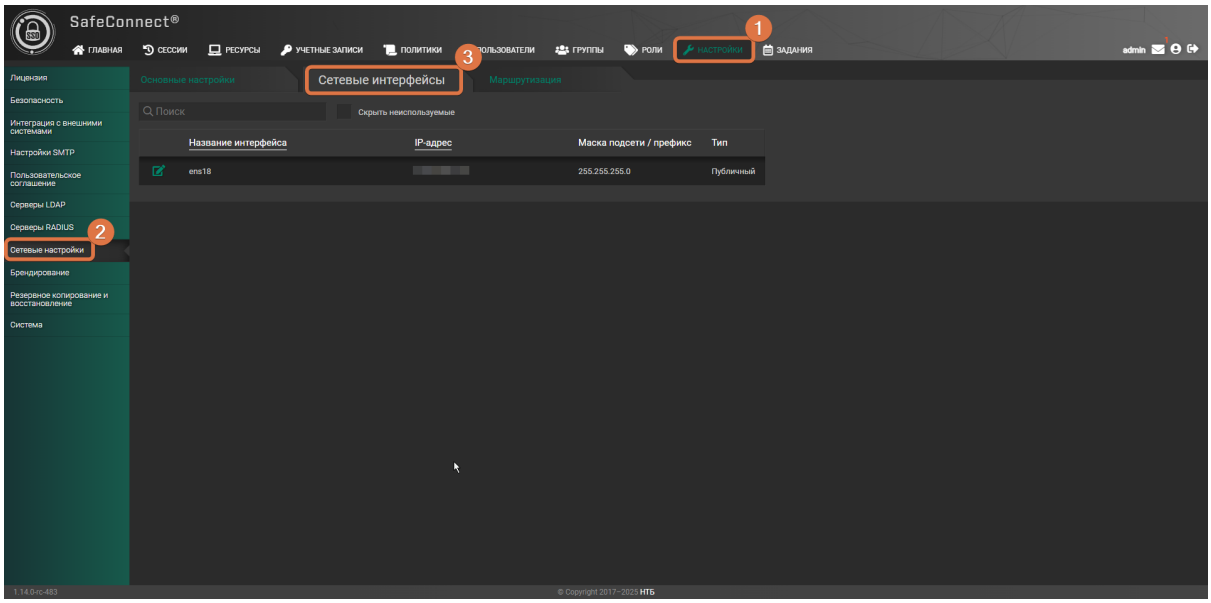


Рис. 3.84. Сетевые настройки, вкладка «Сетевые интерфейсы»

Во вкладке **Маршрутизация** (Рис.3.85) для редактирования маршрута следует нажать на  и в открывшейся форме редактирования внести изменения, затем нажать **Сохранить**. Для редактирования доступны поля:

- **Маршрут / шлюз по умолчанию** – установить или снять флажок  (при необходимости);
- **Адрес назначения** – адрес сети или узла назначения;
- **Маска сети назначения** – для указания единичного узла сети используется маска 255.255.255.255;
- **Шлюз** – адрес маршрутизатора в сети, на который необходимо направлять пакеты, следующие до указанного адреса назначения;
- **Сетевой интерфейс** – сетевой интерфейс, через который доступен шлюз (выбор из выпадающего списка);
- **Метрика** – числовой показатель, определяющий предпочтительность маршрута.

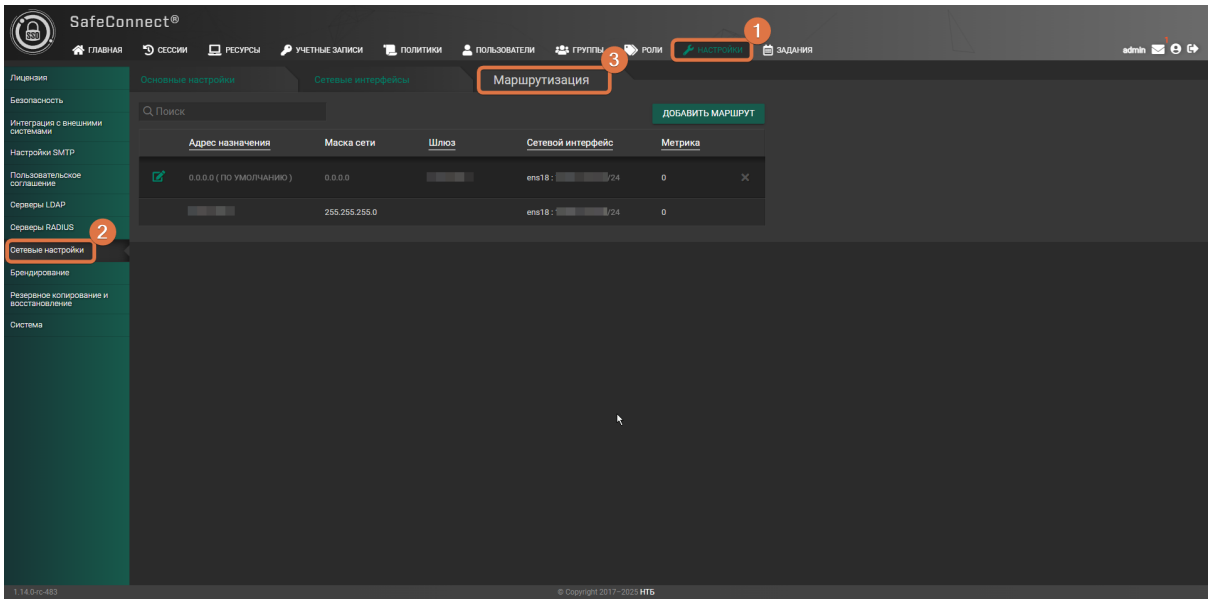


Рис. 3.85. Сетевые настройки, вкладка «Маршрутизация»

Во вкладке **Маршрутизация** для добавления маршрута следует нажать кнопку **Добавить** и в открывшейся форме добавления заполнить необходимые поля, затем нажать **Сохранить** (Рис.3.86) :

- **Маршрут / шлюз по умолчанию** – установить или снять флажок (при необходимости);
- **Адрес назначения** – адрес сети или узла назначения;
- **Маска сети назначения** – для указания единичного узла сети используется маска 255.255.255.255;
- **Шлюз** – адрес маршрутизатора в сети, на который необходимо направлять пакеты, следующие до указанного адреса назначения;
- **Сетевой интерфейс** – сетевой интерфейс, через который доступен шлюз (выбор из выпадающего списка);
- **Метрика** – числовой показатель, определяющий предпочтительность маршрута.

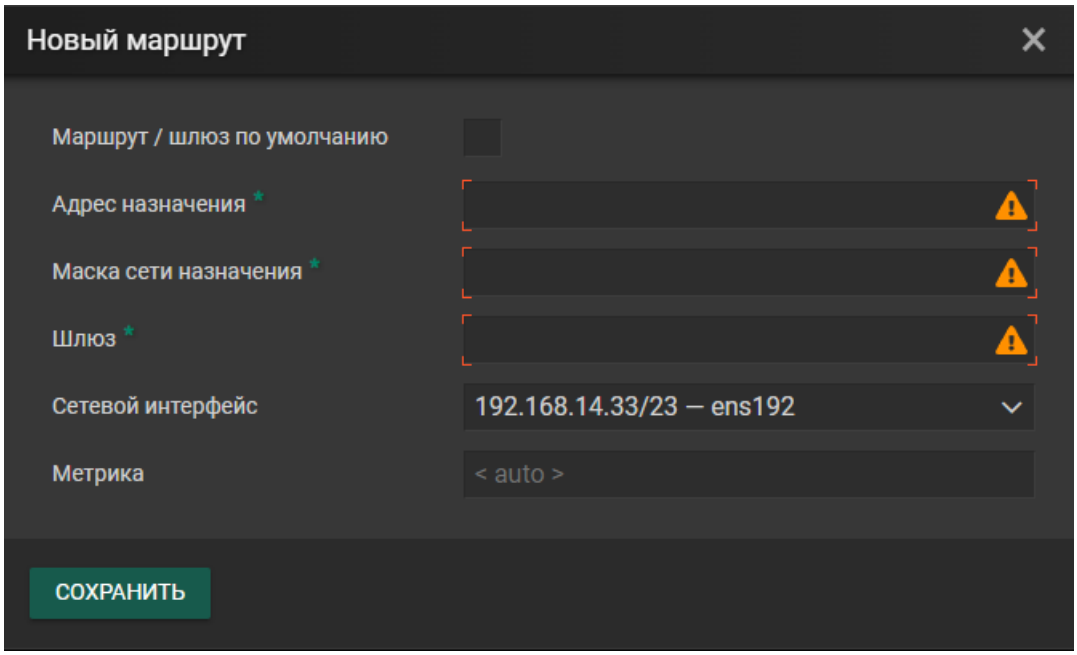


Рис. 3.86. Добавление нового маршрута

3.13.10. Брендирование

Для настройки визуального оформления пользовательского интерфейса в SafeConnect реализованы расширенные возможности.

Чтобы настроить пользовательский интерфейс:

1. Перейти в раздел **Настройки > Брендирование**;
2. Далее станут доступны два блока:
   - **Брендирование** (Рис.3.90);
   - **Предварительный просмотр** (Рис.3.88).
3. Внесите необходимые изменения в стандартные настройки:
   - Загрузить логотип по кнопке **Загрузить логотип** (для удаления логотипа нажать **Удалить логотип** внизу блока **Брендирование** (Рис.3.89));
   - Указать **Заголовок / наименование организации** (Рис.3.91). Наименование будет отображаться в левом верхнем углу вместо заголовка «SafeConnect» (Рис.3.91);
   - Выбрать **цветовую схему** (одну из предложенного списка) (Рис.3.92);
   - **Тема:** на выбор темная или светлая;
   - **Основной цвет:** установить курсор в поле выбора цвета > выбрать цвет с помощью шкалы цвета (1, Рис.3.93) > установить интенсивность цвета с помощью курсора (2, Рис.3.93) > установить яркость с помощью шкалы прозрачности (3, Рис.3.93);

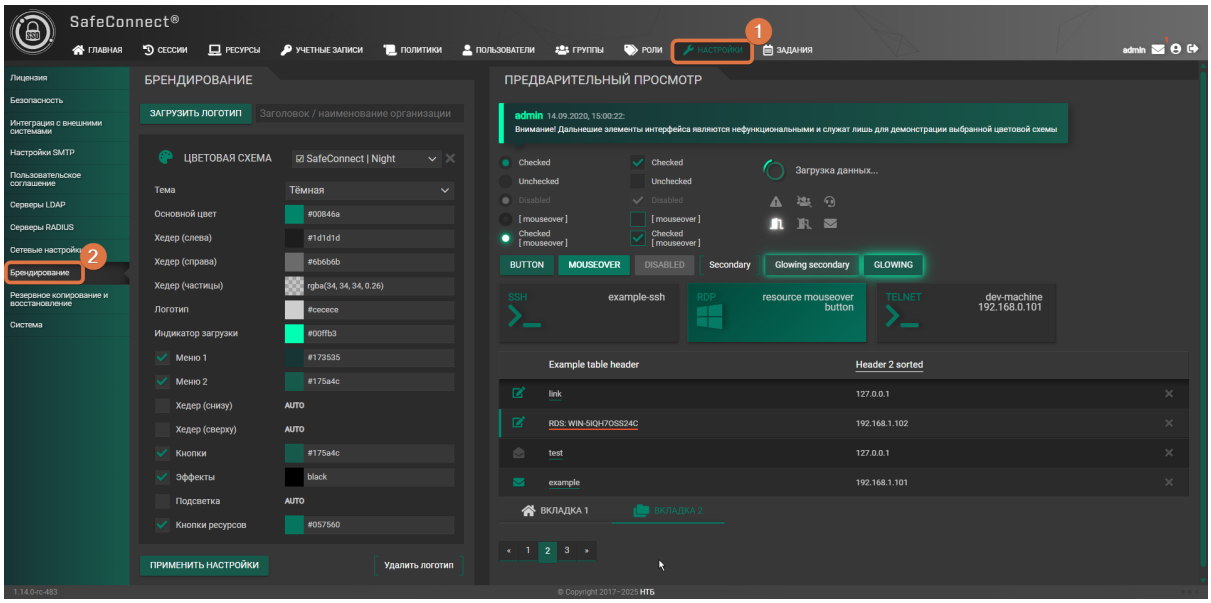


Рис. 3.87. Брендирование

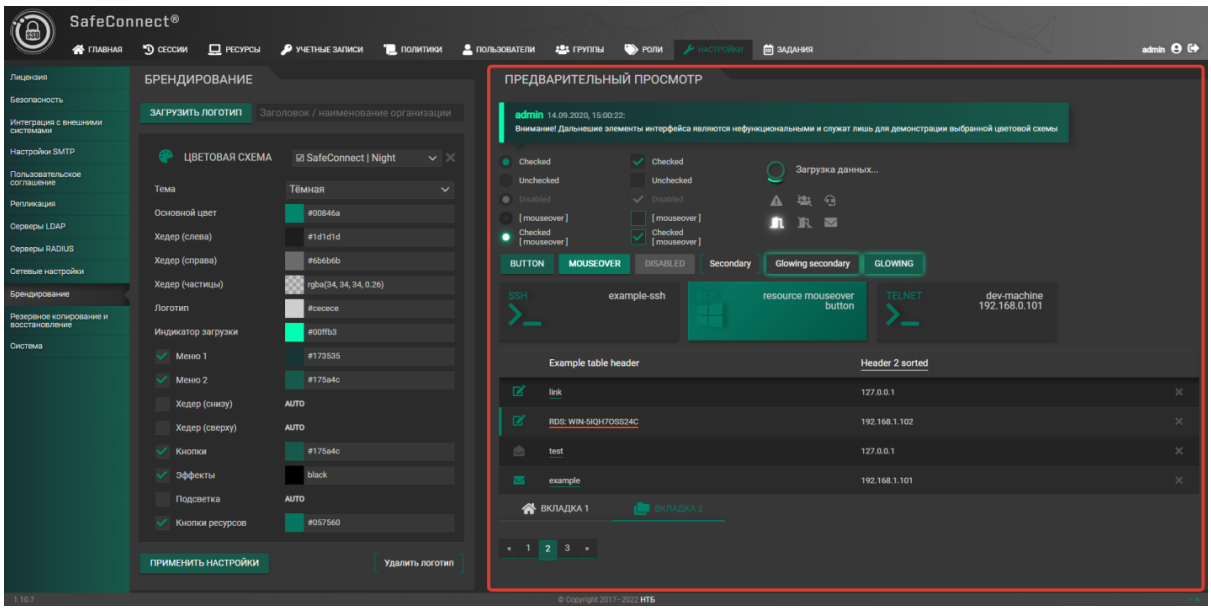


Рис. 3.88. Предварительный просмотр

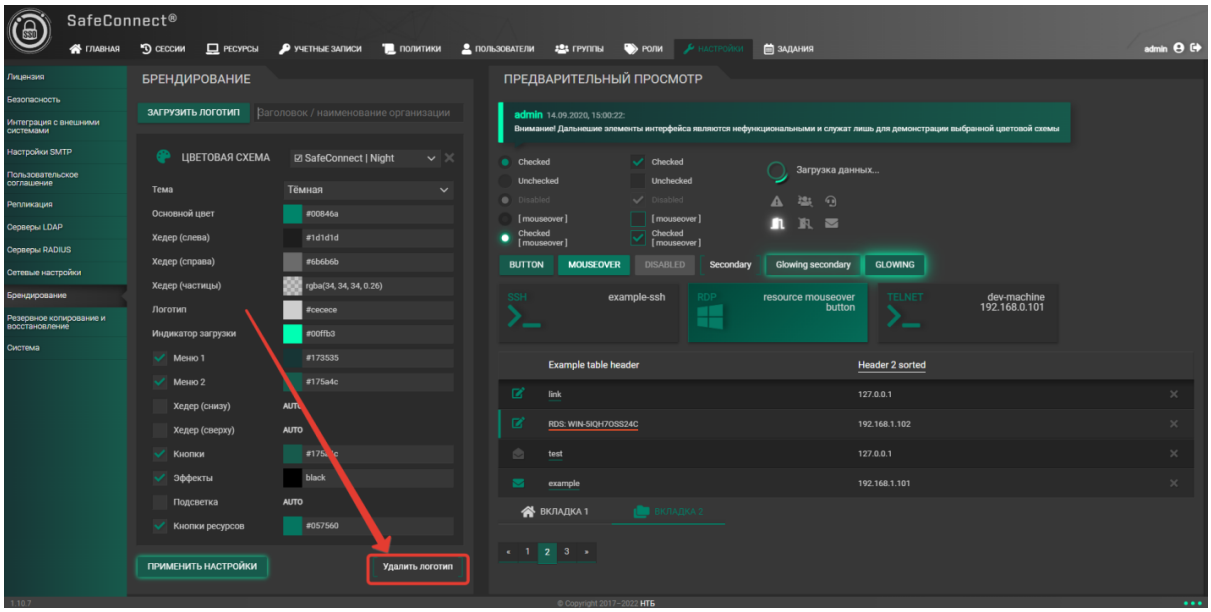


Рис. 3.89. Удаление логотипа

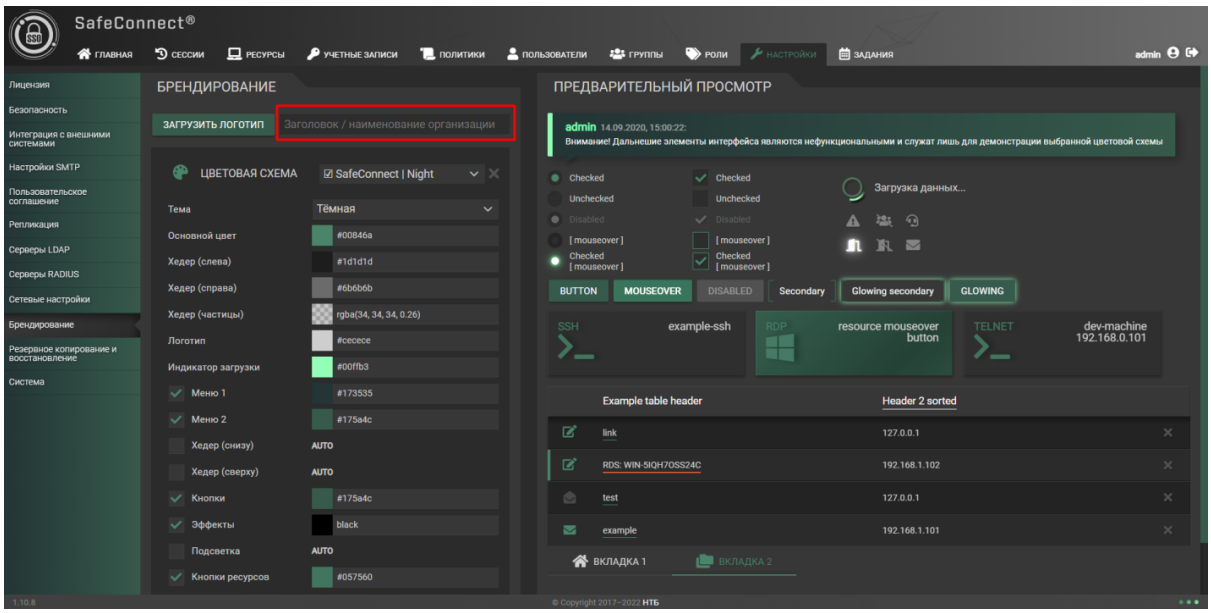


Рис. 3.90. Заголовок / наименование организации

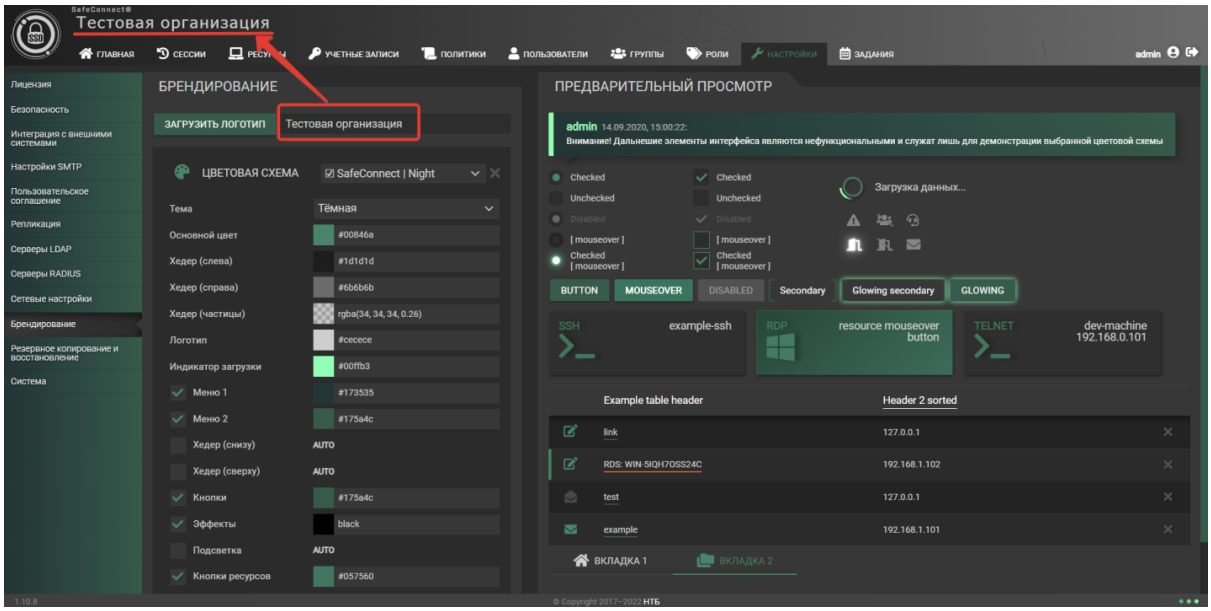


Рис. 3.91. Отображение наименования организации

- **Хедер (слева)** – установить курсор в поле выбора цвета > выбрать цвет с помощью шкалы цвета (1, Рис.3.93) > установить интенсивность цвета с помощью курсора (2, Рис.3.93) > установить яркость с помощью шкалы прозрачности (3, Рис.3.93);

- **Хедер (справа)** – установить курсор в поле выбора цвета > выбрать цвет с помощью шкалы цвета (1, Рис.3.93) > установить интенсивность цвета с помощью курсора (2, Рис.3.93) > установить яркость с помощью шкалы прозрачности (3, Рис.3.93);

Примечание

При выборе цвета для хедера слева и справа – фоновый цвет в «шапке» интерфейса будет отображен градиентом (Рис.3.94).

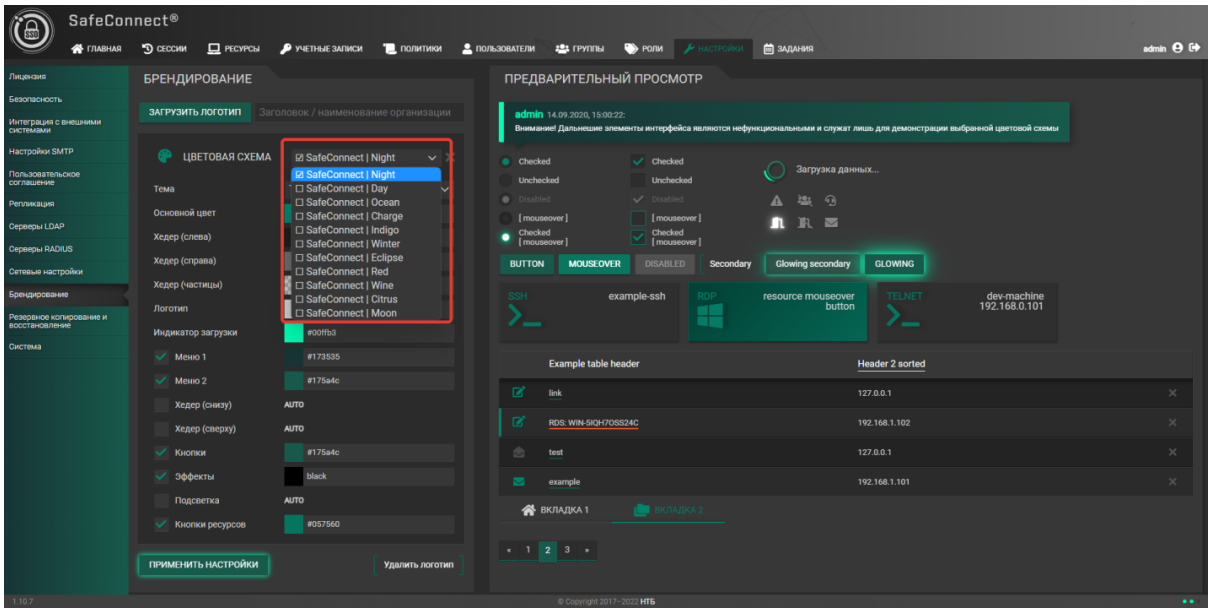


Рис. 3.92. Выбор цветовой схемы

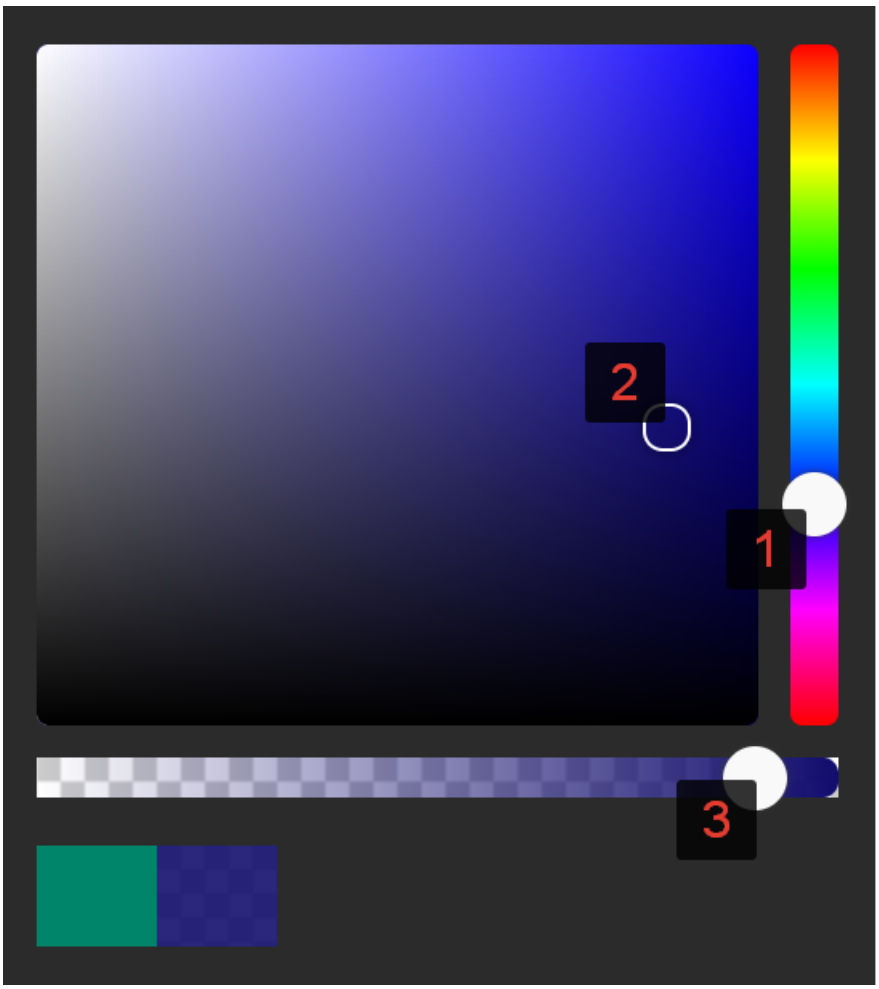


Рис. 3.93. Выбор цветовой гаммы

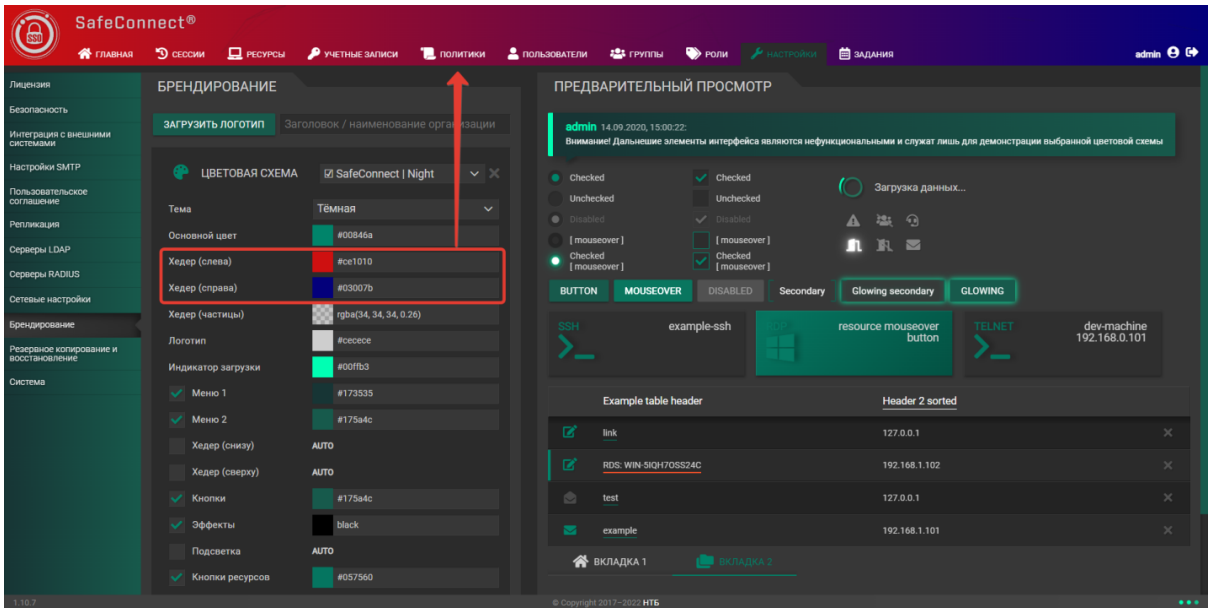


Рис. 3.94. Хедер слева и справа

- **Хедер (частицы)** – установить курсор в поле выбора цвета > выбрать цвет с помощью шкалы цвета (1, Рис.3.93) > установить интенсивность цвета с помощью курсора (2, Рис.3.93) > установить яркость с помощью шкалы прозрачности (3, Рис.3.93). В результате геометрические фигуры в «шапке» интерфейса примут выбранный цвет;

- **Логотип** – установить курсор в поле выбора цвета > выбрать цвет с помощью шкалы цвета (1, Рис.3.93) > установить интенсивность цвета с помощью курсора (2, Рис.3.93) > установить яркость с помощью шкалы прозрачности (3, Рис.3.93). В результате логотип и название «SafeConnect» примут выбранный цвет;

- **Индикатор загрузки** – установить курсор в поле выбора цвета > выбрать цвет с помощью шкалы цвета (1, Рис.3.93) > установить интенсивность цвета с помощью курсора (2, Рис.3.93) > установить яркость с помощью шкалы прозрачности (3, Рис.3.93). Изменения при выборе цвета будут отображены в блоке **Предварительный просмотр** (Рис.3.95);

- **Меню 1** – установить курсор в поле выбора цвета > выбрать цвет с помощью шкалы цвета (1, Рис.3.93) > установить интенсивность цвета с помощью курсора (2, Рис.3.93) > установить яркость с помощью шкалы прозрачности (3, Рис.3.93). Изменения при выборе цвета будут отображены в блоке **Предварительный просмотр**;

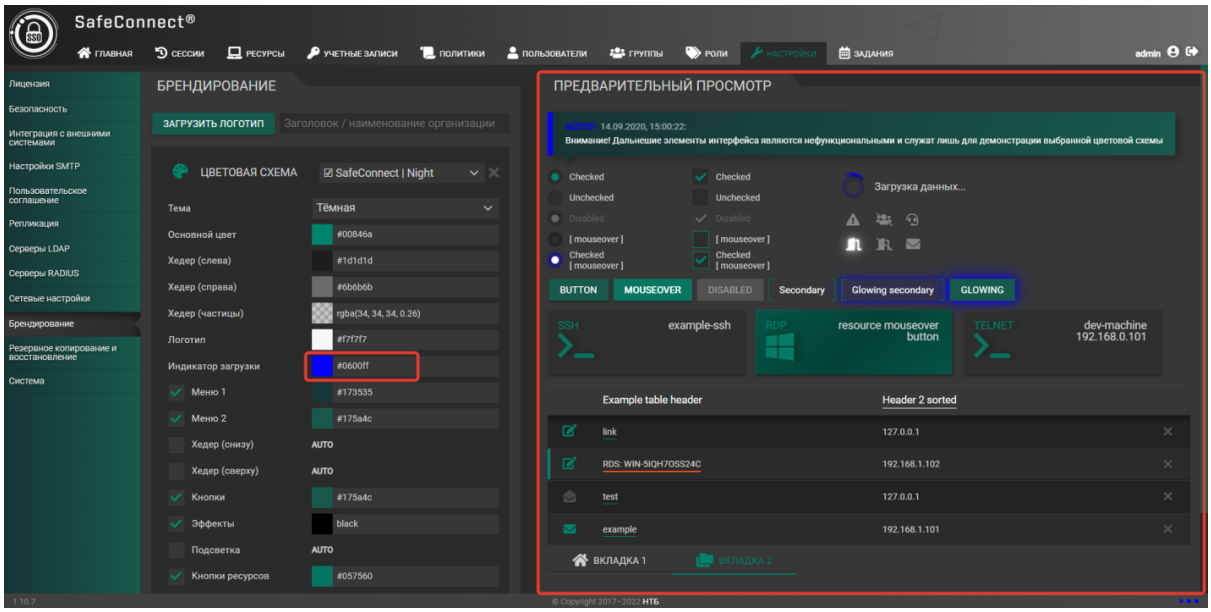


Рис. 3.95. Индикатор загрузки

- **Меню 2** – установить курсор в поле выбора цвета > выбрать цвет с помощью шкалы цвета (1, Рис.3.93) > установить интенсивность цвета с помощью курсора (2, Рис.3.93) > установить яркость с помощью шкалы прозрачности (3, Рис.3.93). Изменения при выборе цвета будут отображены в блоке **Предварительный просмотр**;

Примечание

При выборе цвета для меню 1 и меню 2 – фоновый цвет в меню интерфейса будет отображен градиентом (Рис.3.97).

- **Хедер (снизу)** – установить курсор в поле выбора цвета > выбрать цвет с помощью шкалы цвета (1, Рис.3.93) > установить интенсивность цвета с помощью курсора (2, Рис.3.93) > установить яркость с помощью шкалы прозрачности (3, Рис.3.93);
- **Хедер (сверху)** – установить курсор в поле выбора цвета > выбрать цвет с помощью шкалы цвета (1, Рис.3.93) > установить интенсивность цвета с помощью курсора (2, Рис.3.93) > установить яркость с помощью шкалы прозрачности (3, Рис.3.93);

Примечание

При выборе цвета для хедера сверху и снизу – фоновый цвет в «шапке» интерфейса будет отображен градиентом (Рис.3.97).

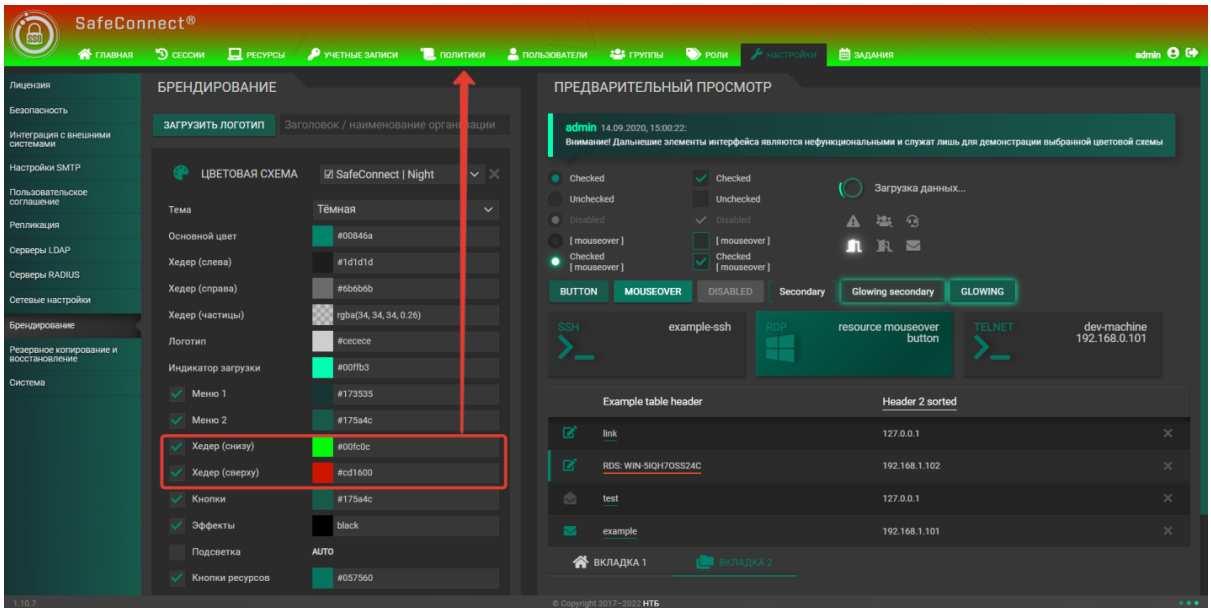


Рис. 3.96. Меню

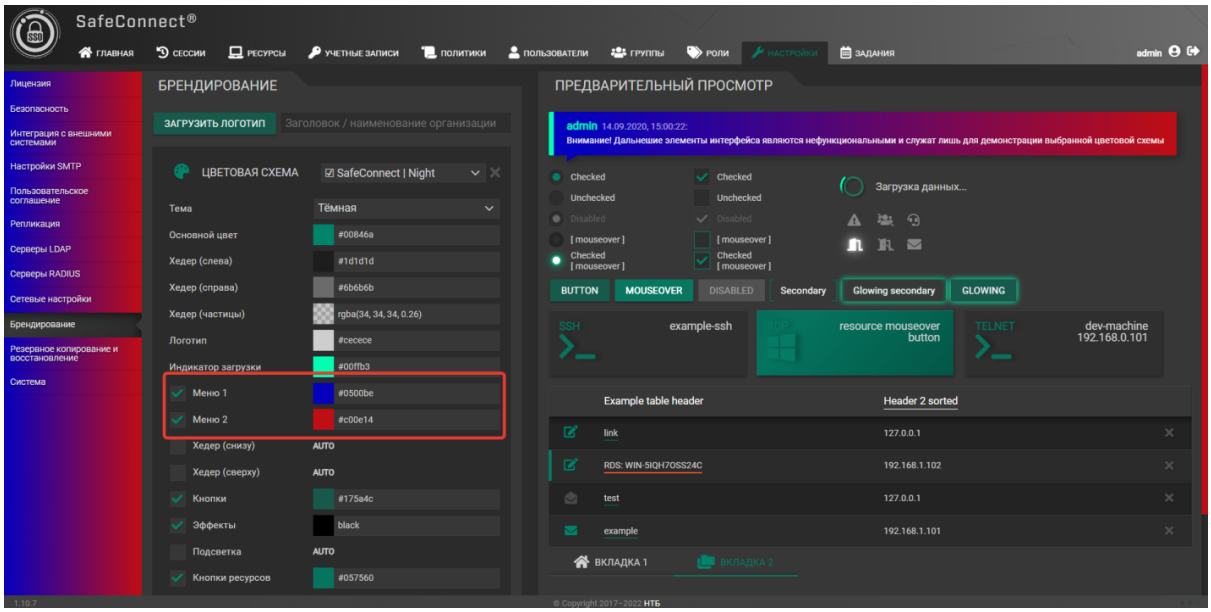


Рис. 3.97. Хедер снизу и сверху

- **Кнопки** – установить курсор в поле выбора цвета > выбрать цвет с помощью шкалы цвета (1, Рис.3.93) > установить интенсивность цвета с помощью курсора (2, Рис.3.93) > установить яркость с помощью шкалы прозрачности (3, Рис.3.93). Изменения при выборе цвета будут отображены в блоке **Предварительный просмотр**;

- **Эффекты** – установить курсор в поле выбора цвета > выбрать цвет с помощью шкалы цвета (1, Рис.3.93) > установить интенсивность цвета с помощью курсора (2, Рис.3.93) > установить яркость с помощью шкалы прозрачности (3, Рис.3.93). Изменения при выборе цвета будут отображены в блоке **Предварительный просмотр**;

- **Подсветка** – установить курсор в поле выбора цвета > выбрать цвет с помощью шкалы цвета (1, Рис.3.93) > установить интенсивность цвета с помощью курсора (2,

Рис.3.93) > установить яркость с помощью шкалы прозрачности (3, Рис.3.93). Изменения при выборе цвета будут отображены в блоке **Предварительный просмотр**;

- **Кнопки ресурсов** – установить курсор в поле выбора цвета > выбрать цвет с помощью шкалы цвета (1, Рис.3.93) > установить интенсивность цвета с помощью курсора (2, Рис.3.93) > установить яркость с помощью шкалы прозрачности (3, Рис.3.93). Изменения при выборе цвета будут отображены в блоке **Предварительный просмотр**.

  1. При внесении изменений ввести название пользовательской цветовой схемы;
  2. Нажать **Применить настройки** для сохранения настроек.

Сохраненная цветовая схема будет отображаться в списке цветовых схем (Рис.3.92).

3.13.11. Резервное копирование и восстановление

3.13.11.1. Создание резервной копии

Для создания резервной копии состояния системы и дальнейшего восстановления системы следует:

1. Перейти в раздел **Настройки > Резервное копирование и восстановление** (Рис.3.100).

   По умолчанию откроется вкладка **Резервное копирование**, в которой необходимо заполнить поля;

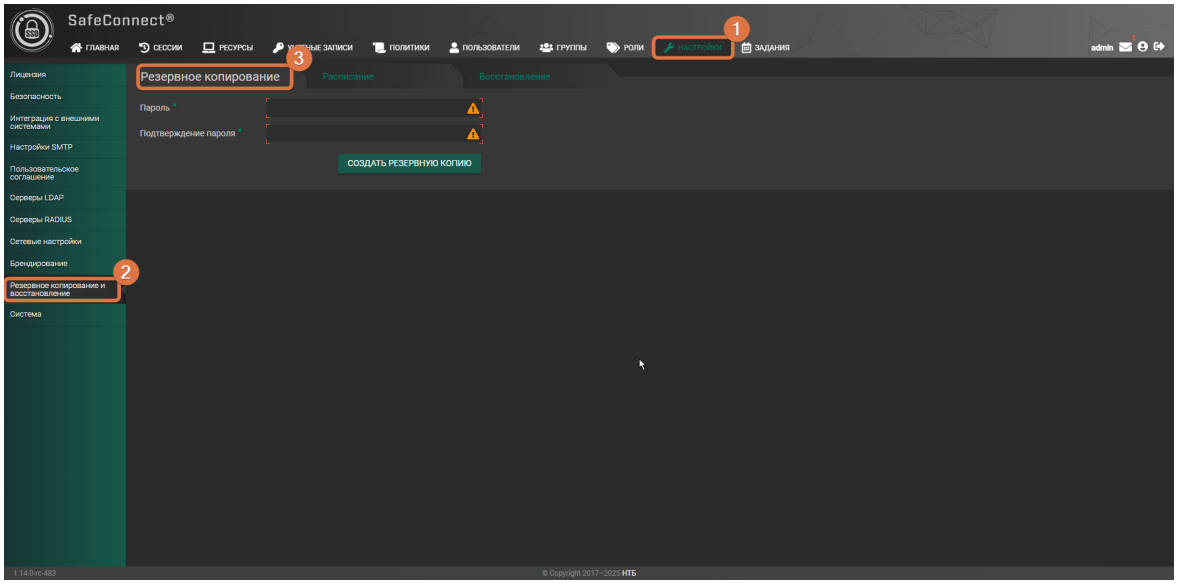


Рис. 3.98. Резервное копирование

2. Задать пароль для доступа к backup–файлу;
3. Ввести его повторно для проверки;
4. Нажать кнопку **Создать резервную копию**.

В результате резервная копия будет сохранена на ваше локальное хранилище.

3.13.11.2. Создание резервной копии по расписанию

Для создания резервной копии по расписанию следует:

1. Перейти в раздел **Настройки > Резервное копирование и восстановление**;
2. Перейти на вкладку **Расписание** (Рис.3.99);

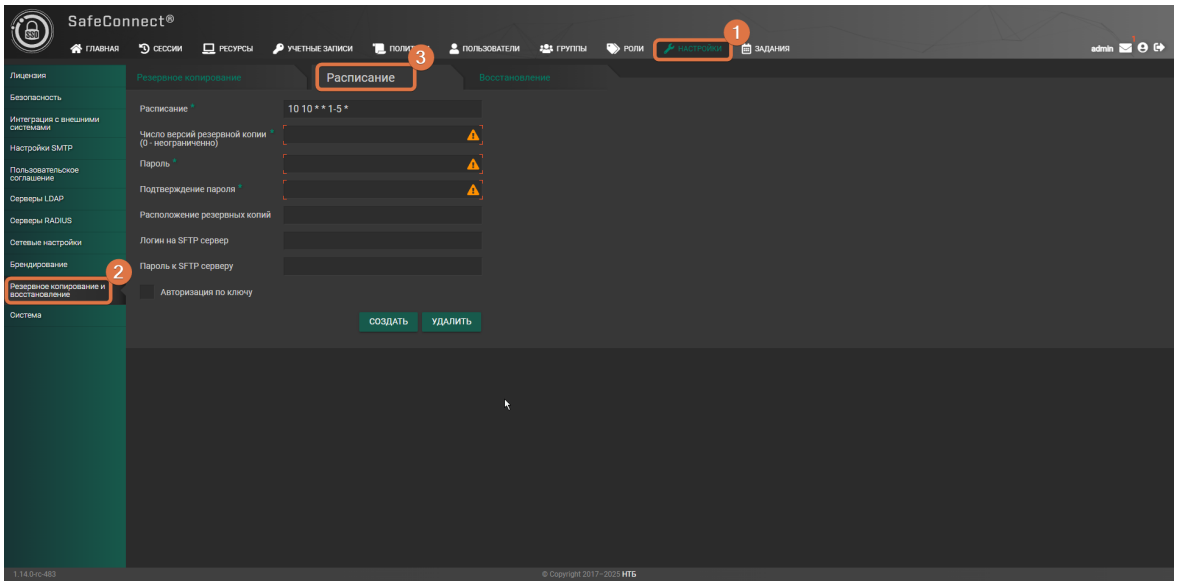


Рис. 3.99. Резервное копирование по расписанию

3. Заполнить поле **Расписание** (Рис.3.100).

   Доступны для заполнения: минуты, часы, числа, месяцы, дни недели, годы.

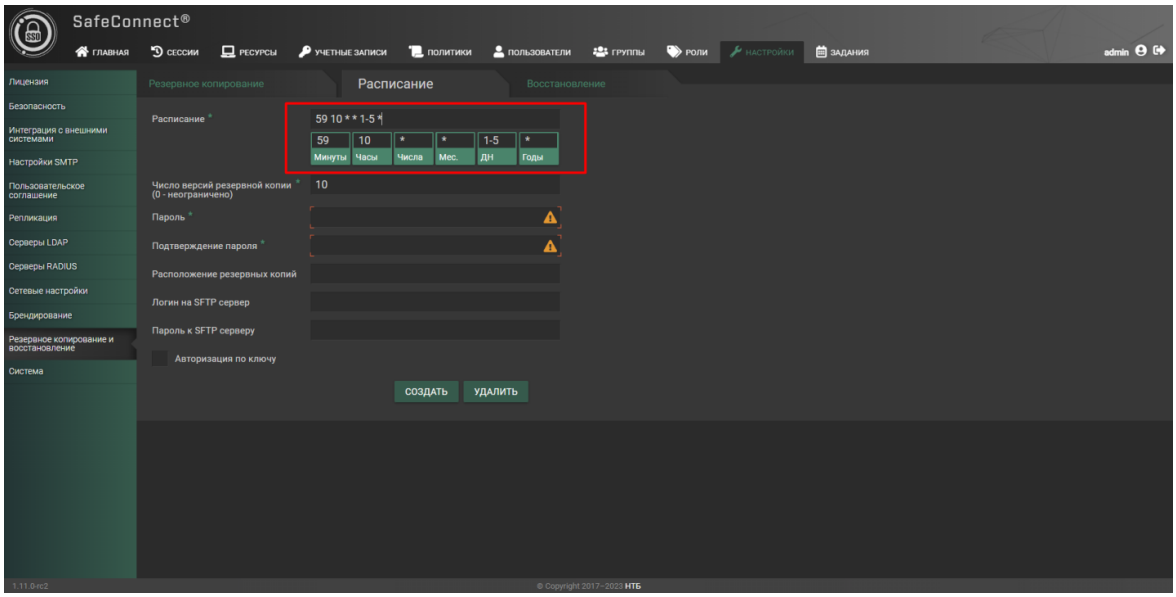


Рис. 3.100. Поле «Расписание»

4. Заполнить поле **Число версий резервной копии** (0 – не ограничено);

5. Заполнить поля **Пароль** и **Подтверждение пароля**;

6. При необходимости заполнить поля:

   - расположение резервных копий (полный путь на SFTP–сервере в формате [hostname:/path]). Если расположение не указано, резервные копии будут сохраняться локально (**/var/opt/sc–manager/backups**);
   - **логин на SFTP–сервер**;
   - **пароль к SFTP–серверу**;
   - авторизация по ключу – установить флажок  для авторизации по ключу (использовать ключ из раздела **Безопасность**, подробнее об использовании публичного ssh–ключа в разделе **Публичный**).

7. Нажать **Создать** для сохранения изменений и создания расписания.

Примечание

*Чтобы удалить расписание резервного копирования, следует нажать кнопку **Удалить**.*

3.13.11.3. Восстановление системы из резервной копии

Внимание!

Для корректного восстановления системы при настроенной репликации запуск восстановления из резервной копии обязателен с мастер-ноды.

Для восстановления системы следует:

1. Переключиться на вкладку **Восстановление** (Рис.3.101);
2. Нажать кнопку **Выберите файл**;
3. Выбрать сохраненный файл с резервной копией;
4. Ввести заданный пароль для этого файла;
5. При необходимости установить флажок **Восстановить системную конфигурацию** (настройки сети не восстанавливаются, если резервная копия была сделана на другой машине);
6. Нажать кнопку **Восстановить из файла**;
7. Дождаться окончания процесса восстановления.

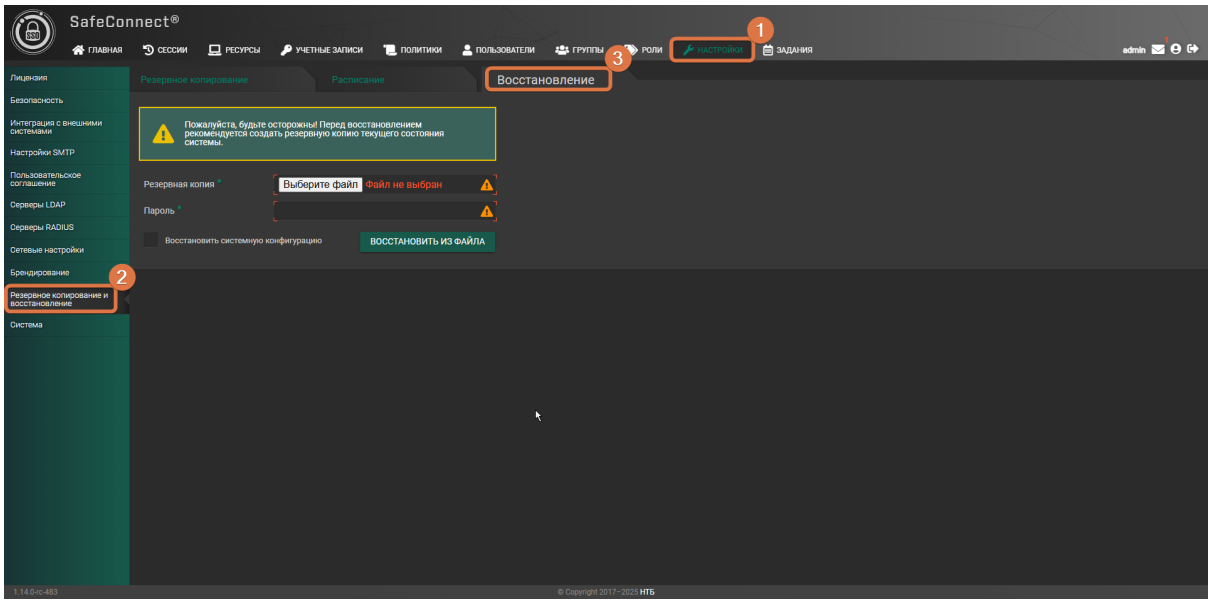


Рис. 3.101. Восстановление

3.13.12. Система

Раздел **Система** предназначен для обновления системы до более новой версии, для создания резервной копии, скачивания логов, завершения работы SafeConnect, перезагрузки системы, а также для перезапуска сервисов системы.

Раздел представлен тремя вкладками:

- Настройки;
- Обновление системы;
- Логи.

3.13.12.1. Вкладка «Настройки»

Во вкладке **Настройки** (Рис.3.102) доступны следующие функции:

- Установить периодичность синхронизации;

Примечание

На странице настроек системы отображается последний статус синхронизации.

- Завершить работу;
- Перегрузить систему;
- Перезапустить сервисы.

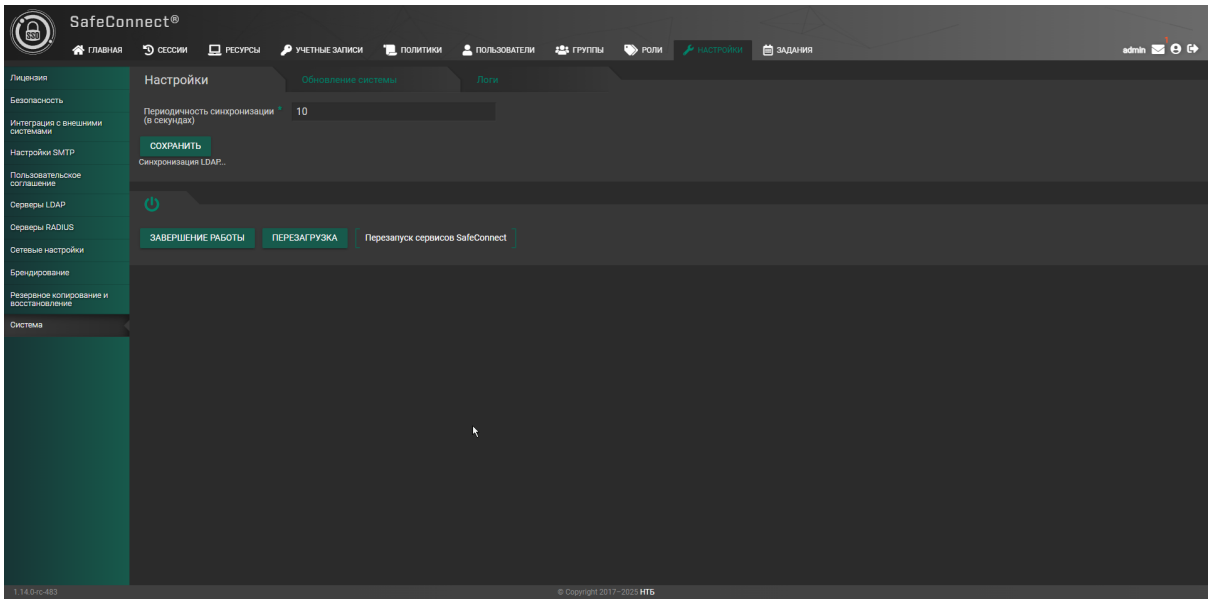


Рис. 3.102. Вкладка «Настройки»

Для установки периодичности синхронизации:

1. Перейти на вкладку **Настройки > Система**, вкладка **Настройки** (Рис.3.102);
2. В поле **Периодичность синхронизации (в секундах)** (Рис.3.107) установить время паузы (в секундах) между запусками синхронизации с каталогом LDAP и SafeInspect. В данном поле возможны значения от 1 до 3600.
3. Для сохранения изменений необходимо нажать кнопку **Сохранить**.

Примечание

Слишком частые синхронизации могут вызвать повышение нагрузки на SafeConnect и внешние сервисы.

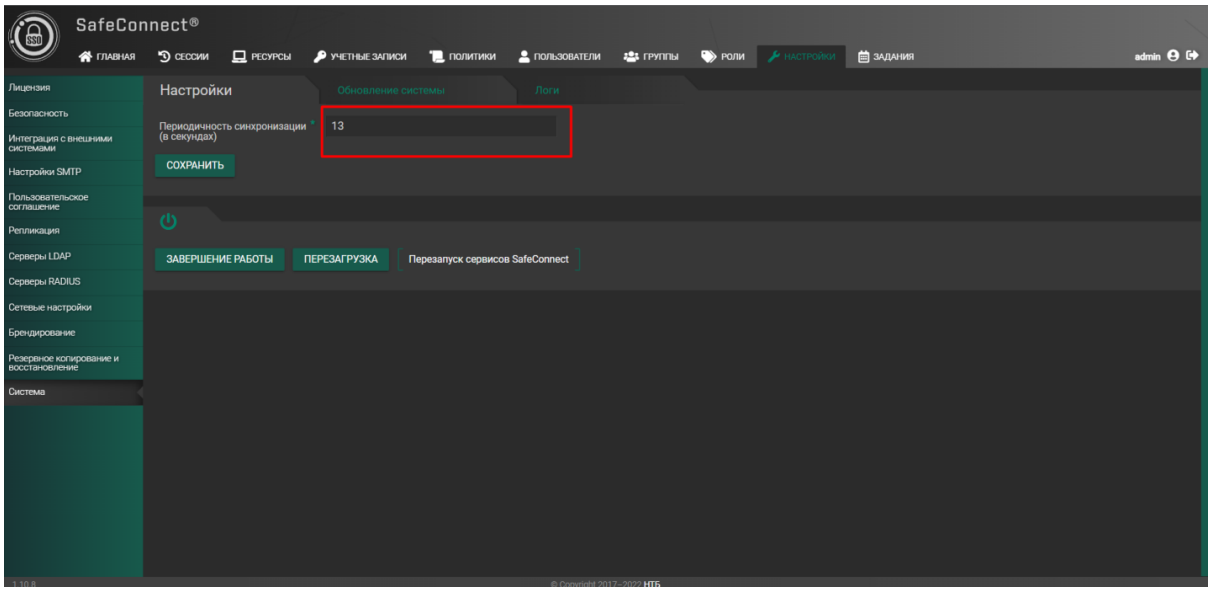


Рис. 3.103. Настройка периодичности синхронизации

Блок **Завершение работы и перезагрузка** расположен в рабочей области вкладки **Настройки** (Рис.3.104) .

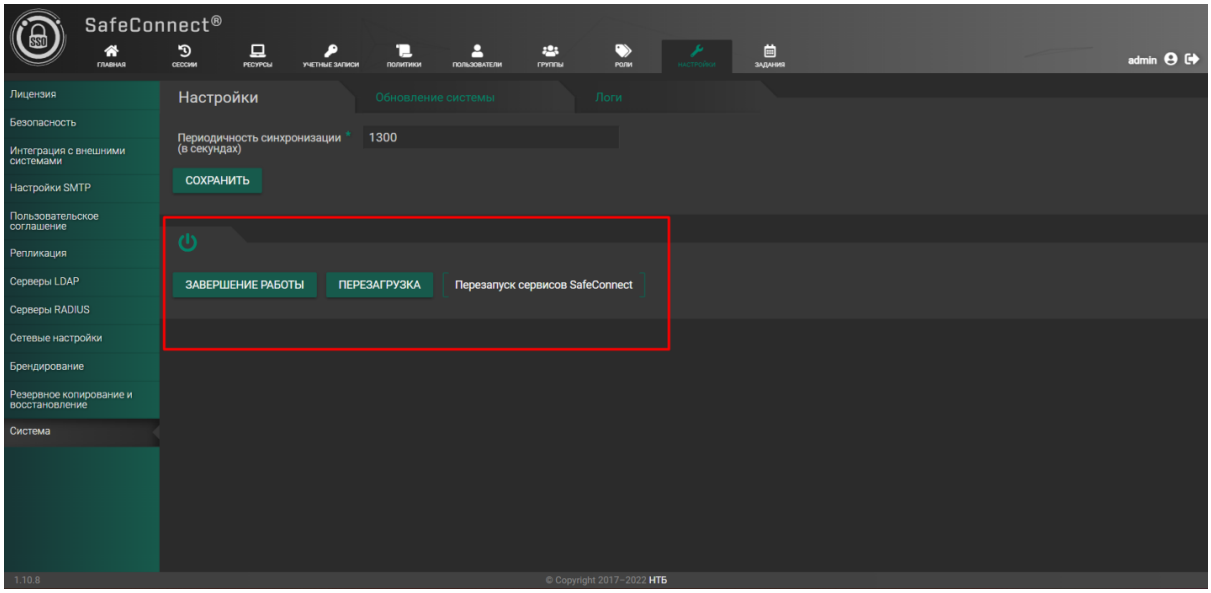


Рис. 3.104. Завершение и перезагрузка системы

Для завершения работы необходимо нажать кнопку **Завершение работы**, подтвердить завершение работы, нажав кнопку **ОК** в предупреждающем сообщении (Рис.3.105). В результате происходит выключение физической (виртуальной) машины через одну минуту (для корректного завершения всех процессов).

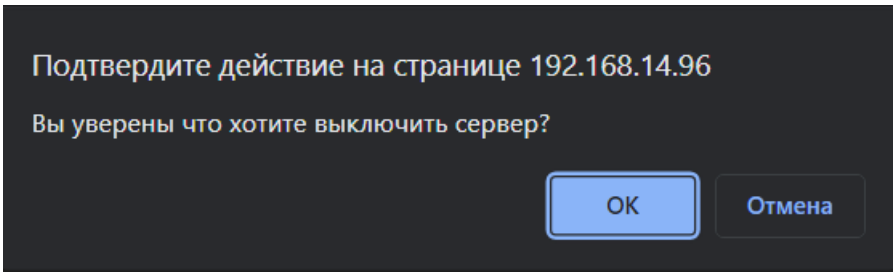


Рис. 3.105. Подтверждение выключения

Для перезагрузки системы необходимо воспользоваться кнопкой **Перезагрузка**, затем подтвердить перезагрузку, нажав кнопку **ОК** в предупреждающем сообщении (Рис.3.106). В результате происходит перезагрузка физической (виртуальной) машины через одну минуту (для корректного завершения всех процессов).

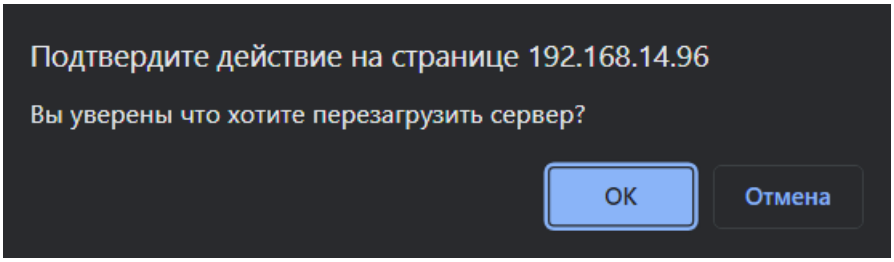


Рис. 3.106. Подтверждение перезагрузки

Для перезапуска сервисов необходимо воспользоваться кнопкой **Перезапуск сервисов** , затем подтвердить перезапуск, нажав кнопку **ОК** в предупреждающем сообщении (Рис.3.107). В результате происходит перезагрузка всех сервисов SafeConnect (manager, rdp, ssh, kiosk).

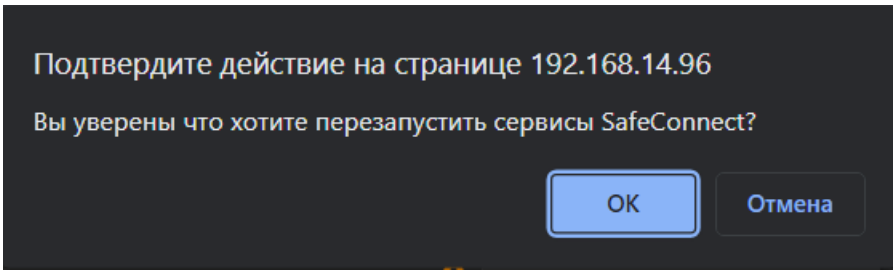


Рис. 3.107. Подтверждение перезапуска сервисов

3.13.12.2. Вкладка «Обновление системы»

Во вкладке **Обновление системы** (Рис.3.108) администратору предоставляется возможность создать резервную копию базы данных и обновить версию системы. В этом разделе отображается информация о текущей установленной версии, а также доступны функции завершения работы и перезагрузки SafeConnect.

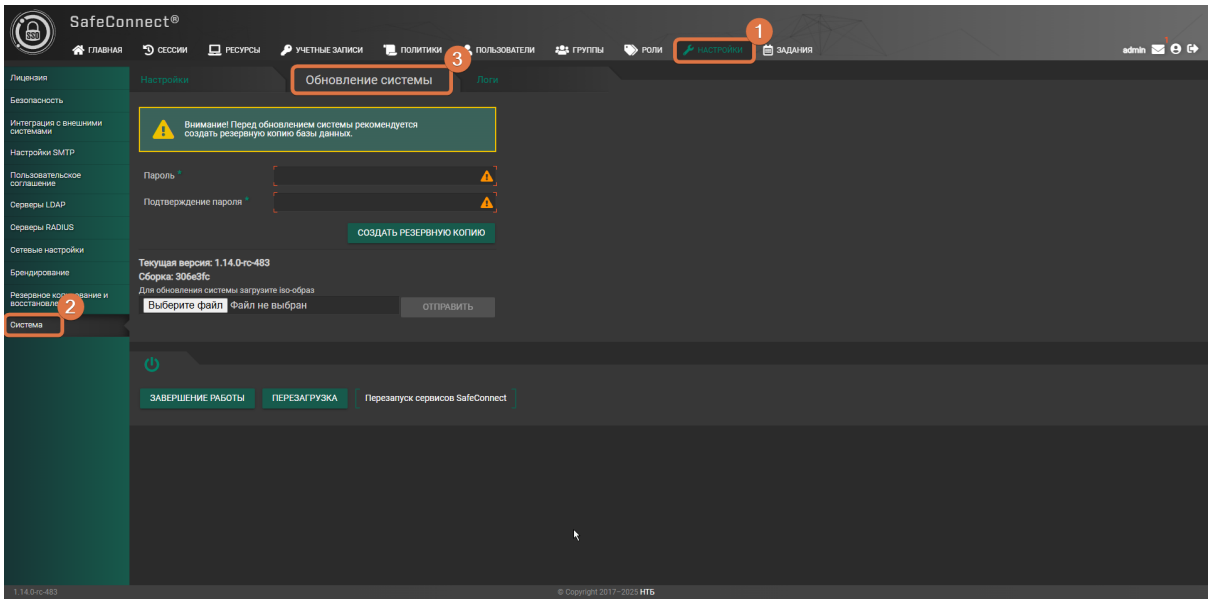


Рис. 3.108. Подраздел «Система»

3.13.12.2.1. Обновление системы

Внимание!

Перед обновлением системы необходимо ознакомиться с особенностями обновления системы в зависимости от версии, описанными в документе Solar_SafeConnect_X.XX.X_Release_Notes (где X.XX.X – номер версии системы).

Для обновления системы необходимо:

- **Создать резервную копию** базы данных (Рис.3.109):
  - Задать пароль для доступа к backup–файлу;
  - Ввести его повторно для проверки;
  - Нажать кнопку **Создать резервную копию**. Резервная копия будет сохранена на локальное хранилище пользователя.

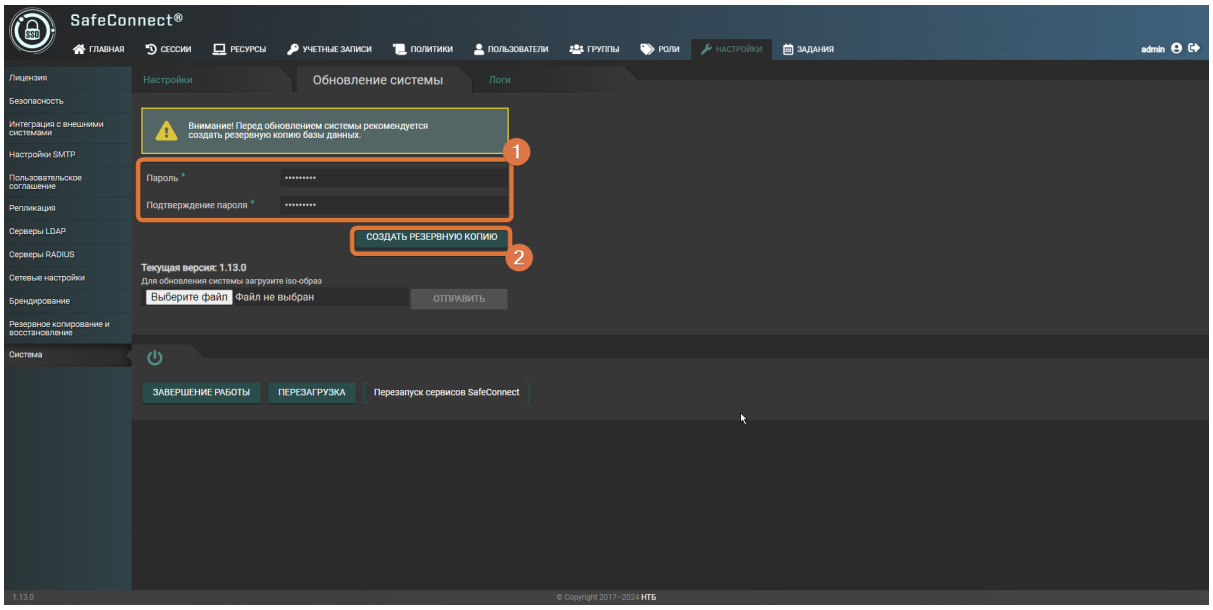


Рис. 3.109. Создание резервной копии

- Обновить систему (Рис.3.110):
  - Перейти на вкладку **Настройки > Система**, вкладка **Обновление системы**;
  - Нажать кнопку**Выберите файл**;
  - Выбрать iso –образ системы (после выбора файла обновления кнопка **Отправить** станет активной);
  - Нажать кнопку **Отправить**.

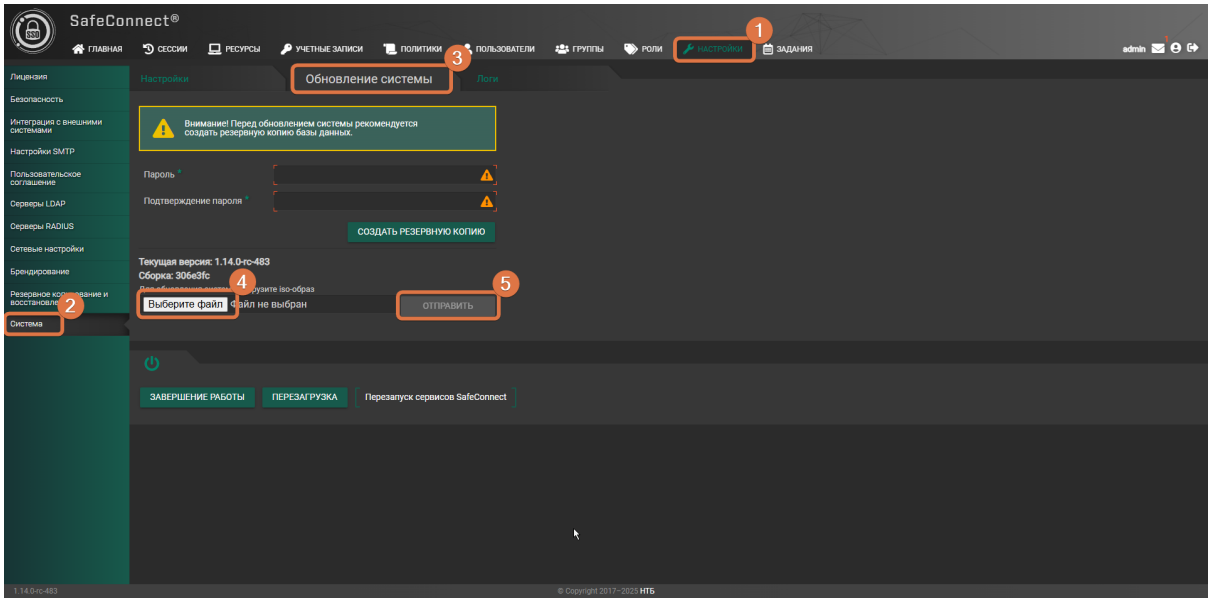


Рис. 3.110. Обновление системы

Процесс загрузки файла отображается с помощью прогресс–бара. По окончании загрузки отобразится строка состояния готовности обновления и кнопка **Установить**. Далее начнется процесс обновления системы, во время которого работа SafeConnect будет при-

остановлена. После завершения обновления стандартная работа SafeConnect будет возобновлена.

3.13.12.2.2. Завершение работы

Блок **Завершение работы и перезагрузка** расположен внизу рабочей области вкладки **Обновление системы** (Рис.3.111) .

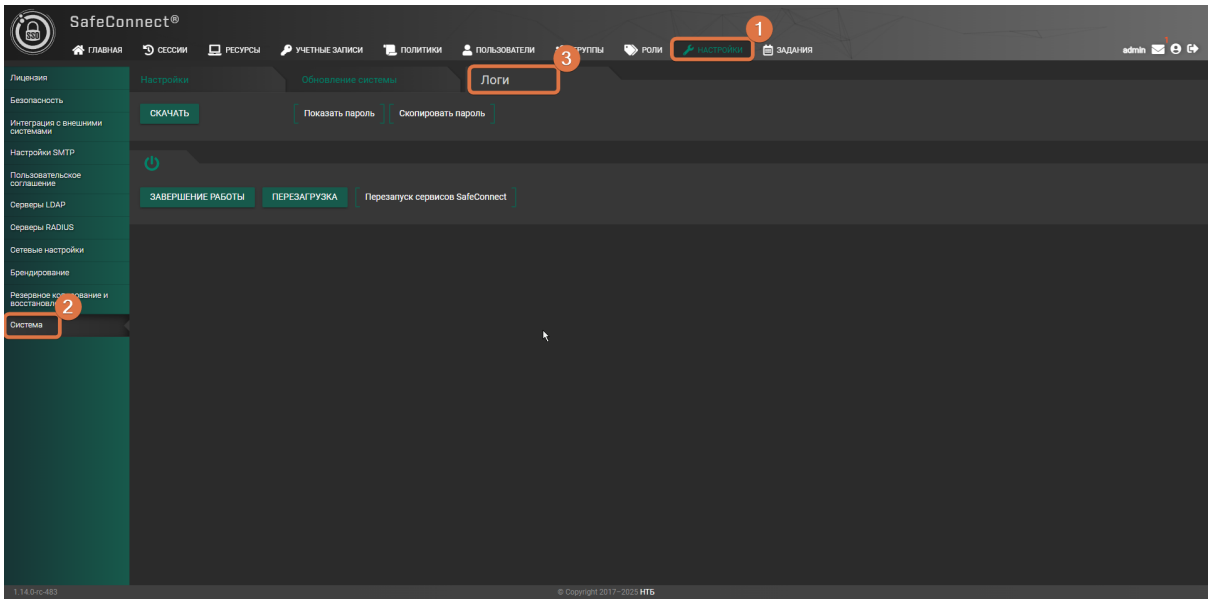


Рис. 3.111. Завершение и перезагрузка системы

Для завершения работы SafeConnect необходимо нажать кнопку **Завершение работы**, подтвердить завершение работы, нажав кнопку **ОК** в предупреждающем сообщении (Рис.3.112). В результате происходит выключение физической (виртуальной) машины через одну минуту (для корректного завершения всех процессов).

Для перезагрузки системы необходимо воспользоваться кнопкой **Перезагрузка**, затем подтвердить перезагрузку, нажав кнопку **ОК** в предупреждающем сообщении (Рис.3.106). В результате происходит перезагрузка физической (виртуальной) машины через одну минуту (для корректного завершения всех процессов).

Для перезапуска сервисов необходимо воспользоваться кнопкой **Перезапуск сервисов** , затем подтвердить перезапуск, нажав кнопку **ОК** в предупреждающем сообщении (Рис.3.107). В результате происходит перезагрузка всех сервисов SafeConnect (manager, rdp, ssh, kiosk).

3.13.12.3. Вкладка «Логи»

3.13.12.3.1. Загрузка и просмотр логов SafeConnect:

Для загрузки и просмотра логов SafeConnect:

1. Перейти на вкладку **Настройки > Система > Логи**;
2. Нажать кнопку **Скачать**. В результате на локальное хранилище будет скачан архив (с паролем), содержащий логи системы;

3. Нажать кнопку **Скопировать пароль**, чтобы скопировать пароль от архива, или нажать кнопку **Показать пароль**, чтобы ввести пароль вручную;

4. Необходимо воспользоваться данным паролем, чтобы открыть файлы скачанного архива, и посмотреть информацию в логах.

Блок **Завершение работы и перезагрузка** расположен в рабочей области вкладки **Логи** (Рис.3.112).

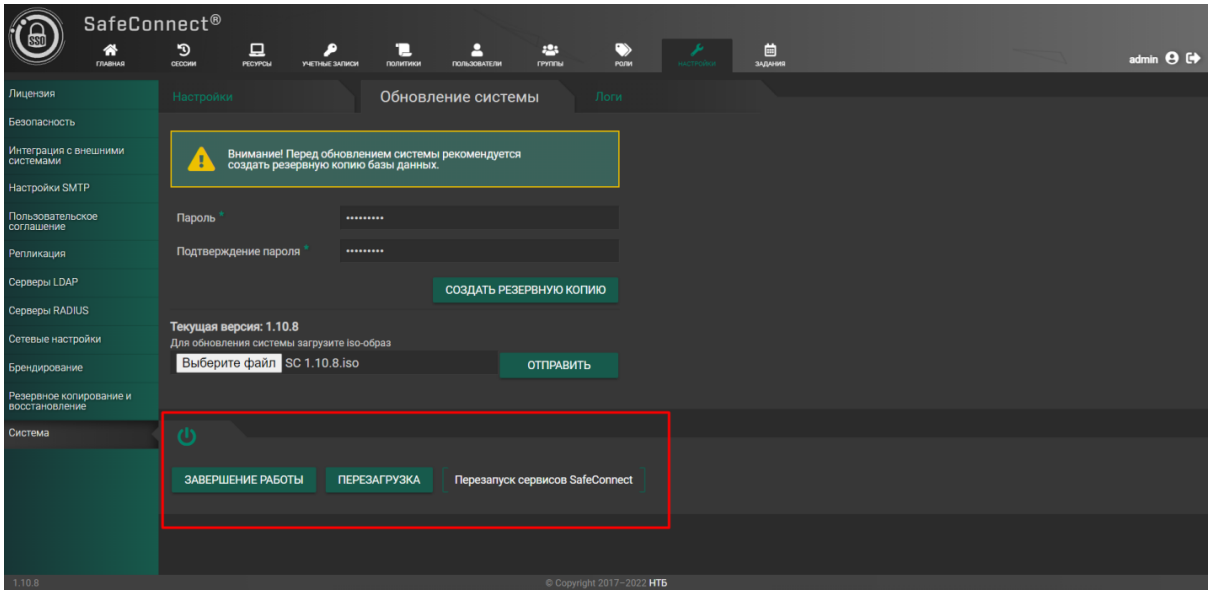


Рис. 3.112. Завершение и перезагрузка системы

Для завершения работы SafeConnect необходимо нажать кнопку **Завершение работы**, подтвердить завершение работы, нажав кнопку **ОК** в предупреждающем сообщении (Рис.3.112). В результате происходит выключение физической (виртуальной) машины через одну минуту (для корректного завершения всех процессов).

Для перезагрузки системы необходимо воспользоваться кнопкой **Перезагрузка**, затем подтвердить перезагрузку, нажав кнопку **ОК** в предупреждающем сообщении (Рис.3.106). В результате происходит перезагрузка физической (виртуальной) машины через одну минуту (для корректного завершения всех процессов).

Для перезапуска сервисов необходимо воспользоваться кнопкой **Перезапуск сервисов** , затем подтвердить перезапуск, нажав кнопку **ОК** в предупреждающем сообщении (Рис.3.107). В результате происходит перезагрузка всех сервисов SafeConnect (manager, rdp, ssh, kiosk).

3.13.12.3.2. Описание событий syslog

Раздел содержит систематизированную информацию о событиях, возникающих в процессе работы **SafeConnect**. Понимание структуры данных событий необходимо для эффективного мониторинга состояния системы, оперативного выявления инцидентов и проведения диагностических работ.

В представленной ниже таблице приведена классификация наиболее часто встречающихся типов событий, их функциональное назначение и характеристики.

Табл. 3.12. Описание распространенных событий

№	Пример сообщения	Описание	Тип события
1	Nov 26 15:49:53 nstportal sc-manager[172076]: [I 251126 15:49:53 login:126] Login: toor, Status: SUCCESS, Src IP: 10.201.167.190, Host name: (null), User agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Chromium GOST) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36	Удачная попытка входа в SafeConnect с локальной учетной записью	Login, Status: SUCCESS
2	Dec 11 15:51:16 nstportal sc-manager[52314]: [I 251211 15:51:16 login:28] Login: toor, Status: REJECT, Src IP: 172.17.0.2, Host name: (null), User agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36, Error: Неверный логин/пароль	Неудачная попытка входа в SafeConnect с локальной учетной записью	Login, Status: REJECT
3	Nov 18 15:35:57 nstportal sc-manager[692]: [I 251118 15:35:57 res:40] Resource_created: ID: 5, Name: rdp-93.185:3389, Address: 10.201.93.185, Port: 3389	Добавление ресурса	Resource_created
4	Nov 26 15:51:54 nstportal sc-manager[172076]: [I 251126 15:51:54 utils:49] Resource_changed, Id: 6, Name: rdp-93.192:3389, Params: Port 3389 to: 3388, Description to: 123	Изменение ресурса	Resource_changed
5	Nov 26 15:52:03 nstportal sc-manager[172076]: [I 251126 15:52:03 res:79] Resource_deleted, ID: 6, Name: rdp-93.192:3389, Address: 10.201.93.192, Port: 3388	Удаление ресурса	Resource_deleted
6	Dec 09 16:59:29 nstportal sc-manager[47819]: [I 251209 16:59:29 creds:32] Account_created, ID: 1, Login: toor	Создание учетной записи	Account_created
7	Nov 19 12:14:45 nstportal sc-manager[692]: [I 251119 12:14:45 utils:49] Account_changed, Id: 1, Name: tr, Params: Description to: ds!21343@'	Изменение учетной записи	Account_changed
8	Dec 12 20:27:22 email.pam.local sc-manager[52314]: [I 251212 20:27:22 creds:72] Account_deleted, ID: 2, Login: us1	Удаление учетной записи	Account_deleted
9	Nov 26 15:19:58 nstportal sc-manager[172076]: [I 251126 15:19:58 ldap:766] Starting sync LDAP: pam.local, LDAP vendor: Active Directory	Запуск синхронизации	Starting sync
10	Nov 26 15:19:58 nstportal sc-manager[172076]: [I 251126 15:19:58 ldap:665] Synchronization completed successfully	Успешное завершение синхронизации	Synchronization completed successfully
11	Nov 26 15:19:58 nstportal sc-manager[172076]: [I 251126 15:19:58 ldap:689] Starting sync LDAP users...	Запуск синхронизации пользователей LDAP	Starting sync LDAP users..
12	Nov 26 15:19:59 nstportal sc-manager[172076]: [I 251126 15:19:59 ldap:747] 29 users found in pam.local	Количество найденных пользователей	users found in
13	Nov 26 15:19:59 nstportal sc-manager[172076]: [I 251126 15:19:59 ldap:709] Sync LDAP users completed successfully.	Успешное завершение синхронизации пользователей LDAP	Sync LDAP users completed successfully
14	Dec 12 20:24:11 email.pam.local sc-manager[52314]: [I 251212 20:24:11 polices:51] Policy_created, ID: 3, Name: fff, Collector ID: None, Radius ID: None	Создание политики	Policy_created
15	Dec 12 20:28:04 email.pam.local sc-manager[52314]: [I 251212 20:28:04 polices:107] Policy_deleted, ID: 2, Name: 123, Collector ID: None, Radius ID: None	Удаление политики	Policy_deleted
16	Dec 12 20:26:48 email.pam.local sc-manager[52314]: [I 251212 20:26:48 utils:49] Policy_changed, Id: 3, Name: fff, Params:	Изменение политики	Policy_changed

№	Пример сообщения	Описание	Тип события
17	Nov 25 17:39:54 nstportal sc-manager[148306]: [I 251125 17:39:54 users:55] User_created, ID: 34, Name: batman, Status: 2	Создание пользователя	User_created
18	янв 15 12:31:18 nstportal sc-manager[205826]: [I 260115 12:31:18 utils:47] User_changed, Id: 3, Name: batman, {'Active': 1}, Params: Description to: batman	Изменение пользователя	User_changed
19	Dec 03 16:34:34 nstportal sc-manager[235899]: [I 251203 16:34:34 users:124] User_deleted, ID: 33, Name: local, Status: 2	Удаление пользователя	User_deleted
20	Dec 12 12:03:32 email.pam.local sc-manager[52314]: [I 251212 12:03:32 groups:55] UserGroup_created, ID: 29, Login: Test	Создание группы	UserGroup_created
21	Nov 25 18:39:46 nstportal sc-manager[148306]: [I 251125 18:39:46 utils:49] UserGroup_changed, Id: 101, Name: 123, Params: , Users [] to: ['batman']	Изменение группы	UserGroup_changed
22	Nov 19 12:19:33 nstportal sc-manager[90930]: [I 251119 12:19:33 groups:98] UserGroup_deleted, ID: 128, Login: 123213	Удаление группы	UserGroup_deleted
23	Dec 12 17:24:39 email.pam.local sc-manager[52314]: [I 251212 17:24:38 roles:39] Role_created, ID: 12, Name: Тест, Rights: []	Создание роли	Role_created
24	янв 15 12:34:35 nstportal sc-manager[205826]: [I 260115 12:34:35 utils:49] Role_changed, Id: 11, Name: Администратор политик, Params:	Изменение роли	Role_changed
25	Dec 12 17:24:59 email.pam.local sc-manager[52314]: [I 251212 17:24:59 roles:78] Role_deleted, ID: 12, Name: Тест, Rights: []	Удаление роли	Role_deleted
26	Nov 19 12:18:03 nstportal sc-manager[90844]: [I 251119 12:18:03 license:32] License loaded, active	Лицензия загружена, активна	License loaded, active
27	Nov 19 12:18:03 nstportal sc-manager[90844]: [I 251119 12:18:03 license:33] { ... Nov 19 12:18:03 nstportal sc-manager[90844]: "expiry_date": "2026-02-25 14:01:27",	Дата истечения срока действия лицензии	license expiry_date
28	Nov 19 12:18:03 nstportal sc-manager[90844]: [I 251119 12:18:03 license:33] { ... Nov 19 12:18:03 nstportal sc-manager[90844]: "creation_date": "2025-02-25 14:01:27",	Дата создания лицензии	license creation_date
29	Nov 19 12:18:03 nstportal sc-manager[90844]: [I 251119 12:18:03 license:33] { ... Nov 19 12:18:03 nstportal sc-manager[90844]: "server_resource_limit": 10000,	Максимальное количество ресурсов (хостов)	license server_resource_limit
30	Nov 19 12:18:03 nstportal sc-manager[90844]: [I 251119 12:18:03 license:33] { ... Nov 19 12:18:03 nstportal sc-manager[90844]: "serial_number": "294762472445801-38809676716587",	Серийный номер лицензии	license serial_number

№	Пример сообщения	Описание	Тип события
31	Nov 19 12:18:03 nstportal sc-manager[90844]: [I 251119 12:18:03 license:33] { ... Nov 19 12:18:03 nstportal sc-manager[90844]: "version": "1.9"	Версия продукта загруженной лицензии	license version
32	Dec 16 18:21:17 email.pam.local sc-manager[52314]: [D 251216 18:21:17 base:353] {'background_timeout': '1812'}	Изменена периодичность синхронизации	background_timeout
33	Dec 16 18:11:52 email.pam.local sc-manager[52314]: [I 251216 18:11:52 requests_api:192] Request_created, Request Id: 3, Subject: test_ks_zzz, Task: dsfsdgdagadgasg, Request type: 0, Access: [], External request id: , Assignee_users: [], Assignee_groups: []	Добавлено задание на техническую поддержку	Request_created
34	Dec 16 18:13:07 email.pam.local sc-manager[52314]: [I 251216 18:13:07 utils:49] Request_changed, Id: 3, Name: test_ks_fff, Params: Subject test_ks_zzz to: test_ks_fff	Изменено задание на техническую поддержку	Request_changed
35	Dec 16 18:14:28 email.pam.local sc-manager[52314]: [I 251216 18:14:28 messages:46] Request_new_comment, Task Id: 3, Name: test_ks_fff, Message: test test test, Author: root	Добавлен комментарий к заданию	Request_new_comment
36	Dec 16 18:14:36 email.pam.local sc-manager[52314]: [I 251216 18:14:36 requests_api:271] Request_completed, Task Id: 3, Subject: test_ks_fff, Status: Closed	Задание на техническую поддержку завершено	Request_completed
37	Dec 16 18:15:55 email.pam.local sc-manager[52314]: [I 251216 18:15:55 requests_api:192] Request_created, Request Id: 4, Subject: test_ks_ddddd, Task: орлорлорлорло, Request type: 1, Access: [], External request id: , Assignee_users: [], Assignee_groups: []	Добавлено задание	Request_created
38	Dec 16 18:16:25 email.pam.local sc-manager[52314]: [I 251216 18:16:25 utils:49] Request_changed, Id: 4, Name: test_ks_xxxxxx, Params: Subject test_ks_ddddd to: test_ks_xxxxxx	Изменено задание	Request_changed
39	Dec 16 18:20:27 email.pam.local sc-manager[52314]: [I 251216 18:20:27 requests_api:271] Request_completed, Task Id: 4, Subject: test_ks_xxxxxx, Status: Closed	Задание завершено	Request_completed
40	Restarting server after backup recovery	Начало восстановления из бэкапа	Restarting server
41	User: username privacy accepted: True	Пользователь принял пользовательское соглашение	privacy accepted: True
42	Nov 26 15:50:16 nstportal sc-manager[172076]: [I 251126 15:50:16 ldap:766] Starting sync LDAP: pam.local, LDAP vendor: Active Directory	Начало синхронизации с LDAP	Starting sync LDAP
43	Starting Sync local Users SI: 10.20.30.40	Начало синхронизации объектов с SafeInspect	Starting sync ... SI

3.14. Раздел «Задания»

Раздел **Задания** предназначен для формирования заданий пользователям SafeConnect и просмотра заданий, полученных от пользователей. В рабочей области раздела расположена таблица со списком заданий (Рис.3.113).

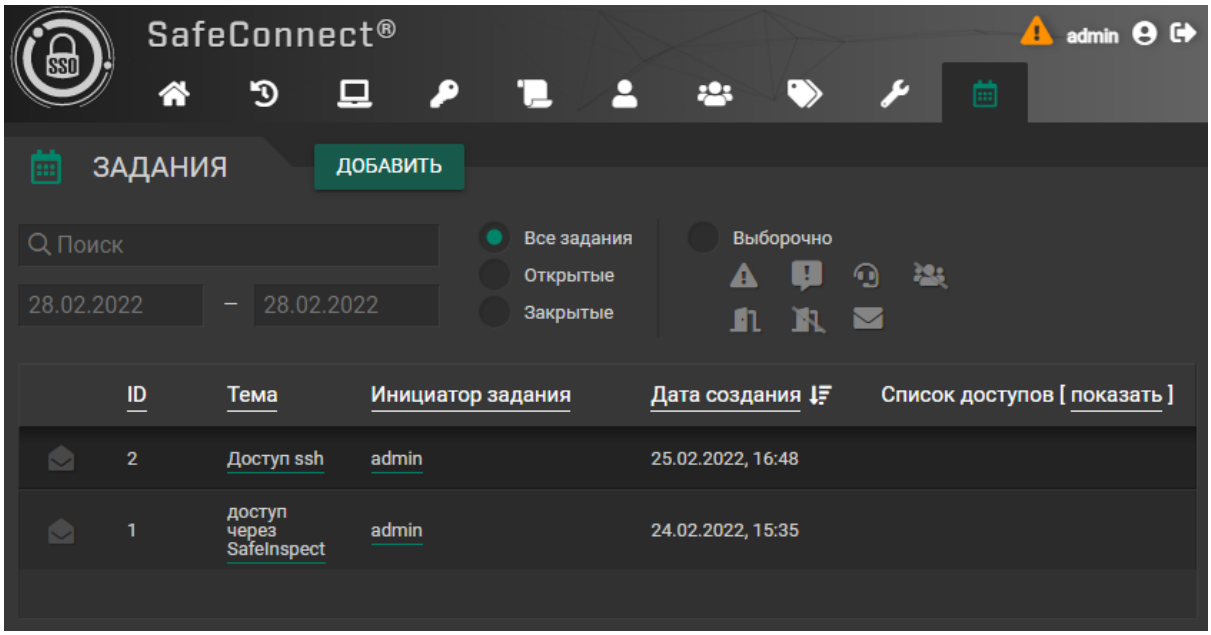


Рис. 3.113. Раздел «Задания»

По каждому заданию отображается следующая информация:

- **ID** – идентификационный номер задания;
- **Тема** – заголовок задания;
- **Инициатор задания** – имя отправителя;
- **Дата создания** – дата и время создания сообщения;
- **Список доступов** (с дополнительной кнопкой **показать/скрыть**) – раскрывает/скрывает список доступов, который участвует в задании, тип его авторизации, адрес, а также отображает будет ли идти соединение через Коллектор и его адрес.

Для удобства пользователя имеется возможность фильтрации списка заданий по теме, номеру задания, имени пользователя, названию ресурса, интервалу времени.

3.14.1. Добавление задания

Для добавления задания следует:

1. Перейти в раздел **Задания**;
2. Нажать кнопку **Добавить**;
3. На форме **Новое задание** выбрать тип сообщения:
   - Доступ к ресурсам (Рис.3.114);
   - Техническая поддержка (Рис.3.115);
4. Заполнить поля соответствующей формы:
   - Форма Доступ к ресурсам

- Форма Техническая поддержка.

Форма **Доступ к ресурсам**:

1. Заполнить поля:
   - **Тема** – ввести тему задания;
   - **Описание** – добавить описание;
   - **Номер задания** во внешней системе (при наличии);
2. Для добавления исполнителей (пользователей или групп) нажать **Добавить**. Появится окно **Исполнители** .
3. Выбрать вкладку **Группы** (Рис.3.114) или **Пользователи** (Рис.3.114).
4. С помощью флажков отметить необходимые элементы из списка (для выбора всех – установить флажок в шапке таблицы (Рис.3.114)). Для поиска пользователя или группы из списка необходимо воспользоваться полем **+ Добавить группу из списка** / **+ Добавить пользователя из списка**: начать вводить название и выбрать из выпадающего списка кликом мыши (Рис.3.119).
5. Нажать **Применить**.
6. Для добавления доступов нажать кнопку **Добавить**, появится окно **Доступ к ресурсу**:
7. Выбрать ресурс из выпадающего списка;
8. Выбрать тип авторизации:
   - **Сквозная**;
   - **Сопоставление**
   - **Интерактивная**.
9. Выбрать из списка удаленную учетную запись (для типа авторизации сопоставление);
10. Указать количество подключений;
11. С помощью флажков отметить необходимые политики;
12. Нажать **Применить**;

После внесения информации нажать кнопку **Сохранить**. Информация о созданном задании появится в списке заданий.

Примечание

После добавления доступа в задание, он остается в неподтвержденном состоянии!

Для подтверждения доступа нажать кнопку **Подтвердить**, статус изменится на **Разрешено**, и задание станет отображаться исполнителю.

Для отклонения доступа нажать кнопку , статус изменится на **Отменено**.

Для удаления доступа нажать на значок «крестик», статус изменится на **Отмечен на удаление**. Затем требуется подтвердить удаление кнопкой **Сохранить**, статус изменится на **Удален**.

Примечание

До момента подтверждения/отклонения/удаления доступа есть возможность редактирования задания по кнопке  *(подробнее в разделе 3.14.4).*

Форма **Техническая поддержка**:

1. Заполнить поля:
   - **Тема** – ввести тему задания;
   - **Описание** – добавить описание;
   - **Номер задания** во внешней системе (при наличии);
2. Для добавления исполнителей (пользователей или групп) нажать **Добавить**Появится окно **Исполнители**
3. Выбрать вкладку **Группы** (Рис.3.120) или **Пользователи** (Рис.3.120);
4. С помощью флажков отметить необходимые элементы из списка (для выбора всех – установить флажок в шапке таблицы (Рис.3.118)). Для поиска пользователя или группы из списка необходимо воспользоваться полем **+ Добавить группу из списка** / **+ Добавить пользователя из списка**: начать вводить название и выбрать из выпадающего списка кликом мыши (Рис.3.119);
5. Нажать **Применить**;
6. Нажать кнопку **Сохранить** для сохранения задания.

Информация о созданном задании появится в списке заданий.

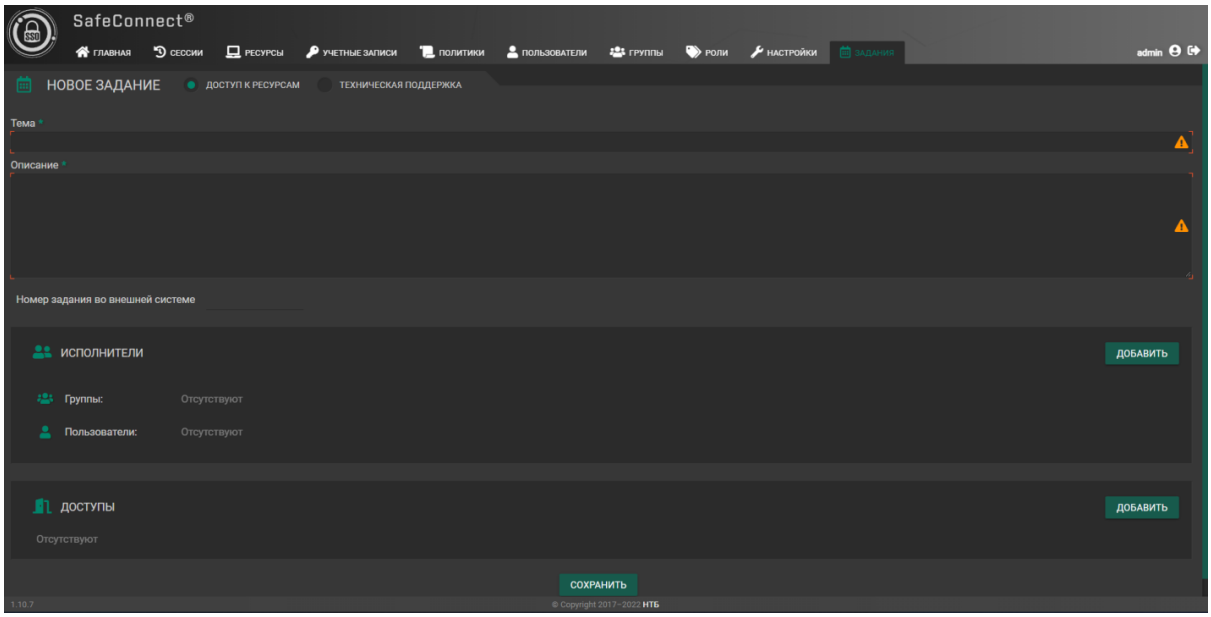


Рис. 3.114. Доступ к ресурсам

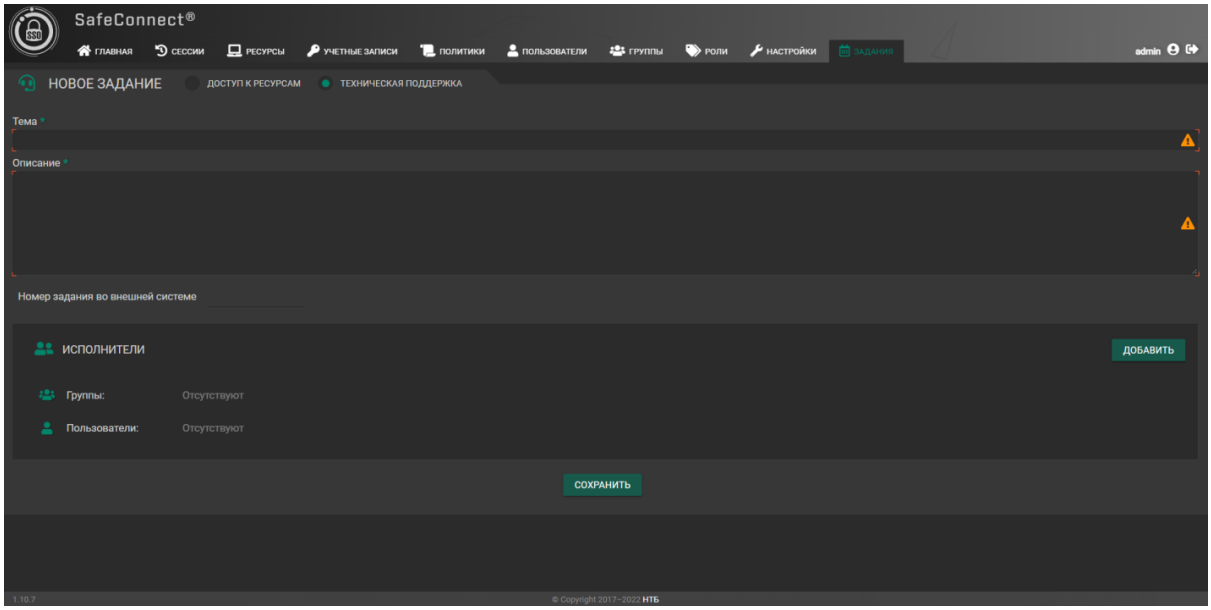


Рис. 3.115. Техническая поддержка

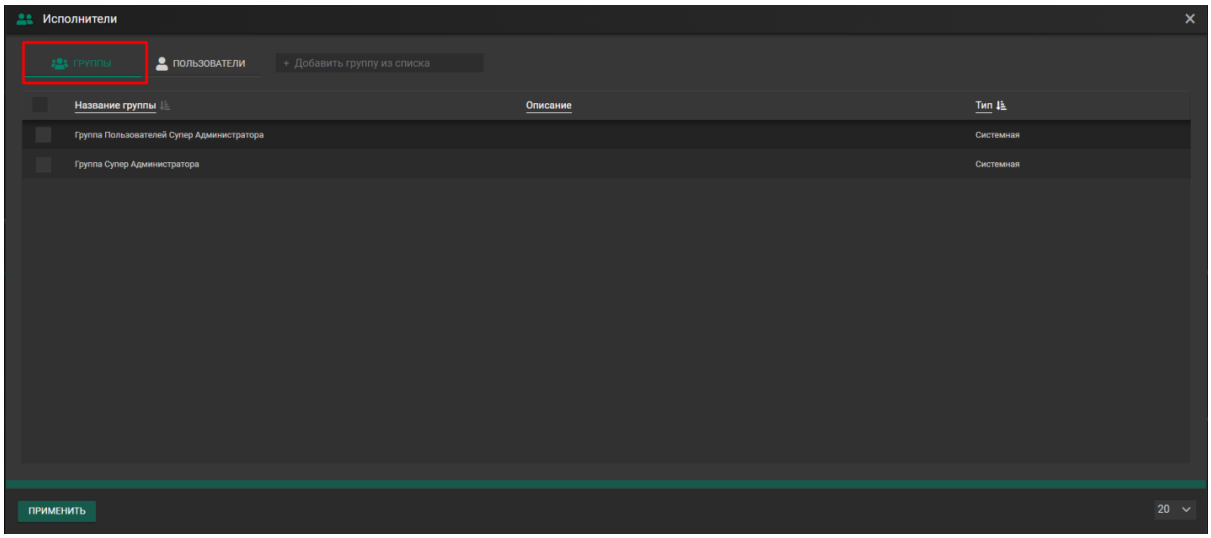


Рис. 3.116. Добавление исполнителей (групп)

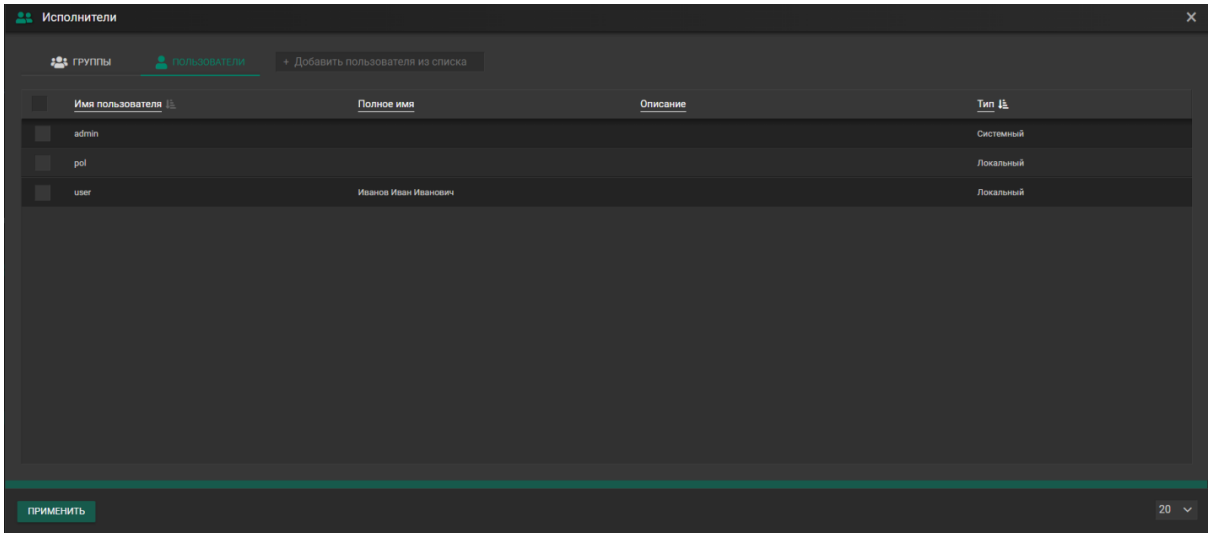


Рис. 3.117. Добавление исполнителей (пользователей)

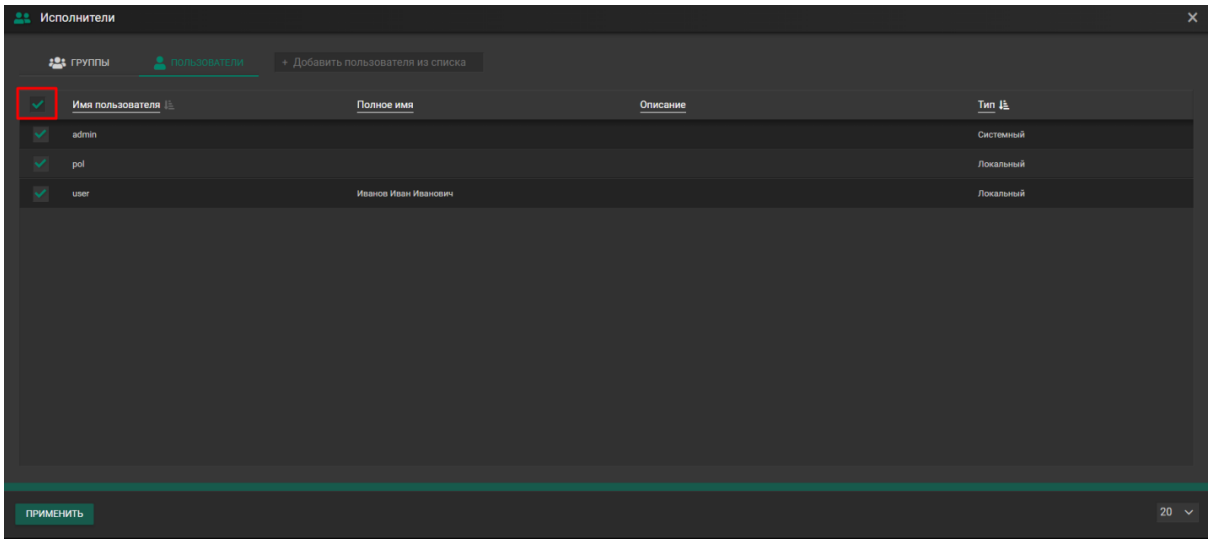


Рис. 3.118. Выбор всех элементов из списка

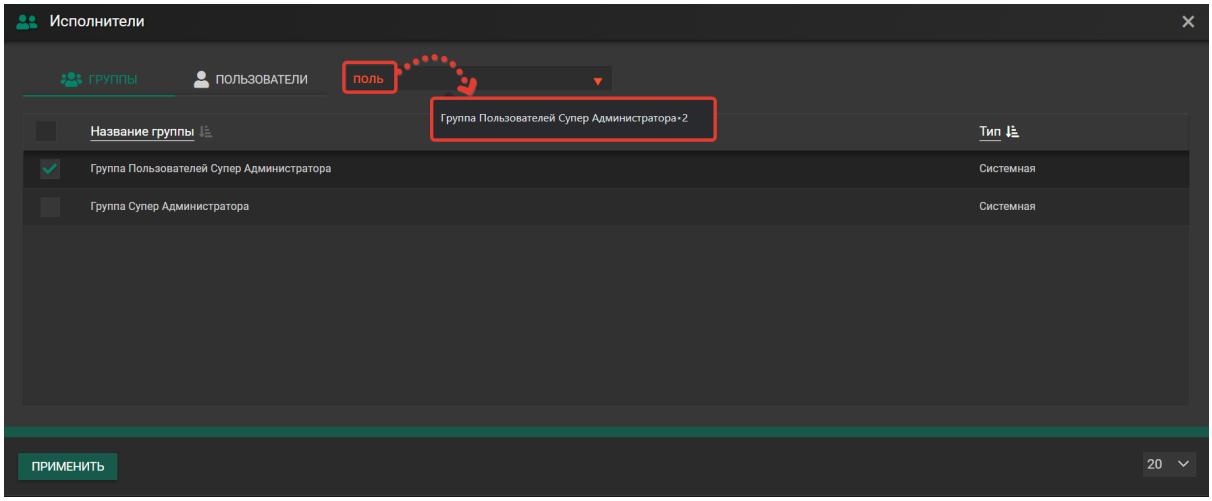


Рис. 3.119. Поиск элементов из списка

3.14.2. Просмотр задания

Чтобы открыть задание для просмотра, следует кликнуть мышкой по теме задания. В результате откроется окно, в котором отображается полная информация о задании и история его обработки.

В разделе реализована возможность .

Для просмотра информации о подключениях и статистике:

1. Перейти в раздел **Задания**.
2. Кликнуть мышью по теме интересующего вас задания.
3. Нажать кнопку **Подключения и статистика** (Рис.3.125).

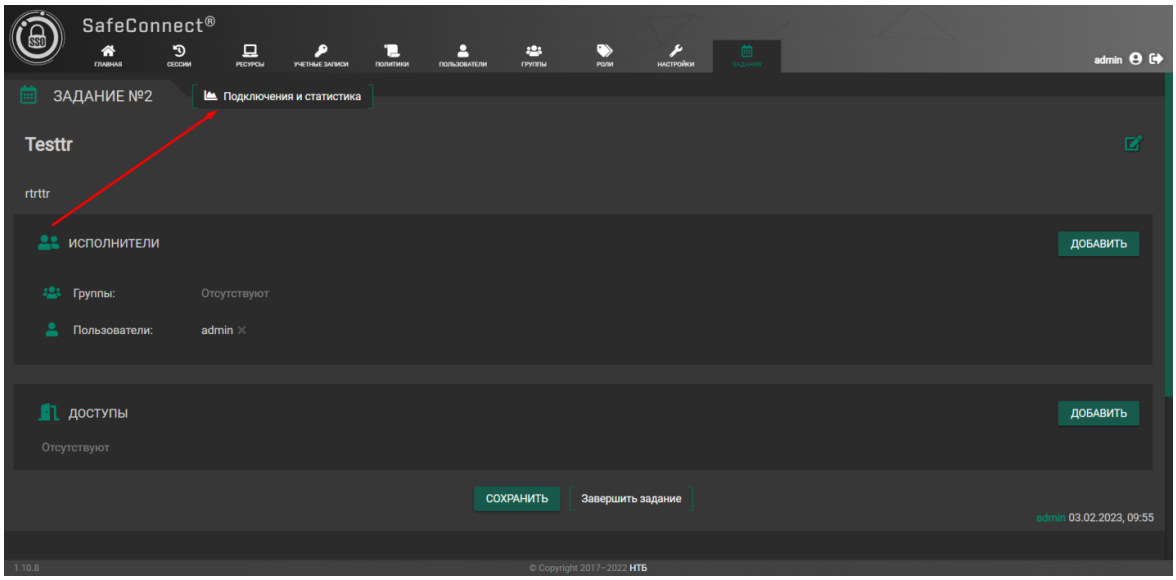


Рис. 3.120. Расположение кнопки «Подключение и статистика»

Для просмотра станут доступны статистика и информация по подключениям пользователя (Рис.3.121).

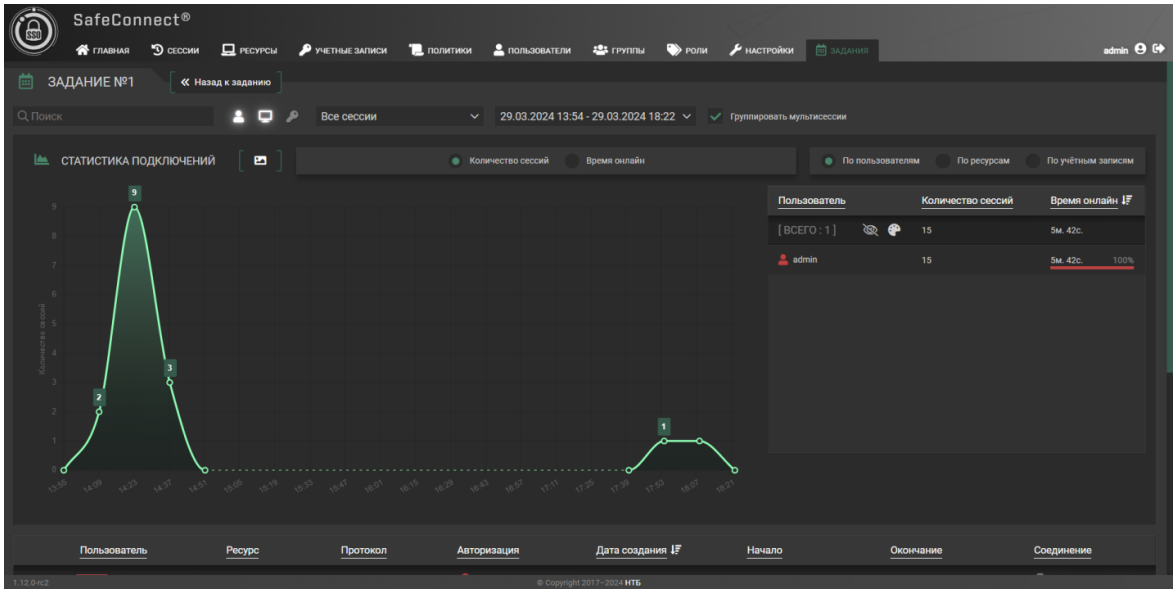


Рис. 3.121. Статистика подключений

4. Выбрать отображаемые сессии (Рис.3.126):
   - Все сессии;
   - Установленные соединения;
   - Сейчас онлайн;

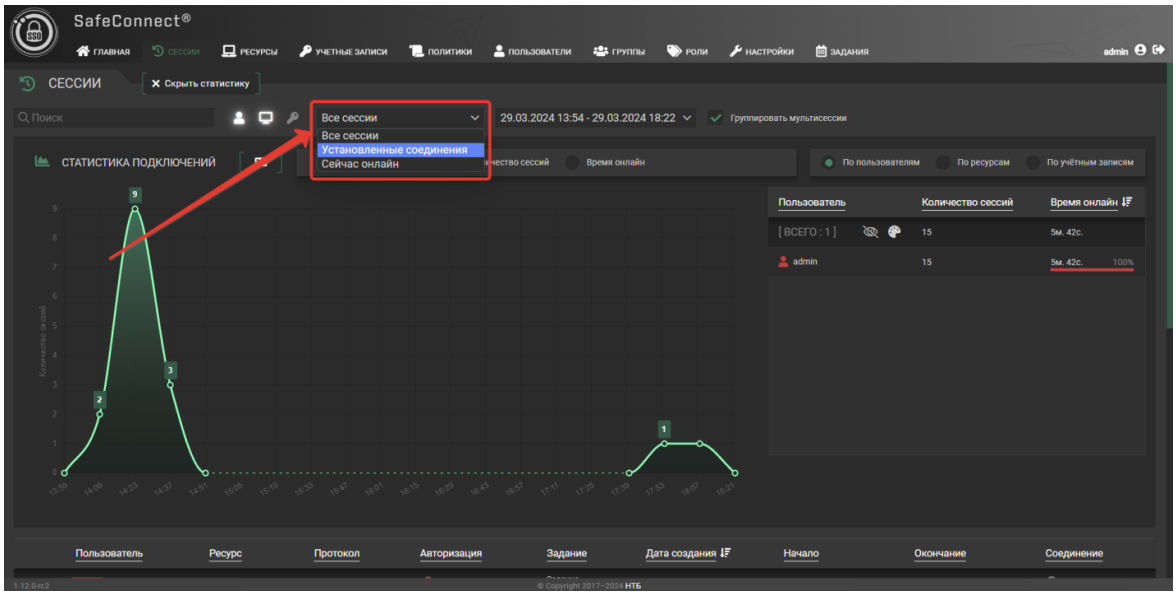


Рис. 3.122. Отображение сессий

5. Установить временной период (Рис.3.123). Для этого выбрать период из списка (Рис.3.128):

   - Сегодня;
   - Вчера;
   - На этой неделе;
   - В этом месяце;
   - В этом году;

   По завершению выбора диапазона нажать кнопку **Применить**, для выхода без изменений нажать кнопку **Отмена**.

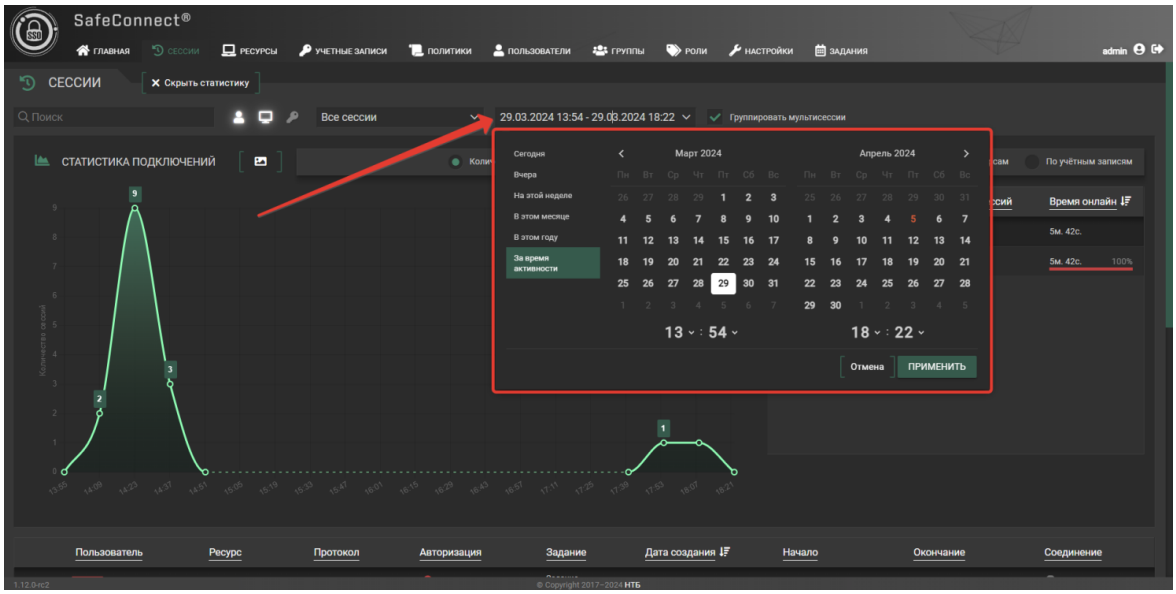


Рис. 3.123. Установка временного периода

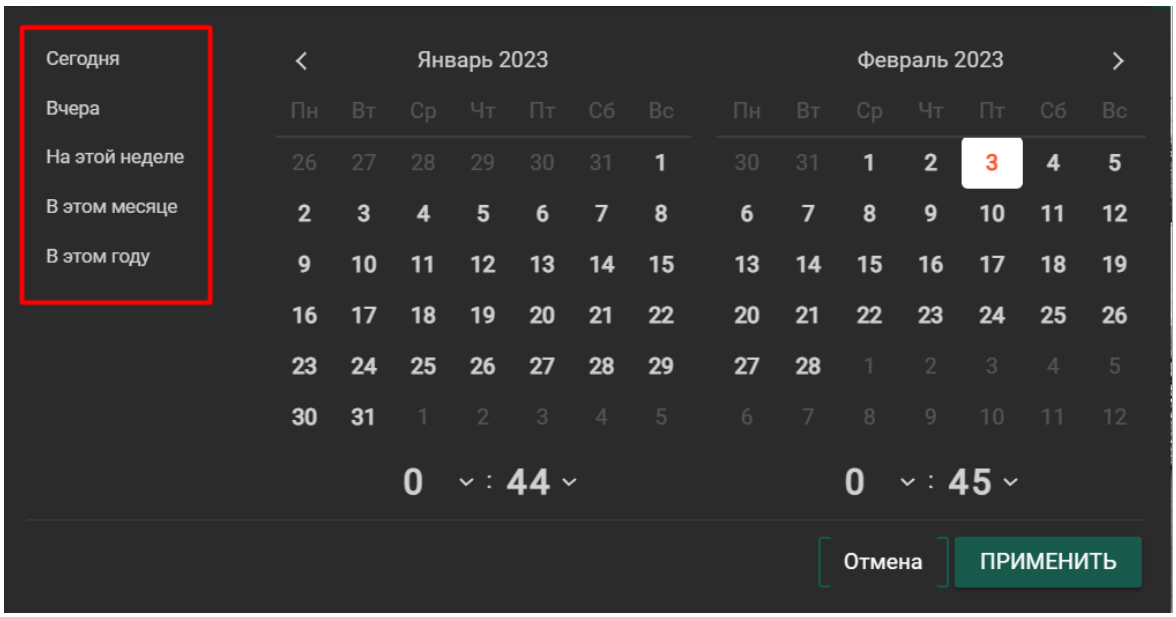


Рис. 3.124. Выбор периода из списка

Для выбора периода вручную нажать одним щелчком на дату начала периода, затем одним щелчком мыши на дату окончания периода (Рис.3.130). Для перехода между месяцами использовать стрелки < и > (Рис.3.130).

По завершению выбора диапазона нажать кнопку **Применить**, для выхода без изменений нажать кнопку **Отмена**.

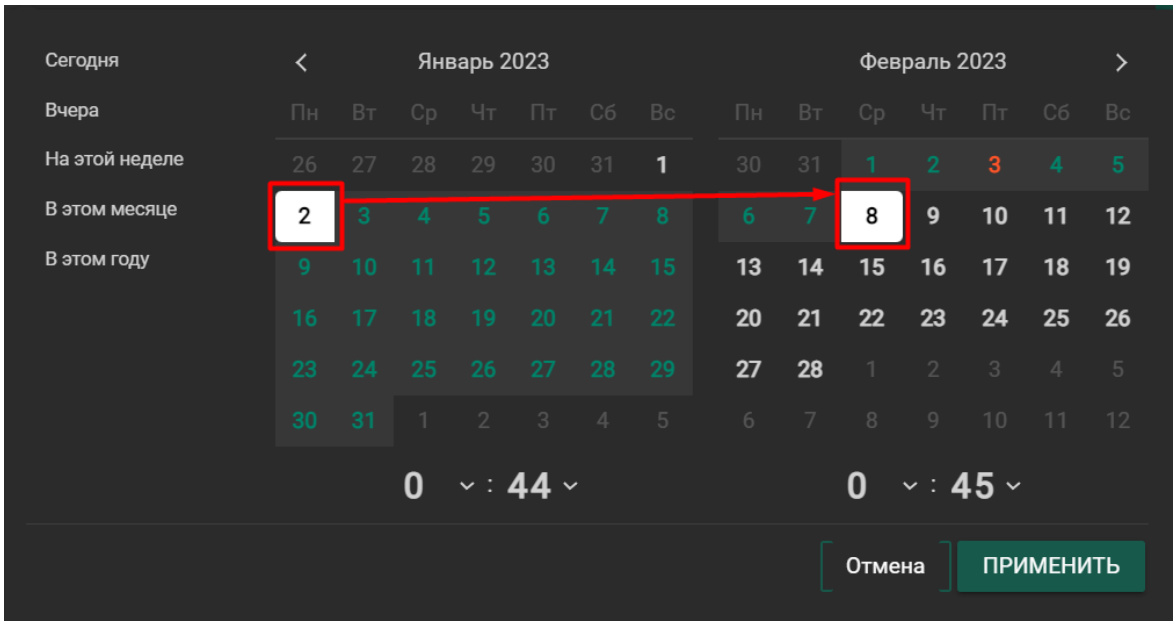


Рис. 3.125. Выбор периода вручную

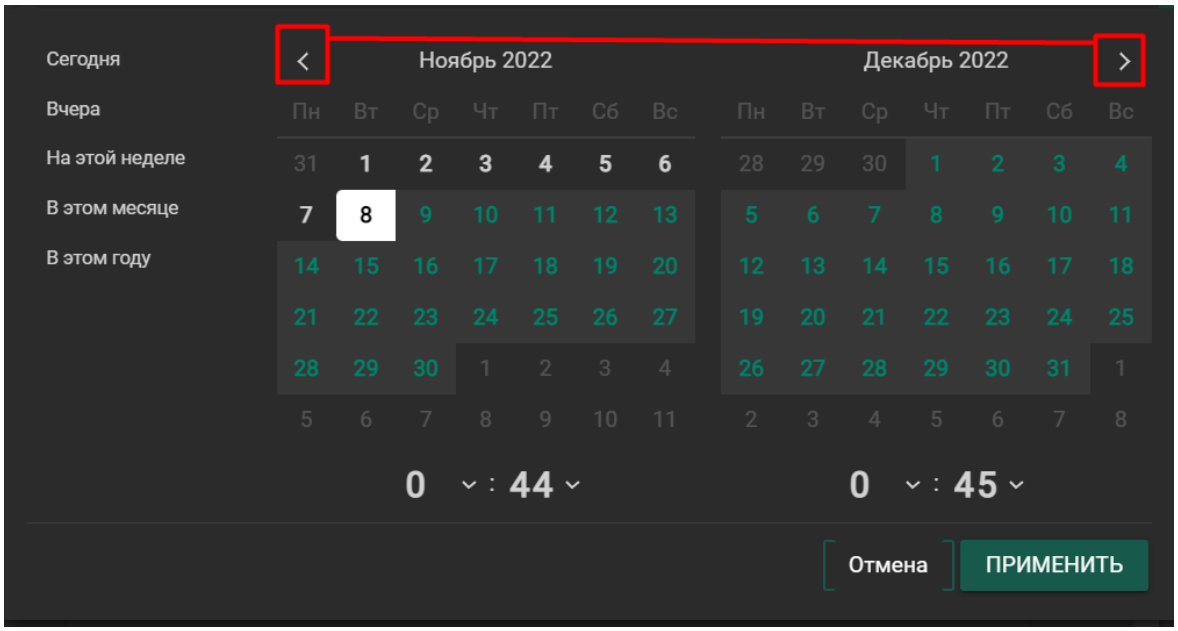


Рис. 3.126. Переход по месяцам

Для добавления временного диапазона необходимо воспользоваться временными шкалами и установить время начала диапазона и время окончания диапазона: последовательно нажать на цифру со значением часа, чтобы развернуть шкалу, затем на цифру со значением минут, чтобы развернуть шкалу минут (Рис.3.131). Аналогичные действия выполняются для установки времени начала и времени окончания диапазона.

По завершению выбора диапазона нажать кнопку **Применить**, для выхода без изменений нажать кнопку **Отмена**.

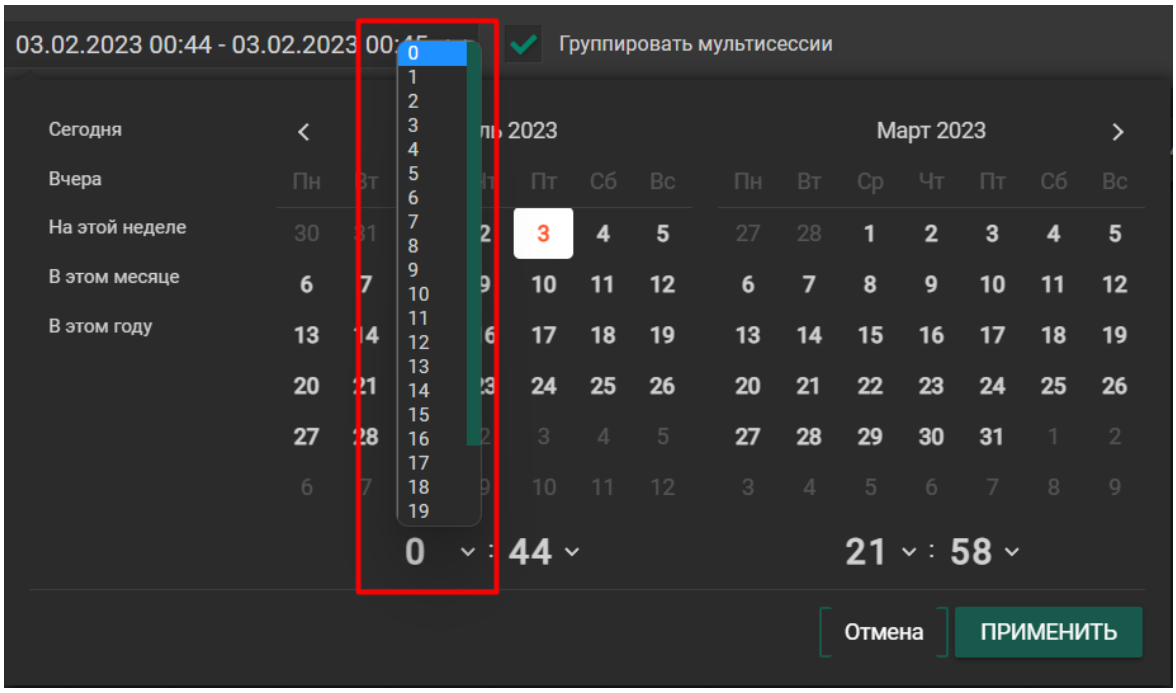


Рис. 3.127. Установка времени

Установить дату и время также можно отредактировав верхнее поле с отображением диапазона (Рис.3.128) .

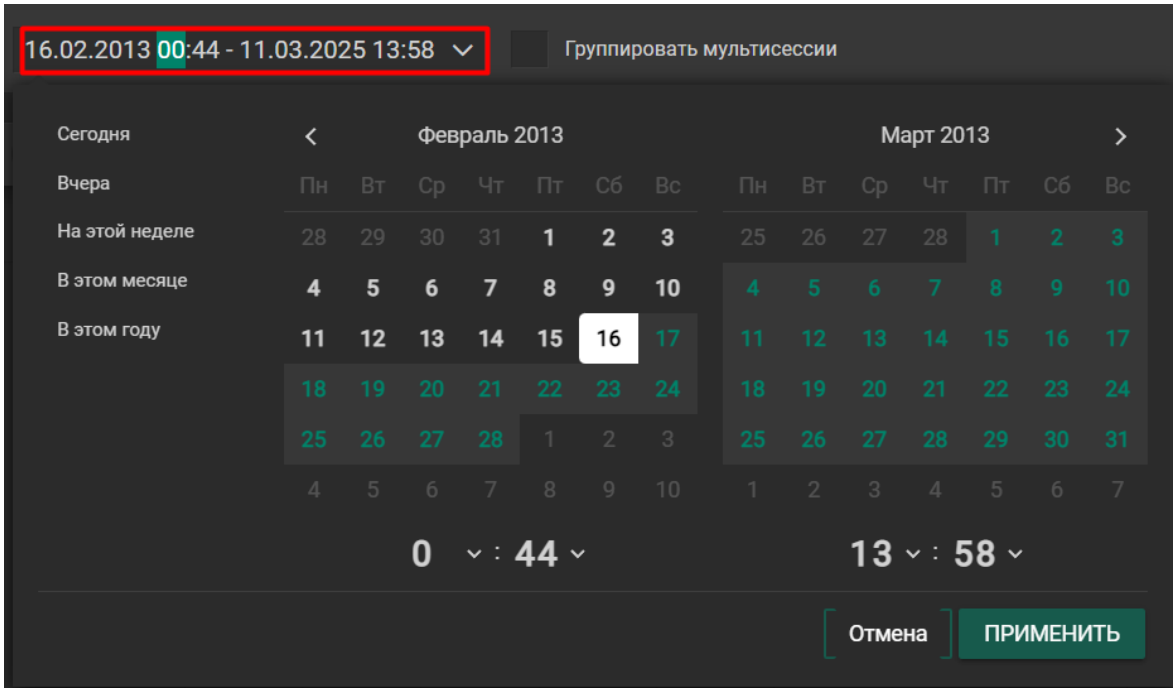


Рис. 3.128. Настройка даты и времени

6. Для группировки сессий необходимо установить флажок **Группировать мультисессии** (Рис.3.129). Для разгруппировки необходимо снять данный флажок.

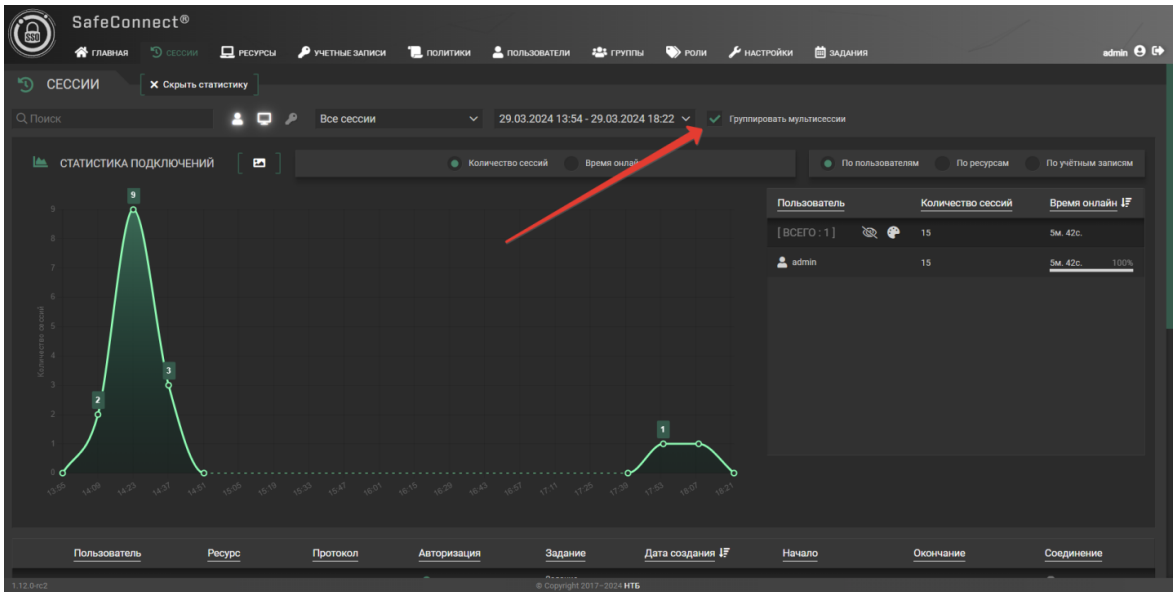


Рис. 3.129. Группировка мультисессий

Выбор отображаемой информации:

Количество сессий / Время онлайн. Для выбора одного из значений необходимо включить необходимую радиогруппу (Рис.3.130).

По пользователям / По ресурсам / По учётным записям. Для выбора одного из значений необходимо включить необходимую радиогруппу (Рис.3.130).

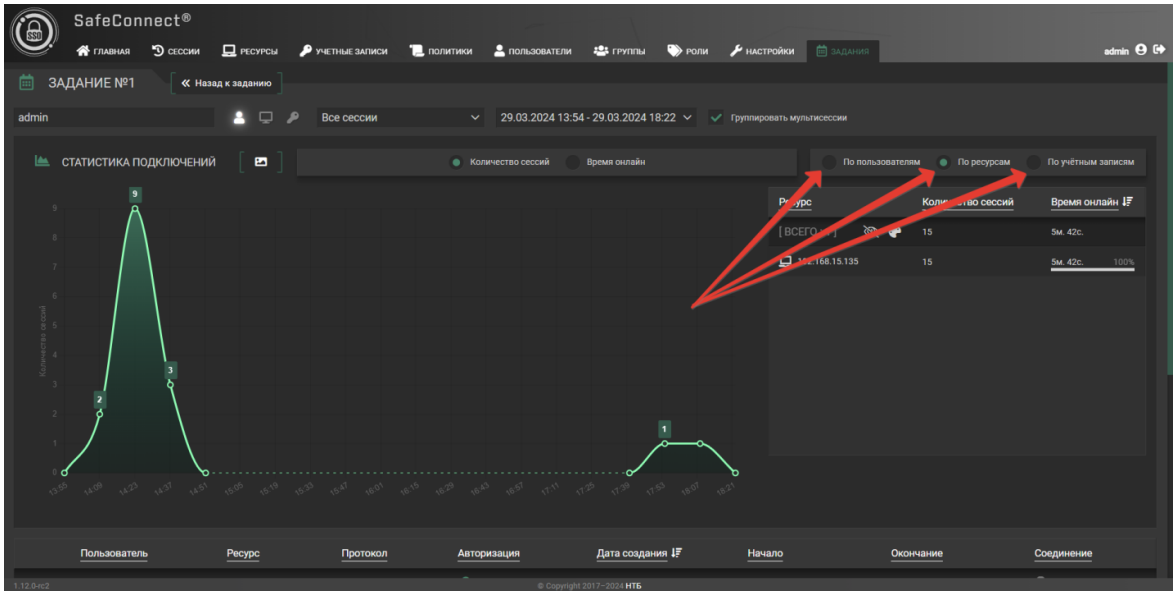


Рис. 3.130. Выбор отображаемой информации

В разделе **Подключения и статистика** доступна функция **поиска.** Для отображения искомой информации необходимо ввести значение в поле поиска. Также имеется возможность уточнить поиск:

- Искать в имени пользователя (включить или выключить поиск по имени пользователя);
- Искать в названии ресурса (включить или выключить поиск по названию ресурса);
- Искать в названии учетной записи (включить или выключить поиск по названию учетной записи).

Для сохранения графика подключений необходимо воспользоваться кнопкой . В результате на локальное хранилище пользователя будет скачан файл–изображение графика в формате *.PNG.

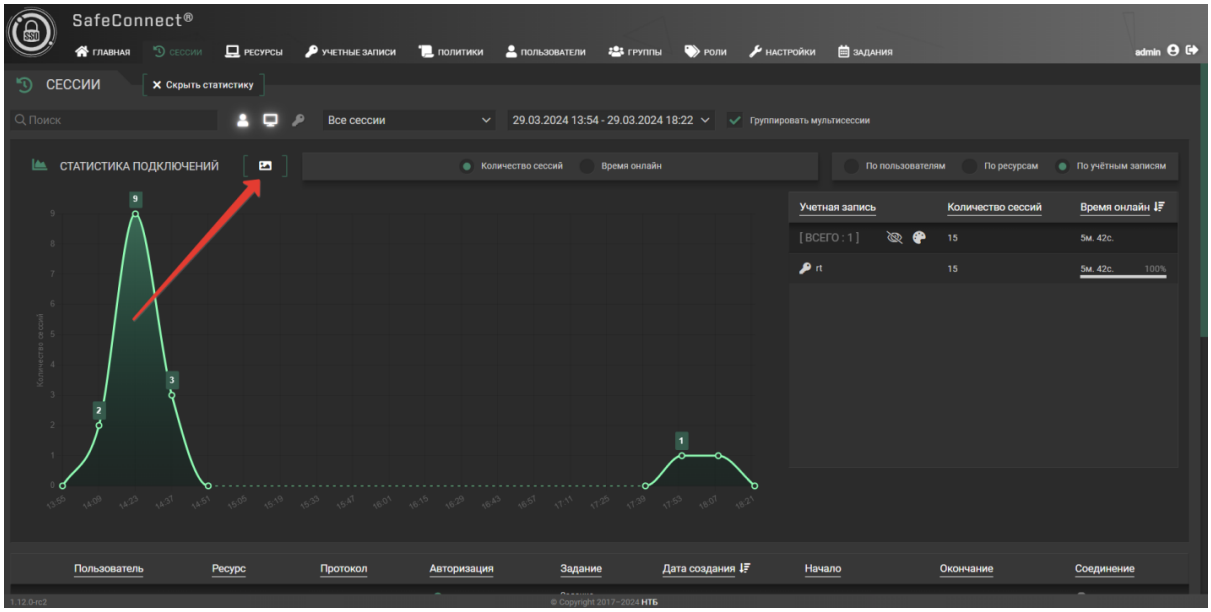


Рис. 3.131. Сохранение графика

Под графиком расположены области с информацией об учетных записях и пользователях (Рис.3.132). В данной области есть возможность сортировки по столбцам. Для включения сортировки нажать на название столбца (рядом с выбранным столбцом отобразится значок сортировки по убыванию или по возрастанию).

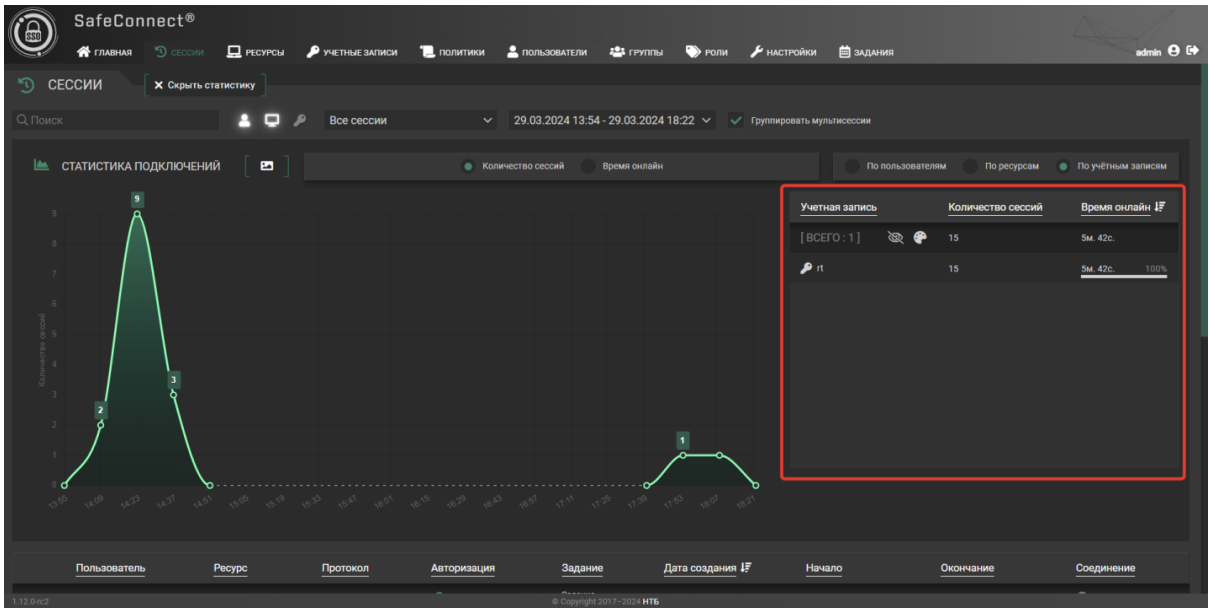


Рис. 3.132. Информация об учетных записях и пользователях

Также реализованы следующие возможности:

- при помощи кнопок скрыть  или отобразить  строчки с общим количеством записей (пользователей, ресурсов или учетных записей). Это позволяет отобразить, или скрыть общее число суммы всех записей (Рис.3.133, Рис.3.134);

У отдельных пользователей, ресурсов и учетных записей отсутствует возможность включения и выключения отображения.

- окрасить записи с текущей страницы .

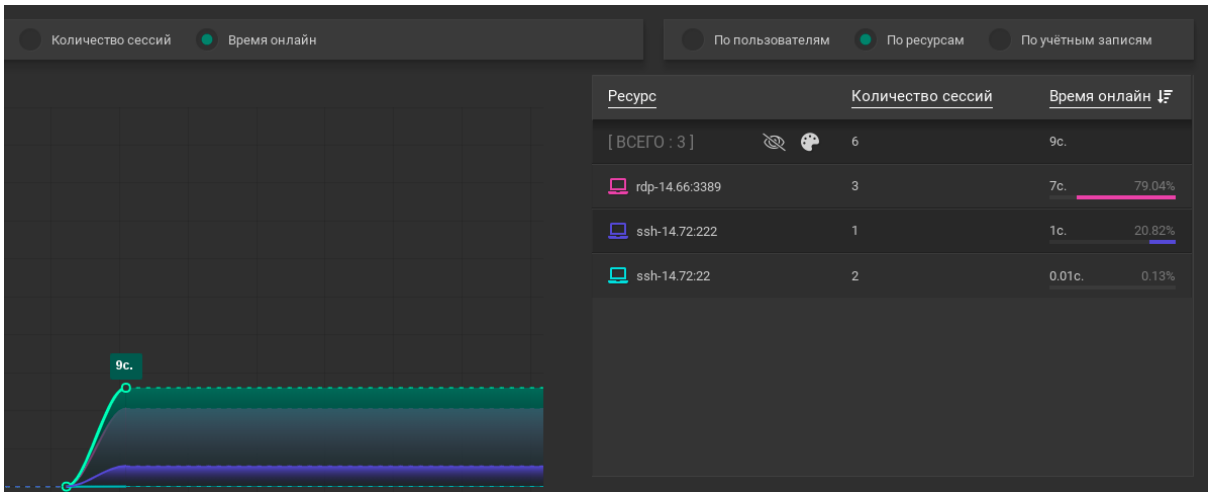


Рис. 3.133. Отображение включено

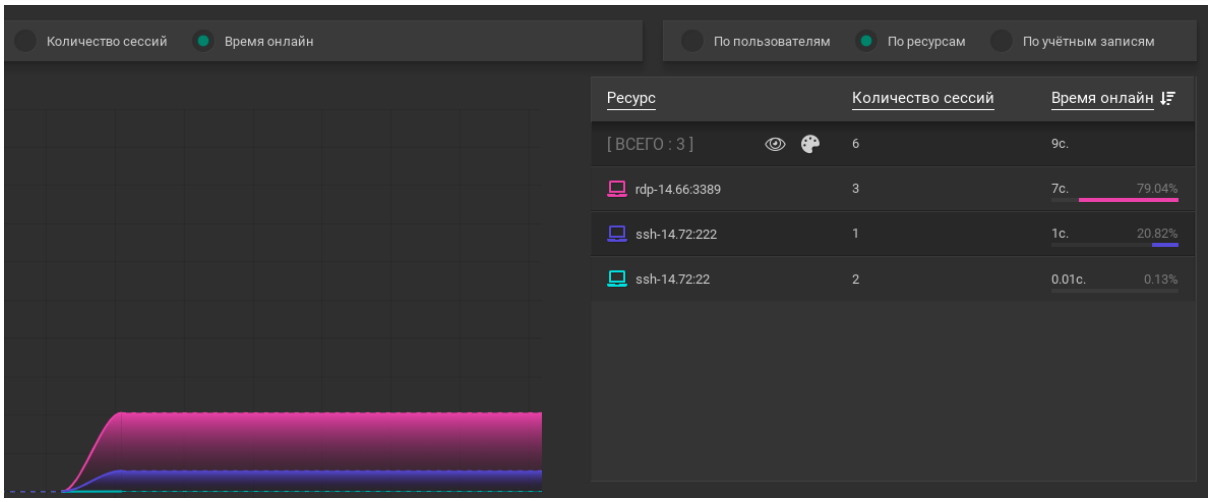


Рис. 3.134. Отображение выключено

Для выхода из просмотра статистики нажать **Назад к заданию**.

3.14.3. Поиск задания

Для поиска заданий из списка необходимо воспользоваться функциями поиска:

- **Поиск по теме, номеру задания, имени инициатора** – ввести искомое значение в поле поиска;
- **Поиск по заданному диапазону** – ввести искомый диапазон дат;
- **Фильтрация поиска** (отметить радиогруппы на выбор):
- **Все задания / Открытые / Закрытые** – отобразить все задания / отобразить открытые задания / отобразить закрытые задания;
- **Выборочно** (возможен выбор сразу нескольких значений из списка, для включения нажать на соответствующий значок):
  - – с доступами, требующими подтверждения;
  - – требуется подтверждение на запуск сессии;
  - – техподдержка;
  - – без исполнителей;
  - – с действующими доступами;
  - – без действующих доступов;
  - – непрочитанные.

3.14.4. Редактирование задания

Чтобы открыть задание для редактирования, следует кликнуть мышкой по теме задания. В результате откроется окно, в котором отображается полная информация о задании и история его обработки:

1. Нажать кнопку (Рис.3.137);
2. Внесите необходимые изменения (описание полей задания см. в разделе 3.14.1);
3. Нажать **Сохранить** для сохранения внесенных изменений.

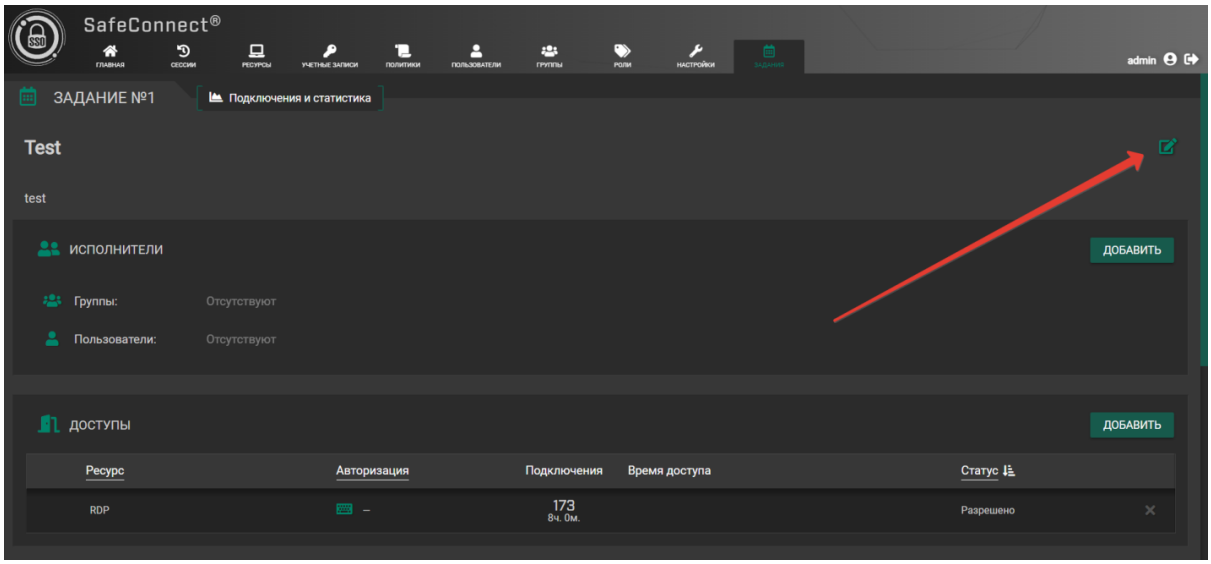


Рис. 3.135. Редактирование задания

3.14.5. Завершение задания

Чтобы завершить задание, перейти в раздел **Задание**, выбрать задание для закрытия, кликнуть мышкой по теме задания. В результате откроется окно, в котором отображается полная информация о задании и история его обработки. Нажать **Завершение задания** и подтвердить закрытие в предупреждающем сообщении (Рис.3.136) .

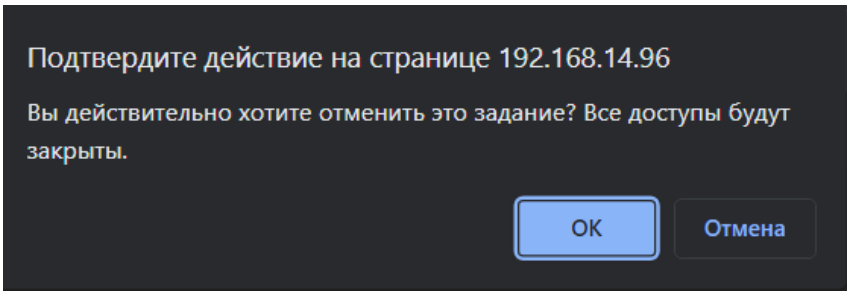


Рис. 3.136. Подтверждение закрытия задания

3.14.6. Управление доменными пользователями в заданиях

В разделе описаны расширенные возможности по управлению привилегированным доступом, предоставляя детальный контроль над исполнителями в заданиях через прямую

работу с доменными пользователями. Администраторы могут гибко назначать конкретных пользователей, интегрированных из **Active Directory**, к заданиям, что повышает точность управления доступом и упрощает администрирование.

В SafeConnect реализована полноценная поддержка операций создания, просмотра, обновления и удаления для доменных пользователей непосредственно в контексте заданий SafeConnect:

1. Создание нового задания с добавлением доменных пользователей:

   - Главные администраторы и пользователи SafeConnect с соответствующими правами могут добавлять отдельных доменных пользователей (импортированных через интеграцию с LDAP-сервером) в создаваемое задание. Это устраняет необходимость привязки всего задания к доменным группам (для обеспечения корректной работы с интеграцией SafeInspect, при добавлении исполнителей будут отображаться только доменные пользователи, входящие в группы **AD Users** и **Domain Users**).

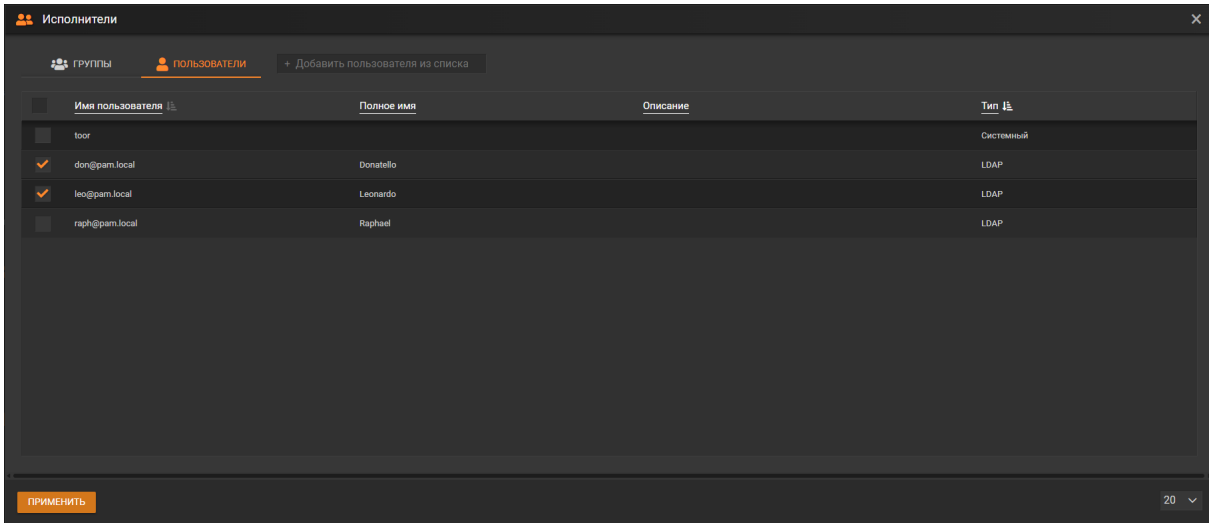


Рис. 3.137. Исполнители

1. Редактирование существующего открытого задания и добавление доменных пользователей:

   - Главные администраторы и пользователи SafeConnect с правами на редактирование заданий могут добавлять доменных пользователей, интегрированных из LDAP, в уже существующие, находящиеся в открытом статусе задания.

2. Редактирование существующего задания и удаление доменных пользователей:

   - Администраторы SafeConnect и пользователи с правами на редактирование заданий могут удалять доменных пользователей из уже существующих, открытых заданий.

Эти нововведения предоставляют администраторам SafeConnect больше гибкости и контроля над управлением доступом, позволяя точно настраивать исполнителей для каждого задания, а также поддерживают согласованность данных в реплицированных средах.

Примечание

Задания, в которых исполнителями назначены исключительно доменные пользователи, будут автоматически закрыты при отключении интеграции с LDAP или деактивации этих пользователей. Обратите внимание, что при восстановлении интеграции или повторной активации пользователей, ранее закрытое задание не будет открыто автоматически!

3.15. Интеграция с SafeInspect

Если в информационной системе компании настроена система контроля привилегированных пользователей SafeInspect, следует произвести интеграцию Портала с SafeInspect.

Подключение интеграции с SafeInspect позволяет осуществлять синхронизацию пользователей, групп пользователей и доступов для них между SafeConnect и SafeInspect, а также использовать большинство возможностей SafeInspect.

Перед интеграцией следует убедиться, что SafeConnect и SafeInspect не имеют пользователей и групп пользователей с одинаковыми именами.

После интеграции SafeConnect будет автоматически добавлять своих пользователей и группы пользователей, используемых в заданиях, в SafeInspect.

Примечание

Подключение нескольких SafeConnect к одному SafeInspect не допускается.

3.15.1. Сетевые взаимодействия SafeInspect и SafeConnect

Для интеграции SafeInspect с SafeConnect используется несколько портов взаимодействия. Основные порты, используемые при интеграции со стороны SafeConnect, это 443, 22 и 41798–42507.

Интеграция с RDP, SSH и другими протоколами требует открыть соответствующие порты (например, 3389, 22, 80 и т.д.). Если вы используете измененные порты, убедитесь, что SafeConnect и SafeInspect имеет к ним доступ.

Для интеграции с LDAP SafeConnect и SafeInspect используют порты 389, 53 и 636.

Интеграция с RADIUS для 2FA потребует открыть порты 1812 и 1813 либо специальный порт, если вы его меняли.

Другие интеграции, требующие доступ по UDP или TCP, так же требуют открытия соответствующих портов, ознакомьтесь с документацией используемых систем для открытия соответствующих доступов.

3.15.2. Настройка интеграции с SafeInspect

Внимание!

*Настройку интеграции с внешними системами необходимо проводить одновременно на каждом из продуктов SafeInspect и SafeConnect: в случае настроенной конфигурации **LDAP** и (или) **RADIUS** на одном из продуктов, такая же настройка должна быть произведена и на другом.*

Для настройки интеграции SafeInspect и SafeConnect необходимо сгенерировать и загрузить в SafeConnect файл конфигурации API:

1. Войти в SafeInspect с учетной записью, обладающей правами создания администраторов.
2. Перейти на одну из вкладок:
   - вкладка **Администраторы > Локальные учетные записи** (для версии системы SafeInspect 2.4.3);
   - вкладка **Настройки > Администраторы > Локальные учетные записи** (для версии системы SafeInspect 2.4.4).
3. Добавить учетную запись администратора соответствующей кнопкой.
4. Ввести имя пользователя (например, «scadmin»).
5. Ввести и повторить пароль.
6. Установить флажок **Активный**.
7. Выбрать роли: Administrator, Mapping manager, Auditor, Operator, User manager, Host manager.
8. Сохранить изменения кнопкой **Сохранить**.

Для успешной интеграции в меню SafeInspect:

1. Перейти на одну из вкладок:
   - **Настройки > Внешняя аутентификация > Сервера LDAP** (для версии системы SafeInspect 2.4.3);
   - **Настройки > Внешние сервисы > Внешняя аутентификация > Серверы LDAP** (для версии системы SafeInspect 2.4.4);
2. В поле Адрес вписать имя домена, а не контроллера домена, например: *domain.local*, а не *dc.domain.local*.
3. Скачать файл конфигурации API. Для этого в меню управления перейти:
   - на вкладку **Администраторы > Локальные учетные записи** (для версии системы SafeInspect 2.4.3) и выбрать ранее созданного для SafeConnect администратора;

- на вкладку **Настройки > Администраторы > Локальные учетные записи** (для версии системы SafeInspect 2.4.4) и выбрать ранее созданного для SafeConnect администратора.

Примечание

Сгенерировать конфигурацию API необходимо от ранее созданного для SafeConnect администратора.

4. SafeConnect после распаковки файла конфигурации будет считать, что все правила, пользователи и другая информация, ранее созданная в SafeInspect выбранным администратором, созданы через SafeConnect. Поэтому необходимо создать отдельного администратора для SafeConnect, и сгенерировать файл конфигурации API от его имени. Тогда при дальнейшей работе все, что будет создано в SafeConnect, и автоматически перенесено в SafeInspect, будет выполнено от имени отдельного администратора для SafeConnect, и в данные, созданные другими администраторами, не будут происходить вмешательства.

5. В блоке **Клиент API** загрузить файл по кнопке **Сгенерировать конфигурацию API** (Рис.3.138.

Примечание

Для корректной настройки ключ интеграции должен быть длиной больше 2048 бит!

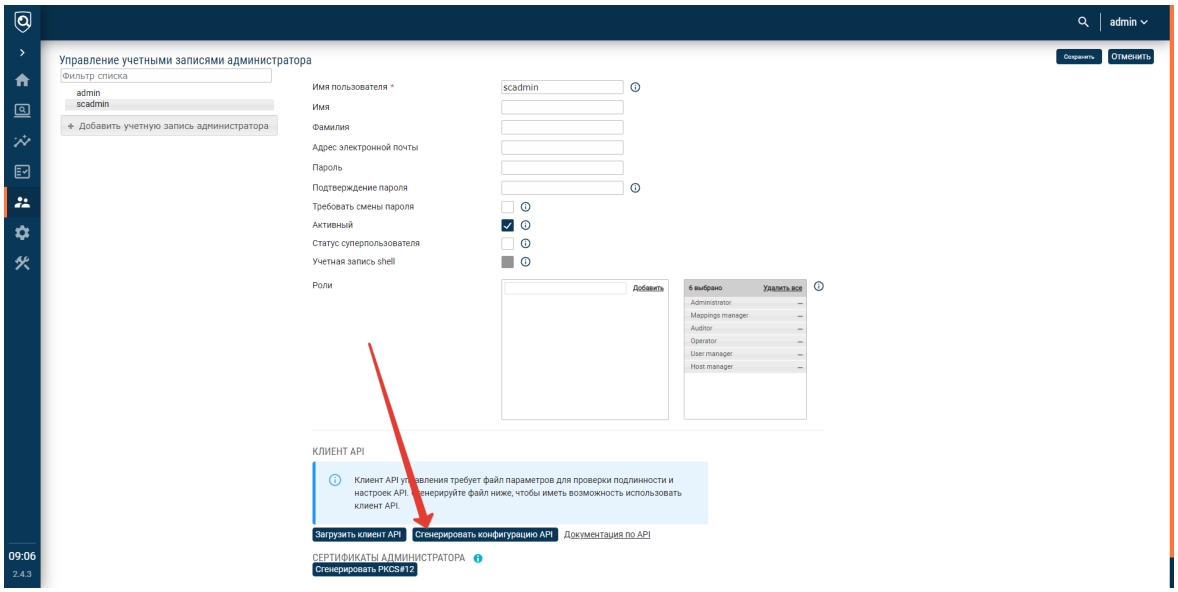


Рис. 3.138. Сгенерировать конфигурацию API

6. Полученный файл **admin–api–config.dat** загрузить в SafeConnect:

- Зайти в SafeConnect с **учетной записью, обладающей правами редактирования системных настроек**;

- Перейти на вкладку **Настройки > Интеграция с внешними системами > SafeInspect**;
- Загрузить файл конфигурации API, полученный из SafeInspect, кнопкой **Загрузить файл** (Рис.3.139).

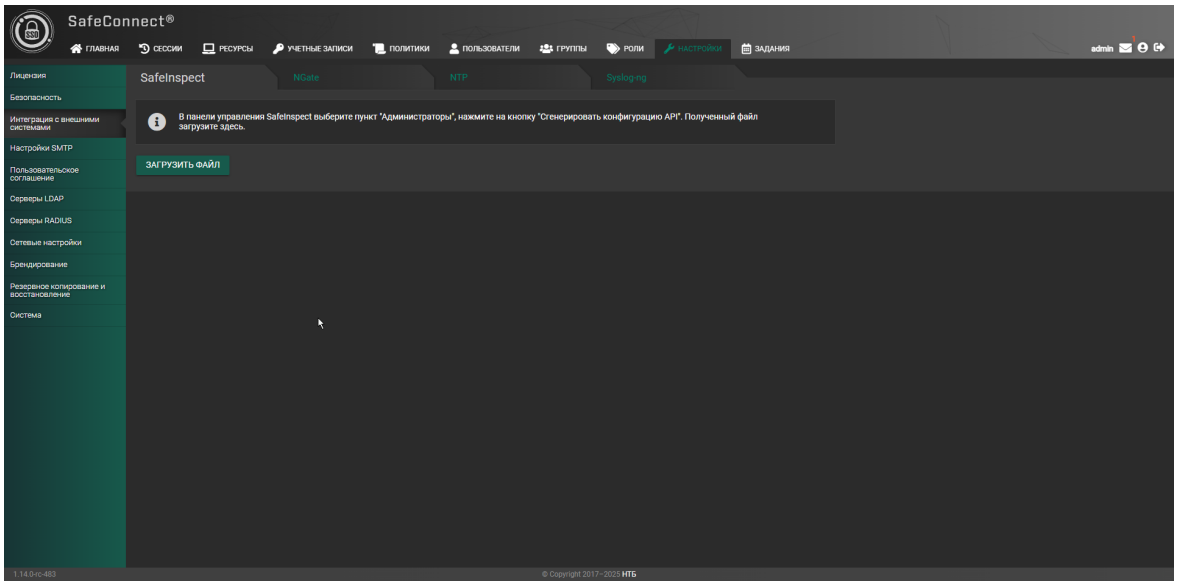


Рис. 3.139. Загрузка файла конфигурации

7. После загрузки файла конфигурации API во вкладке **Интеграция с внешними системами > SafeInspect** будет отображаться IP–адрес SafeInspect, учетная запись администратора SafeInspect, от имени которого была сгенерирована конфигурация API, а также флажки частичной синхронизации, синхронизации сопоставлений и кнопка удаления интеграции с SafeInspect (Рис.3.140, Рис.3.140) .

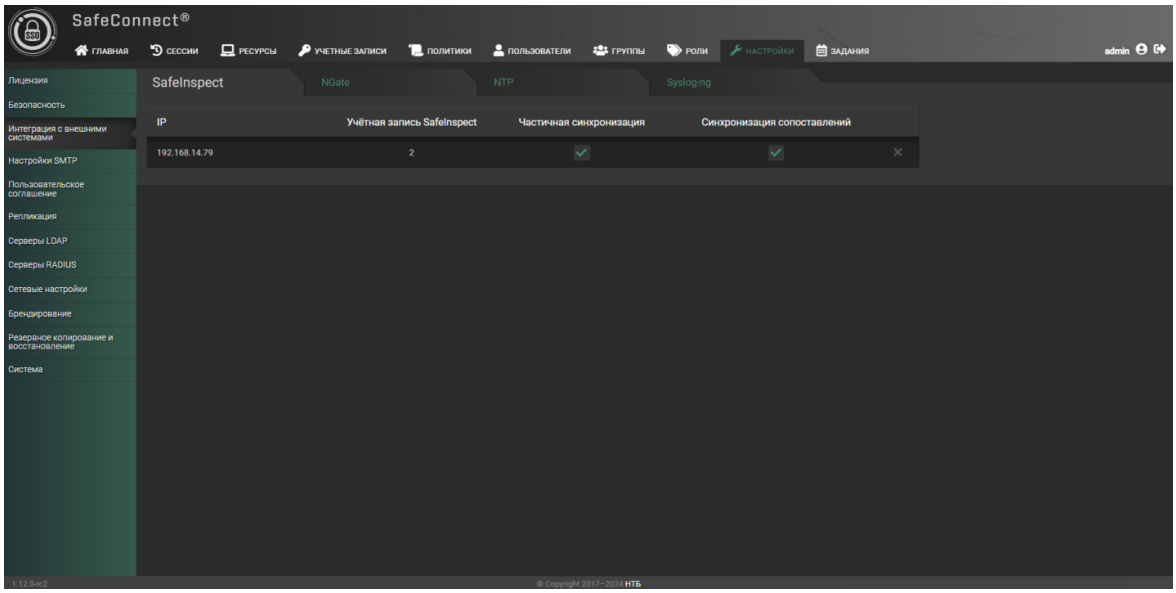


Рис. 3.140. Интеграция с SafeInspect

При загрузке файла конфигурации API, SafeConnect автоматически создаст в SafeInspect имеющихся у себя пользователей и группы, которые используются в заданиях.

8. Для того чтобы доступы пользователей SafeConnect проходили через SafeInspect, следует добавить нужный коллектор SafeInspect в политику SafeConnect, используемую для доступов:

   - Войти в SafeConnect с учетной записью **с правами администратора политик**;
   - Перейти на вкладку **Политики;**
   - Открыть для редактирования политику, которую предполагается использовать в доступах, которые должны идти через SafeInspect;
   - В поле **SafeInspect Бастион** (Рис.3.141 147) выбрать из списка IP–адрес нужного коллектора SafeInspect, оставив установленным флажок **Синхронизация обработчиков и правил** (Рис.3.142 148);

   Внимание!

   *При указании в политике адреса **SafeInspect Бастион**, подключения **HTTP(S)** фактически будут устанавливаться **напрямую** с SafeConnect до целевой системы. На SafeInspect в данном случае будут переданы **только данные сессий** для возможности воспроизводить сессию как видео.*

9. Сохранить изменения политики кнопкой **Сохранить**.

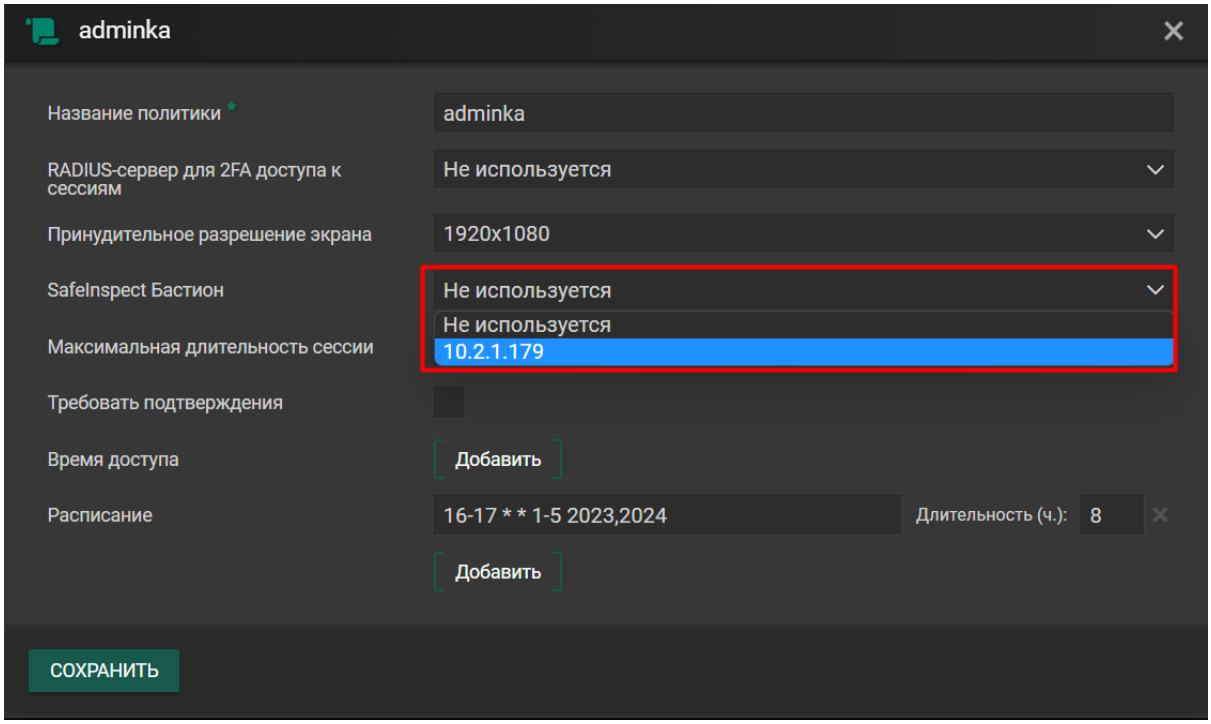


Рис. 3.141. Поле «SafeInspect Бастион»

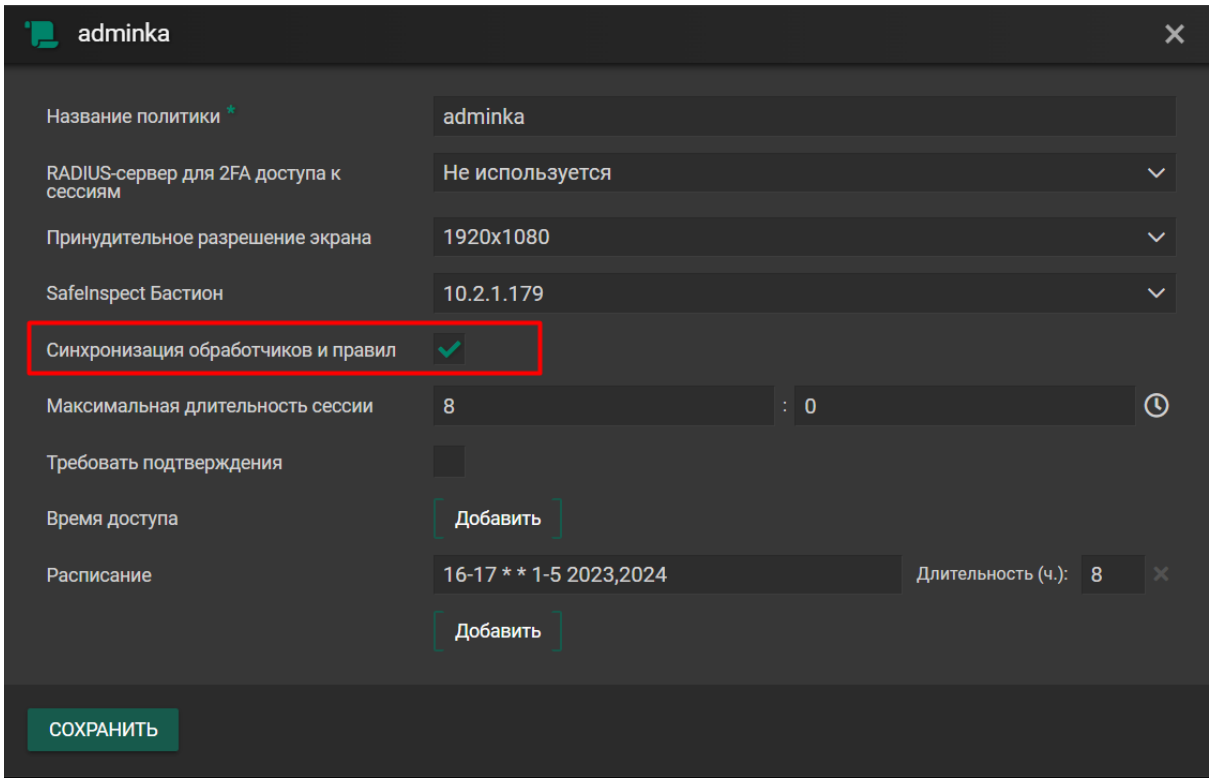


Рис. 3.142. Синхронизация обработчиков и правил

При сохранении политики, в которой указан SafeInspect и включена синхронизация обработчиков и правил, SafeConnect автоматически создаст в SafeInspect необходимые обработчики и правила для них.

Политики, использующие SafeInspect, в списке политик и в задании отображаются соответствующим значком и адресом выбранного коллектора (Рис.3.143 Рис.3.143) .

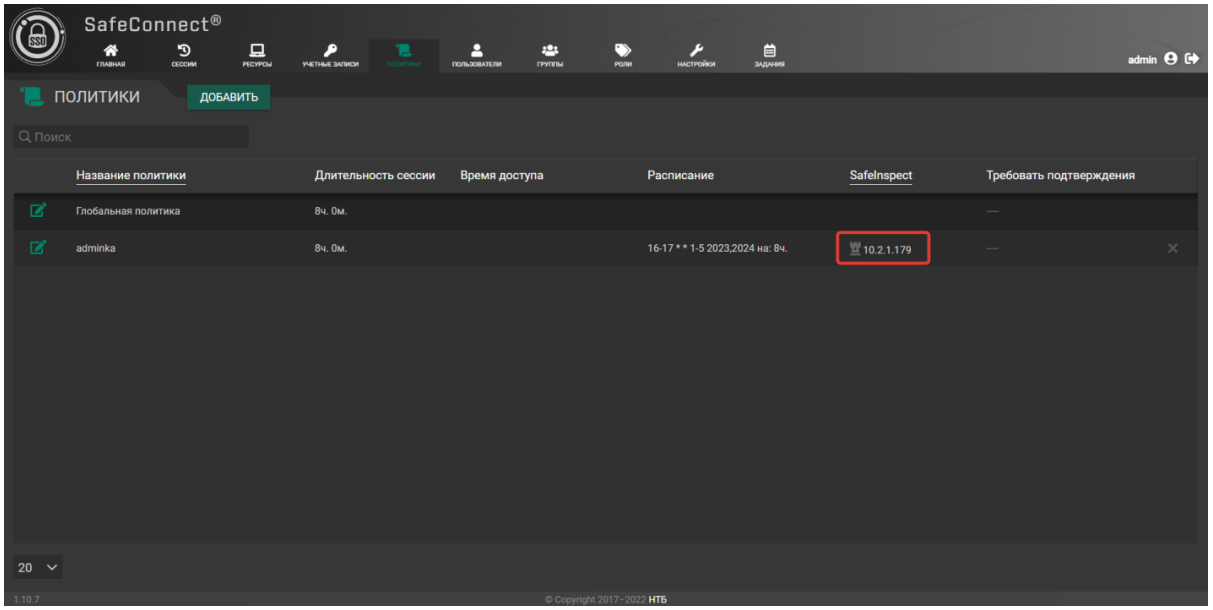


Рис. 3.143. Политики, использующие SafeInspect

При использовании такой политики в задании SafeConnect автоматически будет создавать соответствующие сопоставления и в SafeInspect для указанных в задании пользователей и групп.

Если не требуется синхронизация обработчиков и правил в SafeInspect, то можно во вкладке **Политики** в соответствующей политике снять одноименный флажок.

Если не требуется создание сопоставлений для доступа в SafeInspect, то можно во вкладке **Настройки > Интеграция с внешними системами** снять одноименный флажок.

3.16. Интеграция с КриптоПро NGate

В разделе осуществляется настройка совместной работы с VPN–шлюзом КриптоПро NGate.

Интеграция выполняется с целью универсализации доступа и используемых ключевых и других параметров доступа через один шлюз.

Для организаций, использующих, например, шифрование передаваемых данных в каналах связи (например, удаленный доступ по TLS-протоколу), возможна интеграция с такими системами. Схема взаимодействия показана на рисунке (Рис.3.144).

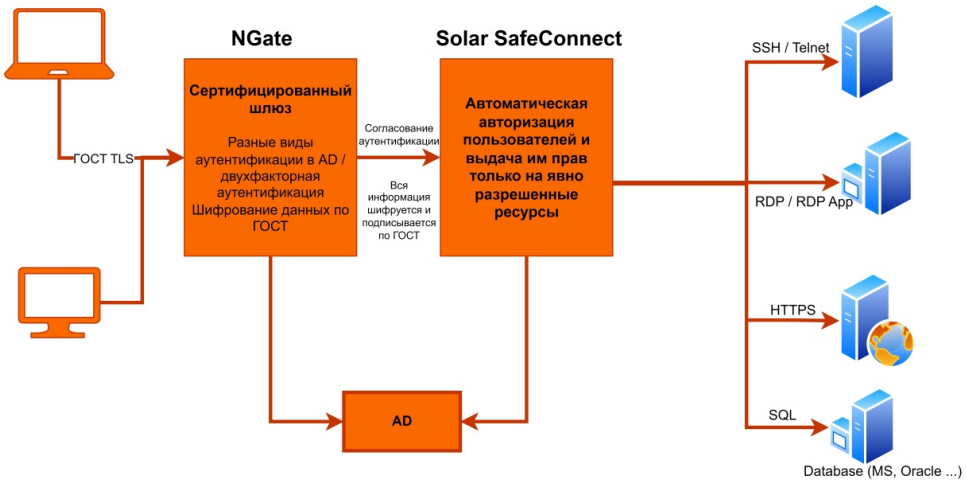


Рис. 3.144. Схема взаимодействия

ПАК КриптоПро NGate используется для обеспечения доступа всех пользователей компании, обеспечивая при этом, доступ в соответствии со всеми требованиями регуляторов, в том числе и по сертификации.

SafeConnect и шлюз NGate подключаются друг к другу, и при необходимости подключения пользователя к ресурсам сети с использованием, например, протокола SSH, шлюз NGate автоматически перенаправляет его на SafeConnect. В результате взаимодействия с NGate, портал получает необходимые аутентификационные данные для авторизации

пользователя. После прохождения успешной авторизации, пользователь получает доступ к явно назначенным ему ресурсам, по необходимым протоколам.

Служебные данные, данные пользователя, необходимые для авторизации, передаются в зашифрованном виде, с подписью. Шифрование и подпись соответствуют требованиям регуляторов (ГОСТ).

Для настройки взаимодействия между NGate и SafeConnect, необходимо выполнить следующие действия:

Настройка параметров SafeConnect:

1. В веб–интерфейсе SafeConnect перейти в раздел **Настройки > Интеграция с внешними системами > NGate** (Рис.3.145);

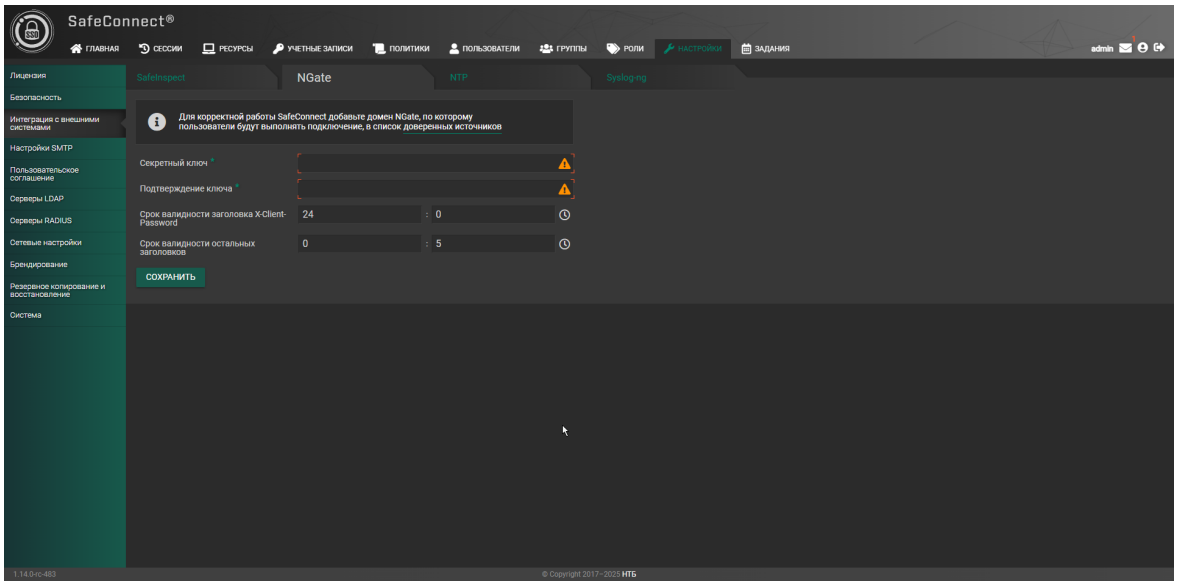


Рис. 3.145. Интеграция с NGate

2. Ввести пароль, на основе которого будут вырабатываться ключи шифрования и подписи. Пароль должен совпадать на стороне NGate и на стороне SafeConnect;

3. Установить срок, который будет определять валидность передаваемой информации.

Примечание

Данный параметр необходим, если в NGate и в SafeConnect, по какой–то причине, не одинаково настроено время. Кроме того, некоторые данные могут использоваться неоднократно и в некоторых случаях, они могут устаревать. Следует ориентироваться на параметр длительности сессии, который устанавливается на NGate.

4. Для сохранения настроек необходимо нажать кнопку **Сохранить**;

Настройка параметров КриптоПро NGate:

1. В NGate необходимо настроить соответствующий Портал и указать, что это **Single WEB-resource** (Рис.3.146).

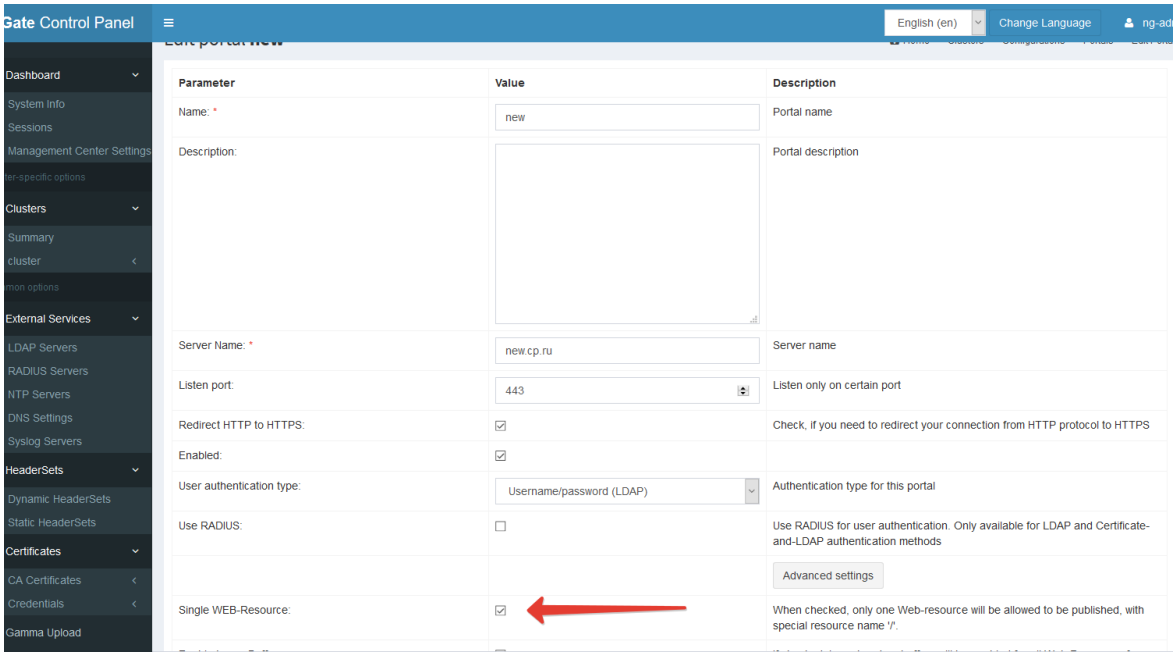


Рис. 3.146. Single WEB–resource

2. В параметрах активной конфигурации необходимо ввести общий для NGate и SafeConnect пароль в поле **Secure Headers password** (Рис.3.147).

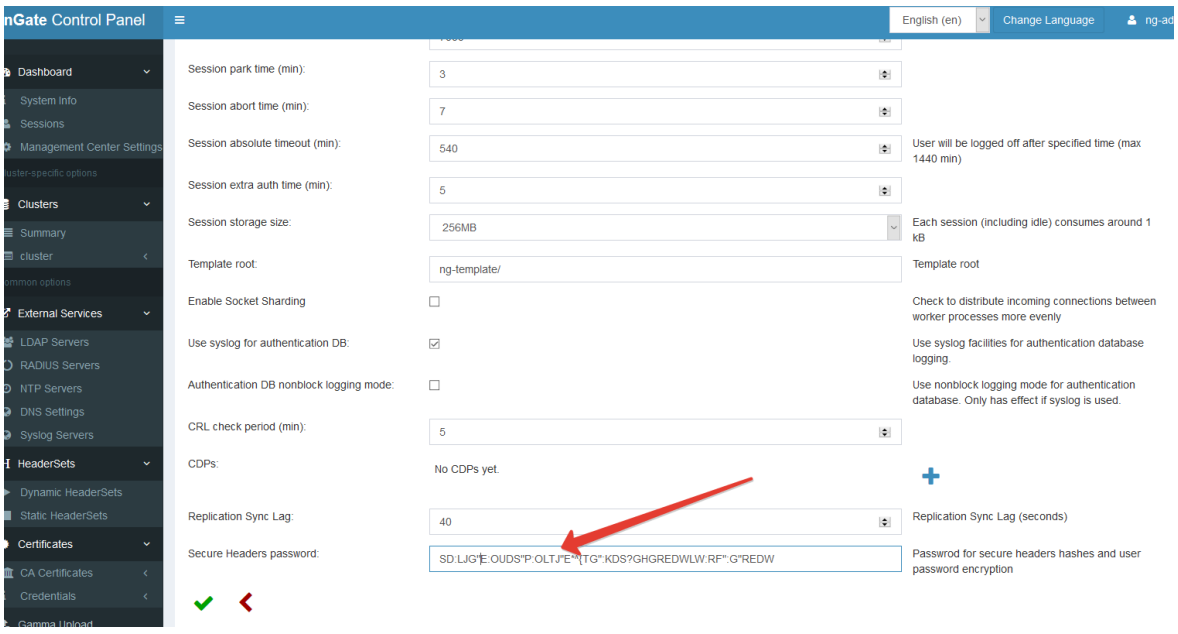


Рис. 3.147. Secure Headers password

3. Создать конфигурацию передачи динамических заголовков (Рис.3.148).

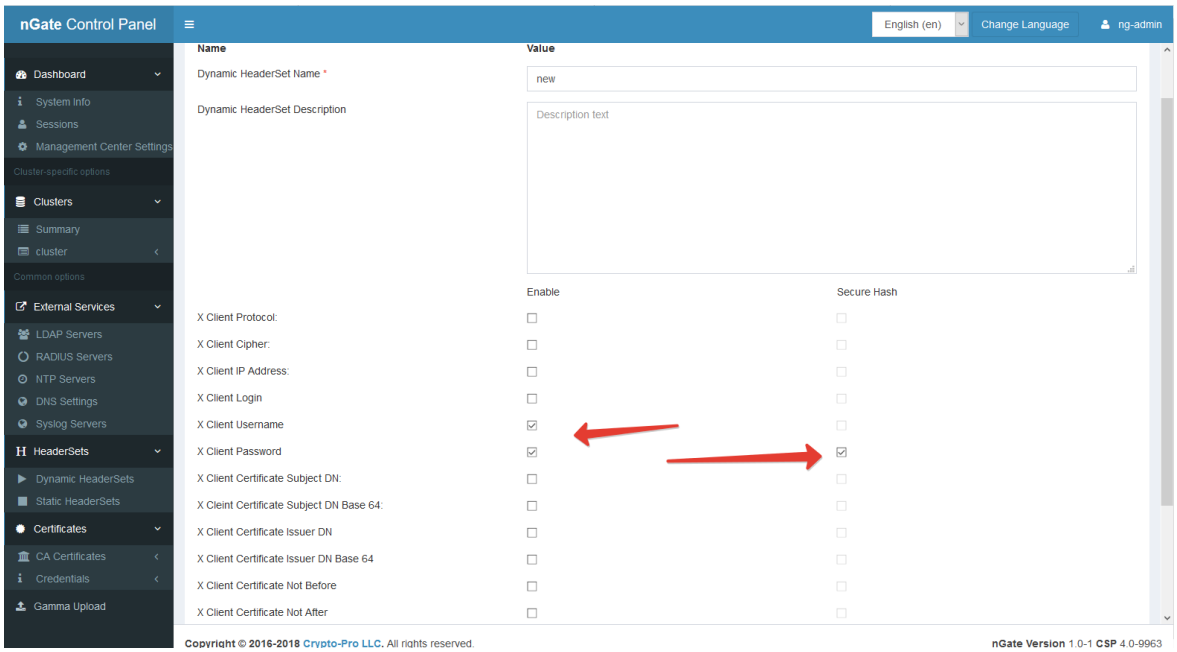


Рис. 3.148. Конфигурация передачи динамических заголовков

4. Для корректной совместной работы задать конфигурацию передачи статических заголовков, как это показано на рисунке (Рис.3.149).

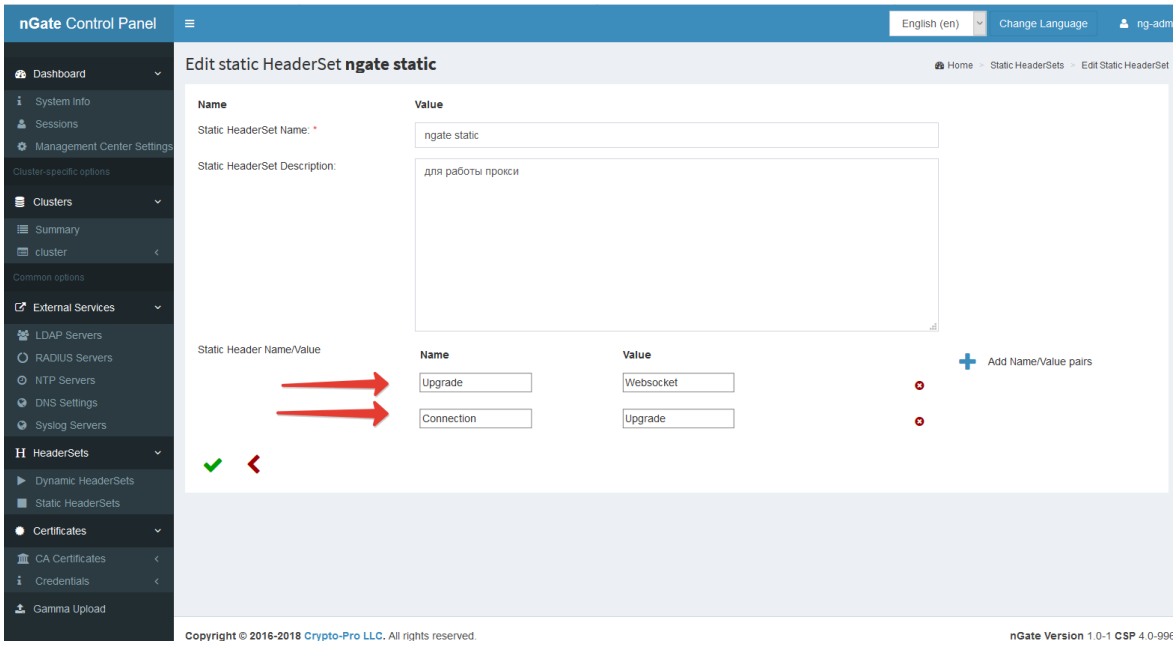


Рис. 3.149. Конфигурация передачи статических заголовков

5. Подключить конфигурации динамических и статических заголовков к конфигурации ресурса, который описывает SafeConnect (Рис.3.150).

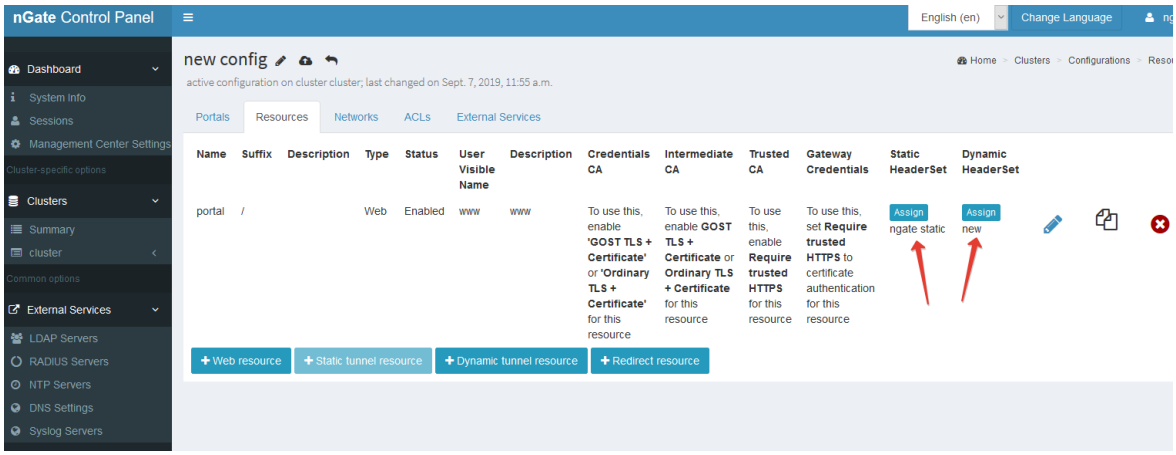


Рис. 3.150. Подключение конфигураций

На этом интеграция SafeConnect и NGate завершена. Теперь пользователь, подключающийся к SafeConnect через NGate, после успешной аутентификации на NGate будет автоматически получать свою персональную страницу с доступами на SafeConnect.

Примечание

Более подробно настройки NGate смотрите в Руководстве администратора КриптоПро NGate.

3.17. Пример настройки локальным пользователям доступа к удаленным ресурсам

Все назначения пользователям доступов к удаленным ресурсам происходят через систему заданий, расположенную на вкладке **Задания**. Добавить задание может любой пользователь SafeConnect, но добавить в задание доступы, других пользователей и разрешить им пользоваться этими доступами может только администратор с соответствующими правами. У главного администратора по умолчанию есть все права. В зависимости от инфраструктуры компании исполнители заданий, типы ресурсов, авторизации и используемых политик могут быть различными.

Обязательными для заполнения в задании являются поля **Тема** и **Описание**. Они заполняются, чтобы лучше понимать, для чего и для кого это задание было создано. Остальные параметры задания являются необязательными и будут рассмотрены в примере ниже. После заполнения полей **Тема** и **Описание** задание следует сохранить нажатием кнопки **Сохранить** (Рис.3.151), в противном случае задание не будет сохранено.

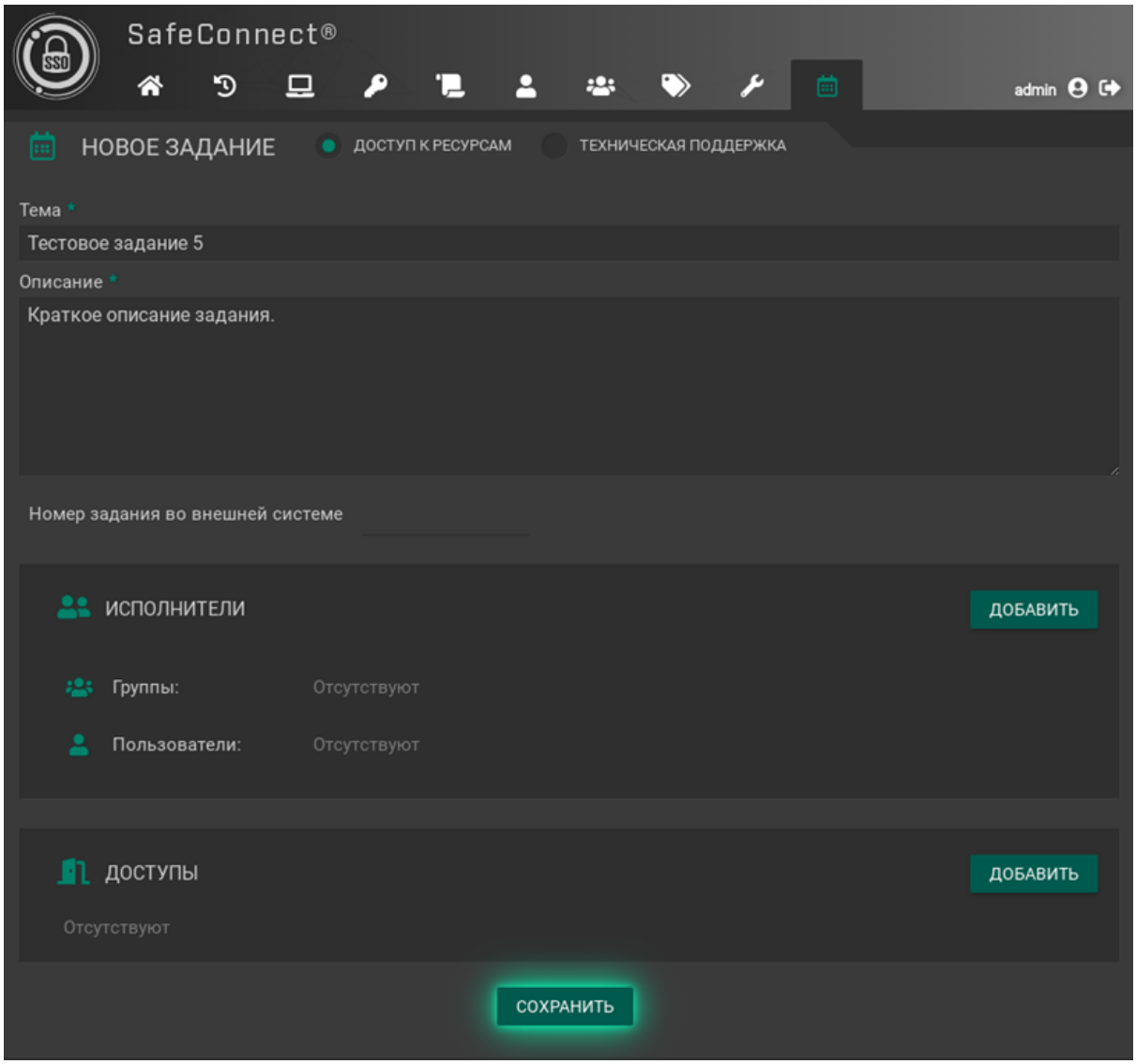


Рис. 3.151. Новое задание

Добавлять и удалять доступы и пользователей можно не только в новых заданиях, но также и в других уже открытых заданиях.

Для организации доступа локальных пользователей к удаленным ресурсам необходимо:

1. Перейти на вкладку **Ресурсы** и нажать кнопку **Добавить**.
2. Выбрать нужный протокол ресурса и заполнить обязательные поля формы.
3. Сохранить ресурс нажатием кнопки **Создать**.
4. Перейти на вкладку **Учетные записи** и нажать кнопку **Добавить**.
5. Заполнить обязательные поля формы.
6. Сохранить учетную запись нажатием кнопки **Создать**.
7. Перейти на вкладку **Пользователи** нажать кнопку **Добавить**.

8. Заполнить обязательные поля формы.

9. Сохранить пользователя нажатием кнопки **Создать.**

10. Перейти на вкладку **Задания** нажать кнопку **Добавить**.

11. Заполнить обязательные поля формы.

12. Открыть список возможных исполнителей нажатием кнопки **Добавить**, откроется список всех групп и пользователей, которых можно добавить в это задание (Рис.5.1).

13. Установить флажки тех групп и пользователей, которые будут в этом задании и смогут пользоваться доступами из него. Нажать кнопку **Применить**.

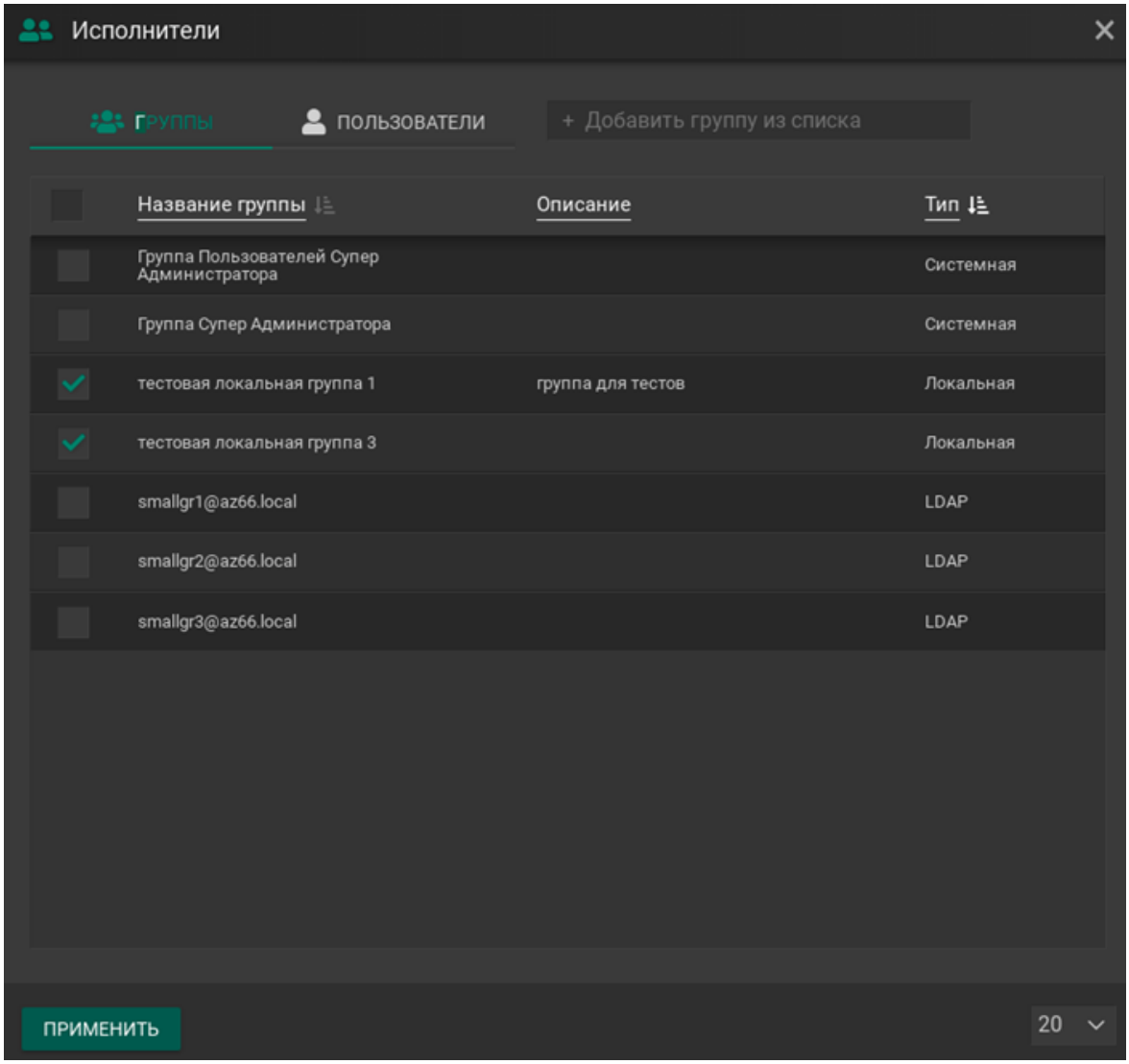


Рис. 3.152. Список исполнителей

14. Открыть список возможных доступов нажатием кнопки **Добавить**, откроется окно настройки доступа со списком всех ресурсов, учетных записей и политик (Рис.3.153).

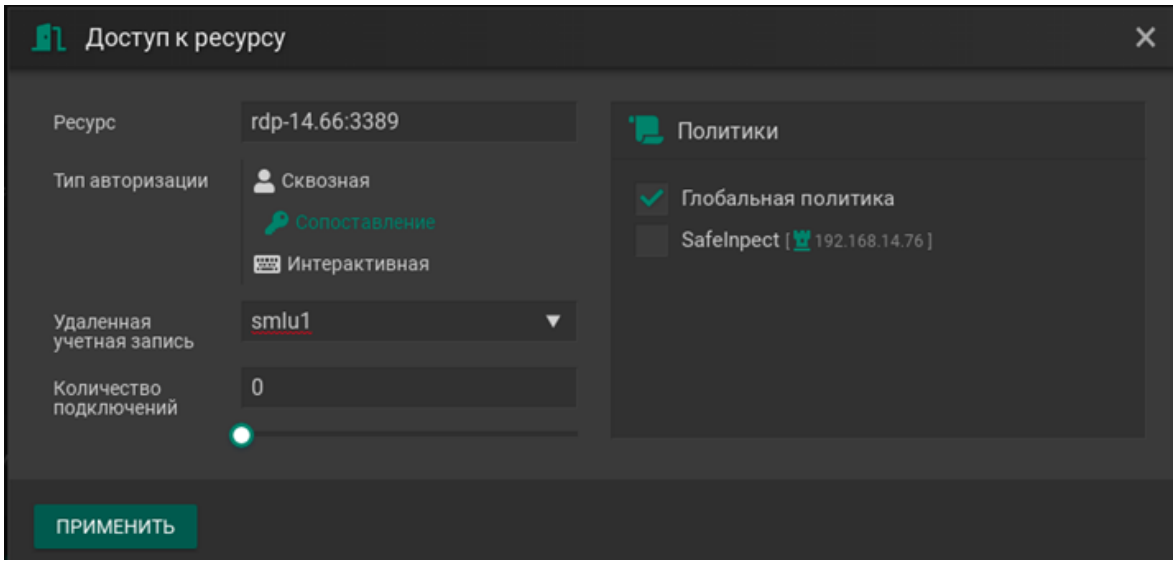


Рис. 3.153. Доступ к ресурсу

15. Выбрать из выпадающего списка нужный ресурс, тип авторизации, удаленную учетную запись (если необходима), количество подключений и политику. Нажать кнопку **Применить;**

16. После добавления исполнителей и доступов нужно сохранить задание кнопкой **Сохранить**;

17. После этого у добавленного доступа появятся кнопки **Подтвердить** и , которые, соответственно, разрешают использование этого доступа исполнителям этого задания или отменяют назначение этого доступа (Рис.3.154).

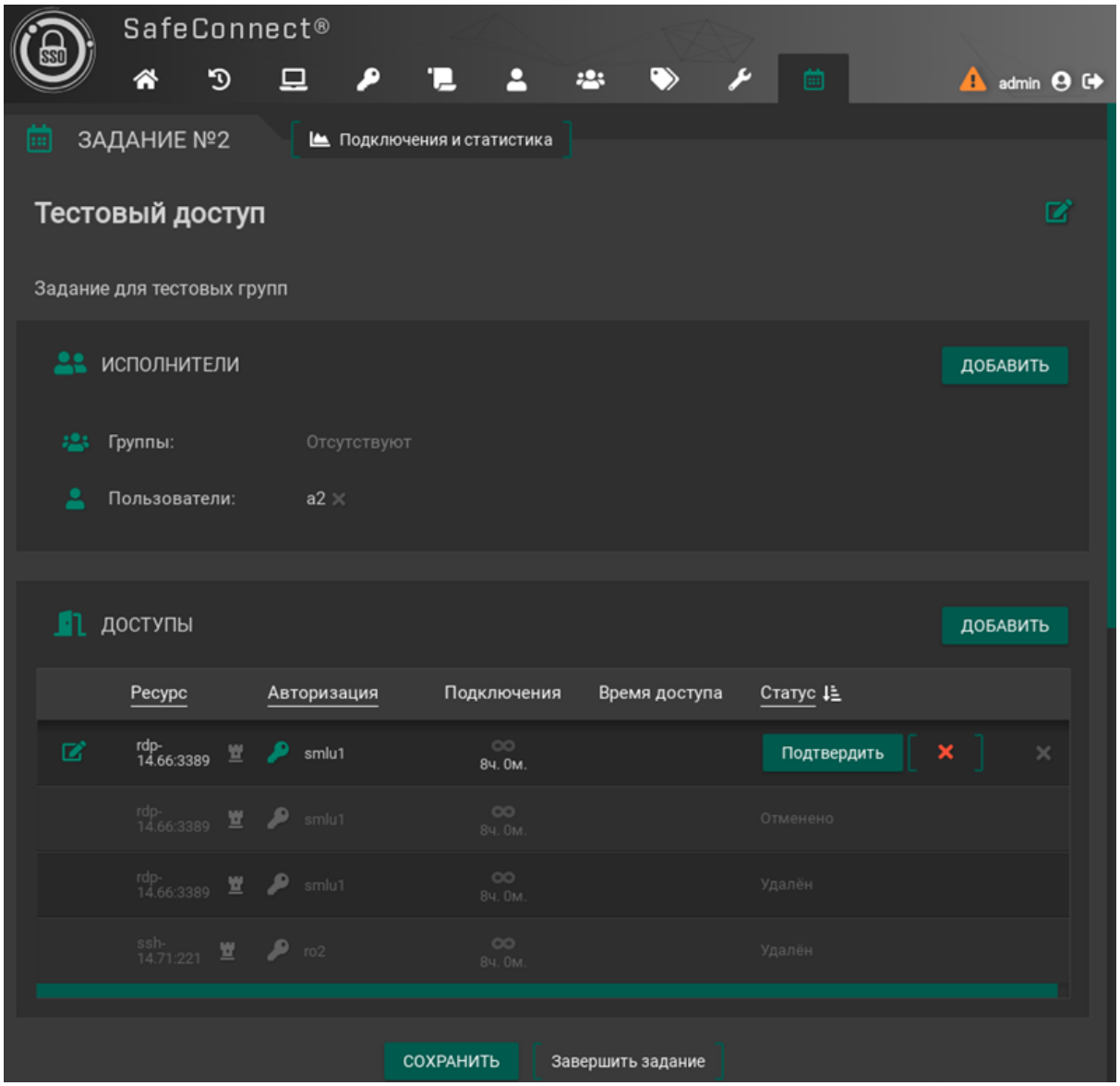


Рис. 3.154. Доступ к ресурсу (подтвердить/отменить)

После этого доступ из этого задания будет активен для всех исполнителей, которые в нём указаны. При логине исполнителя в SafeConnect доступ будет отображаться на главной странице, а также в списке заданий будет видно то задание, участником которого он является. Удалить конкретный доступ из задания можно, нажав на , напротив соответствующего ресурса. Завершить задание можно по кнопке **Завершить задание**, при этом все доступы из этого задания для всех исполнителей будут отменены, а также нельзя будет больше редактировать и комментировать задание и добавлять исполнителей и доступы.

4. Защита от атак подбора учетных данных

Для усиления безопасности системы и предотвращения атак подбора учётных данных реализован **механизм ограничения частоты попыток входа**. Этот функционал позволяет контролировать количество попыток аутентификации в течение определённого временного интервала и автоматически блокировать потенциально вредоносные источники.

Примечание

Система поставляется с предварительно настроенными параметрами для защиты от подбора учётных данных, обеспечивающими базовый уровень безопасности:

Лимит попыток: 3 запроса на вход в систему в течение 60 секунд.

Длительность блокировки: 180 секунд (3 минуты) при превышении установленного лимита.

Временное окно: интервал в 60 секунд (1 минута), в пределах которого отслеживаются попытки входа.

Этот механизм значительно повышает устойчивость системы к атакам, направленным на компрометацию учётных записей, обеспечивая при этом ясность для легитимных пользователей, которые могли случайно превысить лимит попыток.

Установка интервалов и лимитов для попыток входа

Для изменения конфигурации необходимо отредактировать файлы системы **/etc/sc/configs/sc-manager.conf** и **/opt/sc-ansible/roles/sc-common/defaults/main/main.yml**:

1. Откройте файл **/etc/sc/configs/sc-manager.conf** и внесите необходимые изменения в следующие параметры:
   - login_rate_limit: определяет максимальное количество попыток входа в систему, разрешённое с одного источника (IP-адреса) в течение login_rate_window.
   - login_rate_window: устанавливает временное окно (в секундах), в рамках которого подсчитываются попытки входа.
   - login_rate_block_duration: задаёт длительность блокировки (в секундах) для источника, превысившего установленный лимит попыток входа.
2. Откройте файл **/opt/sc-ansible/roles/sc-common/defaults/main/main.yml** и внесите изменения аналогично предыдущему пункту.
3. После внесения всех изменений в конфигурационные файлы для применения настроек необходимо выполнить перезапуск:

   ```
   systemctl restart sc-manager
   ```

5. Выход из программы

Для завершения работы с SafeConnect следует нажать на  в правом верхнем углу окна (Рис.5.1) .

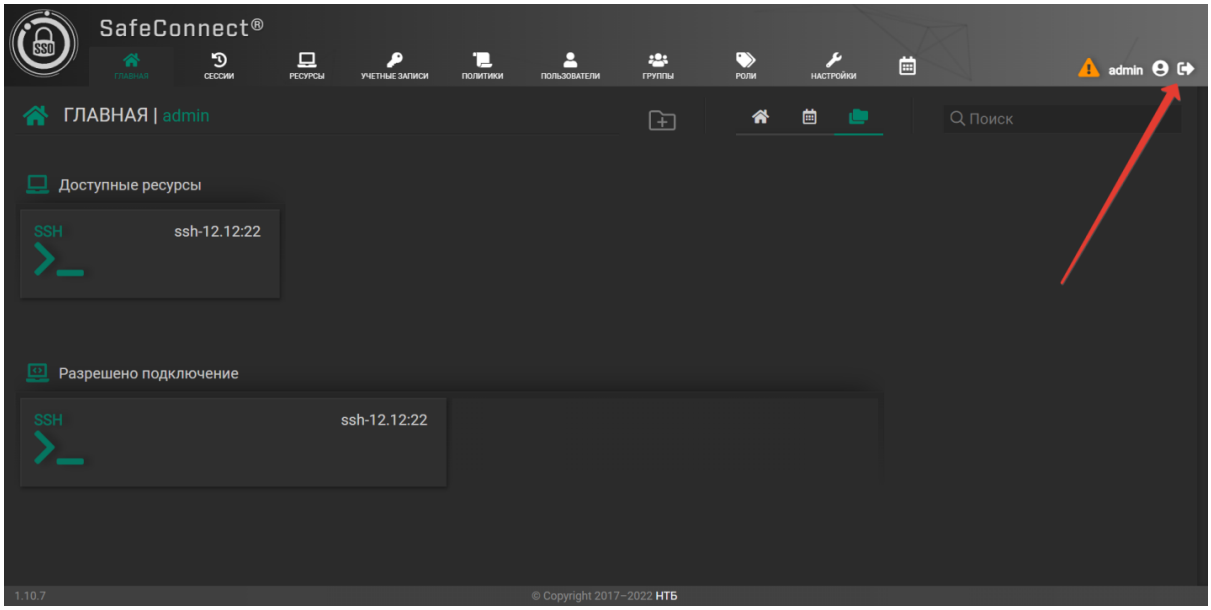


Рис. 5.1. Выход из программы

6. Устранение неполадок

В случае возникновения неполадок при работе системы SafeConnect, при которых отсутствует возможность загрузки логов посредством раздела **Настройки > Система**, вкладка **Логи** (п.3.12.12.3), реализована возможность резервной сборки логов.

Для загрузки и отправки обращения в службу поддержки клиентов с архивом логов SafeConnect наберите в адресной строке:

```
https://<ip–адрес_конкретного_узла_системы>/logs
```

В результате на локальное хранилище будет скачан архив (с паролем), содержащий логи системы.

При отправке запроса в службу технической поддержки указать описание проблемы, и приложить архив с логами системы.