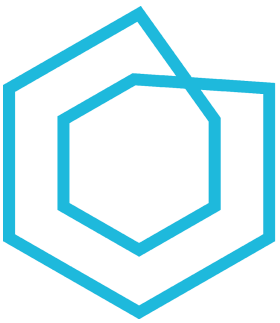
ООО «ВЭБ КОНТРОЛ ДК»



sPACE

Система Управления Привилегированным Доступом

sPACE PAM

ВЕРСИЯ 2.0.2

РУКОВОДСТВО АДМИНИСТРАТОРА

Москва, 2025

СОДЕРЖАНИЕ

ОБ ЭТОМ ДОКУМЕНТЕ

Этот документ является руководством администратора Системы управления привилегированным доступом sPACE PAM (далее Система, «программа», «программный продукт»).

Документ включает в себя главы с общим описанием программы, описанием ее структуры и пошаговыми инструкциями и пояснениями по основным ее функционалам, а также с действиями в случае аварийных ситуаций. Документ адресован специалистам, отвечающим за обеспечение работоспособности и настройку Системы.

ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ, ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

Термин/сокращение	**Определение**
Привилегированный доступ (ПД)	Неограниченный доступ для просмотра и изменения данных, изменения параметров конфигурации, запуска программ и т.д.
Сеанс привилегированного доступа	Интерактивный обмен данными, имеющий ограниченный временной интервал, в ходе которого владельцу учетной записи предоставляется привилегированный доступ. Сеанс считается запущенным с момента отображения на экране пользователя окна инструмента администрирования и законченным в момент выхода из инструмента администрирования.
Наряд-допуск (НД)	Разрешение на выполнение определенной задачи с использованием sPACE, в котором содержится название задачи, срок действия наряда-допуска, инициирующее и согласующее лицо, обоснование и объекты администрирования.
ОА	Объект администрирования. Целевая система, действия с которой производятся с использованием привилегированного доступа
ИА	Инструмент Администрирования. Приложение, запускаемое на сервере ЗСА, с помощью которого осуществляются привилегированный доступ к ОА.
ЗСА, СЗС	Защищенная Среда Администрирования. Сервер защищенной среды: выделенный сервер, на котором выполняется сеанс привилегированного доступа (также защищенный сервер - ЗС).
FQDN	Fully Qualified Domain Name, имя домена, не имеющее неоднозначностей в определении. Включает в себя имена всех родительских доменов иерархии DN
ВСАС	Внутренняя система аудита сеансов, осуществляющая запись скриншотов действий пользователей.
ПУЗ	Привилегированная учетная запись ОА
ИС/АС	Информационные и автоматизированные системы, к которым осуществляется привилегированный доступ
СОС	Система Обмена Сообщениями. Служба, обеспечивающая коммуникацию между компонентами sPACE.

1. ОБЩИЕ СВЕДЕНИЯ О СИСТЕМЕ sPACE

1.1. Назначение программы

Система sPACE PAM представляет собой автоматизированную систему организации и управления рабочим процессом привилегированных пользователей с интегрированной защищенной средой реализации их полномочий с минимальными правами, а также подсистемой управления жизненным циклом паролей и ключей доступа.

Целью Системы sPACE PAM является обеспечение безопасного технологического (гранулированного) доступа пользователей Оператора к информационным и автоматизированным системам (далее ИС/АС) с минимально необходимыми привилегиями. Решение позволяет исключить накопление у пользователей избыточных прав и контролирует действия пользователей по администрированию защищаемых ИТ-систем.

Система предназначена для автоматизации работы привилегированных пользователей, повышения уровня безопасности учетных данных, адресного предоставления привилегированным пользователям минимально необходимых привилегий на ограниченное время, повышения скорости предоставления привилегированным пользователям необходимых для работы прав, децентрализации процесса предоставления привилегированного доступа и организации объективного контроля сеансов привилегированного доступа для любых целевых ИС/АС.

Система sPACE PAM должна использоваться в совокупности с другими средствами защиты информации для повышения уровня информационной безопасности и исключения негативных инцидентов на целевых информационных и аппаратных системах.

1.3. Функции программы

В результате разворачивания Изделия на целевой инфраструктуре ИС/АС Система обеспечивает интегрированное выполнение следующих основных блоков своего функционала:

1. Портал sPACE: создание единой точки входа для всех пользователей Системы через веб-интерфейс с правами доступа только к своему личному кабинету с поставленными задачами администрирования.

2. Хранение всех привилегированных прав изолировано от пользователей любых ролей и осуществляется в СУПД sPACE PAM в виде отдельных привилегированных УЗ с настраиваемым алгоритмом их регулярного обновления.

3. В Системе реализован функционал нарядов-допусков для организации всех процессов привилегированного доступа к объектам администрирования (ОА) через гранулирование доступа (предоставление временного доступа для решения каждой задачи в составе НД), с автоматизацией процессов постановки и согласования НД ответственными сотрудниками организации.

4. В СУПД sPACE PAM возможно добавление любых ОА и сценариев запуска внутри Системы соответствующих приложений ПО удаленного администрирования, которые используются для управления целевых ИС/АС.

5. Система устанавливает соединение авторизованного пользователя для выполнения задачи администрирования, автоматически запуская разрешенные для него сеансы удаленного доступа на основе нарядов-допусков.

6. В sPACE реализован функционал онлайн мониторинга и хранения данных всех сеансов для использования сотрудниками с ролью “аудитор” в целях контроля за действиями пользователей.

7. В СУПД sPACE PAM обеспечены возможности администраторов Системы для настройки всех параметров и функций.

В частности, в программе реализованы следующие функции:

- предоставление защищенной среды администрирования (ЗСА), изолированной от потенциально вредоносной среды рабочей станции, с которой осуществляется привилегированный доступ;
- автоматизация процесса согласования привилегированного доступа;
- хранение паролей без раскрытия пользователю в защищенном хранилище, их ротация (настраиваемое автоматическое обновление);
- контроль доступа к совместным привилегированным учетным данным;
- контроль команд и действий, выполняемых специалистами;
- мониторинг и запись сеансов привилегированного доступа;
- поддержка протоколов удаленного администрирования;
- предоставление журналов событий и данных о действиях привилегированных пользователей с помощью консоли, отчетов и аналитики;
- двухфакторная аутентификация с использованием технологии RuToken, TOTP;
- ролевое разграничение доступа администраторов Системы к управлению программой;

- управление настройками и мониторинг корректной работы системы ;
- добавление новых объектов администрирования и инструментов привилегированного доступа;
- аварийный режим;
- возможность интеграции с существующими системами информационной безопасности посредством API;
- работа в разных тенантах;
- формирование отчетности об использовании системы (экспорт журнала событий и сеансов).

1.3. Перечень эксплуатационной документации

Для работы с Системой пользователю необходимо ознакомиться с настоящим Руководством администратора, Руководством пользователя, Инструкцией по развертыванию.

1.4. Уровень подготовки пользователя

Для работы с Системой пользователи системы должны обладать навыками администрирования серверов Linux, Windows, баз данных, базовым знанием языков автоматизации Expect и AutoIt, знанием основных инструментов администрирования, протоколов администрирования, навыками администрирования сетевой инфраструктуры компании.

1.5. Права доступа к функционалу sPACE

Роли пользователей в Системе sPACE

Персоналу, работающему с Системой, могут быть назначены следующие роли:

- базовый пользователь;
- стандартный пользователь;
- продвинутый пользователь;
- администратор;
- технический администратор;
- аудитор;
- продвинутый аудитор;
- привилегированный администратор

Администраторам системы также могут быть назначены дополнительные API роли:

- API_MANAGEMENT,
- API_DATA,
- API_RESOURCE_MANAGEMENT,
- API_SECURITY.

Сотрудникам, работающим с Системой, может быть назначено несколько ролей.

Базовый пользователь

Базовый пользователь имеет следующие права:

- запуск сеансов привилегированного доступа в защищенной среде.

Под сеансом привилегированного доступа понимается интерактивный обмен данными, имеющий ограниченный временной интервал, в ходе которого владельцу учетной записи предоставляется неограниченный в правах доступ для просмотра и изменения данных, изменения параметров конфигурации, запуска программ и т. д. Сеанс считается запущенным с момента отображения на экране пользователя окна инструмента администрирования и законченным в момент выхода из инструмента администрирования.

Для запуска сеанса привилегированного доступа базовому пользователю необходимо иметь согласованный наряд-допуск к конкретному информационному ресурсу. Наряд-допуск согласуется сотрудником, отвечающим за предоставление привилегированного доступа к данному объекту администрирования.

Под нарядом-допуском в данном документе понимается разрешение на выполнение определенной задачи с использованием sPACE, в котором содержится следующая информация:

- название задачи;
- информационный ресурс (объект), к которому запрашивается доступ;
- инструмент взаимодействия (оснастки, инструменты администрирования, программы, интерфейс) с информационным ресурсом, к которому запрашивается доступ;
- срок действия разрешения;
- учетное имя, используемое для доступа к ресурсу;
- лицо, согласующее доступ к данному информационному ресурсу;
- обоснование запроса на получение привилегированного доступа к данному информационному ресурсу (номер заявки из ITSM системы, например, текстовое описание ситуации, которая привела к

необходимости получить привилегированный доступ к данному информационному ресурсу (объекту));

- разнообразные настройки работы сеанса, подробнее о которых можно почитать в справке на портале.

Стандартный пользователь

Стандартный пользователь системы имеет следующие права:

- запуск сеансов привилегированного доступа в защищенной среде;
- запрос наряда-допуска для себя;
- согласование нарядов-допусков, если пользователь входит в группу согласования;
- просмотр записей собственных сеансов, если для них есть соответствующие данные ВСАС.

Сотрудник с ролью «Стандартный пользователь» имеет право согласовывать наряд-допуск, если его учетное имя добавлено в список лиц, согласующих наряд-допуск к данному информационному ресурсу (объекту администрирования). Он также имеет возможность просматривать записи собственных сеансов.

Продвинутый пользователь

Продвинутый пользователь имеет следующие права:

- запуск сеансов привилегированного доступа;
- запрос наряда-допуска для себя и для других пользователей;
- согласование нарядов-допусков, если пользователь входит в группу согласования;
- просмотр записей собственных сеансов, если для них есть соответствующие данные ВСАС.

Сотрудник с ролью «Продвинутый пользователь» имеет право согласовывать наряд-допуск, если его учетное имя добавлено в список лиц, согласующих наряд-допуск к данному информационному ресурсу (объекту администрирования). Он также имеет возможность просматривать записи собственных сеансов и запрашивать наряд-допуск для другого пользователя.

Администратор

Администратор sPACE осуществляет управление задачами на работу с информационными ресурсами, инструментами администрирования и учетными

записями в рамках **одного** тенанта. Он также может входить в группу согласования и согласовывать наряды-допуски.

Примечание: Тенант - обособленная в рамках одной инсталляции sPACE PAM область, настраиваемая техническим администратором системы. Каждый тенант позволяет использовать весь целевой функционал системы, имеет своего администратора и пользователей, свои привилегированные учетные записи и объекты администрирования, доступные только в рамках своего тенанта и без права доступа в другие тенанты sPACE. Тенанты могут создаваться для обособленных подразделений/площадок в рамках холдинговой структуры.

Технический администратор

Технический администратор sPACE осуществляет управление всеми объектами ИТ-инфраструктуры компании, настраивает приложения, пользовательские роли и осуществляет мониторинг состояния системы в рамках **всех** тенантов. Также именно он настраивает тенанты.

Аудитор

Аудитор имеет право просматривать сеансы привилегированного доступа в реальном времени и в архиве.

Продвинутый аудитор

Помимо стандартных возможностей аудитора, данный тип пользователей имеет право на просмотр данных из key-log и clipboard для сеансов привилегированного доступа.

Привилегированный администратор

Привилегированный администратор – это сотрудник, который в дополнение к правам обычного администратора имеет право перевода Системы в аварийный режим.

Примечание*:* Аварийный режим – это режим Системы, при котором базовые, стандартные и продвинутые пользователи имеют возможность узнать учетные данные объектов администрирования, доступ к которым для них согласован.

Перечень функционала, доступного для каждой роли

Таблица Функционал, доступный каждой роли

Наименование	**Права**	**Описание роли в веб интерфейсе**	**Имя группы в каталоге домена** (при активной галочке по умолчанию)
Базовый пользователь	**Доступен раздел "Сеансы"**	**ROLE_SPACE_RESTRICTED_USER**	**SPACE_RESTRICTEDUSERS**

Наименование	**Права**	**Описание роли в веб интерфейсе**	**Имя группы в каталоге домена** (при активной галочке по умолчанию)
	● Запуск сеансов администрирования на основе согласованных "Нарядов-допусков".		
Стандартный пользователь	**Доступен раздел "Сеансы"** ● Просмотр объектов администрирования, сгруппированных в виде задач. ● Запрос наряда-допуска на объекты администрирования для своей учетной записи. ● Запуск сеансов администрирования на основе согласованных нарядов-допусков. ● Согласование нарядов-допусков, если пользователь входит в группу согласующих для соответствующей задачи администрирования. ● Просмотр записей собственных сеансов, если для них есть соответствующие данные BCAC.	**ROLE_SPACE_STANDARD_USER**	**SPACE_STANDARDUSERS**
Продвинутый пользователь	**Доступен раздел "Сеансы"** ● Просмотр объектов администрирования, сгруппированных в виде задач. ● Возможность запросить "Наряд-допуск" на объекты администрирования для своей учетной записи и для чужих учетных записей. ● Запуск сеансов администрирования на основе согласованных "Нарядов-допусков". ● Согласование "Нарядов-допусков", если пользователь входит в группу согласующих для соответствующей задачи администрирования.	**ROLE_SPACE_USER**	**SPACE_USERS**

Наименование	**Права**	**Описание роли в веб интерфейсе**	**Имя группы в каталоге домена** (при активной галочке по умолчанию)
	● Просмотр записей собственных сеансов, если для них есть соответствующие данные ВСАС.		
Администратор	**Доступен раздел "Управление системой"** ● Управление пользователями. ● Управление группами согласования. ● Управление привилегированными учетными записями. ● Управление объектами администрирования. ● Управление задачами. ● Управление нарядами-допусками. ● Управление доменами. ● Управление агентами паролей. ● Управление фильтрацией ввода. ● Просмотр информации о сеансах, операциях с секретами, статусе компонентов и статистике использования системы.	**ROLE_SPACE_ADMIN**	**SPACE_ADMINS**
Технический администратор	**Доступен раздел "Управление ресурсами"** ● Управление тенантами ● Управление пользователями. ● Управление интерпретаторами ● Управление приложениями и сценариями их запуска. ● Управление серверами защищенной среды (ЗС). ● Управление пользовательскими ролями. ● Управление системными настройками.	**ROLE_SPACE_TECH_ADMIN**	**SPACE_TECH_ADMINS**

Наименование	**Права**	**Описание роли в веб интерфейсе**	**Имя группы в каталоге домена** (при активной галочке по умолчанию)
	• Просмотр журнала событий и управление параметрами фильтрации. • Управление внутренней системой видеоаудита (BCAC) и хранилищами для нее. • Просмотр полной таблицы статуса компонентов. • Управление лицензией. • Просмотр статистики.		
Аудитор	**Доступен раздел "Аудит"** • Просмотр журнала доступа пользователя. • Просмотр сеансов администрирования в реальном времени. • Просмотр видеозаписей данных сеансов. • Просмотр списка сеансов.	**ROLE_SPACE_AUDITOR**	**SPACE_AUDITORS**
Продвинутый аудитор	**Доступен раздел "Аудит"** • Просмотр журнала доступа пользователя. • Просмотр сеансов администрирования в реальном времени. • Просмотр видеозаписей данных сеансов. • Просмотр списка сеансов. • Просмотр данных key-log и clipboard для сеансов.	**ROLE_SPACE_TRUSTED_AUDITOR**	**SPACE_TRUSTED_AUDITORS**
Привилегированный администратор	**Доступен раздел "Управление системой"** • Управление пользователями. • Управление группами согласования.	**ROLE_SPACE_SUPERADMIN**	**SPACE_SUPERADMINS**

Наименование	Права	Описание роли в веб интерфейсе	Имя группы в каталоге домена (при активной галочке по умолчанию)
	• Управление привилегированными учетными записями. • Управление объектами администрирования. • Управление задачами. • Управление нарядами-допусками. • Управление доменами. • Управление агентами паролей. • Управление фильтрацией ввода. • Просмотр информации о сеансах, операциях с секретами, статусе компонентов и статистике использования системы. • Перевод Системы в аварийный режим.		

Настройка прав доступа для каждой роли

При работе Система автоматически добавляет в Систему пользователей из соответствующих групп службы каталогов LDAP (AD для Windows). Для этого необходимо настроить в Системе соответствующий домен, а также наличие в этом домене пользователей в LDAP/AD.

Назначение или изменение роли учетной записи происходит путем добавления пользователя в соответствующую группу службы каталогов. Рекомендуемое соответствие ролей в Системе группам в каталогах LDAP/AD приводится в Инструкции по развертыванию.

1.6. Состав и содержание дистрибутивного носителя данных

Программный продукт sPACE PAM распространяется в виде архива, доступного для загрузки по индивидуальной ссылке.

В состав дистрибутива системы входят следующие файлы:

- spaceinstall – исполняемый файл, предназначенный для установки на машину Linux, который осуществляет установку компонентов системы sPACE Mono (Base);

- linux_js_installer.gz — архив, с помощью которого осуществляется установка JS Linux.
- space-installer-3.0.1.exe — исполняемый файл, который осуществляет установку JS Windows.

Для работы sPACE необходимо осуществить как минимум одну установку Ядра и одну установку сервера защищенной среды (JS).

В состав дистрибутива входит программное обеспечение сторонних производителей, которое необходимо для работы Системы. Список стороннего ПО представлен в следующем разделе, процедура установки Системы описана в Инструкции по развертыванию.

1.7. Условия работоспособности Системы

Серверные компоненты Системы устанавливаются как на физические серверы под управлением MS Windows Server 2012R2 и выше/Linux, так и виртуальные серверы на платформах виртуализации VMWare, Hyper-V, Zen. Допускается развертывание компонентов Системы в гибридной среде.

Компоненты Системы могут быть расположены как на одной машине в пределах одной компании/ЦОД, так и быть географически распределены.

Стороннее программное обеспечение, необходимое для работы sPACE

Для работы sPACE необходимо стороннее ПО, которое может входить в состав дистрибутива. Краткий список представлен в таблице 2, полный отчет об opensource компонентах можно найти в файле «Приложение_Opensource компоненты sPACE.html».

Таблица Перечень стороннего ПО

ПО	Описание
JRE	Java SE Runtine Environment (x64)
JCE	Java Cryptography Extension
PostgreSQL DB	База данных PostgreSQL
Tomcat	Контейнер сервлетов (x64)
NATS	Платформа, реализующая систему обмена сообщениями (COC)
AutoIt	Скрипт для автоматизации выполнения задач в ОС Microsoft Windows.

ПО	Описание
Docker CE	Система контейнеров для Linux.

Требования к аппаратному обеспечению серверной части

Таблица Требования к аппаратному обеспечению серверов

Сервер	Характеристики физического сервера
Сервер sPACE Mono (Base)	Процессор: 4 ядра, 2,2 ГГц Оперативная память: 8 ГБ Дисковое пространство: 150 ГБ
Сервер 3CA	Процессор: 4 ядра, 2,2 ГГц Оперативная память: 8 ГБ Дисковое пространство: 150 ГБ
Хранилище архива сессий	Требуется рассчитать дополнительно.

Требования к программному обеспечению серверной части

Таблица Требования к программному обеспечению серверов

Сервер	Состав ПО
Сервер sPACE Mono (Base)	CentOS 7-8, Ubuntu 22 и выше, Astra Linux «Орёл», Red OS «Муром» 7.3.2; OpenSSL 1.1.1 и выше; Docker 24.0 и выше.
Сервер 3CA	Microsoft Windows Server 2012-2019; Remote Desktop Server (RDS); Windows PowerShell 5.1 и выше.
Сервер 3CA Linux	CentOS 7-8, Ubuntu 20 и выше, Astra Linux «Орёл», Red OS «Муром» 7.3.2; OpenSSL 1.1 и выше; Expect.

Требования к аппаратному обеспечению рабочих станций

Таблица Требования к аппаратному обеспечению рабочих станций

Компонент	Минимальная конфигурация
Процессор	Intel Pentium 1.8 ГГц (или совместимый аналог), число ядер – 2
Оперативная память (RAM)	3 ГБ
Жесткий диск (доступное место на диске)	HDD или SSD, 2 ГБ
Видеоадаптер	Любой
Сетевая плата	Ethernet 100 Мбит/с (рекомендуется 1 Гбит/с)
Дополнительное оборудование	Монитор 1024x768 и больше (рекомендуется 1920x1080), мышь, клавиатура

Требования к программному обеспечению рабочих станций

Таблица Требования к программному обеспечению рабочих станций

Компонент	Конфигурация
Операционная система	Microsoft Windows 7-10, Linux (CentOS 7-8, Ubuntu 18.04, Ubuntu 20.04, Astra Linux «Орёл»), Mac OS 10.11 и выше, iOS 8.0 и выше, Android 4.1 и выше, …
Прикладное ПО	Microsoft Edge 79.0 и выше, Google Chrome 119.0 и выше, Chromium 121 и выше; Mozilla Firefox 115.0 и выше; Совместимый клиент RDP; Open Secure Shell (для работы с сервером ЗСА Linux); Windows PowerShell 5.1 и выше (для работы с сервером ЗСА Linux).

Установка, настройка и использование Системы должны осуществляться в соответствии с эксплуатационной документацией. Перед началом работы необходимо установить все доступные обновления для компонентов Системы. Система должна эксплуатироваться на компьютерах, отвечающих минимальным требованиям, приведенным выше.

Для работы через Сервер ЗСА Linux на ПК, с которого осуществляется запуск задачи, требуется установить ssh-клиент. То есть в случае, если доступ осуществляется с рабочего места под управлением Windows, ssh-клиент должен быть установлен на это рабочее место..

Для работы с ПК под управлением Linux также потребуется установка Windows Powershell не ниже версии 5.1.

2. СТРУКТУРА СИСТЕМЫ sPACE

Архитектура Системы представляет собой программный комплекс, в состав которого входят различные компоненты, обеспечивающие взаимодействие между пользователями и объектами ИТ-инфраструктуры, включая объекты привилегированного доступа, каталоги учетных данных, системы сторонних производителей. Для связи компонентов друг с другом, обеспечения масштабируемости и отказоустойчивости, используется кластер серверов очередей сообщений.

Система sPACE состоит из 3 базовых компонентов:

- защищенная среда администрирования (ЗСА);
- портал sPACE;
- sPACE Mono (Base).

Взаимодействие между 3 базовыми компонентами осуществляется при помощи системы (серверов) обмена сообщениями.

Для аутентификации и авторизации пользователей и сбора информации об информационных ресурсах Система взаимодействует со службами каталогов операционной системы.

2.1. Защищенная среда администрирования

Защищенная среда администрирования (ЗСА) — это выделенный сервер, на котором выполняется сеанс привилегированного доступа (ПД). Привилегированные учетные данные используются изолированно от потенциально вредоносной среды рабочей станции пользователя. Этот компонент представляет собой набор элементов (RDP RemoteApp, ssh и др), каждый из которых реализует возможность графического или командного удаленного доступа. Эти элементы используются для запуска и управления сеансов ПД. Сеансы могут быть запущены на разных платформах (Windows, Linux) на основе протоколов удалённого доступа RDP, SSH, Citrix. В базовой конфигурации один сервер ЗСА поддерживает до 50 параллельных сеансов.

2.2. Портал sPACE

Портал sPACE является единой точкой входа пользователей всех ролей. На Портале происходит выбор информационного ресурса, выбор инструмента подключения к этому ресурсу и выбор учетной записи, от имени которой осуществлять это подключение.

2.3. Ядро sPACE

Ядро sPACE – основной программный компонент Системы, который осуществляет обработку запросов от остальных компонентов на сохранение, загрузку, модификацию и удаление всех объектов, которыми оперирует система.

2.4. Система обмена сообщениями

Системы sPACE построена на основе микросервисной архитектуры, для управления потоками между микросервисами используется система обмена сообщениями (СОС) NATS. Сервис обмена сообщениями маршрутизирует запросы к серверам ЗСА, повышает устойчивость соединения, распределяет потоки данных, в том числе при масштабировании, снижает задержку при доступе к администрируемой системе и обеспечивает гибкость схемы подключения.

2.5. Архитектура Системы

Архитектурно система состоит кластера, включающего Ядро (два Ядра в отказоустойчивом варианте установки) и серверы ЗСА (Jump server), на которых запускаются средства администрирования ИС/АС заказчика. Таких кластеров может быть установлено несколько в зависимости от специфики и разнесенности площадок с ИС/АС. Все компоненты системы объединены Системой обмена сообщениями с зашифрованным трафиком данных. Подключение пользователей идет через вэб-интерфейс на Портале sPace. Архитектура Системы представлена на Рисунке 1. Подробно о ней можно прочитать в Инструкции по развертыванию sPACE.

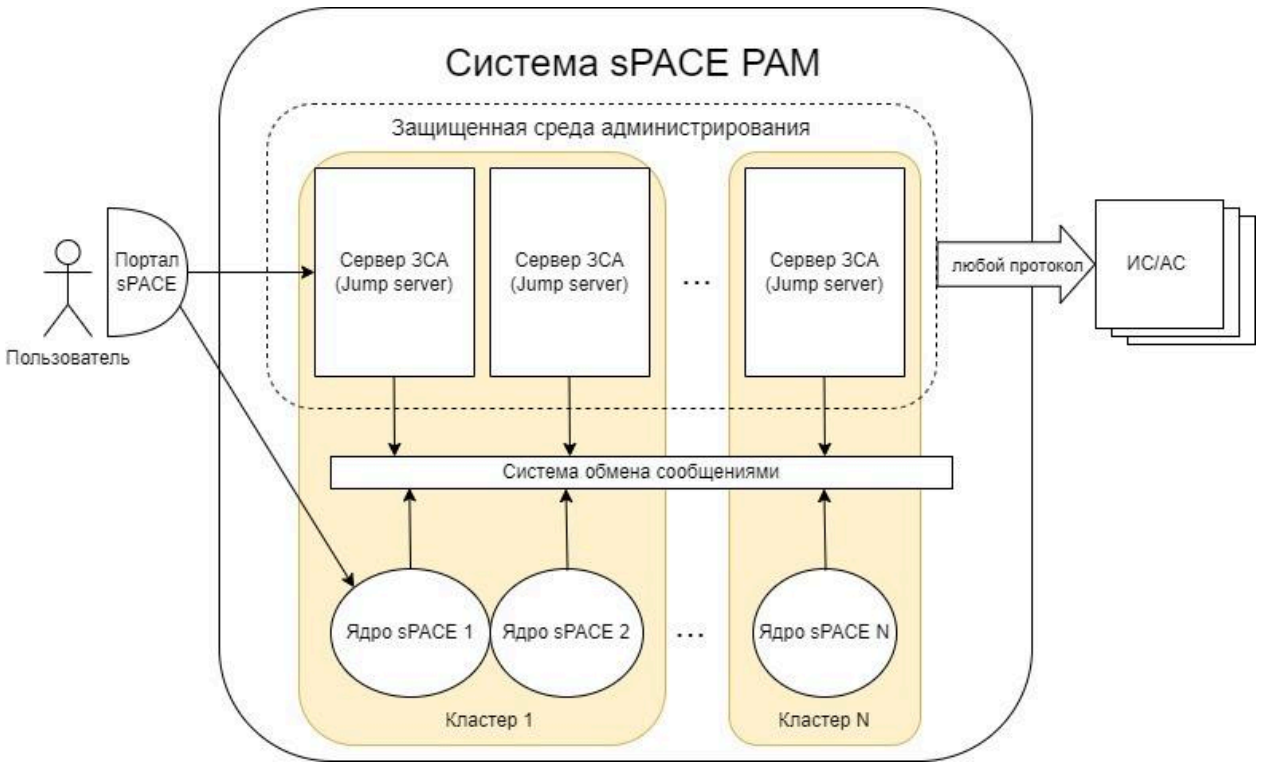


Рис. 3.1. Архитектура Системы

3. НАСТРОЙКА И УПРАВЛЕНИЕ sPACE

Для функционирования sPACE на аппаратное обеспечение должно быть установлено программное обеспечение. Установка и настройка программного обеспечения, необходимого для работы sPACE, описана в Инструкции по развертыванию. В данном разделе приводится описание действий по настройке Системы в условиях конкретной ИТ-инфраструктуры компании.

Настройка Системы происходит через интерфейс Системы. Для выполнения действий по начальной настройке sPACE необходимо наличие роли «Технический администратор», настройки для пользователей и объектов администрирования задаются “Администраторами” и “Привилегированными администраторами”.

Функционал Системы предполагает выполнение следующих действий по настройке Системы.

- Управление пользователями;
- Управление пользовательскими ролями и настройка имен ролей в AD;
- Управление группами согласования;
- Управление привилегированными учетными записями;
- Управление объектами и инструментами администрирования;
- Управление задачами;
- Управление нарядами-допусками;
- Управление доменами;
- Управление агентами паролей;
- Управление операциями с секретами;
- Управление внутренней системой видеоаудита (ВСАС);
- Управление сеансами привилегированного доступа;
- Просмотр статистики;
- Осуществление аудита системы;
- Управление параметрами фильтрации ввода;
- Управление тенантами;
- Управление интерпретаторами;
- Управление сценариями запуска приложений;
- Управление серверами защищенной среды (ЗС);
- Просмотр системных настроек;

- Удаленная установка и удаление компонентов системы (Ядра и серверов ЗС);
- Формирование отчетности о событиях;
- Просмотр статуса компонентов системы;
- Управление лицензией.

Раздел «Управление системой» служит для просмотра и редактирования информации об имеющихся в тенанте сущностях, доступен только для пользователей с правами администраторов тенанта (ROLE_SPACE_ADMIN). Раздел представлен в виде следующих узлов:

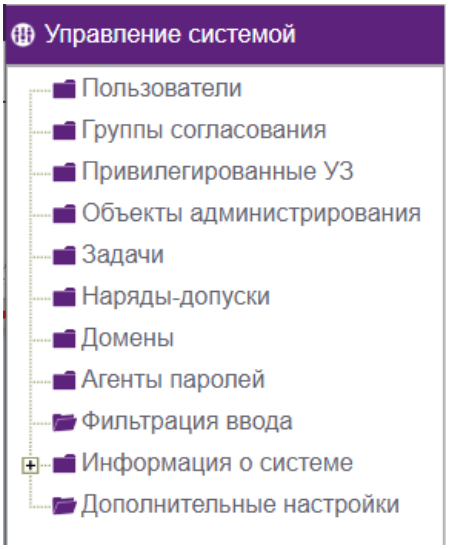


Рис. 3.1 Раздел «Управление системой»

Раздел «Управление ресурсами» служит для просмотра и редактирования информации о сущностях, имеющихся во всех тенантах и отвечающих за всю систему в целом, доступен только для пользователей с правами технических администраторов. Тенант - это своеобразная "копия" системы, которая предназначается для использования, например, одним из подразделений компании. Пользователь одного тенанта не может попасть на другой тенант, т. к. разные тенанты изолированы друг от друга. У каждого из тенантов может быть своя инфраструктура, которая задается во вкладке "Управление системой" и может редактироваться пользователем с ролью Администратор или Привилегированный администратор тененаta.

Элементы системы, которые задаются в панели "Управление ресурсами", являются общими для всех тенантов, ими может управлять только пользователь с ролью "Технический администратор". Этот раздел представлен в виде следующих узлов:

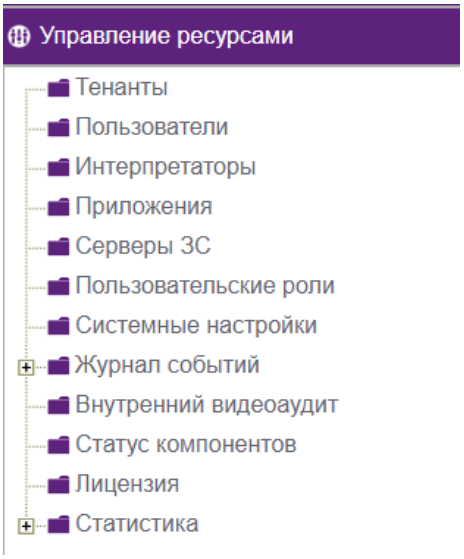


Рис. 3.2. Раздел «Управление ресурсами»

Вкладка "Аудит" служит для получения объективных качественных и количественных оценок о текущем состоянии портала, имеющихся в нем сеансов, пользователей и их действий. Она представлена в виде следующих узлов:

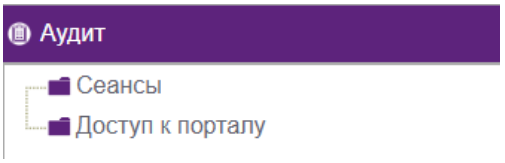


Рис. 3.2. Раздел «Аудит»

3.1. Управление пользователями разных тенантов

Для управления пользователями необходимо перейти в узел **Пользователи** раздела «Управление системой», если нужен пользователь в том же тенанте, что и администратор, или раздела «Управление ресурсами», если нужен пользователь в любом тенанте.

Функционал для двух вкладок почти аналогичен, различается лишь тем, что

- на вкладке «Управлении ресурсами» технический администратор производит манипуляции в любом тенанте, но только с внутренними пользователями,
- на вкладке «Управление системой» администратор тенанта может работать только с пользователями своего тенаната, включая внутренних и доменных пользователей.

Примечание:

Внутренний пользователь - учетная запись которого:

- создается через веб-интерфейс Системы,

- пароль создается администратором тенанта или техническим администратором,
- пароль хранится внутри СУПД sPACE,
- в карточке пользователя в поле домена указано internal.

Доменный (внешний) пользователь:

- пользователь, его пароль и его роль создаются в стороннем домене вне Системы,
- пароли внешних пользователей не хранятся внутри СУПД sPACE,
- в карточке пользователя указывается имя домена для привязки к Системе.

Действия , которые может выполнить администратор с пользователями:

- просмотреть список всех пользователей Системы;
- добавить новых пользователей, в том числе внутренних;
- редактировать данные существующих пользователей;
- удалить существующих пользователей;
- ограничить существующих пользователей;
- отключить поддержку двухфакторной аутентификации.

3.1.1. Просмотр списка всех пользователей Системы

Для просмотра списка и данных сотрудников, имеющих доступ к Системе, необходимо перейти в узел «Пользователи». Данные сотрудников представлены в виде таблицы, содержащей следующие поля:

- Имя пользователя;
- Домен;
- ФИО;
- 2FA (2-факторная аутентификация);
- Ограничен.

Рис. 3.1.1 Список пользователей

3.1.3. Добавление новых пользователей

Для добавления новых пользователей необходимо перейти в узел **Пользователи** раздела **Управление системой** и щелкнуть мышью на кнопке **Добавить**. Добавить можно только того пользователя, который уже создан в на внешнем домене или же пользователя внутреннего домена.

Форма добавления пользователей Пользователь содержит следующие поля (на рисунке ниже полужирным шрифтом выделены поля, обязательные для заполнения):

- Имя пользователя (обязательное поле) – наименование пользовательской учетной записи;
- Фамилия – фамилия пользователя;
- Имя – имя пользователя;
- Отчество – отчество пользователя;
- Домен (обязательное поле) – наименование домена, в котором зарегистрирована пользовательская учетная запись;
- Мобильный телефон – мобильный телефон пользователя;
- Телефон – стационарный телефон пользователя;
- Электронный адрес – адрес электронной почты пользователя;
- Ограничить – если поставить галочку, пользователь не сможет авторизоваться на портале и пользоваться его возможностями, такими как, например, запуск сеансов.

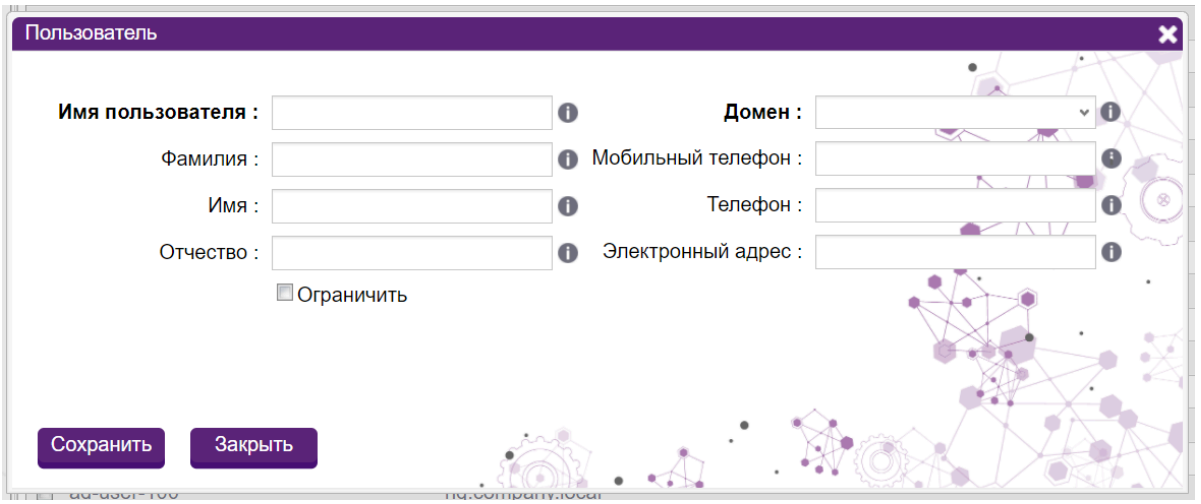


Рис. 3.1.2 Форма добавления новых пользователей

Если вы добавляете пользователя для внутреннего домена, то появятся дополнительные поля:

- Пароль (обязательное поле) – пароль пользователя в системе. При необходимости пароль можно сгенерировать с помощью соответствующей кнопки;
- Подтверждение пароля (обязательное поле) - нужно для того, чтобы продублировать пароль и не ошибиться в нем.
- Роль (обязательное поле) – одна или несколько ролей, которые соответствуют функционалу, доступному этому пользователю на портале.

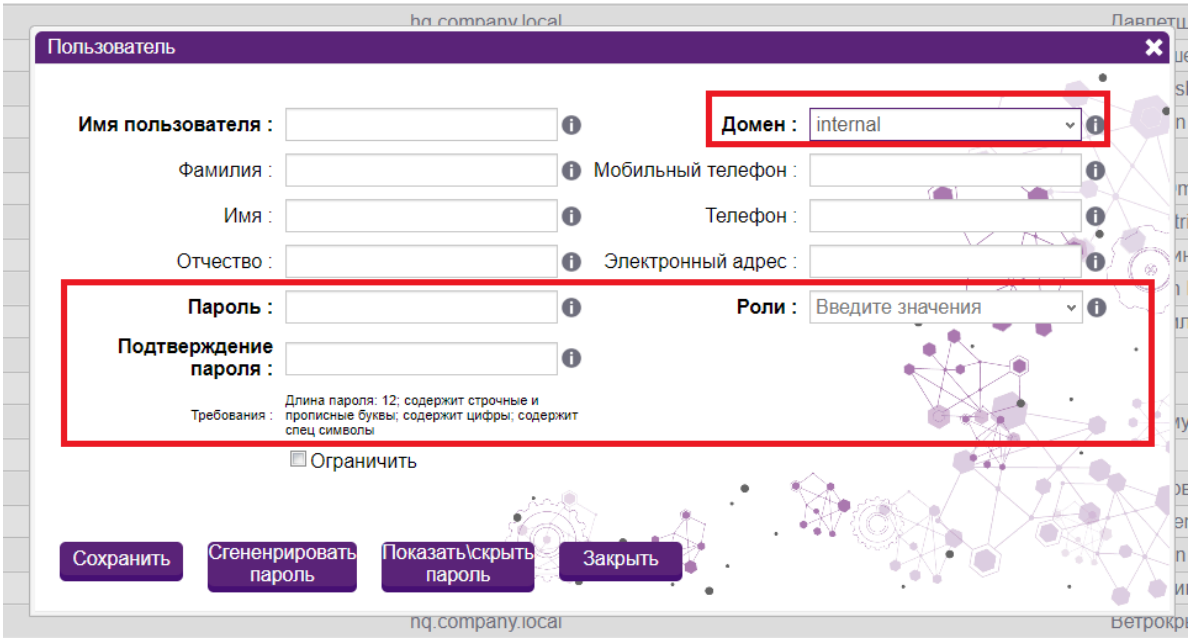


Рис. 3.1.3 Добавление внутреннего пользователя

Если добавление пользователя происходит через вкладку «Управление ресурсами», то вместо графы «Домен» будет выведена строка выбора тенанта. Это связано с тем, что все пользователи, добавленные через вкладку «Управление ресурсами», будут внутренними.

3.1.3. Редактирование данных существующего пользователя

Для редактирования данных пользователя необходимо перейти в узел **Пользователи** раздела **Управление системой** и дважды щелкнуть мышью на имени пользователя в списке пользователей. В появившемся окне **Пользователь** можно просмотреть все данные пользователя.

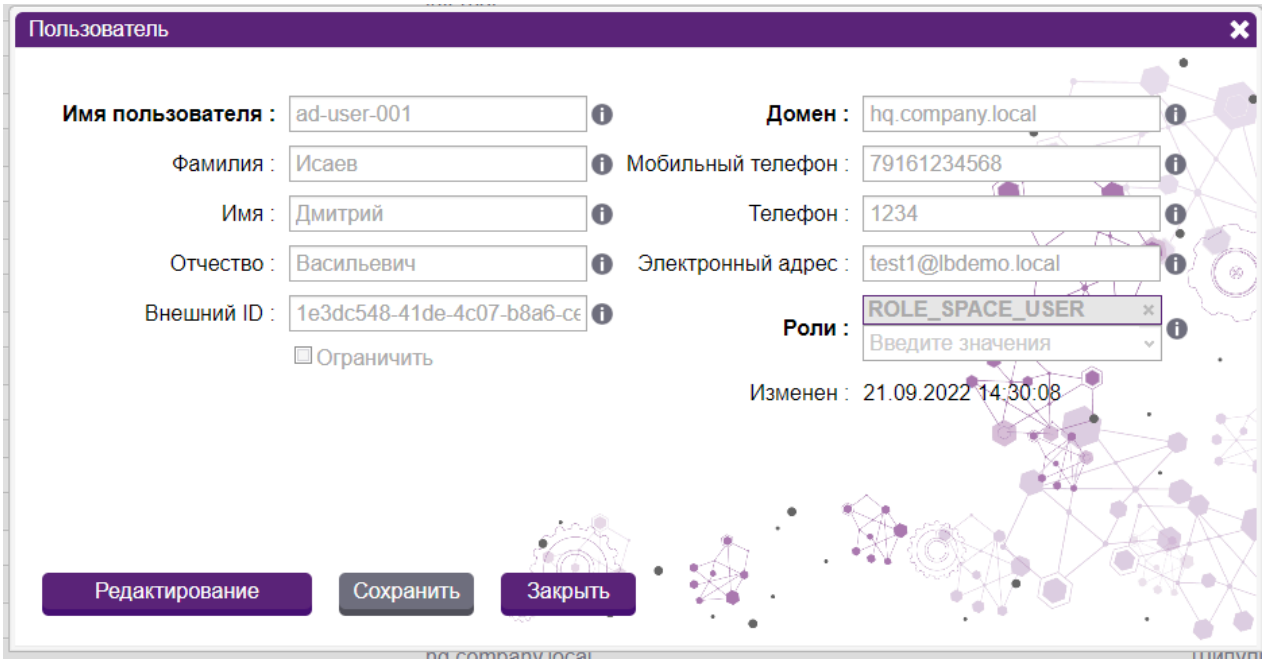


Рис. 3.1.4. Форма просмотра данных пользователя

После щелчка мышью на кнопке **Редактирование** появляется форма **Редактирование пользователя**, в которой доступны для редактирования все поля, кроме **Имя пользователя, Внешний ID** и **Домен**. Чтобы сохранить изменения необходимо щелкнуть на кнопке **Сохранить**. При нажатии кнопки **Закрыть** никаких изменений в карточке пользователя не произойдет.

Примечание. Внешний ID - уникальный идентификатор всех создаваемых пользователями информационных объектов sPACE, в частности, используемый для интеграции внешних систем через API sPACE с данной сущностью.

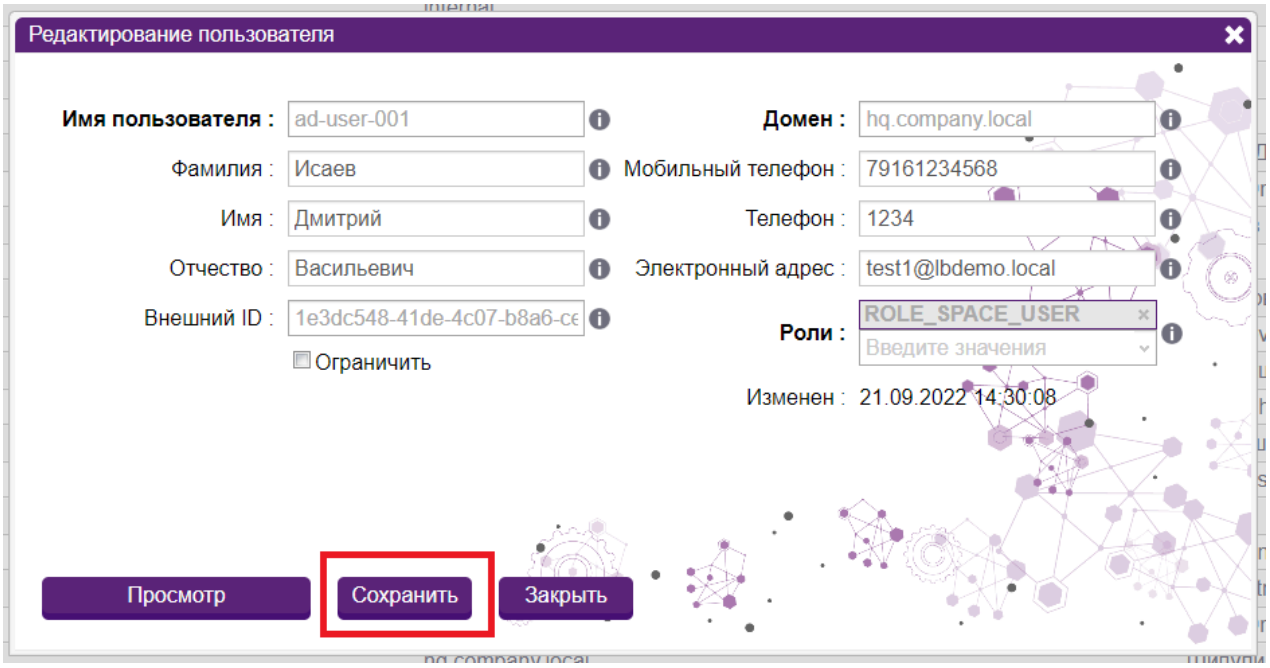


Рис. 3.1.5 Форма редактирования данных пользователя

Если редактирование пользователя происходит через вкладку «Управление ресурсами», то вместо графы «Домен» будет выведена строка выбора тенанта. Это связано с тем, что все пользователи, добавленные через вкладку «Управление ресурсами», будут внутренними.

3.1.4. Удаление пользователей из Системы

Для удаления пользователя из Системы необходимо перейти в узел **Пользователи** раздела **Управления системой**, поставить флажок в соответствующем поле слева и щелкнуть на кнопке **Удалить**. Таким образом можно удалить несколько пользователей.

Внешних пользователей тоже можно так удалить, но из-за того что они заведены в контроллере домена, они смогут снова войти. Удаленный пользователь снова появится в списке, но с другим ID и без информации "старого" пользователя (НД, сеансов и т.д.)

3.1.5. Обновление таблицы пользователей

Для обновления записей в таблице пользователей служит соответствующая кнопка **Обновить**, расположенная в правой части верхней панели.

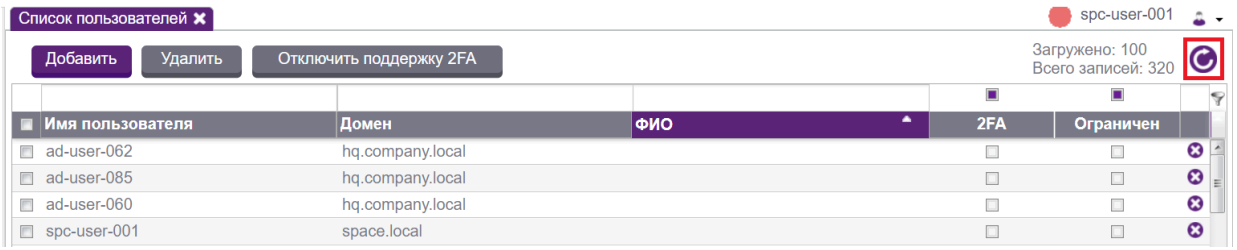


Рис. 3.1.6 Форма редактирования данных пользователя

3.1.6. Добавление или отключение поддержки двухфакторной аутентификации

Поддержку двухфакторной аутентификации пользователь настраивает самостоятельно. Для отключения поддержки двухфакторной аутентификации у одного или нескольких пользователей администратору необходимо перейти в узел **Пользователи** раздела **Управление системой**, выделить нужных пользователей галочкой слева (у них должна стоять отметка о включении 2FA в соответствующем столбце), после чего станет активной кнопка "Отключить поддержку 2FA", расположенная сверху над таблицей. Подробнее о подключении двухфакторной аутентификации вы можете прочитать в руководстве пользователя в разделе 6.5.1.

3.2. Управление группами согласования

Группа согласования — это определенная группа пользователей, которые имеют право согласовать (одобрять) наряды-допуски на управление объектами

администрирования для выполнения конкретной задачи. При создании задачи обязательно должна указываться та группа пользователей, которая будет ее согласовывать.

После щелчка мышью на узле **Группы согласования** дерева навигации раздела **Управление системой** пользователю отображается окно **Группы согласования**, которое представляет собой таблицу с двумя столбцами: **Имя группы** и **Пользователей**.

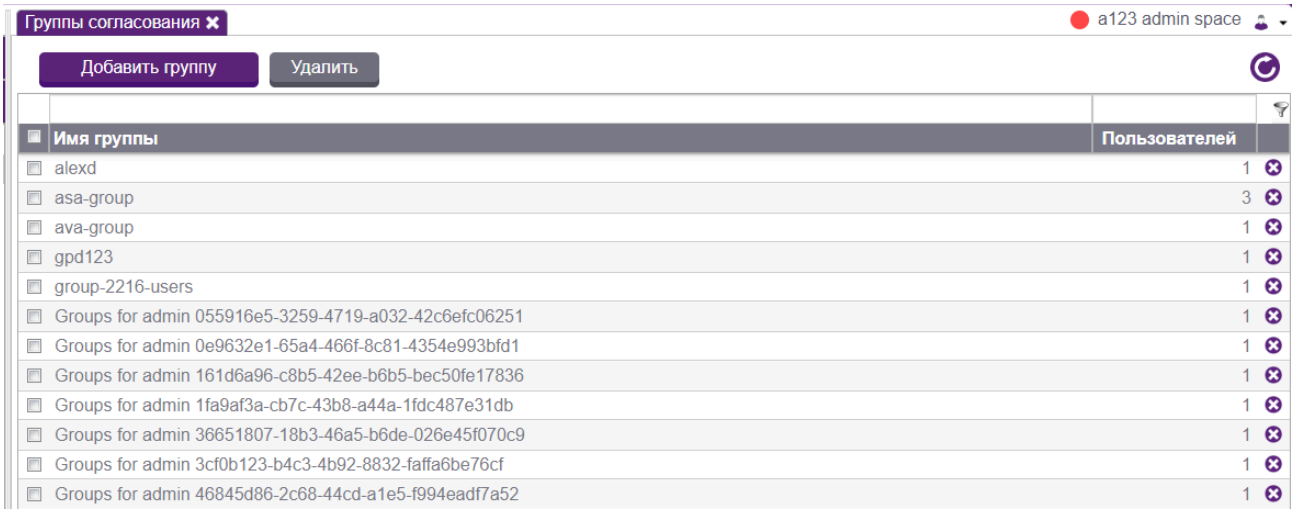


Рис. 3.2.1. Окно «Группы согласования»

В поле **Имя группы** отображается наименование группы, в поле **Пользователей** отображается количество человек в группе.

В рамках управления группами администратор может выполнять следующие действия:

- добавлять группы согласования;
- редактировать группы согласования;
- добавлять пользователей в группу согласования;
- удалять пользователей из группы согласования;
- удалять группу согласования.

3.2.1. Добавление групп согласования

Для добавления группы согласования необходимо перейти в узел **Группы согласования** раздела **Управление системой** и щелкнуть на кнопке **Добавить группу** панели инструментов **Группы согласования**.

В появившейся форме «Создание группы» необходимо заполнить следующие поля:

- Имя (обязательное поле) – наименование группы согласования;

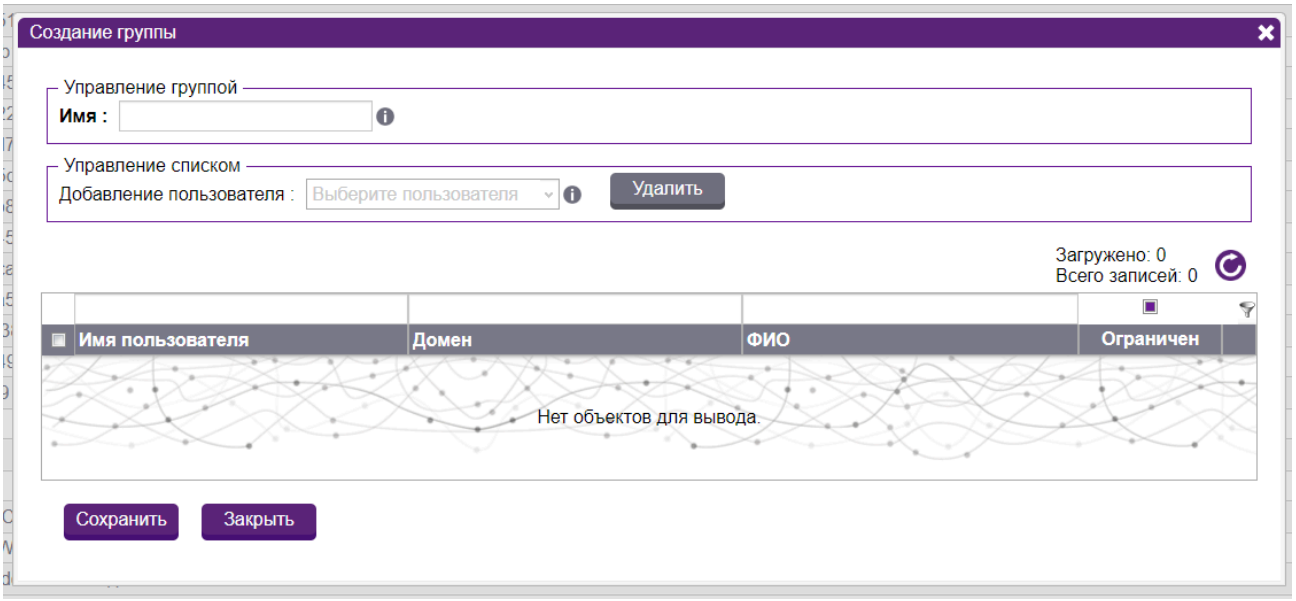


Рис. 3.2.2. Форма создания группы

Для добавления пользователей в группу согласования необходимо создать группу, а после этого войти в режим редактирования группы (см. ниже).

После заполнения необходимого поля и нажатия кнопки **Сохранить** новая группа согласования будет добавлена в таблицу **Группы согласования**.

3.2.2. Редактирование группы согласования

Для редактирования группы необходимо перейти в узел **Группы согласования** раздела **Управление системой** и дважды щелкнуть мышью на имени группы в таблице **Группы согласования**. В появившейся карточке группы можно просмотреть все данные о группе. Чтобы отредактировать данные, нужно щелкнуть мышью на кнопке **Редактировать**.

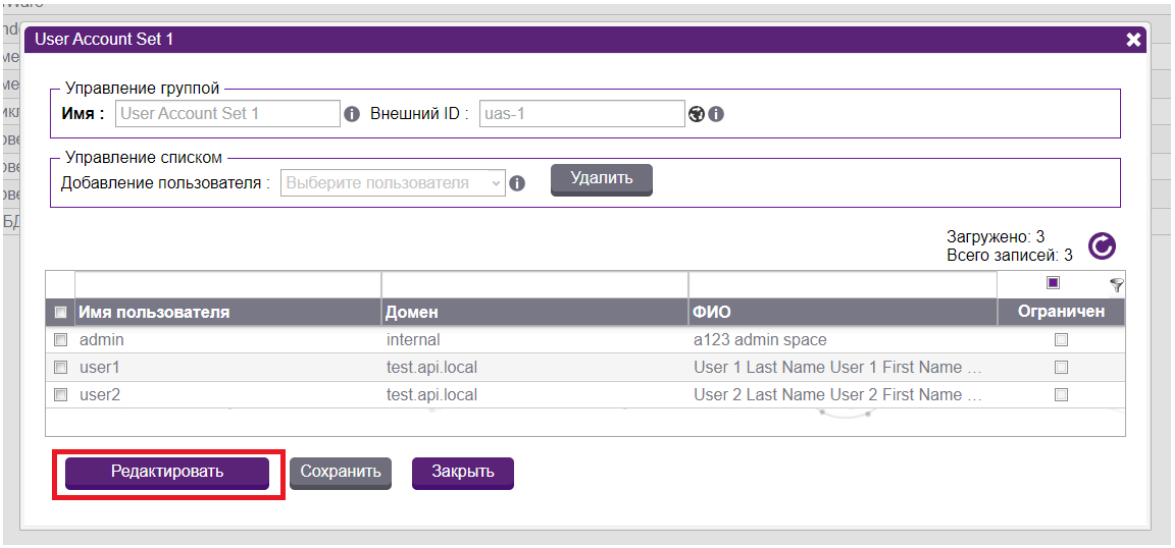


Рис. 3.2.3. Кнопка «Редактировать»

В появившейся форме редактирования группы можно изменить имя группы, добавить в группу или удалить из группы пользователей, зарегистрированных в Системе. Чтобы сохранить изменения необходимо щелкнуть на кнопке **Сохранить**. При щелчке на кнопке **Закрыть** никаких изменений в карточке группы не произойдет.

3.2.3. Добавление пользователей в группу согласования

Для добавления пользователя в группу согласования необходимо в окне редактирования группы выбрать имя пользователя из выпадающего списка поля **Добавление пользователя**. Пользователь будет добавлен автоматически.

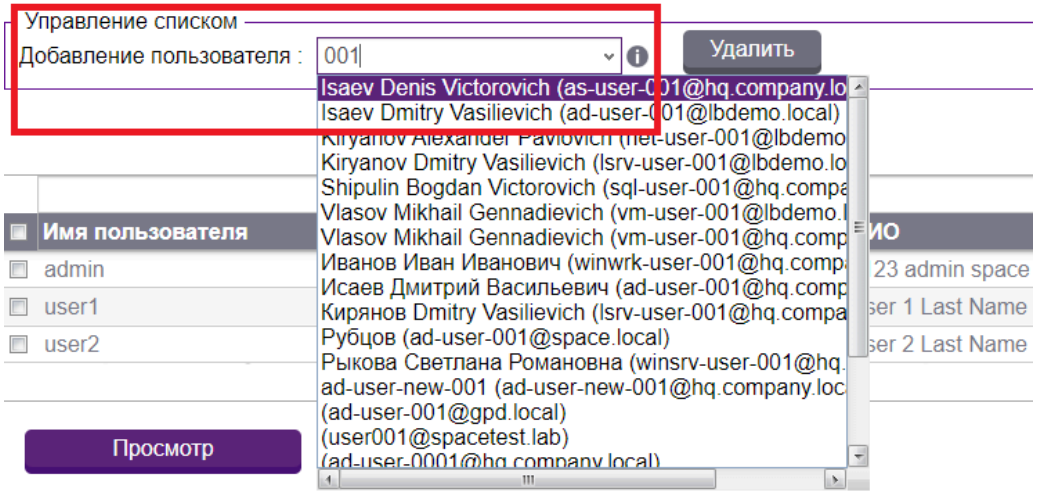


Рис. 3.2.4. Выбор пользователя из списка

Добавить в группу можно любого пользователя. Если у него нет роли, включающей в себя возможность согласования НД, то ему просто не будет показан такой раздел.

3.2.4. Удаление пользователей из группы согласования

Для удаления пользователя из списка «Группы согласования» необходимо нажать на соответствующий значок в строке пользователя в карточке группы и подтвердить действие в диалоговом окне.

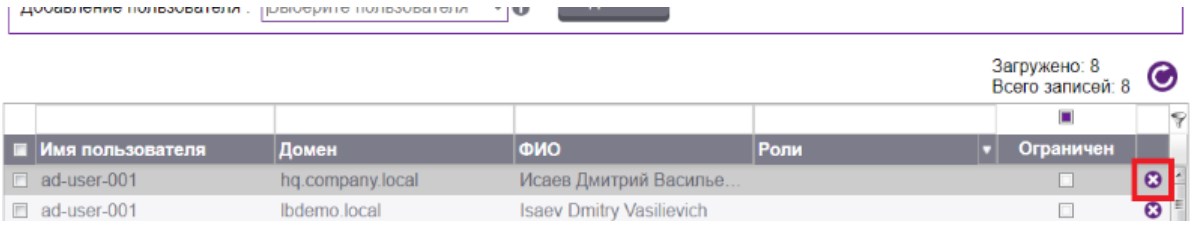


Рис. 3.2.5 Значок удаления пользователя

Для удаления нескольких пользователей одновременно необходимо выделить желаемые записи в таблице пользователей карточки группы, установив флажок в соответствующем поле слева от поля **Имя пользователя**, после чего станет активной кнопка **Удалить** над таблицей.

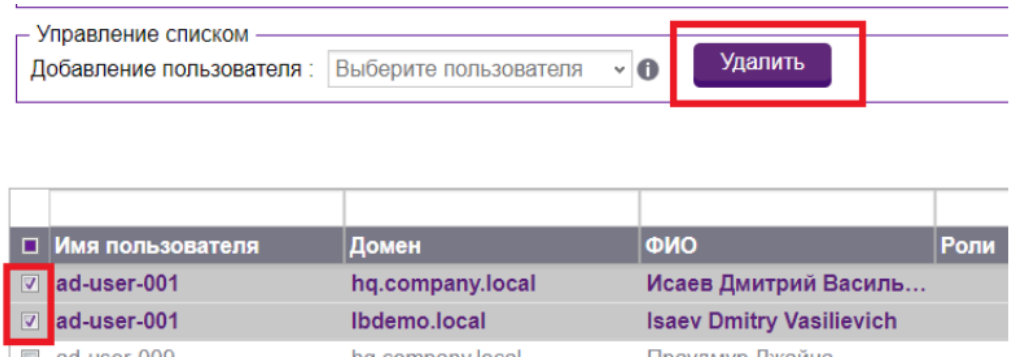


Рис. 3.2.6. Кнопка «Удалить» активна

3.2.5 Удаление группы согласования

При удалении группы согласования, если есть зависимые сущности (например, задача, где эта группа указана), то будет выведено соответствующее предупреждение с предложением удалить зависимые сущности.

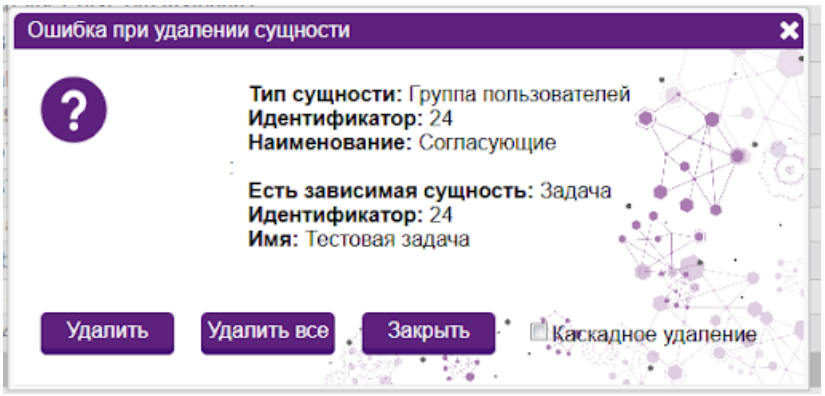
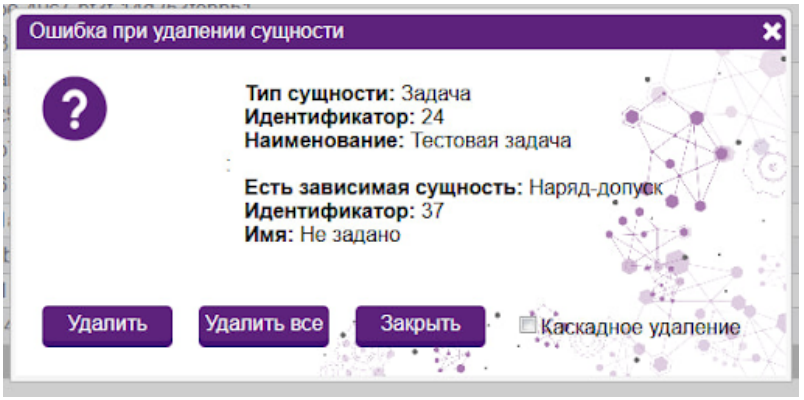


Рис. 3.16. Предупреждение о наличии зависимой сущности при удалении группы согласования

При этом если на эту задачу есть НД, то после нажатия на "Удалить" тоже появится окно о зависимых сущностях.



приме

Рис. 3.17. Предупреждение о наличии зависимой сущности при удалении задачи

3.3. Управление привилегированными учетными записями

Привилегированные учетные записи (ПУЗ) служат для подключения к объектам администрирования в рамках Наряда-допуска, и в обычной ситуации пользователь не знает их пароля. Администраторы тенанта могут выполнять следующие действия с привилегированными учетными записями:

- Добавлять учетную запись;
- Редактировать учетную запись;
- Обновлять таблицы учетных записей;
- Удалять строки в таблице учетных записей;
- Удалять нескольких записей из таблицы учетных записей одновременно;
- Импортировать привилегированные учетные записи из файла;
- Включать и выключать аварийный режим.

Примечание: для перевода Системы в аварийный режим необходимо наличие роли «Привилегированный администратор».

3.3.1. Добавление привилегированной учетной записи

Для добавления учетной записи необходимо перейти в узел **Привилегированные УЗ** раздела **Управление системой** и щелкнуть мышью на кнопке **Добавить** в таблице **Привилегированные УЗ**.

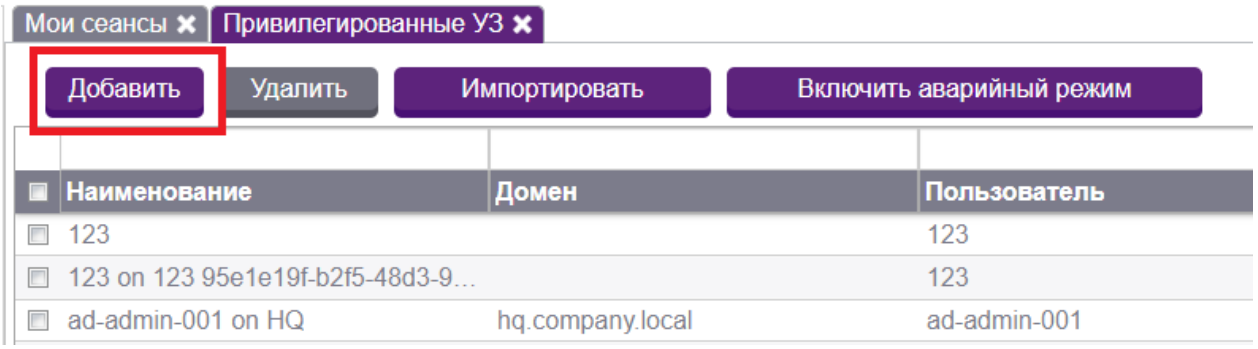


Рис. 3.3.1. Кнопка «Добавить»

Появившаяся форма добавления “**Привилегированная УЗ**” содержит следующие поля:

- **Наименование** (обязательное поле) – произвольное наименование ПУЗ в Системе, по которому пользователь может удобным образом обозначить для себя назначение ПУЗ;
- Домен (обязательное поле для доменных ПУЗ) – сокращенное наименование домена, к которому принадлежит учетная запись. Можно выбрать из раскрывающегося списка доменов, добавленных в Систему. Если УЗ является локальной для домена под управлением ОС Windows, то поле можно не заполнять;
- **Пользователь** (обязательное поле) – логин для этой привилегированной учетной записи, с которой пользователь системы sPACE получает доступ на конечный объект администрирования;
- FQDN – Fully Qualified Domain Name, имя домена, не имеющее неоднозначностей в определении. Включает в себя имена всех родительских доменов иерархии DNS. Поле обязательно для заполнения, когда учетная запись используется для работы с объектами под управлением ОС Windows. Если учетная запись является локальной для ОА под Windows, то необходимо указать точку: ".";
- Владелец – владелец (пользователь) данной привилегированной учётной записи. После выбора владельца учётная запись становится персонифицированной - в дальнейшем её можно привязать к задаче, назначенной другому пользователю, но такая задача не запустится. Если владелец не указан, то учетная запись является общедоступной;
- Объект администрирования – объекты, с которыми работает пользователь-владелец ПУЗ. Если поле остается пустым — учетная запись может быть использована на любом объекте администрирования. Если поле заполнено — использовать данную учетную запись можно только с тем объектом администрирования, который указан в данном поле;
- Агент паролей – тип password agent-а для управления паролем ПУЗ;

- Агент рандомизации паролей – выбор агента рандомизации паролей во вкладке "Агенты паролей" для рандомизации паролей ПУЗ;
- Рандомизация пароля – настройка, показывающая, когда необходимо производить рандомизацию паролей для ПУЗ (до или после сеанса, по расписанию и др.);
- Управление расписанием – активно, если в поле "Рандомизация паролей" выбрано "Рандомизировать по расписанию". Необходимо для указания периодичности и времени рандомизации.

После создания привилегированной учетной записи при ее сохранении появится окно **Задать секрет**. Наличие пароля является обязательным условием корректной работы Системы с привилегированной УЗ. Для тех учетных записей, которые используются в сценариях без автоматического ввода пароля, можно указать заведомо неправильный пароль.

Примечание: Для учетных записей, которые будут использоваться в работе с интерпретатором AutoIt (на сервере ЗСА Windows) существуют ограничения по использованию в пароле следующих спец-символов: **!**, **#**, **+**, **^**, **{**, **}**. AutoIt воспринимает эти символы как команды и прерывает ввод пароля. Рекомендуем не пользоваться этими символами, либо, если их использование в пароле необходимо, при вводе пароля в Системе использовать фигурные скобки. Пример: пароль «Examp^lE!» должен быть введен в системе в виде «Examp{^}lE{!}».

Также важно задать FQDN для привилегированной УЗ перед тем, как использовать ее для запуска сеанса.

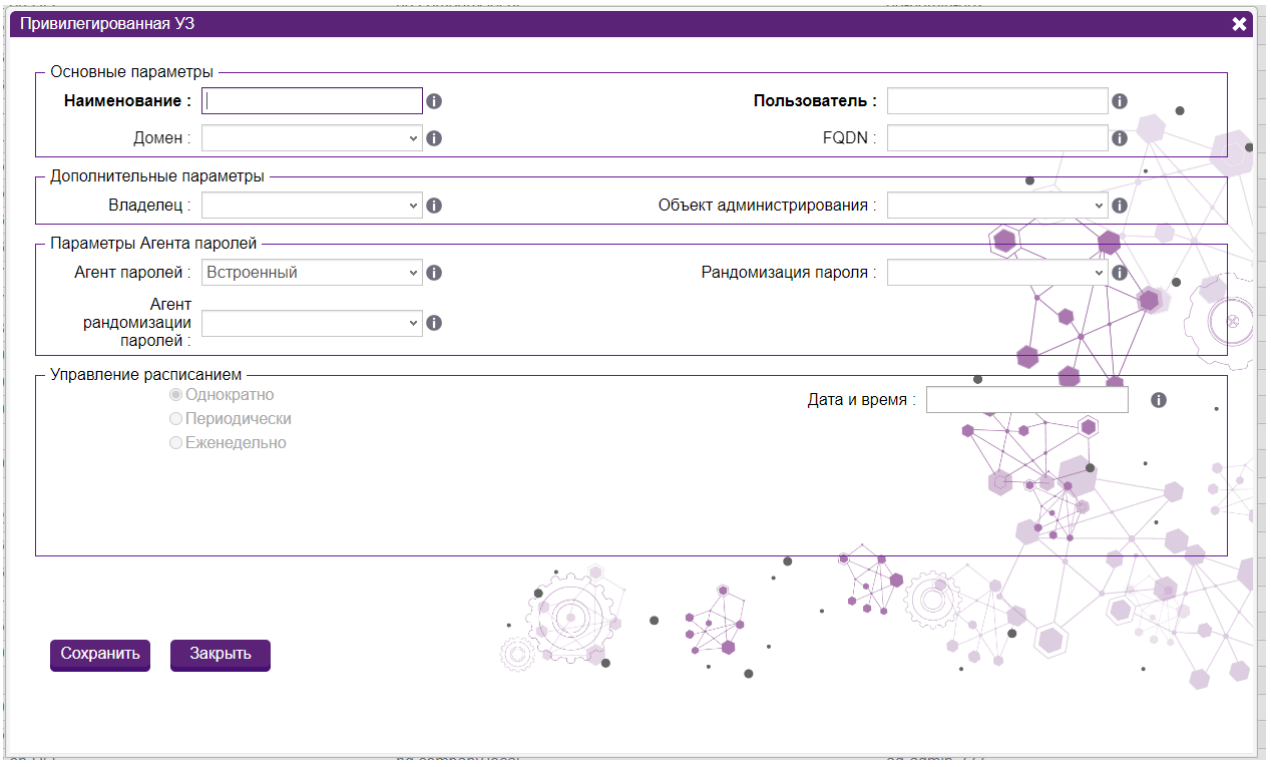


Рис. 3.3.2. Форма добавления учетной записи

3.3.2. Редактирование учетной записи

Для редактирования учетной записи необходимо перейти в узел **Привилегированные УЗ** раздела **Управление системой** и дважды щелкнуть на строке учетной записи в таблице учетных записей.

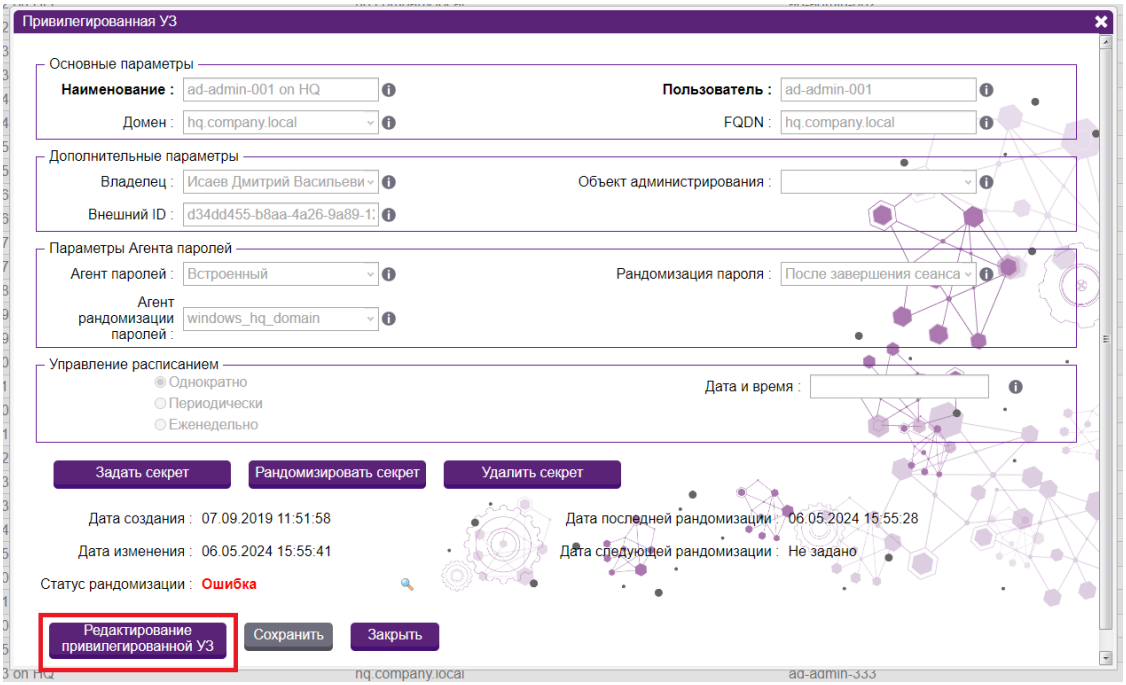


Рис. 3.3.3. Окно «Учетная запись». Кнопка редактирования активна

В появившемся с информацией об учетной записи **Учетная запись** будет активна кнопка **Редактирование учетной записи**.

После нажатия на кнопку **Редактирование** на экране отобразится форма **Редактирование учетной записи**. Все поля, кроме Внешнего ID, доступны для редактирования. Чтобы сохранить изменения, необходимо нажать кнопку **Сохранить**. При нажатии кнопки **Закрыть** никаких изменений в карточке пользователя не произойдет.

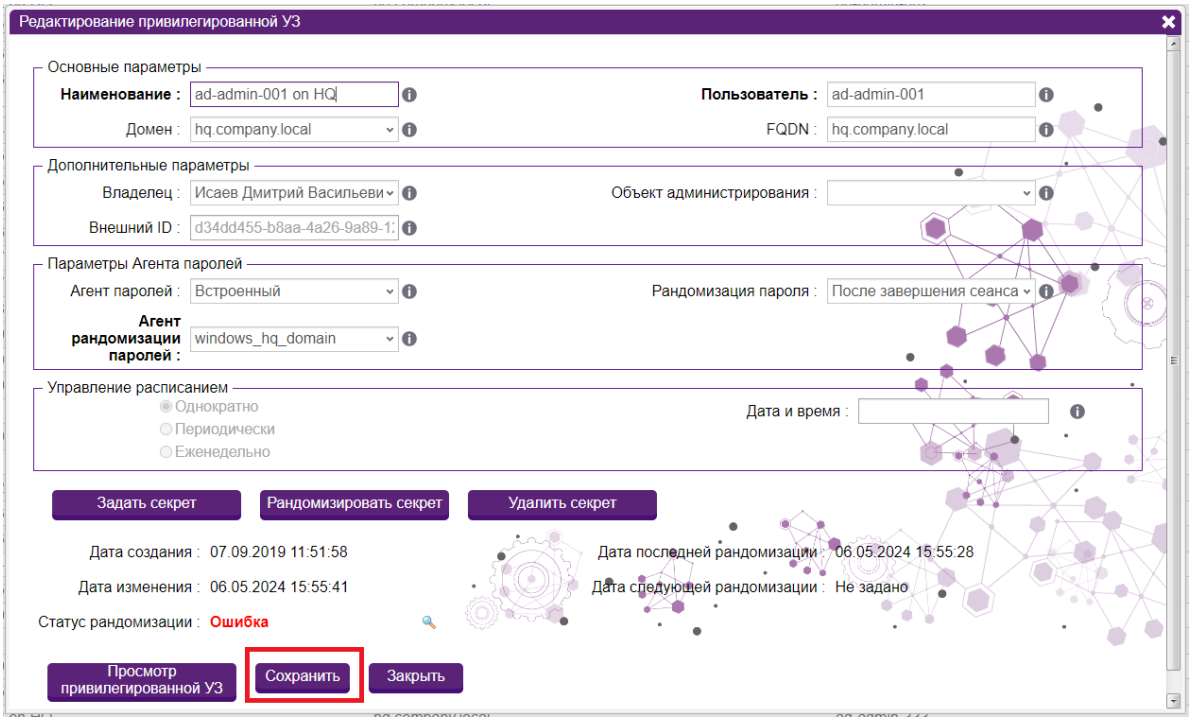


Рис. 3.3.4. Форма редактирования данных учетной записи

3.3.3 Обновление таблицы учетных записей

Для обновления записей в таблице пользователей необходимо перейти в узел **Привилегированные УЗ** раздела **Управление системой** и щелкнуть на значке обновления, расположенном в правой части панели инструментов.

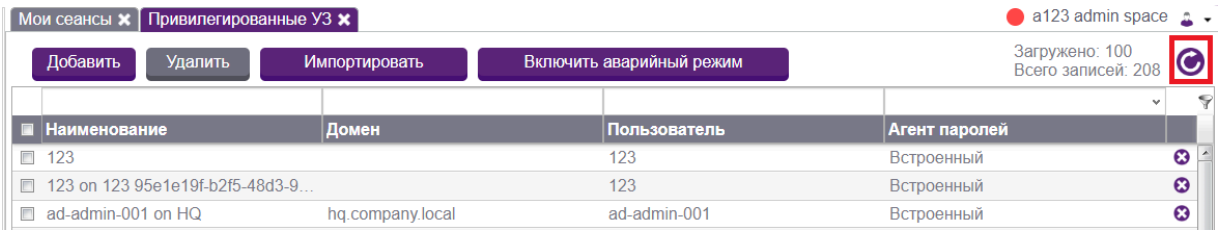


Рис. 3.3.5. Кнопка обновления таблицы учетных записей

3.3.4. Удаление ПУЗ в таблице

Для удаления строки в таблице пользователей необходимо перейти в узел **Привилегированные УЗ** раздела **Управление системой** и щелкнуть на кнопке удаления, расположенной в правой части строки учетной записи.

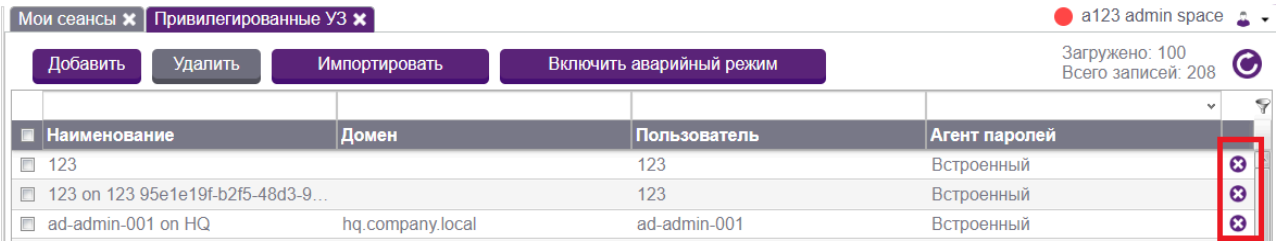


Рис. 3.3.6. Кнопка удаления учетной записи

3.3.5. Удаление нескольких записей из таблицы учетных записей одновременно

Для одновременного удаления нескольких записей необходимо перейти в узел **Привилегированные УЗ** раздела **Управление системой**, выделить нужные записи в таблице, установив флажок в соответствующем поле слева от поля **Наименование**, после чего станет активной кнопка **Удалить**, расположенная на панели инструментов.

3.3.6. Импортирование учетных записей из файла

Для импорта массива учетных записей необходимо нажать на кнопку **Импортировать** вверху таблицы.

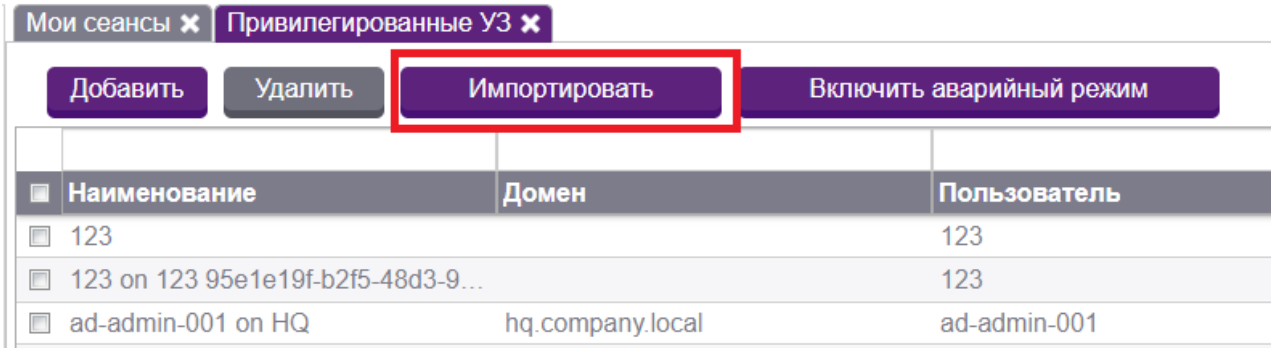


Рис. 3.3.7. Кнопка импорта учетных записей

Откроется окно, в котором необходимо выбрать .csv файл для импорта. Также можно указать параметры для добавляемых учетных записей, хотя это не является обязательным:

- Домен - домен, в котором будут находиться новые привилегированные УЗ.
- Владелец - пользователь, который будет владеть привилегированными УЗ.
- Объект администрирования - для которого будут использоваться привилегированные УЗ.

- Агент паролей - тот, что будет использоваться для создаваемых привилегированных УЗ. Если выбран "Встроенный" (он всегда выбран по умолчанию), то появится детальный выбор Агента рандомизации паролей. Для иных случаев будет выведено окно для ввода Строки интеграции (поле, специфичное для типа системы, с которой требуется интеграция).
- Рандомизация пароля - выбор момента относительно запуска сеанса, согласно которому будет производиться изменение пароля для привилегированных УЗ.
- Управление расписанием - выбор графика, когда будет генерироваться новый пароль для УЗ.
- Заменить существующие привилегированные УЗ - если УЗ с таким названием уже присутствуют в списке портала, то они будут заменены только что добавленными.

Подробнее об этих полях можно прочитать выше, в разделе добавление/редактирование привилегированных учетных записей.

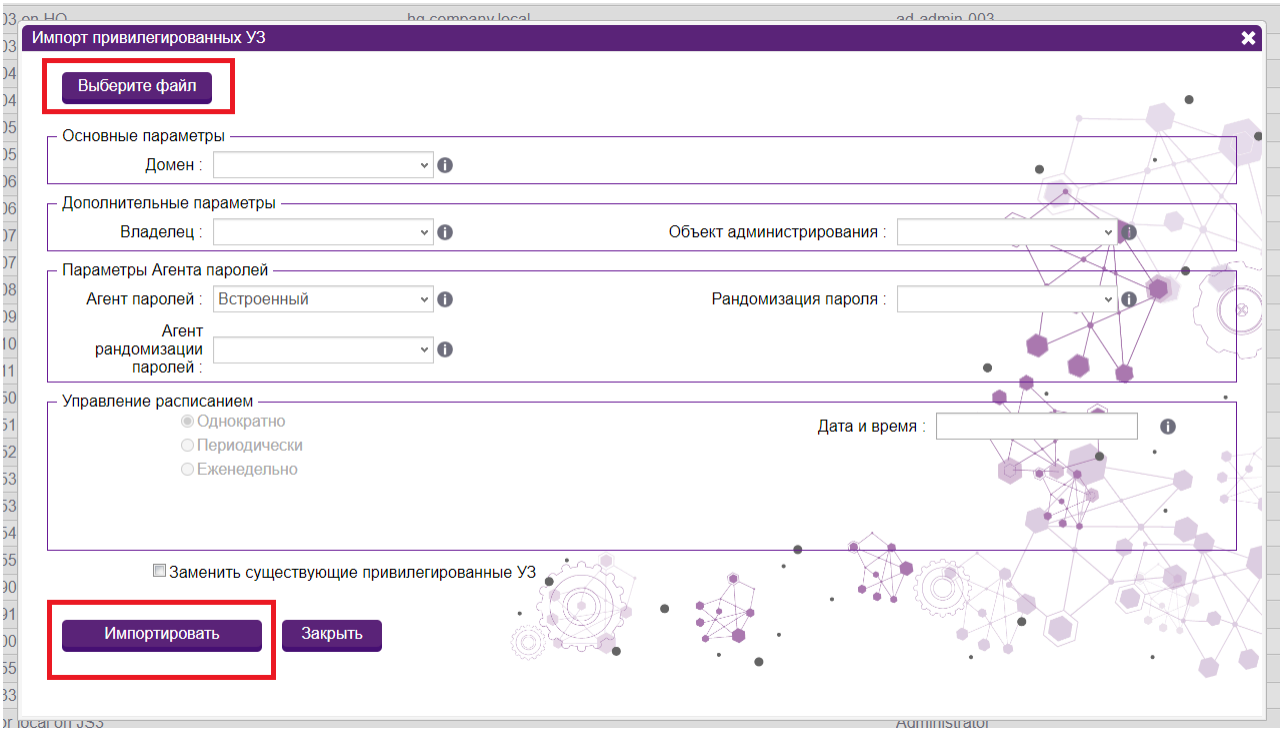


Рис. 3.3.8. Окно импорта учетных записей

Пример оформления .csv файла (через запятую должны быть перечислены Наименование ПУЗ, логин ПУЗ, Внешний ID, Пароль УЗ):

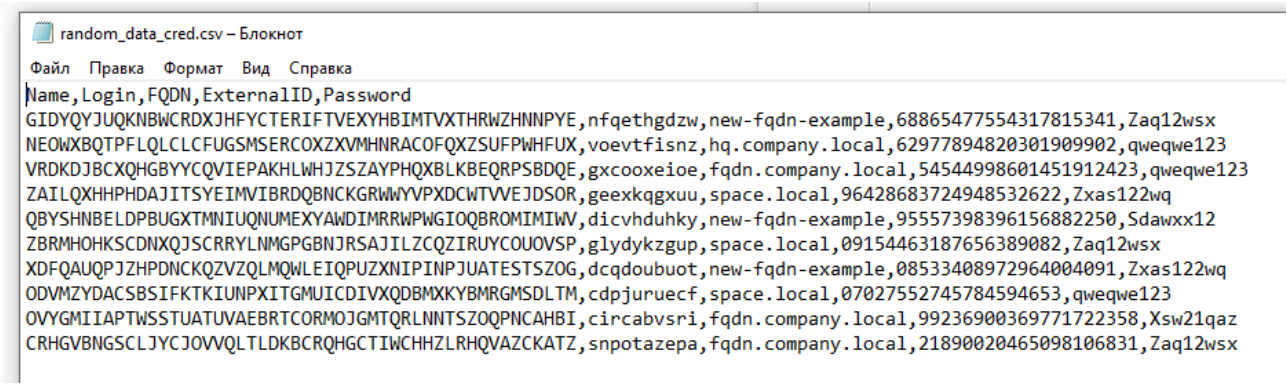


Рис. 3.3.9. Пример файла для импорта учетных записей

После загрузки .csv файла и выбора всех параметров нужно нажать на кнопку **Импортировать**. Появится уведомление о том, что УЗ импортированы, и они отобразятся в списке всех УЗ.

3.3.7. Включение и выключение аварийного режима

В случае чрезвычайных ситуаций привилегированный администратор системы с ролью ROLE_SPACE_SUPERADMIN) может включить аварийный режим системы. При этом все пользователи с активным НД узнают пароли ПУЗ в своих сеансах.

Для этого требуется нажать на кнопку **Включить аварийный режим** в разделе **Привилегированные УЗ**.

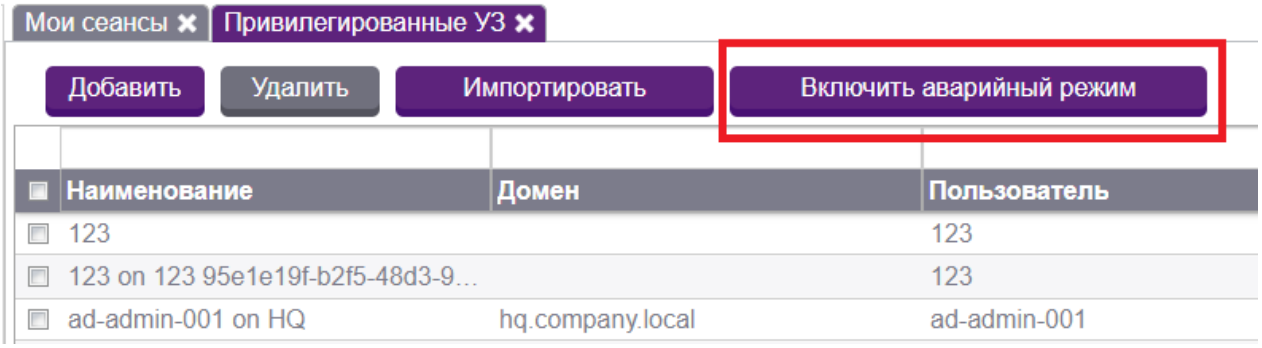


Рис. 3.3.10. Местонахождение кнопки включения аварийного режима

Примечание Для устранения возможного несанкционированного доступа после использования аварийного режима необходимо обратить внимание на следующее:

- параметр “рандомизация пароля” в карточках всех привилегированных записей Системы должен быть установлен на обновление пароля для каждого сеанса;
- привилегированный администратор может рандомизировать раскрытые пароли самостоятельно в ручном режиме.

3.4. Управление объектами администрирования

Управление объектами администрирования в рамках одного тенанта происходит в узле **Объекты администрирования** раздела **Управление системой**.

Объект администрирования — это объект защищенной среды, на который пользователь не может попасть напрямую, а только через сервер ЗСА.

Тип объекта администрирования — конкретная разновидность объекта администрирования, определяющая правила работы с объектом.

В окне **Объекты администрирования** отображаются две таблицы: **Список объектов** и **Список типов объектов администрирования**. В таблицах окна **Объекты администрирования** содержатся следующие поля:

- Объект администрирования – это объект защищенной среды, на который пользователь не может попасть напрямую, а только через сервер защищенной среды.
- Тип объекта администрирования – конкретная разновидность объекта администрирования, определяющая правила работы с объектом.
- FQDN – Fully Qualified Domain Name, имя домена, не имеющее неоднозначностей в определении. Включает в себя имена всех родительских доменов иерархии DNS.
- Имя – наименование типа объекта.
- Описание – описание типа объекта.

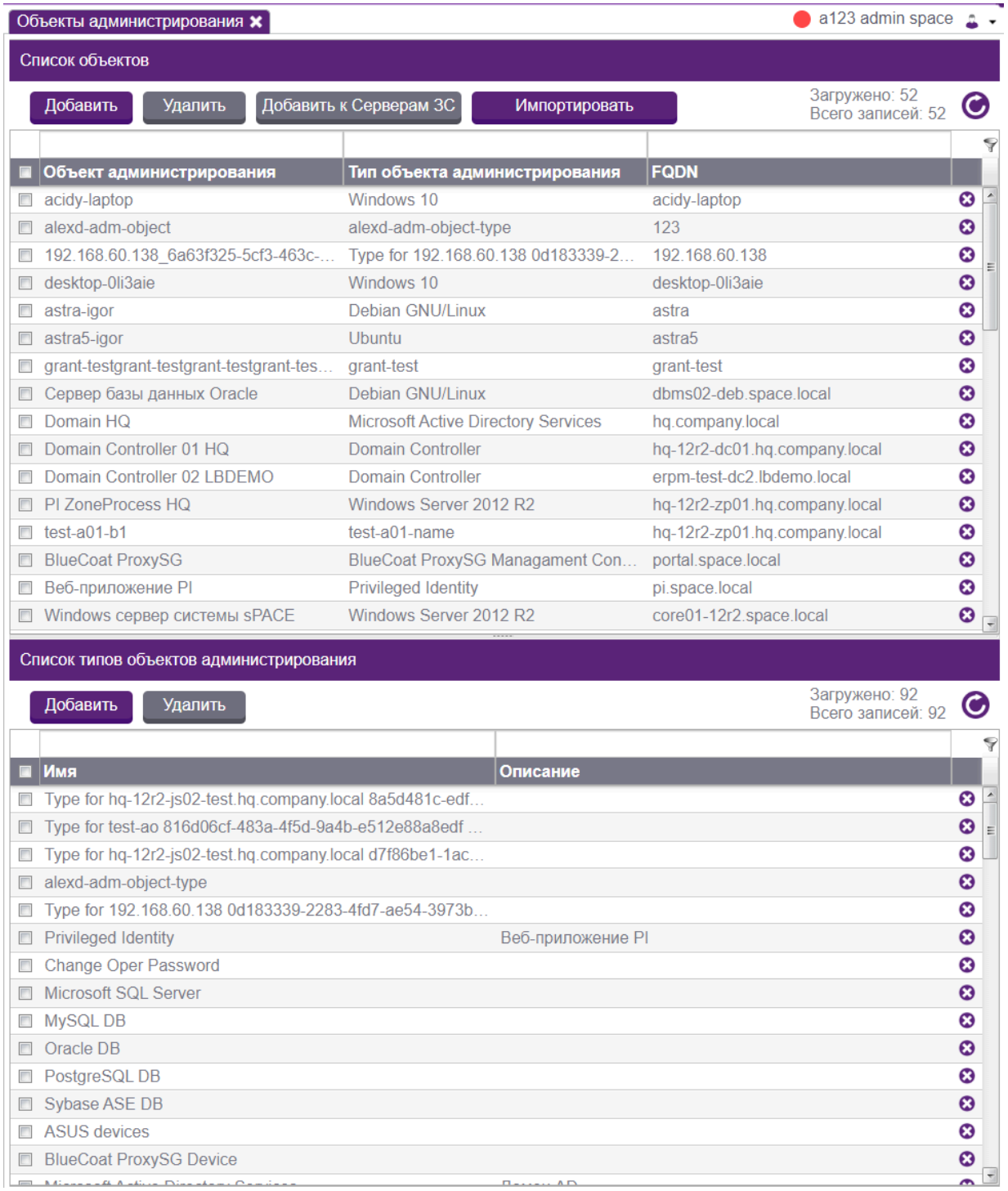


Рис. 3.4.1. Окно «Объекты администрирования»

В данном узле пользователи с соответствующими правами могут:

- Добавлять объект администрирования/тип объекта администрирования.
- Редактировать объект администрирования/тип объекта администрирования.
- Обновлять таблицу объекта администрирования/типа объекта администрирования.

- Удалять строки в таблице объекта администрирования/типа объекта администрирования.
- Удалять несколько записей из таблицы одновременно.
- Добавлять один или несколько объектов администрирования к определённому серверу защищённой среды.
- Импортировать объекты администрирования из файла.

3.4.1 Добавление объекта администрирования/типа объекта администрирования

Для добавления объекта администрирования необходимо перейти в узел **Объекты администрирования** и щелкнуть мышью на кнопке **Добавить** в таблице **Список объектов** окна **Объекты администрирования**.

На экране отобразится форма добавления объекта администрирования.

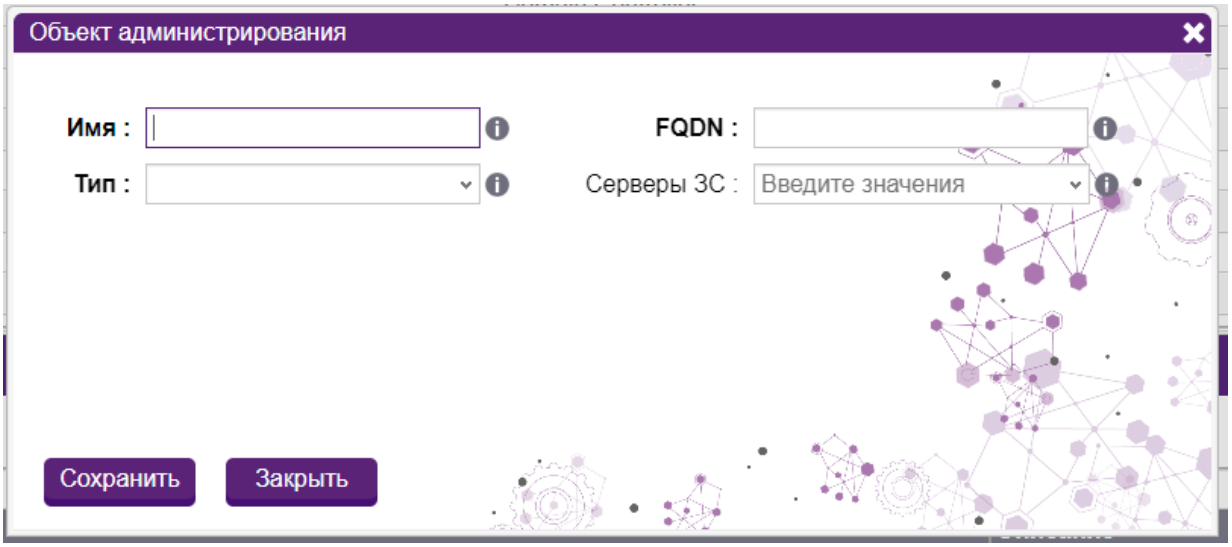


Рис. 3.4.2. Форма добавления объекта администрирования

Форма содержит следующие поля (поля, выделенные полужирным шрифтом, являются обязательными для заполнения):

- Имя (обязательное поле) – наименование объекта администрирования;
- Тип (обязательное поле) – тип объекта администрирования;
- FQDN (обязательное поле) – Fully Qualified Domain Name, имя домена, не имеющее неоднозначностей в определении. Включает в себя имена всех родительских доменов иерархии DNS;
- Серверы ЗС – наименование сервера ЗСА, через который осуществляется взаимодействие с объектом администрирования.

Для добавления типа объекта администрирования необходимо щелкнуть мышью на кнопке **Добавить** в таблице **Список типов объектов администрирования** окна **Объекты администрирования**.

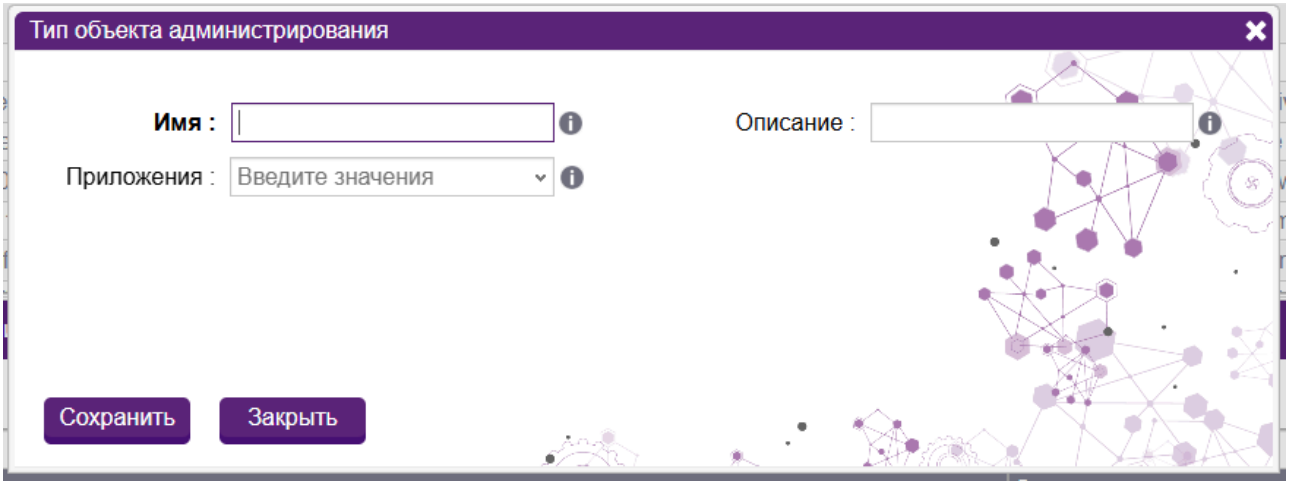


Рис. 3.4.3. Форма добавления типа объекта администрирования

На экране отобразится форма добавления типа объекта администрирования.

Форма содержит следующие поля (поля, выделенные полужирным шрифтом, являются обязательными для заполнения):

- **Имя (обязательное поле)** — имя объекта;
- Описание — описание объекта администрирования.
- Приложения — приложения, которые будут использоваться для администрирования этого типа ОА.

Редактирование объекта администрирования/типа объекта администрирования.

Для редактирования объекта администрирования необходимо дважды щелкнуть мышью на строке объекта в таблице **Список объектов**. В отобразившейся карточке объекта необходимо щелкнуть мышью на кнопке **Редактирование**.

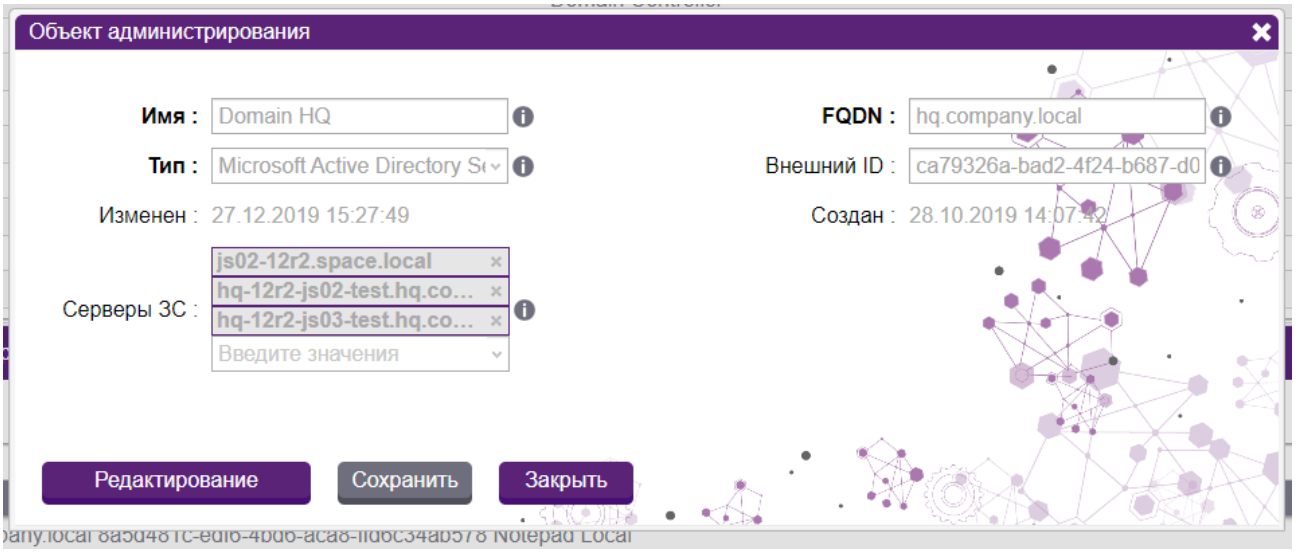


Рис. 3.4.5. Карточка объекта администрирования

Форма редактирования объекта администрирования содержит следующие поля:

- Имя (обязательное поле) – наименование объекта администрирования;
- Тип (обязательное поле) – тип объекта администрирования;
- FQDN (обязательное поле) – Fully Qualified Domain Name, имя домена, не имеющее неоднозначностей в определении. Включает в себя имена всех родительских доменов иерархии DNS;
- Внешний ID – уникальный идентификатор для интеграции внешних систем через API sPACE с данной сущностью;
- Серверы ЗС – наименование сервера ЗСА, через который осуществляется взаимодействие с объектом администрирования.

Все поля, кроме Внешнего ID, доступны для редактирования. Чтобы сохранить изменения, необходимо нажать кнопку **Сохранить**. При нажатии кнопки **Закрыть** изменения не сохранятся.

Для редактирования типа объекта администрирования необходимо дважды щелкнуть мышью на строке типа объекта в таблице **Список типов объектов**. В появившейся карточке объекта необходимо щелкнуть мышью на кнопке **Редактирование**.

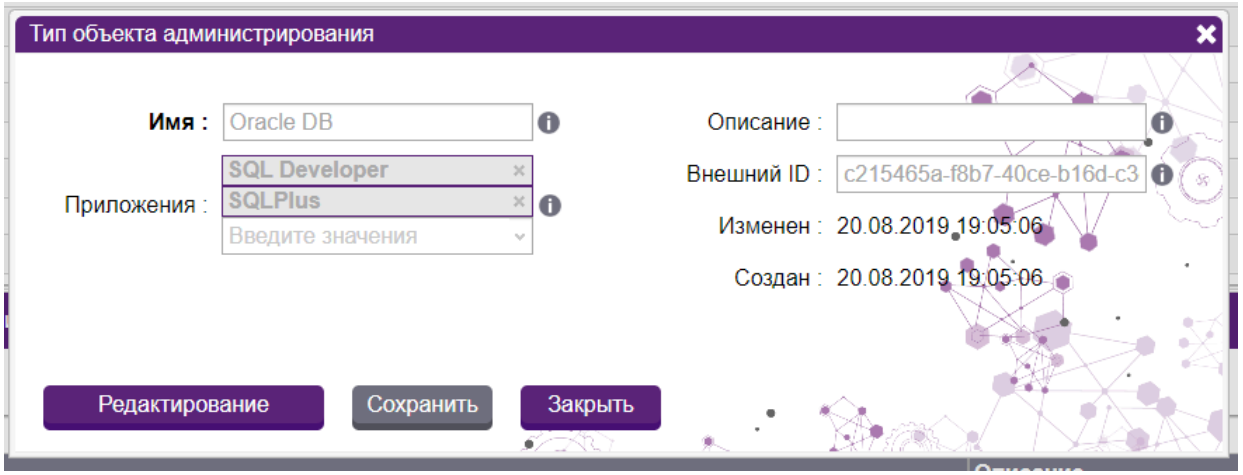


Рис. 3.4.6 Карточка типа объекта администрирования

Форма редактирования типа объекта администрирования содержит следующие поля:

- Имя (обязательное поле) – имя объекта;
- Описание – описание объекта администрирования.
- Приложения — наименование программного обеспечения с написанным сценарием запуска в sPACE, которое будет использоваться для администрирования этого типа ОА.
- Внешний ID – Внешний ID: уникальный идентификатор для интеграции внешних систем через API sPACE с данной сущностью;

Все поля, кроме Внешнего ID, доступны для редактирования. Чтобы сохранить изменения, необходимо нажать кнопку **Сохранить**. При щелчке на кнопке **Закрыть** никаких изменений в карточке типа объекта администрирования не произойдет.

3.4.2. Обновление таблицы объекта администрирования/типа объекта администрирования

Для обновления записей в таблицах необходимо перейти в узел **Объекты администрирования** раздела **Управление системой** и щелкнуть мышью на кнопке обновления в правой верхней части таблиц. Обновление таблицы типов объектов администрирования происходит аналогичным способом.

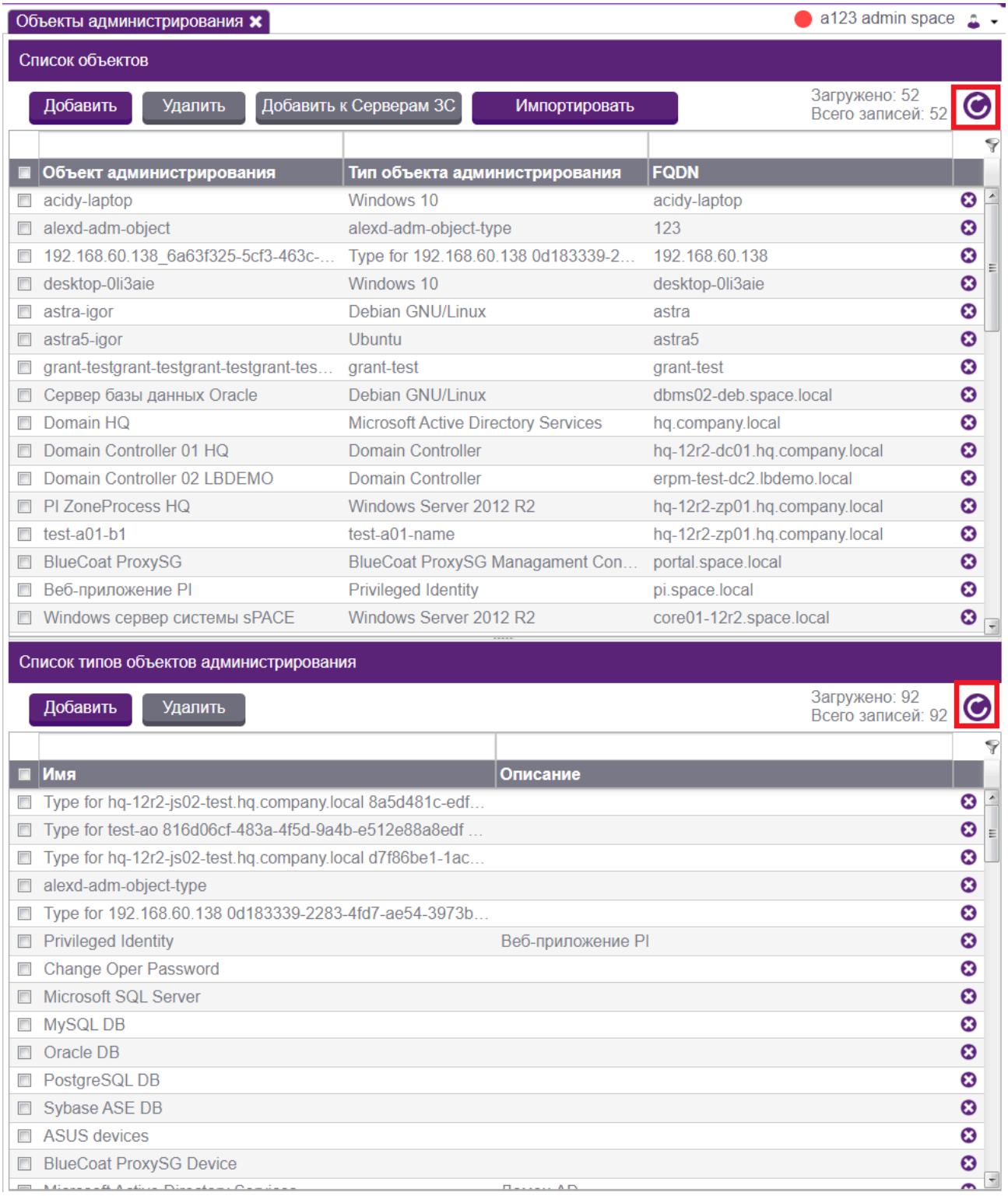


Рис. 3.4.7. Кнопка обновления записей таблицы

3.4.3. Удаление в таблице объекта администрирования/типа объекта администрирования

Для удаления строки в таблице объекта администрирования необходимо щелкнуть мышью на кнопке удаления, располагающейся справа в строке объекта администрирования. Удаление из таблицы типов объектов администрирования происходит аналогичным способом.

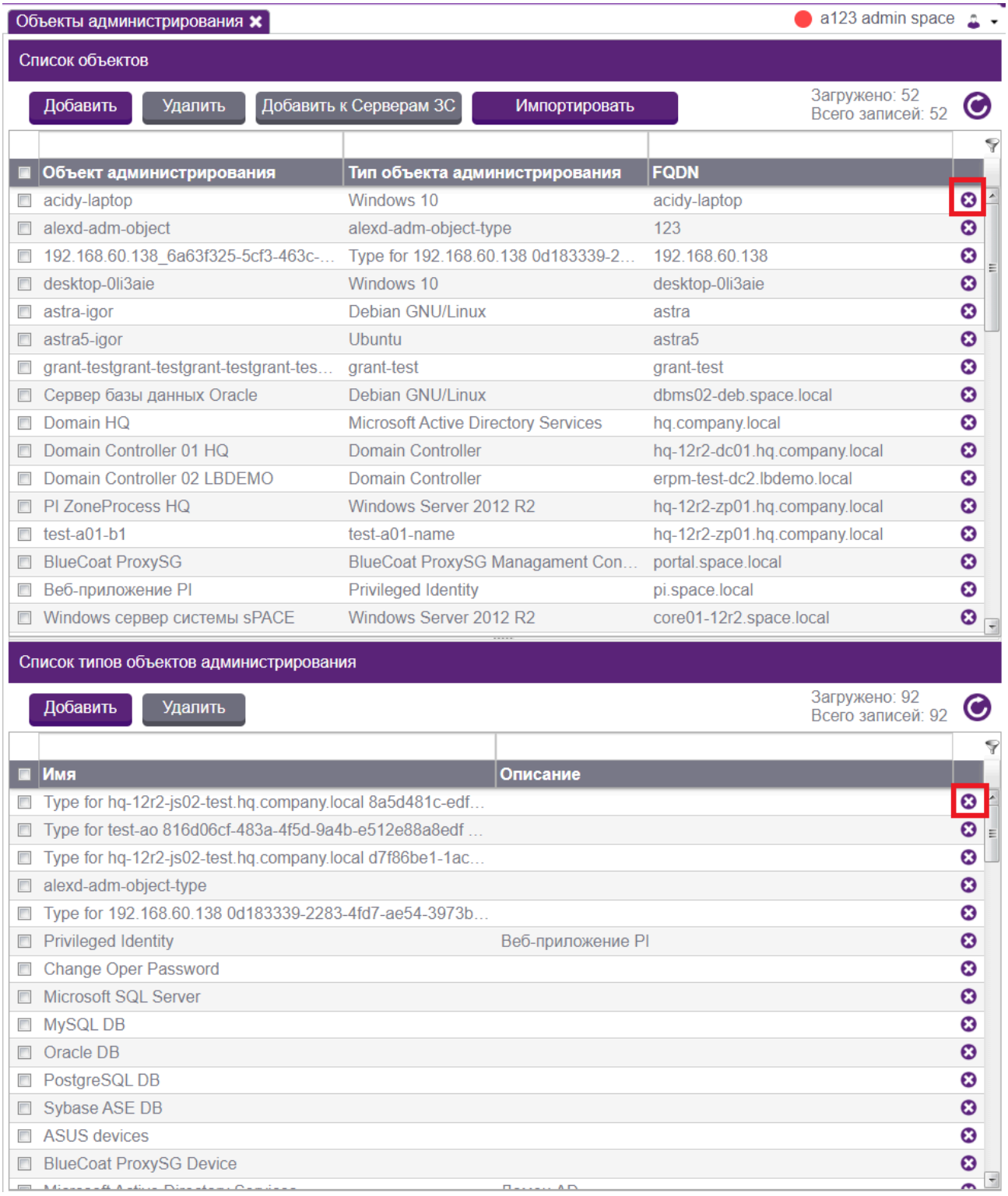


Рис. 3.4.8. Кнопка удаления строки

3.4.4. Удаление нескольких записей из таблицы одновременно

Для удаления нескольких записей одновременно необходимо сначала выделить желаемые записи в таблице, установив флажок в соответствующем поле слева от поля **Объект администрирования**, после чего станет активной кнопка

Удалить, расположенная на панели инструментов. Удаление нескольких строк из таблицы типов объектов администрирования происходит аналогичным способом.

3.4.5. Одновременное добавление серверов ЗС для нескольких объектов администрирования

Для одновременного добавление серверов ЗС для нескольких ОА сначала следует выделить желаемые записи в таблице галочкой слева, после чего станет активной кнопка **Добавить к Серверам ЗС**, расположенная сверху над таблицей. После нажатия на данную кнопку необходимо будет выбрать сервера ЗС из списка доступных.

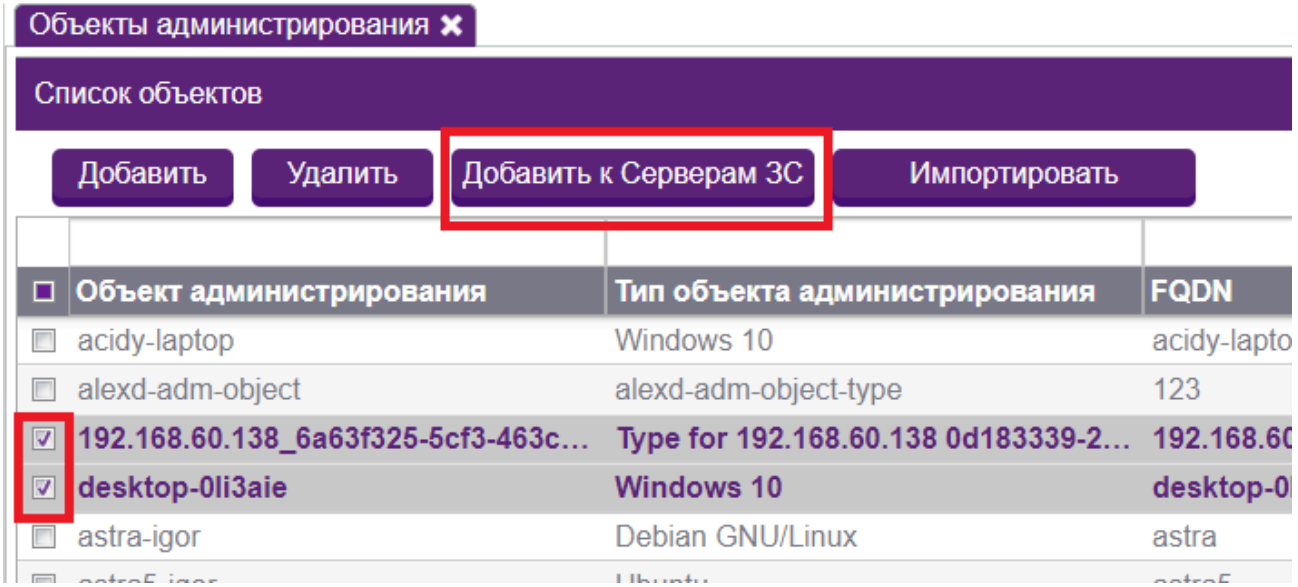


Рис. 3.4.9. Кнопка для добавления к серверам ЗС

3.4.5. Импортирование объектов администрирования из файла

Для импорта массива объектов администрирования необходимо нажать на кнопку "Импортировать" вверху таблицы.

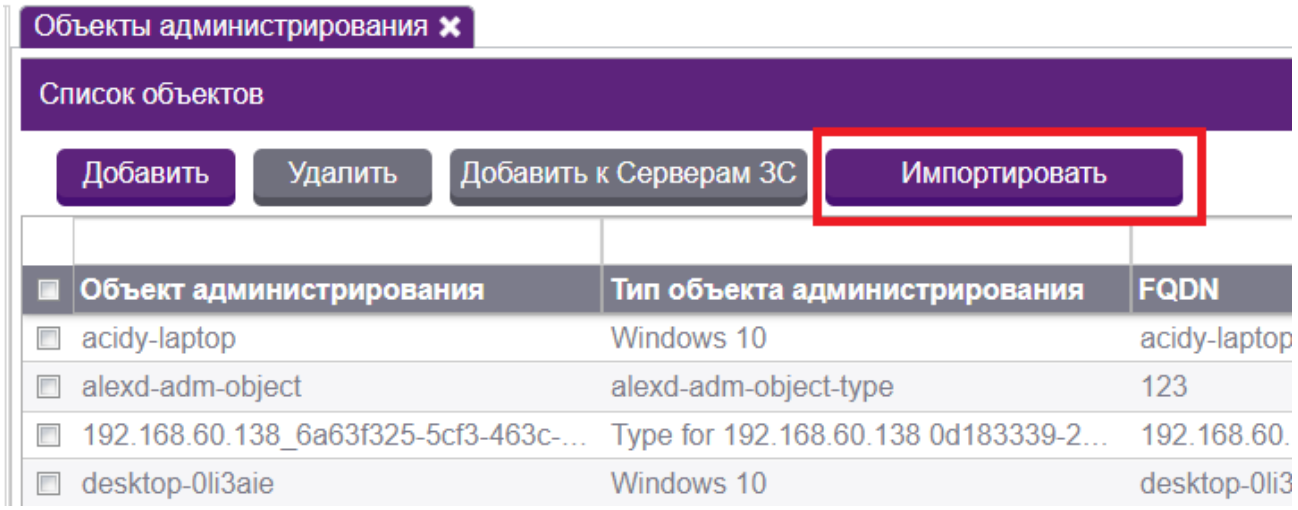


Рис. 3.4.10. Кнопка для добавления к серверам ЗС

Откроется окно, в котором необходимо выбрать .csv файл для импорта.

Также нужно указать параметры для добавляемых объектов администрирования:

- Серверы ЗС — к которым будут привязаны импортированные объекты администрирования
- Тип (обязательное поле) — тип, к которому относятся импортированные объекты.
- Заменить существующие объекты администрирования — если ОА с таким названием уже присутствуют в списке портала, то они будут заменены только что добавленными.

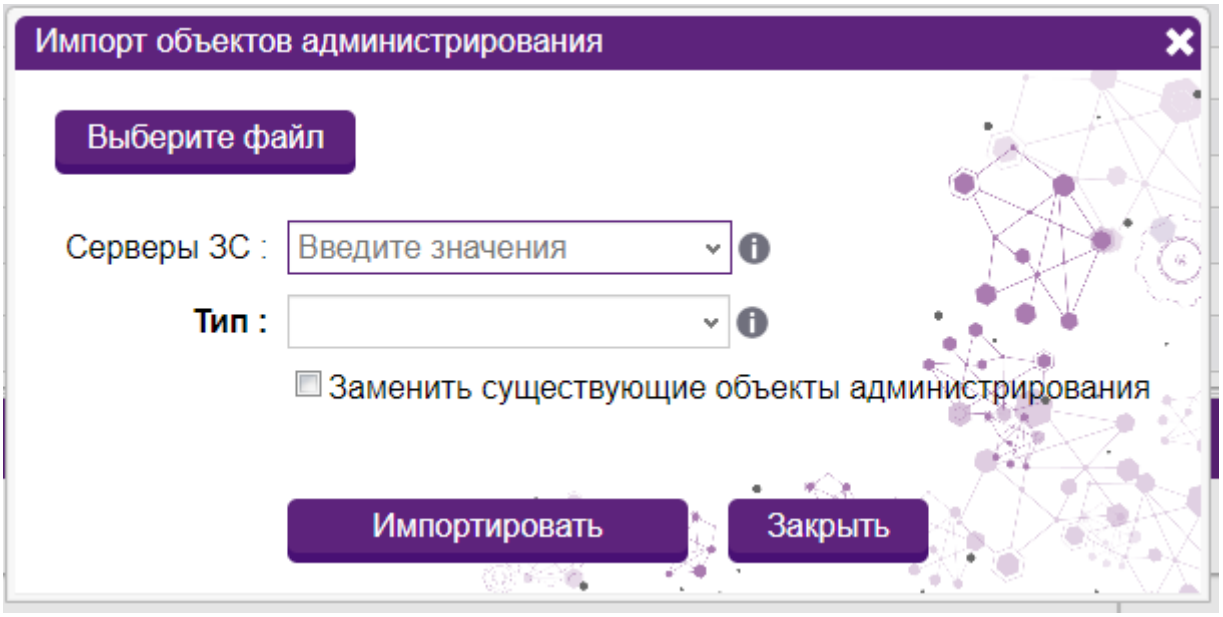


Рис. 3.4.11. Кнопка для добавления к серверам ЗС

Пример оформления .csv файла (через запятую после названия ОА надо указать FQDN):

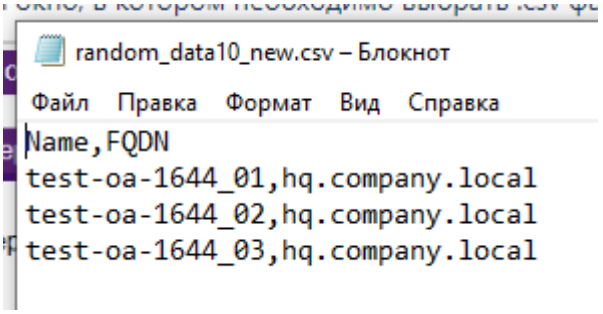


Рис. 3.4.12 Пример файла

После загрузки .csv файла и выбора всех параметров нужно нажать на кнопку **Импортировать**. Появится уведомление о том, что ОА импортированы, и после

обновления таблицы при помощи кнопки **Обновить** вверху справа они отобразятся в списке всех ОА.

3.5. Управление задачами администрирования

Работа sPACE основана на принципе минимальных привилегий, когда доступ к объектам администрирования предоставляется пользователям исключительно для выполнения задачи, к которой согласован наряд-допуск. Для выбора пользователями задач администрирования необходимо предварительно добавить их в Систему. Настройка и управление задачами на администрирование объектами осуществляет в узле **Задачи** раздела **Управление системой**.

Окно **Задачи** содержит таблицу с тремя столбцами: **Задача**, **Объекты администрирования**, **Учетные записи** и **Согласующие**:

- Задача – наименование задачи;
- Объекты администрирования – объекты защищенной среды в рамках данной задачи;
- Кол-во привилегированных УЗ - количество учетных записей, которым разрешена работа в рамках данной задачи;
- Согласующие – группа пользователей, имеющие право на согласование данной задачи.

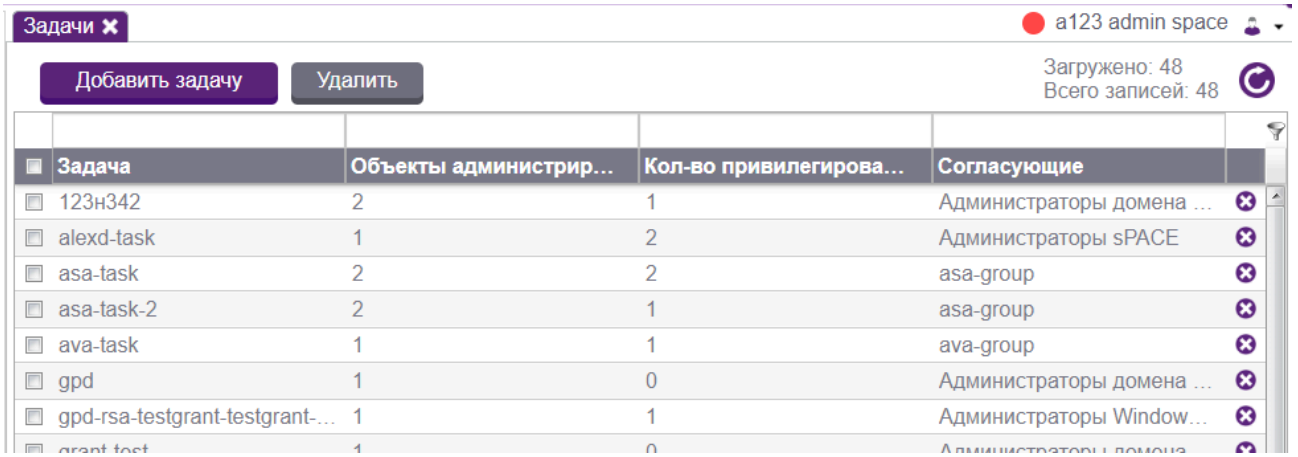


Рис. 3.5.1. Окно узла «Задачи»

В данном узле администраторы могут:

- Добавлять задачу;
- Редактировать задачу;
- Обновлять таблицу задач;

- Удалять строку в таблице задач;
- Удалять несколько записей из таблицы задач одновременно.

3.5.1. Добавление задачи

Для добавления задачи необходимо щелкнуть мышью на кнопке **Добавить задачу** на панели инструментов узла **Задачи**. На экране отобразится форма добавления задачи.

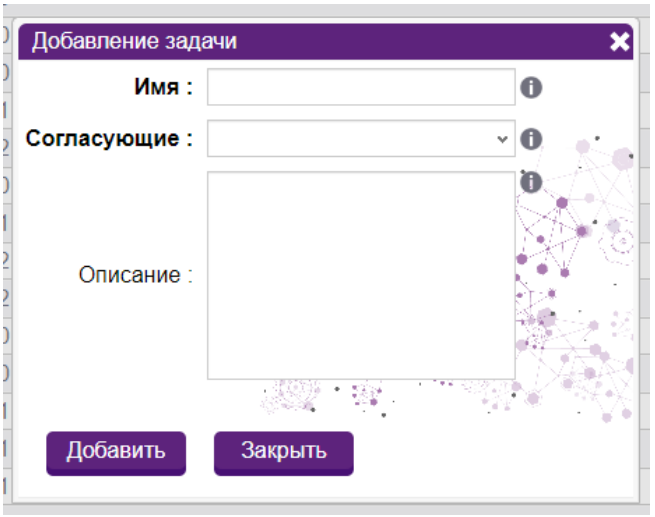


Рис. 3.5.2. Форма добавления задачи

Форма **Добавление задачи** содержит следующие поля (поля, обязательные для заполнения, выделены полужирным шрифтом):

- Имя (обязательное поле) – наименование задачи;
- Согласующие (обязательное поле) – пользователи, имеющие право согласовать данную задачу;
- Описание – описание задачи;

После добавления задачи нужно добавить в нее привилегированные учетные записи и объекты администрирования. Это делается через меню редактирования.

3.5.2 Редактирование задачи

Для редактирования задачи необходимо дважды щелкнуть на строку задачи в таблице задач. В появившейся карточке задачи отображается вся информация о задаче.

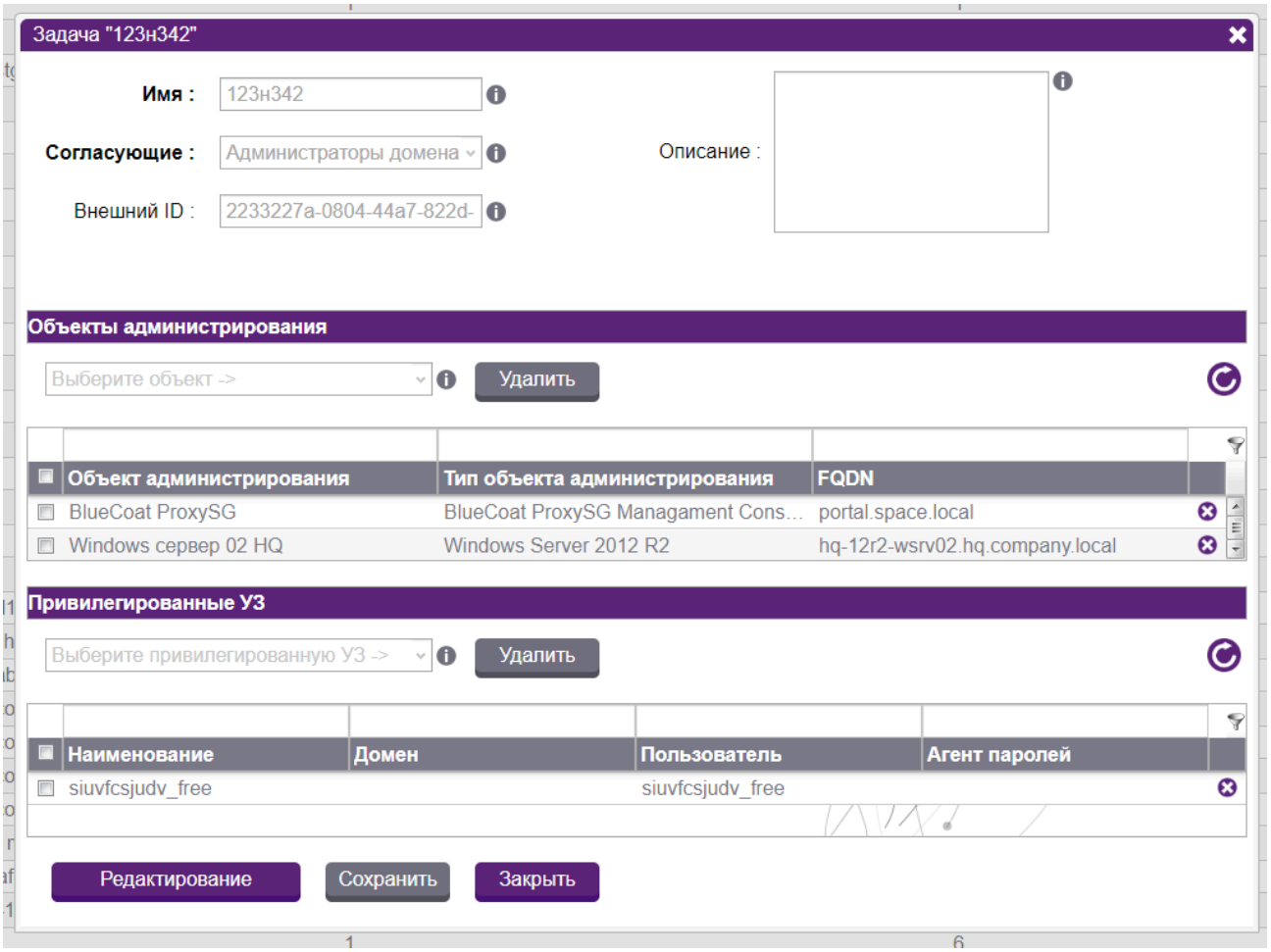


Рис. 3.5.3. Карточка задачи

После щелчка на кнопке **Редактирование** на экран выводится форма редактирования задачи, в которой все поля, кроме Внешнего ID, доступны для редактирования. Чтобы сохранить изменения, необходимо нажать кнопку **Сохранить**. При нажатии кнопки **Закрыть** никаких изменений в карточке пользователя не произойдет.

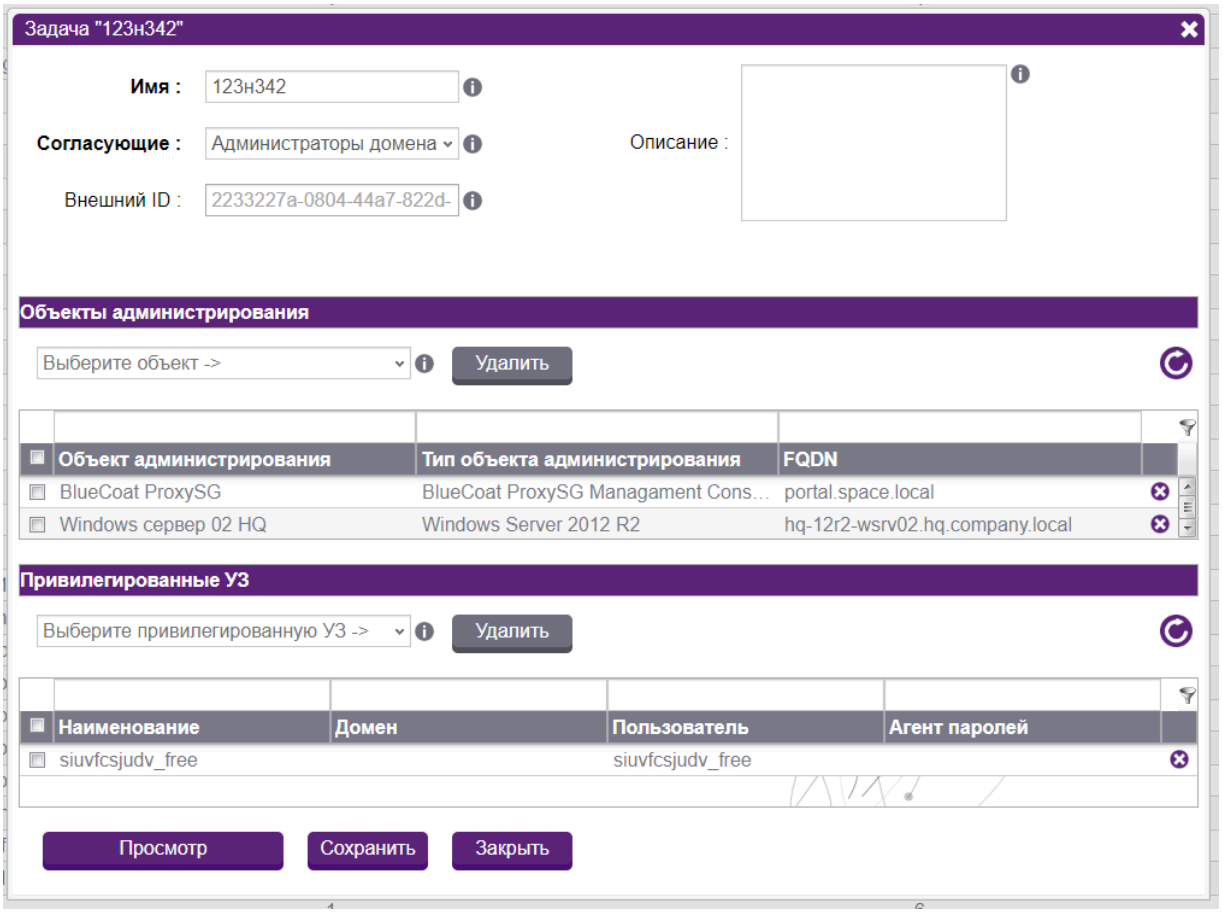


Рис. 3.5.4. Форма редактирования задачи

3.5.3. Обновление таблицы задач

Для обновления записей в таблице задач необходимо щелкнуть мышью на кнопке обновления , расположенной на панели инструментов справа.

3.5.4. Удаление строки в таблице задач

Для удаления строки из таблицы задач щелкните мышью на кнопке удаления в правой части строки записи.

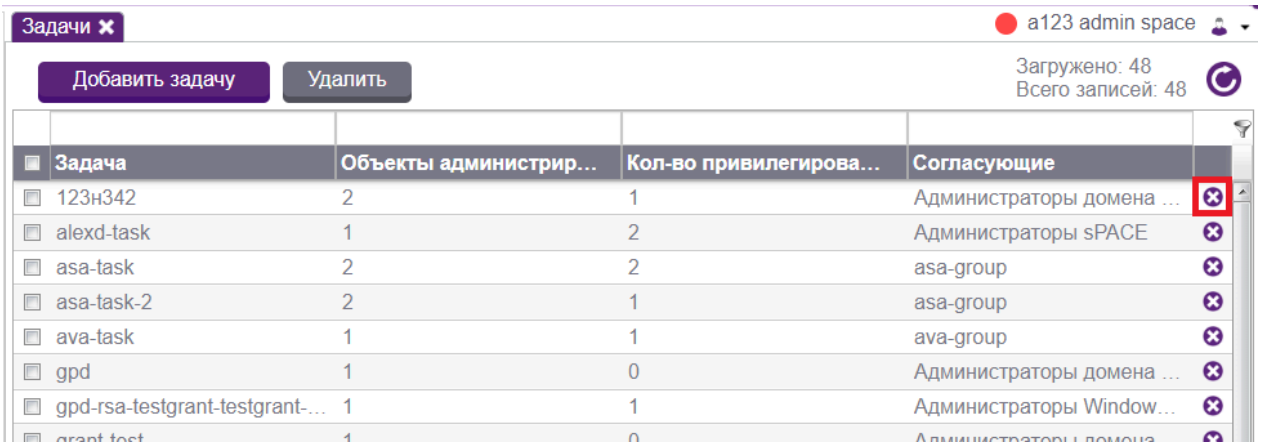


Рис. 3.5.5. Кнопка удаления

3.5.5. Удаление нескольких записей из таблицы задач одновременно

Для удаления нескольких записей из таблицы задач одновременно необходимо сначала выделить необходимые записи в таблице, установив флажок в соответствующем поле слева от поля **Задача**, после чего станет активной кнопка **Удалить** на панели инструментов.

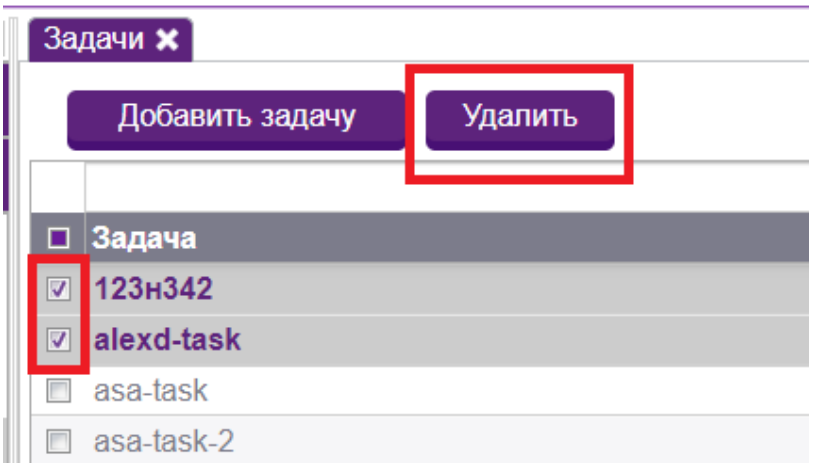


Рис. 3.5.6. Выбраны две записи таблицы. Кнопка «Удалить» активна

3.6. Настройка и управление нарядами-допусками

Доступ к объектам администрирования осуществляется на основании наряда-допуска. Наряд-допуск (НД) – это задание на выполнение определенной задачи в рамках Системы, в котором содержится название задачи, срок действия наряда-допуска, инициирующее и согласующее лицо, основание и объекты администрирования.

Все наряды-допуски, имеющиеся в Системе, отображаются в узле **Наряды-допуски** в виде таблицы с 6 столбцами:

- Наряд-допуск – номер наряда-допуска с датой создания;
- Пользователь – пользователь, запросивший данный наряд-допуск;
- Статус – статус наряда-допуска;
- Задача – задача, осуществляемая в рамках данного наряда-допуска;
- Дата согласования – дата, когда данный наряд-допуск был согласован;
- Действителен до – срок окончания действия наряда-допуска.

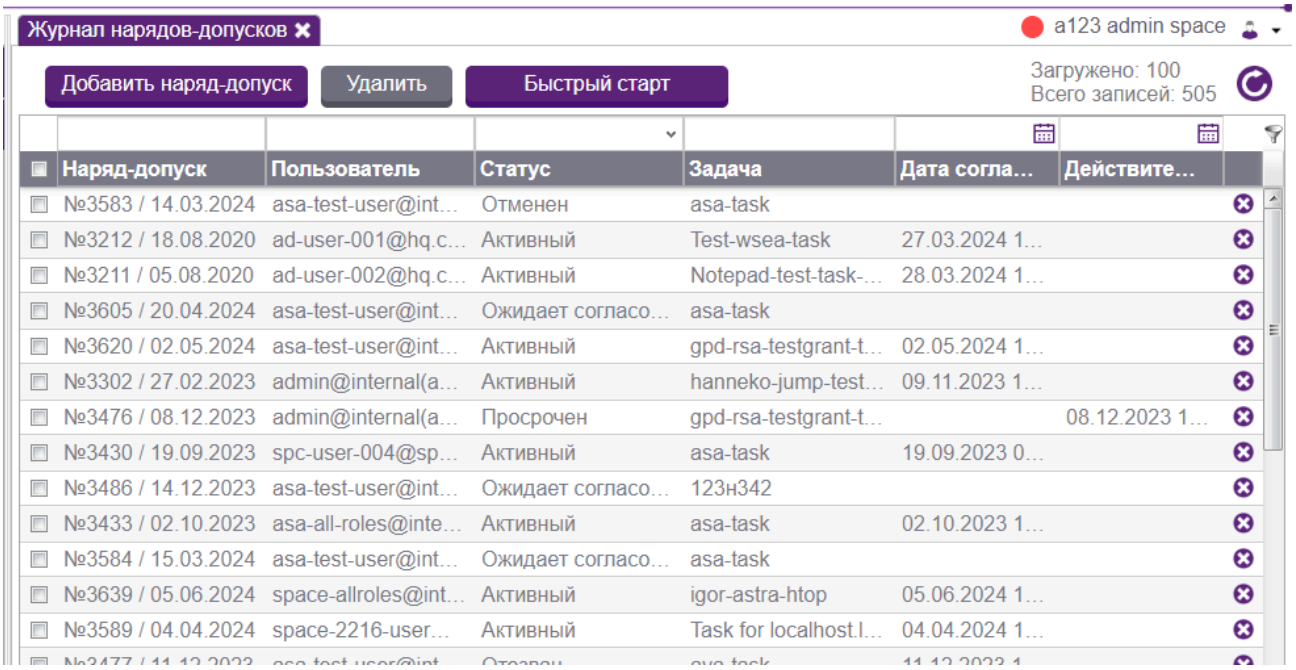


Рис. 3.6.1. Окно узла «Наряды-допуски

В рамках настройки и управления нарядами-допусками администраторы и продвинутые пользователи могут выполнять следующие действия:

- добавлять наряды-допуски;
- просматривать информацию о нарядах-допусках;
- обновлять таблицу нарядов-допусков;
- удалять строки в таблице нарядов-допусков;
- удалять несколько записей из таблицы нарядов-допусков одновременно;

3.6.1. Добавление наряда-допуска

Для добавления наряда-допуска необходимо щелкнуть на кнопке **Добавить наряд-допуск** на панели инструментов. В появившемся окне необходимо заполнить поля, выделенные полужирным шрифтом. Если пользователь находится в группе согласования для данной задачи, то будет активна кнопке **Согласовать**. Подробно о полях можно прочитать в Руководстве пользователя или в справке на портале.

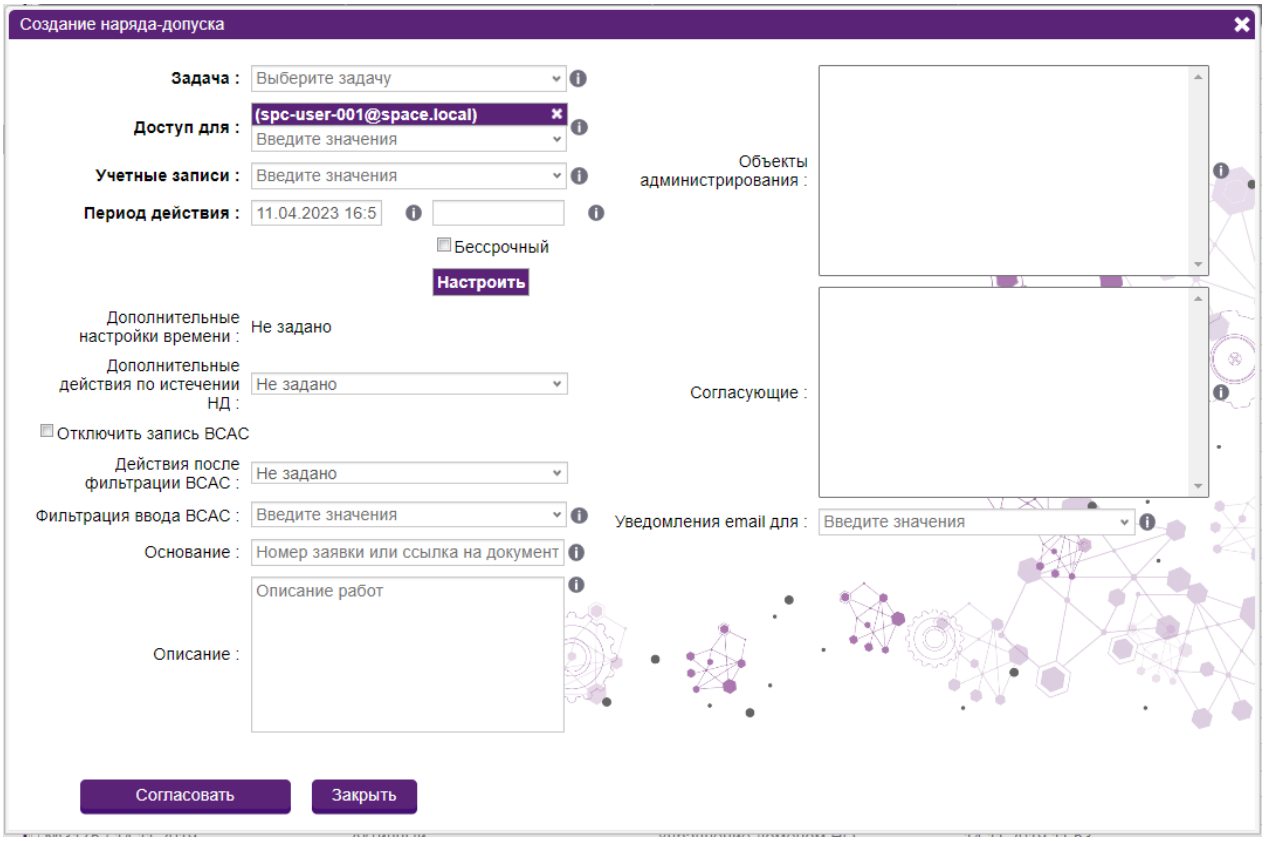


Рис. 3.6.2. Форма создания наряда-допуска

3.6.2. Просмотр информации о нарядах-допусках

Для просмотра информации о конкретном наряде-допуске следует дважды щелкнуть левой кнопкой мыши на строку данного наряда-допуска в таблице. Если пользователь находится в группе согласования для данного наряда-допуска, и наряд-допуск находится в состоянии "ожидает согласования", то будет активна кнопка **Согласовать** или **Отклонить**.

Для уже согласованного и активного наряда-допуска в случае наличия соответствующих прав будет активна кнопка **Отозвать**. Отозванные наряды-допуски можно просмотреть без возможности редактирования.

3.6.3. Обновление таблицы нарядов-допусков

Для обновления записей в таблице нарядов-допусков необходимо щелкнуть мышью на кнопке обновления , располагающейся в правой верхней части таблицы.

3.6.4. Удаление строк в таблице нарядов-допусков

Для удаления строки в таблице нарядов-допусков необходимо щелкнуть на кнопке удаления, расположенную справа в строке записи нарядов-допусков.

3.6.5. Удаление нескольких записей из таблицы нарядов-допусков

Для удаления нескольких записей из таблицы нарядов-допусков одновременно необходимо выделить желаемые записи в таблице, установив флажок в соответствующем поле слева от поля **Наряд-допуск**, после чего станет активной кнопка **Удалить**, расположенная сверху над таблицей.

3.7. Управление Доменами

Вкладка **Домены** раздела **Управление системой** позволяет осуществлять ряд действий для настройки доменов системы. В рамках Системы реализованы следующие возможности, доступные администратору:

- Просмотр доменов Системы;
- Добавление нового домена;
- Редактирование домена;
- Удаление домена;
- Обновление таблицы доменов;
- Управление пользователями LDAP.

Внешне раздел **Домены** представлен в виде таблицы.

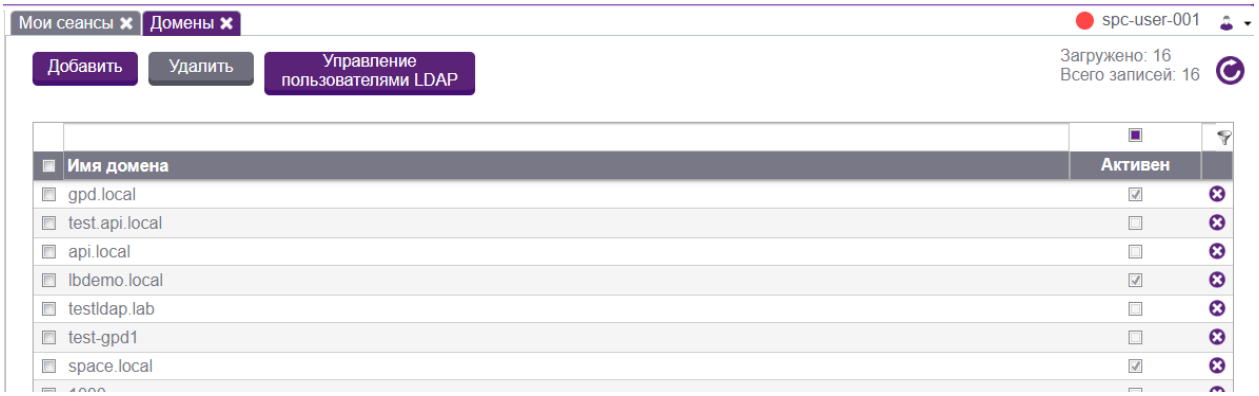


Рис. 3.7.1. Раздел «Домены»

3.7.1. Просмотр доменов Системы

Страница «Домены» представлена в виде одной таблицы. Описание столбцов приведено ниже:

- Имя домена – идентификатор домена;
- Активен – является ли этот домен активным.

3.7.2. Добавление нового домена

Функционал добавления домена вызывается нажатием на кнопку **Добавить**, расположенную в верхней части таблицы.

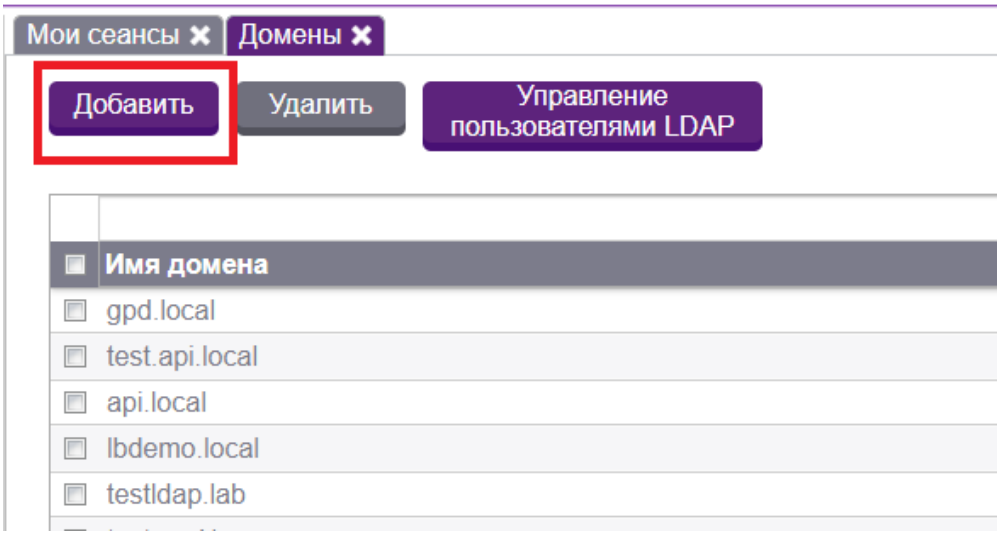


Рис. 3.7.2. Кнопка «Добавить домен»

При нажатии на эту кнопку пользователю будет выведена форма добавления домена, она состоит из одного обязательного поля с наименованием домена. После ввода нужного имени требуется нажать на кнопку "Сохранить".

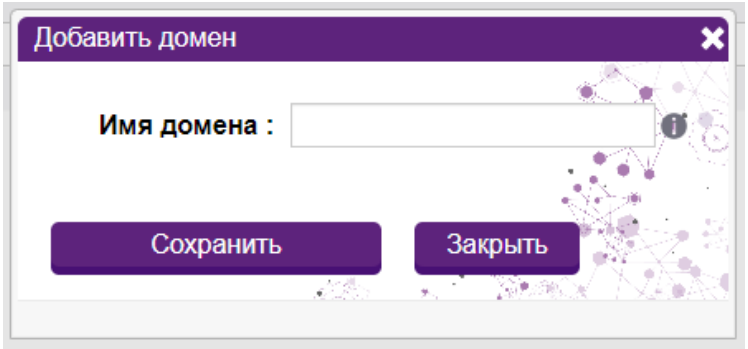


Рис. 3.7.3. Добавление домена

3.7.3. Редактирование домена

Функционал редактирования домена вызывается при двойном щелчке на наименовании домена в таблице.

Будет выведено окно с информацией о домене и активной кнопкой **Редактирование**. После нажатия на эту кнопку поля станут доступны для редактирования. Также необходимо отредактировать расширенные настройки домена, для этого требуется нажать на соответствующую кнопку "Расширенные настройки".

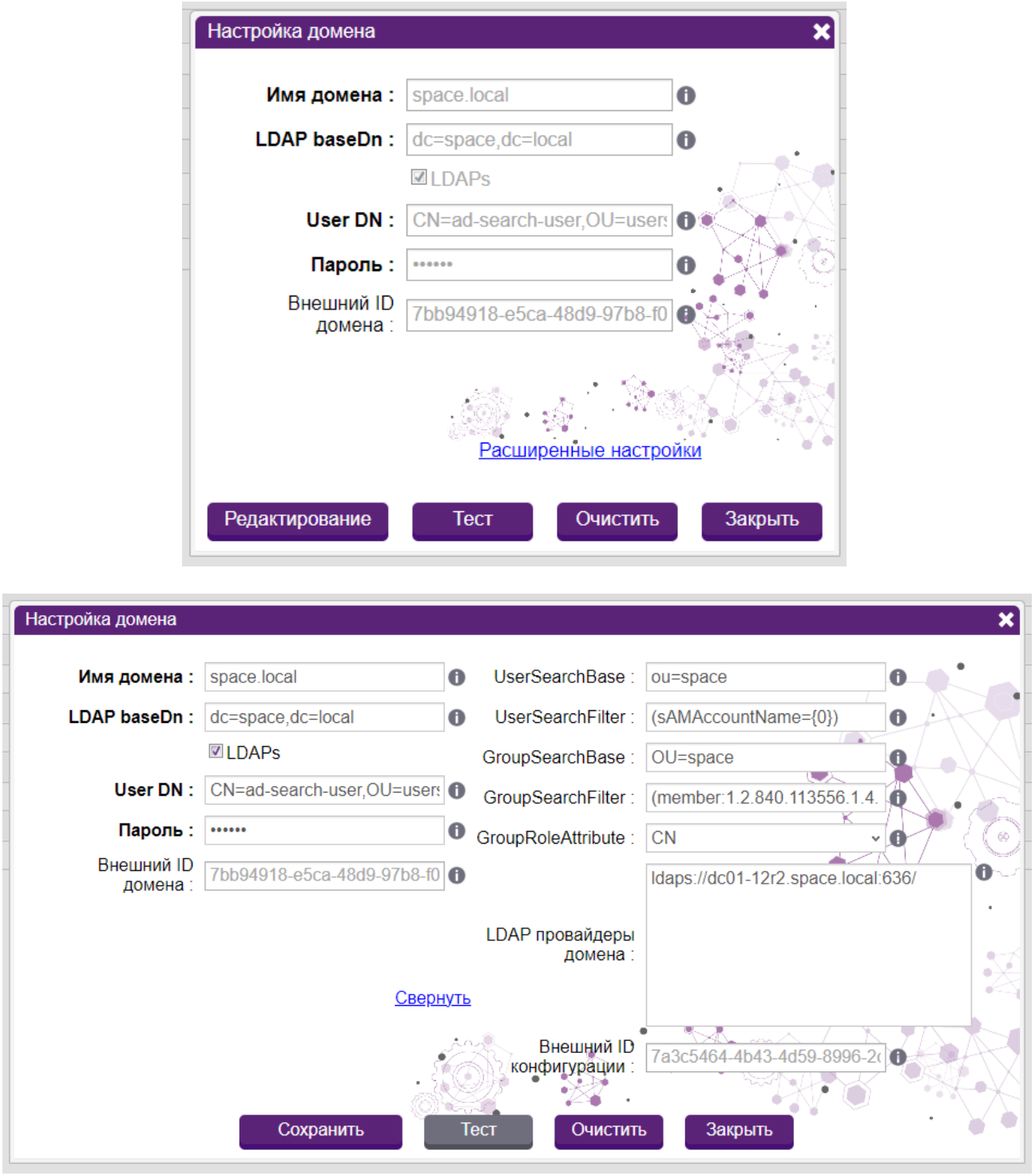


Рис. 3.7.4. Окно редактирования домена и окно расширенных настроек

Все поля доступны для редактирования. Поля, выделенные жирным, являются обязательными для заполнения. Для настройки подключения к домену (Microsoft AD или другой LDAP каталог) потребуется учетная запись, у которой совпадают поля CN и PN, (пример на рис. 3.7.5).

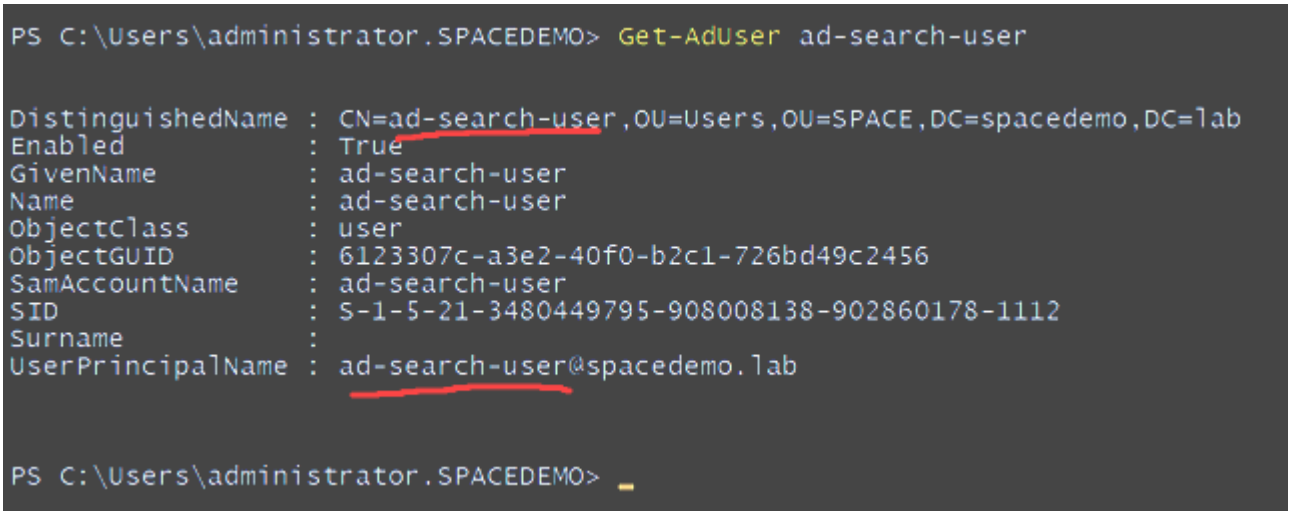


Рис. 3.7.5. Пример проверки на идентичность CN и PN

В расширенных настройках строки **UserSearchBase** и **GroupSearchBase** изначально пустые. Если их не заполнить - поиск будет осуществляться по всему домену. Зону поиска можно ограничить, указав в данных полях OU, соответствующую расположению используемых групп и пользователей.

В строке **UserSearchFilter** присутствует плейсхолдер {0}, он используется для того, чтобы заменять нужный параметр на имя каждого пользователя, для которого осуществляется поиск. Поля **UserSearchFilter** и **GroupSearchFilter** заполняются данными автоматически, их не рекомендуется изменять вручную или стирать во избежание ошибки подключения "Error: Empty filter".

Чтобы сохранить изменения, необходимо нажать кнопку **Сохранить**. При нажатии кнопки **Закрыть** никаких изменений в карточке домена не произойдет. Нажатие на кнопку **Тест** позволяет узнать, являются ли введённые данные верными. Если все правильно, то после такой проверки статус домена будет «Активен». В случае обнаружения ошибок домен будет переведён в неактивные, а результат теста укажет, в чем заключается обнаруженная ошибка. Комментарии к распространенным ошибкам можно найти на портале https://webcontrol.aspro.cloud/hc/3 в разделе «**Ошибки при подключении домена**».

Кнопка **Очистить** позволяет автоматически очистить все поля данного окна.

3.7.4. Обновление таблицы доменов

Для обновления записей в таблице доменов необходимо щелкнуть мышью на кнопке обновления , расположенной в правой верхней части таблицы.

3.7.5. Удаление строки в таблице доменов

Для удаления строки в таблице доменов необходимо щелкнуть на кнопке удаления, расположенной справа в строке доменов.

3.7.6. Удаление нескольких записей из таблицы доменов одновременно

Для удаления нескольких записей из таблицы доменов одновременно необходимо сначала выделить нужные записи в таблице, установив флажок в соответствующем поле слева от поля **Имя**, после чего станет активной кнопка **Удалить**, расположенная сверху над таблицей.

3.7.7. Управление пользователями LDAP

Пользователи LDAP - это тип пользователей, которые могут с одним и тем же логином и паролем авторизовываться как на портале sPACE, так и для выполнения сеансов на Сервере 3С Linux.

Для того, чтобы открыть панель управления пользователями LDAP, необходимо нажать на соответствующую кнопку над таблицей доменов. В данный момент Управление пользователями LDAP доступно только пользователям с ролью Технический администратор.

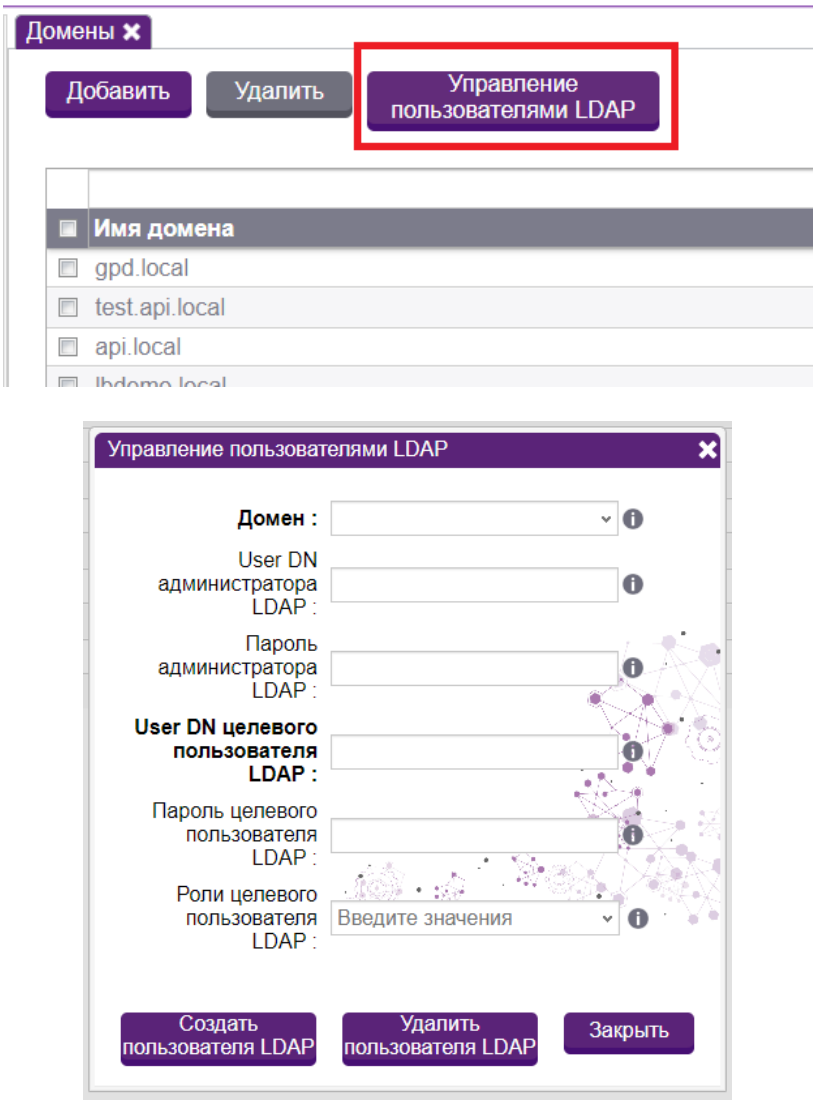


Рис. 3.7.6. Расположение кнопки «Управление пользователями LDAP» и просмотр этого окна

- Домен - сконфигурированный домен, к которому будет осуществляться подключение. Он выбирается для того, чтобы не пришлось дублировать все его настройки.
- User DN администратора LDAP - имя учетной записи LDAP, которая имеет права на создание других пользователей. Если в конфигурации домена указана учетная запись с правами администратора, то ее здесь можно не указывать, она подставится автоматически. Пример имени: cn=admin,dc=spaceldap,dc=lab
- Пароль администратора LDAP - пароль учетной записи LDAP, которая имеет права на создание других пользователей.
- User DN целевого пользователя LDAP - имя пользователя LDAP, который должен быть создан или удален. Пример имени: CN=test-user1,OU=people,DC=spaceldap,DC=lab
- Пароль целевого пользователя LDAP - пароль пользователя LDAP, который должен быть создан. Это поле можно не заполнять, если пользователя нужно не создать, а удалить.
- Роли целевого пользователя LDAP - роли, которые нужно присвоить пользователю LDAP. Про их возможности можно почитать на странице Пользовательские роли (1.4.0). Это поле можно не заполнять, если пользователя нужно не создать, а удалить.

После заполнения параметров нужно нажать на кнопку **Создать пользователя LDAP** или **Удалить пользователя LDAP**.

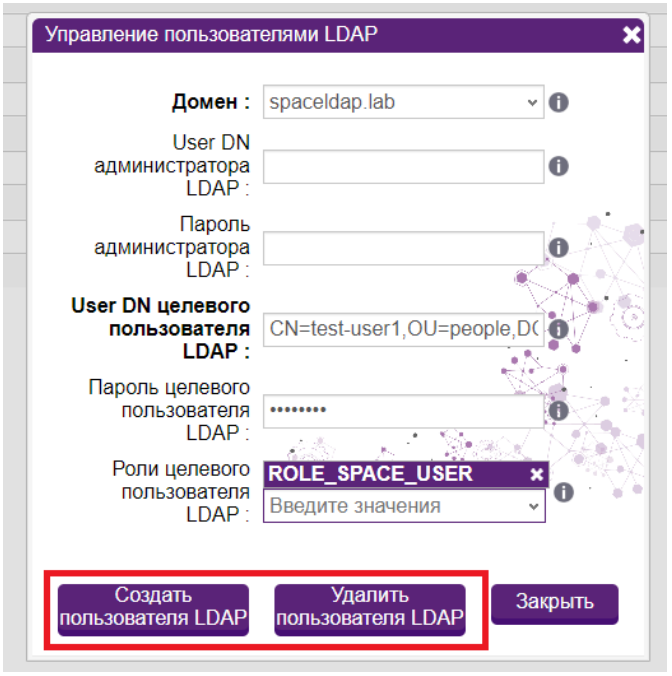


Рис. 3.7.7. Создание или удаление пользователя LDAP

3.8. Управление агентами паролей

Агенты паролей служат для рандомизации паролей учётных записей. В рамках Системы реализованы следующие возможности, доступные администратору:

- Просмотр агентов паролей;
- Добавление нового агента паролей;
- Редактирование агента паролей;
- Обновление таблицы агентов и типов агентов;
- Удаление строки в таблице агентов;
- Единовременное удаление нескольких записей из таблицы агентов;

3.8.1. Просмотр агентов паролей

Страница «Агенты паролей» состоит из двух таблиц: **Агенты** и **Типы агентов**.

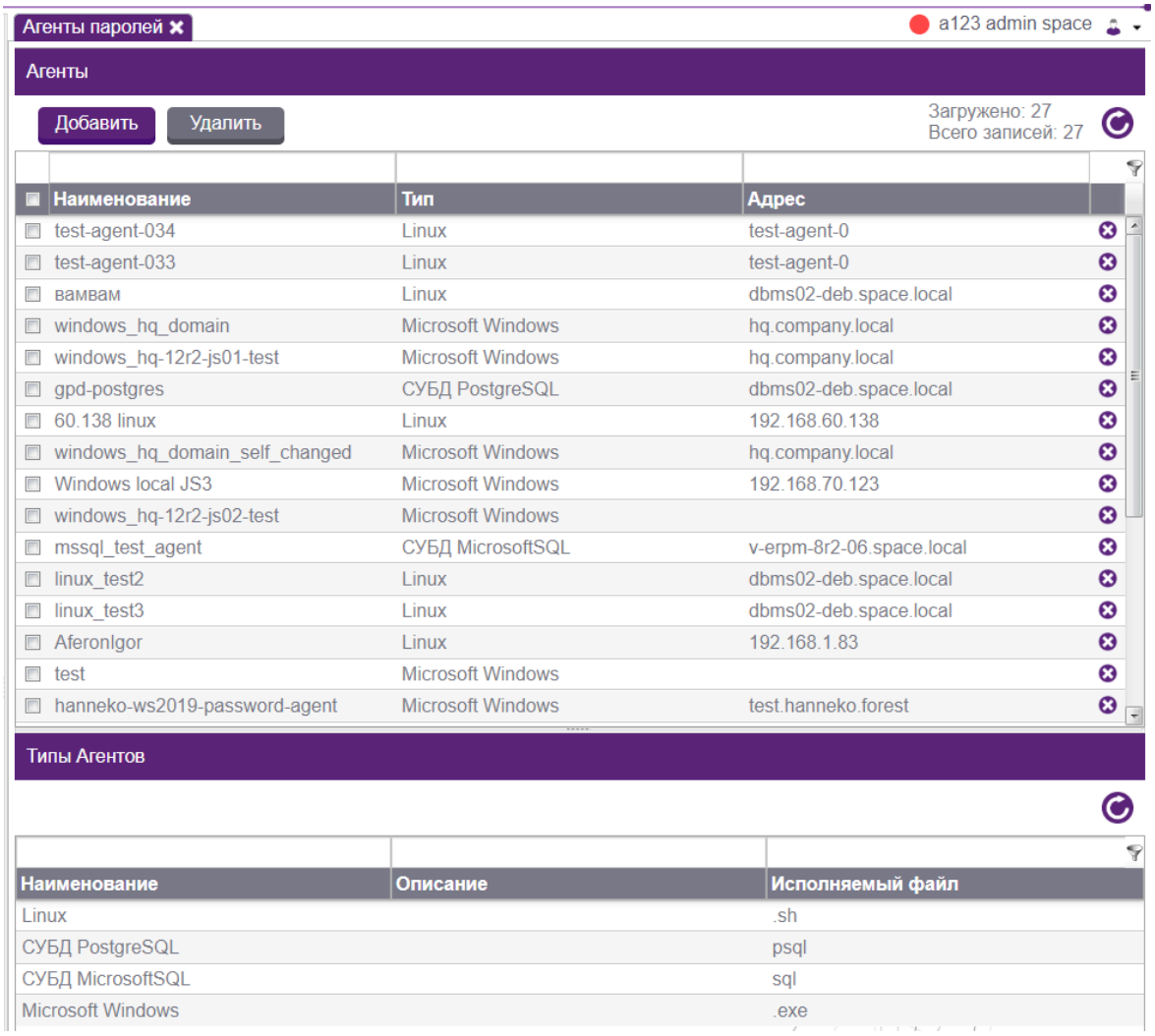


Рис. 3.8.1. Страница «Агенты паролей»

Описание параметров приведено ниже.

Поля таблицы **Агенты**:

- Наименование – наименование выбранного агента паролей;
- Тип – выбранного агента паролей;
- Адрес – адрес, по которому расположен данный агент паролей.

Поля таблицы **Типы Агентов**:

- Наименование – наименование выбранного типа агента паролей;
- Описание – словесное описание выбранного типа агента паролей;
- Исполняемый файл – формат исполняемого файла.

3.8.2. Добавление агента паролей

Функционал добавления Агентов паролей вызывается нажатием на кнопку **Добавить**, расположенную в верхней части таблицы.

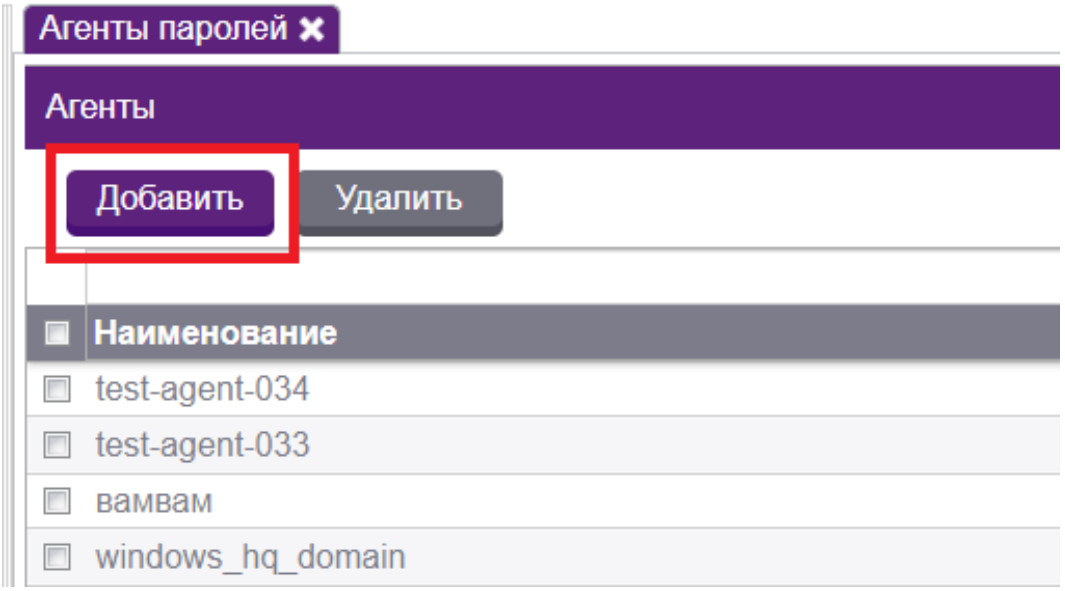


Рис. 3.8.2. Кнопка «Добавить» агент паролей

При нажатии на эту кнопку пользователю будет выведена форма добавления Агента, содержащая в себе несколько полей. Поля, выделенные жирным, обязательны для заполнения.

Список полей формы **Агент рандомизации Linux**:

- Наименование (обязательное поле) – имя создаваемого агента паролей;
- Серверы ЗС (обязательное поле) – сервера ЗС, на котором расположен данный агент;

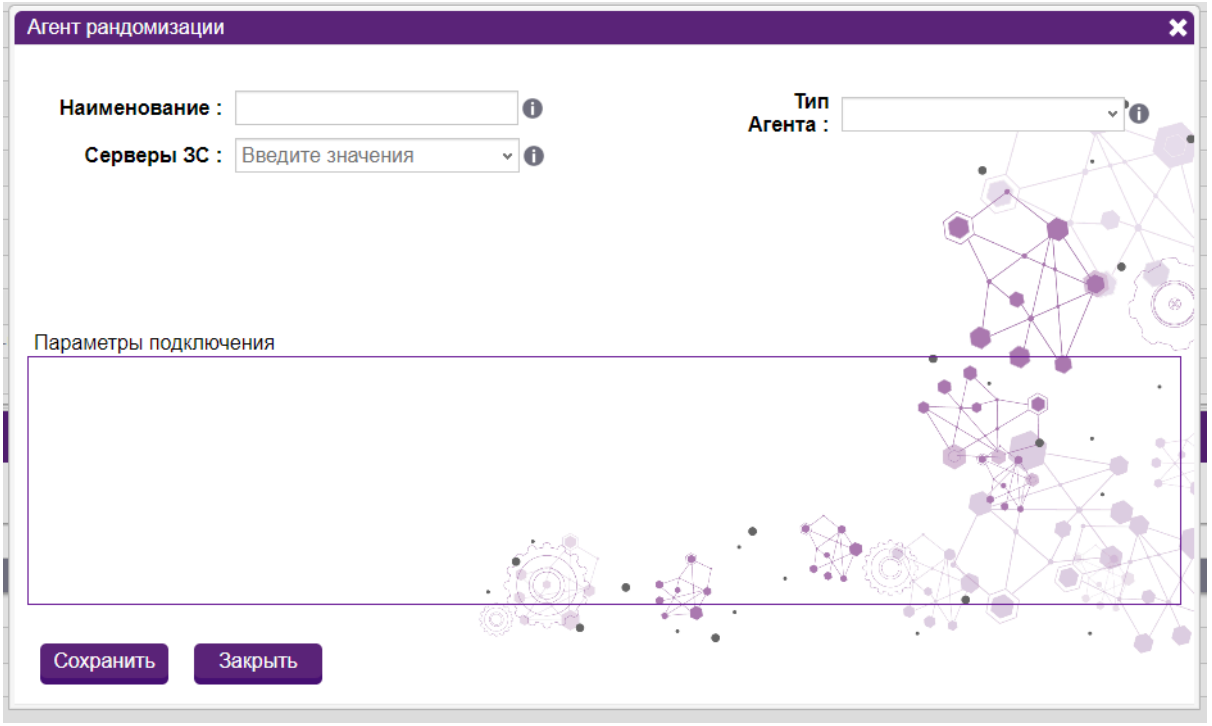


Рис. 3.8.3. Добавление агента паролей

- Тип Агента (обязательное поле) – тип создаваемого агента рандомизации;
- Адрес (обязательное поле) – адрес, на который производится подключения агента;
- Порт – порт, на который производится подключение агента;
- Привилегированная УЗ – УЗ, под которой производится подключение агента (должна обладать правами на смену пароля);
- Учетная запись для логина – УЗ для логина на подключаемую машину (может совпадать с Привилегированной УЗ).

Список полей формы **Агент рандомизации Microsoft Windows**:

- Наименование (обязательное поле) – имя создаваемого агента паролей;
- Серверы ЗС (обязательное поле) – сервера ЗС, на котором расположен данный агент;
- Тип Агента (обязательное поле) – тип создаваемого агента рандомизации;
- Адрес (обязательное поле) – адрес, на который производится подключения агента;
- Привилегированная УЗ – УЗ, под которой производится подключение агента (должна обладать правами на смену пароля)..

3.8.3. Редактирование агента паролей

Функционал редактирования Агента паролей вызывается при двойном щелчке на наименовании агента в таблице.

Будет выведено окно с информацией об Агенте и активной кнопкой **Редактирование**. После нажатия на эту кнопку поля станут доступны для редактирования.

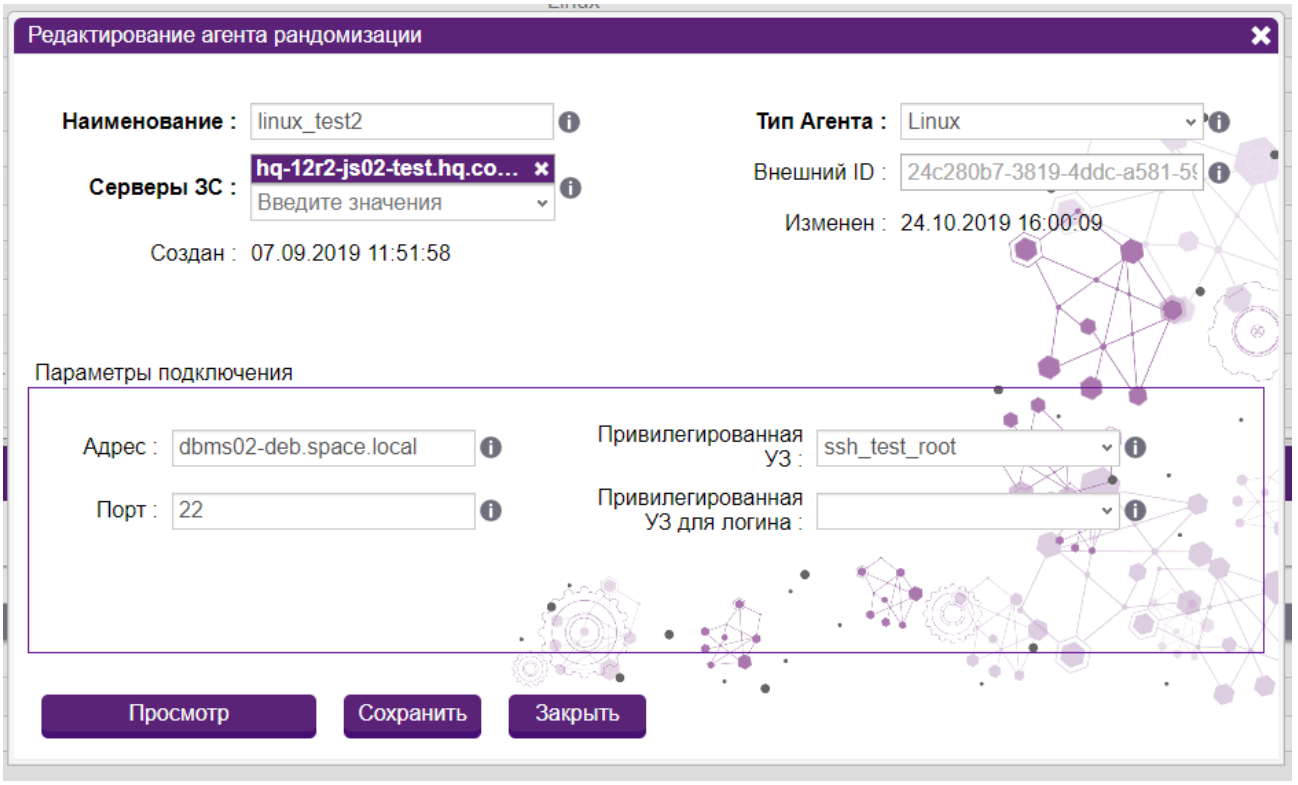


Рис. 3.8.4. Окно редактирования агента паролей

Все поля, кроме Внешнего ID, доступны для редактирования. Чтобы сохранить изменения, необходимо нажать кнопку **Сохранить**. При нажатии кнопки **Отмена** никаких изменений в карточке Агента паролей не произойдет.

3.8.4. Обновление таблицы агентов и типов агентов

Для обновления записей в таблице служит соответствующая кнопка **Обновить**, расположенная в правой части верхней панели.

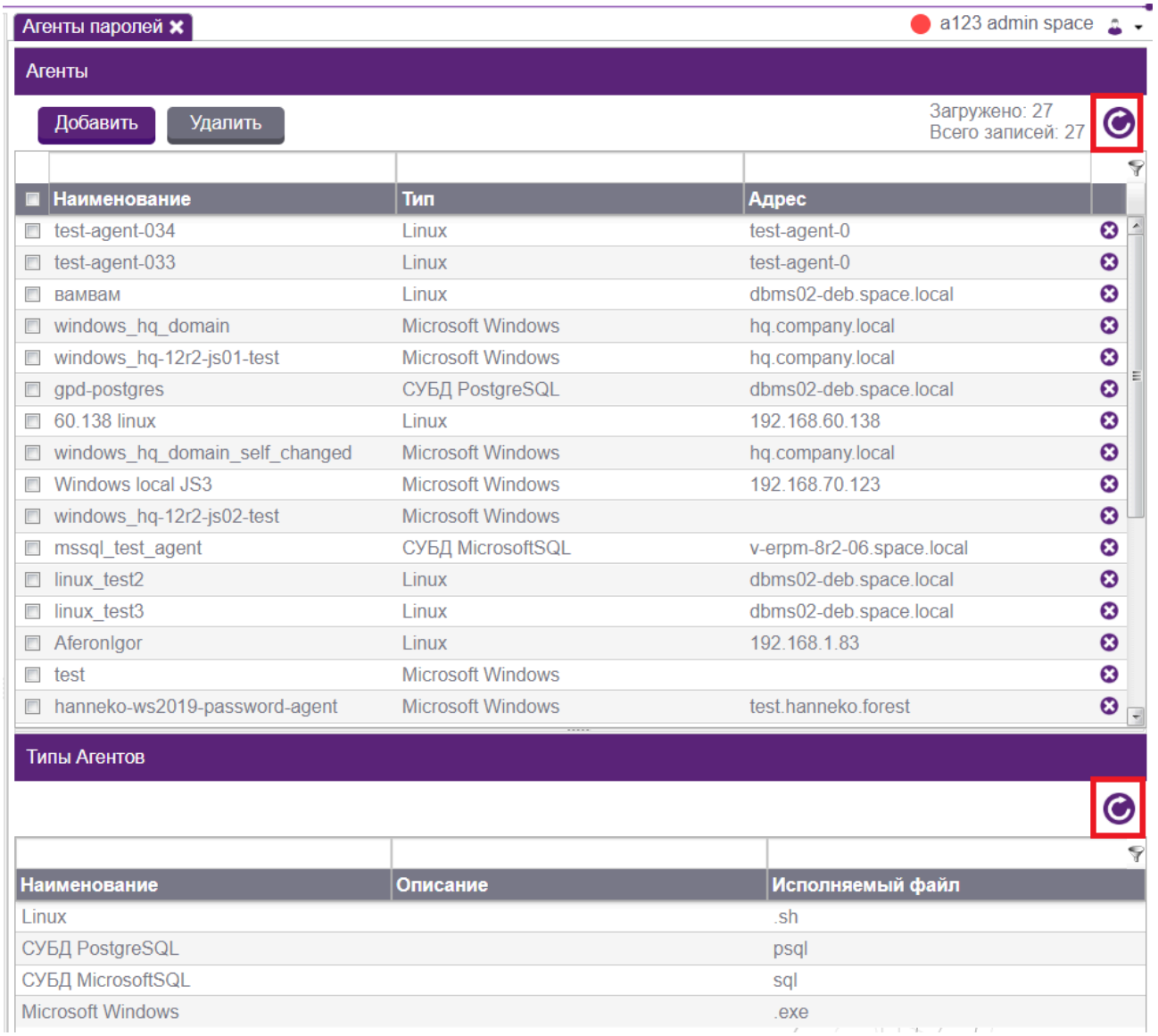


Рис. 3.8.5. Расположение кнопки «Обновить»

3.8.5. Удаление строки в таблице агентов

Для удаления строки в таблице служит соответствующая иконка **Удалить**, расположенная в правой части строки записи.

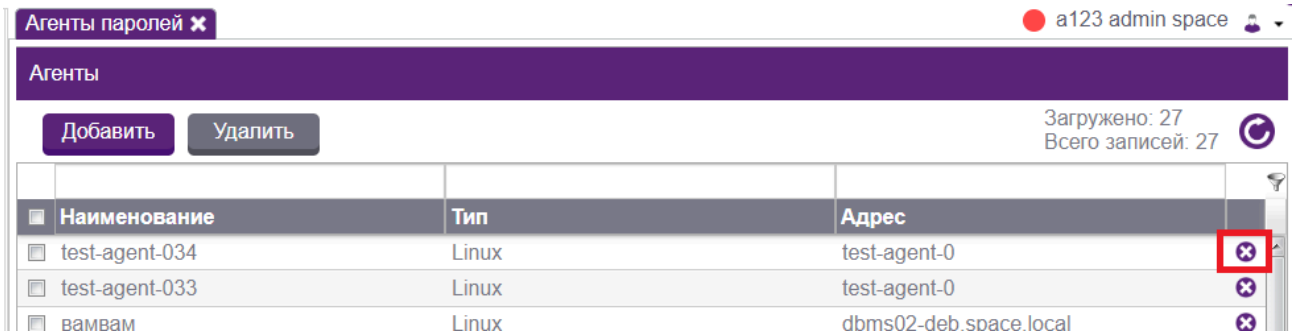


Рис. 3.8.6. Расположение кнопки «Удалить»

3.8.6. Одновременное удаление нескольких записей из таблицы агентов

Для одновременного удаления нескольких записей сначала следует выделить желаемые записи в таблице галочкой слева, после чего станет активной кнопка **Удалить**, расположенная сверху над таблицей.

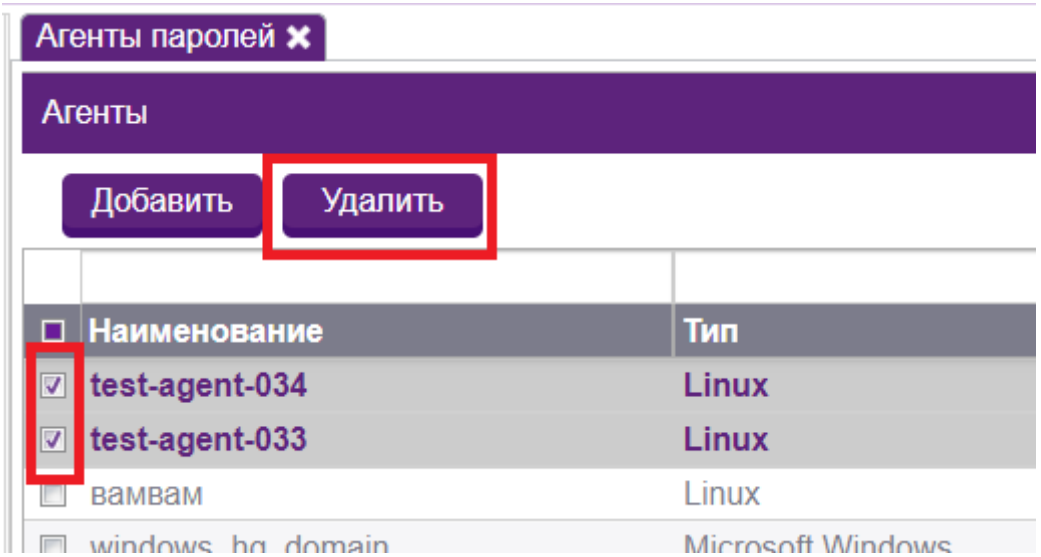


Рис. 3.8.7. Удаление двух агентов паролей

3.9. Управление фильтрацией ввода

Данная страница позволяет настроить модели данных для фильтрации, которую будет осуществлять внутренняя системы видеоаудита (ВСАС). Фильтрация ввода служит для того, чтобы установить ряд запрещенных команд, при вводе которых во время активного сеанса пользователь может быть автоматически ограничен.

В рамках просмотра этой страницы администраторы могут выполнять следующие действия:

- Обновлять страницы фильтрации ввода;
- Добавлять и редактировать фильтрацию ввода;
- Обновлять таблицу списков фильтрации ввода;
- Удалять строки в таблице списков фильтрации ввода;
- Единовременно удалять несколько записей из таблицы списков фильтрации ввода.

3.9.1. Добавление фильтрации ввода

Функционал добавления фильтрации ввода вызывается нажатием на кнопку **Добавить**, расположенную в верхней части таблицы.

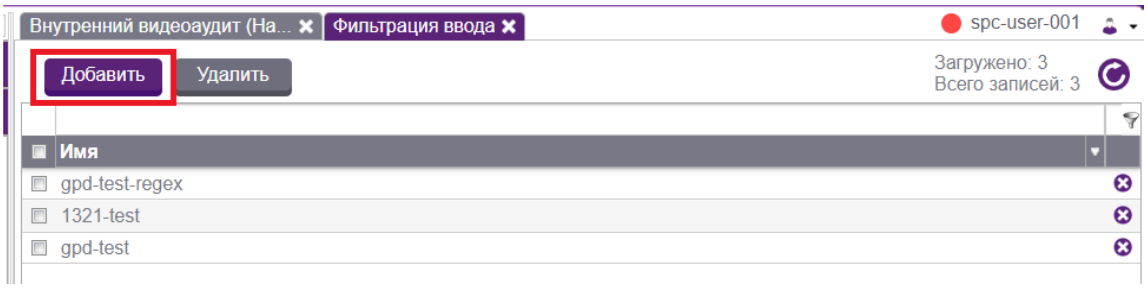


Рис. 3.9.1. Кнопка «Добавить»

При нажатии на эту кнопку пользователю будет выведена форма добавления списка фильтрации ввода, содержащая в себе несколько полей. Поля, выделенные жирным, обязательны для заполнения.

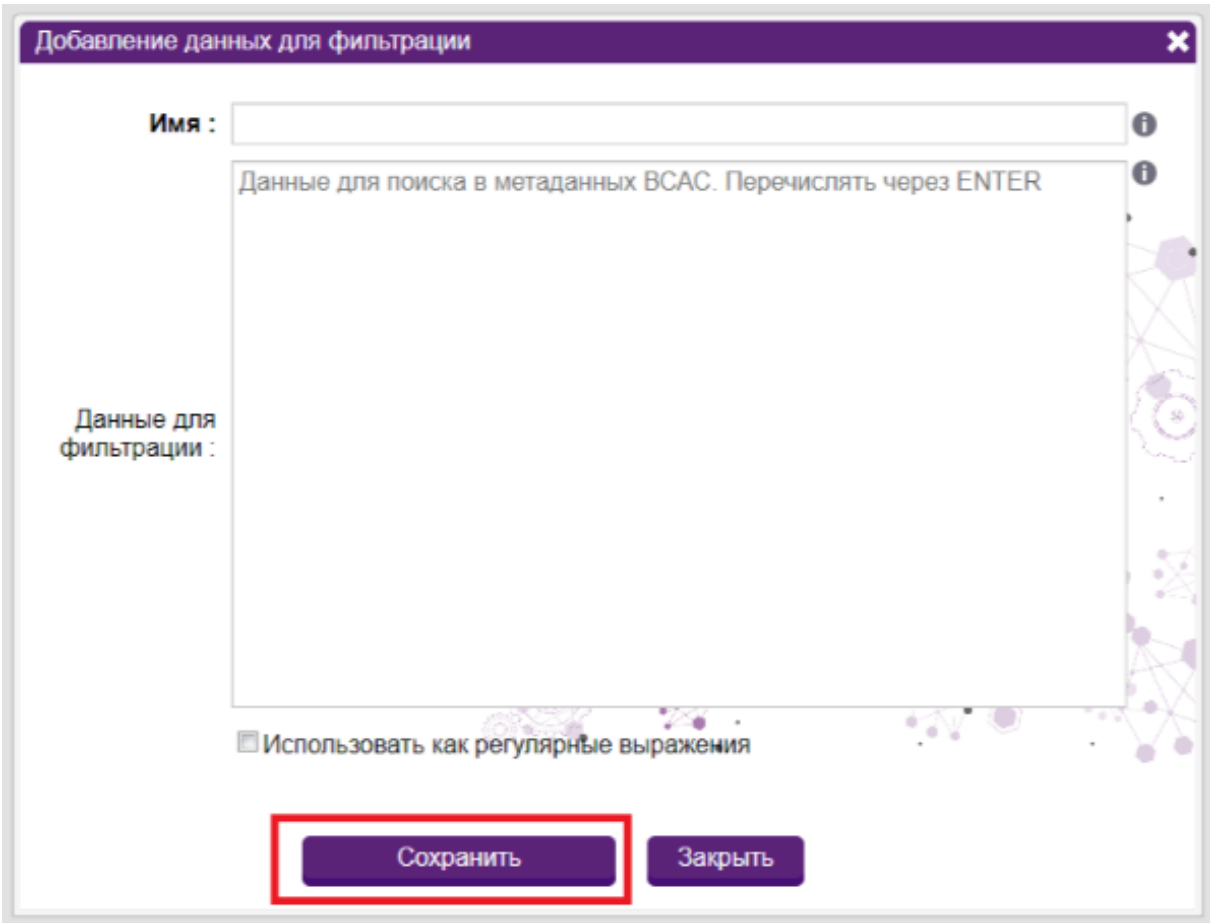


Рис. 3.9.2. Добавление данных для фильтрации

Список полей формы **Добавление данных для фильтрации**:

- Имя (обязательное поле) - наименование списка фильтрации ввода;

- Данные для фильтрации - перечень слов и символов, которые пользователю запрещено вводить. Перечисление различных пунктов нужно делать через клавишу "Enter".
- В данных списка для фильтрации можно использовать регулярные выражения - для этого необходимо поставить соответствующую галочку. Когда эта опция включена, система будет использовать регулярные выражения для проверки ввода, что даёт ей возможность искать не только точные совпадения, но и учитывать разные варианты написания, замену символов, частичное совпадение и другие возможности.

Примечание: Регулярные выражения — это особый формат, с помощью которого можно задавать гибкие правила поиска и соответствия для более сложных случаев. Функция "Использовать как регулярное выражение" позволяет интерпретировать слова или фразы в поле “Данные для фильтрации” не как точные строки, а как шаблоны, которые могут соответствовать множеству вариантов текста.

Пример: Если в “Данных для фильтрации” используется регулярное выражение ".*test.*", то это выражение будет означать следующее:

- .* — это шаблон, который соответствует любому количеству любых символов (включая отсутствие символов) до или после слова "test";
- test — это буквальная строка, которую нужно найти.

Таким образом, выражение ".*test.*" при включенной опции “Использовать как регулярное выражение” будет блокировать любые строки, в которых содержится слово "test", независимо от того, что перед или после него (например, "test", "mytest", "test123", "this is a test message" и т.д.).

После заполнения всех данных необходимо нажать на кнопку Сохранить. Чтобы фильтрация ввода стала работать, необходимо также указать ее в соответствующей графе Наряда-допуска. Там же можно указать действия при нахождении в сеансе запрещенных команд. Подробнее рассказано в разделе о создании наряда-допуска.

3.9.2 Редактирование фильтрации ввода

Функционал редактирования фильтрации ввода вызывается при двойном щелчке на строку с фильтрацией ввода в таблице.

Будет выведено окно с информацией о данных для фильтрации и активной кнопкой **Редактирование**. После нажатия на эту кнопку поля станут доступны для редактирования. Поля, выделенные жирным, обязательны для заполнения.

Список полей формы **Редактирование данных для фильтрации**:

- Имя (обязательное поле) - наименование списка фильтрации ввода;

- Данные для фильтрации - перечень слов и символов, которые пользователю запрещено вводить. Перечисление различных пунктов нужно делать через клавишу "Enter".
- Внешний ID - ID для интеграции с внешними системами.

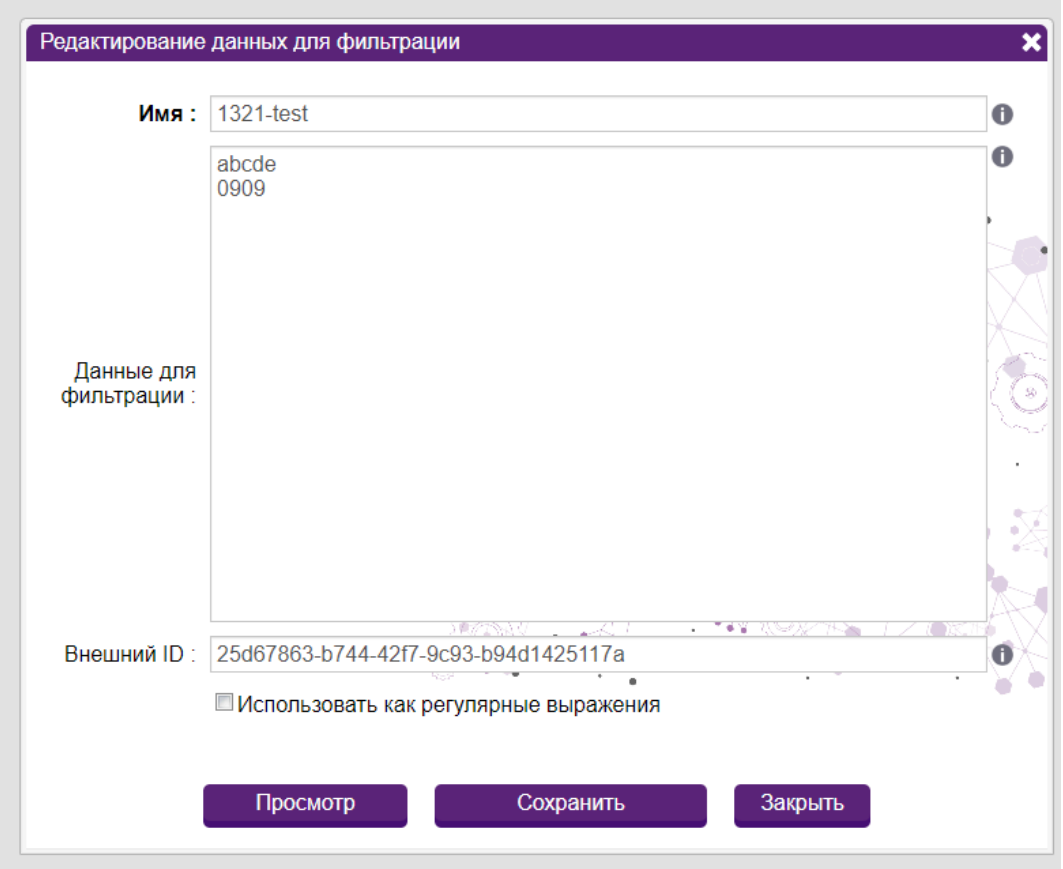


Рис. 3.9.3. Окно редактирования данных для фильтрации

Все поля, кроме Внешнего ID, доступны для редактирования. Чтобы сохранить изменения, необходимо нажать кнопку **Сохранить**. При нажатии кнопки **Закрыть** никаких изменений в карточке данных для фильтрации не произойдет.

3.9.3. Обновление страницы фильтрации ввода

Для обновления страницы фильтрации служит соответствующая кнопка **Обновить**, расположенная в правой части верхней панели.

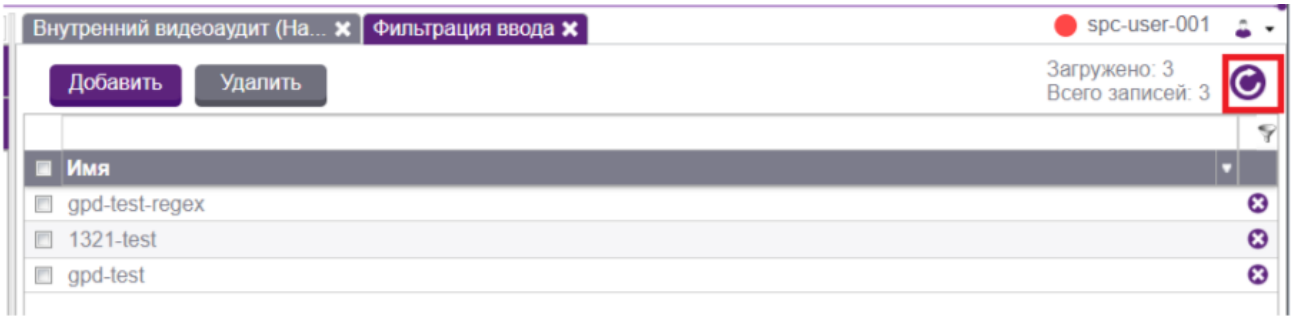


Рис. 3.9.4. Кнопка «Обновить»

3.9.5. Удаление строки в таблице списков фильтрации ввода

Для удаления строки в таблице списков фильтрации ввода необходимо щелкнуть на кнопке удаления, расположенной в правой части строки записи.

3.9.6. Удаление нескольких записей из таблицы списков фильтрации ввода

Для удаления нескольких записей из таблицы списков фильтрации ввода одновременно необходимо сначала выделить нужные записи в таблице, установив флажок в соответствующем поле слева от поля **Имя**, после чего станет активной кнопка **Удалить**, расположенная сверху над таблицей.

3.10. Изменение дополнительных настроек

Вкладка **Дополнительные настройки** раздела **Управление системой** позволяет управлять некоторыми настройками системы sPACE.

В рамках данного раздела администраторы могут выполнять следующие действия:

- Настраивать парольную политику;
- Настраивать DNS серверы;
- Включать и выключать внешнюю тикет-систему;

3.10.1. Настройка парольной политики

Для того, чтобы сменить настройки парольной политики, необходимо нажать на иконку карандаша напротив соответствующей строки в настройках.

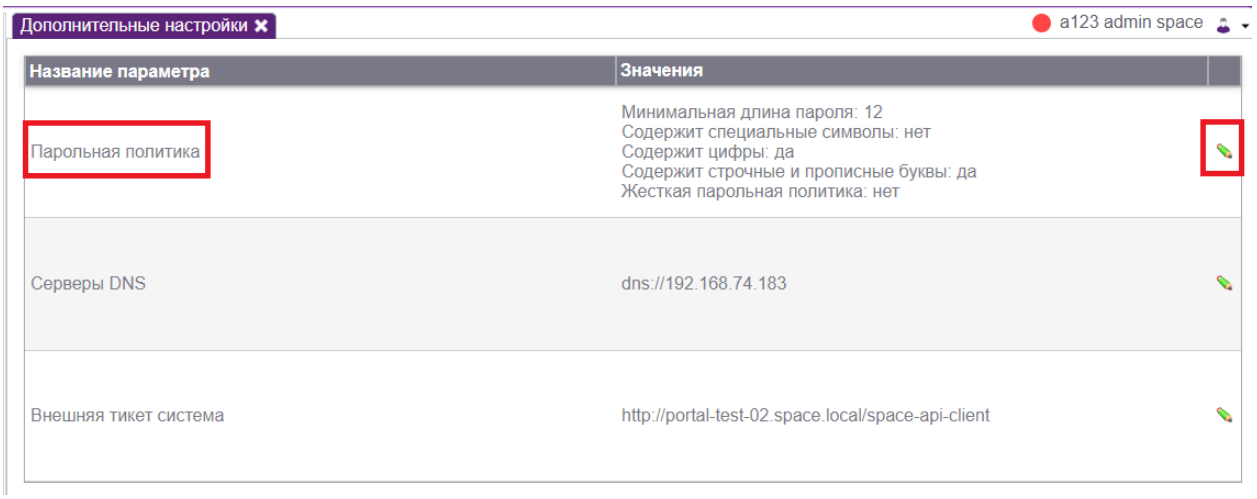


Рис. 3.10.1. Кнопка редактирования парольной политики

Откроется окно настроек парольной политики. Необходимо выбрать новые параметры пароля, затем нажать на кнопку **Сохранить**. Если поставить галочку в

графе **Жесткая парольная политика,** то можно будет создать только пароль, удовлетворяющий всем требованиям. В случае, если такая галочка отсутствует, то при создании простого пароля пользователю будет выведено уведомление о том, что его пароль не соответствует парольной политике, однако он все равно сможет его оставить.

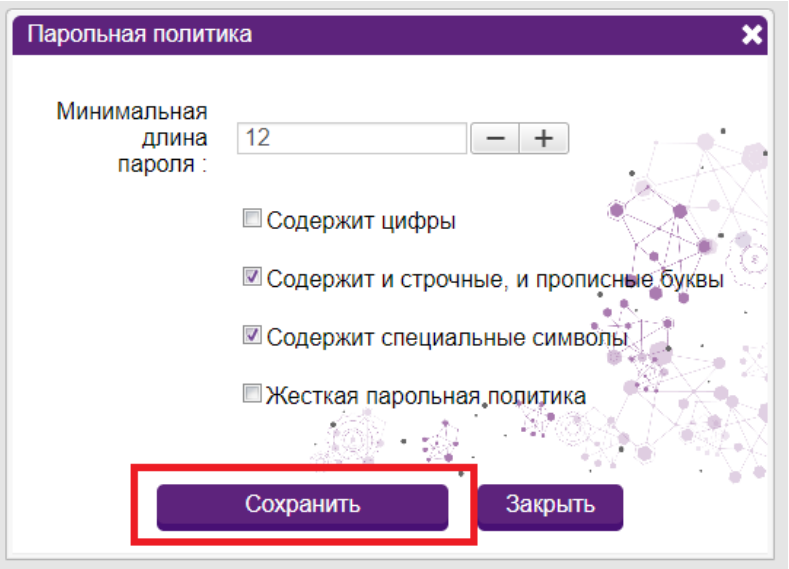


Рис. 3.10.2. Кнопка «Сохранить»

3.10.2. Настройка DNS серверов

DNS сервер - тот, через который происходит подключение к тенанту, их может быть несколько. Для того, чтобы сменить список DNS серверов, необходимо нажать на иконку карандаша напротив соответствующей строки в настройках.

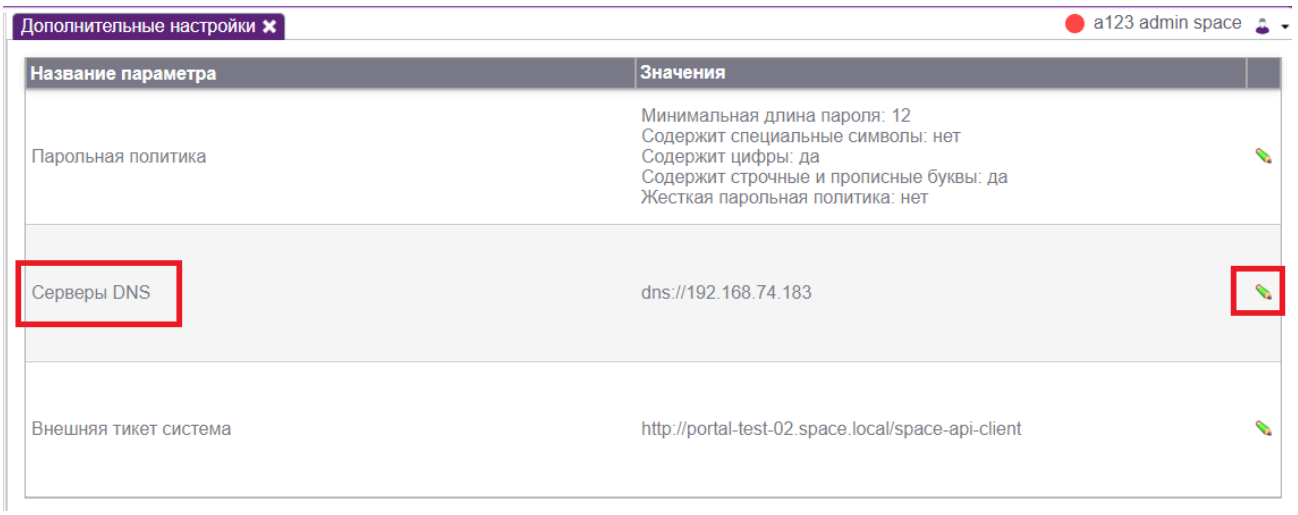


Рис. 3.10.3. Кнопка редактирования серверов DNS

Откроется окно со списком серверов DNS. Чтобы его отредактировать, нужно нажать на кнопку **Редактирование**. В списке можно изменить уже существующие

DNS сервера или внести новые. Если DNS серверов несколько, то каждый новый адрес должен быть указан на новой строчке.

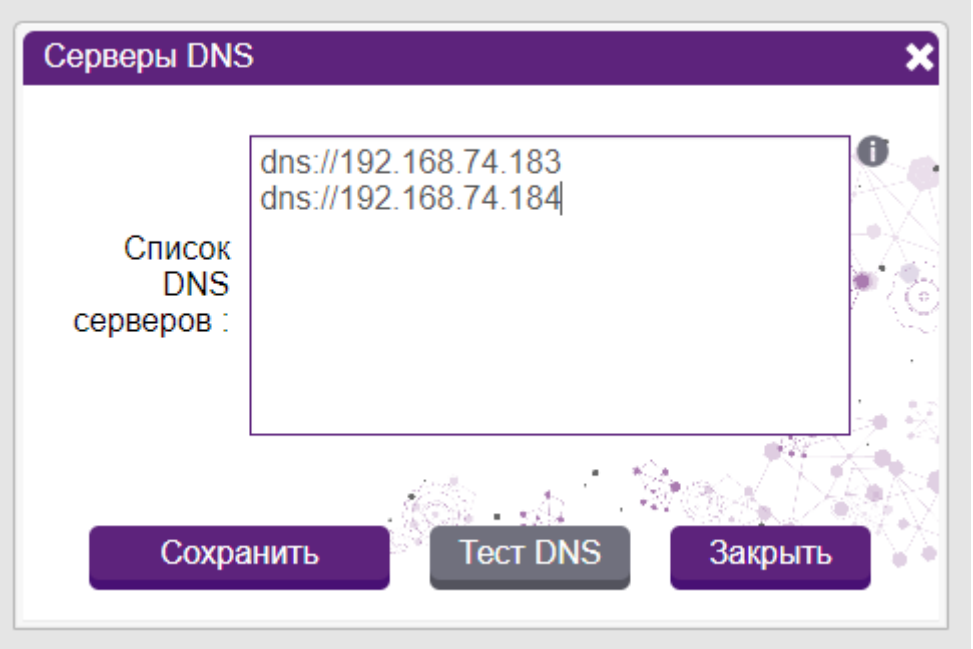


Рис. 3.10.4. Пример корректного заполнения DNS конфигурации

После того, как были указаны или изменены DNS сервера нужно нажать на кнопку **Сохранить**. Далее рекомендуется протестировать их конфигурацию. Для этого надо нажать кнопку **Тест DNS**, которая находится под списком серверов DNS.

Рис. 3.10.5. Пример корректного заполнения DNS конфигурации

Если параметр заполнен верно, то будет выведено соответствующее уведомление. В иных случаях рекомендуется проверить корректность заполнения данного поля.

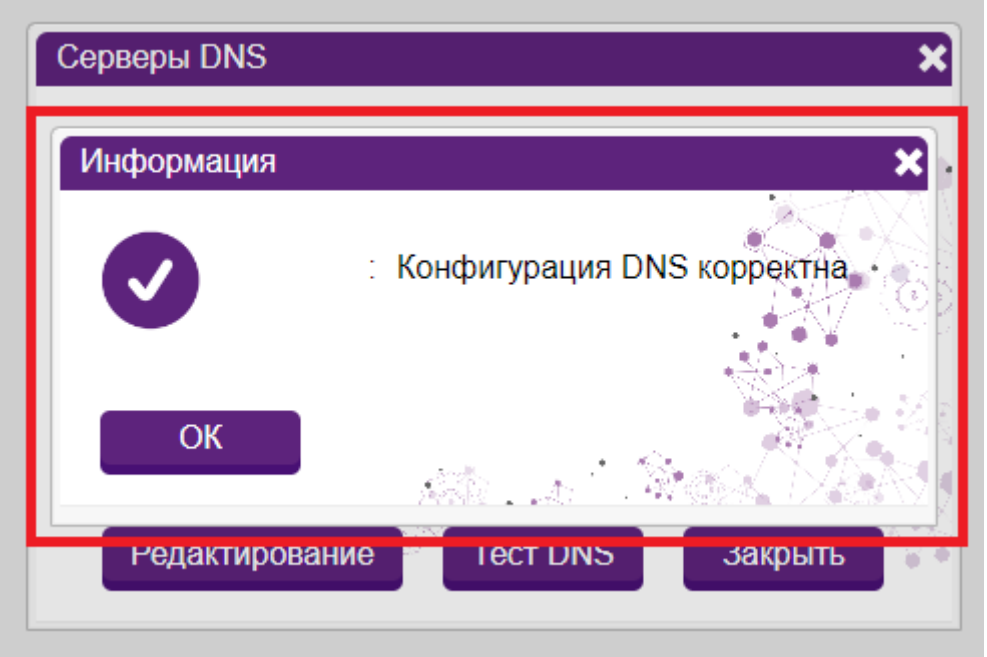


Рис. 3.10.6. Пример корректного тестирования DNS конфигурации

3.10.3. Включение и выключение Внешней тикет системы

Внешняя тикет система - это сторонний портал, через который пользователь может запросить доступ к Наряду-допуску, не авторизуясь при этом на портале системы sPACE.

Для настройки Внешней тикет системы нужно кликнуть на иконку карандаша напротив соответствующей строки в настройках.

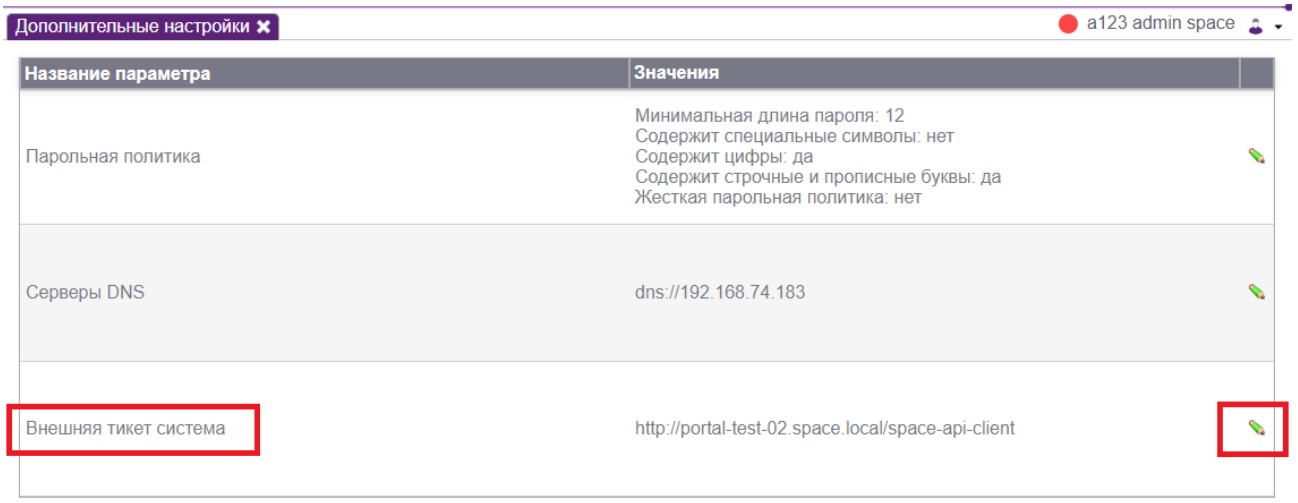


Рис. 3.10.7. Кнопка настройки внешней тикет системы

Откроется окно настройки с активной кнопкой **Редактирование**.

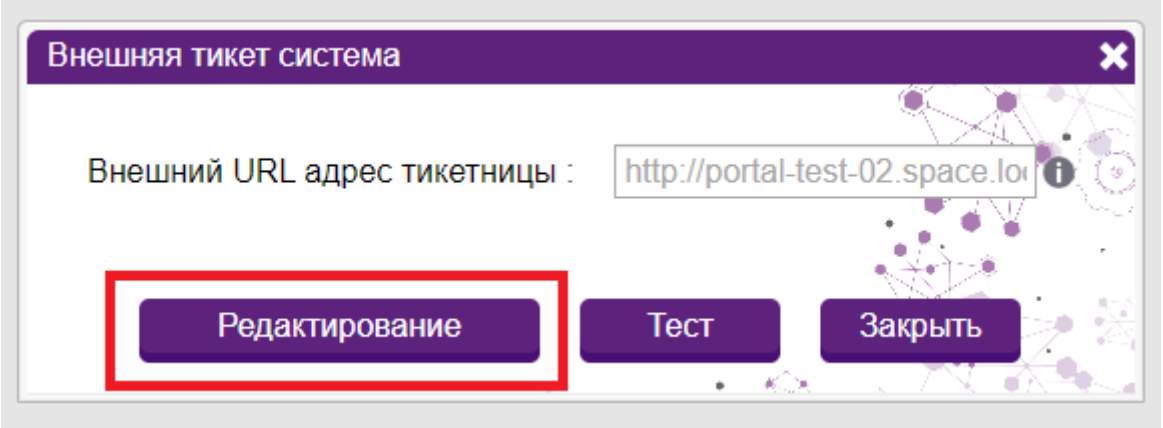


Рис. 3.10.8. Редактирование тикет системы

После нажатия на эту кнопку в доступное поле нужно ввести Внешний URL адрес сторонней тикет системы, которую требуется подключить к порталу (примечание: у него не должно быть символа "/" в конце адреса).

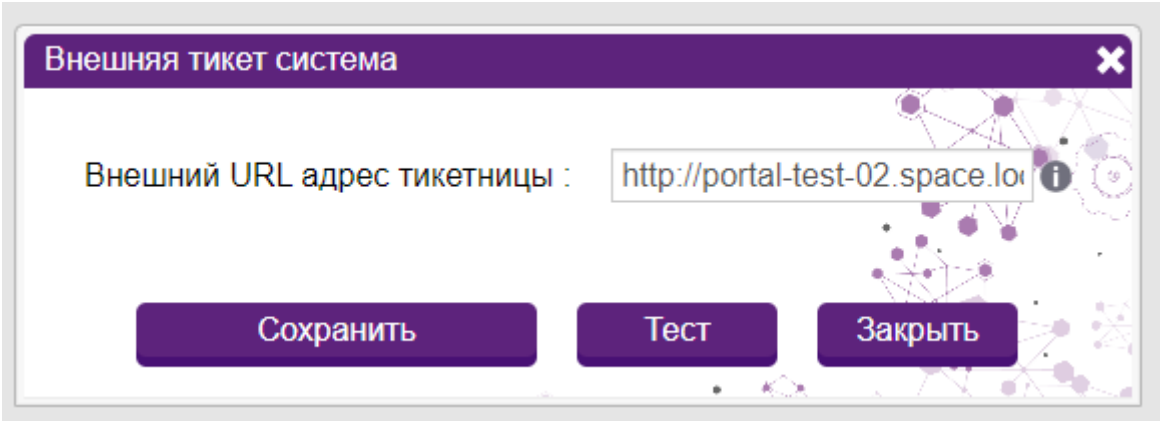


Рис. 3.10.9. Пример корректного заполнения адреса тикет системы

Затем требуется нажать на кнопку **Тест**. Если подключение к сторонней тикетнице прошло корректно, то появится соответствующее уведомление.

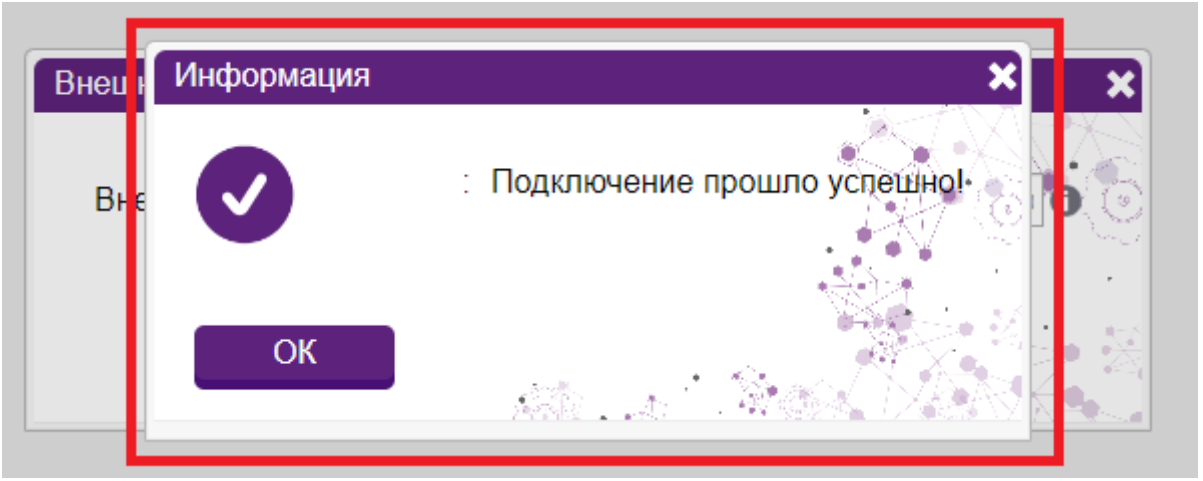


Рис. 3.10.10. Пример корректного тестирования подключения к внешней тикет системе

Для завершения настройки Внешней тикет-системы требуется нажать на кнопку **Сохранить**. Если нажать кнопку **Закрыть**, то адрес тикет системы не сохранится.

Для выключения Внешней тикет системы нужно удалить ее адрес из соответствующего поля и нажать на кнопку **Сохранить**.

3.11. Управление тенантами

Вкладка **Тенанты** раздела **Управление ресурсами** служит для отображения пользователю информации о тенантах, которые присутствуют в системе. Тенант - это своеобразная "копия" системы, которая предназначается для использования, например, одним из подразделений компании. Пользователь одного тенанта не может попасть на другой тенант, т. к. разные тенанты изолированы друг от друга. У каждого из тенантов может быть своя инфраструктура, которая задается во вкладке **Управление системой** и может редактироваться пользователем с ролью Администратор. Элементы системы, которые задаются в панели **Управление ресурсами** являются общими для всех тенантов, ими может управлять только пользователь с ролью "Технический администратор".

В рамках настройки и управления тенантами технические администраторы могут выполнять следующие действия:

- Добавлять тенанты;
- Редактировать тенанты;
- Обновлять таблицу тенантов;
- Удалять тенант в таблице тенантов;
- Единовременно удалять несколько записей в таблице тенантов.

3.11.1. Добавление тенантов

Для добавления тенанта (помимо основного main, который присутствует в системе по умолчанию) необходимо перейти в узел **Тенанты** раздела **Управление ресурсами** и щелкнуть мышью на кнопке **Добавить** в таблице **Тенантов**.

На экране отобразится форма добавления тенанта.

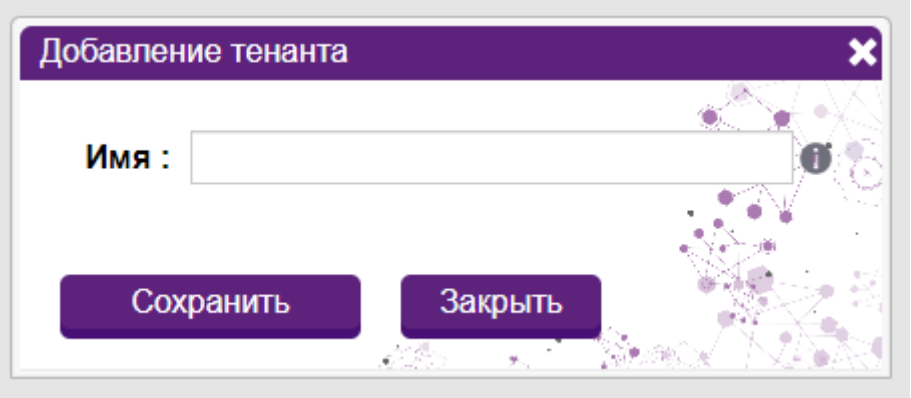


Рис. 3.11.1. Форма добавления тенанта

Форма добавления тенанта содержит в себе одно поле:

- Имя – название добавляемого тенанта;

Как только нужный параметр был указан, требуется нажать на кнопку **Сохранить**.

3.11.2. Редактирование тенанта

Для редактирования тенанта необходимо дважды щелкнуть мышью на имени тенанта в таблице. В появившейся карточке тенанта отображается вся информация о нём.

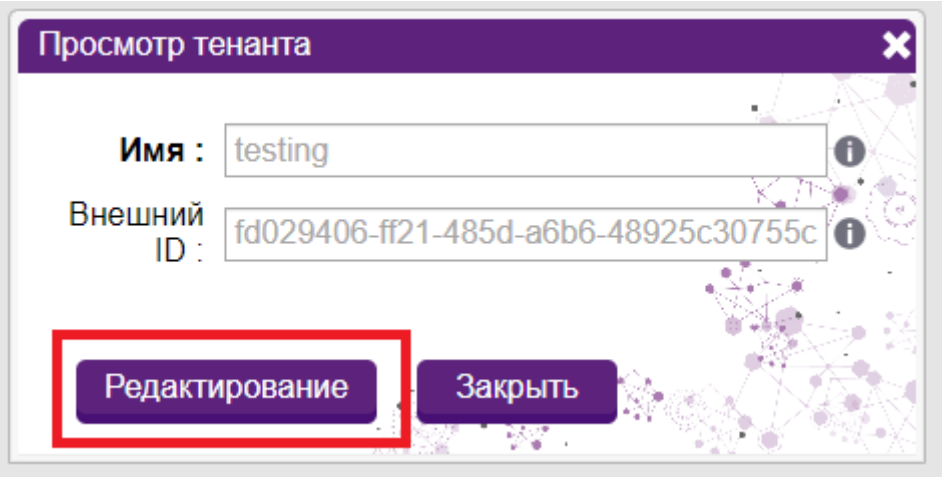


Рис. 3.11.2. Карточка тенанта

При нажатии на кнопку **Редактирование** на экран выводится форма редактирования тенанта.

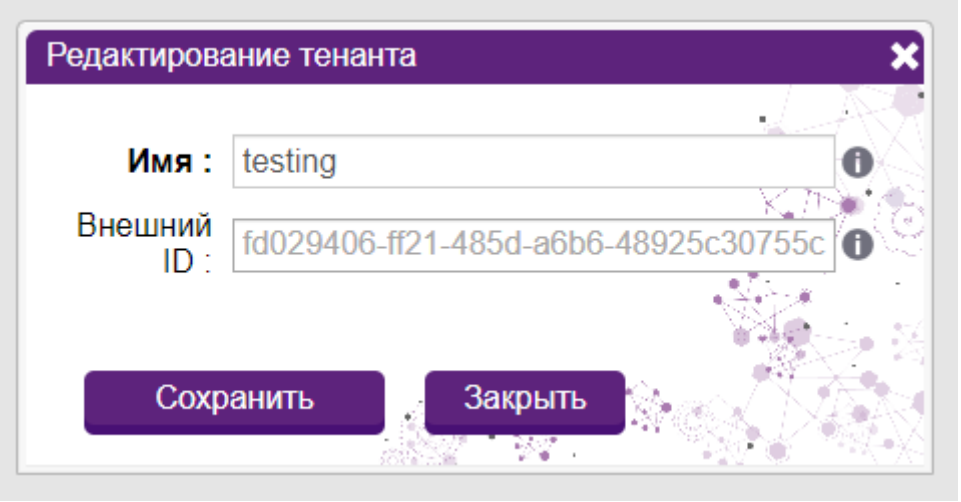


Рис. 3.11.3. Форма редактирования тенанта

Поле **Имя** доступно для редактирования, а поле **Внешний ID** недоступно, так как генерируется автоматически. Чтобы сохранить изменения, необходимо нажать кнопку **Сохранить**. При нажатии кнопки **Закрыть** никаких изменений в карточке тенанта не произойдет.

3.11.3. Обновление таблицы тенантов

Для обновления записей в таблице необходимо перейти в узел **Тенанты** раздела **Управление ресурсами** и щелкнуть мышью на кнопке обновления в правой верхней части таблицы.

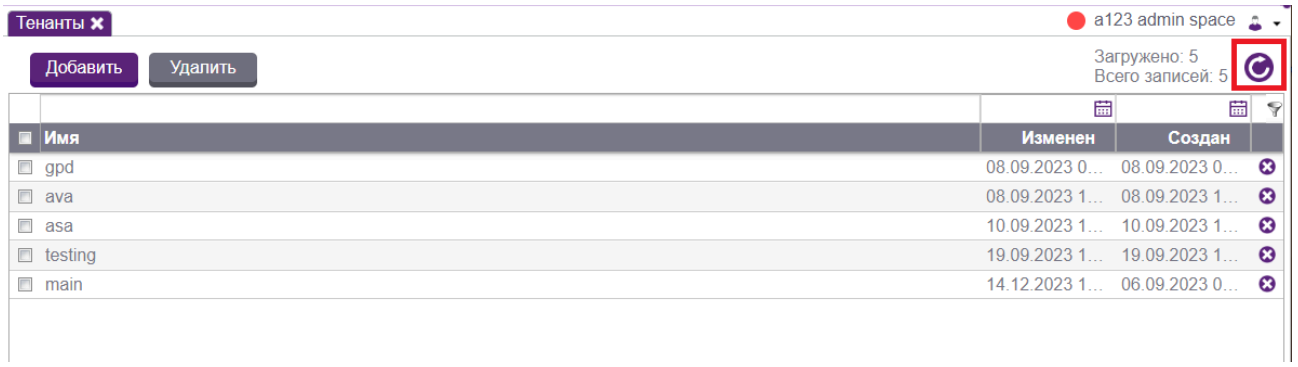


Рис. 3.11.4. Кнопка обновления информации

3.11.4. Удаление в таблице тенантов

Для удаления строки из таблицы тенантов щелкните мышью на кнопке удаления в правой части строки записи.

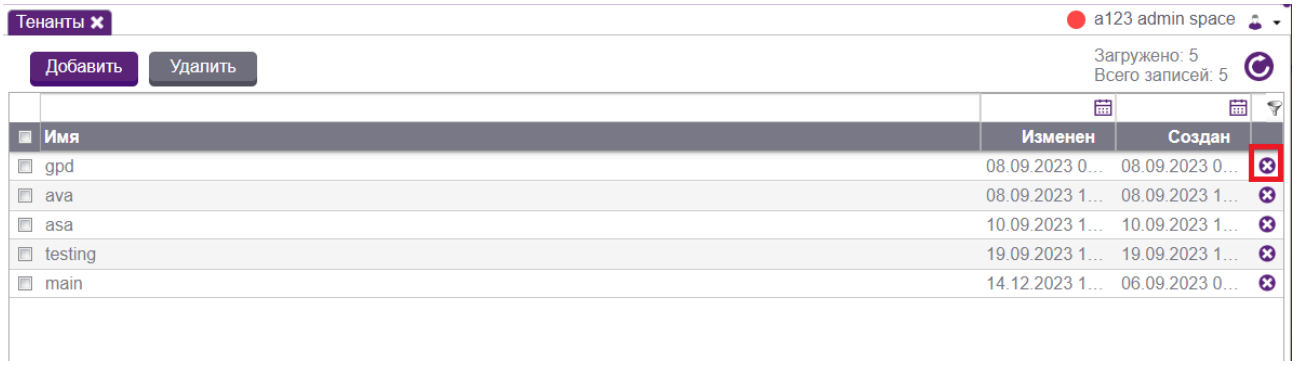


Рис. 3.11.5. Кнопка удаления тенанта

Удаление нескольких записей в таблице тенантов

Для удаления нескольких записей из таблицы тенантов одновременно следует выделить желаемые записи в таблице, установив флажок в соответствующем поле слева от поля **Имя**, после чего станет активной кнопка **Удалить**, расположенная сверху над таблицей.

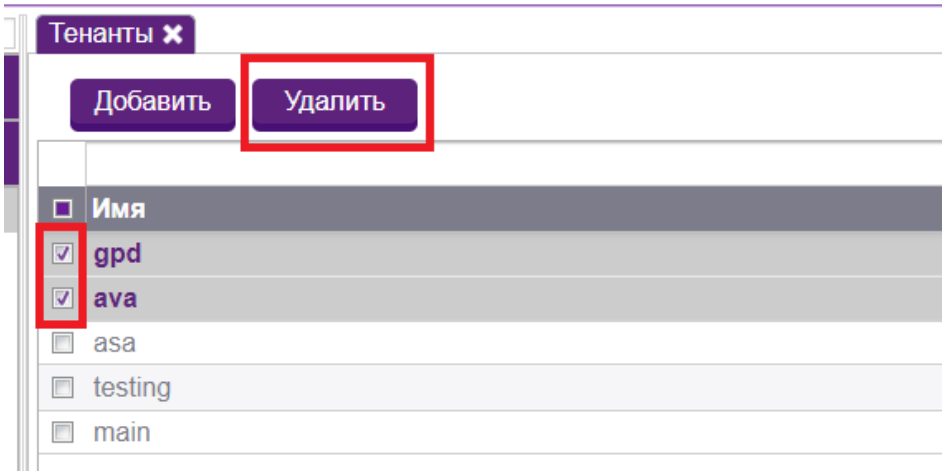


Рис. 3.11.6. Выбор двух записей таблицы и кнопка удаления

3.12. Управление интерпретаторами

После щелчка мышью на узле **Интерпретаторы** дерева навигации раздела **Управление ресурсами** техническому администратору отображается окно **Интерпретаторы сценариев**, которое представляет собой таблицу с тремя столбцами: Имя, Интерпретатор и Расширение для сценария.

В рамках настройки и управления интерпретаторами администраторы могут выполнять следующие действия:

- Добавлять интерпретаторы;
- Редактировать интерпретаторы;

- Обновлять таблицу интерпретаторов;
- Удалять строку в таблице интерпретаторов;
- Единовременно удалять несколько записей в таблице интерпретаторов.

3.12.1. Добавление интерпретаторов

Для добавления учетной записи необходимо перейти в узел **Интерпретаторы** раздела **Управление системой** и щелкнуть мышью на кнопке **Добавить** в таблице **Интерпретаторы сценариев**.

На экране отобразится форма добавления интерпретатора.

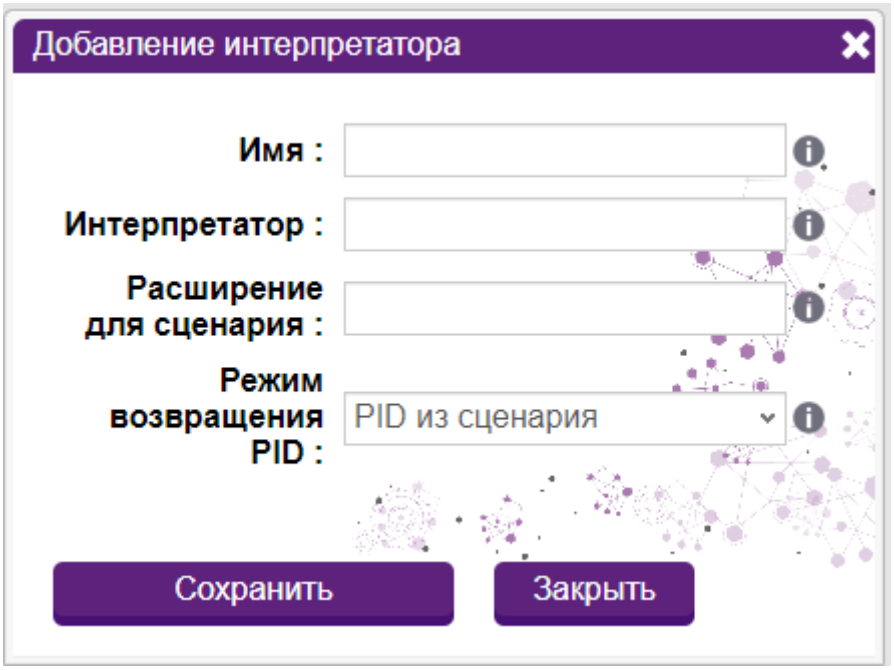


Рис. 3.12.1. Форма добавления интерпретатора

Форма добавления интерпретатора содержит в себе несколько полей (все поля обязательны для заполнения):

- Имя – название добавляемого интерпретатора;
- Интерпретатор – название исполняемого файла для данного интерпретатора;
- Расширение для сценария – расширение, которое должно быть у сценария, чтобы его считывал данный интерпретатор;
- Режим возвращения PID – может быть взят из сценария или быть прямым.

3.12.2. Редактирование интерпретаторов

Для редактирования интерпретатора необходимо дважды щелкнуть мышью на имени интерпретатора в таблице. В появившейся карточке интерпретатора отображается вся информация о нём.

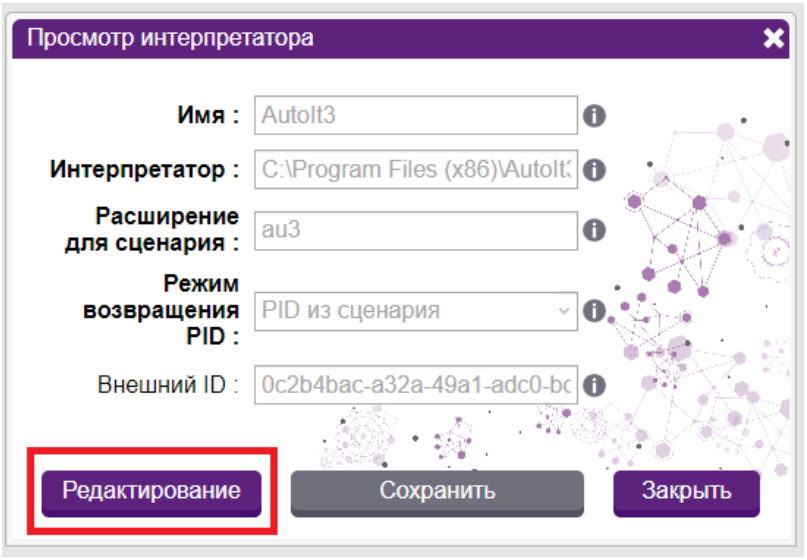


Рис. 3.12.2. Карточка интерпретатора

При нажатии на кнопку **Редактирование** на экран выводится форма редактирования интерпретатора.

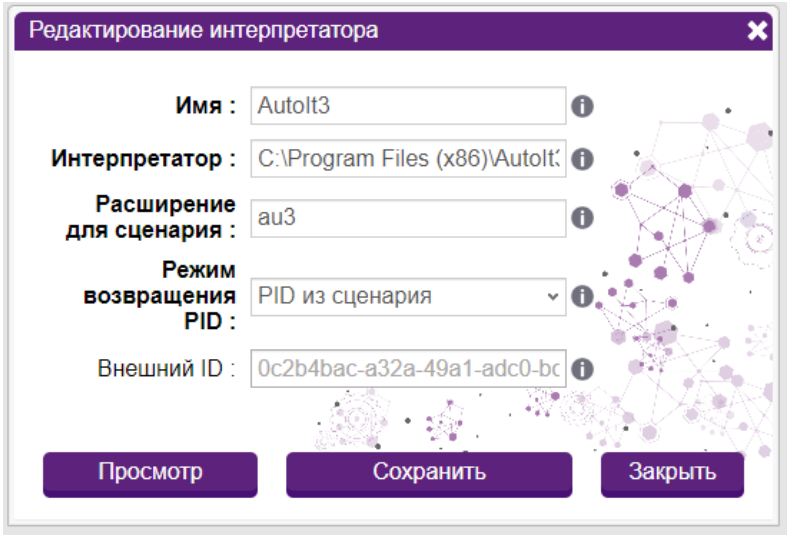


Рис. 3.12.3. Форма редактирования интерпретатора

Все поля, кроме Внешнего ID, доступны для редактирования. Чтобы сохранить изменения, необходимо нажать кнопку **Сохранить**. При нажатии кнопки **Закрыть** никаких изменений в карточке интерпретатора не произойдет.

3.12.3. Обновление таблицы интерпретаторов

Для обновления записей в таблице необходимо перейти в узел **Интерпретаторы** раздела **Управление системой** и щелкнуть мышью на кнопке обновления в правой верхней части таблицы.

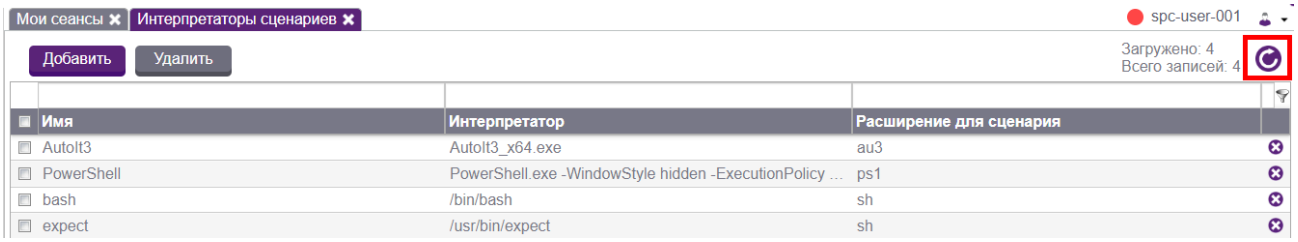


Рис. 3.12.4. Кнопка обновления информации

3.12.4. Удаление строки в таблице интерпретаторов

Для удаления строки из таблицы интерпретаторов щелкните мышью на кнопке удаления в правой части строки записи.

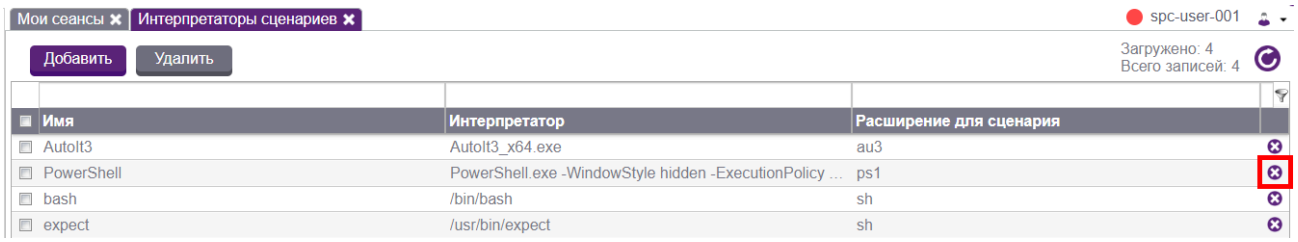


Рис. 3.12.5. Кнопка удаления строки в списке интерпретаторов

3.12.5. Удаление нескольких записей в таблице интерпретаторов

Для удаления нескольких записей из таблицы интерпретаторов одновременно следует выделить желаемые записи в таблице, установив флажок в соответствующем поле слева от поля **Имя**, после чего станет активной кнопка **Удалить**, расположенная сверху над таблицей.

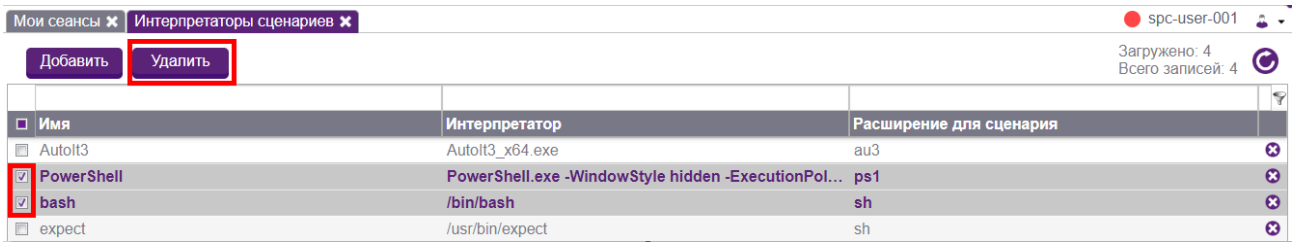


Рис. 3.12.6. Выбор двух записей таблицы и кнопка удаления

3.13. Управление приложениями

Пользователи управляют объектами администрирования при помощи инструментов администрирования (приложений), которые предварительно

настраивает технический администратор. Для настройки приложений и исполняемых сценариев необходимо перейти в узел **Приложения** раздела **Управление ресурсами**.

Окно узла **Приложения** содержит две таблицы: **Список приложений** и **Список сценариев**.

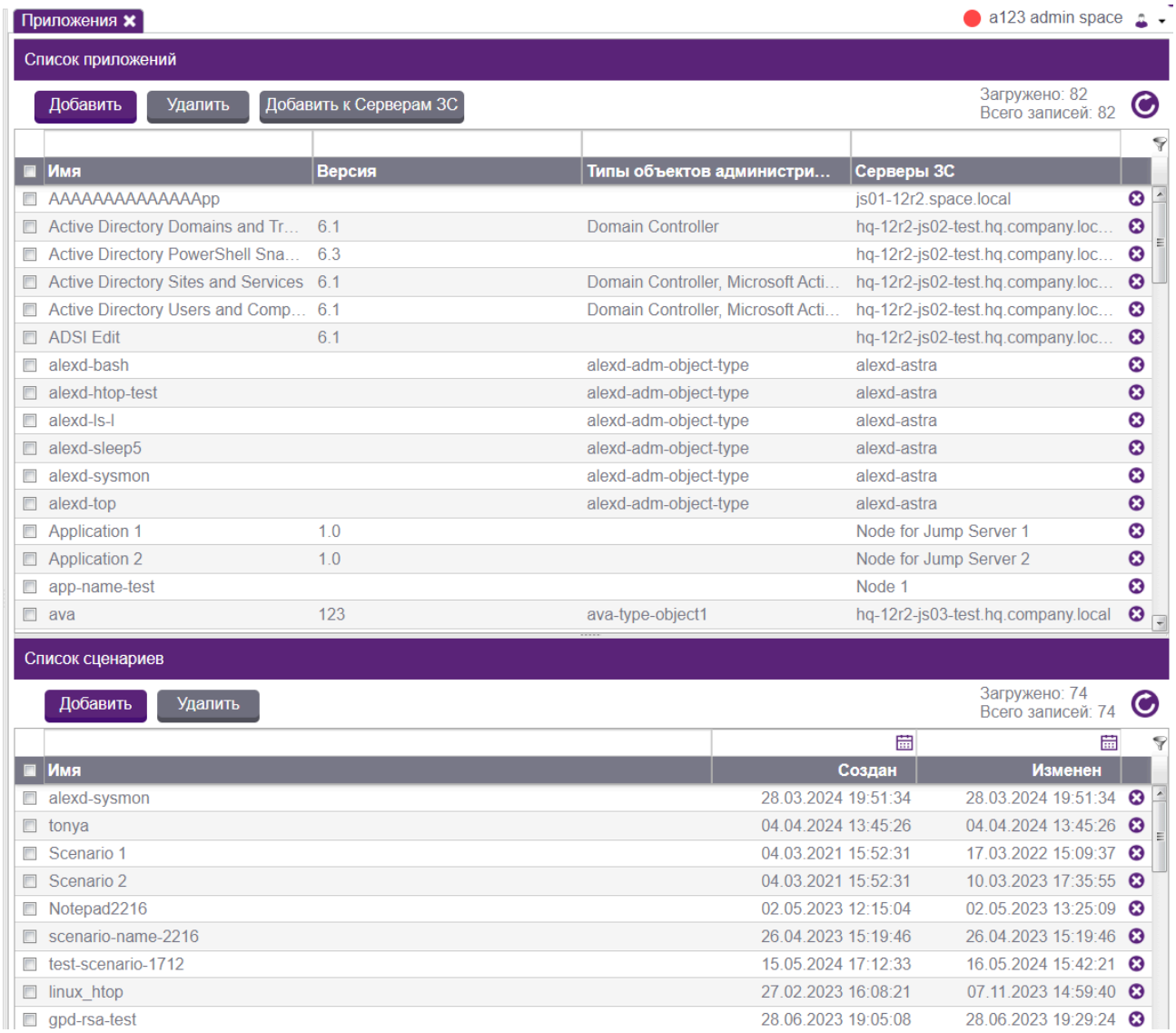


Рис. 3.13.1. Окно «Приложения»

Таблица **Список приложений** содержит следующие поля:

- Имя – наименование приложения;
- Версия – версия приложения;
- Типы объектов администрирования – разновидность объекта администрирования, определяющая правила работы с объектом;
- Серверы 3С – на которых присутствуют данные приложения.

Таблица **Список сценариев** содержит следующие поля:

- Имя – имя сценария;
- Создан – дата создания сценария;
- Изменен – дата изменения сценария.

В рамках настройки и управления приложениями и сценариями запуска приложений администраторы могут выполнять следующие действия:

- Добавлять приложение/сценарий;
- Редактировать приложение/сценарий;
- Обновлять таблицу приложений/сценариев;
- Удалять строку в таблице приложений/сценариев;
- Удалять несколько записей из таблицы одновременно;
- Задавать сервер 3С для нескольких записей одновременно.

3.13.1. Добавление приложения/сценария

Для добавления приложения необходимо перейти в узел **Приложения** раздела **Управление ресурсами** и щелкнуть мышью на кнопке **Добавить** на панели инструментов окна **Список приложений**.

На экране отобразится форма добавления приложения.

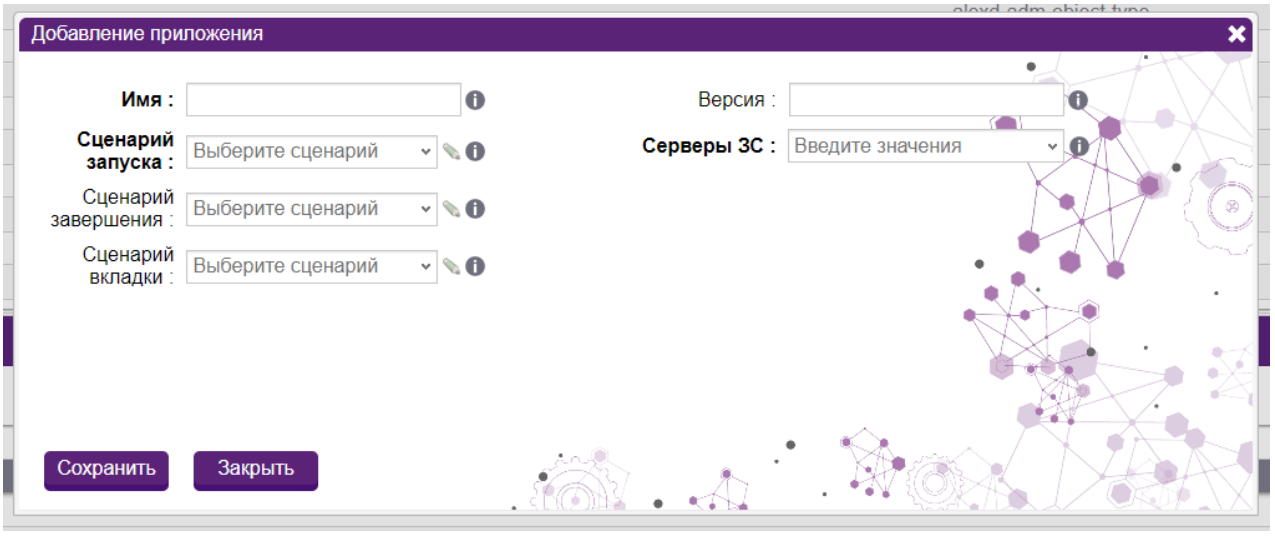


Рис. 3.13.2. Форма добавления приложений

Форма добавления приложения содержит в себе несколько полей (поля, обязательные для заполнения, выделены полужирным шрифтом):

- Имя (обязательное поле) – наименование приложения;
- Сценарий запуска (обязательное поле) – сценарий, по которому будет осуществляться запуск приложения;

- Сценарий завершения – сценарий, по которому будет осуществляться завершение приложения;
- Сценарий вкладки – сценарий, по которому будет осуществляться запуск приложения во вкладке;
- Версия – версия приложения;
- Серверы ЗС (обязательное поле) – перечень серверов ЗС, на которые будут установлены экземпляры приложения.

Для добавления сценария необходимо щелкнуть мышью на кнопке **Добавить** на панели инструментов окна **Список сценариев**. На экране отобразится форма добавления сценария.

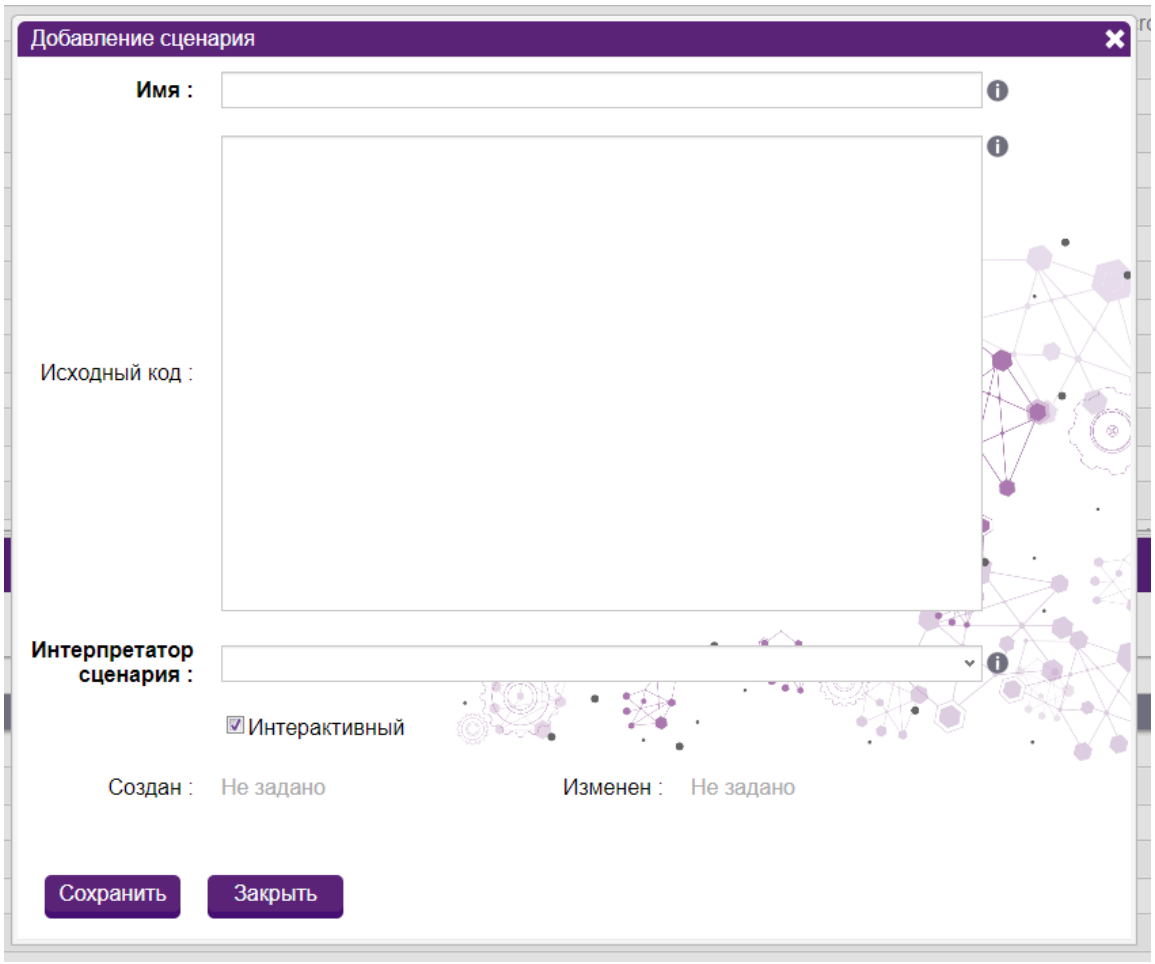


Рис. 3.13.3. Форма добавления сценария

Форма добавления сценария содержит следующие поля:

- Имя (обязательное поле) – наименование сценария;
- Исходный код – исходный код данного сценария;
- Интерпретатор сценария (обязательное поле) – интерпретатор, который будет преобразовывать исходный код сценария в последовательность нужных действий при использовании сценария.
- Интерактивный - возможность пользователя совершать действия в приложении с этим сценарием. Если галочка убрана, то пользователь не сможет ничего вводить или выбирать в приложении с таким сценарием, сеанс будет неинтерактивным.
- Создан - дата создания сценария.

- Изменен - дата последнего редактирования сценария.

При заполнении кода сценария существует ряд переменных — плейсхолдеров, которые используются в сценариях AutoIt для того, чтобы при запуске сценария они автоматически заменялись машиной на необходимую информацию (Эти параметры всегда присутствуют в модели данных и не указываются в **launch_param**):

Имя	Описание
termConnectionUuid	Идентификатор терминального соединения
sessionDescriptorUuid	Идентификатор сеанса
credential.username	Имя пользователя УЗ для сеанса.
credential.password	Пароль УЗ для сеанса.
credential.exclusive	Значение true/false, признак, что УЗ используется для Run as
credential.domain.name	Домен для УЗ (SHORT NAME)
credential.domainFqdn	FQDN домена для УЗ
adminObject.fqdn	Адрес объекта администрирования (FQDN)
adminObject.ip	IP адрес объекта администрирования. В явном виде для объекта администрирования не задается и может быть вычислен из adminObject.fqdn и DNS адресов тенанта.
parentPid	Pid процесса родительского сеанса, для которого открывается вкладка (подставляются с помощью LauncherManager)
parentRdcId	Remote desktop id родительского приложения (для случая, когда запуск сценария осуществляется во вкладке)
userAccountOtherId	Внешний ID пользователя sPACE, который запускает сеанс
userAccountName	Логин пользователя sPACE, который запускает сеанс
userAccountSearchFilter	Фильтр для поиск в LDAP пользователя sPACE, который запускает сеанс
userAccountDomainBaseDn	Base DN домена, в котором находится пользователь sPACE, который запускает сеанс

Имя	Описание
rdcId	Remote desktop connection id для компонента Launcher, запущенного в рамках данного сеанса

Также существует 3 типа сценариев:

id	Устанавливается в (FK)	Описание
Launch Scenario	application.launch_scenario_id application_instance.launch_scenario_id	Сценарий запуска приложения
Tab Scenario	application.tab_scenario_id application_instance.tab_scenario_id	Сценарий открытия вкладки в запущенном приложении
Clean Scenario	application.clean_scenario_id application_instance.clean_scenario_id	Сценарий очистки после выхода из приложения (для удаления временных файлов и освобождения ресурсов)

Пример создания сценария AutoIt

Подготовим шаблон для AutoIt сценария:

```
; AutoIt Version: 3.0
; Language: English
; Script Function:
; Opens Notepad, types in some text and then quits the application.
; Run Notepad ${test.value!"missingData"}
$processId = Run("notepad.exe")
ConsoleWrite("" & $processId & @CRLF)
    ; Wait for the Notepad to become active. The classname "Notepad" is monitored instead of the window title
WinWaitActive("[CLASS:Notepad]")
    ; Now that the Notepad window is active type some text
Send("Hello from Notepad.{ENTER}1 2 3 4 5 6 7 8 9 10{ENTER}Below are credentials from BD.{ENTER}Login is ${username}{ENTER}Password is ${password}{ENTER}")');
```

В тех местах где предполагается использовать значения из модели - вставляем placeholder вида ${имя!"значение_по_умолчанию"}. Возможно использовать простую форму для вставки параметров - ${имя}. Однако в этом случае, вы должны быть уверены, что такое значение будет обязательно присутствовать в модели данных, иначе возникнет исключительная ситуация и сценарий не будет сформирован.

Допускается присутствие в модели данных параметров, не имеющих placeholder в шаблоне. Исключительной ситуации это не вызовет. Но все параметры,

указанные в шаблоне, должны быть либо установлены в процессе обработки шаблона, либо иметь значения по-умолчанию.

Язык FTL допускает различные способы установки значений по-умолчанию, равно как и поддерживает конструкции программирования (if, циклы и т.п.). За подробностями следует обращаться к документации FTL.

Для более полной информации по созданию сценариев AutoIt, Bash или Expect рекомендуется почитать официальную документацию этого языка автоматизации.

3.13.2. Редактирование приложения/сценария

Для редактирования приложения необходимо дважды щелкнуть на строку нужного приложения в таблице приложений. В появившейся карточке приложения отображается вся информация о приложении.

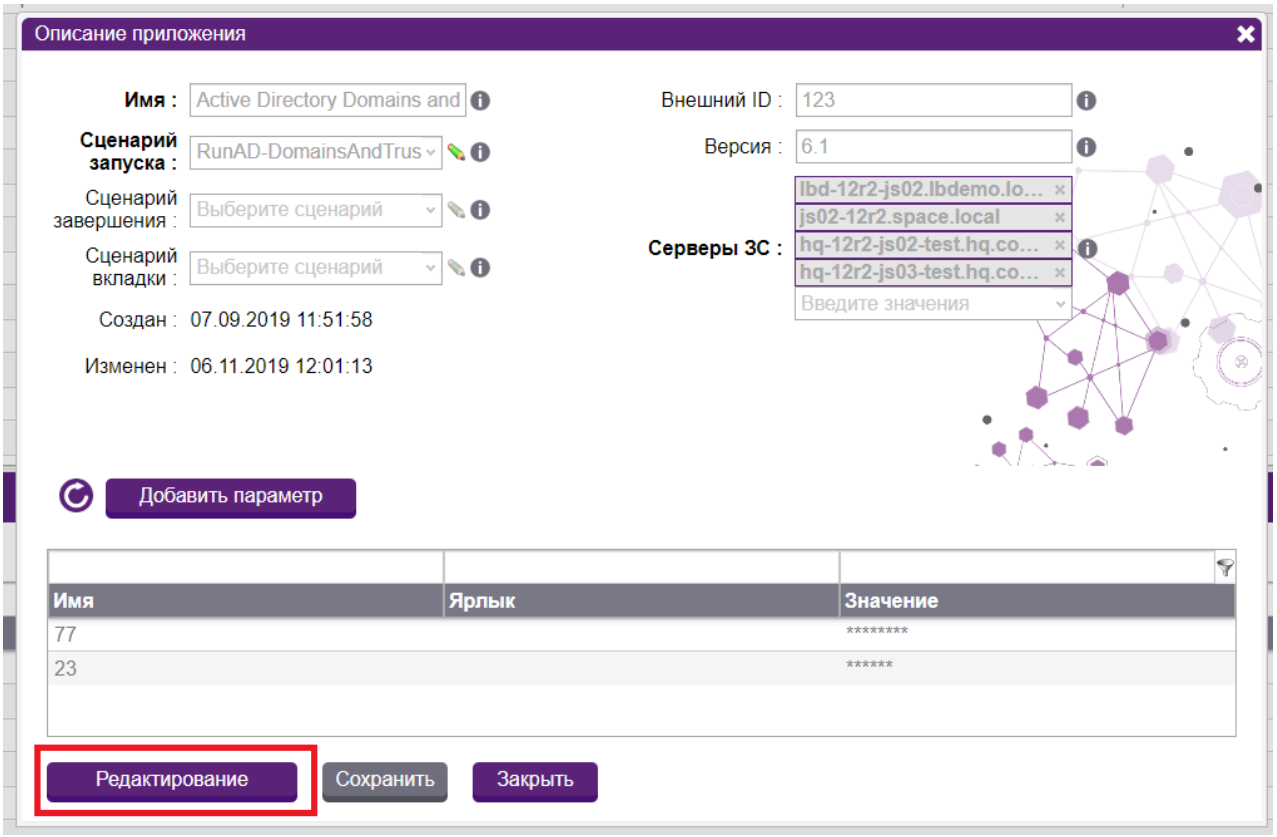


Рис. 3.13.4. Карточка приложения

При нажатии на кнопку **Редактирование** на экран выводится форма редактирования приложения.

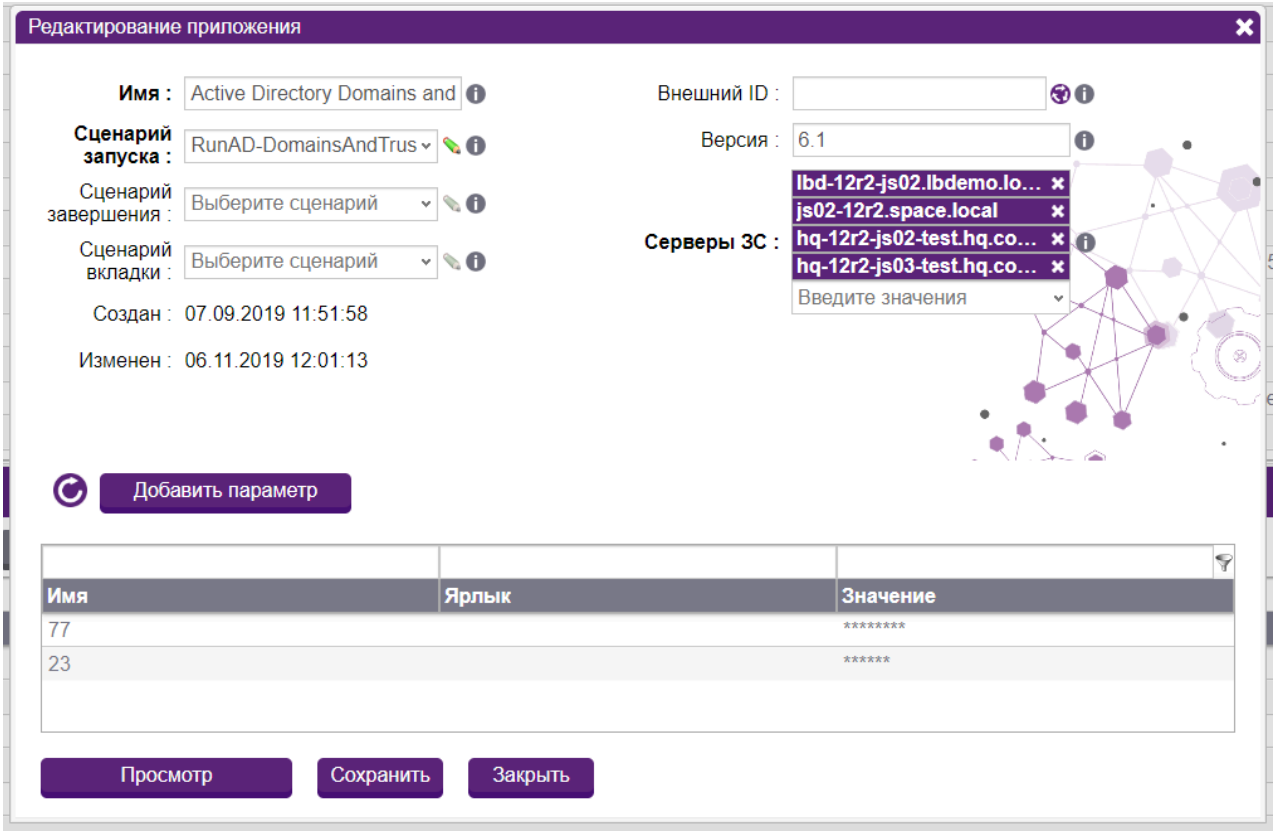


Рис. 3.13.5. Форма редактирования приложения

Все поля (кроме “Внешний ID”, "Создан" и "Изменен") доступны для редактирования. Чтобы сохранить изменения, необходимо нажать кнопку **Сохранить**. При нажатии кнопки **Закрыть** никаких изменений в карточке приложения не произойдет.

Также можно добавлять параметры приложения, для этого требуется нажать на кнопку **Добавить параметр**.

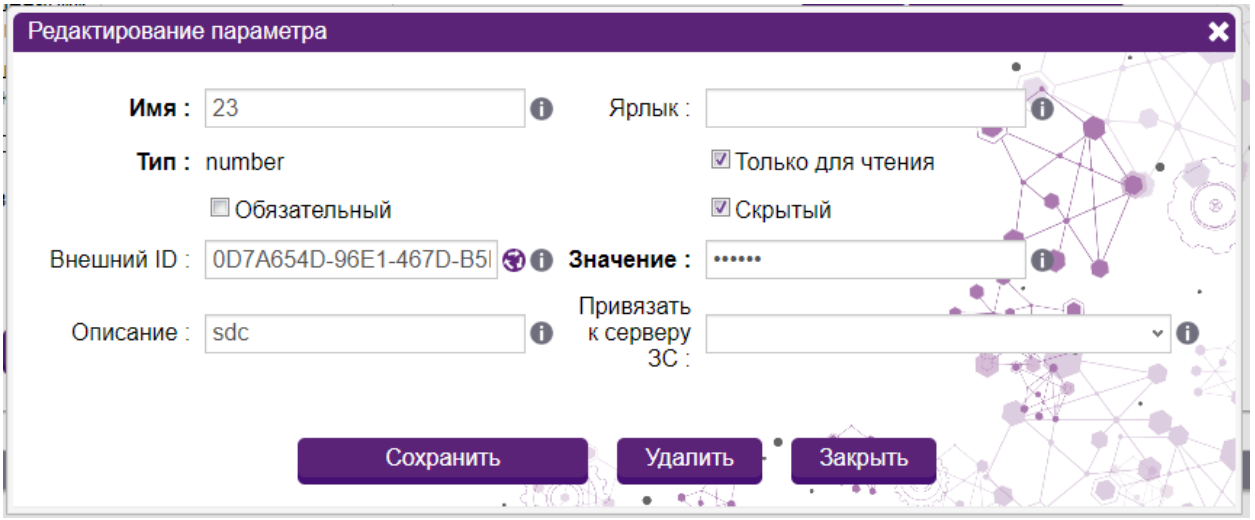


Рис. 3.13.6. Форма добавления/редактирования параметра

Форма "Добавить параметр" служит для добавления параметров к определенному приложению и имеет следующие поля:

- Имя (обязательное поле) – наименование параметра для приложения;
- Тип (обязательное поле) – тип данного параметра;
- Обязательный – индикатор, определяющий, является ли данный параметр обязательным для данного приложения;
- Внешний ID – идентификатор для интеграции внешних систем через API sPACE с данной сущностью;
- Описание – описание данного параметра;
- Ярлык – ярлык для данного параметра;
- Только для чтения – индикатор, показывающий, может ли пользователь изменить значение данного параметра при запуске данного приложения. Если он выключен, то пользователю будет предложено ввести параметр вручную при запуске наряда-допуска с соответствующим приложением. Если он включен, то параметр Значение будет помечен как обязательный;
- Скрытый – индикатор, определяющий, является ли данный параметр скрытым для данного приложения;
- Значение – значение данного параметра. Может вводиться пользователем при запуске сеанса, если не заполнено. Если выше в данной форме стоит галочка «Только для чтения», то значение будет обязательным полем, его надо будет заполнить при сохранении карточки приложения;
- Привязать к серверу 3С – имя сервера 3С, к которому привязан данный параметр;

Чтобы отредактировать уже созданный параметр приложения, требуется нажать на него в таблице параметров.

Для редактирования сценария необходимо дважды щелкнуть на строку объекта в таблице сценариев. В появившейся карточке сценария отображается вся информация о сценарии.

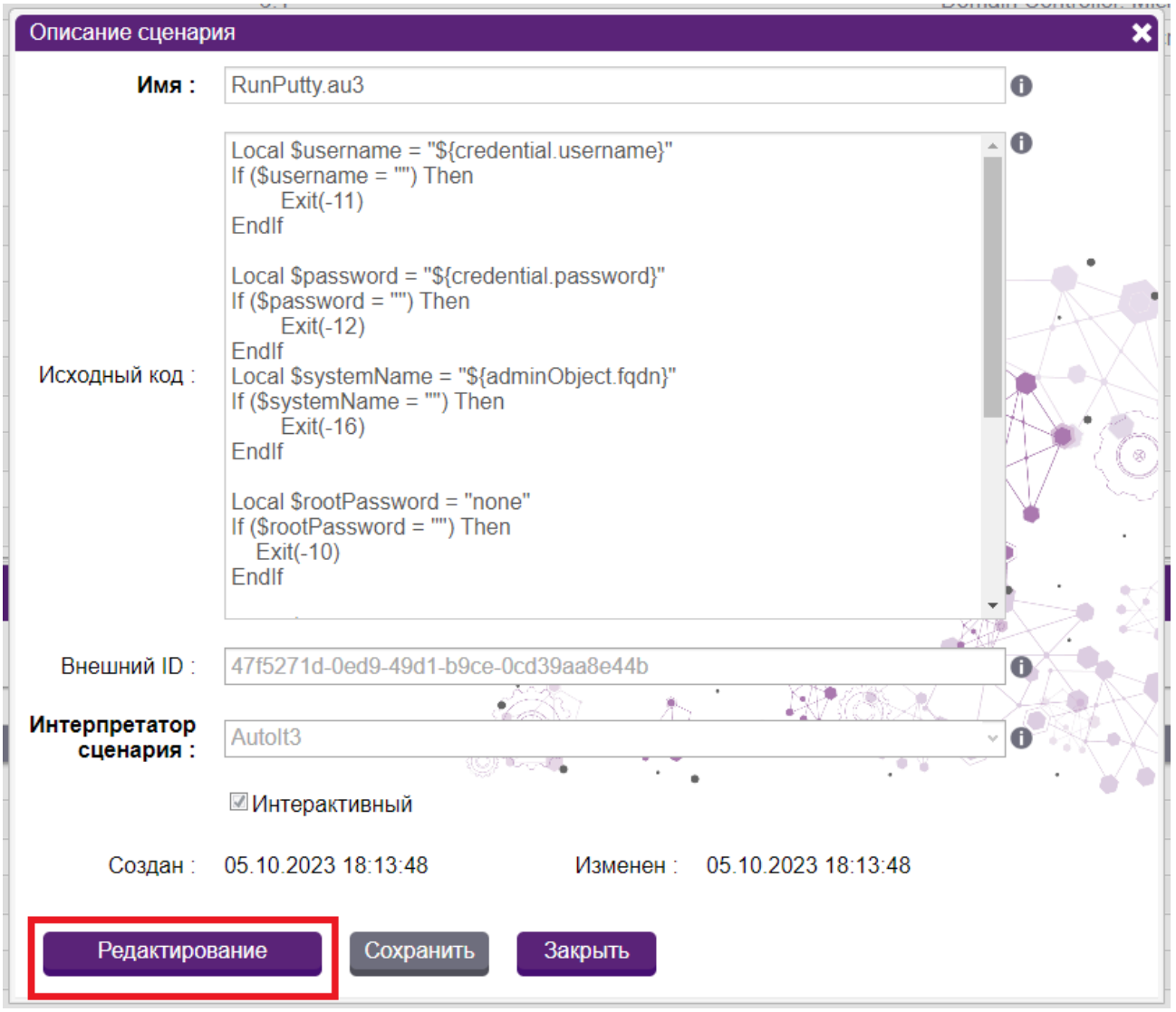


Рис. 3.13.7. Карточка сценария. Кнопка «Редактирование»

При щелчке на кнопке **Редактирование** на экран выводится форма редактирования сценария.

Все поля доступны для редактирования. Чтобы сохранить изменения, необходимо щелкнуть по кнопке **Сохранить**. При нажатии кнопки **Отмена** или **Закрыть** никаких изменений в карточке сценария не произойдет.

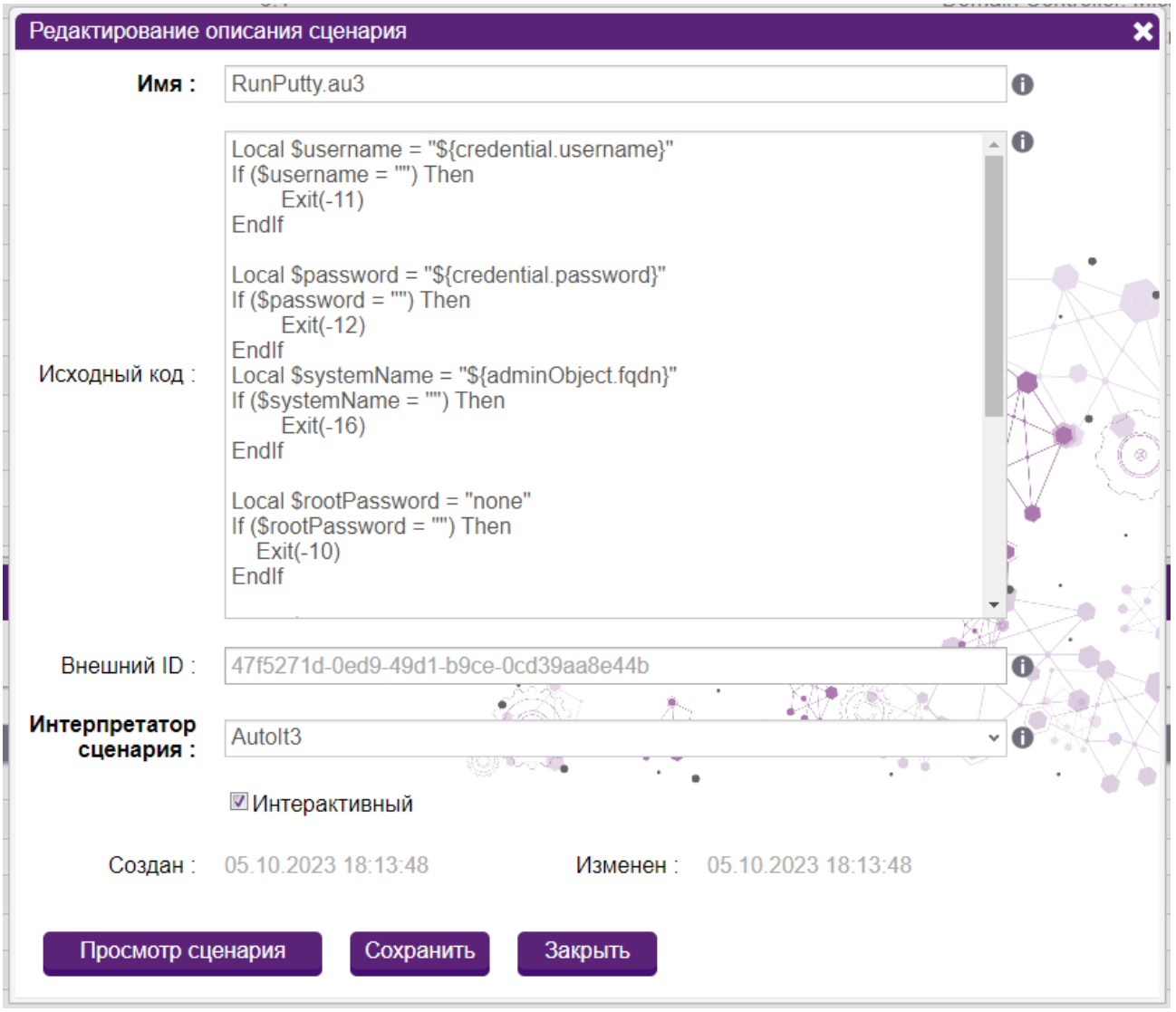


Рис. 3.13.8. Форма редактирования сценария

3.13.3. Обновление таблицы приложений/сценариев

Для обновления записей в таблицах приложений/сценариев необходимо щелкнуть мышью по кнопке обновления, располагающейся на панели инструментов узла.

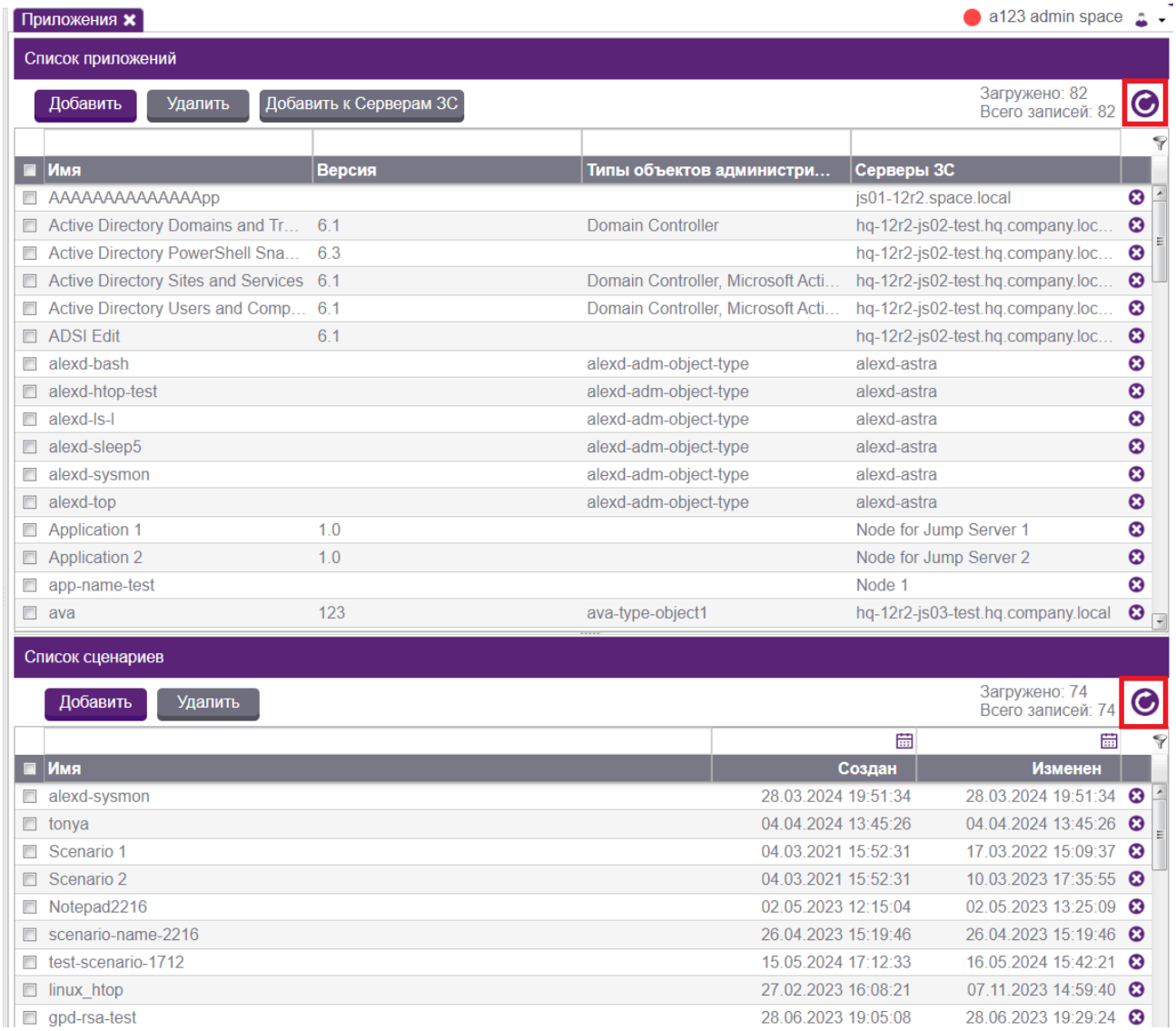


Рис. 3.13.9. Кнопка обновления информации

3.13.4. Удаление строки в таблице приложений/сценариев

Для удаления строки в таблице приложений/сценариев необходимо щелкнуть мышью по кнопке удаления, расположенной справа в строке объекта администрирования.

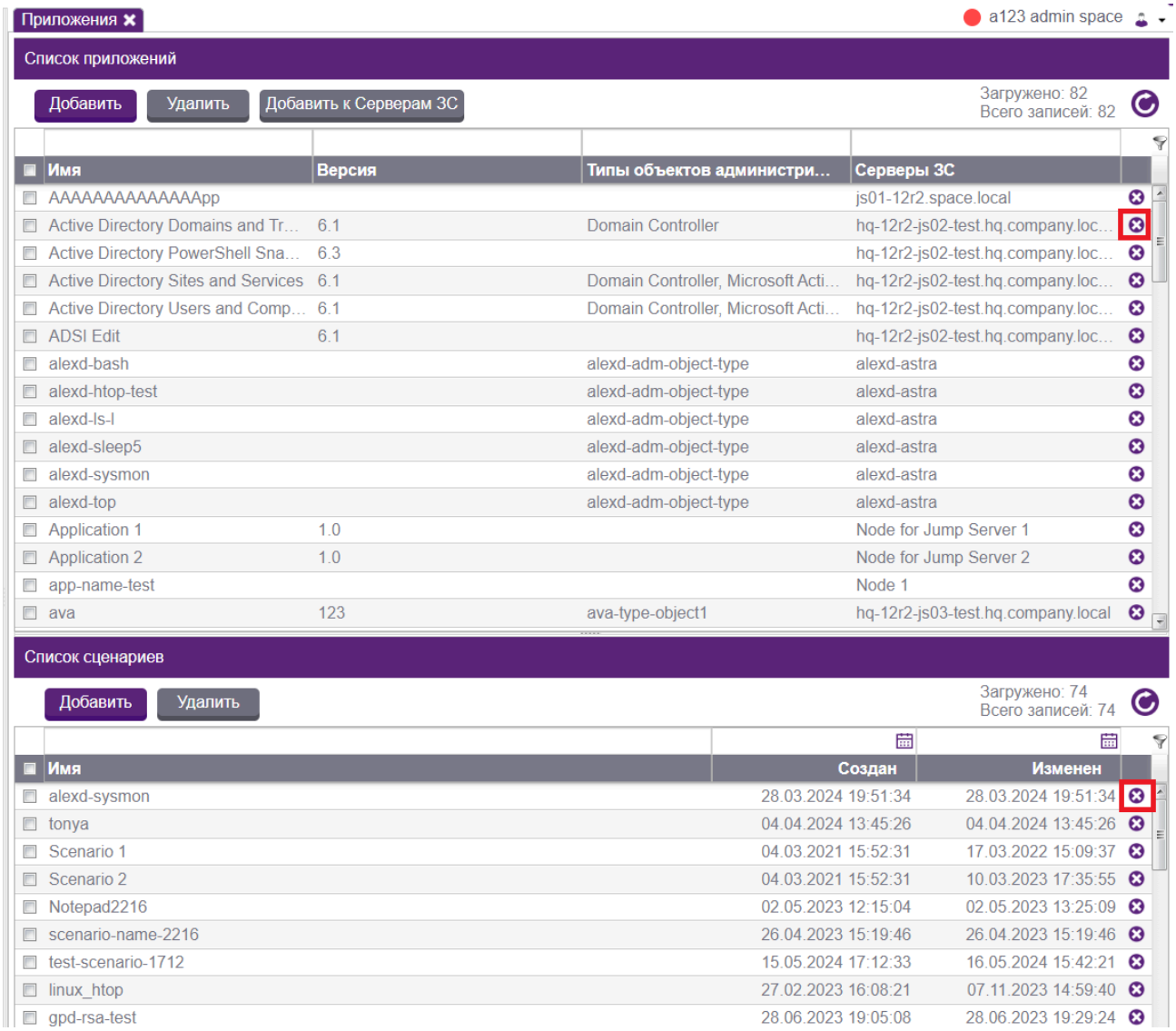


Рис. 3.13.10. Расположение кнопки удаления строки в списке приложений

3.13.5. Удаление нескольких записей из таблицы одновременно

Для удаления нескольких записей из таблицы приложений/сценариев одновременно следует выделить желаемые записи в таблице, установив флажок в соответствующем поле слева от поля **Имя**, после чего станет активной кнопка **Удалить**, расположенная сверху над таблицей.

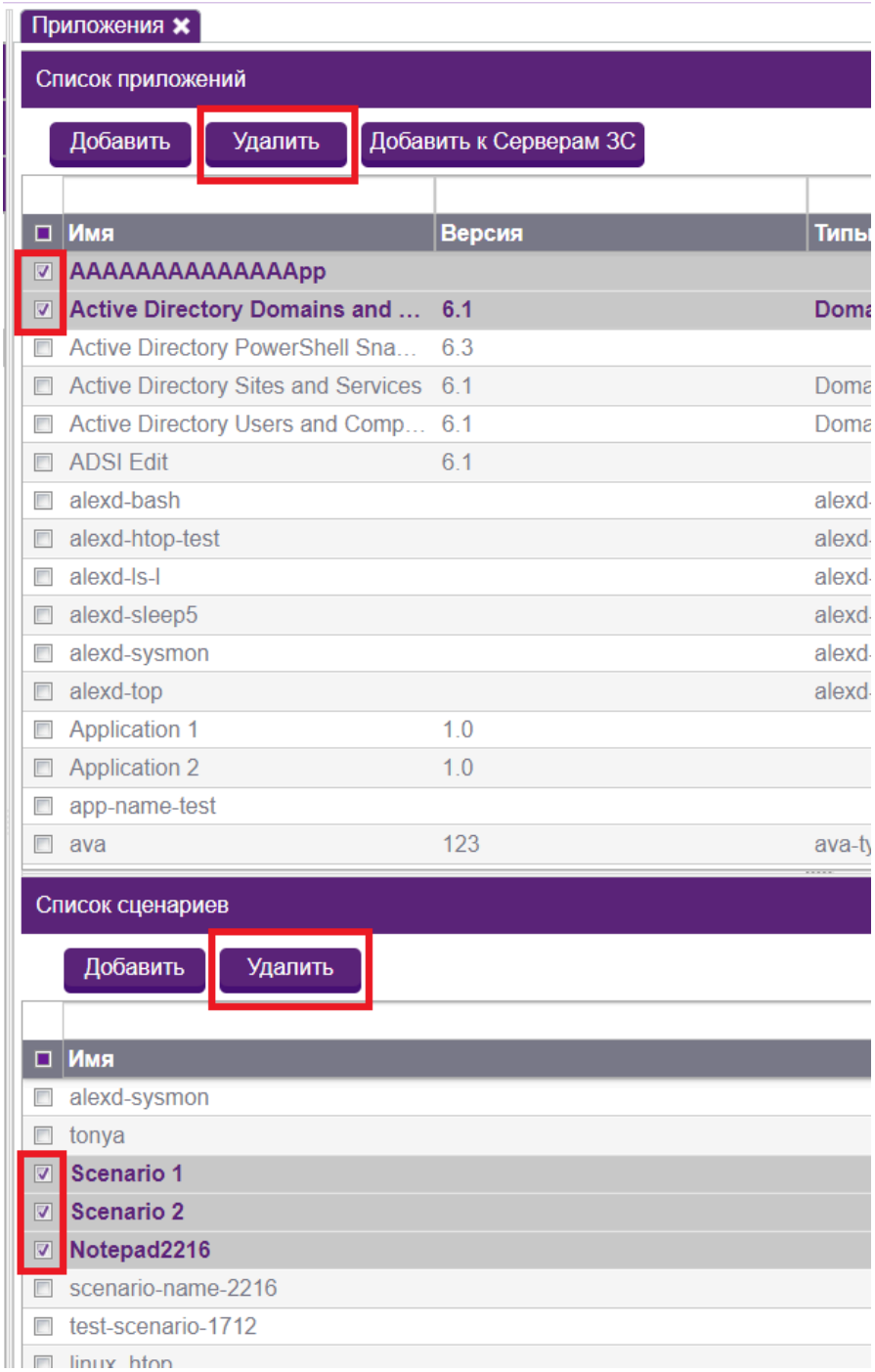


Рис. 3.13.11. Выбор нескольких записей таблицы и кнопка удаления

3.13.6. Одновременное добавление серверов 3С для нескольких приложений

Для одноовременного добавления серверов 3С для нескольких приложений сначала следует выделить желаемые записи в таблице галочкой слева, после чего станет активной кнопка **Добавить к Серверам 3С**, расположенная сверху над таблицей. После нажатия на данную кнопку необходимо будет выбрать сервера 3С из списка доступных.

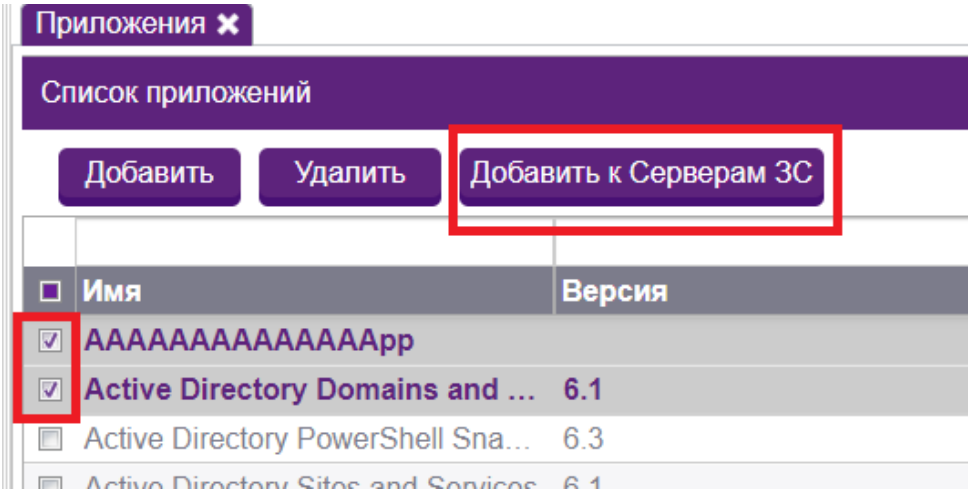


Рис. 3.13.12. Выбор двух записей таблицы и кнопка для добавления к Серверам ЗС

Откроется окно, где необходимо будет выбрать серверы ЗС из списка доступных и нажать на кнопку **Загрузить**.

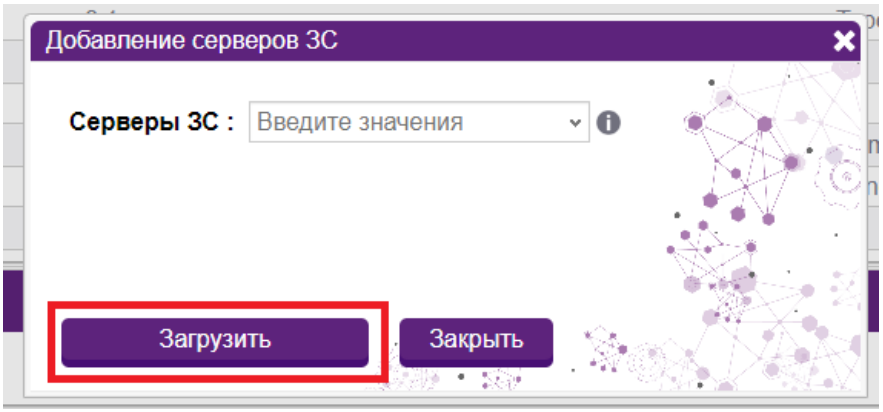


Рис. 3.13.13. Окно добавления приложений к Серверам ЗС

3.14. Управление серверами защищенной среды (ЗС)

Сервер Защищенной Среды Администрирования (PCF) — это выделенный сервер, на котором выполняется сеанс привилегированного доступа. Каждый сервер ЗСА поддерживает выполнение до 50 одновременных сеансов ПД. При увеличении числа привилегированных пользователей или увеличении количества задач по администрированию объектов администрирования может потребоваться настройка серверов ЗСА.

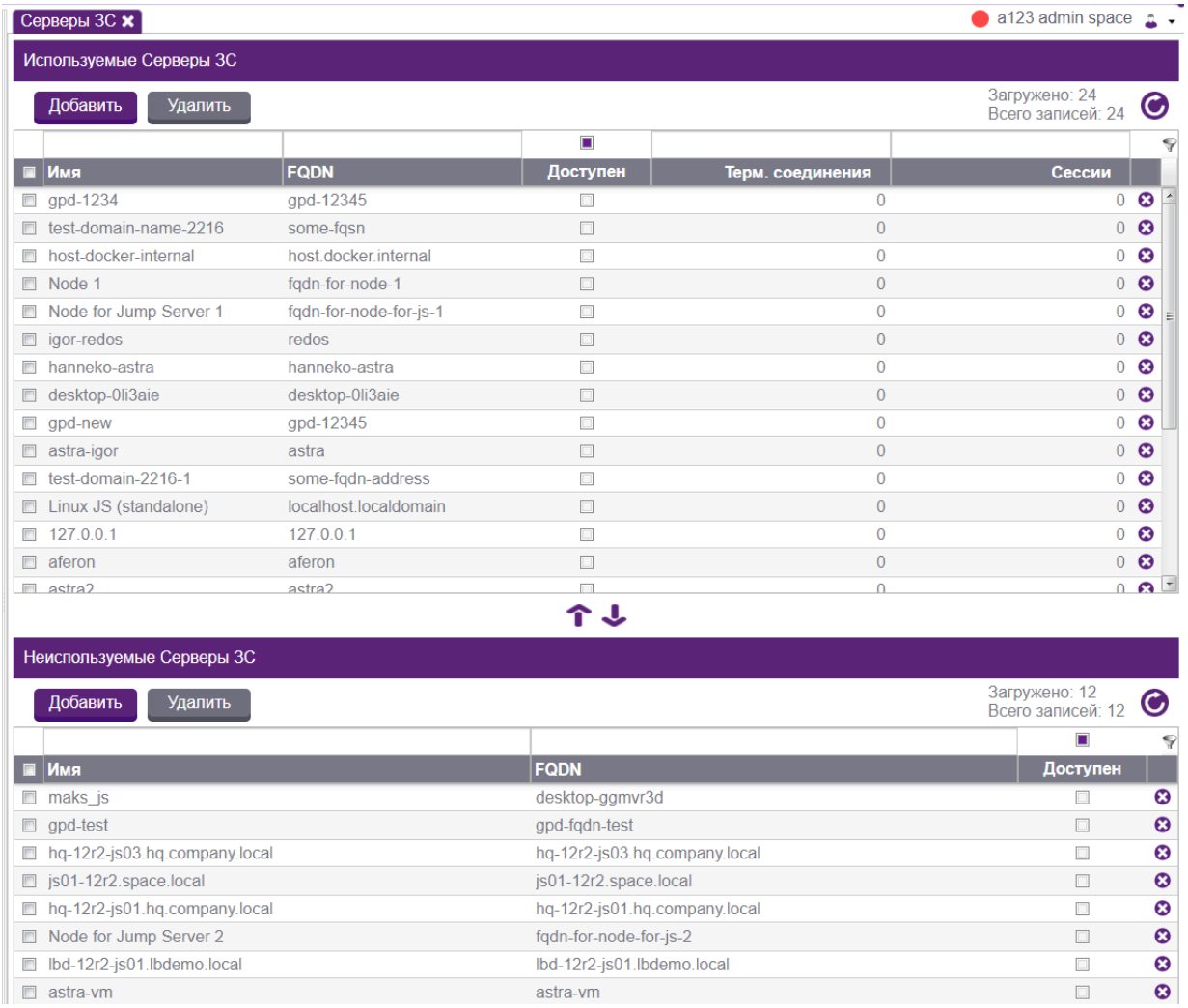


Рис. 3.14.1. Окно «Серверы ЗС» раздела «Управление ресурсами»

Вся информация об имеющихся в Системе серверах ЗСА отображается в узле **Серверы ЗС** раздела **Управление ресурсами** у технического администратора. Внешне раздел представлен в виде двух таблиц. В первой находятся используемые сервера ЗС (в балансировке), а во второй – неиспользуемые. Для смены состояния серверов необходимо воспользоваться специальными кнопками в виде стрелок.

Описание полей таблиц:

- Имя – наименование сервера;
- FQDN – Fully Qualified Domain Name, имя домена, не имеющее неоднозначностей в определении. Включает в себя имена всех родительских доменов иерархии DNS;
- Доступен – статус сервера;
- Терм. соединения – количество терминальных соединений на данном сервере в текущий момент;
- Сессии – сеансы, запущенные через данный сервер.

В рамках настройки и управления серверами ЗСА администраторы могут выполнять следующие действия:

- Добавлять сервера ЗС;
- Редактировать сервера ЗС;
- Обновлять таблицы серверов ЗС;
- Удалять строки в таблице серверов ЗС;
- Удалять несколько записей из таблицы серверов ЗС одновременно;
- Добавлять и удалять сервера из используемых.

3.14.1. Добавление сервера ЗСА

Для добавления сервера ЗСА необходимо щелкнуть мышью по кнопке **Добавить** на панели инструментов окна **Серверы ЗС**.

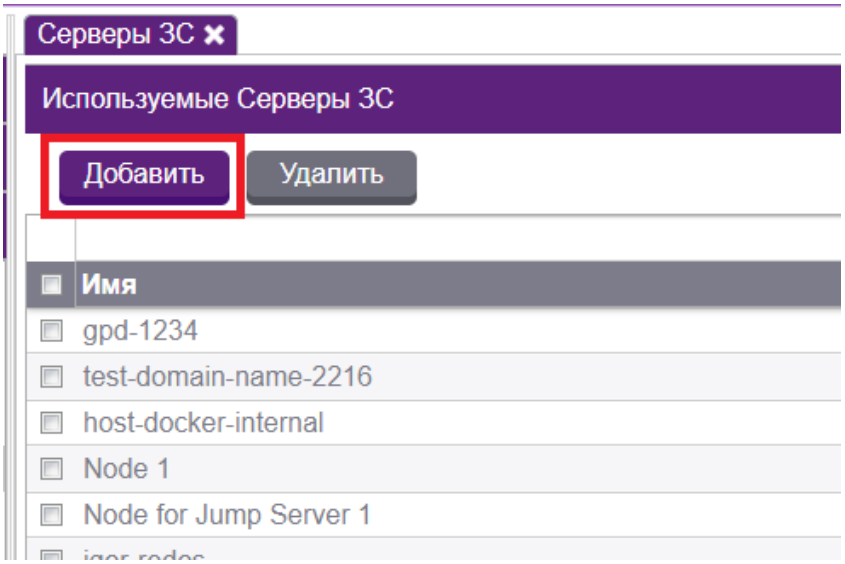


Рис. 3.14.2. Кнопка добавления сервера ЗС

На экране отобразится форма добавления сервера ЗС, в которой содержатся следующие поля (поля, обязательные для заполнения, выделены полужирным шрифтом):

- Имя (обязательное поле) – наименование сервера ЗС;
- FQDN (обязательное поле) – Fully Qualified Domain Name, имя домена, не имеющее неоднозначностей в определении. Включает в себя имена всех родительских доменов иерархии DNS.
- Внешний ID идентификатор для интеграции внешних систем через API sPACE с данной сущностью;

- Домен – наименование домена, в рамках которого находится сервер ЗС;
- Тип ОС (обязательное поле) – тип операционной системы (Windows или Linux);
- Тип подключения (обязательное поле) – тип подключения для добавляемого сервера ЗС;
- Система видеоаудита – тип системы видеоаудита для добавляемого сервера ЗС;
- RD gateway – значение параметра remote desktop gateway.

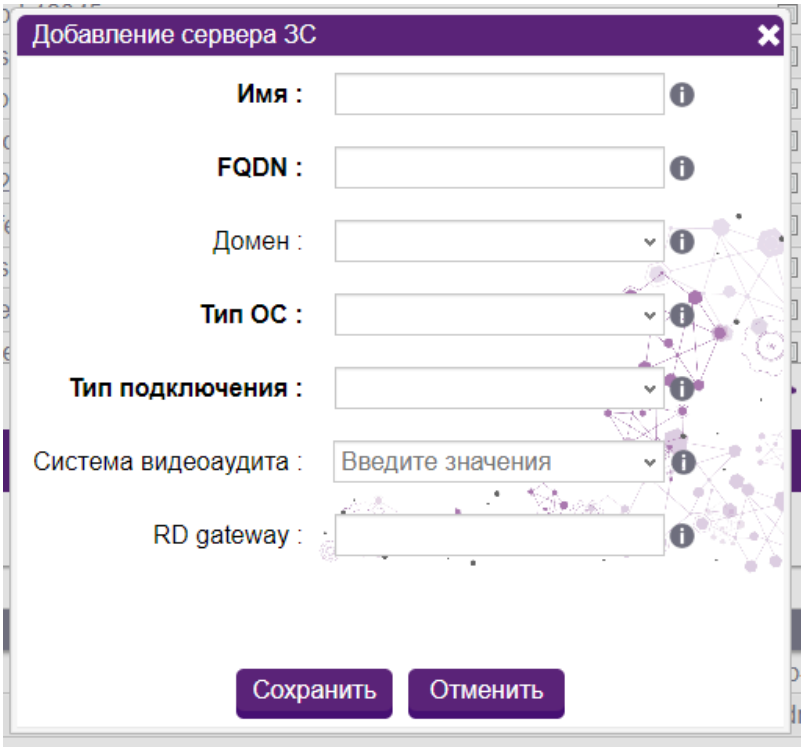


Рис. 3.14.3. Форма «Добавление сервера ЗС»

3.14.2. Изменение настроек сервера ЗСА

Для редактирования сервера ЗС необходимо дважды щелкнуть на строку объекта в таблице **Серверы ЗС**. В появившейся карточке сервера ЗС отображается вся информация о сервере.

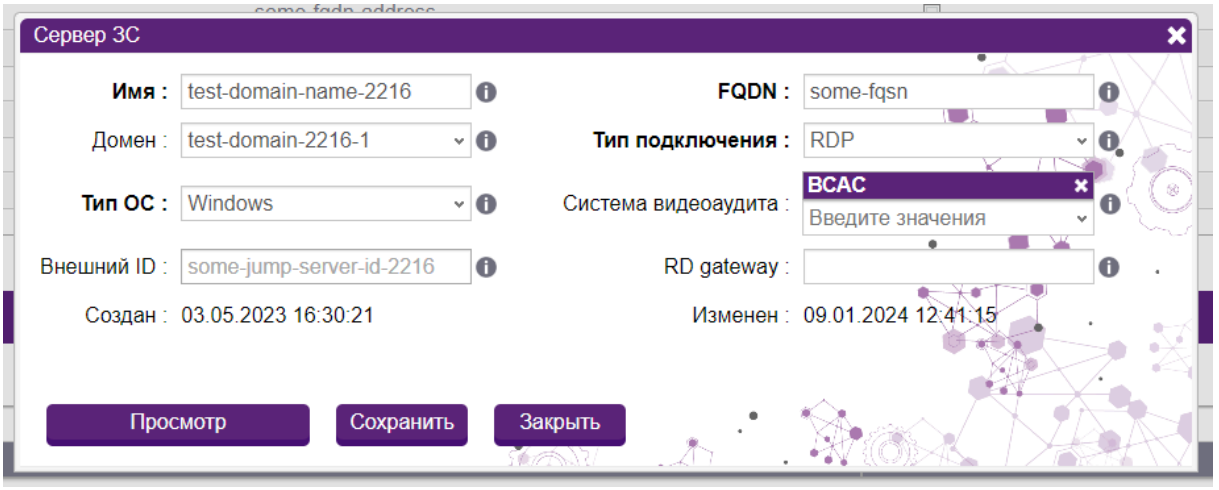


Рис. 3.14.4. Редактирование сервера ЗС

При необходимости изменить данные нужно щелкнуть на кнопке **Редактирование**, после чего на экран выводится форма изменения настроек сервера ЗС.

3.14.3. Дополнительная информация о выборе типа подключения

Тип подключения выбирается на основе того, каким будут запускаемые на данном СЗС сеансы.

Если это будут сеансы с графической оболочкой, то нужно выбирать тип подключения RDP независимо от того, является ли сервер ЗС машиной Windows или Linux.

Если это будут сеансы без графической оболочки, которые запускаются в командной строке рабочей машины пользователя, то нужно выбирать тип подключения SSH.

Ниже представлена более подробная сводная таблица с информацией о разных ОС, типах подключения и типах файлов, которые будут использованы для запуска сеанса.

Тип сервера ЗС	Тип подключения	Тип рабочей машины пользователя	Файл подключения
Windows	RDP	Windows	RDP файл для СЗС Windows
Linux	RDP	Windows	RDP файл для СЗС Linux
Windows	RDP	Linux	Строка XfreeRdp для СЗС Windows

Тип сервера ЗС	Тип подключения	Тип рабочей машины пользователя	Файл подключения
Linux	RDP	Linux	Строка XfreeRdp для СЗС Linux
Windows	SSH	Windows, Linux	-
Linux	SSH	Windows	ps1 файл
Linux	SSH	Linux	Строка SSH
Windows	Citrix	Windows, Linux	ica файл
Linux	Citrix	Windows, Linux	-

3.14.4. Обновление таблицы серверов ЗСА

Для обновления записей в таблице серверов ЗС необходимо щелкнуть мышью на кнопке обновления  , расположенной в правой верхней части таблицы.

3.14.5. Удаление строки в таблице серверов ЗСА

Для удаления строки в таблице сервер ЗС необходимо щелкнуть на кнопке удаления, расположенной справа в строке серверов ЗС.

3.14.6. Удаление нескольких записей из таблицы серверов ЗС одновременно

Для удаления нескольких записей из таблицы серверов ЗС одновременно необходимо сначала выделить нужные записи в таблице, установив флажок в соответствующем поле слева от поля **Имя**, после чего станет активной кнопка **Удалить**, расположенная сверху над таблицей.

3.15. Управление пользовательскими ролями

Вкладка **Пользовательские роли** раздела **Управление ресурсами** позволяет настроить пользовательские роли на портале sPACE. Можно создать как полностью новую роль (персональную), параметры которой задаст Технический администратор, так и изменить названия существующих ролей системы sPACE в

службах каталогов ОС. Очень важно, чтобы каждая роль (включая персональные) была предварительно там создана в и задана нужным пользователям.

В данном разделе администратор может осуществлять:

- Просмотр пользовательских ролей;
- Добавление пользовательских ролей;
- Редактирование пользовательских ролей;
- Обновление таблицы пользовательских полей;
- Удаление строки в таблице пользовательских ролей;
- Одновременное удаление нескольких записей из таблицы пользовательских ролей;
- Просмотр названий ролей AD в sPACE;
- Изменение названий ролей AD в sPACE.

Внешне раздел **Пользовательские роли** представлен в виде таблицы.

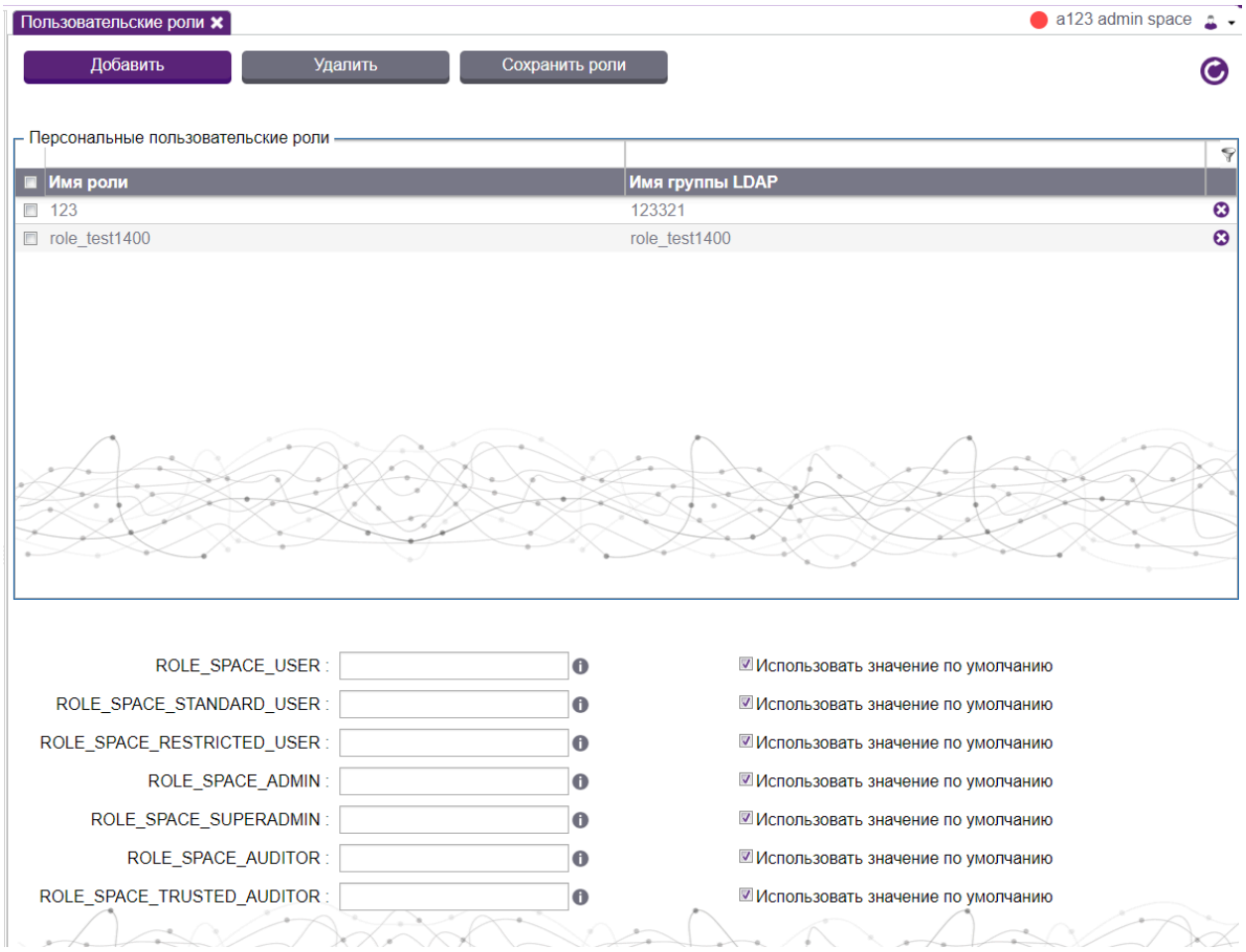


Рис. 3.15.1. Раздел «Пользовательские роли»

Описание столбцов приведено ниже.

- Имя роли – название роли в sPACE;
- Имя группы LDAP – название группы пользователей в Active Directory Users and Computers, которая соответствует этой роли на портале sPACE.

В списке ролей AD в первом столбце перечислены стандартные названия ролей sPACE.

3.15.1. Добавление новой пользовательской роли

Функционал добавления пользовательской роли вызывается нажатием на кнопку **Добавить**, расположенную в верхней части таблицы.

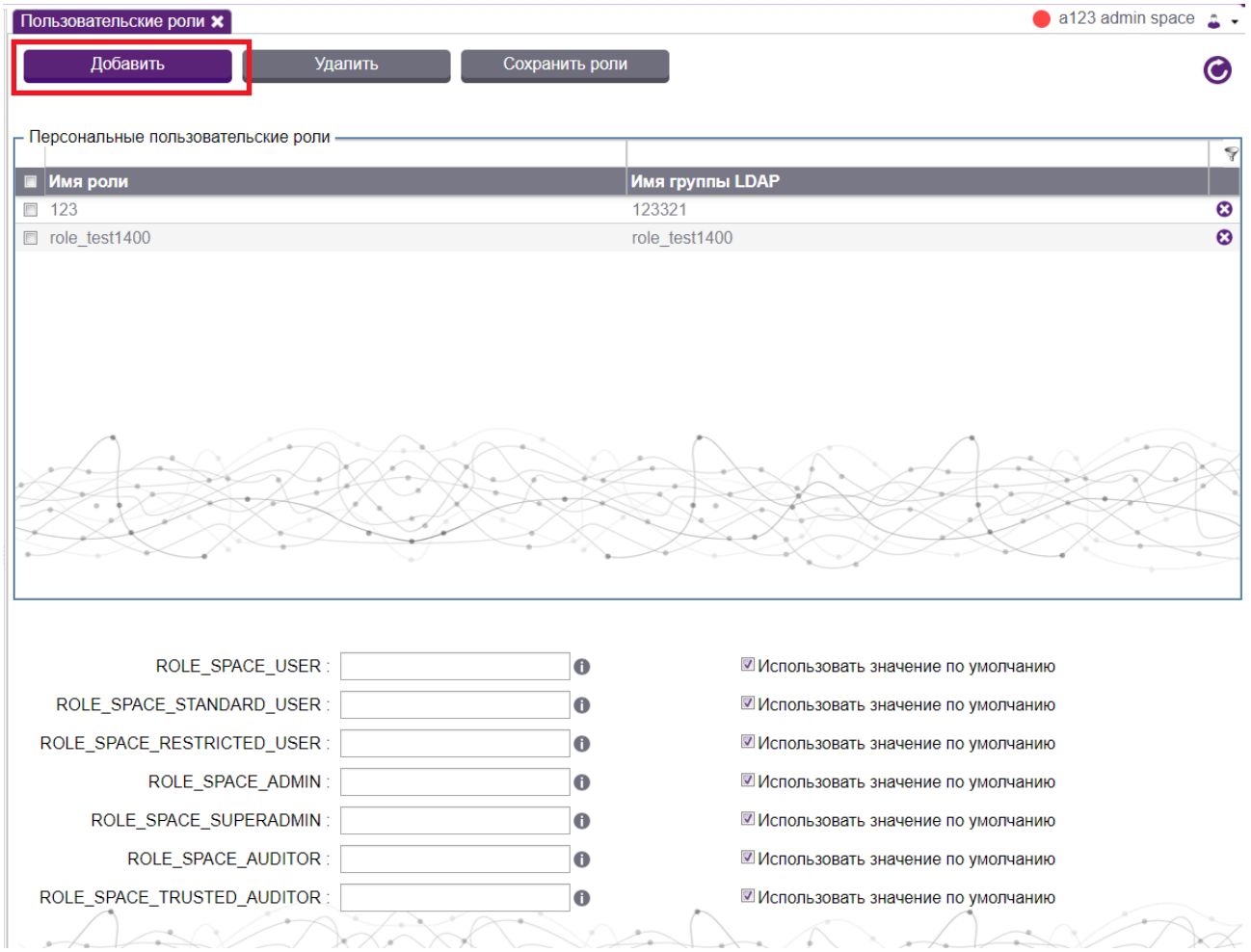


Рис. 3.15.2. Кнопка «Добавить» роль

При нажатии на эту кнопку пользователю будет выведена форма добавления роли. Она состоит из нескольких пунктов:

- Имя роли в sPACE (обязательное поле) – наименование данной роли в системе sPACE;

- Имя группы LDAP (обязательное поле) – название группы пользователей в Active Directory Users and Computers, которая соответствует этой роли на портале sPACE;
- Набор привилегий – возможности, которыми будут обладать пользователи, имеющие на портале эту роль.

После заполнения всех данных необходимо нажать на кнопку "Сохранить".

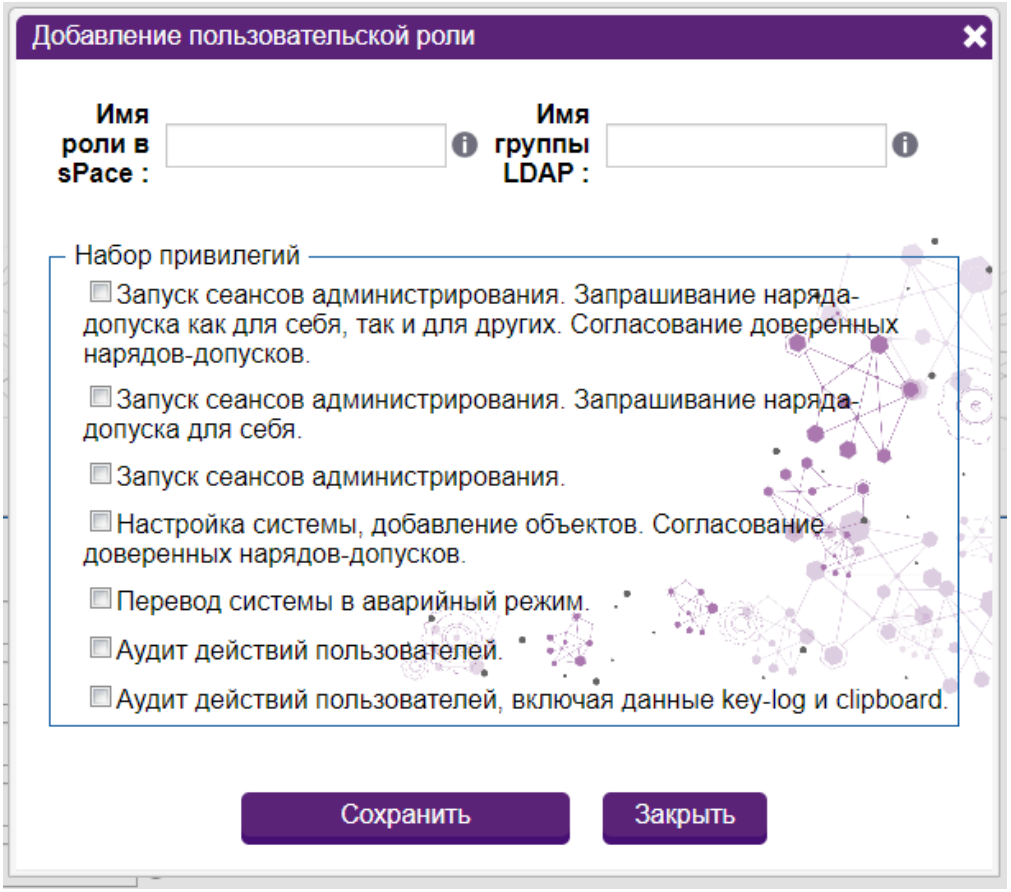


Рис. 3.15.3. Добавление роли

3.15.2. Редактирование пользовательской роли

Функционал редактирования пользовательской роли вызывается при двойном щелчке на наименовании роли в таблице.

Будет выведено окно с информацией о роли и активной кнопкой **Редактирование**. После нажатия на эту кнопку поля станут доступны для редактирования.

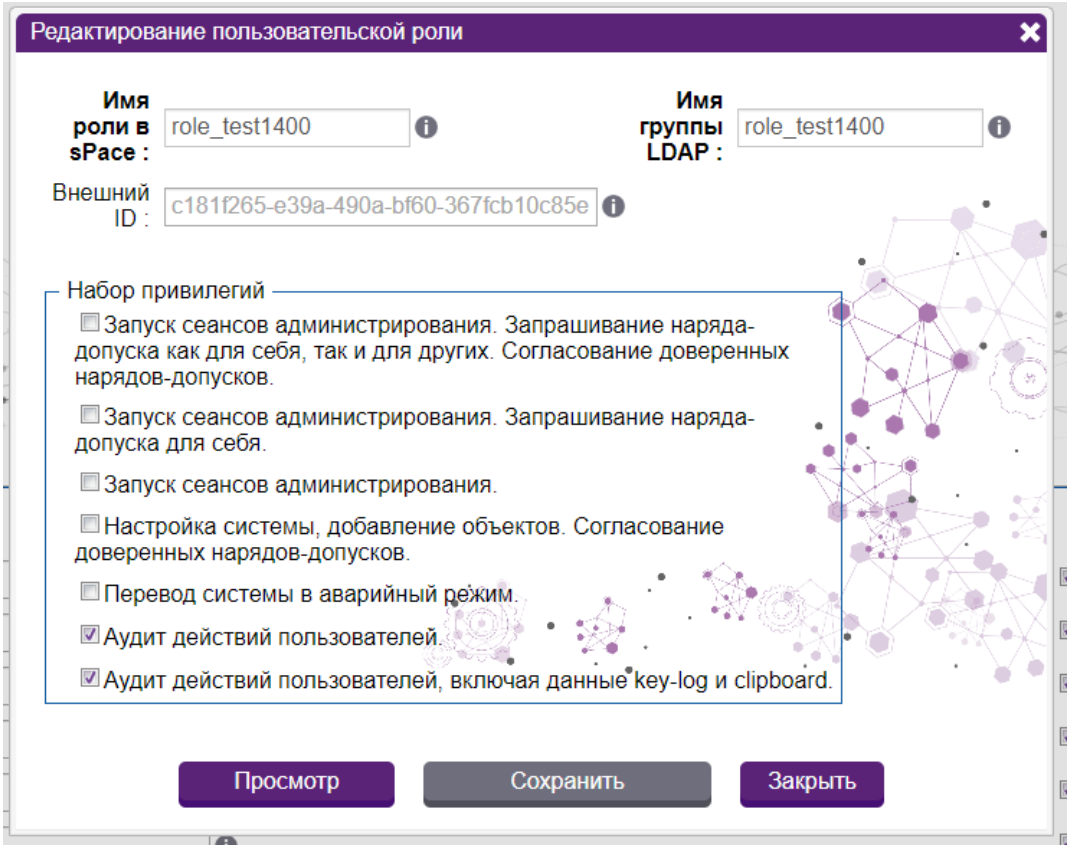


Рис. 3.15.4. Окно редактирования пользовательской роли

Все поля, кроме Внешнего ID, доступны для редактирования. Поля, выделенные жирным, являются обязательными для заполнения. Чтобы сохранить изменения, необходимо нажать кнопку **Сохранить**. При нажатии кнопки **Закрыть** никаких изменений в карточке пользовательской роли не произойдет.

3.15.3. Обновление таблицы персональных пользовательских ролей

Для обновления записей в таблице пользовательских ролей необходимо щелкнуть мышью на кнопке обновления , расположенной в правой верхней части таблицы.

3.15.4. Удаление строки в таблице персональных пользовательских ролей

Для удаления строки в таблице пользовательских ролей необходимо щелкнуть на кнопке удаления, расположенной справа в строке пользовательских ролей.

3.15.5. Удаление нескольких записей из таблицы персональных пользовательских ролей одновременно

Для удаления нескольких записей из таблицы пользовательских ролей одновременно необходимо сначала выделить нужные записи в таблице, установив

флажок в соответствующем поле слева от поля **Имя**, после чего станет активной кнопка **Удалить**, расположенная сверху над таблицей.

3.15.6. Изменение названия ролей

Перед тем, как изменить название стандартной роли в sPACE, требуется нажать на галочку у поля **Использовать значение по умолчанию**, чтобы убрать её. Тогда поле с новым названием для роли станет активно. В этом поле необходимо ввести название, а затем нажать на кнопку **Сохранить роли** вверху вкладки. Требуется удостовериться, что вы заранее создали роль с этим новым названием в Active Directory Users and Computers и задали её нужным пользователям, иначе роль станет для них недоступна. Внутренних пользователей это не коснется. Если на портале в момент изменения названия роли будут находиться активные пользователи, то им всем придется авторизоваться на портале заново.

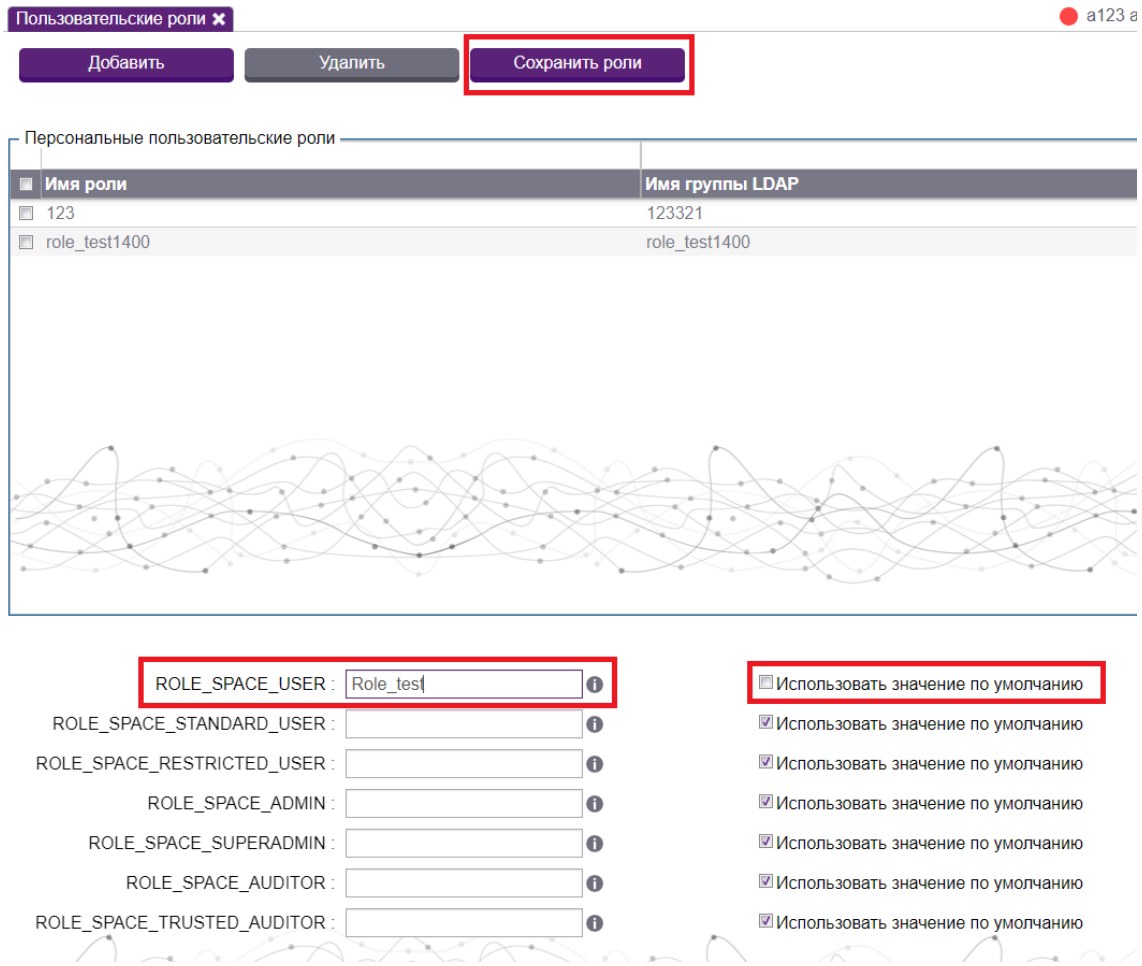


Рис. 3.15.5. Расположение кнопки «Сохранить роли»

Примечание: названия ролей, которые задаются на этой странице, должны совпадать во всех доменах. Например, если вы указали, что роль для пользователя называется NEW_SPACE_USER, то такая роль должна быть и в AD домена hq.company.local, и в AD домена lbdemo.local, а также и во всех остальных доменах.

3.16. Просмотр системных настроек

Узел **Системные настройки** раздела **Управление ресурсами** позволяет просмотреть текущие параметры и изменить некоторые настройки.

Внешне раздел "Системные настройки" выглядит следующим образом:

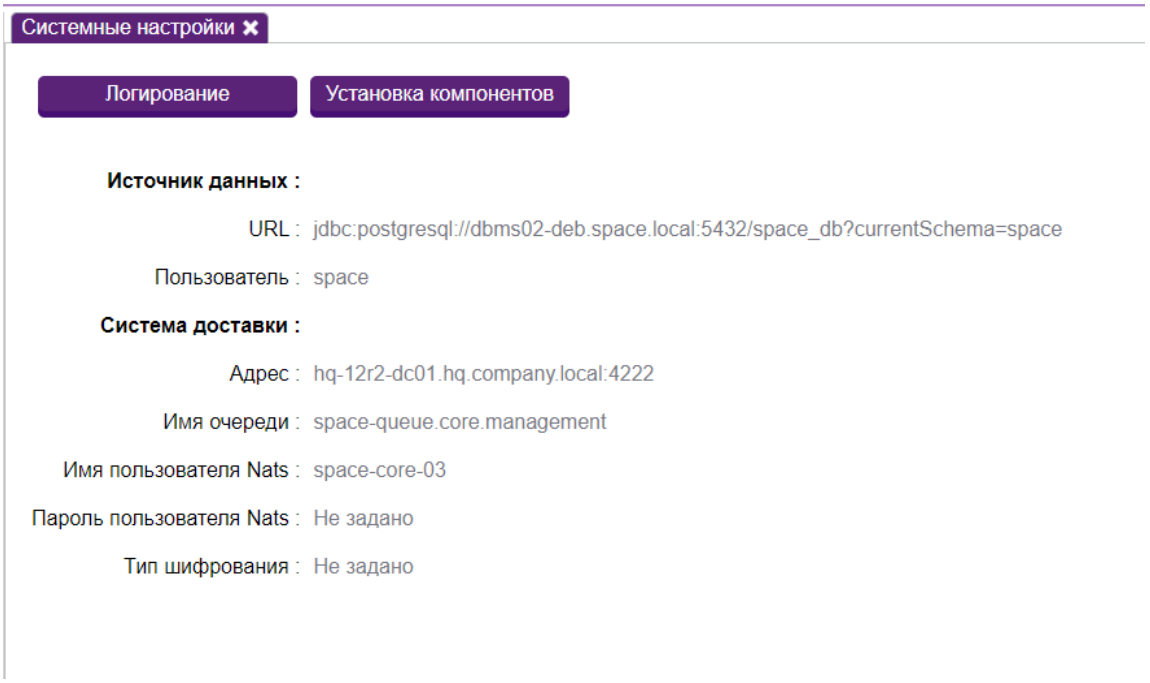


Рис. 3.16.1. Раздел «Системные настройки»

В нём можно узнать перечисленные ниже параметры:

Источник данных:

- URL – URL базы данных, являющейся источником информации для системы;
- Пользователь – пользователь, под которым происходит подключение к источнику данных.

Система доставки:

- Адрес - адрес расположения серверов системы доставки.
- Имя очереди - имя очереди для взаимодействия с системой доставки.
- Имя пользователя Nats - имя пользователя, под которым происходит подключение к Nats.
- Пароль пользователя Nats - пароль пользователя, под которым происходит подключение к Nats.
- Тип шифрования - тип шифрования, выбранный в системе.

3.16.1. Изменение настроек уровня логирования

Для редактирования настроек уровня логирования необходимо щелкнуть на кнопку **Логирование** вверху страницы.

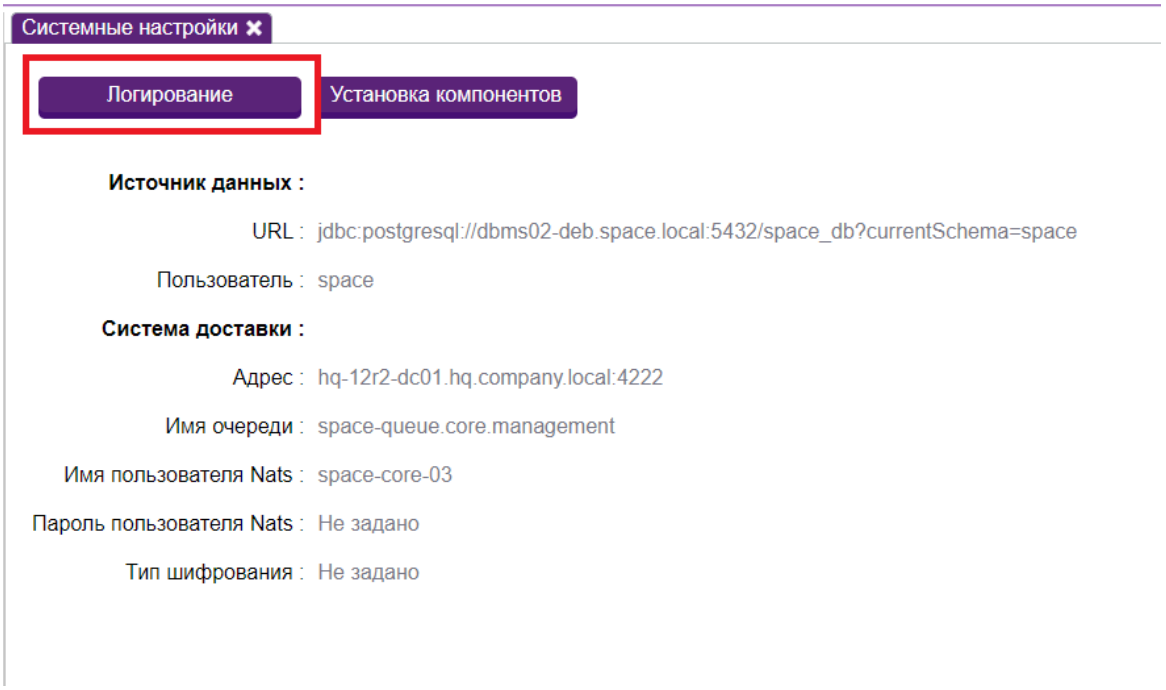


Рис. 3.16.2. Кнопка «Логирование»

Откроется окно настройки логирования. Данное окно позволяет выбрать уровень логирования для различных компонентов системы sPACE. Необходимо выбрать новые параметры, затем нажать на кнопку **Сохранить**.

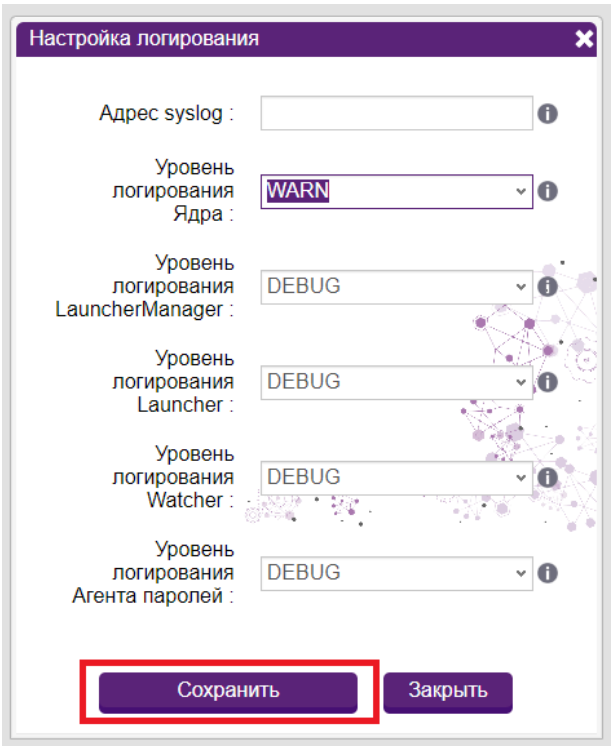


Рис. 3.16.3. Кнопка «Сохранить»

3.16.2. Удаленное управление компонентами

Данный функционал позволяет удаленно управлять компонентами системы, например, устанавливать или удалять серверы ЗС и Ядра, не заходя при этом на соответствующие машины.

Для того, чтобы открыть окно управления компонентами, необходимо нажать на кнопку **Установка компонентов** вверху страницы. Откроется соответствующее окно.

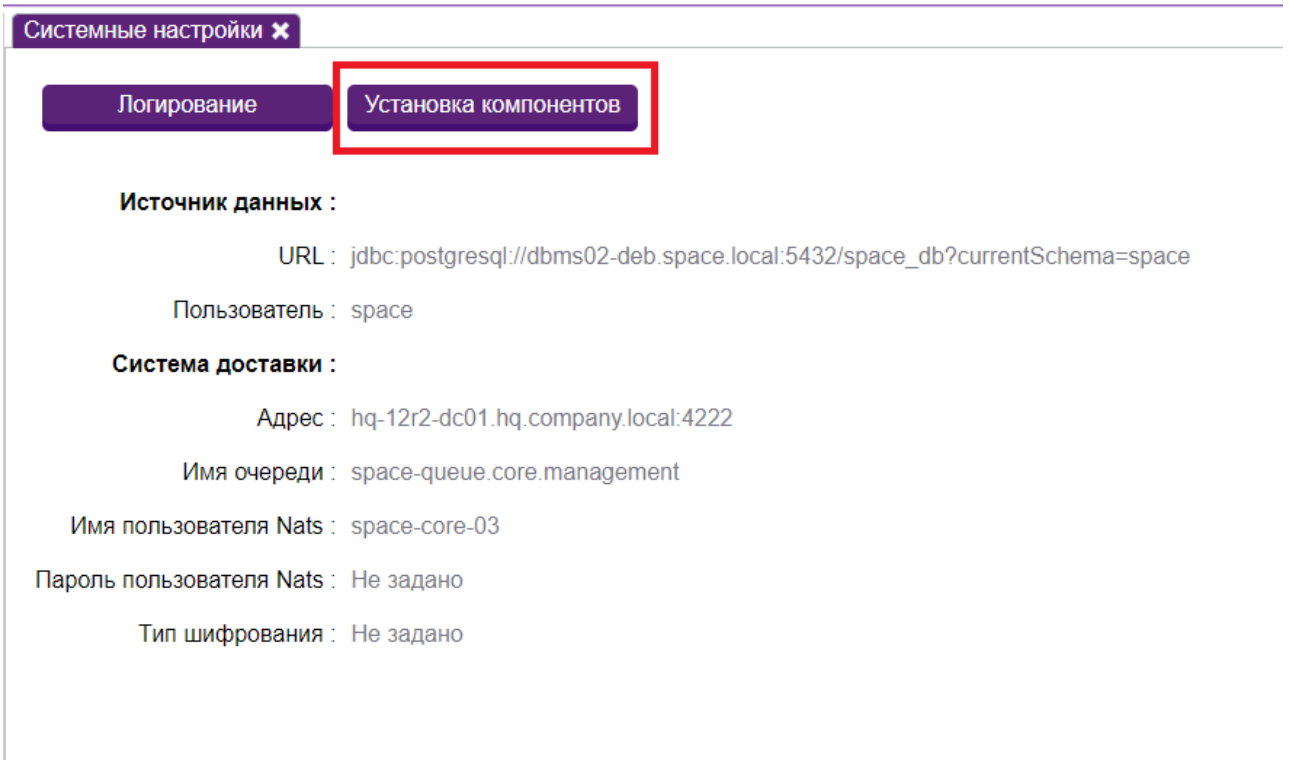


Рис. 3.16.4. Кнопка «Установка компонентов»

В графе **Действие** нужно выбрать, установка/удаление какого компонента потребуется. В зависимости от этого окно слегка изменяется. Для установки оно выглядит следующим образом: в ячейке **Параметры целевой системы** нужно указать данные машины нового сервера ЗС или Ядра, на которой будет произведена установка. В ячейке **Параметры Ядра** нужно указать данные Ядра, с которого происходит текущее подключение к порталу. После заполнения всех полей требуется нажать на кнопку **Выбрать и установить**, выбрать во всплывающем окошке на машине пользователя файл дистрибутива, после чего будет произведена установка, результат которой окажется выведен в графу **Результат**.

При удалении нужно указать аналогичные параметры за исключением параметров Ядра.

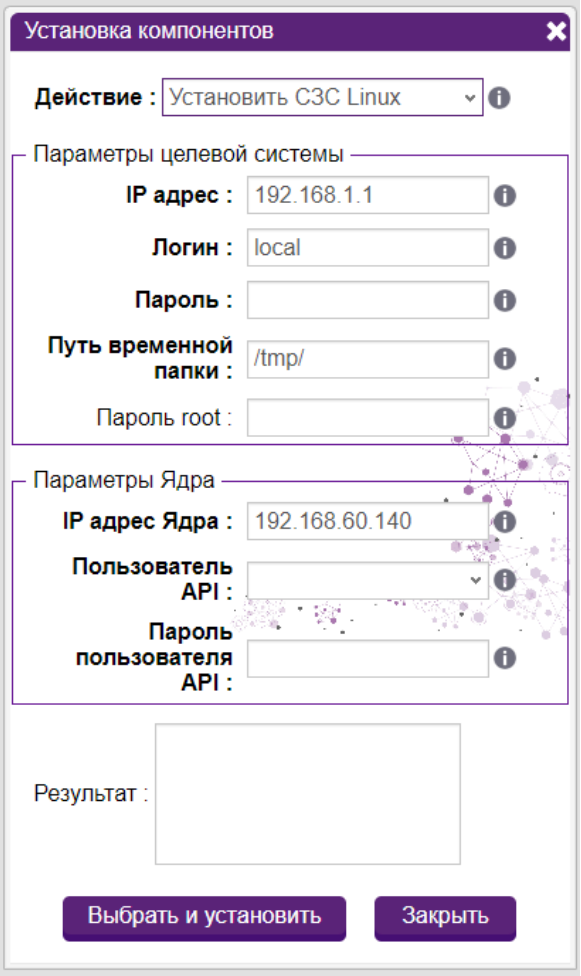


Рис. 3.16.5. Удаленная установка сервера 3С Linux

3.17. Управление параметрами фильтрации

Вкладка **Параметры фильтрации** в узле **Журнал событий** раздела **Управление ресурсами** у технического администратора служит для того, чтобы настраивать уведомления для администраторов или других уполномоченных пользователей об определенных действиях на портале.

Страница **Параметры фильтрации** позволяет техническому администратору:

- Просматривать параметры фильтрации;
- Добавлять/редактировать параметры фильтрации;
- Обновлять страницу параметров фильтрации;
- Удалять параметры фильтрации;
- Одновременно удалять несколько записей из таблицы параметров фильтрации.

3.17.1. Просмотр параметров фильтрации

Внешне раздел представлен в виде таблицы со списком параметров.

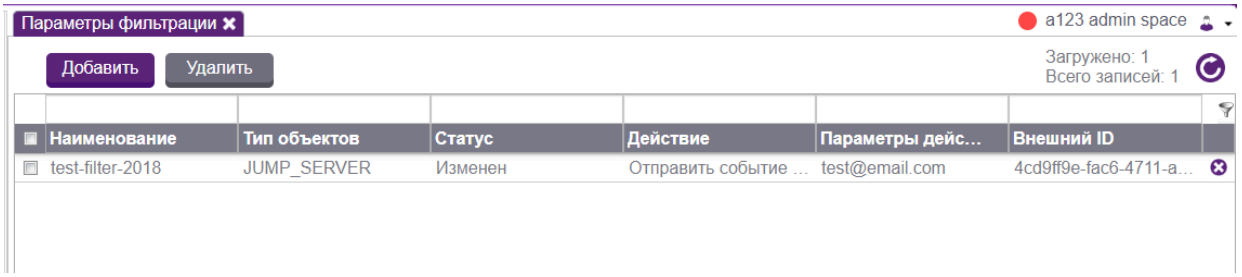


Рис. 3.17.1. Страница «Параметры фильтрации»

Описание параметров фильтрации:

- Наименование - название параметра фильтрации.
- Тип объектов - тип объекта, на действия с которым настроен параметр фильтрации.
- Статус - действие, совершаемое с этим объектом, после которого приходит уведомление.
- Действие - то, каким образом уведомляется администратор или другой пользователь.
- Параметры действия - адрес или электронная почта, куда приходит уведомление.
- Внешний ID - для интеграции сторонних систем с API sPACE.

Добавление нового параметра фильтрации

Функционал добавления параметра фильтрации вызывается нажатием на кнопку **Добавить**, расположенную в верхней части таблицы.

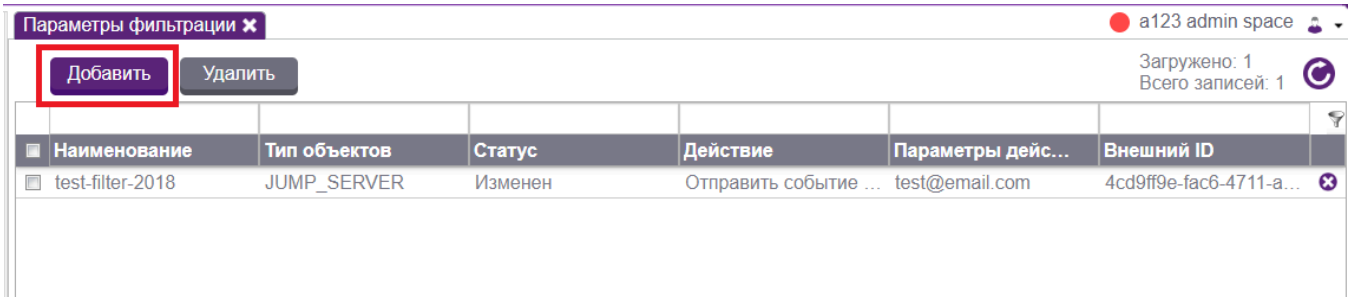


Рис. 3.17.2. Кнопка «Добавить» параметр фильтрации

При нажатии на эту кнопку пользователю будет выведена форма добавления параметра фильтрации. Она состоит из нескольких пунктов:

- Наименование (обязательное поле) - название параметра фильтрации.

- Параметры фильтрации по полю "Описание" - если нужно настроить дополнительно, можно указать это в поле "Описание" объектов.
- Тип объектов - тип объекта, на действия с которым настроен параметр фильтрации.
- Статус - действие, совершаемое с этим объектом, после которого приходит уведомление.
- Идентификатор пользователя - какой пользователь должен совершить это действие. Если поле оставлено пустым, то условие применяется ко всем пользователям.
- Уровень логирования - уровень логирования, на котором должно произойти действие.
- Действие (обязательное поле) - то, каким образом уведомляется администратор. Можно выбрать отправку уведомления по сети логом или на электронную почту.
- Адрес/Почта (обязательное поле) - дополнительное поле, которое появляется после выбора действия. В зависимости от выбранного действия (по сети логом или отправка по почте) здесь требуется указать адрес или электронную почту, куда будет отправлено уведомление для администратора.

После заполнения всех данных необходимо нажать на кнопку **Сохранить**.

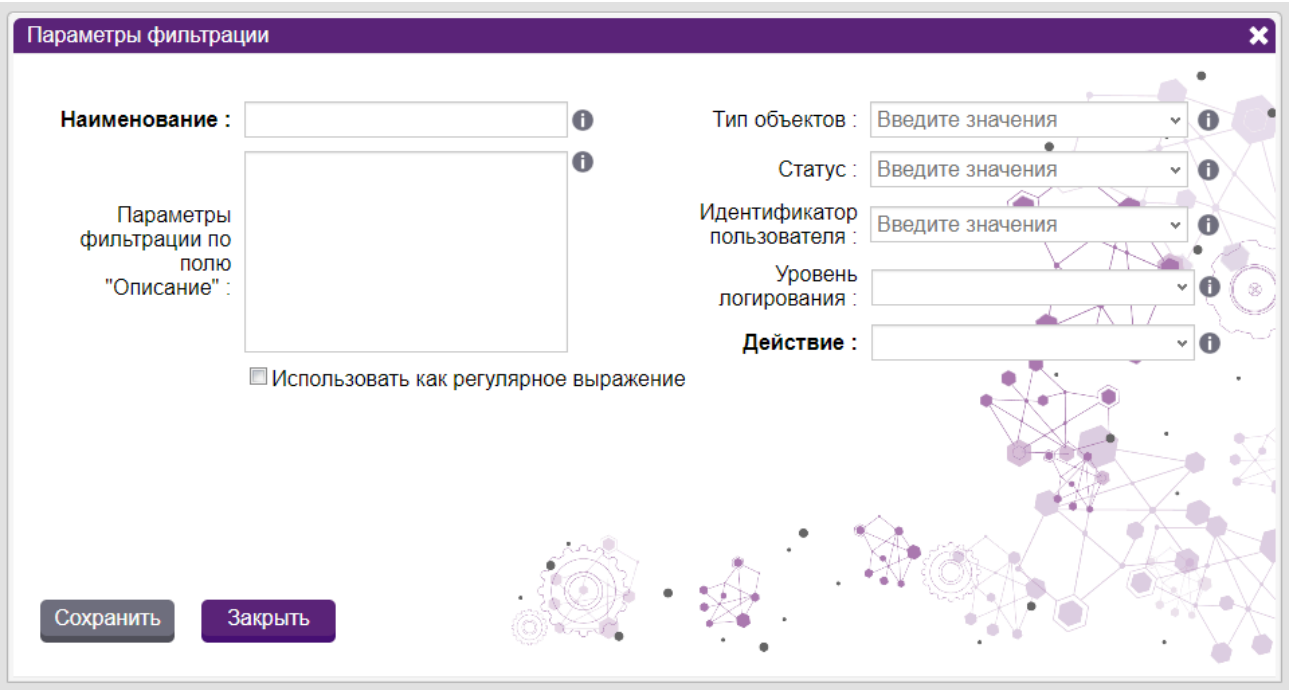


Рис. 3.17.3. Форма «Добавление параметра фильтрации»

3.17.2. Редактирование параметра фильтрации

Функционал редактирования параметра фильтрации вызывается при двойном щелчке на наименовании параметра в таблице.

Будет выведено окно с информацией о параметре и активной кнопкой **Редактирование**. После нажатия на эту кнопку поля станут доступны для редактирования.

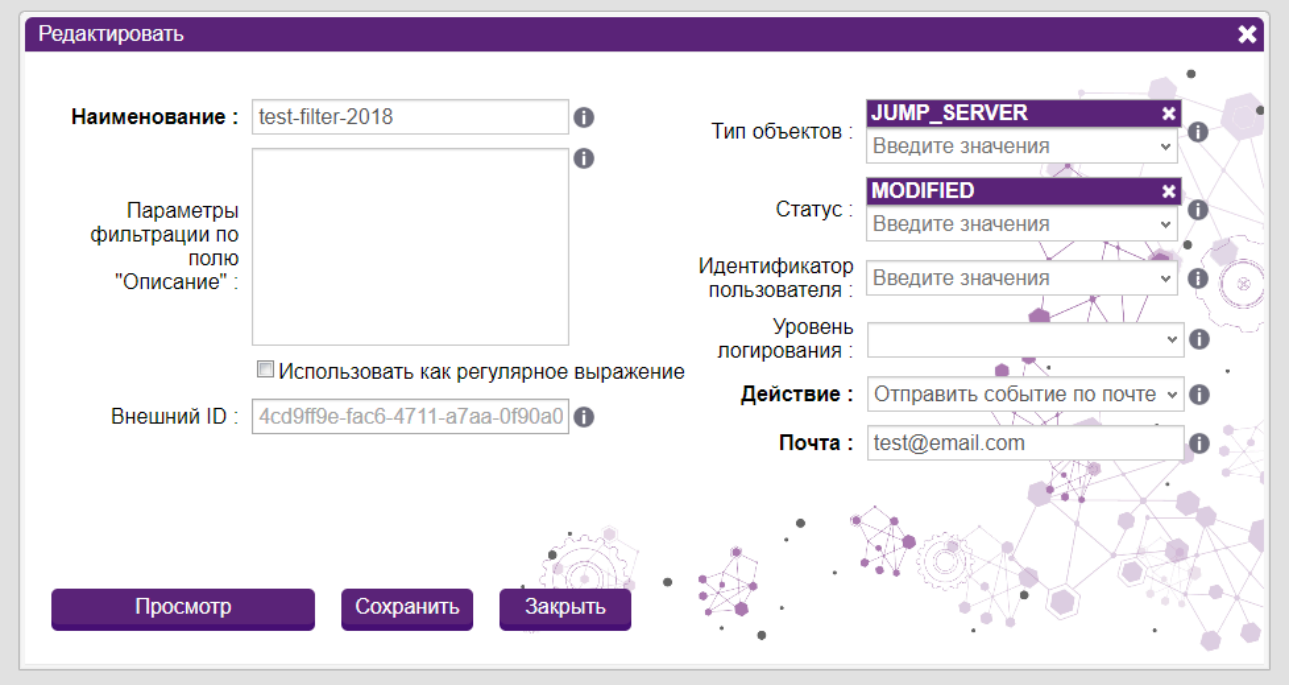


Рис. 3.17.4. Окно редактирования параметра фильтрации

Все поля, кроме Внешнего ID, доступны для редактирования. Поля, выделенные жирным, являются обязательными для заполнения. Чтобы сохранить изменения, необходимо нажать кнопку **Сохранить**. При нажатии кнопки **Закрыть** никаких изменений в карточке параметра фильтрации не произойдет.

3.17.3. Обновление таблицы параметров фильтрации

Для обновления записей в таблице параметров фильтрации необходимо щелкнуть мышью на кнопке обновления , расположенной в правой верхней части таблицы.

3.17.4. Удаление строки в таблице параметров фильтрации

Для удаления строки в таблице параметров фильтрации необходимо щелкнуть на кнопке удаления, расположенной справа в строке параметров фильтрации.

3.17.5. Удаление нескольких записей из таблицы параметров фильтрации одновременно

Для удаления нескольких записей из таблицы параметров фильтрации одновременно необходимо сначала выделить нужные записи в таблице, установив флажок в соответствующем поле слева от поля **Имя**, после чего станет активной кнопка **Удалить**, расположенная сверху над таблицей.

3.18. Управление отчетностью о событиях

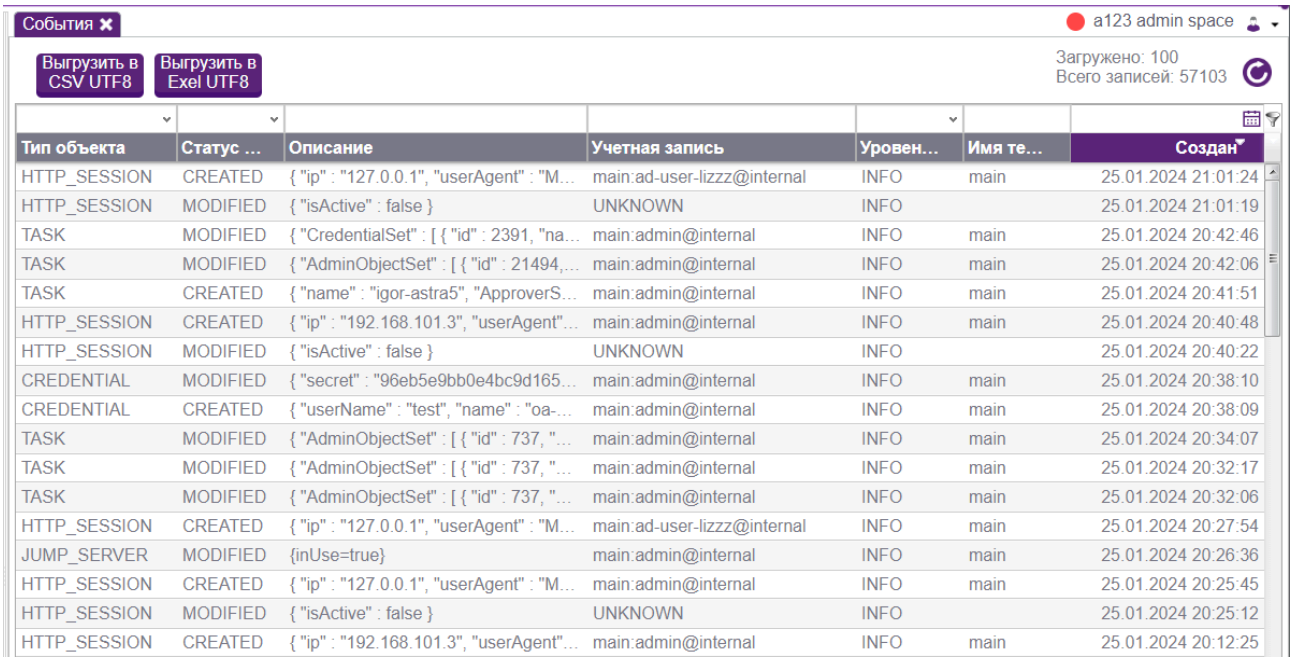
Вкладка **События** в узле **Журнал событий** раздела **Управление ресурсами** служит для того, чтобы технический администратор мог просматривать лог всех действий на портале. Также на этой вкладке он может скачать лог в виде файла себе на рабочую станцию.

Страница **Параметры фильтрации** позволяет техническому администратору:

- Просматривать события на портале;
- Выгружать события в виде лога;
- Обновлять страницу событий.

Просмотр событий на портале

Внешне раздел представлен в виде таблицы со списком параметров.



Тип объекта	Статус ...	Описание	Учетная запись	Уровен...	Имя те...	Создан
HTTP_SESSION	CREATED	{ "ip" : "127.0.0.1", "userAgent" : "M...	main:ad-user-lizzz@internal	INFO	main	25.01.2024 21:01:24
HTTP_SESSION	MODIFIED	{ "isActive" : false }	UNKNOWN	INFO		25.01.2024 21:01:19
TASK	MODIFIED	{ "CredentialSet" : [{ "id" : 2391, "na...	main:admin@internal	INFO	main	25.01.2024 20:42:46
TASK	MODIFIED	{ "AdminObjectSet" : [{ "id" : 21494,...	main:admin@internal	INFO	main	25.01.2024 20:42:06
TASK	CREATED	{ "name" : "igor-astra5", "ApproverS...	main:admin@internal	INFO	main	25.01.2024 20:41:51
HTTP_SESSION	CREATED	{ "ip" : "192.168.101.3", "userAgent"...	main:admin@internal	INFO	main	25.01.2024 20:40:48
HTTP_SESSION	MODIFIED	{ "isActive" : false }	UNKNOWN	INFO		25.01.2024 20:40:22
CREDENTIAL	MODIFIED	{ "secret" : "96eb5e9bb0e4bc9d165...	main:admin@internal	INFO	main	25.01.2024 20:38:10
CREDENTIAL	CREATED	{ "userName" : "test", "name" : "oa-...	main:admin@internal	INFO	main	25.01.2024 20:38:09
TASK	MODIFIED	{ "AdminObjectSet" : [{ "id" : 737, "...	main:admin@internal	INFO	main	25.01.2024 20:34:07
TASK	MODIFIED	{ "AdminObjectSet" : [{ "id" : 737, "...	main:admin@internal	INFO	main	25.01.2024 20:32:17
TASK	MODIFIED	{ "AdminObjectSet" : [{ "id" : 737, "...	main:admin@internal	INFO	main	25.01.2024 20:32:06
HTTP_SESSION	CREATED	{ "ip" : "127.0.0.1", "userAgent" : "M...	main:ad-user-lizzz@internal	INFO	main	25.01.2024 20:27:54
JUMP_SERVER	MODIFIED	{inUse=true}	main:admin@internal	INFO	main	25.01.2024 20:26:36
HTTP_SESSION	CREATED	{ "ip" : "127.0.0.1", "userAgent" : "M...	main:admin@internal	INFO	main	25.01.2024 20:25:45
HTTP_SESSION	MODIFIED	{ "isActive" : false }	UNKNOWN	INFO		25.01.2024 20:25:12
HTTP_SESSION	CREATED	{ "ip" : "192.168.101.3", "userAgent"...	main:admin@internal	INFO	main	25.01.2024 20:12:25

Рис. 3.18.1. Страница «События»

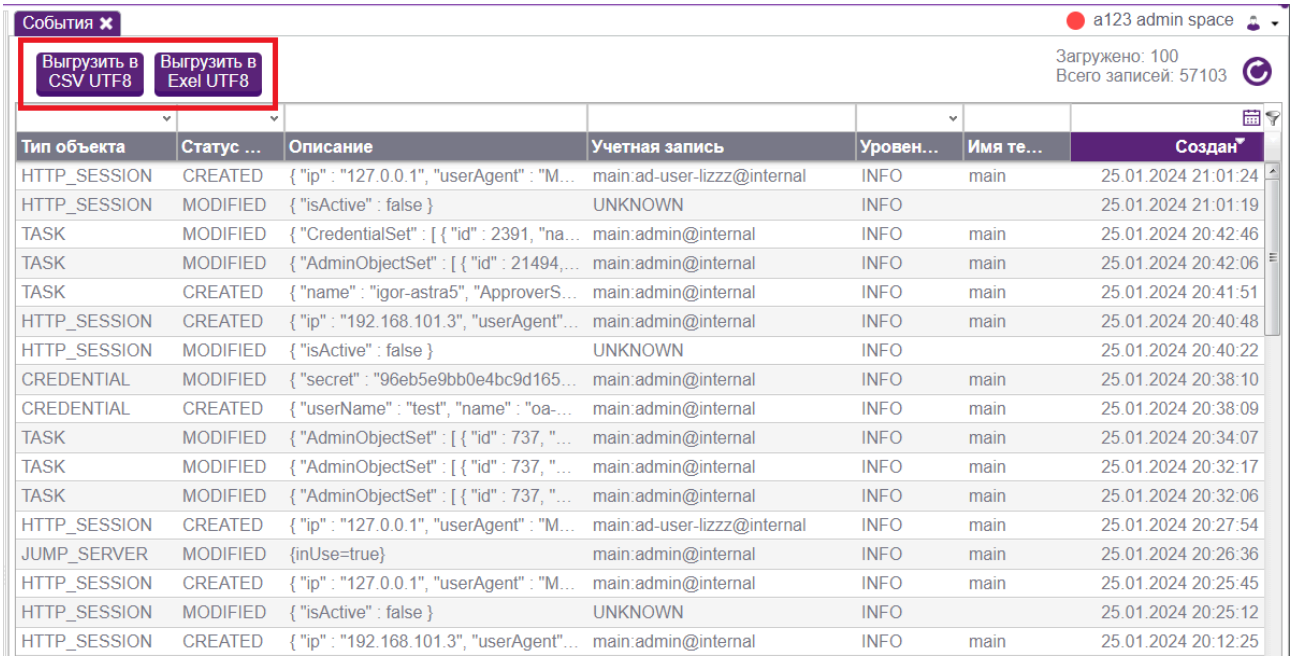
Описание параметров таблицы событий:

- Тип объекта - тип объекта, с которым было произведено действие.

- Статус - действие, совершенное с этим объектом.
- Описание - описание совершенного действия.
- Учетная запись - какой пользователь совершил это действие.
- Уровень логирования - уровень логирования, на котором произошло действие.
- Имя тенанта - тенант, в котором произошло действие.
- Создан - время, когда произошло действие.

3.18.1. Выгрузка лога событий в виде файла

Администратор может загрузить к себе на компьютер файл, в котором собраны события. Это можно сделать в формате .csv и Excel, нажав на соответствующую кнопку над таблицей событий.



Тип объекта	Статус ...	Описание	Учетная запись	Уровен...	Имя те...	Создан
HTTP_SESSION	CREATED	{ "ip" : "127.0.0.1", "userAgent" : "M...	main:ad-user-lizzz@internal	INFO	main	25.01.2024 21:01:24
HTTP_SESSION	MODIFIED	{ "isActive" : false }	UNKNOWN	INFO		25.01.2024 21:01:19
TASK	MODIFIED	{ "CredentialSet" : [{ "id" : 2391, "na...	main:admin@internal	INFO	main	25.01.2024 20:42:46
TASK	MODIFIED	{ "AdminObjectSet" : [{ "id" : 21494,...	main:admin@internal	INFO	main	25.01.2024 20:42:06
TASK	CREATED	{ "name" : "igor-astra5", "ApproverS...	main:admin@internal	INFO	main	25.01.2024 20:41:51
HTTP_SESSION	CREATED	{ "ip" : "192.168.101.3", "userAgent"...	main:admin@internal	INFO	main	25.01.2024 20:40:48
HTTP_SESSION	MODIFIED	{ "isActive" : false }	UNKNOWN	INFO		25.01.2024 20:40:22
CREDENTIAL	MODIFIED	{ "secret" : "96eb5e9bb0e4bc9d165...	main:admin@internal	INFO	main	25.01.2024 20:38:10
CREDENTIAL	CREATED	{ "userName" : "test", "name" : "oa-...	main:admin@internal	INFO	main	25.01.2024 20:38:09
TASK	MODIFIED	{ "AdminObjectSet" : [{ "id" : 737, "...	main:admin@internal	INFO	main	25.01.2024 20:34:07
TASK	MODIFIED	{ "AdminObjectSet" : [{ "id" : 737, "...	main:admin@internal	INFO	main	25.01.2024 20:32:17
TASK	MODIFIED	{ "AdminObjectSet" : [{ "id" : 737, "...	main:admin@internal	INFO	main	25.01.2024 20:32:06
HTTP_SESSION	CREATED	{ "ip" : "127.0.0.1", "userAgent" : "M...	main:ad-user-lizzz@internal	INFO	main	25.01.2024 20:27:54
JUMP_SERVER	MODIFIED	{inUse=true}	main:admin@internal	INFO	main	25.01.2024 20:26:36
HTTP_SESSION	CREATED	{ "ip" : "127.0.0.1", "userAgent" : "M...	main:admin@internal	INFO	main	25.01.2024 20:25:45
HTTP_SESSION	MODIFIED	{ "isActive" : false }	UNKNOWN	INFO		25.01.2024 20:25:12
HTTP_SESSION	CREATED	{ "ip" : "192.168.101.3", "userAgent"...	main:admin@internal	INFO	main	25.01.2024 20:12:25

Рис. 3.18.2. Кнопка «Выгрузить» лог событий

Если событий слишком много, то может потребоваться вручную ввести диапазон в фильтрах таблицы Excel .

3.18.2. Обновление таблицы событий

Для обновления записей в таблице событий необходимо щелкнуть мышью на кнопке обновления , расположенной в правой верхней части таблицы.

3.19. Управление внутренней системой аудита сеансов (ВСАС)

Система sPACE позволяет осуществлять видеоаудит системы, для этого у нее есть специальный встроенный функционал, настройка которого производится в соответствующем разделе. Видеоаудит служит для записи скриншотов сеансов и действий пользователей. Внутренняя система видеоаудита не требует дополнительной установки и поставляется вместе с Системой.

Страница **Внутренний видеоаудит** позволяет техническому администратору:

- Просматривать параметры внутренней системы видеоаудита сеансов;
- Обновлять страницу ВСАС;
- Редактировать параметры ВСАС глобально;
- Настраивать параметры ВСАС для отдельного сервера ЗС;
- Выбирать стратегию балансировки хранилищ ВСАС.

3.19.1. Просмотр параметров внутренней системы видеаудита сеансов

Внешне раздел представлен в виде списка параметров, а также списка настроек записи для всех серверов ЗС.

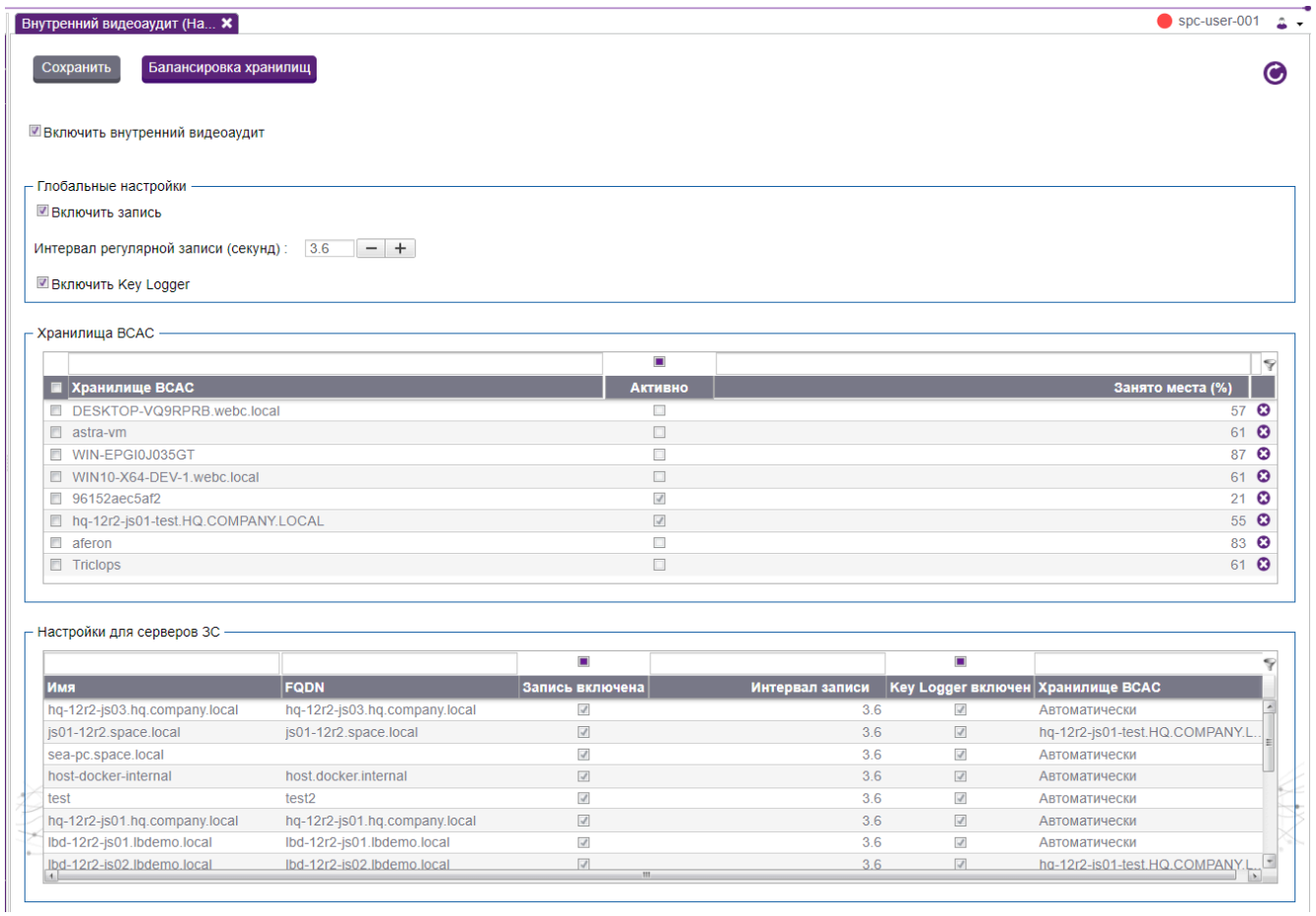


Рис. 3.19.1. Страница «Внутренний видеоаудит»

Описание параметров внутренней системы видеоаудита:

- Включить внутренний аудит – когда этот параметр включен, внутренняя система видеоаудита работает и записывает все сеансы;
- Глобальные настройки – настройки, которые по умолчанию применяются для видеозаписей со всех серверов ЗС, если для них не заданы личные параметры;
- Включить запись – параметр, отвечающий за создание видеозаписи каждого сеанса;
- Интервал регулярной записи (секунд) – промежуток времени, с которым делаются скриншоты сеанса. Чем чаще они делаются, тем более подробной будет запись, но при этом она занимает все больше места;
- Включить Key Logger – при включённом параметре ведётся запись всех клавиш, нажатых пользователем. Для поиска по ним используется поиск по метаданным;
- Настройки для серверов ЗС – персональные настройки перечисленных выше параметров, которые можно установить для каждого сервера ЗС по отдельности;
- Хранилище ВСАС – определенное хранилище для данного сервера ЗС.

3.19.2. Обновление страницы внутреннего видеоаудита

Для обновления страницы внутреннего видеоаудита служит соответствующая кнопка **Обновить**, расположенная в правой части верхней панели.

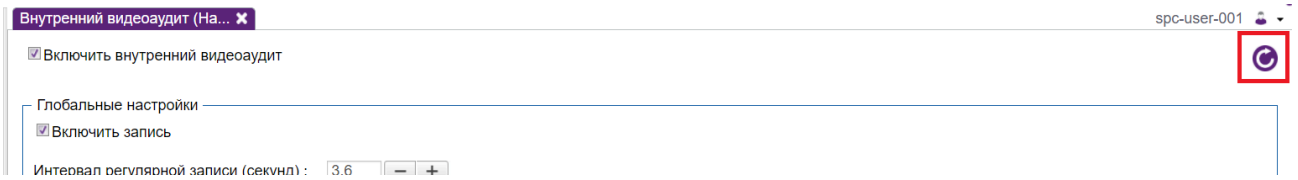


Рис. 3.19.2. Расположение кнопки «Обновить»

3.19.3. Редактирование глобальных настроек внутреннего видеоаудита

Для обновления редактирования глобальных настроек внутреннего видеоаудита достаточно поставить/убрать галочку в нужной графе или изменить значение интервала записи, а потом зафиксировать изменения, нажав на загоревшуюся кнопку **Сохранить**.

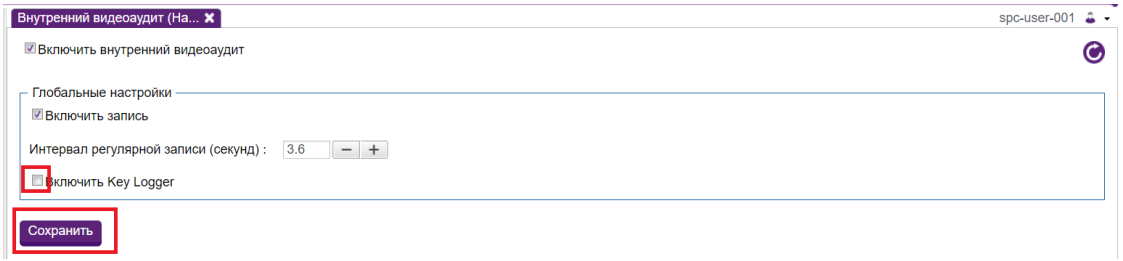


Рис. 3.19.3. Включение функции Key Logger и кнопка «Сохранить»

3.19.4. Удаление хранилища ВСАС

Для удаления хранилища (строки в таблице) служит соответствующая иконка **Удалить**, расположенная в правой части строки записи. Удалить можно только те хранилища, которые не являются активными.

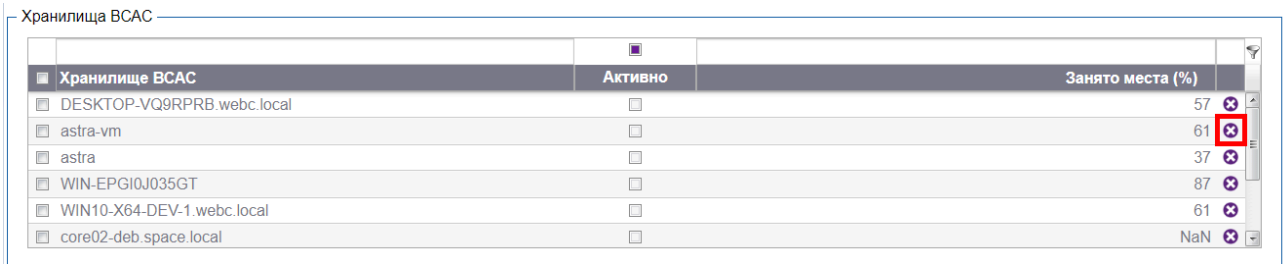


Рис. 3.19.4. Расположение кнопки «Удалить»

3.19.5. Редактирование настроек внутреннего видеоаудита для отдельного сервера ЗС

Чтобы отредактировать настройки ВСАС для одного определённого сервера ЗС, необходимо нажать на название данного сервера в таблице **Настройки для серверов ЗС**:

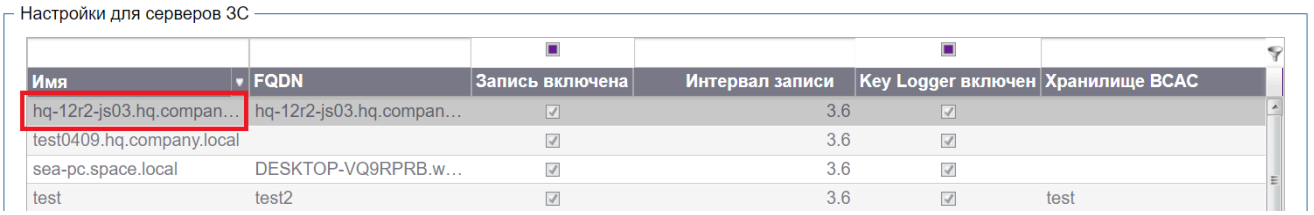


Рис. 3.19.5. Выбор сервера ЗС

После этого откроется окно с параметрами данного сервера ЗС, которые можно изменить по своему желанию и нажать на кнопку **Сохранить** для фиксации результата.

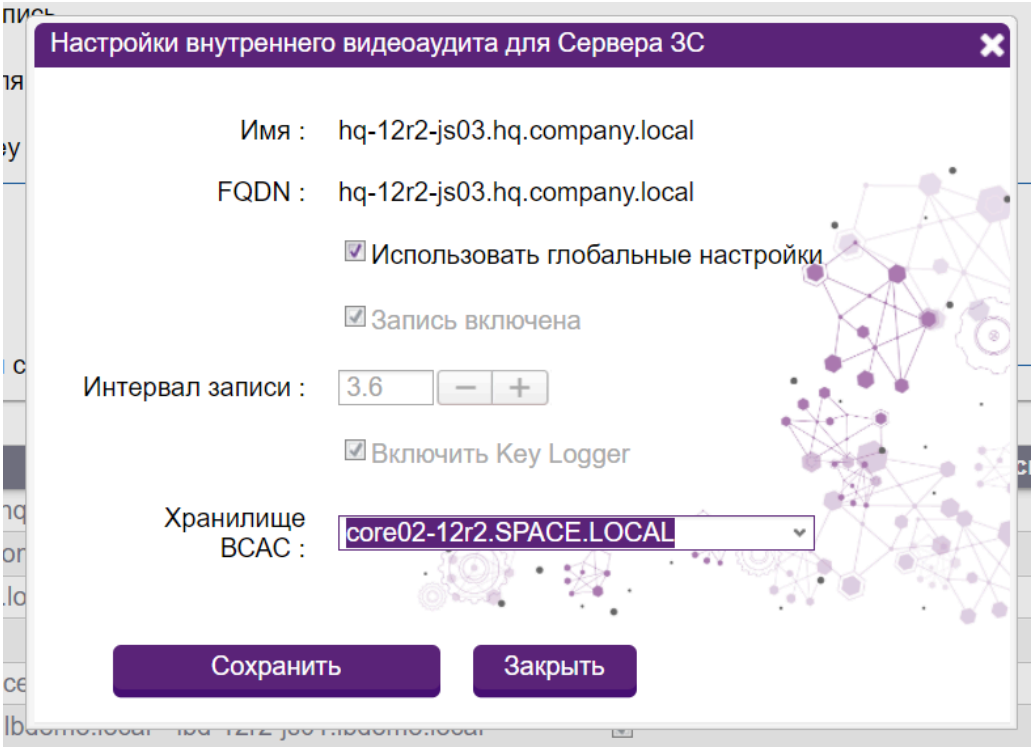


Рис. 3.19.6. Окно настройки внутреннего видеоаудита для сервера 3С

3.19.6. Выбор стратегии балансировки хранилищ ВСАС

Чтобы отредактировать стратегию балансировки хранилищ требуется нажать на кнопку **Балансировка хранилищ** вверху страницы:

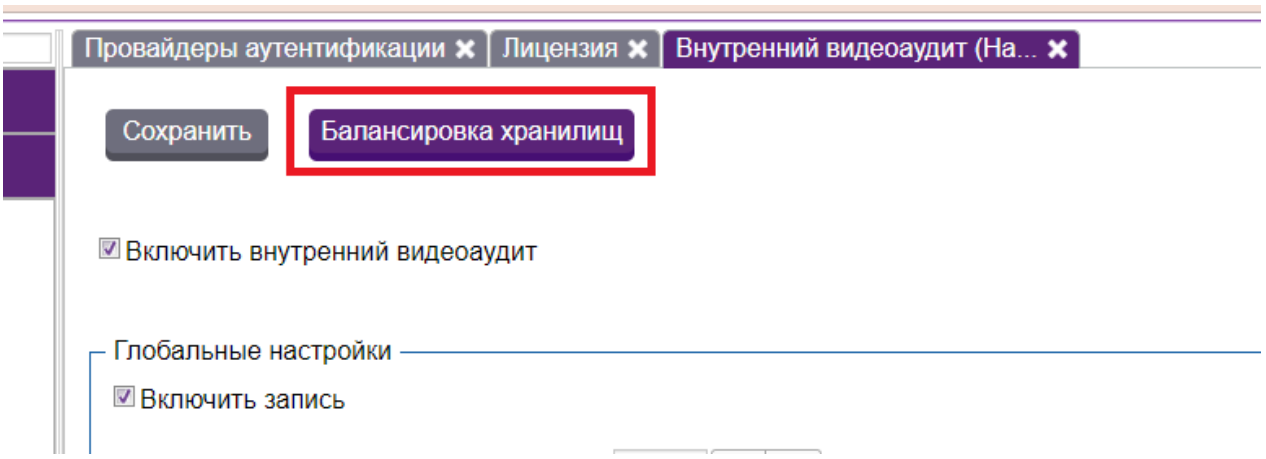


Рис.3.19.7. Кнопка «Балансировка хранилищ»

В появившемся окне можно выбрать стратегию балансировки. В данный момент доступна только балансировка по свободному пространству.

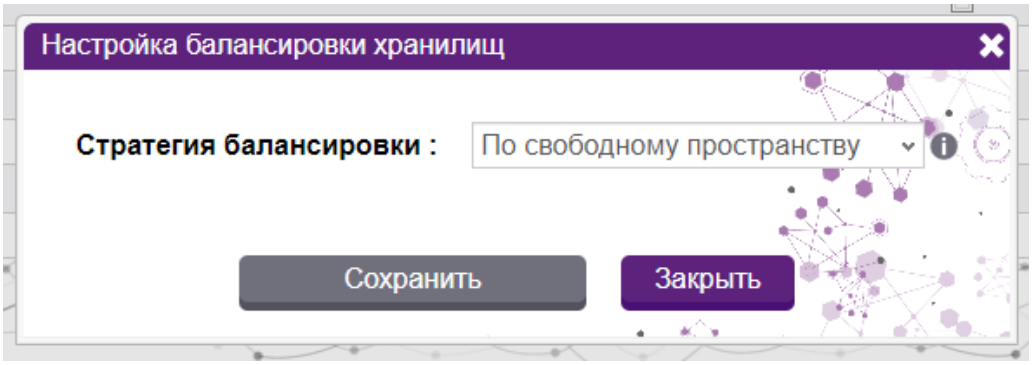


Рис. 3.19.8. Настройка балансировки хранилищ

3.20. Просмотр статуса компонентов Системы

Данная страница позволяет узнать статус всех компонентов Системы. Она присутствует одновременно в разделе **Управление системой** (в узле **Информация о системе**) и в разделе **Управление ресурсами** (как отдельная вкладка). Раздел **Управление системой** доступен для администратора тенанта, поэтому там есть информация только для текущего тенанта (урезанная версия таблицы). Раздел **Управление ресурсами** доступен для технического администратора, и там есть информация по всем тенантам (полная версия таблицы).

В рамках просмотра этой страницы администраторы могут выполнять следующие действия:

- Просматривать информацию о компонентах системы;
- Фильтровать элементы по различным параметрам;
- Обновлять таблицу статуса компонентов;
- Экспортировать компоненты системы в виде html-файла;
- Быстро узнавать о состоянии системы по индикатору «Светофор».

Страница статуса компонентов представлена в виде таблицы, которая выглядит следующим образом:

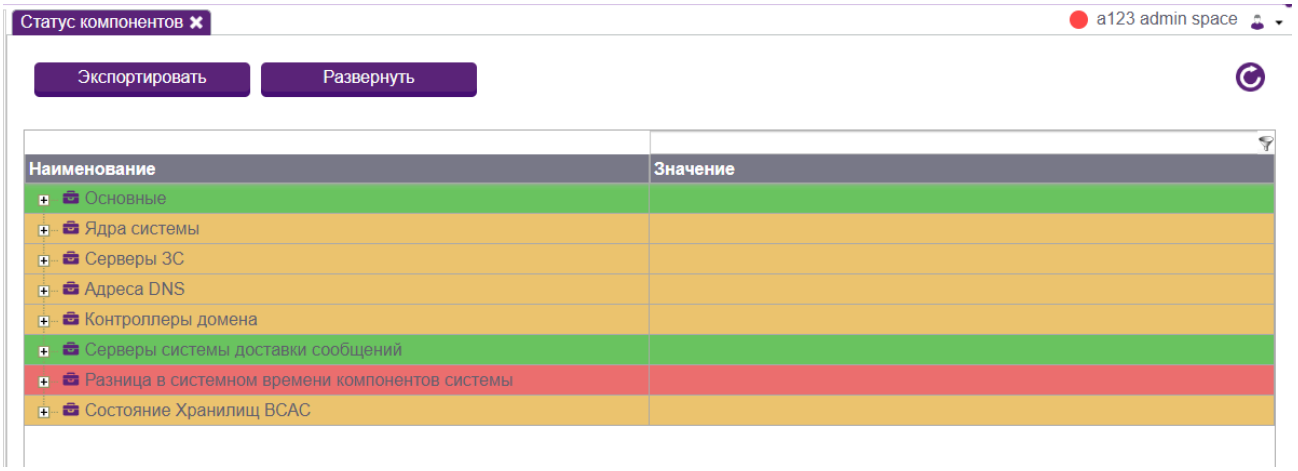


Рис. 3.20.1. Раздел «Статус компонентов»

Параметры:

- Наименование – название компонента системы или вкладки с ними;
- Значение – значение, соответствующее данному компоненту системы.

Цвет строки в таблице соответствует статусу компонента системы:

- Зелёный – все хорошо;
- Жёлтый – есть небольшие отклонения в пределах допустимых;
- Красный – значительные проблемы в работе этого компонента.

3.20.1. Просмотр компонентов системы и их значений

Чтобы просмотреть компоненты определенной категории, необходимо нажать на кнопку **плюс** рядом с наименованием.

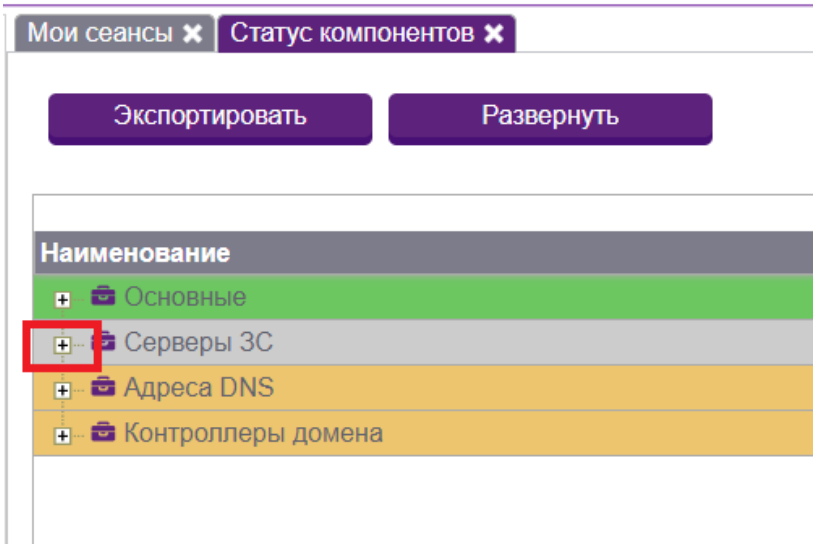


Рис. 3.20.2. Кнопка плюс

После этого раскроется подробный список составляющих.

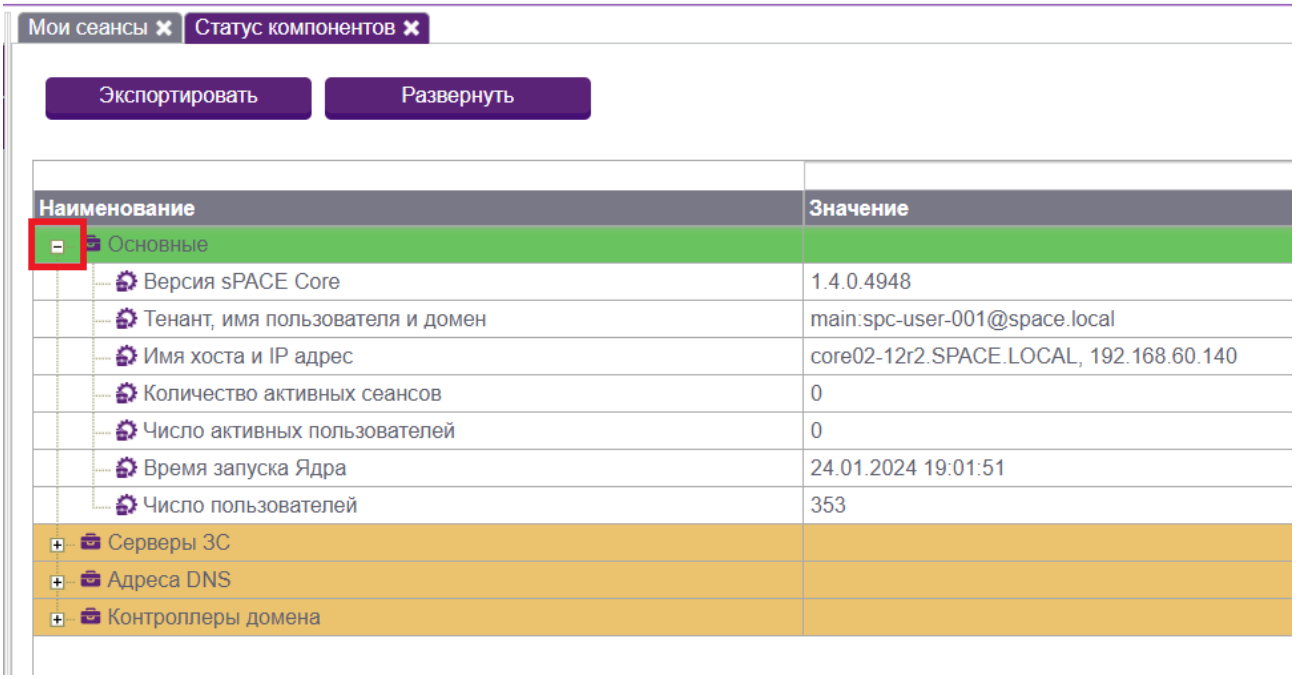


Рис. 3.20.3. Подробная информация о каждом компоненте

3.20.2. Фильтрация элементов раздела

Для фильтрации элементов необходимо нажать на название графы **Наименование** или **Значение** в зависимости от интересующего типа сортировки. Кроме того, можно выбрать параметры сортировки, нажав на стрелку, которая находится с краю. Появится выпадающее меню, в котором можно будет выбрать необходимый параметр.

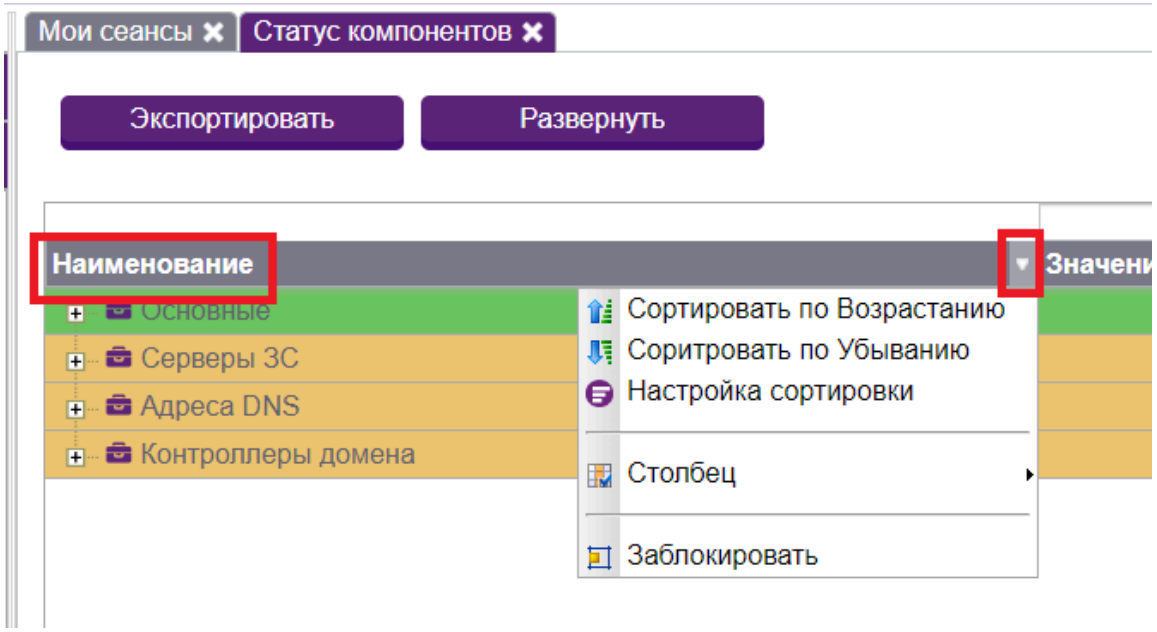


Рис. 3.20.4. Выпадающее меню для выбора типа сортировки

3.20.3. Обновление таблицы статуса компонентов

Для обновления записей в таблице Статуса компонентов служит соответствующая кнопка **Обновить**, расположенная в правой части верхней панели.

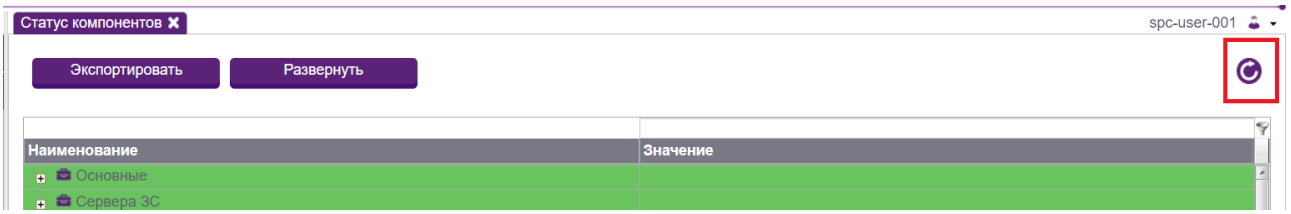


Рис. 3.20.5. Кнопка «Обновить»

3.20.4 Экспорт компонентов в виде html-файла

Для экспорта необходимо нажать на кнопку **Экспортировать**, которая расположена над таблицей компонентов. После этого начнется загрузка html-файла на компьютер.

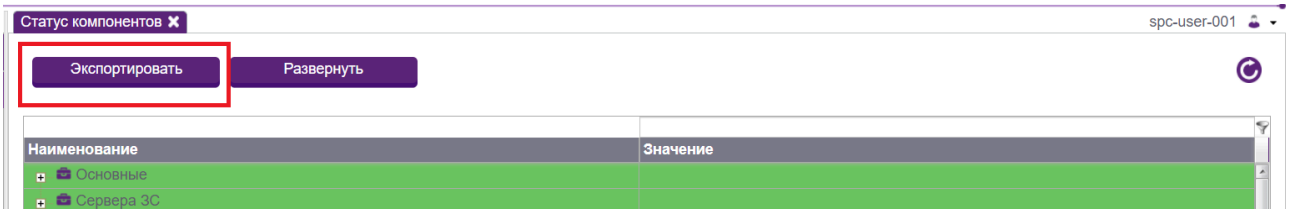


Рис. 3.20.6. Кнопка «Экспортировать»

3.20.5. Индикатор быстрого информирования о состоянии системы "Светофор"

Администраторы могут быстро узнать общее состояние вкладки "Статус компонентов", не открывая ее. Для этого справа вверху, рядом с их именем пользователя на любой странице портала, нарисован специальный индикатор в форме круга. В зависимости от его цвета можно в общих чертах судить о статусе компонентов системы. При нажатии на него администратор попадет на страницу "Статус компонентов".

- Зелёный цвет индикатора - все работает хорошо;
- Желтый цвет индикатора - есть незначительные проблемы, не требующие немедленного вмешательства;
- Красный цвет индикатора - в статусе некоторых компонентов найдены существенные проблемы, рекомендуется их исправить.

Примечание: может случиться ситуация, когда администратор, авторизованный на портале, видит красный индикатор светофора, но когда он переходит на страницу **Статус компонентов**, то там

красной строки нет. Это связано с тем, что у простого Администратора открывается усеченная версия страницы **Статус компонентов**, которая соответствует только его тенанту. Для просмотра полной версии **Статуса компонентов** всей системы из всех тенантов требуется пользователь с ролью Технический администратор с доступом на вкладку **Статуса компонентов** из раздела **Управление ресурсами**.

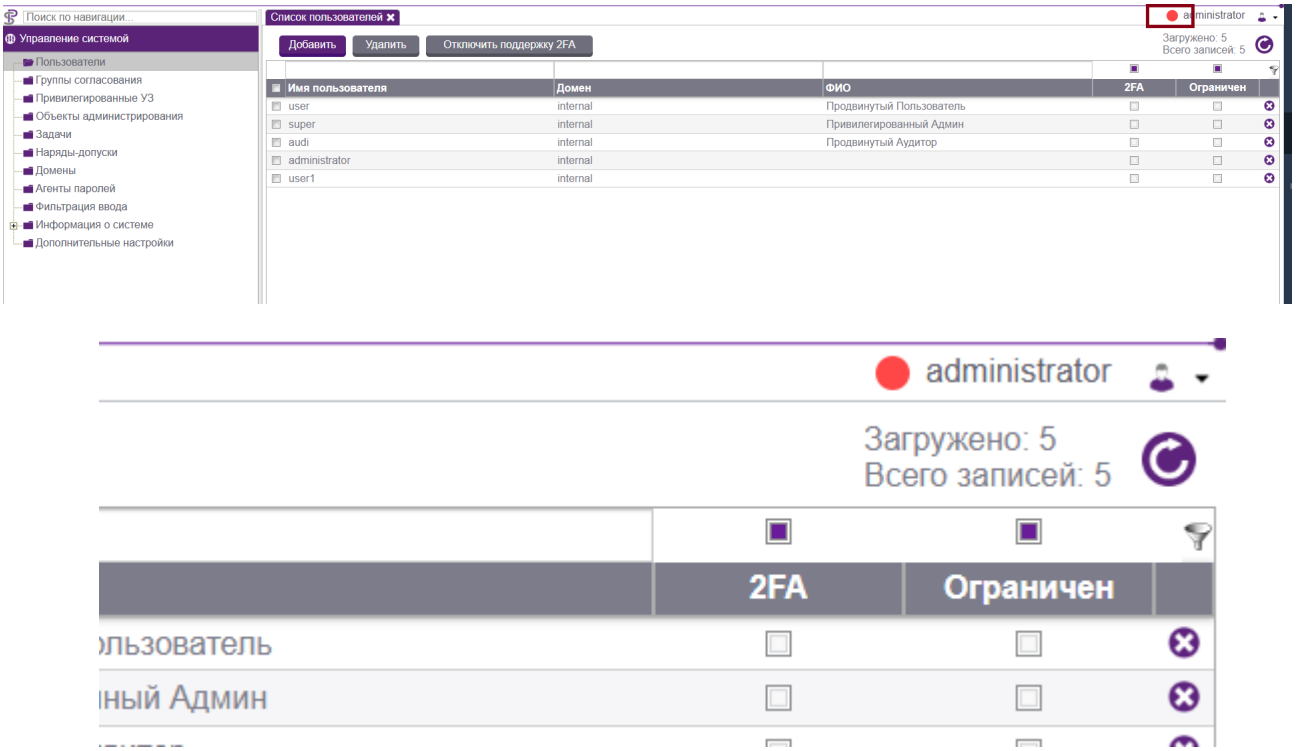


Рис. 3.20.7. Местоположение индикатора «Светофор»

3.21. Управление лицензией

Данная страница позволяет узнать максимально допустимые значения для количества ядер, хранилищ, одновременных сеансов, работающих пользователей и т. д. А также активные сеансы и соединения для различных серверов ЗС.

Для данного раздела реализован следующий функционал:

- Просмотр лицензии.
- Обновление страницы лицензии.
- Скачивание запроса на лицензию
- Загрузка лицензии.

3.21.1. Просмотр лицензии

Страница лицензии выглядит следующим образом:

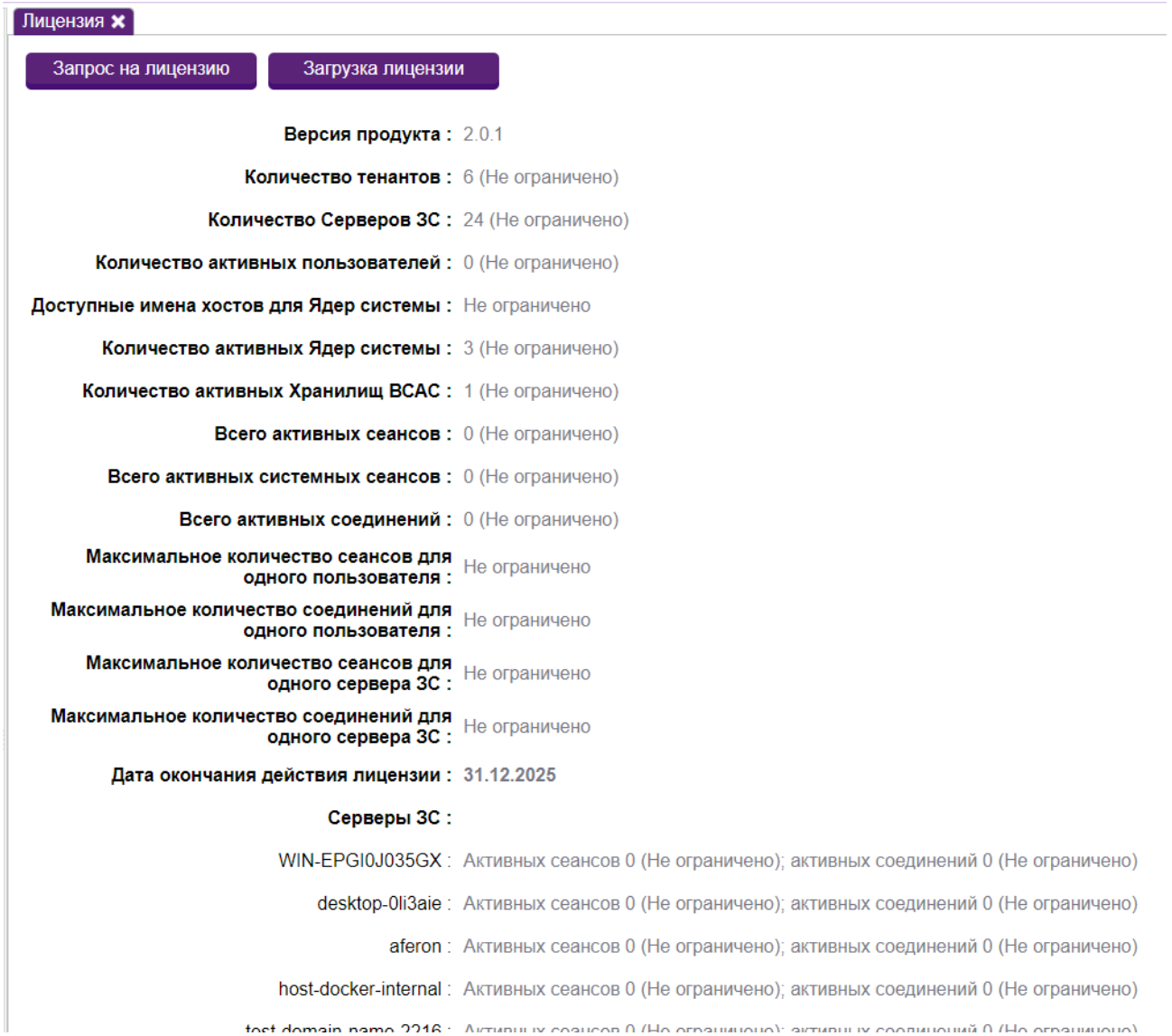


Рис. 3.21.1. Страница «Лицензия»

Описание параметров:

- Версия продукта - версия продукта sPACE.
- Количество тенантов - количество тенантов системы.
- Количество Серверов ЗС - все сервера ЗС, доступные в системе на данный момент, и их максимально разрешённое значение.
- Количество активных пользователей - пользователи, работающие в системе в данный момент, и их максимально разрешённое значение.
- Доступные имена хостов для Ядер системы - ядра, которые доступны в системе.
- Количество активных Ядер системы - ядра системы, находящиеся в данный момент во включённом состоянии, и их максимально разрешённое значение.

- Количество активных Хранилищ ВСАС - хранилища системы, находящиеся в данный момент в активном состоянии, и их максимально разрешённое значение.
- Всего активных сеансов - все сеансы системы, работающие в данный момент, и их максимально разрешённое значение.
- Всего активных системных сеансов - все системные сеансы, работающие в данный момент, и их максимально разрешённое значение.
- Всего активных соединений - все соединения системы, работающие в данный момент, и их максимально разрешённое значение.
- Максимальное количество сеансов для одного пользователя - количество сеансов, которое может быть у одного пользователя одновременно.
- Максимальное количество соединений для одного пользователя - количество соединений, которое может быть у одного пользователя одновременно.
- Максимальное количество сеансов для одного сервера 1С - количество сеансов, которое может быть запущено на одном сервере 1С одновременно.
- Максимальное количество соединений для одного сервера 1С - количество соединений, которое может быть запущено на одном сервере 1С одновременно.
- Дата окончания действия лицензии - дата, до которой действует данная лицензия (включительно).
- Серверы 1С - перечень всех активных серверов 1С и количество сеансов и соединений на них, активных в данный момент.
- Пользователи - перечень всех пользователей, у которых в данный момент есть запущенные сеансы.

3.21.2. Обновление страницы лицензии

Для обновления страницы лицензии служит соответствующая кнопка **Обновить**, расположенная в правой части верхней панели. При обновлении страницы будет показана актуальная (на момент обновления) информация для всех параметров.

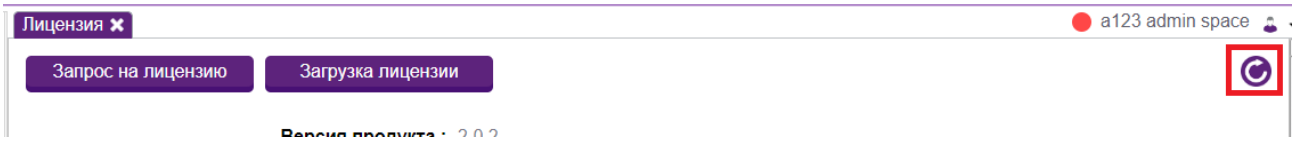


Рис. 3.21.2. Кнопка «Обновить»

3.21.3. Скачивание запроса на лицензию

Чтобы скачать на свой компьютер текстовый файл с параметрами лицензии, нужно нажать на кнопку **Запрос на лицензию**.

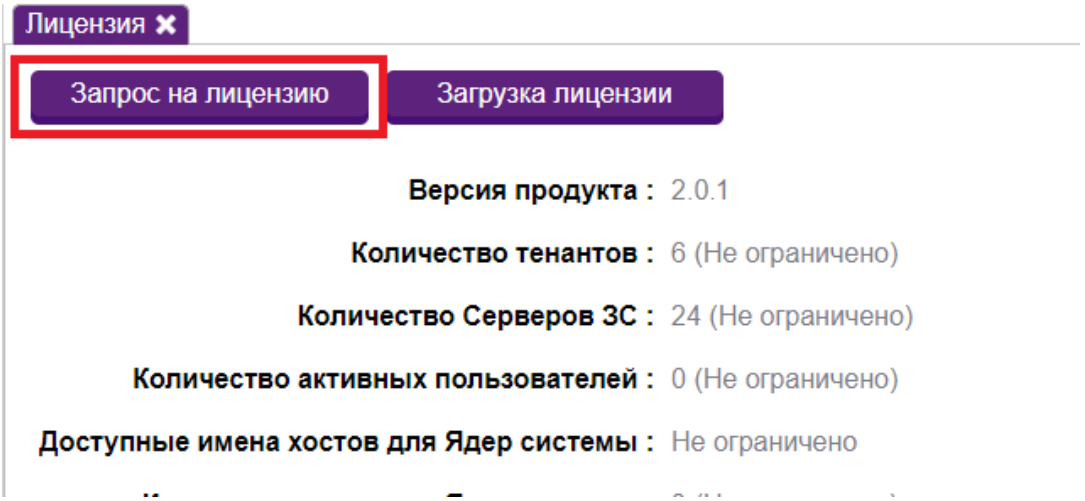


Рис. 3.21.3. Кнопка «Запрос на лицензию»

3.21.4. Загрузка лицензии

Для автоматической загрузки лицензии требуется нажать на кнопку **Загрузка лицензии**.

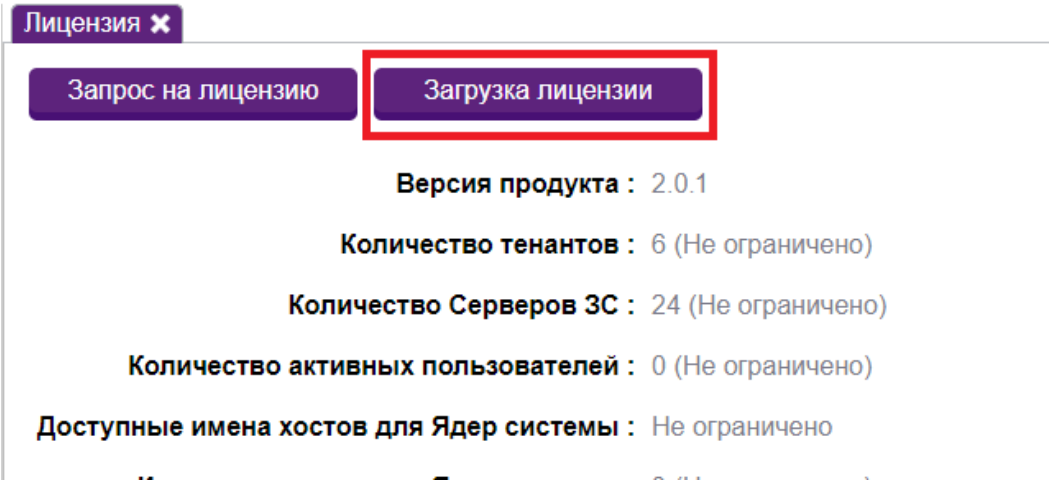


Рис. 3.21.4. Кнопка «Загрузка лицензии»

Откроется окно загрузки лицензии. В нём присутствует поле для загрузки файла лицензии. Перед загрузкой важно удостовериться, что файл лицензии подписан публичным ключом. После загрузки файла в поле нужно нажать на кнопку "Загрузить лицензию".

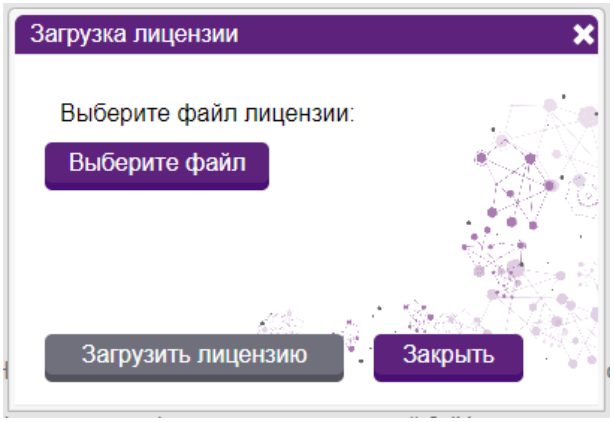


Рис. 3.21.5. Окно загрузки лицензии

3.22. Управление сеансами привилегированного доступа

Все сеансы привилегированного доступа отображаются на странице **Сеансы** в узле **Информация о системе** раздела **Управление системой**.

Рис. 3.22.1. Окно «Сеансы» раздела «Управление системой»

Данные о сеансах представлены в таблице, содержащей следующие столбцы:

- Пользователь – пользователь, запустивший данный сеанс;
- Состояние – статус сеанса;
- Создан – дата запуска сеанса;
- Приложение – приложение, для которого запущен сеанс;
- Объект администрирования – объект администрирования в рамках данного сеанса;

- FQDN – Fully Qualified Domain Name, имя домена, не имеющее неоднозначностей в определении. Включает в себя имена всех родительских доменов иерархии DNS;
- Сервер ЗС – сервер ЗСА, через который осуществляется работа в рамках данного сеанса.

В рамках получения данных о сеансах ПД в Системе администраторы могут выполнять следующие действия:

- фильтровать сеансы по состоянию;
- фильтровать сеансы по дате создания;
- обновлять таблицу сеансов;
- удалять строку в таблице сеансов;
- удалять несколько записей из таблицы сеансов одновременно.

3.22.1. Фильтрация сеансов по состоянию

Для фильтрации сеансов по состоянию необходимо щелкнуть мышью на изображении стрелки и выбрать соответствующий пункт в раскрывающемся меню.

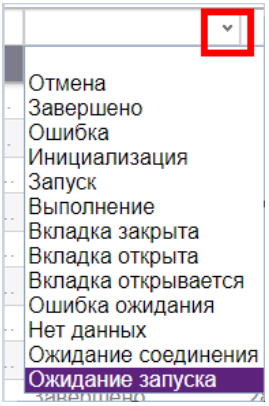


Рис. 3.22.2. Фильтрация сеансов по состоянию. Раскрывающееся меню

3.22.2. Фильтрация сеансов по дате создания

Для фильтрации сеансов по дате создания необходимо щелкнуть мышью на изображении календарь над полем **Создан** и выбрать нужный временной интервал.

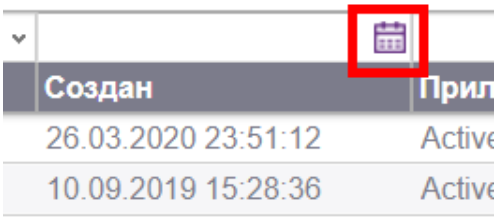


Рис. 3.22.3. Фильтрация сеансов по дате создания

3.22.3. Обновление таблицы сеансов

Для обновления записей в таблице **Сеансы** необходимо щелкнуть мышью на кнопке обновления в правой части верхней панели таблицы.

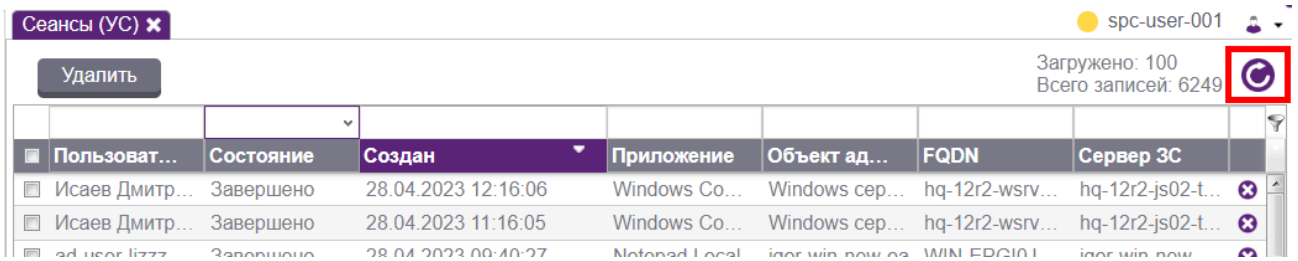


Рис. 3.22.4. Кнопка обновления

3.22.4. Удаление сеансов

Для удаления строки необходимо щелкнуть на кнопке удаления, расположенную в строке справа от поля **Сервер 3С**.

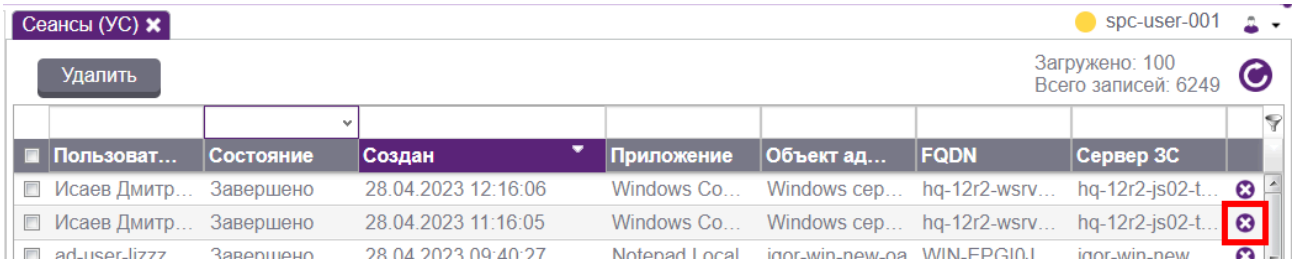


Рис. 3.22.5. Окно «Сеансы». Кнопка удаления строки с сеансом

3.22.5. Удаление нескольких сеансов одновременно

Для удаления нескольких записей из таблицы **Сеансы** одновременно необходимо сначала выделить нужные записи в таблице, установив флажок в соответствующем поле слева от поля **Пользователь**, после чего станет активной кнопка **Удалить**, расположенная сверху над таблицей.

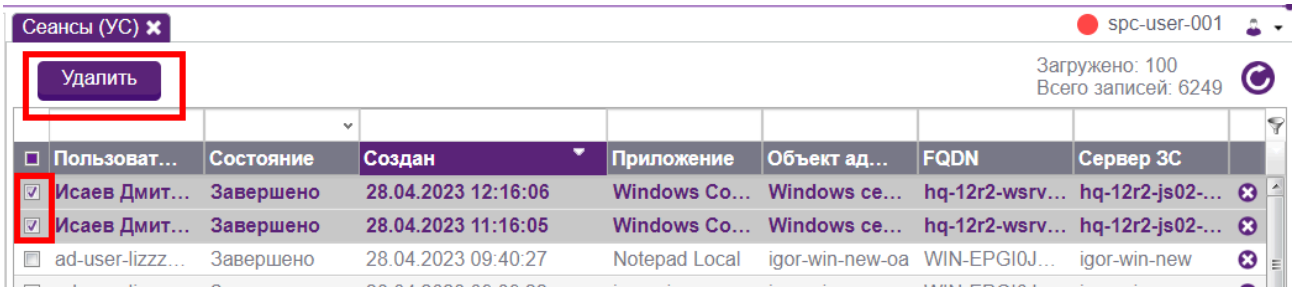


Рис. 3.22.6. Выделены две записи таблицы «Сеансы». Кнопка «Удалить» активна

3.23. Управление операциями с секретами

Доступ к сервисам рандомизации паролей учетных записей (операциям с секретами) осуществляется на странице **Операции с секретами** узла **Информация о системе** раздела **Управление системой**.

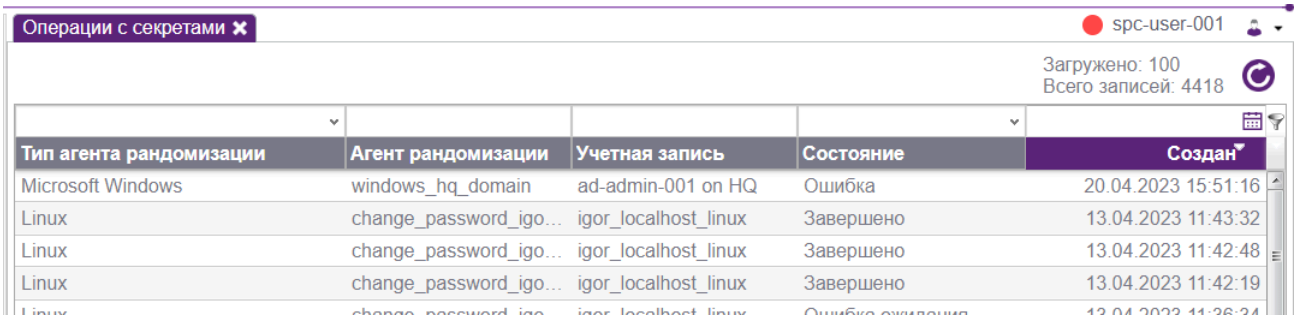


Рис. 3.23.1. Окно «Операции с секретами» раздела «Управление системой»

Данные об операциях рандомизации секретов представлены в таблице, содержащей следующие столбцы:

- Тип агента рандомизации – тип агента, проводившего сеанс рандомизации;
- Агент рандомизации – агент паролей, использовавшийся для проведения сеанса рандомизации;
- Учетная запись – учетная запись, из-под которой проводилась рандомизация;
- Состояние – состояние сеанса;
- Создан – время создания сеанса.

В рамках получения данных об операциях с секретами в Системе администраторы могут выполнять следующие действия:

- фильтровать раздел по состоянию;
- фильтровать раздел по дате создания;

- обновлять таблицу сеансов;
- просматривать детальную информацию о каждом сеансе.

3.23.1. Фильтрация раздела по состоянию

В рамках функционала раздела присутствует фильтрация по состоянию сеансов - для выбора нужного фильтра пользователю необходимо нажать на иконку стрелочки над полем **Состояние** и выбрать соответствующий пункт во всплывающем меню.

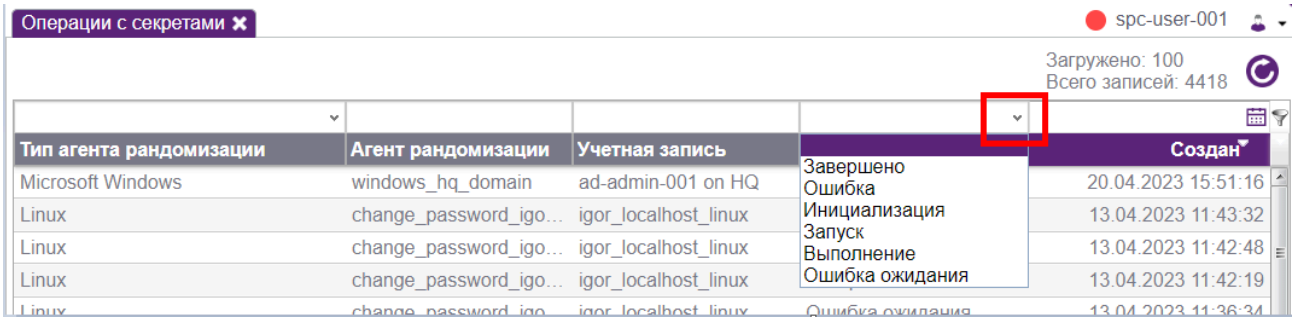


Рис. 3.23.2. Фильтрация сеансов по состоянию. Раскрывающееся меню

3.23.2. Фильтрация раздела по дате создания

Для фильтрации сеансов по дате создания необходимо щелкнуть мышью на изображении календарь над полем Создан и выбрать нужный временной интервал.

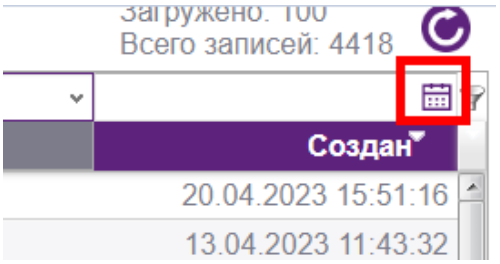


Рис. 3.23.3. Фильтрация сеансов по дате создания

3.23.3. Обновление таблицы операций с секретами

Для обновления записей в таблице Сеансы необходимо щелкнуть мышью на кнопке обновления в правой части верхней панели таблицы.

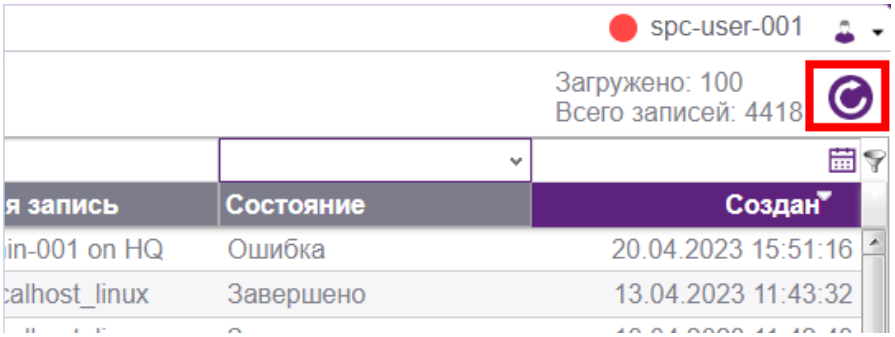


Рис. 3.23.4. Кнопка обновления

3.23.4. Просмотр информации о каждом сеансе

Для просмотра детальной информации о сеансе необходимо дважды щелкнуть левой кнопкой мыши по соответствующей записи в таблице в столбцах **Типа агента рандомизации** или **Агента рандомизации**.

Откроется окно деталей сеанса. В рамках данного окна можно узнать всю необходимую информацию о сеансе.

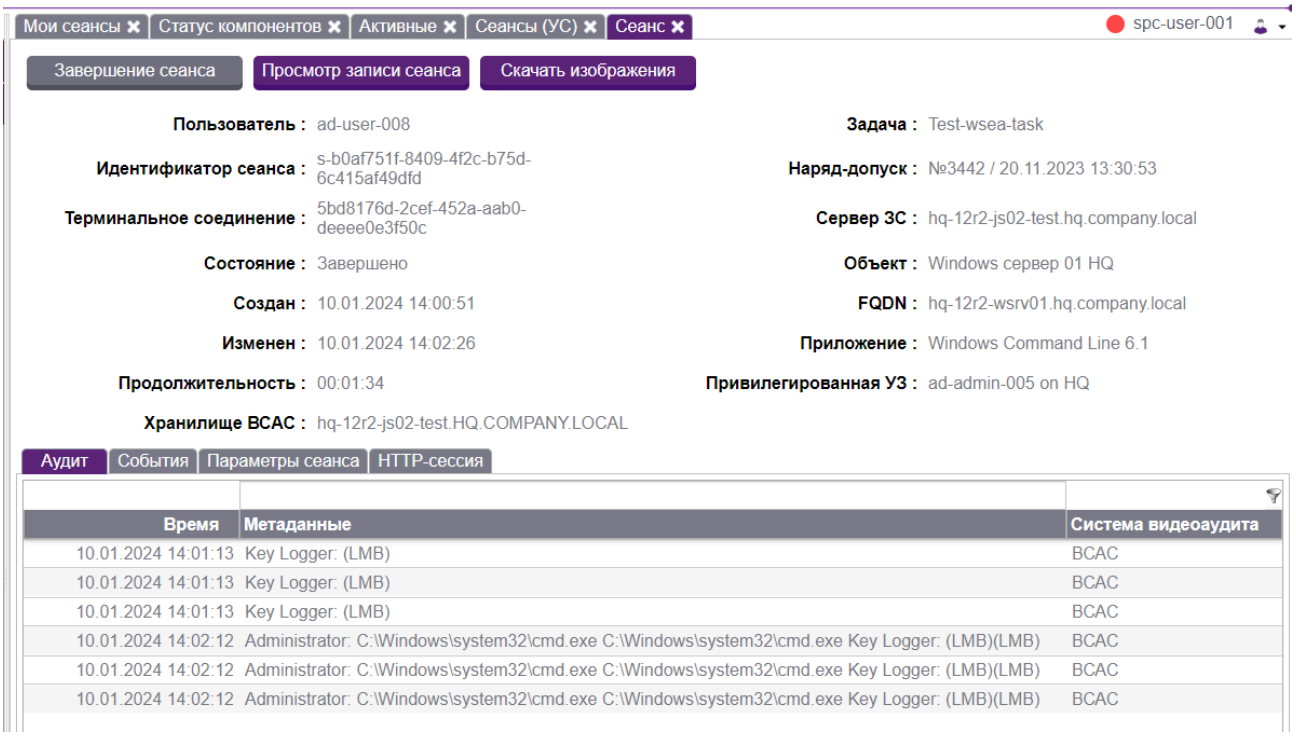


Рис. 3.23.5. Окно подробной информации о сеансе

3.24. Формирование отчетности по использованию Системы

Система sPACE позволяет формировать статистику по использованию системы на основе следующих данных:

- использование системы;
- суммарное количество сеансов за временной интервал;
- максимальное количество одновременных сеансов за определенный интервал времени.


Использование системы

Объект администрирования	Сеансов всего	Успешных	Неуспешных
База данных MSSQL PI @ v-erpm-8r2-06.space.local	0	0	0
Debian сервер системы sPACE @ core01-deb.space.local	0	0	0
PI ZoneProcess HQ @ hq-12r2-zp01.hq.company.local	0	0	0
new AO @ ao.test.ru	0	0	0
Debian сервер 01 HQ @ hq-deb8-lsrv01.hq.company.local	0	0	0
Сервер Nats MQ SPACE @ mq01-deb.space.local	0	0	0
Windows сервер 02 HQ @ hq-12r2-wsrv02.hq.company.local	0	0	0
VMware ESXI HQ @ esx18.webc.local	0	0	0
Domain Controller LBDEMO @ erpm-test-dc.lbdemo.local	0	0	0
VMware vSphere @ webcvc.webc.local	0	0	0
Any @ any	0	0	0
BlueCoat ProxySG @ portal.space.local	0	0	0
Сервер для OIT и PI в sPACE @ v-erpm-8r2-06.space.local	0	0	0
Сервер Nats MQ LBDEMO @ mq01-deb.lbdemo.local	0	0	0
Domain Controller 01 HQ @ hq-12r2-dc01.hq.company.local	0	0	0
Рабочая станция Windows 7 (x86) HQ @ hq-win7-x86.hq.co...	0	0	0
Windows сервер 01 HQ @ hq-12r2-wsrv01.hq.company.local	0	0	0
Domain Controller SPACE @ dc01-12r2.space.local	0	0	0
ObserveIT @ oit.space.local	0	0	0
Domain Controller 02 HQ @ hq-12r2-dc02.hq.company.local	0	0	0
Сервер Nats MQ HQ @ mq01-deb.hq.company.local	0	0	0
Веб-приложение PI - Копия @ pi.space.local	0	0	0
DomainHQ_COMPANY @ hq.company.local	0	0	0
Рабочая станция Windows 7 (x86) @ win7-x86.space.local	0	0	0
База данных MSSQL ObserveIT @ v-erpm-8r2-06.space.local	0	0	0
База данных Oracle SPACE @ dbms01-deb.space.local	0	0	0

Рис. 3.24.1. Статистика по использованию Системы

Технический администратор может сформировать следующую отчетность:

- об использовании приложений, включая общее количество сеансов, число успешных и неуспешных сеансов;
- о количестве сеансов к объектам администрирования, включая число успешных и неуспешных сеансов;
- об использовании Системы пользователями, включая общее количество сеансов, а также число успешных и неуспешных сеансов;
- о суммарном количестве сеансов за час, сутки и месяц;
- о максимальном количестве одновременных сеансов за час, сутки, месяц.

Для формирования отчетности нужно перейти в узел **Статистика** раздела **Управление ресурсами** и выбрать необходимый фильтр в дереве навигации узла **Статистика**.

3.25. Перевод Системы в аварийный режим

В аварийном режиме у пользователей появляется раздел **Аварийный режим**, зайдя в который можно запросить пароль к объекту администрирования в открытом виде.

Функционал перевода системы в аварийный режим доступен сотрудникам с ролью **Привилегированный администратор** (ROLE_SPACE_SUPERADMIN). В случае чрезвычайных ситуаций привилегированный администратор системы может включить аварийный режим системы. Для этого требуется нажать на кнопку **Включить аварийный режим** в разделе Привилегированные **УЗ**.

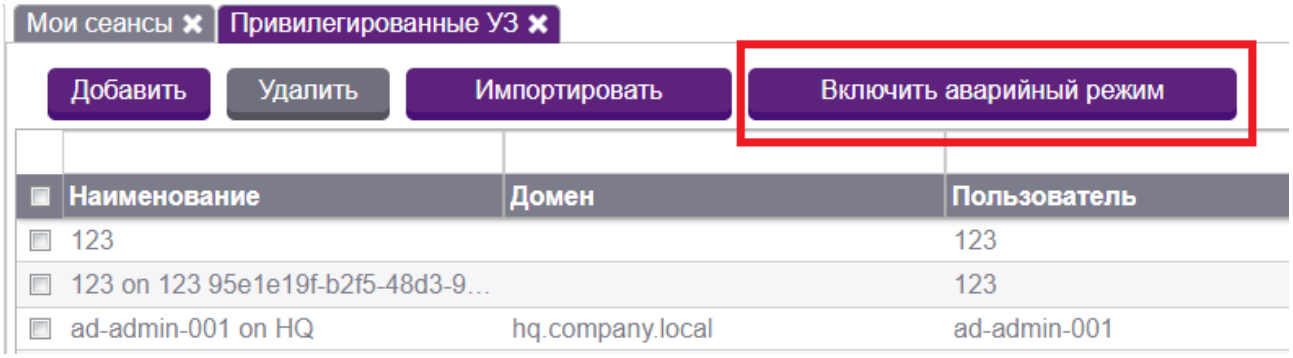


Рис. 3.25.1. Местонахождение кнопки включения аварийного режима

В аварийном режиме в основном меню портала всех пользователей слева отображается новый раздел **Аварийный режим**. Кликнув на него, можно перейти во вкладку **Учетные записи АР**. При нажатии на иконку ключика напротив учетной записи для доступа к объекту администрирования можно будет узнать ее пароль. Будут отображаться только те учетные записи, для которых у пользователя есть согласованный действующий Наряд-допуск.

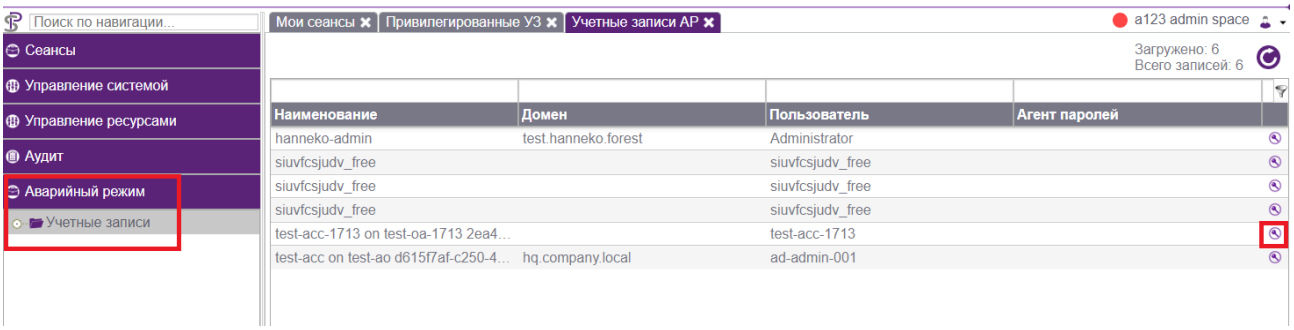


Рис. 3.25.2. Местонахождение раздела аварийного режима

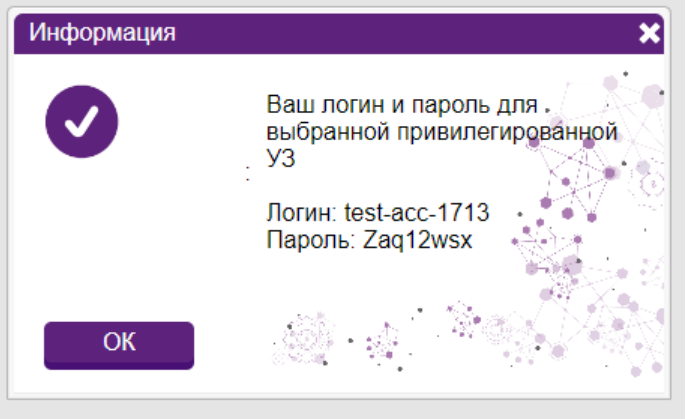


Рис. 3.25.3. Получение пользователем секретов привилегированной учетной записи

Для отключения аварийного режима нужно вернуться в раздел **Привилегированные УЗ** и кликнуть на кнопку **Отключить аварийный режим**. Рекомендуется всегда держать его выключенным.

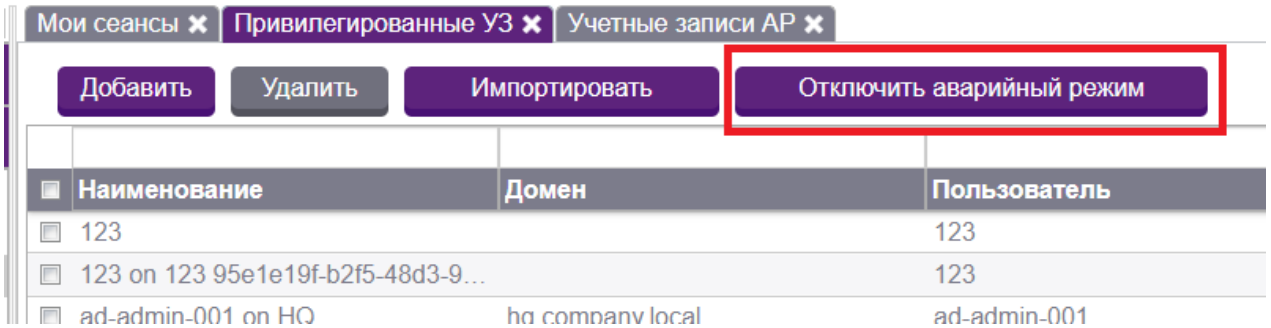


Рис. 3.25.4. Отключение аварийного режима

4. ВОЗМОЖНОСТИ ДЛЯ АУДИТА В sPACE

Система sPACE реализует функционал для аудита в системе, который позволяет получить данные о действиях пользователей на портале.

Для этого служит вкладка **Аудит, доступная в разделе интерфейса пользователей с ролью “аудитор” и “привилегированный аудитор”**. Она необходима для получения объективных качественных и количественных оценок о текущем состоянии портала, имеющихся в нем сеансов, пользователей и их действий.

Данная вкладка представляет из себя древовидную структуру с узлами, позволяющими осуществлять навигацию по разделам.

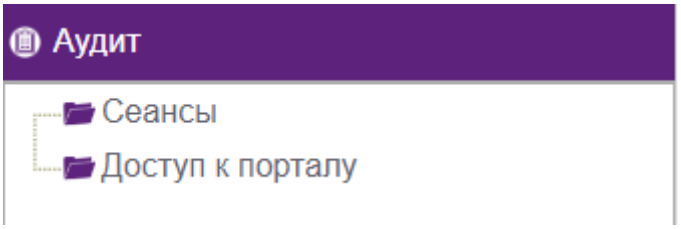
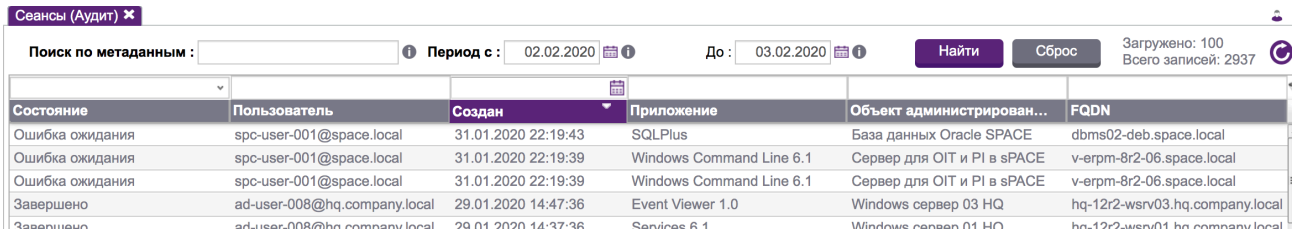


Рис. 4.1. Вкладка «Аудит системы»

4.1. Осуществление аудита сеансов

Вкладка **Сеансы** служит для быстрого доступа и удобного менеджмента всех доступных аудитору сеансов.

Внешне раздел представлен в виде таблицы с шестью столбцами: "Состояние", "Пользователь", "Создан", "Приложение", "Объект администрирования", "FQDN".



Состояние	Пользователь	Создан	Приложение	Объект администрирован...	FQDN
Ошибка ожидания	spc-user-001@space.local	31.01.2020 22:19:43	SQLPlus	База данных Oracle SPACE	dbms02-deb.space.local
Ошибка ожидания	spc-user-001@space.local	31.01.2020 22:19:39	Windows Command Line 6.1	Сервер для OIT и PI в sPACE	v-erpm-8r2-06.space.local
Ошибка ожидания	spc-user-001@space.local	31.01.2020 22:19:39	Windows Command Line 6.1	Сервер для OIT и PI в sPACE	v-erpm-8r2-06.space.local
Завершено	ad-user-008@hq.company.local	29.01.2020 14:47:36	Event Viewer 1.0	Windows сервер 03 HQ	hq-12r2-wsrv03.hq.company.local

Рис. 4.1.1. Вкладка аудита сеансов

Описание параметров в таблице:

- Состояние - статус сеанса;
- Пользователь - пользователь, запустивший данный сеанс;
- Создан - дата запуска сеанса;
- Приложение – приложение, для которого запущен сеанс;

- Объект администрирования - объект администрирования в рамках данного сеанса;
- FQDN - Fully Qualified Domain Name, имя домена, не имеющее неоднозначностей в определении. Включает в себя имена всех родительских доменов иерархии DNS.

В рамках данного раздела реализован следующий функционал:

- Фильтрация раздела по состоянию;
- Фильтрация раздела по дате создания;
- Обновление таблицы Сеансов;
- Просмотр детальной информации о каждом сеансе;
- Просмотр записи сеанса;
- Просмотр записи работающего сеанса в режиме онлайн;
- Скачивание изображений сеанса;
- Экстренное завершение работающего сеанса;
- Поиск по метаданным;
- Просмотр записи сеанса по данным Key Logger.

4.1.1. Фильтрация раздела по состоянию

В рамках функционала раздела присутствует фильтрация по состоянию сеансов: для выбора нужного фильтра пользователю необходимо нажать на иконку стрелочки над полем **Состояние** и выбрать соответствующий пункт во всплывающем меню.

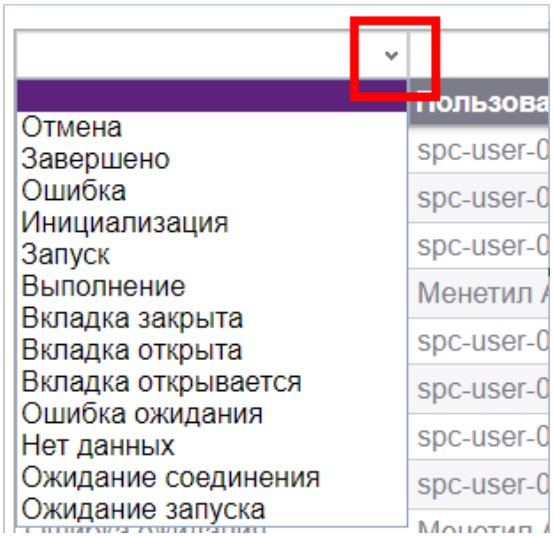


Рис. 4.1.2. Выбор фильтрации по состоянию

4.1.2. Фильтрация раздела по дате создания

В рамках функционала раздела присутствует фильтрация по дате создания сеансов: для выбора нужного фильтра пользователю необходимо нажать на иконку календаря над полем **Создан** и выбрать необходимый временной интервал.

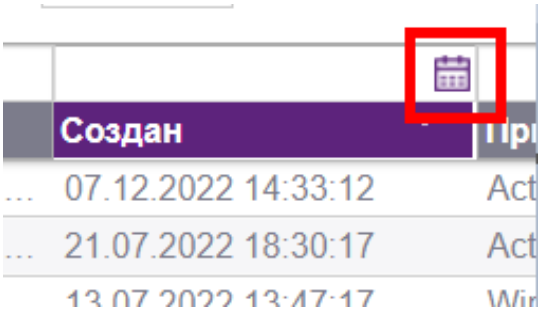


Рис. 4.1.3. Выбор фильтрации по дате создания

4.1.3. Обновление таблицы Сеансы

Для обновления записей в таблице Сеансы служит соответствующая кнопка **Обновить**, расположенная в правой части верхней панели.

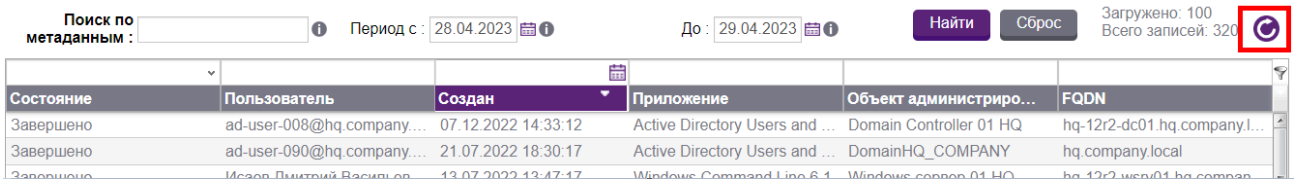


Рис. 4.1.4. Кнопка «Обновить»

4.1.4. Просмотр детальной информации о каждом сеансе

Для просмотра детальной информации о сеансе необходимо дважды щелкнуть левой кнопкой мыши на соответствующей записи в таблице.

Откроется окно деталей сеанса. В рамках данного окна можно узнать всю необходимую информацию о сеансе, а также получить доступ к видеоаудиту сеанса.

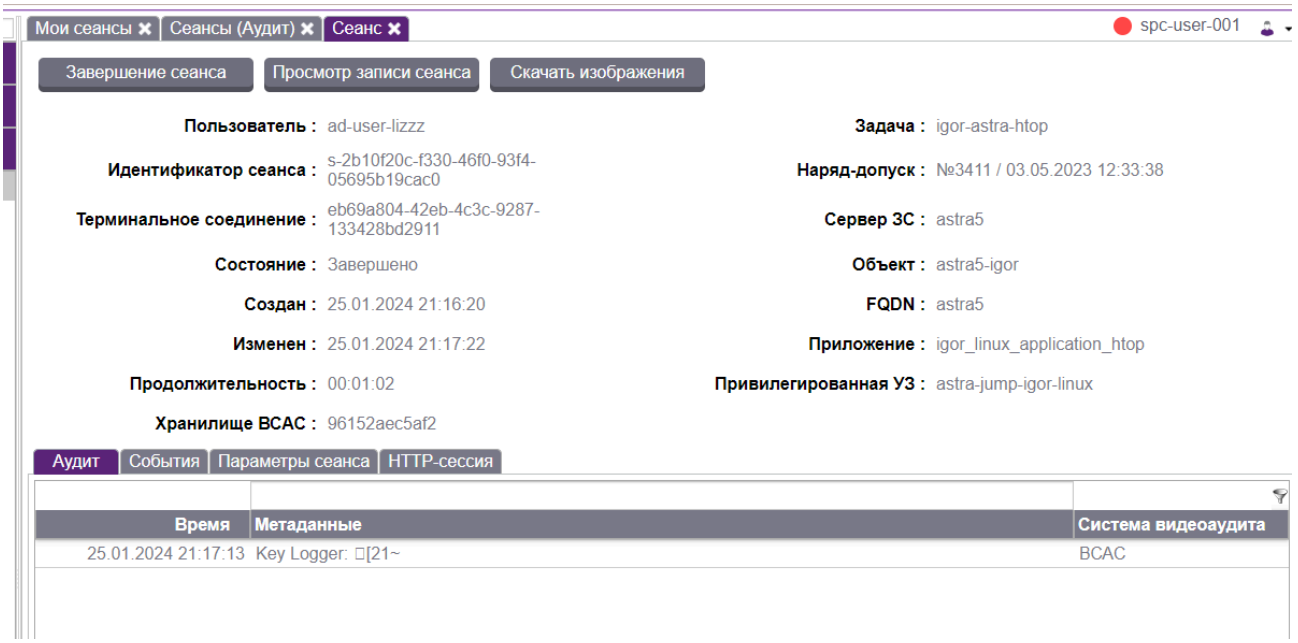


Рис. 4.1.5. Окно подробной информации о сеансе

4.1.5. Просмотр записи сеанса

Для просмотра видеозаписи сеанса необходимо кликнуть на странице сеанса на кнопку **Просмотр записи сеанса**.

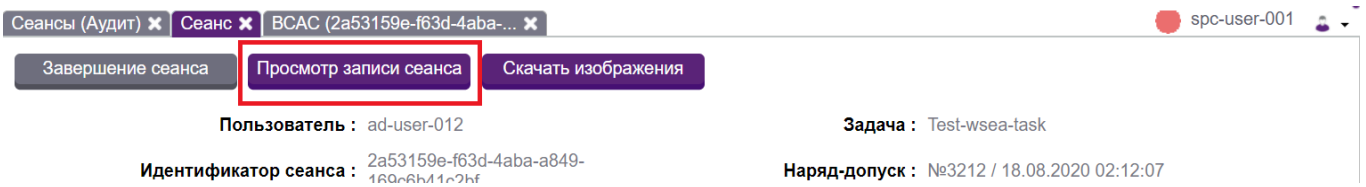


Рис. 160. Местонахождение кнопки «Просмотр записи сеанса»

После нажатия на эту кнопку откроется окно плеера с записанным сеансом.

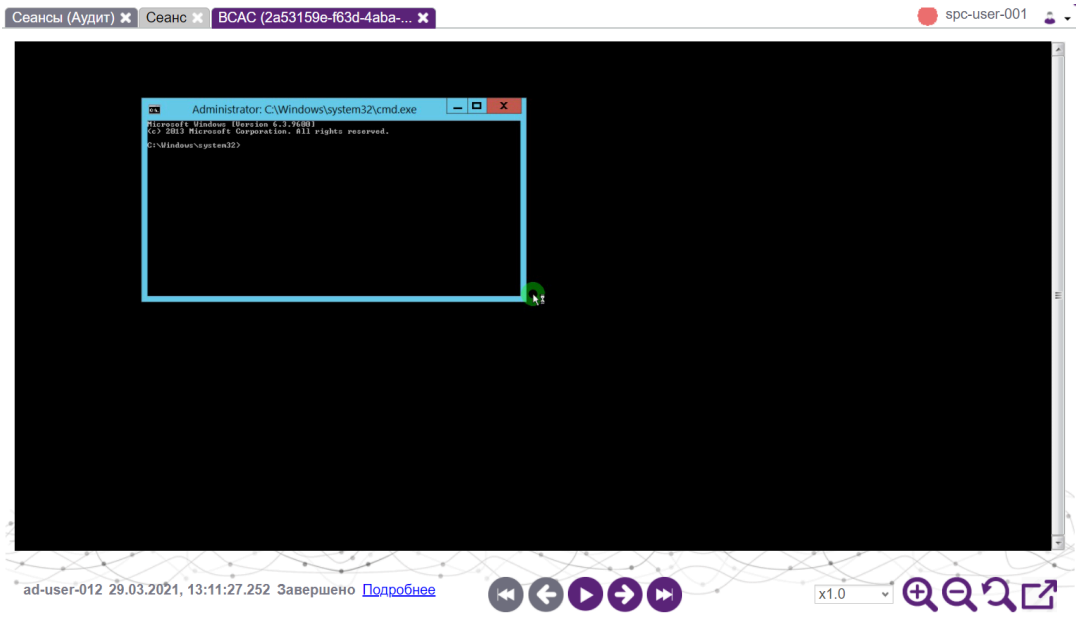


Рис. 4.1.6. Окно плеера

Чтобы узнать более полную информацию о сеансе, нужно нажать на надпись **Подробнее** внизу окна.

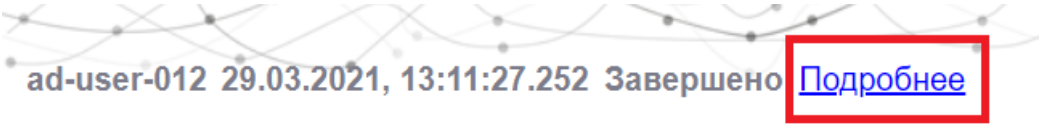


Рис. 4.1.7. Местонахождение кнопки «Подробнее»

После нажатия на эту кнопку на экране появится подробная информация о сеансе.

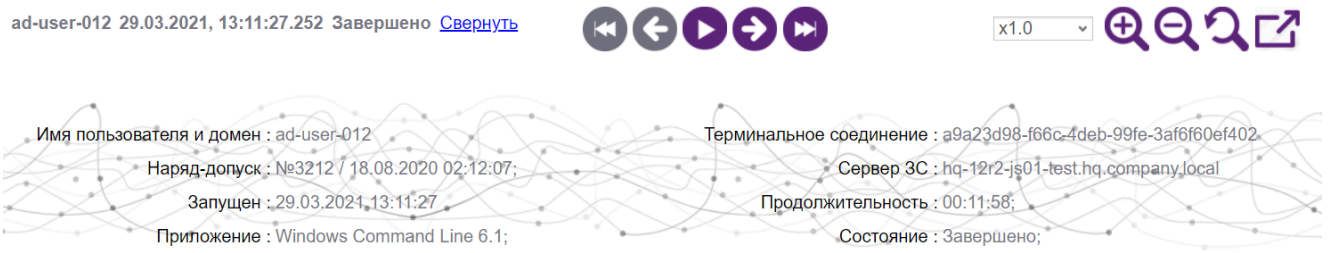


Рис. 4.1.8. Подробная информация о сеансе

При помощи кнопок под окном записанного сеанса можно осуществлять последовательную навигацию по записи: переместиться в ее начало, переместиться на один кадр назад, начать проигрывание записи по порядку с момента, на котором она сейчас остановлена, переместиться на один кадр вперёд, переместиться в конец записи.

Рис. 4.1.9. Кнопки навигации по записи сеанса

Кнопки справа внизу под окном записи сеанса позволяют удобнее просматривать данный сеанс:

- Выпадающий список с x1.0 и другими значениями позволяет увеличить скорость проигрывания записи;
- Кнопка лупа+ позволяет увеличить отображаемую в окне просмотра запись сеанса, а лупа- позволяет уменьшить ее;
- Лупа со стрелочкой вокруг сбрасывает масштабирование на начальное;
- Иконка с прямоугольником и стрелкой позволяет открыть окно просмотра сеанса в отдельной вкладке браузера.

Рис. 4.1.10. Кнопки параметров просмотра записи сеанса

В данный момент подробный плеер, описанный выше, доступен только в сеансах с графикой при типе подключения RDP. Если на сервере ЗС выбран тип подключения SSH, то плеер будет открываться в урезанном формате, только в виде последовательности скриншотов и без панели управления просмотром видеозаписи.

При открытии в отдельной вкладке окно просмотра будет выглядеть следующим образом:

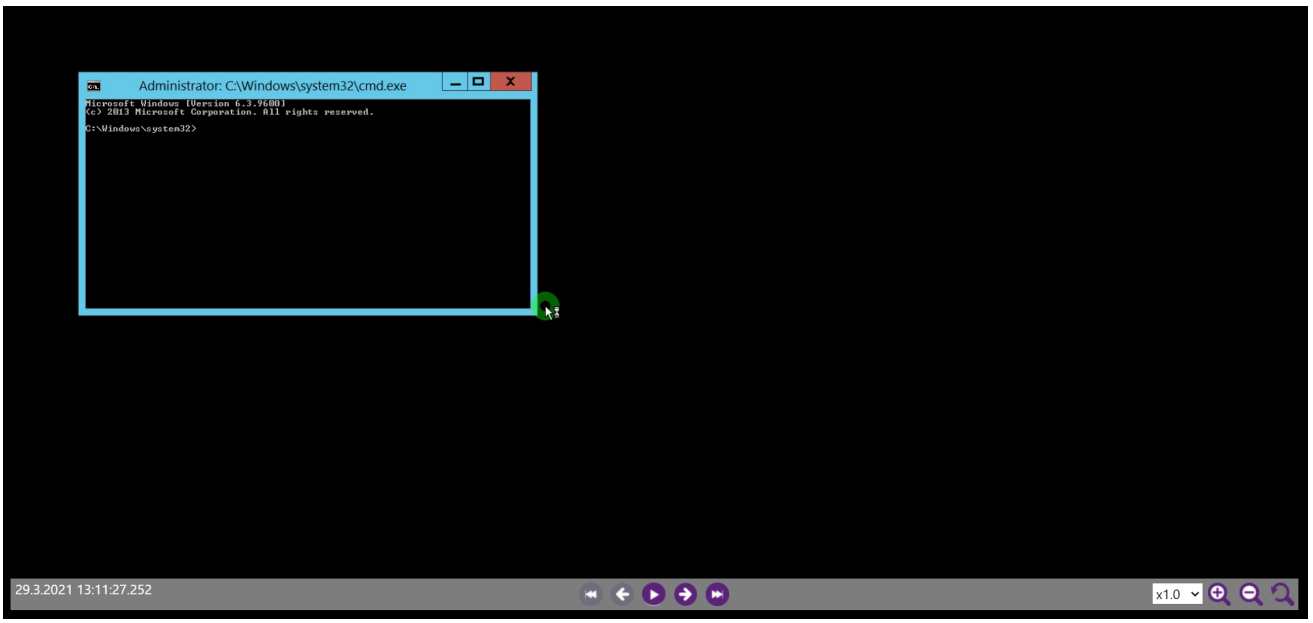


Рис. 4.1.11. Просмотр записи сеанса в отдельной вкладке браузера

Кнопки для управления просмотром в этом окне аналогичны описанным выше.

4.1.6. Просмотр записи работающего сеанса в режиме онлайн

sPACE позволяет просматривать видеозаписи не только завершённых сеансов, но и активных в данный момент. Интерфейс при онлайн просмотре записи работающего сеанса почти не различается с описанным выше просмотром записи из архива, но в нём добавляются дополнительные функции. Если сеанс находится в процессе выполнения, то карточка сеанса выглядит следующим образом:

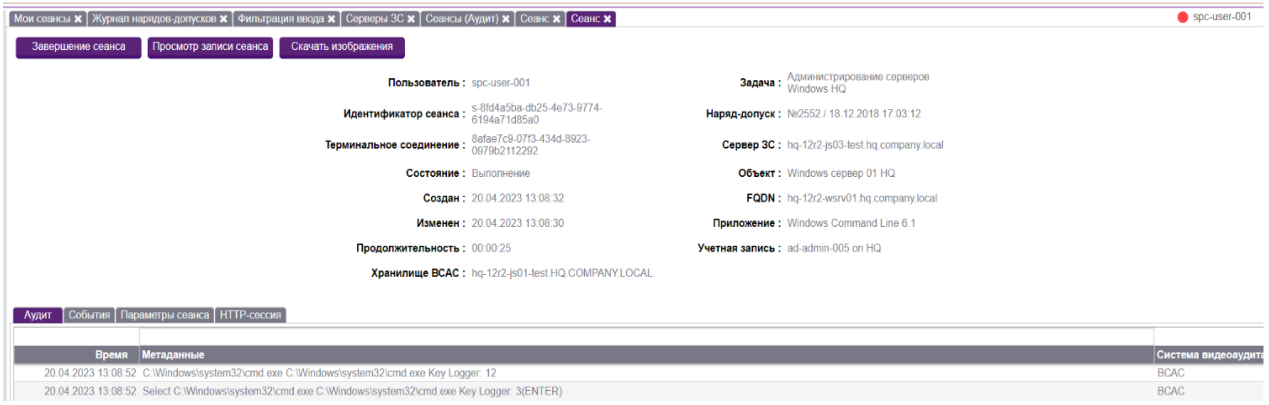


Рис. 4.1.12. Карточка сеанса, работающего в данный момент

После нажатия на кнопку **Просмотр записи сеанса** откроется плеер сеанса, он будет выглядеть следующим образом:

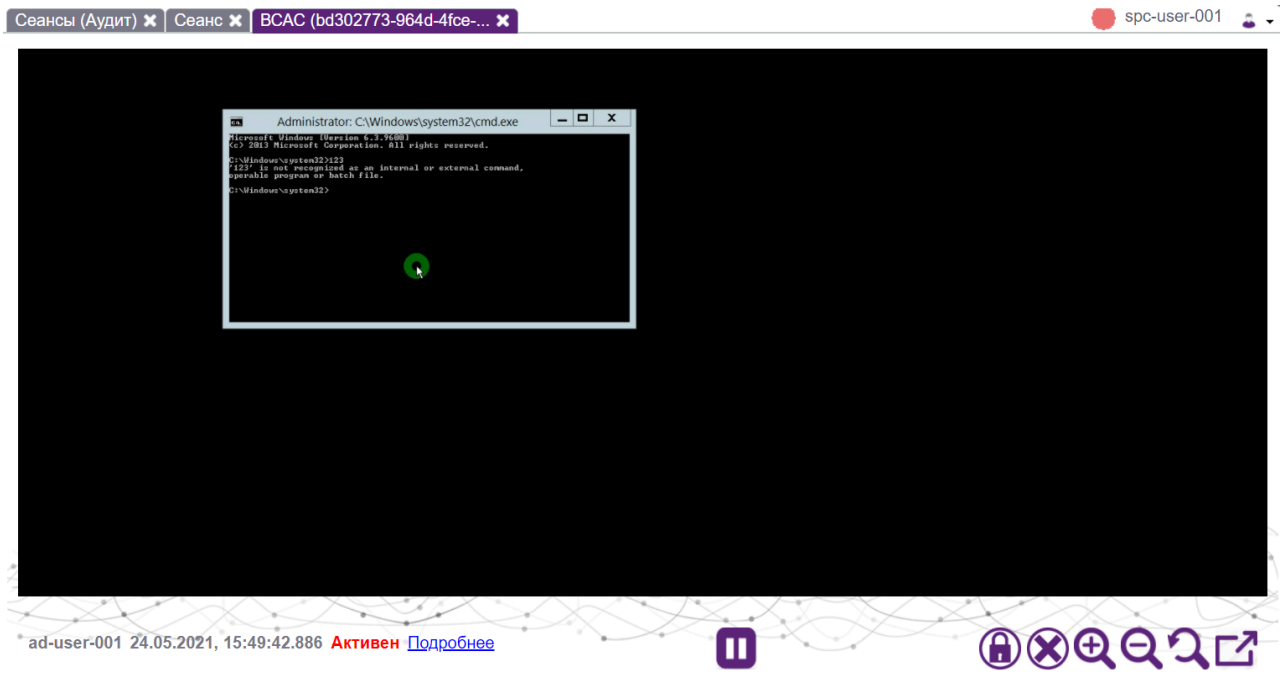


Рис. 4.1.13. Плеер сеанса, работающего в данный момент

В рабочей панели плеера доступны те же функции, что и при просмотре записанного сеанса: пауза, масштабирование, открытие в новой вкладке. Также появляются две новые функции: запрет пользовательского ввода для данного терминального соединения (значок с замочком) и экстренное завершение сессии (крестик). Эти же кнопки доступны также и в плеере в отдельной вкладке.

Рис. 4.1.14. Рабочая панель онлайн плеера

В данный момент подробный плеер, описанный выше, доступен только в сеансах с графикой при типе подключения RDP. Если на сервере ЗС выбран тип

подключения SSH, то плеер будет открываться в урезанном формате, только в виде последовательности скриншотов и без панели управления просмотром видеозаписи.

Для того, чтобы запретить пользовательский ввод для данного терминального соединения требуется нажать на значок с замочком и подтвердить действие. Тогда пользователь не сможет вводить данные с клавиатуры в этой сессии. Чтобы отменить это действие, необходимо вновь нажать на иконку с замочком.

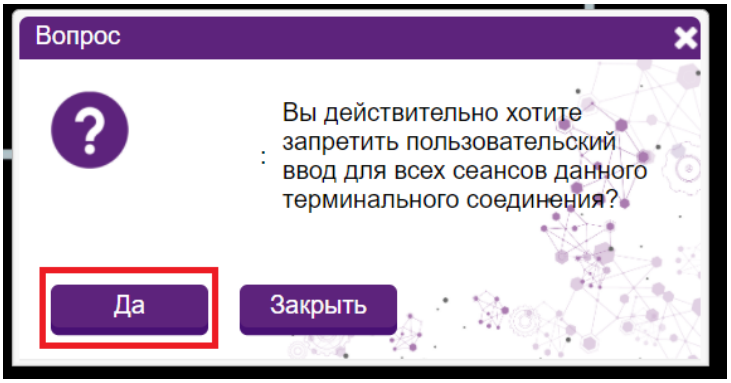


Рис. 4.1.15. Окно подтверждения запрета на пользовательский ввод

Если сеанс был завершен, пока аудитор его просматривал, то в интерфейсе sPACE будет выведено соответствующее уведомление. При нажатии на кнопку **Да** можно перейти к плееру для просмотра записи сеанса.

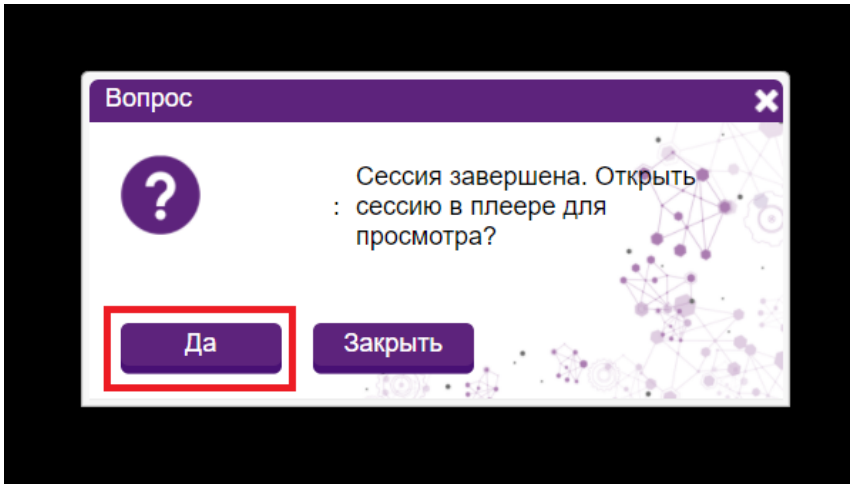


Рис. 4.1.16. Уведомление о завершении сеанса

4.1.7. Скачивание изображений сеанса

sPACE позволяет скачивать записанные скриншоты сеансов на компьютер аудитора. Для этого требуется нажать на кнопку "Скачать изображения" в карточке сеанса. После этого начнётся загрузка архива с изображениями сеанса.

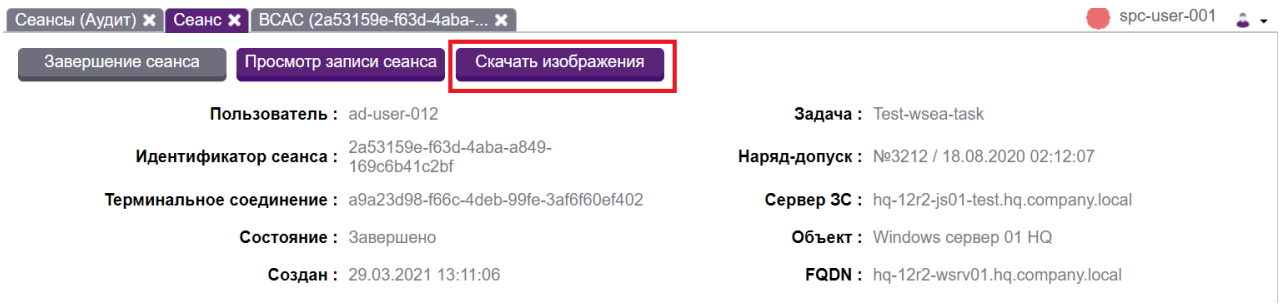


Рис. 4.1.17. Местоположение кнопки для скачивания скриншотов сеанса

4.1.8. Экстренное завершение работающего сеанса

Аудитор в sPACE имеет возможность экстренно завершить работающий сеанс, если со стороны пользователя будут замечены какие-либо неправомерные действия. Для этого есть несколько способов.

Первый способ - закрытие конкретного сеанса. Для этого нужно открыть карточку этого сеанса и нажать на кнопку **Завершение сеанса**. Затем будет показано соответствующее уведомление. Чтобы данный сеанс завершился, нужно нажать на кнопку **Да**.

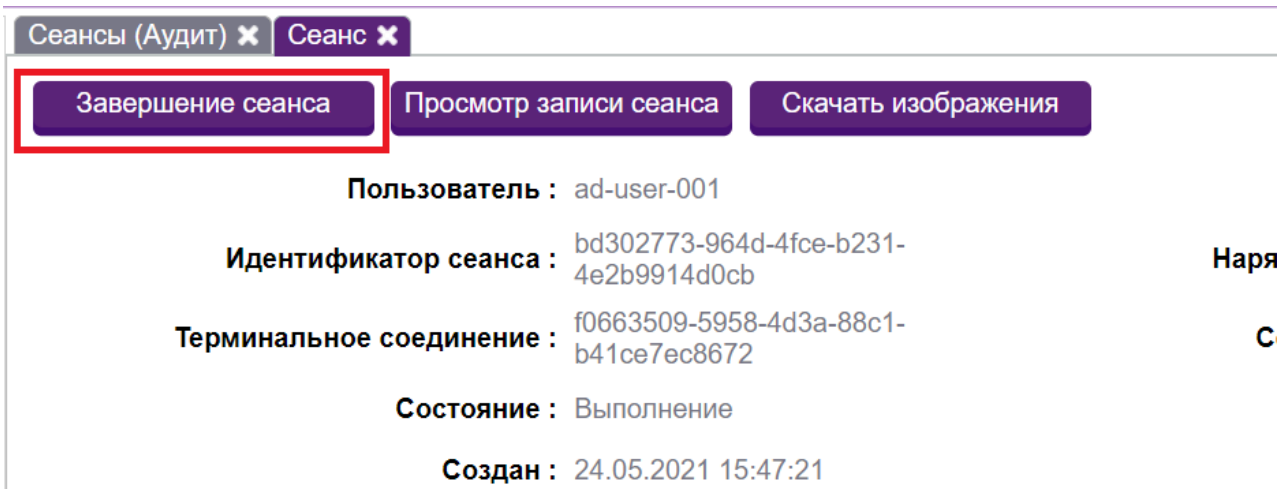


Рис. 4.1.18. Кнопка «Завершение сеанса»

Второй способ - завершение всех сеансов в данной сессии. Для этого нужно открыть плеер сеанса и нажать на кнопку с крестиком в рабочей панели плеера. Будет выведено уведомление. Чтобы завершить сессию, нужно нажать на кнопку **Да**.

Рис. 4.1.19. Местоположение кнопки для завершения всей активной сессии

4.1.9. Поиск по метаданным

Для поиска по метаданным необходимо ввести данные, которые требуется найти в текстовое поле **Поиск по метаданным** на странице со списком всех сеансов, затем задать временной период сеансов, по которым идет поиск, в полях "Период с" и "До", и нажать кнопку **Найти**. Для сброса этих полей необходимо нажать на кнопку **Сброс**.

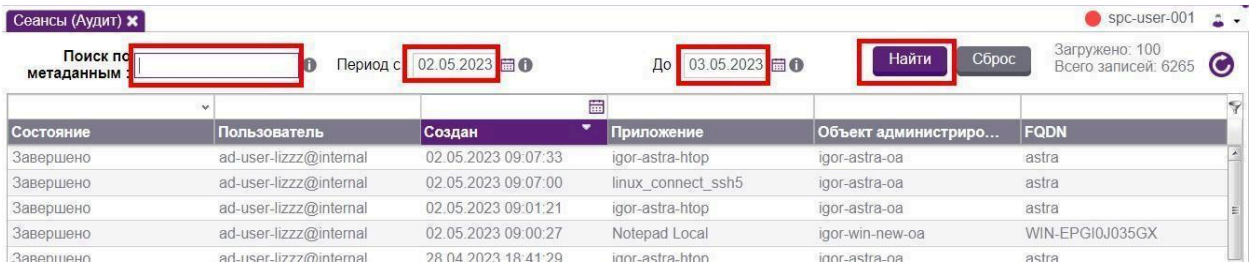


Рис. 175. Поиск по метаданным

4.1.10. Просмотр записи сеанса по данным Key Logger

Интерфейс позволяет просматривать записи по метаданным Key Logger с момента ввода этих данных. Для этого на странице данных сеанса необходимо перейти во вкладку **Аудит** и нажать на одно из записанных действий. После этого плеер сеанса откроется ровно на том моменте, когда было совершено это действие.

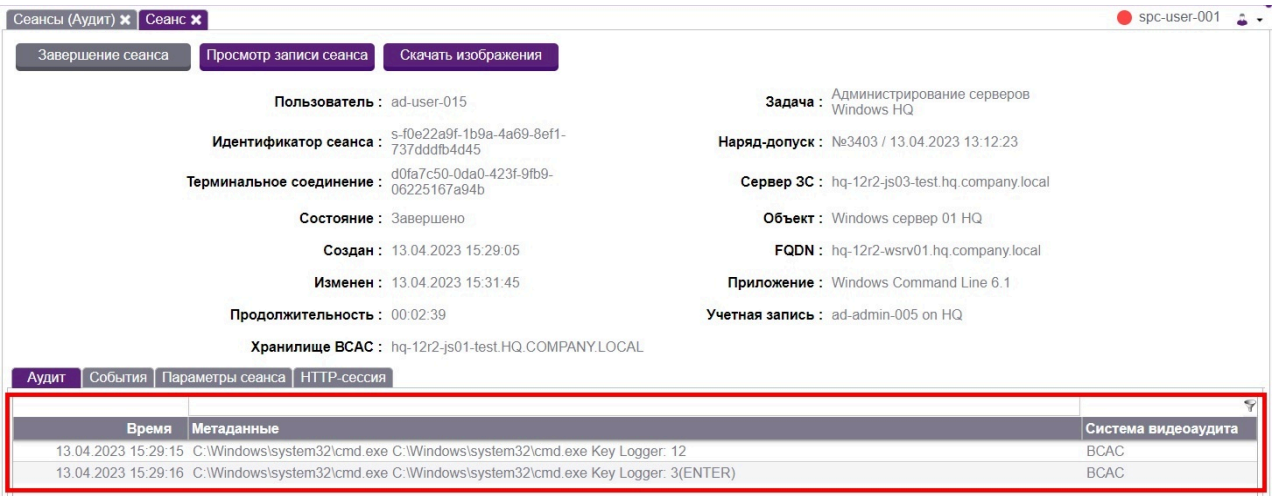
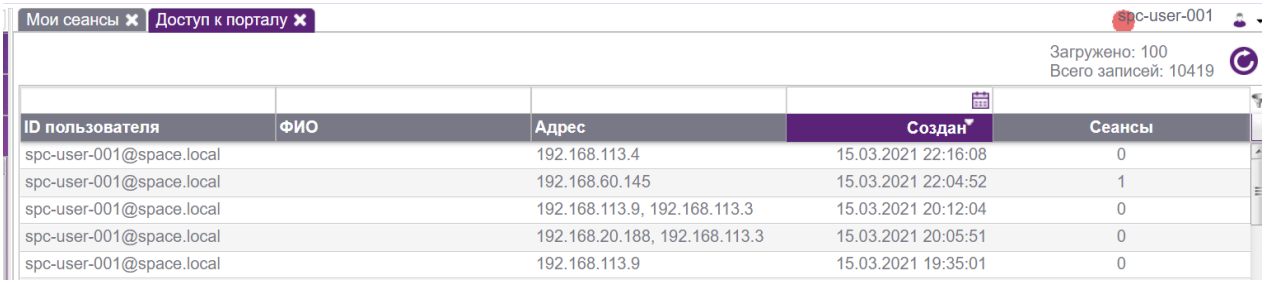


Рис. 176. Данные Key Logger

4.2. Осуществление аудита доступа к порталу

Вкладка **Доступ к порталу** служит для отображения информации по имеющимся в системе учетным записям пользователей и активным сессиям.

Внешне раздел представлен в виде таблицы с пятью столбцами: "ID пользователя", "ФИО", "Адрес", "Создан", "Сеансы".



ID пользователя	ФИО	Адрес	Создан	Сеансы
spc-user-001@space.local		192.168.113.4	15.03.2021 22:16:08	0
spc-user-001@space.local		192.168.60.145	15.03.2021 22:04:52	1
spc-user-001@space.local		192.168.113.9, 192.168.113.3	15.03.2021 20:12:04	0
spc-user-001@space.local		192.168.20.188, 192.168.113.3	15.03.2021 20:05:51	0
spc-user-001@space.local		192.168.113.9	15.03.2021 19:35:01	0

Рис. 4.2.1. Вкладка «Доступ к порталу»

В рамках данного раздела можно получить информацию о пользовательских сессиях:

- ID пользователя – идентификатор пользователя на портале и домен;
- ФИО – личные данные пользователя;
- Адрес – адрес, с которого производился доступ к порталу;
- Создан – дата и время авторизации этого пользователя;
- Сеансы – число запущенных сеансов.

4.2.1. Просмотр информации о пользовательской сессии

Для получения информации о пользовательской сессии необходимо щелкнуть дважды левой кнопкой мыши на запись в столбце **ID пользователя**. Будет выведено окно с информацией об этой сессии.

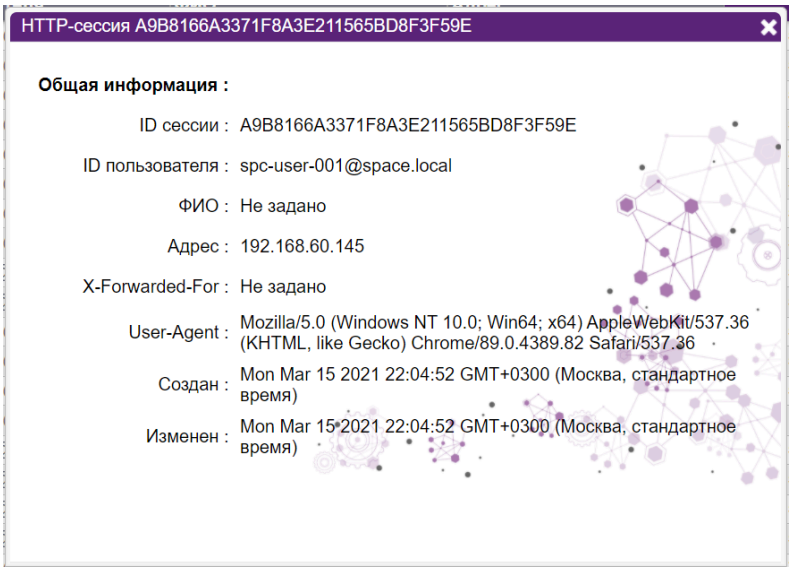


Рис. 4.2.2. Информация о пользовательской сессии

Описание полей:

- ID сессии – идентификатор сессии;
- ID пользователя – идентификатор пользователя на портале и домен;
- ФИО – личные данные пользователя;
- Адрес – адрес, с которого производился доступ к порталу. В случае изменения IP-адреса источника подключений к порталу данная информация фиксируется в этом поле, значения разделяются запятыми: ",";
- X-Forwarded-For – в данном поле фиксируются значения заголовка X-Forwarded-For (XFF). В случае изменения значения заголовка в ходе работы с порталом данная информация фиксируется, значения разделяются точкой с запятой: “;". В случае, если заголовок был удален или имел пустое значение, в данное поле будет добавлена запись “[none];”. Заголовок X-Forwarded-For является стандартным заголовком для идентификации происхождения IP-адреса клиента, подключающегося к веб-серверу через HTTP-прокси или балансировщик нагрузки. Когда трафик перехватывается между клиентами и серверами, журнал доступа в поле “Адрес“ имеет только IP-адреса прокси-сервера или балансировки нагрузки. Чтобы увидеть оригинальный IP-адрес клиента, используется заголовок запроса X-Forwarded-For. Формат значения заголовка: "<client>, <proxy1>, <proxy2>" (где <client> – IP-адрес клиента), "<proxy1>, <proxy2>" – если запрос проходит через несколько прокси-серверов, перечислены IP-адреса каждого последующего прокси-сервера. Это означает, что самый правый IP-адрес – это IP-адрес самого последнего прокси-сервера, а самый левый IP-адрес – это IP-адрес отправляющего клиента;
- User-Agent – браузер, через который произведена авторизация;
- Создан – дата и время авторизации этого пользователя;
- Изменен – дата и время последнего изменения в карточке сессии.

5. ОТКАЗОУСТОЙЧИВОСТЬ СИСТЕМЫ sPACE

5.1. Описание отказоустойчивости системы

Для обеспечения отказоустойчивой работы Системы используется 2+ Ядра. Одним из компонентов системы является СУБД PostgreSQL. СУБД работает по схеме: одна база main на первом ядре, копия базы main на втором (N-ом ядре). Дублирование информации на копии базы осуществляется за счёт NATS-сервера.

На случай выхода из строя первого ядра с базой main техническому администратору требуется вручную прописать в настройках путь ко второй (N-ой) копии базы на другом ядре и перезагрузить все ядра с изменениями. Теперь база main находится на втором (N-ом) ядре, а базы на остальных ядрах являются копиями.

В дальнейшем, при восстановлении работоспособности первого ядра, все новые данные с базы main, расположенной на втором (N-ом) ядре, будут автоматически скопированы в базу данных на первом ядре. На этом этапе можно восстановить статус базы main на первом ядре, либо оставить базу main на втором (N-ом) ядре. В последнем случае необходимо на первом ядре в настройках указать путь к расположению базы на втором (N-ом) ядре и запустить перезагрузку.

5.2. Управление отказоустойчивостью системы

5.2.1. Изменить расположение базы main

В случае выхода из строя первого Ядра с базой main, указать адрес PostgreSQL в файле core.properties, доступном на втором (N-ом) Ядре Linux в папке “/var/opt/space/config”. Параметр “hikaricp.dataSource.url” должен указывать на нынешнюю рабочую базу данных, то есть, расположенную на втором (N-ом) Ядре.

Далее перезагрузить все Ядра, на которых были внесены изменения, командой “sudo docker restart spacetomcat8”.

5.2.2. Восстановить расположение базы main на первом Ядре

После восстановления работоспособности первого Ядра, чтобы вернуть расположение базы main на первое Ядро, необходимо изменить настройки по указанному ранее пути на втором (N-ом) Ядре. Параметр “hikaricp.dataSource.url” должен указывать на прежнюю рабочую базу данных, то есть расположенную на первом Ядре. Далее перезагрузить все Ядра, на которых были внесены изменения, командой “sudo docker restart spacetomcat8”.

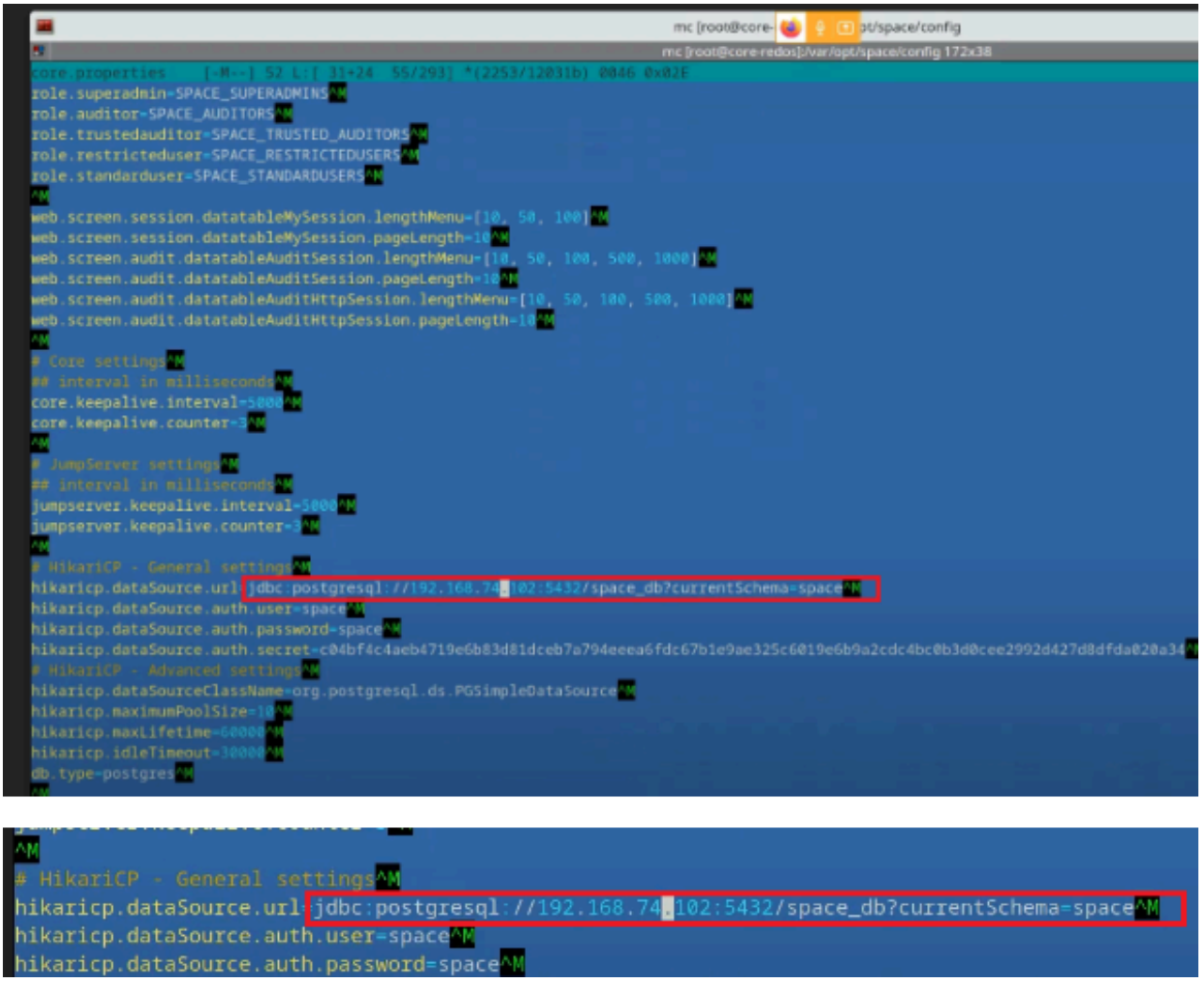


Рис. 171. Изменение параметра расположения базы main

5.2.3. Изменить расположение базы main на первом Ядре

После восстановления работоспособности первого Ядра, чтобы перенастроить расположение базы main на первом Ядре, необходимо изменить настройки по указанному ранее пути на первом Ядре. Параметр “hikaricp.dataSource.url” должен указывать на новую рабочую базу данных, то есть расположенную на втором (N-ом) Ядре. Далее перезагрузить первое Ядро командой “sudo docker restart spacetomcat8”.

6. ПРОВЕРКА sPACE

Проверка работоспособности Системы осуществляется посредством выполнения серии проверок.

6.1. Проверка изоляции сеансов ПД

Сотрудник с ролью Пользователь должен авторизоваться в Портале Системы и продемонстрировать открытие инструмента администрирования на сервере ЗСА:

- Выполнить запуск сеанса, выбрав объект администрирования;
- Выполнить запуск сеанса, выбрав другой объект администрирования;
- Убедиться в том, что оба сеанса были запущены в одном терминальном соединении;
- Убедиться, что в Системе появилась корректная информация о запущенных сеансах.

Результат будет засчитан положительным, если стартующее приложение предварительно отображает окна инициализации RemoteApp, после чего успешно открывается. На рабочей станции пользователя оригинальное имя процесса запущенного приложения не отображается. В узле **Сеансы** раздела **Управление системой** отображаются одинаковые параметры соединения (поле **Соединение**) и корректное отображение их состояния (поле **Выполнение**).

6.2. Отслеживание в реальном времени выполняемых работ

Перед выполнением проверки необходимо убедиться, что в Системе ранее запускались сеансы ПД к объектам администрирования и выполнялись некоторые действия. Аудитор Системы должен авторизоваться на Портале Системы, открыть узел **Сеансы** раздела **Аудит** и продемонстрировать возможность просмотра сеансов, отфильтровать все сеансы по состоянию, затем отфильтровать все сеансы по полю **Выполнение**, затем запустить новый сеанс с ролью Пользователя и обновить таблицу узла **Сеансы** раздела **Аудит**. После этого Аудитор должен продемонстрировать карточку сеанса и запустить просмотр видеозаписи сеанса.

Результат будет засчитан положительным, если Аудитор продемонстрирует таблицу узла **Сеансы** раздела **Аудит**, в которой отображаются сеансы, запускаемые ранее и выполняемые в настоящий момент, а также отобразит только выполняемые в момент испытания сеансы. Затем оператор должен запустить просмотр видеозаписи сеанса, в которой отобразятся выполненные ранее действия.

6.3. Проверка возможности добавления новых объектов администрирования

Администратор должен авторизоваться в Системе, добавить несколько новых объектов администрирования и типов объекта администрирования, создать или отредактировать группу согласования для данных объектов/типов объектов, затем добавить задачи для новых объектов администрирования, запросить НД, авторизовавшись с правами «Пользователя», и согласовать НД, авторизовавшись с правами «Администратора».

Результат будет засчитан положительным, если оператор продемонстрирует таблицы **Список объектов** и **Список типов объектов администрирования** узла **Объекты администрирования** раздела **Управление системой**, в которых отображаются добавленные объекты и типы объектов администрирования, а также согласованный НД.

7. РЕЗЕРВНОЕ КОПИРОВАНИЕ

Полное резервное копирование данных должно осуществляться не менее одного раза в неделю. Инкрементальное резервное копирования должно осуществляться ежедневно. Рекомендуется сохранять последние три резервные копии данных Системы. В случае географически распределенного размещения Системы резервные копии должны храниться в каждом ЦОД, где установлены компоненты Системы.

Все компоненты системы могут быть переустановлены путем запуска процесса инсталляции. При этом функционирование работоспособных компонентов затронута не будет. Сервер очередей сообщений представляет собой кластер, который сохраняет работоспособность в случае отказа части компонентов.

Данные о конфигурации компонентов хранятся частично на дисковых системах серверов, на которых эти компоненты установлены, и могут быть сохранены как отдельные файлы, так и вместе с прочими данными во время резервного копирования.

Данные о конфигурации и прочие данные системы, хранящиеся в базах данных, могут быть сохранены как путем резервного копирования соответствующих баз данных, так и путем резервирования другими средствами, доступными для баз данных (синхронизация с другими серверами), а также путем созданий полных резервных копий всех серверных систем, на которых установлена соответствующая СУБД.

8. ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ API

Для взаимодействия с системами сторонних производителей в sPACE реализован администрированием API следующих типов:

- Component management — конфигурация компонентов системы.
    - Регистрация компонентов
    - Управление конфигурацией компонентов
    - Управление паролями привилегированных УЗ
- DATA management – конфигурация тенанта или синхронизация данных об объектах с внешними системами:
    - Агенты рандомизации паролей;
    - Пользователи и группы пользователей;
    - Домены;
    - Задачи;
    - Наряды-допуски;
    - Объекты администрирования и их типы;
    - Привилегированные учетные записи;
- Resource management — конфигурация системы или синхронизация данных об объектах с внешними системами:
    - Системы видеоаудита;
    - Интерпретаторы;
    - Параметры запуска и их типы;
    - Приложения, их сценарии запуска и экземпляры;
    - Серверы ЗС;
- System audit API – выгрузка данных о логах и сеансах во внешние системы безопасности.